A Unifying Framework to Construct QC-LDPC Tanner Graphs of Desired Girth

Roxana Smarandache, *Senior Member, IEEE*, and David G. M. Mitchell, *Senior Member, IEEE*

***Abstract*—This paper presents a unifying framework to construct low-density parity-check (LDPC) codes with associated Tanner graphs of desired girth. Towards this goal, we highlight the role that a certain square matrix that appears in the product of the parity-check matrix with its transpose has in the construction of codes with graphs of desired girth and further explore it in order to generate the set of necessary and sufficient conditions for a Tanner graph to have a given girth between 6 and 12. For each such girth, we present algorithms to construct codes of the desired girth and we show how to use them to compute the minimum necessary value of the lifting factor. For girth larger than 12, we show how to use multi-step graph lifting methods to deterministically modify codes in order to increase their girth. We also give a new perspective on LDPC protograph-based parity-check matrices by viewing them as rows of a parity-check matrix equal to the sum of certain permutation matrices and obtain an important connection between all protographs and those with variable nodes of degree 2. We also show that the results and methodology that we develop for the all-one protograph can be used and adapted to analyze the girth of the Tanner graph of any parity-check matrix and demonstrate how this can be done using a well-known irregular, multi-edge protograph specified by the NASA Consultative Committee for Space Data Systems (CCSDS). Throughout the paper, we exemplify our theoretical results with constructions of LDPC codes with Tanner graphs of any girth between 6 and 14 and give sufficient conditions for a multi-step lifted parity-check matrix to have girth between 14 and 22.**

***Index Terms*—Low-density parity-check (LDPC) codes, quasi-cyclic codes, girth, protograph, Tanner graph.**

I. Introduction

LOW-DENSITY parity-check (LDPC) codes, in particular quasi-cyclic LDPC (QC-LDPC) codes, are now found in many industry standards. One of the main advantages of QC-LDPC codes is that they can be described simply, and as such are attractive for implementation purposes since they can be encoded with low complexity using simple feedback shift-registers [2] and their structure leads to efficiencies in decoder design [3]. The performance of an LDPC code with parity-check matrix H depends on cycles in the associated Tanner graph, since cycles in the graph cause correlation during iterations of belief propagation decoding [4]. Moreover, these cycles form substructures found in the undesirable trapping and absorbing sets that create the error floor. Cycles have also been shown to decrease the upper bound on the minimum distance (see, e.g., [5]). Therefore, codes with large girth are desirable for good performance (large minimum distance and low error floor). Significant effort has been made to design QC-LDPC code matrices with large minimum distance and girth, see [6]–[13] and references therein.

In this paper, we will start from a previous theorem by McGowan and Williamson [14] and the terminology introduced in Wu *et al.* [15] that elegantly relate the girth of H with the girth of $B_t(H) \triangleq \left(HH^\top\right)^{\lfloor t/2 \rfloor} H^{(t \bmod 2)}$, $t \geq 1$, which we state as Theorem 2. The paper [15] uses this theorem to construct an LDPC code with a binomial protograph that has good performance. We take this connection in a different direction: we show how, when applied to a matrix in a general standard form, it yields the necessary and sufficient conditions on the sets of exponents in order for H to attain a desired girth $4 < g \leq 12$. Therefore, we exploit the necessary and sufficient condition given by Theorem 2 in order to obtain *necessary and sufficient conditions* on the sets of exponents which, in turn, we use to generate extremely fast algorithms to construct codes with desired girths. Therefore, the novelty of this paper consists in realizing a previously unstated potential of the theorem. We exemplify this potential on a variety of protographs and showed how one can obtain fast algorithms to construct codes of desired girth. In doing so, we are not trying to compete with any of the codes from the large body of literature on this topic, but use these examples to raise awareness of this technique that can be used to simplify the task of construction and analysis of such codes.

A. Contributions of the Paper

The contributions of the paper are as follows. In Section III, we derive an equivalent statement of Theorem 2, and in doing so we showcase a submatrix C_H of $HH^\top$ of relevance when looking for cycles in the Tanner graph of H. Specifically, we show that the girth of a Tanner graph of an $n_cN \times n_vN$ parity-check matrix H based on the (n_c, n_v)-regular fully connected (all-one) protograph, with lifting factor N, is directly

Manuscript received 7 July 2021; revised 29 November 2021; accepted 11 April 2022. Date of publication 25 April 2022; date of current version 18 August 2022. This work was supported by the National Science Foundation under Grant CCF-2145917, Grant CNS-2148358, Grant HRD-1914635, and Grant OIA-1757207. An earlier version of this paper was presented in part at the 2021 IEEE International Symposium on Information Theory [1] [DOI: 10.1109/ISIT45174.2021.9518241]. *(Corresponding author: David G. M. Mitchell.)*

Roxana Smarandache is with the Department of Mathematics and Electrical Engineering, University of Notre Dame, Notre Dame, IN 46556 USA (e-mail: rsmarand@nd.edu).

David G. M. Mitchell is with the Klipsch School of Electrical and Computer Engineering, New Mexico State University, Las Cruces, NM 88003 USA (e-mail: dgmm@nmsu.edu).

Communicated by R. D. Wesel, Associate Editor for Coding Techniques.

Color versions of one or more figures in this article are available at https://doi.org/10.1109/TIT.2022.3170331.

Digital Object Identifier 10.1109/TIT.2022.3170331

related to the properties of the product $C_H^{\lfloor t/2 \rfloor} H^{(t \mod 2)}$, $t \geq 1$, and then further exploit this connection in order to give the sets of necessary and sufficient conditions for a QC-LDPC code based on an $n_c \times n_v$ all-one protograph, with $n_c = 2, 3$, and 4, respectively, to have any girth between 6 and 12.[1] These conditions are then used to write fast algorithms to construct codes of such desired girth.[2]

We also show that, when constructing parity-check matrices of girth larger than $2l$, we need to consider all $l \times n_v$ submatrices and impose the girth conditions on them. In particular, if we want to construct $n_cN \times n_vN$ protograph-based parity-check matrices of girth larger than 4, 6, and 8, respectively, it is necessary and sufficient to give the girth conditions for the cases $n_c = 2$, 3, and 4, respectively. It follows from these observations that the cases $n_c = 2$, 3, and 4 that we consider in this paper are not just particular cases, but provide the girth framework for the $n_c \times n_v$ all-one protograph, for *all* $n_c \geq 2$.

We also give a new perspective on $n_cN \times n_vN$ LDPC protograph-based parity-check matrices by viewing them as n_cN rows of a parity-check matrix equal to the sum of certain $n_vN \times n_vN$ permutation matrices. Together with our results that the cycles in the Tanner graph of a $2N \times n_vN$ parity-check matrix H based on the $(2, n_v)$-regular fully connected (all-one) protograph correspond one-to-one to the cycles in the Tanner graph of a $N \times N$ matrix C_{12}, obtained from H by adding certain permutation matrices in its composition, we obtain an important connection between $n_c \times n_v$ protographs, for any $n_c \geq 2$, and protographs with check-node degree $n_c = 2$. Therefore, although the case of $2 \times n_v$ protographs seems of limited practical importance on its own or important only as part of a larger protograph, with this above-mentioned new perspective, it is in fact relevant in connection to any $n_c \times n_v$ protograph. In addition, square $n_vN \times n_vN$ parity-check matrices equal to sums of permutation matrices have enjoyed a lot of attention in the context of projective geometry codes [6], [16], [17], so they are important as well.

Although we mostly assume the case of an (n_c, n_v)-regular fully connected protograph, the results and methodology can be used and adapted to analyze the girth of the Tanner graph of any parity-check matrix. We exemplify how this can be done using an irregular, multi-edge protograph (with entries 0, 1, 2 rather than just 1 as in the all-one protograph) specified by the NASA Consultative Committee for Space Data Systems (CCSDS) [18], [19]. Here, we show how to obtain the matrix C_H and how the results from the all-one protograph can be adapted to this type of protograph to give the necessary and sufficient girth conditions.

We also extend our results and methodology to obtain codes with girth larger than 12. QC-LDPC Tanner graphs directly circularly lifted from a protograph containing a 2×3 all-one sub-protograph, referred to as a QC lifting, cannot be considered anymore, see, e.g., [5], therefore, we need to consider a matrix composed of permutation matrices such that some are not circulant. In order to obtain an increase in girth beyond the restrictive upper bound 12 (and/or increased minimum distance), we demonstrate how a deterministic multi-step graph lifting approach, called pre-lifting [11], can be applied. Towards this goal, we first show that any $n_cN \times n_vN$ circularly lifted graph (defining an arbitrary QC-LDPC code) with $N = N_1N_2$ is equivalent to a graph derived from a $n_c \times n_v$ protograph, circularly pre-lifted with a (first) lifting factor N_1 and then circularly lifted with a (second) lifting factor equal to N_2. We then show and exemplify for $n_c = 3$ that graphs of $n_cN \times n_vN$ parity-check matrices can be pre-lifted in a deterministic way in order to increase their girth and/or minimum distance, whereby exponents are modified to break the (circular) limiting structure of the original QC-LDPC code. We used this approach to construct QC-LDPC codes of girth 14 starting from certain QC-LDPC codes of girth 10 or 12 that we deterministically choose such that their equivalent structures in which the pre-lifts are observed allow for slight modifications of the exponents to yield a girth increase. We also give sufficient conditions for a pre-lift to allow for girth from between 14 and 22.

The structure of the paper is as follows. Section II contains the background results and needed terminology, while Section III exploits these results to show how the girth of H is directly related to the properties of the product $C_H^{\lfloor t/2 \rfloor} H^{(t \mod 2)}, t \geq 1$, and how this connection can be used to obtain necessary and sufficient conditions on H to have girth larger than 4, 6, and 8.

In Sections IV and V we give the sets of necessary and sufficient conditions for a QC-LDPC code based on an $n_c \times n_v$ all-one protograph, $n_c = 2, 3, 4$, to have any girth between 6 and 12, and use them to write fast algorithms to construct codes of such desired girth. We also present a new perspective on $n_cN \times n_vN$ LDPC protograph-based parity-check matrices by viewing them as n_cN rows of a parity-check matrix equal to the sum of certain $n_vN \times n_vN$ permutation matrices. In Section V-B, exemplified in the case $n_c = 3$, we extend our results and methodology to obtain codes with girth larger than 12 by considering a 2-step lifting method, and give sufficient conditions for a pre-lift in order to allow for girth from 14 to 22. In Section VI, we show how to obtain the matrix C_H for an irregular, multi-edge protograph used in the NASA CCSDS LDPC code and how to adapt the results for the all-one (regular, single-edge) protograph to this irregular protograph. We then exemplify the modified approach by giving the necessary and sufficient conditions for this protograph to have girth larger than 4. Section VII contains computer simulations of some of these codes, confirming the expected robust error control performance, while Section VIII contains concluding remarks. Lastly, Appendices B and C revisit two of the examples in the paper, Examples 3 and 13,

[1] We note that the necessary and sufficient conditions to obtain a code with no 4-cycles, or equivalently, $HH^T \triangle I = 0$ (see Section II), have been addressed and solved previously in the literature; e.g., the condition $HH^T \triangle I = 0$ is known largely as the row-column (RC)-constraint. However, there are no such results regarding the conditions for the girth to be larger than 6, 8 and 10. In addition, our technique yields the conditions in a compact form and as part of a general classification. Despite not being new, we included the first case of $g > 4$ for completeness of our classification and to emphasize how easily and elegantly it is yielded by applying the theory.

[2] As detailed in the numerical results, the algorithm run-times are typically a fraction of a second, and in all cases in this paper run in less than 2 seconds on a standard laptop computer.

respectively, in order to show how the pre-lifting techniques presented in Section V-B can be used to obtain a girth increase and, possibly, a minimum distance increase.

We emphasize that what we present is a unifying framework, in the sense that every previous construction of codes of a certain girth must fit in this framework, since we provide *the* set of *necessary* and sufficient conditions for a given girth to be achieved. The construction papers so far have given sufficient conditions for a code to have Tanner graphs of a certain girth. For example, the literature on eliminating 4-cycles in LDPC codes by choosing the exponents from difference sets is large [20]–[24]. It is what we do, and it is, in fact, what the Fossorier conditions, displayed here in Corollary 4, do as well. The novelty of this paper is that it shows that these are not only sufficient but also necessary conditions in order to get girth 6 and it provides in a simple minimal format all the conditions that the differences of the exponents must satisfy in order to result in a code of Tanner graph of girth 6, 8, 10, and 12, respectively. In addition, the set of minimal conditions for a desired girth allows for our proposed algorithms to choose lifting exponents to be extremely fast (less than 2 seconds in all considered cases) - in fact they can be evaluated by hand. Lastly, if desired, they can display codes of a given girth for the smallest graph lifting factor N. Therefore, we do not exhaustively visit other constructions found in the literature because of this very different scope of our paper. Although we mostly assume the case of an (n_c, n_v)-regular fully connected protograph, for $n_c = 2, 3$, and 4, the results can be used to analyze the girth of the Tanner graph of any parity-check matrix. We note that the theory would need to be suitably adapted; this is addressed and exemplified in Section VI.

II. Definitions, Notation, and Background

As usual, an LDPC code $\mathcal{C}$ is described as the null space of a parity-check matrix H to which we associate a Tanner graph [25] in the usual way. The girth of the graph of H, denoted by $\mathrm{girth}(H)$, is the length of the shortest cycle(s) in the graph. If a matrix has an entry larger than 1 then we say the corresponding graph has multiple edges between a pair of nodes. We say that a graph has girth 2 if it has multiple edges.[3]

A protograph [19], [26] is a small bipartite graph represented by an $n_c \times n_v$ biadjacency matrix[4] $B_{n_c \times n_v}$ with non-negative integer entries b_{ij}, which we also refer to as a protograph. The parity-check matrix H_{n_c} (or H when n_c is clear from the context) of an LDPC block code based on the protograph $B_{n_c \times n_v}$ can be created by replacing each non-zero entry b_{ij} by a sum of b_{ij} non-overlapping $N \times N$ permutation matrices 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. We call the resulting code a *protograph-based* LDPC code.

Throughout the paper, we use, for any positive integer L, the notation $[L]$ to denote the set $\{1, 2, \ldots, L\}$, while, for any set, we say that it has *maximal size* if all the possible values that can be generated for the set should be distinct.

A special notation used throughout the paper is the elegant triangle operator introduced in [15] between any two non-negative integers $e, f \in \mathbb{Z}$ to define

$$d \triangleq e \triangle f \triangleq \begin{cases} 1, & \text{if } e \geq 2, f = 0 \\ 0, & \text{otherwise} \end{cases},$$

and between two $s \times t$ matrices $E = (e_{ij})_{s \times t}$ and $F = (f_{ij})_{s \times t}$ with non-negative integer entries, to define the matrix $D = (d_{ij})_{s \times t} \triangleq E \triangle F$ entry-wise as $d_{ij} \triangleq e_{ij} \triangle f_{ij}$, for all $i \in [s], j \in [t]$.

We denote the $N \times N$ circulant permutation matrix where the entries of the $N \times N$ identity matrix I are shifted to the left by r positions modulo N, as x^r. Note that 0 and $1 = x^0$ correspond to the all-zero and identity matrices, respectively, where the dimensions are implied by the context. We say that a (permutation) matrix P has *a fixed column (or row)*, and write $(P + I) \triangle 0 \neq 0$,[5] if it overlaps with the identity matrix in at least one column (or row). It follows that any two permutation matrices P and Q have no common column if and only if $(P + Q) \triangle 0 = 0 \Leftrightarrow \left(PQ^{\mathsf{T}} + I\right) \triangle 0 = 0 \Leftrightarrow \left(P^{\mathsf{T}} Q + I\right) \triangle 0 = 0 \Leftrightarrow \left(Q^{\mathsf{T}} P + I\right) \triangle 0 = 0 \Leftrightarrow \left(P^{\mathsf{T}} + Q^{\mathsf{T}}\right) \triangle 0 = 0$ where the matrix addition is performed over $\mathbb{Z}$. In addition, $(P + I) \triangle 0 = 0 \Leftrightarrow (P^i + I) \triangle 0 = 0$, for all integers $i \geq 1$. Lastly, we state the following property in a lemma, since it will be used repeatedly in our results.

Lemma 1: Let $A = (a_{ij})_{s \times t}$ and $B = (b_{ij})_{s \times t}$ be two matrices with non-negative integer entries, then the equality $(A + B) \triangle A = B \triangle A$ holds.

Proof: The claim follows from the entry-wise equalities.

$$(a_{ij} + b_{ij}) \triangle a_{ij} = \begin{cases} 1, & \text{if } a_{ij} + b_{ij} \geq 2, a_{ij} = 0, \\ 0, & \text{otherwise,} \end{cases} =$$

$$\begin{cases} 1, & \text{if } b_{ij} \geq 2, a_{ij} = 0, \\ 0, & \text{otherwise,} \end{cases} = b_{ij} \triangle a_{ij}.$$

■

The triangle operator is used also in the following theorem of [14] and [15] to describe an important connection between $\mathrm{girth}(H)$ and matrices $B_t(H) \triangleq \left(HH^{\mathsf{T}}\right)^{\lfloor t/2 \rfloor} H^{(t \mod 2)}, t \geq 1$. This connection forms the base of our paper.

Theorem 2 ([14] and [15]): A Tanner graph of an LDPC code with parity-check matrix H has $\mathrm{girth}(H) > 2l$ if and only if $B_t(H) \triangle B_{t-2}(H) = 0, t = 2, 3, \ldots, l$.

Lastly, we extend [27], Theorem 2, on cycles in all-one protographs that gives the algebraic conditions imposed by a cycle of length $2l$ in the Tanner graph of an all-one protograph-based LDPC code, to the more general case of any protograph, irregular or/and multi-edge.

[3] A note of caution when using the Magma program to compute the girth of a graph with multiple edges: the command "gir" does not output 2 for the girth of a graph with multiple edges; it outputs the size of the smallest cycle in the single-edge graph obtained from the original by considering each multiple edge as a single edge.

[4] The biadjacency matrix of a finite bipartite graph G with n left vertices and m right vertices is an $n \times m$ matrix where the entry a_{ij} is the number of edges joining left vertex i and right vertex j.

[5] The matrix addition is performed over $\mathbb{Z}$.

Theorem 3: Let C be a code described by a protograph-based parity-check matrix H where each (i,j) entry is the $N \times N$ zero matrix or a sum of $N \times N$ non-overlapping permutation matrices. Then, a cycle of length $2l$ in the Tanner graph associated with H is a lifted cycle of a $2l$-cycle in the protograph, i.e., one that visits sequentially the groups of N copies of check and variable nodes in the same order of the cycle in the protograph. Therefore, the $2l$-cycle is associated with a sequence of permutation matrices $P_{i_0 j_0}, P_{i_1 j_0}, P_{i_1 j_1}, P_{i_2 j_1}, \dots, P_{i_{l-1} j_{l-1}}, P_{i_0 j_{l-1}}$ (with no two equal adjacent permutations) such that $\left(P_{i_0 j_0} P^{\mathsf{T}}_{i_1 j_0} P_{i_1 j_1} P^{\mathsf{T}}_{i_2 j_1} \cdots P_{i_{l-1} j_{l-1}} P^{\mathsf{T}}_{i_0 j_{l-1}} + I\right) \triangle 0 \neq 0$.

Proof: The proof is the same as for single-edge protographs: the path of the $2l$ cycle will touch nodes associated with a sequence of permutation matrices such that any two consecutive matrices visited are different. Unlike codes based on protographs that contain only 0s and 1s, in multi-edge protographs two consecutive matrices can both be in the same position (k,l) in the protograph, if that position has an entry of 2 or larger. ■

Corollary 4: Let C be a code described by a parity-check matrix $H = (P_{i,j}) \in \mathbb{F}_2^{n_c N \times n_v N}$, where each $P_{i,j}$ is an $N \times N$ circulant matrix $x^{s_{ij}}$. Then the Tanner graph associated with H has a cycle of length $2l$ if there exist indices $i_0, i_1, \dots, i_{l-1}$ and $j_0, j_1, \dots, j_{l-1}$ 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 $s \in \{0,1,\dots,l-1\}$, and such that $s_{i_0 j_0} - s_{i_1 j_0} + s_{i_1 j_1} - s_{i_2 j_1} + \cdots + s_{i_{l-1} j_{l-1}} - s_{i_0 j_{l-1}} = 0$.

III. The Matrix C_H and the Relation Between $\mathrm{girth}(C_H)$ and $\mathrm{girth}(H)$

In this section, we use Theorem 2 in order to highlight a relation that exists between $\mathrm{girth}(H)$ and the girth of a certain submatrix C_H of HH^{T}. From this, we obtain the necessary and sufficient conditions for the graph of H to have girth 6, 8, 10, or 12. For simplicity, we assume the case of an $n_c \times n_v$ all-one protograph. However, the techniques developed here can be applied to any protograph as we exemplify in Section VI.

Let H_{n_c} and $C_{H_{n_c}}$ be defined as[6]

$$H = H_{n_c} = \begin{bmatrix} P_{11} & P_{12} & \cdots & P_{1n_v} \\ P_{21} & P_{22} & \cdots & P_{2n_v} \\ \vdots & \vdots & & \vdots \\ P_{n_c 1} & P_{n_c 2} & \cdots & P_{n_c n_v} \end{bmatrix}, \qquad (1)$$

$$C_H \triangleq C_{H_{n_c}} \triangleq \begin{bmatrix} 0 & C_{12} & \cdots & C_{1n_c} \\ C_{21} & 0 & \cdots & C_{2n_c} \\ \vdots & \vdots & & \vdots \\ C_{n_c 1} & C_{n_c 2} & \cdots & 0 \end{bmatrix}, \qquad (2)$$

where

$$C_{ij} \triangleq C^{\mathsf{T}}_{ji} \triangleq P_{i1} P_{j1}{}^{\mathsf{T}} + \cdots + P_{in_v} P_{jn_v}{}^{\mathsf{T}}, \quad i,j \in [n_c], \quad (3)$$

where P_{ij} are permutation matrices, for all $i \in [n_c], j \in [n_v]$. In this paper, we later focus on the case that the permutation matrices are circulants or arrays of circulants (Sections IV and V) since this will result in QC-LDPC codes that are attractive in practice; however, the results in this section hold for arbitrary permutation matrices.

Below, we highlight how the matrix C_H appears in the products B_t:

$$\begin{aligned} &B_0(H) = I, B_1(H) = H, B_2(H) = HH^{\mathsf{T}} = n_v I + C_H, \\ &B_3(H) = n_v H + C_H H, B_4(H) = (n_v I + C_H)^2, \\ &B_5(H) = (n_v I + C_H)^2 H, B_6(H) = (n_v I + C_H)^3, \text{ etc..} \end{aligned}$$

More generally, the following is true for all $m \geq 1$,

$$B_{2m}(H) = C_H^m + n_v f_m(I, C_H, \dots, C_H^{m-1}), \qquad (4)$$

$$B_{2m+1}(H) = C_H^m H + n_v f_m(I, C_H, \dots, C_H^{m-1}) H, \qquad (5)$$

where

$$f_m(I, C_H, \dots, C_H^{m-1}) \triangleq \sum_{l=0}^{m-1} \binom{m}{l} (n_v)^{m-1-l} C_H^l \qquad (6)$$

is a linear function in $I, C_H, \dots, C_H^{m-1}$ with positive coefficients. Indeed,

$$\begin{aligned} &B_{2m}(H) = (HH^{\mathsf{T}})^m = (n_v I + C_H)^m = \\ &C_H^m + \sum_{l=0}^{m-1} \binom{m}{l} C_H^l (n_v I)^{m-l} = \\ &C_H^m + n_v \sum_{l=0}^{m-1} \binom{m}{l} (n_v)^{m-1-l} C_H^l = \\ &C_H^m + n_v f_m(I, C_H, \dots, C_H^{m-1}), \end{aligned}$$

where the function $f_m(I, C_H, \dots, C_H^{m-1})$ is defined in (6). It follows that $B_{2m+1}(H) = (HH^{\mathsf{T}})^m H = (C_H)^m H + n_v f_m(I, C_H, \dots, C_H^{m-1}) H$, which proves (5).

Equations (4) and (5) give the following useful equivalences:

$$\begin{aligned} &B_{2m}(H) \triangle B_{2m-2}(H) = 0 \Leftrightarrow \\ &C_H^m \triangle \left(I + C_H + \cdots + C_H^{m-1}\right) = 0, \qquad (7) \\ &B_{2m+1}(H) \triangle B_{2m-1}(H) = 0 \Leftrightarrow \\ &C_H^m H \triangle \left(H + C_H H + \cdots + C_H^{m-1} H\right) = 0. \qquad (8) \end{aligned}$$

Indeed, $B_{2m}(H) \triangle B_{2m-2}(H) = 0$ if and only if, for each (i,j)-entry $B_{2m-2}(H)(i,j)$ of the matrix $B_{2m-2}(H)$ that is equal to 0, the (i,j)-entry $B_{2m}(H)(i,j)$ of the matrix $B_{2m}(H)$ is less than or equal to 1. Since $B_{2m-2}(H) = (n_v I + C_H)^{m-1}$ is a linear function in $I, C_H, \dots, C_H^{m-1}$ with positive coefficients,

$$\begin{aligned} B_{2m-2}(H)(i,j) = 0 &\Leftrightarrow \left(I + C_H + \cdots + C_H^{m-1}\right)(i,j) = 0 \\ &\Leftrightarrow n_v f_m(I, C_H, \dots, C_H^{m-1})(i,j) = 0. \end{aligned}$$

Therefore,

$$\begin{aligned} &B_{2m}(H)(i,j) \leq 1 \Leftrightarrow (C_H)^m(i,j) \leq 1 \Leftrightarrow \\ &C_H^m(i,j) \triangle \left(I + C_H + \cdots + C_H^{m-1}\right)(i,j) = 0. \end{aligned}$$

We thus obtain the equivalence (7), while the second equivalence (8) is obtained similarly. Therefore, Theorem 2 can now be restated.

[6] We will use the notation H and C_H when n_c is clear from the context.

Theorem 5: A Tanner graph of an LDPC code with parity-check matrix H has $\mathrm{girth}(H) > 2l$ if and only if, for all $t = 2, 3, \ldots, l$,

$$C_H^{\lfloor \frac{t}{2} \rfloor} H^{(t \bmod 2)} \triangle \left(I + C_H + \cdots + C_H^{\lfloor \frac{t}{2} \rfloor - 1} \right) H^{(t \bmod 2)} = 0.$$

We call C_H the *girth-matrix of* H.

In particular, we have the following theorem.

Theorem 6: Let H, C_H, and C_{ij} be defined as in (1), (2), and (3). Then

1) $\mathrm{girth}(H) > 4$ if and only if $C_{ij} \triangle 0 = 0$, for all $i, j \in [n_c], i \neq j$. Equivalently, $\mathrm{girth}(H) > 4$ if and only if C_{ij} does not have multiple edges, for all $i, j \in [n_c], i \neq j$, equivalently, if and only if $\mathrm{girth}(C_H) > 2$;

2) $\mathrm{girth}(H) > 6$ if and only if $C_H \triangle 0 = 0$ and $C_H H \triangle H = 0$. Equivalently, $\mathrm{girth}(H) > 6$ if and only if $C_{ij} \triangle 0 = 0$ and $\sum_{\substack{l=1 \\ l \neq i}}^{n_c} C_{il} P_{lk} \triangle P_{ik} = 0$, for all $k \in [n_v], i, j \in [n_c], i \neq j$;

3) $\mathrm{girth}(H) > 8$ if and only if $C_H \triangle 0 = 0$ and $C_H^2 \triangle (I + C_H) = 0$. Equivalently, $\mathrm{girth}(H) > 8$ if and only if $C_{ij} \triangle 0 = 0$ and $\sum_{\substack{l=1 \\ l \neq j}}^{n_c} C_{il} C_{lj} \triangle C_{ij} = 0$, for all $i, j \in [n_c], i \neq j$;

4) If $n_c = 3$, then $\mathrm{girth}(H) > 8$ if and only if $\mathrm{girth}(C_H) > 4$.[7]

Proof: 1) From Theorem 5, we have the following equivalence $\mathrm{girth}(H) > 4 \iff C_H \triangle I = 0 \iff C_{ij} \triangle 0 = 0 \iff C_{ij}$ does not have multiple edges, for all $i, j \in [n_c], i \neq j$.

2) The condition $C_H H \triangle H = 0$ is equivalent to $\sum_{\substack{l=1 \\ l \neq i}}^{n_c} C_{il} P_{lk} \triangle P_{ik} = 0$, for all $k \in [n_v], i \in [n_c]$, from which the claim follows.

3) We need to show that by satisfying $C_H^2 \triangle (I + C_H) = 0$ we also obtain $C_H H \triangle H = 0$. Let $R_i \triangleq [C_{i1} \ \cdots \ C_{i,i-1} \ 0 \ C_{i,i+1} \ \cdots \ C_{in_c}]$, for all $i \in [n_c]$. Then, $R_i R_i^{\mathsf{T}} \triangle I = 0 \iff \sum_{\substack{l=1 \\ l \neq i}}^{n_c} C_{il} C_{li} \triangle I = 0 \iff \sum_{\substack{l=1 \\ l \neq i}}^{n_c} C_{il} \left(\sum_{k=1}^{n_v} P_{lk} P_{ik}^{\mathsf{T}} \right) \triangle I = 0 \implies \sum_{\substack{l=1 \\ l \neq i}}^{n_c} C_{il} P_{lk} P_{ik}^{\mathsf{T}} \triangle I = 0 \iff \sum_{\substack{l=1 \\ l \neq i}}^{n_c} C_{il} P_{lk} \triangle P_{ik} = 0$, for all $k \in [n_v], i \in [n_c]$, which is equivalent to $B_3(H) \triangle B_1(H) = 0$.

4) For $n_c = 3$, $C_H^2 \triangle (I + C_H) = 0$ implies that, for all $i \in [3]$, $\sum_{\substack{l=1 \\ l \neq i}}^{3} C_{il} C_{li} \triangle I = 0$, and, equivalently, based on Theorem 2, that $\mathrm{girth}\, [C_{12} \quad C_{13}] > 4$, $\mathrm{girth}\, [C_{21} \quad C_{23}] > 4$, and $\mathrm{girth}\, [C_{31} \quad C_{32}] > 4$. However, since for a matrix with $n_c = 3$, a 4-cycle occurs in C_H if and only if it occurs in a row of C_H, we obtain that $\mathrm{girth}(C_H) > 4$.

Reversely, if $\mathrm{girth}(C_H) > 4$, then $C_H^2 \triangle I = 0$ which also implies the weaker condition $C_H^2 \triangle (I + C_H) = 0$. Therefore, for $n_c = 3$, we obtain that $C_H^2 \triangle (I + C_H) = 0$ is in fact equivalent to $C_H^2 \triangle I = 0$. ■

Similar theorems can be stated for girth larger than 10, 12, and so on.

We exemplify how the matrix C_H is obtained and that its girth is 6, as expected, for $n_c = 3$, by revisiting the following $3N \times 4N$ protograph-based code of girth 10 that can be found in [11] and [28].

Example 1: Let

$$H = \begin{bmatrix} P_{11} & P_{12} & P_{13} & P_{14} \\ P_{21} & P_{22} & P_{23} & P_{24} \\ P_{31} & P_{32} & P_{33} & P_{34} \end{bmatrix} \triangleq \left[\begin{array}{cc|cc|cc|cc} 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ \hline 1 & 0 & x & 0 & 0 & x^{10} & 0 & x^{13} \\ 0 & 1 & 0 & x^5 & x^{10} & 0 & x^{13} & 0 \\ \hline 1 & 0 & 0 & x^7 & x^{11} & 0 & x^2 & 0 \\ 0 & 1 & x^7 & 0 & 0 & x^{11} & 0 & x^4 \end{array} \right].$$

Here, the permutation matrices are $N_1 \times N_1 = 2 \times 2$ arrays of $N_2 \times N_2$ circulant matrices, such that $N = N_1 N_2$. This double lifting is referred to as *pre-lifting*, and results in a QC-LDPC matrix if the second lifting is circulant [11]. The matrices C_{ij} and C_H associated with H are

$$C_{21} = C_{12}^{\mathsf{T}} = \begin{bmatrix} 1 + x & x^{10} + x^{13} \\ x^{10} + x^{13} & 1 + x^5 \end{bmatrix},$$

$$C_{31} = C_{13}^{\mathsf{T}} = \begin{bmatrix} 1 + x^2 + x^{11} & x^7 \\ x^7 & 1 + x^4 + x^{11} \end{bmatrix},$$

$$C_{23} = C_{32}^{\mathsf{T}} = \begin{bmatrix} 1 & x^{-6} + x^{-1} + x^9 \\ x^{-1} + x^{-2} + x^{11} & 1 \end{bmatrix},$$

$$C_H = \begin{bmatrix} 0 & C_{12} & C_{13} \\ C_{21} & 0 & C_{23} \\ C_{31} & C_{32} & 0 \end{bmatrix},$$

where C_H is shown explicitly in (9) at the bottom of the next page.

The $3N \times 3N = 6N_2 \times 6N_2$, relatively dense $(8, 8)$-regular matrix C_H has girth 6 for $N_2 = 27$, for example. Equivalently, the $(3, 4)$-regular H has girth 10 for any such N_2. Moreover, codes with parity-check matrices that are submatrices of H based on 2×4 all-one (sub-)protographs have girth 12, for these N_2. □

Remark 1: The matrix C_H is therefore relevant when discussing the girth of H. In particular, we have observed the following two equivalences

$$\boxed{\mathrm{girth}(H) > 4 \iff \mathrm{girth}(C_H) > 2,}$$

$$\boxed{\text{for } n_c = 3, \mathrm{girth}(H) > 8 \iff \mathrm{girth}(C_H) > 4.}$$

Unfortunately, we cannot keep increasing the girth of C_H in hope to obtain higher girth for the associated H, because, if $n_c \geq 3$, C_H cannot have girth larger than 6, and if $n_c \geq 4$, C_H cannot have girth larger than 4, no matter what lifting or pre-lifting we choose. The 6-cycles and 4-cycles, respectively, are easy to observe. We state this fact below as Lemma 7. □

Lemma 7: Let H and C_H be matrices defined as in (1) and (2). If $n_c = 3$, then $\mathrm{girth}(C_H) \leq 6$, and if $n_c \geq 4$, $\mathrm{girth}(C_H) \leq 4$.

Proof: The proof can be found in Appendix A. ■

The following theorems connect, for some particular cases, codes with parity-check matrix H_{n_c} based on a protograph B

[7] Due to Lemma 7, we obtain that, for $n_c = 3$, $\mathrm{girth}(H) > 8$ if and only if $\mathrm{girth}(C_H) = 6$.

of size $n_c \times n_v$ to codes with parity-check matrix H_m based on a sub-protograph of B with size $m \times n_v$, $m < n_c$. This allows one to expand $mN \times n_vN$ protograph-based matrices to $n_cN \times n_vN$ matrices of the same girth after making sure that the $mN \times n_vN$ protograph-based matrices based on the sub-protograph of size $m \times n_v$, $m < n_c$ of B have the desired girth.

We start with a simple observation that formally states the following connection between $C_{H_{n_c}}$ and $C_{H_{n_c-1}}$, which can be useful in obtaining the girth conditions for $n_cN \times n_vN$ codes by starting from $(n_c-1)N \times n_vN$ codes of desired girth and adding an extra row.

Lemma 8: Let $n_c \geq 3$, $C_{H_{n_c}}$, $C_{H_{n_c-1}}$ be defined as in (2), and $C_{n_c,j}$ be defined as in (3) with $i = n_c$, for all $j \in [n_c - 1]$. The following decomposition of $C_{H_{n_c}}$ into two submatrices $X_{H_{n_c-1}}$ that contains information about the first $n_c - 1$ rows H_{n_c-1} of H_{n_c} (through $C_{H_{n_c-1}}$), and $Y_{H_{n_c}}$ that contains information about the new added row in H_{n_c} (through C_{n_c}), can be observed,

$$C_{H_{n_c}} = \underbrace{\begin{bmatrix} C_{H_{n_c-1}} & 0_{(n_c-1)\times 1} \\ 0_{1\times(n_c-1)} & 0_{1\times 1} \end{bmatrix}}_{X_{H_{n_c-1}}} + \underbrace{\begin{bmatrix} 0_{(n_c-1)\times(n_c-1)} & C_{n_c} \\ C_{n_c}^{\mathsf{T}} & 0_{1\times 1} \end{bmatrix}}_{Y_{H_{n_c}}},$$

where

$$C_{n_c}^{\mathsf{T}} \triangleq \begin{bmatrix} C_{n_c1} & \cdots & C_{n_c,n_c-1} \end{bmatrix}.$$

This lemma can be used to obtain the conditions for girth larger than g for a matrix H_{n_c} with check-node degree n_c when we start from a matrix H_{n_c-1} with check node degree $n_c - 1$ of girth larger than g and add an extra row of permutations. For example, to obtain the conditions for girth larger than 8 for a matrix H_4 with $n_c = 4$, we start from a matrix H_3 with $n_c = 3$ of girth larger than 8 and add an extra row of permutations. The necessary condition for girth larger than 8 is $C_{H_4}^2 \triangle (C_{H_4} + I) = 0$, which can be rewritten as $(X_{H_3} + Y_{H_4})^2 \triangle (X_{H_3} + Y_{H_4} + I) = 0$, from which we obtain, based on the many zeros in the description of $X_{H_3}^2$, $Y_{H_4}^2$, $X_{H_3}Y_{H_4}$, and $Y_{H_3}X_{H_4}$, the following three entry-wise conditions (obtained by writing the condition $C_{H_4}^2 \triangle (C_{H_4} + I) = 0$ entry-wise):

$$(C_{H_3}^2 + C_4C_4^{\mathsf{T}}) \triangle (C_{H_3} + I) = 0,$$
$$C_{H_3}C_4 \triangle C_4 = 0, \text{ and } C_4^{\mathsf{T}}C_4 \triangle I = 0,$$

where $C_4^{\mathsf{T}} \triangleq \begin{bmatrix} C_{41} & C_{42} & C_{43} \end{bmatrix}$. If we start from a $3 \times n_v$ matrix of girth larger than 8, then $C_{H_3}^2 \triangle (C_{H_3} + I) = 0$ is already satisfied; therefore, from the conditions given by this equality, we only need to record the conditions involving C_4. Consequently, Lemma 8 can be efficiently used to obtain conditions on the permutation matrices on the 4th row of H_4.

In addition, we also have the following connection.

Theorem 9: Let H_{n_c} be defined as in (1), and let $m \geq 2$. Then $\text{girth}(H_{n_c}) > 2m$ if and only if all $\min(m, n_c) \times n_v$ submatrices of H_{n_c} have girth greater than $2m$.

Proof: If $m \leq n_c$, an $2m$-cycle cannot involve more than m rows of H_{n_c}; a cycle involving $m + 1$ rows of H_{n_c}, must be of length strictly larger than $2m$. If $m > n_c$, then the claim holds trivially. ■

In particular, this theorem gives the following corollary.

Corollary 10: Let H_{n_c} be defined as in (1). Then

- If $n_c \geq 2$, then $\text{girth}(H_{n_c}) > 4$ if and only if all $2 \times n_v$ submatrices of H_{n_c} have girth > 4, and, equivalently, if and only if matrices C_{ij} have no multiple edges, for all $i, j \in [n_c]$, $i \neq j$;
- If $n_c \geq 3$, then $\text{girth}(H_{n_c}) > 6$ if and only if all $3 \times n_v$ submatrices have girth > 6, and, equivalently, if and only if all 3×3 submatrices of H_{n_c} have the permanent over $\mathbb{Z}$ of maximum possible weight;
- If $n_c \geq 4$, then $\text{girth}(H_{n_c}) > 8$ if and only if all $4 \times n_v$ submatrices of H_{n_c} have girth > 8;
- If $n_c \geq 5$, then $\text{girth}(H_{n_c}) > 10$ if and only if all $5 \times n_v$ submatrices have girth > 10.

Lastly, a weaker result can also be stated.

Corollary 11: Let H_{n_c}, $C_{H_{n_c}}$, and C_{ij} be defined as in (1), (2), and (3). Let $m \geq 2$. Then, for all $1 \leq i < j \leq n_c$,

$$\text{girth}(H_{n_c}) > 2m \Longrightarrow \text{girth}(C_{ij}) > m.$$

Proof: In order for the graph of H_{n_c} to have a certain girth $2m$, we need all its submatrices to have girth at least $2m$, including all its $2 \times n$ submatrices, graphs of which have twice the girths of their associated C_{ij} matrices. ■

Remark 2: It follows that, when constructing parity-check matrices of girth $2m$, we need to make sure that the associated matrices C_{ij} have girth at least m. In addition, we need to consider all $m \times n_v$ submatrices and impose the girth conditions on them. Thus, we can start from a $2 \times n_v$ matrix of girth $2m$ and add one row at a time imposing the girth conditions such that the newly formed matrix maintains the girth $2m$. □

In the next sections, we will use the above results to construct H_{n_c} of various girths for the cases of $n_c = 2, 3,$ and 4.

IV. The Girth of $2N \times n_vN$ Matrices H_2

Although the case of a $2 \times n_v$ protograph seems of limited practical importance on its own, it is essential when seen as

$$C_H = \left[\begin{array}{cc|cc|cc} 0 & 0 & 1+x^{-1} & x^{-10}+x^{-13} & 1+x^{-2}+x^{-11} & x^{-7} \\ 0 & 0 & x^{-10}+x^{-13} & 1+x^{-5} & x^{-7} & 1+x^{-4}+x^{-11} \\ \hline 1+x & x^{10}+x^{13} & 0 & 0 & 1 & x^{-6}+x^{-1}+x^{9} \\ x^{10}+x^{13} & 1+x^{5} & 0 & 0 & x^{-1}+x^{-2}+x^{11} & 1 \\ \hline 1+x^{2}+x^{11} & x^{7} & 1 & x+x^{2}+x^{-11} & 0 & 0 \\ x^{7} & 1+x^{4}+x^{11} & x^{6}+x+x^{-9} & 1 & 0 & 0 \end{array}\right]. \quad (9)$$

part of a larger protograph, since each $n_c \times n_v$ protograph of girth $2m$, with $n_c \geq 3$, has $\binom{n_c}{2}$ $2 \times n_v$ protographs that need to have girth at least $2m$. In addition, we show in the next theorem that the cycles in the Tanner graph of H_2 are in one-to-one correspondence with the cycles of the Tanner graph of a sum of permutation matrices in the composition of H_2. Parity-check matrices equal to a sum of some permutation matrices have enjoyed a lot of attention in the context of projective geometry codes [6], [16], [17].

In particular, any $n_c N \times n_v N$ protograph-based LDPC parity-check matrix can be seen as a submatrix of a square $n_v N \times n_v N$ matrix that is, in fact, a sum of permutation matrices of size $n_v N \times n_v N$. For example, the $n_v \times n_v$ all-one matrix is a sum of n_v distinct permutation matrices $1+x+x^2+\cdots+x^{n_v-1}$, each of size $n_v \times n_v$. These matrices are then lifted with lifting factor N to obtain permutation matrices $P_1, P_2, \ldots, P_{n_v}$, each of size $n_v N \times n_v N$, giving a sum of the same size. So any $n_c N \times n_v N$ LDPC monomial matrix can be seen as a submatrix of such a square matrix $P_1+P_2+\cdots+P_{n_v}$.

The following example demonstrates this important fact: how a protograph-based parity-check matrix can be decomposed (not uniquely) as a sum of permutation matrices. The code we use is the $(128, 64)$ NASA CCSDS standard code [18].

Example 2: Let $N = 16$ and $H_{(128,64)}$ be as shown in (10) at the bottom of the next page. Then $H_{(128,64)}$ is a sum of 8 permutation matrices P_i of size $8N \times 8N$, $N = 16$, from which we only take the first $4N$ rows. Indeed, let P_1, P_2, P_3, P_4, P_5, P_6, P_7, and P_8 be of size $8N \times 8N$, obtained by taking the following 8×8 permutation matrices and then lifting them with circulants of size $N = 16$ (circulants are only given for the first 4 rows since the rest are arbitrary) as follows: the identity matrix 1 lifted with 1, 1, 1, 1 (boxed in the matrix above), the identity matrix 1 lifted with x^7, x^{15}, x^{15}, x^{13} (boxed in red), the circulant matrix x lifted with x^6, x, x^9, 1 (circled), the circulant matrix x^2 lifted with x^4, x, x^{13}, x^7 (shaded red), the circulant matrix x^3 lifted with 1, 1, 1, x^3 (blue), the circulant matrix x^5 lifted with x^6, 1, 1, 1 (red), the circulant matrix x^6 lifted with x^{14}, x, x^{11}, x (green), and the circulant matrix x^7 lifted with x^2, 1, x^{14}, x^{14} (orange), respectively.

Then $H_{(128,64)} = \sum_{i=1}^{8} P_i'$, where P_i' is the matrix formed by the first $4N$ rows of P_i, and thus is a submatrix of a sum of $n_v = 8$ permutation matrices. We will revisit this matrix in Examples 6 and 18. □

We conclude from the above that the case of a $2 \times n_v$ protograph is important in its own right, and will explore some of the above-mentioned facts below.

Theorem 12: Let

$$H_2 = \begin{bmatrix} I & I & \cdots & I \\ P_1 & P_2 & \cdots & P_{n_v} \end{bmatrix}, \quad C_{21} = C_{12}^{\mathsf{T}} \triangleq \sum_{i=1}^{n_v} P_i. \quad (11)$$

Then,

$$\operatorname{girth}(H_2) = 2 \operatorname{girth}(C_{12}).$$

Note that, without loss of generality, P_1 could be chosen equal to I.

Proof: We show that any cycle of size $2l$ in H_2 corresponds one-to-one to a cycle of size l in C_{12}. Indeed, from Theorem 3, the Tanner graph associated with H_2 has a cycle of length $2l$ if and only if there exist indices $i_1, i_2, \ldots, i_l \in [n_v]$, such that $i_s \neq i_{s+1}$ and such that $IP_{i_1}^{\mathsf{T}} P_{i_2} I^{\mathsf{T}} I P_{i_3}^{\mathsf{T}} P_{i_4} I^{\mathsf{T}} \cdots P_{i_{l-1}}^{\mathsf{T}} P_{i_l} I^{\mathsf{T}} \triangle I \neq 0 \iff P_{i_1}^{\mathsf{T}} P_{i_2} P_{i_3}^{\mathsf{T}} P_{i_4} \cdots P_{i_{l-1}}^{\mathsf{T}} P_{i_l} \triangle I \neq 0$. Equivalently, there exist $m_1, m_2, \ldots, m_l$ such that $P_{i_1}(m_2, m_1) = P_{i_2}(m_2, m_3) = P_{i_3}(m_4, m_3) = \cdots = P_{i_l}(m_l, m_1) = 1$, which is equivalent to the existence of an l-cycle in C. ■

Since a $2l$-cycle in H_2 is equivalent to an l-cycle in C_{12}, and any bipartite graph can only have even size cycles, l must be even, leading to the $2l$-cycle in H_2 to have the size a multiple of 4. Therefore, the girth of a $2 \times n_v$ parity-check matrix H_2 must be multiple of 4.

Corollary 13: Let

$$H_2 = \begin{bmatrix} P_1 & P_2 & \cdots & P_{n_v} \\ Q_1 & Q_2 & \cdots & Q_{n_v} \end{bmatrix}, \quad C_{21} \triangleq C_{12}^{\mathsf{T}} \triangleq \sum_{i=1}^{n_v} P_i^{\mathsf{T}} Q_i.$$

Then

$$\operatorname{girth}(H_2) = 2 \operatorname{girth}(C_{21}).$$

Proof: The graph of H_2 is equivalent to the graph of the matrix $\begin{bmatrix} I & \cdots & I \\ P_1^{\mathsf{T}} Q_1 & \cdots & P_{n_v}^{\mathsf{T}} Q_{n_v} \end{bmatrix}$ which, based on Theorem 12 has twice the girth of C_{21}. ■

The following remark is a well known fact, see for example [5] for more details. We state it here because it can be seen as another corollary of the results regarding the $2 \times n_v$ protographs.

Remark 3: Let H_{n_c} be an LDPC code based on a protograph $B = (B_{ij})_{n_c \times n_v}$, with $B_{ij} \geq 0$ integers. If B has a 2×3 submatrix that has all its entries lifted to circulant matrices in H_{n_c}, then $\operatorname{girth}(H_{n_c}) \leq 12$. □

Example 3: Let

$$H_2 = \begin{bmatrix} I & I & I \\ I & P_2 & P_3 \end{bmatrix}.$$

Then the $4l$-cycles in the Tanner graph of the $2N \times 3N$ matrix H_2 are in one-to-one correspondence with the $2l$-cycles in the Tanner graph of $C_{12} = I+P_2+P_3$. To insure that $\operatorname{girth}(H_2) = 8$ we need to choose matrices P_2 and P_3 such that the matrix $I + P_2 + P_3$ does not have multiple edges (and thus has girth greater than 2), while in order for H_2 to have girth 12, we need to choose P_2 and P_3 such that the girth of $I + P_2 + P_3$ has girth 6. For example, we can take P_2 and P_3 to be circulant, equal to x and x^3, respectively, and $N = 7$. Then the matrix $I + P_2 + P_3 = 1 + x + x^3$ corresponds to the 7×7 parity-check matrix of the cyclic projective code of size 7, which has girth 6. Therefore, the corresponding 14×21 matrix H_2 has girth 12.

Any choice of P_2 and P_3 where both are circulants restricts the girth of $I + P_2 + P_3$ to be at most 6 (see Remark 3); therefore, in order to obtain a girth of H_2 larger than 12, we need to take P_2 and P_3 non-circulant. A convenient way to do this is by a 2-step lifting method consisting of a *prelifting*, i.e., forming a square matrix (circulant or not) by lifting with N_1, and then lifting it with circulant permutation matrices of size N_2, i.e., forming a permutation matrix as a $N_1 \times N_1$ array of $N_2 \times N_2$ circulants. For example, the matrices P_2 and P_3 below are obtained by first lifting each to a 3×3 matrix given by the circulant permutation matrices 1 and x^2 with $N_1 = 3$, respectively, and then applying a second lifting with circulants x, x^{13}, x^7 and x, x, x^2, respectively, i.e.,

$$P_2 = \begin{bmatrix} x & 0 & 0 \\ 0 & x^{13} & 0 \\ 0 & 0 & x^7 \end{bmatrix}, \; P_3 = \begin{bmatrix} 0 & x & 0 \\ 0 & 0 & x^2 \\ x & 0 & 0 \end{bmatrix}$$

such that

$$I + P_2 + P_3 \triangleq \begin{bmatrix} 1+x & x & 0 \\ 0 & 1+x^{13} & x^2 \\ x & 0 & 1+x^7 \end{bmatrix}.$$

The matrix $I + P_2 + P_3$ has girth 8 for $N_2 = 11$, girth 10 if the lifting is increased to $N_2 = 31$, and girth 12 if the lifting is increased to $N_2 = 41$. Therefore, the $2N \times 3N = 6N_2 \times 9N_2$ parity-check matrix H_2 formed with the above P_2 and P_3 has girth 16, 20, and 24, for $N = 11$, $N = 31$, and $N = 41$, respectively. (As a side note, the matrix $I + P_2 + P_3$ has minimum distance 48 for $N = 31$.) □

In Appendix B, we revisit Example 3 to show how the techniques of Sec. V-B were used in order to obtain matrices of girth beyond 12.

The following section provides algorithms to construct $2N \times n_v N$ protograph-based codes of various girth $4m$ and, equivalently, to construct sums of $n_v N \times n_v N$ permutation matrices of girth $2m$, $m \geq 1$.

A. Case of girth$(H) = 4m$, *for* $m = 2, 3$

Theorem 14: Let H_2 and C_{21} be defined as in (11), and let $P_j = x^{i_j}$, for all $j \in [n_v]$, and $i_1 = 0$.

1) girth$(H_2) = 4m > 4 \Leftrightarrow$ girth$(C_{21}) > 2$ if and only if the set $\{i_j \mid j \in [n_v]\}$ is of maximal size.[8]
2) girth$(H_2) = 4m > 8$ if and only if the set $\{i_j - i_l \mid j, l \in [n_v], j \neq l\}$ is of maximal size.[9]

The following are two algorithms based on the conditions of Theorem 14 to construct H_2 with girth larger than 4 and 8, respectively. We note that the conditions consist of only additions and subtractions to compute the forbidden sets. The algorithms, as exemplified below, run in a fraction of a second for all of the considerd cases on a standard laptop. They will later be extended to larger protographs and girths.

Algorithm 1 Constructing Codes with $n_c = 2$, $g > 4$

```
$i_1 := 0$
for $l := 2$ to $n_v$ do
    Choose $i_l \notin \{i_a \mid a \in [l-1]\}$
end for
```

Algorithm 2 Constructing Codes with $n_c = 2$, $g > 8$

```
$i_1 := 0$
for $l := 2$ to $n_v$ do
    Choose $i_l \notin \{i_a + i_b - i_c \mid a, b, c \in [l-1]\}$.
end for
```

Example 4: We construct a $2 \times n_v$ protograph-based matrix of girth $4m$, for $m = 2, 3$, following Algorithms 1 and 2 and choosing the smallest possible exponents at each step, giving

$$H_{2,g>4} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & x & x^2 & x^3 & x^4 & x^5 & x^6 & x^7 \end{bmatrix},$$

$$H_{2,g>8} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & x & x^3 & x^7 & x^{12} & x^{20} & x^{30} & x^{44} \end{bmatrix}.$$

The matrix $H_{2,g>4}$, constructed using Algorithm 1, has girth 8 for $N = 8$. In this case $C_{21} = 1 + x + \cdots + x^7$ is the 8×8 all-one matrix of girth 4. The matrix $H_{2,g>8}$, constructed using Algorithm 2, has girth 12 for $N = 77$, for example. Equivalently, the corresponding 77×77 matrix $C_{21} = 1 + x + x^3 + x^7 + x^{12} + x^{20} + x^{30} + x^{44}$ has girth 6. □

The following lemma gives an easy way to choose the next exponent values such that they are larger than the ones in the forbidden sets.

Lemma 15: Let H_2 and C_{21} be defined as in (11). Let i_l be defined recursively as

$$i_l = 1 + 2i_{l-1}, \; i_1 = 0, \; l \geq 2.$$

Then the Tanner graph of the code with parity-check matrix H_2 has girth 12 for some N. Equivalently, C_{21} has girth 6.

We exemplify this easy method below.

Example 5: The following matrix has girth 12 for $N = 73$

$$H_2 = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & x & x^3 & x^7 & x^{15} & x^{31} & x^{63} & x^{127} \end{bmatrix}.$$

The corresponding 73×73 matrix $C_{21} = 1 + x + x^3 + x^7 + x^{15} + x^{31} + x^{63} + x^{127}$ has girth 6. We reduce the exponents modulo $N = 73$ to obtain $C_{21} = 1 + x + x^3 + x^7 + x^{15} + x^{31} + x^{63} + x^{54}$. Note that this N is not the minimum for which a code can be found, but it can be easily obtained by hand and it is faster than Algorithm 2.

We also note that the component matrix $C_{21} = 1 + x + x^3 + x^7 + x^{15}$ of the denser C_{21} above has girth 6 for $N = 25$ while,

$$H_{(128,64)} = \begin{bmatrix} \boxed{1} + \boxed{x^7} & x^2 & x^{14} & x^6 & 0 & 1 & \colorbox{pink}{x^{13}} & \enclose{circle}{1} \\ \enclose{circle}{x^6} & \boxed{1} + \boxed{x^{15}} & 1 & x & 1 & 0 & 1 & \colorbox{pink}{x^7} \\ \colorbox{pink}{x^4} & \enclose{circle}{x} & \boxed{1} + \boxed{x^{15}} & x^{14} & x^{11} & 1 & 0 & x^3 \\ 1 & \colorbox{pink}{x} & \enclose{circle}{x^9} & \boxed{1} + \boxed{x^{13}} & x^{14} & x & 1 & 0 \end{bmatrix}. \quad (10)$$

[8] Recall that by *maximal size*, we indicate that all the possible values that can be generated for the set should be distinct.

[9] We note that the sets in Theorem 14 could be obtained directly by applying Fossorier's girth conditions, so the results of this theorem are not new. The novelty of this theorem is obtaining them using C_{12} and using the "maximal size" set terminology.

as expected, $C_{21} = 1 + x + x^3$ has girth 6 for $N = 7$ (this is the projective code [17]). □

We now review Example 2 in view of the connection of Theorem 12.

Example 6: Let P_i defined in Example 2 and let

$$H_2 \triangleq \begin{bmatrix} I & I & I & I & I & I & I & I \\ P_1 & P_2 & P_3 & P_4 & P_5 & P_6 & P_7 & P_8 \end{bmatrix}_{256 \times 1024}.$$

Theorem 12 says that $\text{girth}(H_2) = 2\,\text{girth}(C_{12})$ where $C_{12} = \sum_{i=1}^{8} P_i$ and has girth 6. Therefore H_2 is matrix of girth 12. By itself, this is not an interesting code; however, the strongly connected C_{12} is, since the parity-check matrix $H_{(128,64)}$ of the NASA CCSDS (128, 64) code is contained as a submatrix and thus $\text{girth}(H_{(128,64)}) \geq \text{girth}(C_{12})$. □

Remark 4: While the C_{12} matrices we construct can be invertible, there are cases of N for which the null-space is non-zero, thus giving codes worth considering. For example, the matrix $C_{21} = 1 + x + x^3$ has girth 6 for different values of N; however, the values of $N = 7, 14$, etc., are needed in order for the code with parity-check matrix C_{21} to have non-zero codewords (due to the fact that $1 + x + x^3$ is a polynomial divisor of $x^7 - 1$). □

B. Case of $\text{girth}(H_2) = 4m$*, for* $m \geq 4$

If we want to obtain matrices H_2 of girth larger than 12, then at least one of the matrices P_i has to be non-circulant. In our constructions, we follow a prelifting (double lifting) approach, as demonstrated already in Examples 1 and 3. For example, permutation matrix P below can be seen as the entry 1 in the protograph, first pre-lifted to the $N_1 \times N_1 = 3 \times 3$ circulant matrix x^2, before the second lifting with circulants x^a, x^b, x^c with lifting factor $N_2 = N/N_1$, i.e.,

$$P = \begin{bmatrix} 0 & x^a & 0 \\ 0 & 0 & x^b \\ x^c & 0 & 0 \end{bmatrix}, \text{ with } x^2 = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}.$$

The following theorem gives the necessary and sufficient conditions for girth larger than 12.

Theorem 16: Let H_2 be given as in (11). Then, $\text{girth}(H_2) > 12$ if and only if $C_{21} C_{12}^{\mathsf{T}} C_{21} \triangle C_{21} = 0$.

Example 7: The $2N \times 5N$ matrix H_2 with P_2, P_3, P_4, P_5, and C_{21} listed below (in this order) has girth 16 and, equivalently, the $3N \times 3N$ matrix C_{21} has girth 8:

$$\begin{bmatrix} 0 & 0 & x \\ 1 & 0 & 0 \\ 0 & x^7 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & x^3 \\ x^5 & 0 & 0 \\ 0 & x^{11} & 0 \end{bmatrix}, \begin{bmatrix} x^6 & 0 & 0 \\ 0 & x^{23} & 0 \\ 0 & 0 & x^{29} \end{bmatrix},$$
$$\begin{bmatrix} 0 & x^{15} & 0 \\ 0 & 0 & x^{19} \\ x^{42} & 0 & 0 \end{bmatrix}, \begin{bmatrix} x^6 + 1 & x^{15} & x + x^3 \\ 1 + x^5 & x^{23} + 1 & x^{19} \\ x^{42} & x^7 + x^{11} & x^{29} + 1 \end{bmatrix}.$$

The pre-lifted protograph used for $[P_1\ P_2\ P_3\ P_4\ P_5]$ corresponds to $[1\ \ x\ \ x\ \ 1\ \ x^2]$. □

Example 8: In this example, we start from a 5×5 pre-lifted protograph $[1\ \ x\ \ x^2\ \ x^3\ \ x^4]$ for sub-matrix $[P_1\ P_2\ P_3\ P_4\ P_5]$ because it has girth 6. This would insure that the structures P_{12}, P_{14}, P_{16} that limit the girth to 12, 14, and 16 (listed in [8] and in Appendix D) are all avoided. The lifted matrices $[P_2\ P_3\ P_4\ P_5]$ are (in order)

$$\begin{bmatrix} 0 & 0 & 0 & 0 & x \\ 1 & 0 & 0 & 0 & 0 \\ 0 & x^0 & 0 & 0 & 0 \\ 0 & 0 & x^{51} & 0 & 0 \\ 0 & 0 & 0 & x^{68} & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 0 & x^2 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ x^{12} & 0 & 0 & 0 & 0 \\ 0 & x^{79} & 0 & 0 & 0 \\ 0 & 0 & x^{94} & 0 & 0 \end{bmatrix},$$

$$\begin{bmatrix} 0 & 0 & x^4 & 0 & 0 \\ 0 & 0 & 0 & x^4 & 0 \\ 0 & 0 & 0 & 0 & x^{26} \\ x^{109} & 0 & 0 & 0 & 0 \\ 0 & x^{180} & 0 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & x^9 & 0 & 0 & 0 \\ 0 & 0 & x^{10} & 0 & 0 \\ 0 & 0 & 0 & x^{67} & 0 \\ 0 & 0 & 0 & 0 & x^{164} \\ x^{309} & 0 & 0 & 0 & 0 \end{bmatrix},$$

giving a matrix H_2 of girth 20 for $N = 458$ and, equivalently, the matrix

$$C_{21} = P_1 + P_2 + \cdots + P_5 = \begin{bmatrix} 1 & x^9 & x^4 & x^2 & x \\ 1 & 1 & x^{10} & x^4 & 1 \\ x^{12} & 1 & 1 & x^{67} & x^{26} \\ x^{109} & x^{79} & x^{51} & 1 & x^{164} \\ x^{309} & x^{180} & x^{94} & x^{68} & 1 \end{bmatrix}$$

of girth 10 for $N = 458$. □

Remark 5: Note that by taking a 3×5 submatrix of $P_1 + P_2 + \cdots + P_5$ above, we obtain a (3, 5)-regular LDPC code of girth 10. For example, the matrix H_{sub} below gives a code of minimum distance 24 and girth 10 for a minimum value $N = 101$ (and other larger)

$$H_{\text{sub}} \triangleq \begin{bmatrix} 1 & x^9 & x^4 & x^2 & x \\ 1 & 1 & x^{10} & x^4 & 1 \\ x^{12} & 1 & 1 & x^{67} & x^{26} \end{bmatrix}.$$

Since all protograph-based $n_c N \times n_v N$ parity-check matrices can be seen as submatrices of $n_v N \times n_v N$ square matrices that are equal to sums of n_v lifted permutation matrices, we can construct codes by constructing sums of permutation matrices with good girth, and either use them as the parity-check matrices (for a proper value of N), or take submatrices, like we did in the above example. □

V. THE GIRTH OF $n_c N \times n_v N$ MATRICES H_{n_c}, $n_c = 3, 4$

This section provides necessary and sufficient conditions[10] and associated algorithms to find $3 \times n_v$ and $4 \times n_v$ QC-LDPC protograph-based codes of various girth $2m \geq 6$. The algorithms start by constructing a $2 \times n_v$ protograph-based code of girth $\geq 2m$ and expanding it to a $3 \times n_v$, then to $4 \times n_v$. Cases of $n_c \geq 5$ can be solved similarly.

As before, we will consider H_{n_c} to be in the *reduced form*, i.e., it has identity matrices on the first row and first column, since the conditions are simpler to see. In addition, we will assume that the matrix H_{n_c} is composed of circulant matrices $x^{i_l}, x^{j_l}, x^{k_l}$, for all $l \in [n_v]$, with $i_1 = j_1 = k_1 = 0$.

[10] These conditions are minimal, in the sense that no condition is implied by other conditions.

A. Case of $4 < \mathrm{girth}(H_{n_c}) \leq 12$

In this section we will consider H_{n_c} as defined below, for $n_c = 2, 3$, and 4, respectively, alongside the corresponding matrices $C_{H_{n_c}}$ and C_{ij}. As mentioned above, we assume, without loss of generality, that $i_1 = j_1 = k_1 = 0$ (i.e., H_{n_c} is in reduced form):

$$H_2 = \begin{bmatrix} 1 & \cdots & 1 \\ x^{i_1} & \cdots & x^{i_{n_v}} \end{bmatrix}, \quad C_{H_2} \triangleq \begin{bmatrix} 0 & C_{12} \\ C_{21} & 0 \end{bmatrix};$$

$$H_3 = \begin{bmatrix} & H_2 & \\ x^{j_1} & \cdots & x^{j_{n_v}} \end{bmatrix} = \begin{bmatrix} 1 & \cdots & 1 \\ x^{i_1} & \cdots & x^{i_{n_v}} \\ x^{j_1} & \cdots & x^{j_{n_v}} \end{bmatrix}, \tag{12}$$

$$C_{H_3} \triangleq \begin{bmatrix} 0 & C_{12} & C_{13} \\ C_{21} & 0 & C_{23} \\ C_{31} & C_{32} & 0 \end{bmatrix} = \begin{bmatrix} C_{H_2} & C_3 \\ C_3^{\mathsf{T}} & 0 \end{bmatrix};$$

$$H_4 = \begin{bmatrix} & H_3 & \\ x^{k_1} & \cdots & x^{k_{n_v}} \end{bmatrix} = \begin{bmatrix} 1 & \cdots & 1 \\ x^{i_1} & \cdots & x^{i_{n_v}} \\ x^{j_1} & \cdots & x^{j_{n_v}} \\ x^{k_1} & \cdots & x^{k_{n_v}} \end{bmatrix}, \tag{13}$$

$$\begin{aligned} C_{H_4} &\triangleq \begin{bmatrix} 0 & C_{12} & C_{13} & C_{14} \\ C_{21} & 0 & C_{23} & C_{24} \\ C_{31} & C_{32} & 0 & C_{34} \\ C_{41} & C_{42} & C_{43} & 0 \end{bmatrix} = \begin{bmatrix} C_{H_3} & C_4 \\ C_4^{\mathsf{T}} & 0 \end{bmatrix}; \\ C_{12} = C_{21}^{\mathsf{T}} &\triangleq \sum_{l=1}^{n_v} x^{-i_l}, \qquad C_{23} = C_{32}^{\mathsf{T}} \triangleq \sum_{l=1}^{n_v} x^{i_l - j_l}, \\ C_{13} = C_{31}^{\mathsf{T}} &\triangleq \sum_{l=1}^{n_v} x^{-j_l}, \qquad C_{24} = C_{42}^{\mathsf{T}} \triangleq \sum_{l=1}^{n_v} x^{i_l - k_l}, \\ C_{14} = C_{41}^{\mathsf{T}} &\triangleq \sum_{l=1}^{n_v} x^{-k_l}, \qquad C_{34} = C_{43}^{\mathsf{T}} \triangleq \sum_{l=1}^{n_v} x^{j_l - k_l}, \\ C_3 &\triangleq \begin{bmatrix} C_{13} \\ C_{23} \end{bmatrix}, \quad C_4 \triangleq \begin{bmatrix} C_{14} \\ C_{24} \\ C_{34} \end{bmatrix}. \end{aligned} \tag{14}$$

Theorem 17: Let H_4 and C_{H_4} be defined as in (13) and (14). Then $\mathrm{girth}(H_4) > 4$ if and only if each one of the six sets $\{i_1, \ldots, i_{n_v}\}, \{j_1, \ldots, j_{n_v}\}, \{k_1, \ldots, k_{n_v}\}, \{i_1 - j_1, \ldots, i_{n_v} - j_{n_v}\}, \{i_1 - k_1, \ldots, i_{n_v} - k_{n_v}\}$, and $\{j_1 - k_1, \ldots, j_{n_v} - k_{n_v}\}$ is of maximal size.

Proof: In order to avoid 4-cycles, we need to insure that the codes based on the $2 \times n_v$ sub-protographs have no 4 cycles, for all such sub-protographs, and, equivalently, that $C_{ij} \triangle 0 = 0$, for all $1 \leq i < j \leq 4$. The claim on the sets above follows from this. ■

Remark 6: The conditions for $\mathrm{girth}(H_3) > 4$ are obtained from Theorem 17 by ignoring the sets above that contain any k_j, i.e., $\mathrm{girth}(H_3) > 4$ if and only if each one of the 3 sets $\{i_1, \ldots, i_{n_v}\}, \{j_1, \ldots, j_{n_v}\}, \{i_1 - j_1, \ldots, i_{n_v} - j_{n_v}\}$ is of maximal size. □

We now present an algorithm to choose these exponents in which we first choose $i_1, i_2, \ldots, i_{n_v}$ (sequentially), and then choose $j_1, j_2, \ldots, j_{n_v}$, and then all $k_1, k_2, \ldots, k_{n_v}$, such that, at each step, the conditions of Theorem 17 are satisfied. This algorithm is an extension of Algorithm 1 for $2N \times n_v N$ parity-check matrices H_2. To obtain an algorithm for $n_c = 3$, we simply ignore Lines 8–10 that choose the exponents k_l, $l \in [n_v]$.

Algorithm 3 Constructing Codes with $n_c = 4$, $g > 4$

```
1: $i_1 := 0, j_1 := 0, k_1 := 0$.
2: for $l := 2$ to $n_v$ do
3:     Choose $i_l \notin \{i_a \mid a \in [l-1]\}$.
4: end for
5: for $l := 2$ to $n_v$ do
6:     Choose $j_l \notin \{j_a, i_l + (j_a - i_a) \mid a \in [l-1]\}$.
7: end for
8: for $l := 2$ to $n_v$ do
9:     Choose $k_l \notin \{k_a, i_l + (k_a - i_a), j_l + (k_a - j_a) \mid a \in [l-1]\}$.
10: end for
```

We now extend this to larger girth in Theorem 18 and Algorithm 4.

Theorem 18: Let H_4 and C_{H_4} be defined as in (13) and (14). Then $\mathrm{girth}(H) > 6$ if and only if, for all $l \in [n_v]$, each one of the sets

$$\begin{aligned} &\{i_l - i_s, j_l - j_s, k_l - k_s \mid s \in [n_v], s \neq l\}, \\ &\{i_s, i_s - j_s + j_l, i_s - k_s + k_l \mid s \in [n_v], s \neq l\}, \\ &\{j_s, j_s - i_s + i_l, j_s - k_s + k_l \mid s \in [n_v], s \neq l\}, \\ &\{k_s, k_s - i_s + i_l, k_s - j_s + j_l \mid s \in [n_v], s \neq l\} \end{aligned}$$

is of maximal size.

Proof: From Theorem 6 we see that in order to avoid 6-cycles, we need to insure that, for all $l \in [n_v]$, and all $s, t \in [n_v] \setminus \{l\}$,

$$\begin{aligned} (C_{12}x^{i_l} + C_{13}x^{j_l} + C_{14}x^{k_l}) \triangle 1 &= 0, \\ (C_{21} + C_{23}x^{j_l} + C_{24}x^{k_l}) \triangle x^{i_l} &= 0, \\ (C_{31} + C_{32}x^{i_l} + C_{34}x^{k_l}) \triangle x^{j_l} &= 0, \\ (C_{41} + C_{42}x^{i_l} + C_{43}x^{j_l}) \triangle x^{k_l} &= 0. \end{aligned}$$

Equivalently, the following equalities hold,

$$\begin{aligned} \sum_{\substack{s=1 \\ s \neq l}}^{n_v} \left(x^{i_l - i_s} + x^{j_l - j_s} + x^{k_l - k_s}\right) \triangle 1 &= 0, \\ \sum_{\substack{s=1 \\ s \neq l}}^{n_v} \left(x^{i_s} + x^{i_s - j_s + j_l} + x^{i_s - k_s + k_l}\right) \triangle x^{i_l} &= 0, \\ \sum_{\substack{s=1 \\ s \neq l}}^{n_v} \left(x^{j_s} + x^{j_s - i_s + i_l} + x^{j_s - k_s + k_l}\right) \triangle x^{j_l} &= 0, \\ \sum_{\substack{s=1 \\ s \neq l}}^{n_v} \left(x^{k_s} + x^{k_s - i_s + i_l} + x^{k_s - j_s + j_l}\right) \triangle x^{k_l} &= 0, \end{aligned}$$

from which the claim follows. ■

Example 9: We construct two 4×8 protograph-based matrices, one of girth larger than 4, and one of girth larger than 6, starting from the 2×8 matrix $H_{2,g>4}$ from Example 4 and adding a 3rd and a 4th row such that the conditions of Algorithms 3 and 4 are satisfied, respectively. Choosing the exponent at each step as the smallest positive integer not in

Algorithm 4 Constructing Codes with $n_c = 4$, $g > 6$

```
1: $i_1 := 0, j_1 := 0, k_1 := 0$.
2: for $l := 2$ to $n_v$ do
3:     Choose $i_l \notin \{i_a \mid a \in [l-1]\}$.
4: end for
5: for $l := 2$ to $n_v$ do
6:     Choose $j_l \notin \{j_a, i_t + j_a - i_a, i_l + j_a - i_t \mid a \in [l-1], t \in [n_v]\}$.
7: end for
8: for $l := 2$ to $n_v$ do
9:     Choose $k_l \notin \{i_l + (k_s - i_t), j_l + (k_s - j_t), i_t + (k_s - i_s), j_t + (k_s - j_s), j_l + (k_s - i_s) + (i_t - j_t), i_l + (k_s - j_s) + (j_t - i_t) \mid s \in [l-1], t \in [n_v]\}$
10: end for
```

the forbidden set yields

$$H_{4,g>4} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & x & x^2 & x^3 & x^4 & x^5 & x^6 & x^7 \\ 1 & x^2 & x & x^5 & x^7 & x^3 & x^{10} & x^4 \\ 1 & x^3 & x^5 & x & x^9 & x^2 & x^7 & x^{11} \end{bmatrix},$$

$$H_{4,g>6} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & x & x^2 & x^3 & x^4 & x^5 & x^6 & x^7 \\ 1 & x^8 & x^{15} & x^{21} & x^{26} & x^{32} & x^{39} & x^{47} \\ 1 & x^9 & x^{17} & x^{24} & x^{30} & x^{37} & x^{45} & x^{54} \end{bmatrix}.$$

□

Remark 7: At each step, we can choose i_l, j_l, and k_l to be the minimum positive integer such that they satisfy the conditions of the algorithm (as done in Example 9), but the resulting matrix may not necessarily have the smallest N possible for that girth, nor be the best code. The above algorithms can be modified to, e.g., select exponents randomly, avoiding those values in the forbidden set, or so that they are larger than the maximum value in the forbidden set. Different choice of exponents will yield different minimum N (see also Remark 10). Since the forbidden sets are generated in the same way, the run-time in any realization will be similar, but can result in codes with varying performance. Finally, we note that the algorithms can also be modified to pick exponents column-by-column, rather than row-by-row as presented here; see [1] for examples. Again, this will typically result in different codes which may or may not yield improved performance. □

Similar theorems can be stated for $\mathrm{girth}(H_4) > 8$ and $\mathrm{girth}(H_4) > 10$, but the number of conditions increase; so, for clarity we only present them for $n_c = 3$ and refer the reader to Remark 14 for how to extend these conditions to the case $n_c = 4$. We also refer the reader to [29] for a list of these conditions.

Theorem 19: Let H_3 and C_{H_3} be defined as in (12) and (14). Then $\mathrm{girth}(H_3) > 8$ if and only if each two of the following sets of differences

$$\{i_u - i_v \mid u \neq v, u, v \in [n_v]\}, \{j_u - j_v \mid u \neq v, u, v \in [n_v]\},$$
$$\{(i_u - j_u) - (i_v - j_v) \mid u \neq v, u, v \in [n_v]\}$$

contains non-equal values and each set is of maximal size.

Equivalently, $\mathrm{girth}(H_3) > 8$ if and only if each one of the three sets $\{i_u - i_v, j_u - j_v \mid u \neq v, u, v \in [n_v]\}$, $\{i_u - i_v, (i_u - j_u) - (i_v - j_v) \mid u \neq v, u, v \in [n_v]\}$, $\{j_u - j_v, (i_u - j_u) - (i_v - j_v) \mid u \neq v, u, v \in [n_v]\}$ is of maximal size.

Proof: We have $\mathrm{girth}(H_3) > 8$ if and only if $\mathrm{girth}(C_{H_3}) = 6$ if and only if $C^2_{H_3} \triangle I = 0$. By expanding this last equality into the equivalent conditions we obtain:

$$(C_{12}C_{21} + C_{13}C_{31}) \triangle I = 0,$$
$$(C_{21}C_{12} + C_{23}C_{32}) \triangle I = 0,$$
$$(C_{31}C_{13} + C_{32}C_{23}) \triangle I = 0.$$

Equivalently,

$$\sum_{u,v \in [n_v]} x^{i_u - i_v} + \sum_{u,v \in [n_v]} x^{j_u - j_v} \qquad \triangle 1 = 0,$$
$$\sum_{u,v \in [n_v]} x^{i_u - i_v} + \sum_{u,v \in [n_v]} x^{(i_u - j_u) - (i_v - j_v)} \qquad \triangle 1 = 0,$$
$$\sum_{u,v \in [n_v]} x^{j_u - j_v} + \sum_{u,v \in [n_v]} x^{(i_u - j_u) - (i_v - j_v)} \qquad \triangle 1 = 0.$$

The claim follows. ■

Remark 8: Since C_{H_3} has girth 6, it means that C_{ij} have girth 6, for all $1 \leq i < j \leq 3$. Therefore, all $2N \times n_v N$ sub-matrices have girth 12 when, overall, H_3 has girth 10. □

Algorithm 5 Constructing Codes with $n_c = 3$, $g > 8$

```
1: $i_1 := 0, j_1 := 0$.
2: for $l := 2$ to $n_v$ do
3:     Choose $i_l \notin \{i_u + i_s - i_t \mid u, t, s \in [l-1]\}$.
4: end for
5: for $l := 2$ to $n_v$ do
6:     Choose $j_l \notin \{j_u + j_s - j_t, j_u + i_a - i_b, j_u + (j_s - i_s) - (j_t - i_t), i_l + i_a - i_b + (j_u - i_u), i_l + (j_u - i_u) + (j_s - i_s) - (j_t - i_t), i_l + j_s - j_t + (j_u - i_u) \mid a, b \in [n_v], u, s, t \in [l-1]\}$.
7: end for
```

Remark 9: We note that in Step 6 in Algorithm 5 (and also in Algorithm 6 later), the range $t \in [l-1]$ assumes that the exponents j_l are chosen to be increasing in value with l. This is how we have implemented the algorithms in our examples. However, for general exponent selection (increasing in value or not) we should amend Step 6 to have $t \in [l]$ to ensure that the conditions in the corresponding theorem are met, i.e., $2j_l \notin \{j_u + j_s, j_u + (j_s - i_s) + i_t, 2i_l + (j_u - i_u) + (j_s - i_s), i_l + j_s + (j_u - i_u) \mid u, s \in [l-1]\}$. □

Remark 10: Given a parity-check matrix H_3 that meets the conditions of Theorem 19 (i.e., it can achieve girth larger than 8) then the lifting factors $N \in \mathbb{Z}^+$ for which the parity-check matrix has girth 10 (or larger) are given by $N \nmid \{i_s + i_t - i_u - i_v, j_u - j_v + i_s - i_t, j_u - j_v + j_s - j_t, j_u - j_v + (j_s - i_s) - (j_t - i_t), (j_s - i_s) - (j_t - i_t) + (j_u - i_u) - (j_v - i_v), (j_s - i_s) - (j_t - i_t) + i_u - i_v \mid s, t, u, v \in [n_v]\}$, where the smallest such value is denoted $N_{\min}$ and the notation $a \nmid b$ denotes that a does not divide b. Similar statements can be made to determine viable (and minimum) N for general H_{n_c} and desired girth by using the conditions in the associated theorem or, equivalently, algorithm. We note that picking a larger N than $N_{\min}$ may often yield better performance provided that the girth is maintained, see Section VII. □

Example 10: Note that in Example 4, we used Algorithm 2 (the first part of Algorithm 5) to obtain a $2N \times n_v N$ matrix $H_{2,g>8}$ of girth 12 for $N = 77$. The circulants x^{i_l} are

$$\begin{bmatrix} x^{i_1} & x^{i_2} & x^{i_3} & \cdots & x^{i_8} \end{bmatrix} = \begin{bmatrix} 1 & x & x^3 & x^7 & x^{12} & x^{20} & x^{30} & x^{44} \end{bmatrix}.$$

The matrix $C_{21} = 1 + x + x^3 + x^7 + x^{12} + x^{20} + x^{30} + x^{44}$ has, equivalently, girth 6 for $N = 77$.

Therefore, we need to choose the row $\begin{bmatrix} x^{j_1} & x^{j_2} & x^{j_3} & \cdots & x^{j_8} \end{bmatrix}$ such that $C_{31} = x^{j_1} + \cdots + x^{j_8}$ has girth 6, but also such that the resulting matrix $C_{32} = x^{j_1 - i_1} + x^{j_2 - i_2} + x^{j_3 - i_3} + \cdots + x^{j_8 - i_8}$ has girth 6, and also C_H has girth 6. So we choose j_l such that the difference between j_l and any exponent already found in C_{21} or C_{31} does not appear among the differences of the exponents already found, and we impose the same for $j_l - i_l$, i.e., that the difference between $(j_l - i_l)$ and any exponent already found in C_{21} or C_{32} does not appear among the differences of the exponents already found.

We obtained the following matrix with Tanner graph of girth 10 for $N_{\min} = 514$ (applying Remark 10)

$$H = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & x & x^3 & x^7 & x^{12} & x^{20} & x^{30} & x^{44} \\ 1 & x^{66} & x^{461} & x^{106} & x^{144} & x^{194} & x^{274} & x^{385} \end{bmatrix}.$$

Note that C_{12}, C_{13}, and C_{23} all have girth 6, giving 3 $(2, 8)$-regular codes of girth 12. □

The following lemma extends Lemma 15 for $2N \times n_v N$ parity-check matrices H_2 of $\operatorname{girth}(H_2) > 8$ to $3N \times n_v N$ matrices H_3. It gives an easy way to choose the next exponent values such that they are larger than the ones in the forbidden sets, i.e., sets that would decrease the girth to 8 or lower.

Lemma 20: Let H_3 and C_{H_3} be defined as in (12) and (14). Let i_l and j_l be defined recursively as

$$\begin{cases} i_1 = 0, \\ i_l = 1 + 2i_{l-1}, \ l \geq 2, \end{cases} \text{and} \begin{cases} j_1 = 0, \ j_2 = 1 + i_2 + 2i_{n_v}, \\ j_l = 1 + 2j_{l-1} + i_l, \ l \geq 3. \end{cases}$$

The Tanner graph of the code with parity-check matrix H_3 has girth 10 for some N.

Proof: Note that $i_l > i_{l-1} > \cdots > i_1$ and $j_l > j_{l-1} > \cdots > j_1$. We obtain that $i_l = 1 + 2j_{l-1} > i_u + i_s \geq i_u + i_s - i_t$, for all $u, s, t \in [l-1]$. The forbidden set for j_2 is $\{j_1 + j_1 - j_1 = 0, j_1 + i_a - i_b = i_a - i_b, j_1 + (j_1 - i_1) - (j_1 - i_1) = 0, i_2 + i_a - i_b + (j_1 - i_1) = i_2 + i_a - i_b, i_2 + (j_1 - i_1) + (j_1 - i_1) - (j_1 - i_1) = i_2, i_2 + j_1 - j_1 + (j_1 - i_1) = i_2 \mid a, b \in [n_v]\} = \{0, i_a - i_b, i_2 + i_a - i_b, i_2 \mid \ a, b \in [n_v]\}$ and $1 + i_2 + 2i_{n_v}$ is definitely larger than each of these values. Lastly, $j_l = 1 + 2j_{l-1} + i_l > i_l + j_u + j_s$, for all $s, t \in [l-1]$, and so, it is larger than any of the values in its forbidden set $\{j_u + j_s - j_t, j_u + i_a - i_b, j_u + (j_s - i_s) - (j_t - i_t), i_l + i_a - i_b + (j_u - i_u), i_l + (j_u - i_u) + (j_s - i_s) - (j_t - i_t), i_l + j_s - j_t + (j_u - i_u) \mid \ a, b \in [n_v], u, s, t \in [l-1]\}$. ■

Remark 11: Instead of the choice of j_l above, we can alternatively choose, for example, $j_l = 1 + 3j_{l-1}$ or $j_l = 1 + j_{l-1} + \max\{j_{l-2}, i_{n_v}\} + \max\{j_{l-3}, i_{n_v}\}$ to obtain a QC-LDPC code matrix H_3 with girth 10 for some N. Such choices hold since each of the chosen values satisfy the conditions of Algorithm 5, where they can be seen to be, at each step, larger than the largest forbidden value. □

We exemplify this easy method below.

Example 11: We construct a 3×7 matrix based on Lemma 20 to obtain the first matrix $H_{3,g>8}$ below of girth 10 for $N_{\min} = 433$. After reducing the exponents modulo $N = 433$, this matrix is equal to the second matrix, which has girth 10 for $N_{\min} = 347$:

$$H_{3,g>8} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & x & x^3 & x^7 & x^{15} & x^{31} & x^{63} \\ 1 & x^{128} & x^{260} & x^{528} & x^{1072} & x^{2176} & x^{4416} \end{bmatrix} \equiv \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & x & x^3 & x^7 & x^{15} & x^{31} & x^{63} \\ 1 & x^{128} & x^{260} & x^{95} & x^{206} & x^{11} & x^{86} \end{bmatrix}.$$

If we write $260 = -87$ and $206 = -141$, we obtain the first matrix below of girth 10 for the new minimum value $N = 327$, for which $-141 = 186$ and $-87 = 240$, as shown in the second matrix below

$$H_{3,g>8} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & x & x^3 & x^7 & x^{15} & x^{31} & x^{63} \\ 1 & x^{128} & x^{-87} & x^{95} & x^{-141} & x^{11} & x^{86} \end{bmatrix} \equiv \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & x & x^3 & x^7 & x^{15} & x^{31} & x^{63} \\ 1 & x^{128} & x^{240} & x^{95} & x^{186} & x^{11} & x^{86} \end{bmatrix}.$$

This last matrix has girth 10 for $N_{\min} = 278$.

Note that this N is not the minimum for which a code can be found with girth 10, since the minimum with the algorithm is $N = 219$. But it can be easily obtained by hand. □

Theorem 21: Let H_3 and C_{H_3} be as defined in (12) and (14). Then $\operatorname{girth}(H) > 10$ if and only if, for all $l \in [n_v]$,

1) each two of the four sets of differences $\{i_u - i_v \mid u \neq v, u, v \in [n_v], u \neq l\}, \{j_u - j_v \mid u \neq v, u, v \in [n_v], u \neq l\}, \{-j_u + j_v - i_v + i_l \mid u \neq v, u, v \in [n_v], v \neq l\}, \{-i_u + i_v - j_v + j_l \mid u \neq v, u, v \in [n_v], v \neq l\}$ contain non-equal values, for all $l \in [n_v]$, and each set is of maximal size.
2) each two of the four sets of differences $\{i_u - j_u + j_v \mid u \neq v, u, v \in [n_v], v \neq l\}, \{i_u - i_v + i_l \mid u \neq v, u, v \in [n_v], v \neq l\}, \{(i_u - j_u) - (i_v - j_v) + i_l \mid u \neq v, u, v \in [n_v], v \neq l\}, \{i_u - j_v + j_l \mid u \neq v, u, v \in [n_v], v \neq l\}$ contain non-equal values, and each set is of maximal size.
3) each two of the four sets of differences $\{j_u - i_u + i_v \mid u \neq v, u, v \in [n_v], v \neq l\}, \{j_u - i_v + i_l \mid u \neq v, u, v \in [n_v], v \neq l\}, \{j_u - j_v + j_l \mid u \neq v, u, v \in [n_v], v \neq l\}, \{j_u - i_u + i_v - j_v + j_l \mid u \neq v, u, v \in [n_v], v \neq l\}$ contain non-equal values, and each set is of maximal size.

Proof: We apply the condition $C_{H_3}^2 H_3 \triangle (H_3 + C_{H_3} H_3) = 0$ to obtain

$$\begin{aligned}&\left(C_{12}C_{21} + C_{13}C_{31} + C_{13}C_{32}x^{i_l} + C_{12}C_{23}x^{j_l}\right) \triangle \\ &(C_{12}x^{i_l} + C_{13}x^{j_l} + I) = 0,\\ &\left(C_{23}C_{31} + (C_{21}C_{12} + C_{23}C_{32})\, x^{i_l} + C_{21}C_{13}x^{j_l}\right) \triangle \\ &(C_{21} + C_{23}x^{j_l} + x^{i_l}) = 0,\\ &\left(C_{32}C_{21} + C_{31}C_{12}x^{i_l} + (C_{31}C_{13} + C_{32}C_{23})\, x^{j_l}\right) \triangle \\ &(C_{31} + C_{32}x^{i_l} + x^{j_l}) = 0,\end{aligned}$$

from which we obtain (15)-(17), shown at the bottom of the next page. These three equalities hold if any two monomials on the left side of the triangle operator are not equal, unless they are equal to one of the monomial on the right side of the triangle operator. We obtain the claim of the theorem. ■

The following Algorithm 6 uses Theorem 21 to construct a parity-check matrix H_3 such that the girth is 12. Similar to the above, the exponents i_u, $u \in [n_v]$ are chosen first, i.e., it chooses the row of the matrices x^{i_l} such that the girth of the $2N \times n_v N$ matrix is equal to 12. (Note that this matrix would be the same as for $\mathrm{girth}(H_2) > 8$ from Algorithm 2.) Following this, one more row is added with the additional conditions above to insure that the girth is 12 rather than ≥ 10 as in Algorithm 5.

Algorithm 6 Constructing Codes with $n_c = 3$, $g > 10$

```
1: $i_1 := 0, j_1 := 0$.
2: for $l := 2$ to $n_v$ do
3:     Choose $i_l \notin \{i_u + i_s - i_t \mid u, t, s \in [l-1]\}$.
4: end for
5: for $l := 2$ to $n_v$ do
6:     Choose $j_l \notin \{i_a - i_b + j_s, i_a + j_s - j_t + (j_u - i_u), i_a + i_b - i_c + (j_s - i_s), -i_a + j_s + j_u - (j_t - i_t), j_s - (j_t - i_t) + (j_u - i_u), i_a + (j_s - i_s) - (j_t - i_t) + (j_u - i_u), i_l + i_a - j_t + (j_s - i_s) + (j_u - i_u), i_l - i_a + j_s - (j_t - i_t) + (j_u - i_u), i_l - i_a + j_s + j_u - j_t, i_l + i_a - i_b - i_c + j_s, j_s + j_u - j_t \mid a, b, c \in [n_v], s, u, v, t \in [l-1]\}$
7: end for
```

Remark 12: Again, for general exponent selection (increasing in value or not) we should amend Step 6 to have $t \in [l]$ to ensure that the conditions in the corresponding theorem are met, i.e., $2j_l \notin \{i_a + j_s + (j_u - i_u), -i_a + j_s + j_u + i_l, j_s + i_l + (j_u - i_u), i_a + (j_s - i_s) + i_l + (j_u - i_u), i_l + i_a + (j_s - i_s) + (j_u - i_u), 2i_l - i_a + j_s + (j_u - i_u), j_s + j_u \mid a \in [n_v], s, u \in [l-1]\}$ (see Remark 9). □

The following is such an example. We start from $H_{2,g>8}$ and use Algorithm 6 to find the third row.

Example 12: The matrix

$$H = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1\\ 1 & x & x^3 & x^7 & x^{12} & x^{20} & x^{30} & x^{44}\\ 1 & x^{66} & x^{144} & x^{232} & x^{336} & x^{526} & x^{664} & x^{747}\end{bmatrix}$$

has girth 12 for $N_{\min} = 1245$ (length $n_v N_{\min} = 9960$), for example. □

Remark 13: An alternative way to obtain a girth 12 matrix is by starting from a girth 10 matrix and modifying the exponent of a circulant matrix that is a component of a 10-cycle. Since a girth 10 matrix H_3 must have all $2 \times n_v$ and 3×2 sub-protographs lifted to girth 12 codes, we can check the girth of the 3×3, 3×4, etc., submatrices to find out which ones are of girth 12 (if any) and which are of girth 10. If we find out that an entry decreases the girth from 12 to 10, we can change its exponent to a much larger one to break the 10 cycle. We do this in the following example. □

Example 13: Let us consider the $(3,5)$-regular submatrix $H_{3,g>8}$ below obtained from the $(3,8)$-regular QC-LDPC code of girth 10 for $N = 514$ constructed in Example 10. Note that, for this N, all 2×3 and 2×5 submatrices of the 3×5 matrix $H_{3,g>8}$ correspond to $(2,3)$-regular and $(2,5)$-regular protograph-based codes, respectively, with girth 12, since $C_{H_{3,g>8}}$ has girth 6 and hence the submatrices C_{ij} all have girth 6 (they cannot be higher), resulting in associated matrices of girth 12. Since the girth of $H_{3,g>8}$ is 10, there must be some 10-cycles in $H_{3,g>8}$ in a 3×3 submatrix of $H_{3,g>8}$. We check the girth of each 3×4 submatrix and find that the 3×4 submatrix obtained from columns 1, 2, 3, and 5 of $H_{3,g>8}$ has girth 12, and so does the 3×5 matrix obtained from $H_{3,g>8}$ by masking x^{144} (substituting it with 0). Hence the 10-cycle visits this circulant. We make a substitution, for example, x^{244} instead of x^{144}, to obtain $H_{3,g>10}$ below of girth 12 for $N_{\min} = 328$:

$$H_{3,g>8} = \begin{bmatrix} I & I & I & I & I\\ 1 & x & x^7 & x^{12} & x^{20}\\ 1 & x^{66} & x^{106} & x^{144} & x^{194}\end{bmatrix} \rightsquigarrow$$
$$H_{3,g>10} = \begin{bmatrix} I & I & I & I & I\\ 1 & x & x^7 & x^{12} & x^{20}\\ 1 & x^{66} & x^{106} & x^{244} & x^{194}\end{bmatrix}.$$

We note that $H_{3,g>8}$ has girth 10 for $N_{\min} = 158$ and $H_{3,g>10}$ has girth 10 for $N_{\min} = 222$, obtained using Remark 10, but $H_{3,g>8}$ cannot achieve girth 12 for any N. □

In Appendix C, we revisit Example 13 to show how we can use the girth 10 construction together with the pre-lifting techniques presented in Section V-B, in order to obtain a girth 12 code and possibly increase the minimum distance.

We conclude this section with a remark concerning the extension of the $n_c = 3$ results given above to $n_c = 4$.

Remark 14: The conditions in the case of $n_c = 4$ can be obtained by starting from a $3 \times n_v$ matrix of the desired girth and using the connection between C_{H_4} and C_{H_3}. In Section III, we show how to use Lemma 8 efficiently to do this in the case $\mathrm{girth}(H) > 8$, for which $C_H^2 \triangle (C_H + I) = 0$ must be satisfied, and, equivalently,

$$\begin{aligned}&(C_{H_3}^2 + C_4 C_4^{\mathsf{T}}) \triangle (C_{H_3} + I) = 0,\\ &C_{H_3} C_4 \triangle C_4 = 0, \text{ and } C_4^{\mathsf{T}} C_4 \triangle I = 0.\end{aligned}$$

This results in an "inductive" construction: we start from a $3 \times n_v$ matrix of girth larger than 8 to insure that $C_{H_3}^2 \triangle (C_{H_3} + I) = 0$ and thus reduce the above 3 conditions to only the ones that derive conditions on exponents k_l. In [29], we provide all conditions for $n_c = 4$ (derived using a more direct approach) together with simulations of constructions using the algorithms. □

B. Case of Girth $\mathrm{girth}(H_{n_c}) = 2m > 12$

If we want girth larger than 12, we cannot take H_{n_c} to be composed solely of circulants, since it is well-known that a circulant lifting of a 2 × 3 all-one protograph limits the girth to be 12, see, e.g., [5]; therefore, we need to consider a matrix composed of permutation matrices such that some are not circulant. For $n_c = 3$, let P_i, Q_i permutation matrices and

$$H_3 = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ P_1 & P_2 & \cdots & P_{n_v} \\ Q_1 & Q_2 & \cdots & Q_{n_v} \end{bmatrix}, \tag{18}$$

where we can take $P_1 = Q_1 = 1$ without loss of generality.

We start with the remark that the parity-check matrix of every QC-LDPC code with lifting factor $N = N_1 N_2$ can be seen as a pre-lifted matrix formed by following a sequence of liftings, one of factor N_1 followed by a lifting of factor N_2. So one way to construct codes of larger girth than 12 (or to increase its minimum distance) is to rewrite the parity-check matrix of a QC-LDPC code of girth 12 as an equivalent pre-lifted matrix, and then modify some of the exponents to increase the girth and/or the minimum distance.

Theorem 22: Every QC-LDPC code with parity-check matrix H of length $N = N_1 N_2$ is equivalent to a pre-lifted QC-LDPC code of pre-lift size (first lifting factor) N_1 and circulant size (second lifting factor) N_2.

Proof: We can transform each polynomial entry $g(x) = g_0(x^{N_1}) + x g_1(x^{N_1}) + \cdots + x^{N_1 - 1} g_{N_1 - 1}(x^{N_1})$ of H into an $N_1 \times N_1$ equivalent matrix, $[g(x)] \triangleq$

$$\begin{bmatrix} g_0(x) & x g_{N_1-1}(x) & x g_{N_1-2}(x) & \cdots & x g_1(x) \\ g_1(x) & g_0(x) & x g_{N_1-1}(x) & \cdots & x g_{N_1-2}(x) \\ \vdots & \vdots & \cdots & \vdots & \\ g_{N_1-1}(x) & g_{N_1-2}(x) & g_{N_1-3}(x) & \cdots & g_0(x) \end{bmatrix}.$$

In the scalar matrix H we can see this equivalence by performing a sequence of column and row permutations (reordering of the columns and rows). We abuse the notation and use the equality sign between the two equivalent representations (which result in equivalent graphs). ■

For example, if $N_1 = 2$ and $N = 2N_2$, then the entries $x^{2a} = (x^2)^a$ and $x^{2a+1} = x(x^2)^a$ give the following transformations

$$[x^{2a}] = \begin{bmatrix} x^a & 0 \\ 0 & x^a \end{bmatrix} \quad \text{and} \quad [x^{2a+1}] = \begin{bmatrix} 0 & x^{a+1} \\ x^a & 0 \end{bmatrix}.$$

Similarly, if $N = 3N_2$, the equivalent code is

$$[x^{3a}] = \begin{bmatrix} x^a & 0 & 0 \\ 0 & x^a & 0 \\ 0 & 0 & x^a \end{bmatrix}, \quad [x^{3a+1}] = \begin{bmatrix} 0 & 0 & x^{a+1} \\ x^a & 0 & 0 \\ 0 & x^a & 0 \end{bmatrix},$$

and

$$[x^{3a+2}] = \begin{bmatrix} 0 & x^{a+1} & 0 \\ 0 & 0 & x^{a+1} \\ x^a & 0 & 0 \end{bmatrix},$$

with component matrices of size $N_2 \times N_2$. In Appendix B, we revisit Example 3 to show how Theorem 22 can be used to obtain matrices of girth 24.

Example 14: In Appendix C, we consider the $(3, 5)$-regular matrix $H_{3,g>8}$ from Example 13 of girth 10. To improve performance, we first rewrite the code to display a pre-lifted protograph with $N_1 = 2$ and then modify the exponents to achieve girth 12 for the same code length as the single lifting of $H_{3,g>10}$ from Example 13 (giving a code of length 1640 in both cases). The simulated decoding performance of both the original codes, the pre-lifted code, and a random QC-LDPC code with similar parameters are provided in Section VII. □

As mentioned above, the pre-lifted protograph must be free of a 2 × 3 all-one matrix to achieve QC-LDPC matrices with girth larger than 12. In the next examples, we demonstrate how the (equivalent) pre-lift of earlier designs limit the girth to be 12 and how a pre-lift can be selected to avoid such limiting sub-structures.

Example 15: Consider the $(3, 5)$-regular matrix $H_{3,g>10}$ of girth 12 constructed in Example 13. Suppose that we write it as a $N_1 = 3$ prelift, described compactly as (19), shown at the bottom of the next page. As can be seen, several 4-cycles exist in the submatrix (one such example is highlighted by boxed values) that correspond to 2×3 submatrices along with the identity matrices to the left (not shown). Hence, simply modifying exponents could not possibly increase the girth beyond 12 for any N_2.

One can also try to modify the protograph to avoid as many 2×3 all-one matrices as possible. The matrix (20), shown at the bottom of the next page, was modified from (19) using some non-circulant matrices for the pre-lift, but it still contains such 2×3 submatrices (where entries involved are denoted with variables A, B, and C). Again, any choice of circulants in those entries would limit the girth to 12 or less; however, setting $A = B = C = 0$ (masking) eliminates the limiting structures and thus it is possible to further increase the girth.

$$\sum_{u,v \in [n_v]} \left(x^{i_u - i_v} + x^{j_u - j_v} + x^{i_l + (j_u - i_u) - j_v} + x^{j_l + (i_u - j_u) - i_v} \right) \triangle \left(1 + \sum_{u \in [n_v]} \left(x^{i_l - i_u} + x^{j_l - j_u} \right) \right) = 0, \tag{15}$$

$$\sum_{u,v \in [n_v]} \left(x^{(i_u - j_u) + j_v} + x^{i_l + i_u - i_v} + x^{i_l + (i_u - j_u) + (j_v - i_v)} + x^{j_l + (i_u - j_v)} \right) \triangle \left(x^{i_l} + \sum_{u \in [n_v]} \left(x^{i_u} + x^{j_l + i_u - j_u} \right) \right) = 0, \tag{16}$$

$$\sum_{u,v \in [n_v]} \left(x^{(j_u - i_u) + i_v} + x^{i_l + j_u - i_v} + x^{j_l + (j_u - j_v)} + x^{j_l + (j_u - i_u) + (i_v - j_v)} \right) \triangle \left(x^{j_l} + \sum_{u \in [n_v]} \left(x^{j_u} + x^{i_l + j_u - i_u} \right) \right) = 0. \tag{17}$$

Indeed, masking and modifying the exponents as shown above gives a girth 14 irregular code for $N = 891$. Setting $A = x^{1199}$, $B = x^{1239}$, and $C = x^{-579}$ gives a $(3,5)$-regular matrix with girth 12, but where many 12-cycles were eliminated by choosing the original exponents to give an (irregular) code of girth 14. Both the irregular code of girth 14 and the regular code of girth 12 are simulated for $N = 891$ (or length $n = 13,365$) in Section VII. □

In Example 15 we were not successful in obtaining a $(3,5)$-regular QC-LDPC matrix of girth 14, since it is not trivial to avoid the limiting sub-structures in the pre-lifted protograph without thought. We now show that the pre-lifted protograph can be chosen/designed in a deterministic way to avoid such structures. We note that starting from a known 'good' code, e.g., one with a parity-check matrix of girth 12, provides a good base that can be modified relatively easily to increase the girth. Indeed, we see below that some good codes can be observed as derived from a good pre-lifted protograph.

Example 16: We construct a matrix H_3 with submatrix

$$\begin{bmatrix} P_2 & P_3 & P_4 & P_5 \\ Q_2 & Q_3 & Q_4 & Q_5 \end{bmatrix} = \begin{bmatrix} x & x^7 & x^{18} & x^{44} \\ x^3 & x^{158} & x^{136} & x^{106} \end{bmatrix}.$$

This matrix has girth 12 for $N = 279 = 3^2 \cdot 31$. The (submatrix) expansion of H_3 as an equivalent code with an observed 3-prelift is given in (21), shown at the bottom of the next page, where we note that the original matrix was carefully selected such that the pre-lift is free of 2×3 all-one submatrices. The pre-lifted protograph of (21) corresponds to

$$\begin{bmatrix} x & x & 1 & x^2 \\ 1 & x^2 & x & x \end{bmatrix}$$

which does not result in any 2×3 all-one submatrix (even though 4-cycles exist in the protograph) because each row multiplied by x and x^2 does not overlap with the other rows in more than 2 positions.

The submatrix in (22), shown at the bottom of the next page, is obtained by modifying certain exponents in the above that participate in 12-cycles. It has girth 14 for $N = 752$ (code length $n = 11,280$) and also, e.g., for $N = 903$ (code length $n = 13,545$) that we simulate in Section VII to compare with codes of similar lengths from Example 15. □

The final example demonstrates a construction of a girth 14 regular code obtained from a pre-lifted protograph of size $N_1 = 5$ that corresponds to a protograph of girth 6. This choice ensures *a priori* that the 5-cover does not have any 2×3 all-one submatrix.

Example 17: The matrix H_3 with

$$\begin{bmatrix} P_2 & P_3 & P_4 & P_5 \\ Q_2 & Q_3 & Q_4 & Q_5 \end{bmatrix} = \begin{bmatrix} x & x^7 & x^{18} & x^{44} \\ x^{32} & x^{54} & x^{141} & x^{133} \end{bmatrix}$$

as in (23), shown at the bottom of the next page, has girth 12 for $N = 245 = 5 \cdot 49$, i.e., $N_1 = 5, N_2 = 49$. Note that the pre-lifted protograph of H_3 corresponds to

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & x & x^2 & x^3 & x^4 \\ 1 & x^2 & x^4 & x & x^3 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & x & x^2 & x^3 & x^4 \\ 1 & x^2 & x^4 & x^6 & x^8 \end{bmatrix},$$

which has girth 6. So not only does it not have any 2×3 all-one submatrix, it also does not have any 2×2 all-one submatrix, which is a substructure contained in the matrices of P_{12} and P_{14}, both matrices of P_{16}, the first of the matrices listed in P_{18}, and the first two matrices of P_{20}, where P_{2i} are protograph substructures shown in [8] to restrict the girth to $2i$, $i \geq 6$, listed for easier reference in Appendix D. Therefore, a pre-lifted protograph of girth 6 has potential to lead to a girth 14, 16, or 18 code. In fact, if the pre-lift avoids the 6-cycles of the second matrix of P_{18} and the 6-cycles of the last two matrices of P_{20}, then it has potential to yield a girth 20 or a girth 22 code.

We modified the above exponents to obtain a girth 14 matrix for $N = 605$ given by

$$\begin{bmatrix} P_2 & P_3 & P_4 & P_5 \\ Q_2 & Q_3 & Q_4 & Q_5 \end{bmatrix}$$

as in (24), shown at the bottom of the next page. Such modification can be achieved relatively easily by masking and then unmasking circulants one by one and choosing them such that the girth is 14 (or larger as desired). □

Theorem 23: Let B be an (n_c, n_v)-regular $n_c N_1 \times n_v N_1$ parity-check matrix of a protograph-based QC-LDPC code of girth 6. Then there exist a lifting factor N_2 for which B can be lifted to obtain a QC-LDPC code with parity-check matrix H_{n_c} of girth 14, 16, or 18, as desired.

$$\begin{bmatrix} P_2 & P_3 & P_4 & P_5 \\ Q_2 & Q_3 & Q_4 & Q_5 \end{bmatrix} = \left[\begin{array}{ccc|ccc|ccc|ccc} 0 & 0 & x & 0 & 0 & \boxed{x^3} & x^4 & 0 & 0 & 0 & \boxed{x^7} & 0 \\ 1 & 0 & 0 & x^2 & 0 & 0 & 0 & x^4 & 0 & 0 & 0 & x^7 \\ 0 & 1 & 0 & 0 & x^2 & 0 & 0 & 0 & x^4 & x^6 & 0 & 0 \\ \hline x^{22} & 0 & 0 & 0 & 0 & \boxed{x^{36}} & 0 & 0 & x^{82} & 0 & \boxed{x^{65}} & 0 \\ 0 & x^{22} & 0 & x^{35} & 0 & 0 & x^{81} & 0 & 0 & 0 & 0 & x^{65} \\ 0 & 0 & x^{22} & 0 & x^{35} & 0 & 0 & x^{81} & 0 & x^{64} & 0 & 0 \end{array}\right]. \tag{19}$$

$$\begin{bmatrix} P_2 & P_3 & P_4 & P_5 \\ Q_2 & Q_3 & Q_4 & Q_5 \end{bmatrix} = \left[\begin{array}{ccc|ccc|ccc|ccc} 0 & 0 & x & 0 & 0 & x^3 & 0 & x^{39} & 0 & 0 & x^{29} & 0 \\ 1 & 0 & 0 & x^9 & 0 & 0 & 0 & 0 & x^4 & 0 & 0 & x^{59} \\ 0 & 1 & 0 & 0 & x^{17} & 0 & x^{11} & 0 & 0 & x^{71} & 0 & 0 \\ \hline 0 & x^{118} & 0 & 0 & 0 & x^{136} & 0 & 0 & x^{290} & x^{353} & 0 & 0 \\ 0 & 0 & x^{32} & 0 & x^{479} & 0 & A & 0 & 0 & 0 & B & 0 \\ x^{209} & 0 & 0 & C & 0 & 0 & 0 & x^{800} & 0 & 0 & 0 & x^{-319} \end{array}\right]. \tag{20}$$

Proof: From the limiting substructures found in [8] and listed for easier reference in Appendix D, we observe that all the structures that need to be avoided in order to allow for girth 14, 16, and 18 contain a 2 × 2 all-one submatrix (they have girth 4). These structures are discussed in Example 17. Since B is of girth 6 and it acts as a pre-lifted protograph used on an $n_c \times n_v$ all-one protograph to obtain H_{n_c}, then H_{n_c} cannot possibly contain any of these substructures. ■

Remark 15: We remind the reader that for girth 14 and above we use the computer to search for the next good value and used a value of N large enough to allow such a value. Algorithms like the ones we presented in Section V-A for girth up to 12 could be developed, but due to the fact that each protograph needs to be considered separately, it will answer only this case rather than allow for a general algorithm like those earlier. This could nevertheless be attractive if the protograph has been optimized; we show how this could be done for the NASA CCSDS protograph in Section VI. □

Theorem 24: Let B be an (n_c, n_v)-regular $n_cN_1 \times n_vN_1$ parity-check matrix of a protograph-based QC-LDPC code of girth 8. Then there exist lifting factors N_2 for which B can be lifted to obtain a QC-LDPC code with parity-check matrix H_{n_c} of girth 20 or 22, as desired.

Proof: From the limiting substructures found in [8] and listed for easier reference in Appendix D, and from the discussions in Example 17, most of the forbidden structures P_{18} and P_{20} for girth 20 and 22 contain a 2×2 all-one matrix. There is one structure in P_{18} and two in P_{20} that have girth 6. Taking B of girth 8 guarantees that these structures are not present in the lifted H_{n_c} from B. ■

Remark 16: Theorems 23 and 24 are only sufficient but not necessary. Example 16 does not satisfy these theorems but demonstrates that a 3 × 5 matrix of girth 14 can be obtained

$$\left[\begin{array}{ccc|ccc|ccc|ccc}
0 & 0 & x & 0 & 0 & x^{3} & x^{6} & 0 & 0 & 0 & x^{15} & 0 \\
1 & 0 & 0 & x^{2} & 0 & 0 & 0 & x^{6} & 0 & 0 & 0 & x^{15} \\
0 & 1 & 0 & 0 & x^{2} & 0 & 0 & 0 & x^{6} & x^{14} & 0 & 0 \\
\hline
x & 0 & 0 & 0 & x^{53} & 0 & 0 & 0 & x^{46} & 0 & 0 & x^{36} \\
0 & x & 0 & 0 & 0 & x^{53} & x^{45} & 0 & 0 & x^{35} & 0 & 0 \\
0 & 0 & x & x^{52} & 0 & 0 & 0 & x^{45} & 0 & 0 & x^{35} & 0
\end{array}\right]. \tag{21}$$

$$\left[\begin{array}{ccc|ccc|ccc|ccc}
0 & 0 & x & 0 & 0 & x^{3} & x^{6} & 0 & 0 & 0 & x^{15} & 0 \\
1 & 0 & 0 & x^{5} & 0 & 0 & 0 & x^{23} & 0 & 0 & 0 & x^{19} \\
0 & x^{7} & 0 & 0 & x^{11} & 0 & 0 & 0 & x^{29} & x^{42} & 0 & 0 \\
\hline
x^{25} & 0 & 0 & 0 & x^{61} & 0 & 0 & 0 & x^{94} & 0 & 0 & x^{153} \\
0 & x^{64} & 0 & 0 & 0 & x^{180} & x^{239} & 0 & 0 & x^{358} & 0 & 0 \\
0 & 0 & x^{9} & x^{143} & 0 & 0 & 0 & x^{256} & 0 & 0 & x^{474} & 0
\end{array}\right]. \tag{22}$$

$$\left[\begin{array}{ccccc|ccccc|ccccc|ccccc}
0 & 0 & 0 & 0 & x & 0 & 0 & 0 & x^{2} & 0 & 0 & 0 & x^{4} & 0 & 0 & 0 & x^{9} & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & x^{2} & 0 & 0 & 0 & x^{4} & 0 & 0 & 0 & x^{9} & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & x & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & x^{4} & 0 & 0 & 0 & x^{9} & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & x & 0 & 0 & 0 & x^{3} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & x^{9} \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & x & 0 & 0 & 0 & x^{3} & 0 & 0 & 0 & x^{8} & 0 & 0 & 0 & 0 \\
\hline
0 & 0 & 0 & x^{7} & 0 & 0 & x^{11} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & x^{29} & 0 & 0 & x^{27} & 0 & 0 \\
0 & 0 & 0 & 0 & x^{7} & 0 & 0 & x^{11} & 0 & 0 & x^{28} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & x^{27} & 0 \\
x^{6} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & x^{11} & 0 & 0 & x^{28} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & x^{27} \\
0 & x^{6} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & x^{11} & 0 & 0 & x^{28} & 0 & 0 & x^{26} & 0 & 0 & 0 & 0 \\
0 & 0 & x^{6} & 0 & 0 & x^{10} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & x^{28} & 0 & 0 & x^{26} & 0 & 0 & 0
\end{array}\right]. \tag{23}$$

$$\left[\begin{array}{ccccc|ccccc|ccccc|ccccc}
0 & 0 & 0 & 0 & x & 0 & 0 & 0 & x^{2} & 0 & 0 & 0 & x^{4} & 0 & 0 & 0 & x^{9} & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & x^{2} & 0 & 0 & 0 & x^{4} & 0 & 0 & 0 & x^{9} & 0 & 0 \\
0 & x^{3} & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & x^{8} & 0 & 0 & 0 & x & 0 \\
0 & 0 & x^{9} & 0 & 0 & 0 & x^{13} & 0 & 0 & 0 & x^{19} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & x^{23} \\
0 & 0 & 0 & x^{7} & 0 & 0 & 0 & x^{19} & 0 & 0 & 0 & x^{34} & 0 & 0 & 0 & x^{44} & 0 & 0 & 0 & 0 \\
\hline
0 & 0 & 0 & x^{29} & 0 & 0 & x^{40} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & x^{79} & 0 & 0 & x^{99} & 0 & 0 \\
0 & 0 & 0 & 0 & x^{29} & 0 & 0 & x^{54} & 0 & 0 & x^{115} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & x^{135} & 0 \\
x^{23} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & x^{73} & 0 & 0 & x^{129} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & x^{215} \\
0 & x^{55} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & x^{145} & 0 & 0 & x^{209} & 0 & 0 & x^{313} & 0 & 0 & 0 & 0 \\
0 & 0 & x^{301} & 0 & 0 & x^{356} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & x^{432} & 0 & 0 & x^{512} & 0 & 0 & 0
\end{array}\right]. \tag{24}$$

from the all-one matrix pre-lifted with $N_1 = 3$ provided that the pre-lifted protograph excludes the limiting structure. □

VI. Protographs With Multiple Edges

In this section, we briefly address the case in which the original protograph is not all-one, to demonstrate how the theory and techniques can be extended to such protographs. In particular, we revisit the earlier example of the NASA CCSDS protograph that was discussed in the context of sums of permutation matrices in Examples 2 and 6, and now connect to the perspectives developed in Section V.

We proceed then to consider a 4×8 protograph that contains entries equal to 2 (multiple edges) and zero matrices as shown in (10). Without loss of generality, we can let $P_8 = Q_5 = R_6 = S_7 = I$ and assume the reduced matrix in (25), shown at the bottom of the next page, because, by multiplying rows/columns with permutation matrices, we obtain equivalent graphs and equivalent corresponding codes.

In this case, $HH^{\mathsf{T}} = AA^{\mathsf{T}} + BB^{\mathsf{T}} = 8I + \underbrace{C_A + C_B}_{C_H}$ where, unlike in the case of protographs without multiple edges, $C_A = (C_{A,ij})_{i,j \in [4]}$ and, therefore $C_H = C_A + C_B$, has non-zero entries on the main diagonal, i.e., $C_{A,ii} \neq 0$, and $C_{H,ii} \neq 0$, respectively. The component matrices $C_{A,ij}$ for C_A are computed as

$$C_{A,11} \triangleq x^{a_1} + x^{-a_1},\ C_{A,22} \triangleq x^{b_2} + x^{-b_2},$$
$$C_{A,33} \triangleq x^{c_3} + x^{-c_3},\ C_{A,44} \triangleq x^{d_4} + x^{-d_4},$$
$$C_{A,12} \triangleq C^{\mathsf{T}}_{A,21} \triangleq x^{-b_1} + x^{a_2} + \sum_{j=1}^{4} x^{a_j - b_j},$$
$$C_{A,13} \triangleq C^{\mathsf{T}}_{A,31} \triangleq x^{-c_1} + x^{a_3} + \sum_{j=1}^{4} x^{a_j - c_j},$$
$$C_{A,14} \triangleq C^{\mathsf{T}}_{A,41} \triangleq x^{-d_1} + x^{a_4} + \sum_{j=1}^{4} x^{a_j - d_j},$$
$$C_{A,23} \triangleq C^{\mathsf{T}}_{A,32} \triangleq x^{-c_2} + x^{b_3} + \sum_{j=1}^{4} x^{b_j - c_j},$$
$$C_{A,24} \triangleq C^{\mathsf{T}}_{A,42} \triangleq x^{-d_2} + x^{b_4} + \sum_{j=1}^{4} x^{b_j - d_j},$$
$$C_{A,34} \triangleq C^{\mathsf{T}}_{A,43} \triangleq x^{-d_3} + x^{c_4} + \sum_{j=1}^{4} x^{c_j - d_j},$$

and the component matrices $C_{B,ij}$ for C_B are

$$C_{B,11} \triangleq 0,\ C_{B,22} \triangleq 0,\ C_{B,33} \triangleq 0,\ C_{B,44} \triangleq 0,$$
$$C_{B,12} \triangleq C^{\mathsf{T}}_{B,21} \triangleq \sum_{j=7,8} x^{a_j - b_j}, C_{B,13} \triangleq C^{\mathsf{T}}_{B,31} \triangleq \sum_{j=6,8} x^{a_j - c_j},$$
$$C_{B,14} \triangleq C^{\mathsf{T}}_{B,41} \triangleq \sum_{j=6,7} x^{a_j - d_j}, C_{B,23} \triangleq C^{\mathsf{T}}_{B,32} \triangleq \sum_{j=5,8} x^{b_j - c_j},$$
$$C_{B,24} \triangleq C^{\mathsf{T}}_{B,42} \triangleq \sum_{j=5,7} x^{b_j - d_j}, C_{B,34} \triangleq C^{\mathsf{T}}_{B,43} \triangleq \sum_{j=5,6} x^{c_j - d_j}.$$

Therefore, we obtain C_H as in (26), shown at the bottom of the next page.

Note that Theorem 5 still holds, so in computing B_t we only need to consider powers of C_H. For example, if we desire to avoid 4-cycles then $C_H \triangle I = 0$ must hold, which is equivalent to

$$\begin{cases} C_{A,ii} \triangle I = 0,\ \text{for all } i \in [4], \\ C_{A,ij} + C_{B,ij} \triangle 0 = 0,\ \text{for all } i, j \in [4], i \neq j. \end{cases}$$

Equivalently, no value in the set $\{2a_1, 2b_2, 2c_3, 2d_4\}$ is 0 modulo N, and each of the sets below are of maximal size

$$\{-b_1, a_2, a_j - b_j, j \in [8], j \neq 5, 6\},$$
$$\{-c_1, a_3, a_j - c_j, j \in [8], j \neq 5, 7\},$$
$$\{-d_1, a_4, a_j - d_j, j \in [8], j \neq 5, 8\},$$
$$\{-c_2, b_3, b_j - c_j, j \in [8], j \neq 6, 7\},$$
$$\{-d_2, b_4, b_j - d_j, j \in [8], j \neq 6, 8\},$$
$$\{-d_3, c_4, c_j - d_j, j \in [8], j \neq 7, 8\}.$$

A fast algorithm with comparative run-times similar to those in Section V-A can be created to construct matrices H satisfying the conditions above.

Example 18: We revisit the matrix $H_{(128,64)}$ from Example 2, this time as a 4×8 protograph-based matrix of the form above, in order to compute the matrix $C_{H_{(128,64)}}$ and show that it satisfies the conditions for the matrix $H_{(128,64)}$ to have girth 6. Indeed, the matrix in (27), shown at the bottom of the next page, with $N = 16$, satisfies all the conditions above (these can be easily checked by hand), and hence it has girth 6. □

A similar approach and theory to that developed above for the NASA CCSDS protograph can be developed for arbitrary protographs with multiple edges.

VII. Simulation Results

To verify the performance of the constructed codes, computer simulations were performed assuming binary phase shift keyed (BPSK) modulation and a binary-input additive white Gaussian noise (AWGN) channel. The sum-product message passing decoder was allowed a maximum of 100 iterations and employed a syndrome-check based stopping rule.

In Fig. 1, we plot the bit error rate (BER) for the $R \approx 2/5$, $(3, 5)$-regular QC-LDPC codes from Example 13. We show the performance of two codes of length $n = 790$ ($N = 158$) and $n = 1640$ ($N = 328$) derived from $H_{3,g>8}$, both with girth 10, the performance of the code of length $n = 1640$ ($N = 328$) derived from $H_{3,g>10}$ with girth 12, and two random QC liftings of the all-ones 3×5 protograph with the same length ($N = 328$) and respective girths of 6 and 8. We observe that the larger lifting factor results in an improved waterfall as expected and that the error floors of the large girth codes are lower than the random code.[11] Finally, also shown is the pre-lifted version of the code from Example 14 and Appendix C with $N_1 = 2$ and $N_2 = 164$, which results in a $(3, 5)$-regular code of length $n = 1640$. In this construction, some exponents were modified to break some circular sub-structures and we see that the error floor is lowered compared to the single lifts.

[11] An additional example comparing single lifts to random codes with various girth was presented in [1].

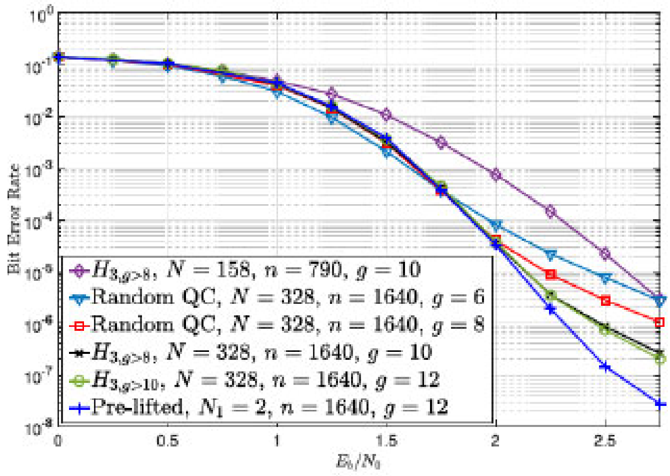

Fig. 1. Simulated decoding performance in terms of BER for the $R = 2/5$ QC-LDPC codes from Examples 13 and 14.

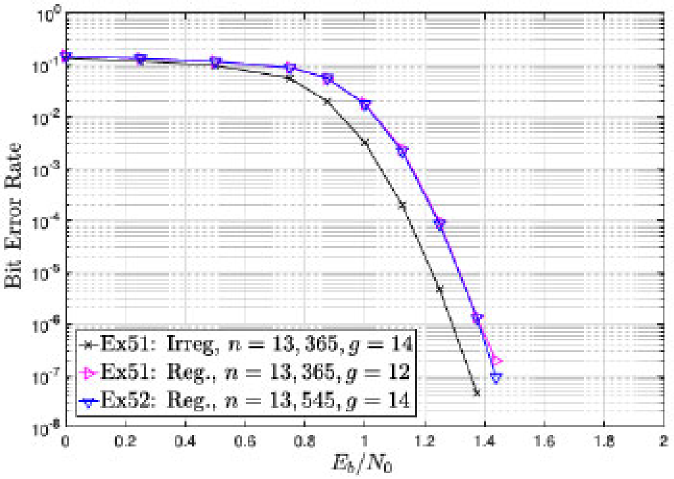

Fig. 2. Simulated decoding performance in terms of BER for the $R = 2/5$ QC-LDPC codes from Examples 15 and 16.

In Fig. 2, we plot the BER for the $R \approx 2/5$ QC-LDPC codes with longer block lengths from Examples 15 and 16. We remark that these high girth codes display no indication of an error-floor, at least down to a BER of 10^{-7}. The regular codes from Example 15 (reduced multiplicity of 12 cycles) and 16 (with girth 14) have similar performance in the simulated range, but we anticipate deviation at higher SNRs where the 12-cycles are involved in trapping sets. For reference, the iterative decoding threshold for $(3, 5)$-regular LDPC codes is 0.96dB [30]. The irregular code of girth 14 is shown to outperform the regular codes in the simulated range. We remind the reader that the irregular code was obtained by masking some circulants from the pre-lifted code to increase the girth. Such a strategy can yield good optimized irregular LDPC codes.[12]

[12] We note that although the emphasis in this paper is not to construct optimized QC-LDPC codes, the performance of these codes is superior to those of, e.g., comparable high girth but longer codes from [31].

$$H \triangleq [\ A \mid B\ ] \triangleq \left[\begin{array}{cccc|cccc} I+P_1 & P_2 & P_3 & P_4 & 0 & P_6 & P_7 & P_8 \\ Q_1 & I+Q_2 & Q_3 & Q_4 & Q_5 & 0 & Q_7 & Q_8 \\ R_1 & R_2 & I+R_3 & R_4 & R_5 & R_6 & 0 & R_8 \\ \multicolumn{4}{c|}{\underbrace{S_1 \qquad\quad S_2 \qquad\quad S_3 \qquad\quad I+S_4}_{A}} & \multicolumn{4}{c}{\underbrace{S_5 \quad S_6 \quad S_7 \quad 0}_{B}} \end{array}\right]$$
$$= \left[\begin{array}{cccc|cccc} 1+x^{a_1} & x^{a_2} & x^{a_3} & x^{a_4} & 0 & x^{a_6} & x^{a_7} & x^{a_8} \\ x^{b_1} & 1+x^{b_2} & x^{b_3} & x^{b_4} & x^{b_5} & 0 & x^{b_7} & x^{b_8} \\ x^{c_1} & x^{c_2} & 1+x^{c_3} & x^{c_4} & x^{c_5} & x^{c_6} & 0 & x^{c_8} \\ x^{d_1} & x^{d_2} & x^{d_3} & 1+x^{d_4} & x^{d_5} & x^{d_6} & x^{d_7} & 0 \end{array}\right]. \tag{25}$$

$$\begin{bmatrix} x^{-a_1}+x^{a_1} & x^{-b_1}+x^{a_2}+\sum\limits_{\substack{j\in[8]\\ j\neq 5,6}} x^{a_j-b_j} & x^{-c_1}+x^{a_3}+\sum\limits_{\substack{j\in[8]\\ j\neq 5,7}} x^{a_j-c_j} & x^{-d_1}+x^{a_4}+\sum\limits_{\substack{j\in[8]\\ j\neq 5,8}} x^{a_j-d_j} \\ x^{-a_2}+x^{b_1}+\sum\limits_{\substack{j\in[8]\\ j\neq 5,6}} x^{-a_j+b_j} & x^{-b_2}+x^{b_2} & x^{-c_2}+x^{b_3}+\sum\limits_{\substack{j\in[8]\\ j\neq 6,7}} x^{b_j-c_j} & x^{-d_2}+x^{b_4}+\sum\limits_{\substack{j\in[8]\\ j\neq 6,8}} x^{b_j-d_j} \\ x^{-a_3}+x^{c_1}+\sum\limits_{\substack{j\in[8]\\ j\neq 5,7}} x^{-a_j+c_j} & x^{-b_3}+x^{c_2}+\sum\limits_{\substack{j\in[8]\\ j\neq 6,7}} x^{-b_j+c_j} & x^{-c_3}+x^{c_3} & x^{-d_3}+x^{c_4}+\sum\limits_{\substack{j\in[8]\\ j\neq 7,8}} x^{c_j-d_j} \\ x^{-a_4}+x^{d_1}+\sum\limits_{\substack{j\in[8]\\ j\neq 5,8}} x^{-a_j+d_j} & x^{-b_4}+x^{d_2}+\sum\limits_{\substack{j\in[8]\\ j\neq 6,8}} x^{-b_j+d_j} & x^{-c_4}+x^{d_3}+\sum\limits_{\substack{j\in[8]\\ j\neq 7,8}} x^{-c_j+d_j} & x^{-d_4}+x^{d_4} \end{bmatrix}. \tag{26}$$

$$H_{(128,64)} \triangleq \left[\begin{array}{cccc|cccc} 1+x^7 & x^2 & x^{14} & x^6 & 0 & 1 & x^{13} & 1 \\ x^6 & 1+x^{15} & 1 & x & 1 & 0 & 1 & x^7 \\ x^4 & x & 1+x^{15} & x^{14} & x^{11} & 1 & 0 & x^3 \\ 1 & x & x^9 & 1+x^{13} & x^{14} & x & 1 & 0 \end{array}\right]. \tag{27}$$

VIII. Concluding Remarks

In this paper we provided a unifying framework under which all constructions of girth between 6 and 12 can be included. Towards this goal, we gave necessary and sufficient conditions for the Tanner graph of a protograph-based QC-LDPC code to have girth between 6 and 12. We also showed how these girth conditions can be used to write fast (run-time of several seconds) algorithms to construct such codes and how to employ a double graph-lifting procedure, called pre-lifting, in order to exceed girth 12. We showed that the cases of variable node degrees $n_c = 2$, 3, and 4 that we consider in this paper are not just particular cases, but provide the girth framework for the $n_c \times n_v$ all-one protograph, for *all* $n_c \geq 2$.

We also presented a new perspective on $n_cN \times n_vN$ LDPC protograph-based parity-check matrices by viewing them as n_cN rows of a parity-check matrix equal to the sum of certain $n_vN \times n_vN$ permutation matrices and highlighted an important connection between $n_c \times n_v$ protographs, for any $n_c \geq 2$, and protographs with $n_c = 2$. Finally, we exemplifed how the results and methodology can be used and adapted to analyze the girth of the Tanner graph of any parity-check matrix on an irregular, multi-edge protograph of the NASA CCSDS LDPC code.

Appendix A
Proof of Lemma 7

Proof: Every matrix H has a graph that is equivalent to that of a matrix in reduced form, where the first row as well as the first column of H are made of identity matrices. For this reduced matrix, the corresponding matrix C_{ij} contains the identity matrix as a submatrix. It follows that set of N 6-cycles must exist, where a cycle is formed by tracking edges going from any entry 1 in the position (i, i) of C_{21} (which exists because C_{21} has I as submatrix) to the 1 in the position (i, i) of C_{31}, to the 1 in the position (i, i) of C_{32}, to the 1 in the position (i, i) of C_{12}, to the 1 in the position (i, i) of C_{13}, to the 1 in the position (i, i) of C_{23}, and back to the 1 in the position (i, i) of C_{21}, thereby visiting the matrices as shown in the following diagram:

$$\begin{tikzcd}
 & C_{12} \arrow[r] & C_{13} \arrow[d] \\
C_{21} \arrow[d] & & C_{23}. \arrow[ll] \\
C_{31} \arrow[r] & C_{32} \arrow[uu] &
\end{tikzcd}$$

(We can easily generalize this sequence following the example above.) We obtain that $\mathrm{girth}(C_H) \leq 6$, for any $n_c \times n_v$ protograph based matrix with all ones.

Similarly, if $n_c \geq 4$, $\begin{bmatrix} C_{13} & C_{14} \\ C_{23} & C_{24} \end{bmatrix}$ is always a submatrix of C_H. As above, we can reduce these matrices such that I is a submatrix of each one of C_{ij} in the above matrix, thereby exposing at least N 4-cycles in the graph of C_H. ■

Appendix B
Example 3 Revisited

In order to exemplify Theorem 22, we revisit Example 3 and show how we obtained the matrices of girth 24. Suppose that a 2×3 protograph based code has $I + P_2 + P_3 = 1 + x^2 + x^3$ of girth 6 (it satisfies the conditions of girth 6) or, equivalently, $\mathrm{girth}(H) = 12$. We rewrite this as

$$1 + x^2 + x^3 = \begin{bmatrix} 1+x & x^2 \\ x & 1+x \end{bmatrix} = I + \begin{bmatrix} x & 0 \\ 0 & x \end{bmatrix} + \begin{bmatrix} 0 & x^2 \\ x & 0 \end{bmatrix},$$
$$P_2 = \begin{bmatrix} x & 0 \\ 0 & x \end{bmatrix}, \; P_3 = \begin{bmatrix} 0 & x^2 \\ x & 0 \end{bmatrix}.$$

We now slightly modify one entry in this quasi-cyclic parity-check matrix, enough to break the equivalence to the cyclic code. For example, the 18×18 matrix

$$I + P_2' + P_3 \triangleq \begin{bmatrix} 1+x & x^2 \\ x & 1+x^5 \end{bmatrix},$$
$$P_2' = \begin{bmatrix} x & 0 \\ 0 & x^5 \end{bmatrix}, \; P_3 = \begin{bmatrix} 0 & x^2 \\ x & 0 \end{bmatrix},$$

has an associated graph with girth 8. Note that we had to increase the size of the circulant matrices in order to observe an increase in girth. It follows that the LDPC code with 36×54 parity-check matrix

$$\begin{bmatrix} I & I & I \\ I & P_2' & P_3 \end{bmatrix} = \left[\begin{array}{c|cc|cc} I & \multicolumn{2}{c|}{I} & \multicolumn{2}{c}{I} \\ \hline \multirow{2}{*}{I} & x & 0 & 0 & x^2 \\ & 0 & x^5 & x & 0 \end{array}\right]$$
$$= \left[\begin{array}{cc|cc|cc} 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ \hline 1 & 0 & x & 0 & 0 & x^2 \\ 0 & 1 & 0 & x^5 & x & 0 \end{array}\right]$$

has girth 16.

Similarly, we can start from the cyclic code of length 21 with the same parity-check matrix $1 + x^2 + x^3$. We reorder the rows and the columns of the parity-check matrix or, equivalently, make the replacements such that

$$I + P_2 + P_3 = \begin{bmatrix} 1+x & x & 0 \\ 0 & 1+x & x \\ 1 & 0 & 1+x \end{bmatrix},$$
$$P_2 = \begin{bmatrix} x & 0 & 0 \\ 0 & x & 0 \\ 0 & 0 & x \end{bmatrix}, \; P_3 = \begin{bmatrix} 0 & x & 0 \\ 0 & 0 & x \\ 1 & 0 & 0 \end{bmatrix}.$$

We modify it as

$$I + P_2' + P_3' \triangleq \begin{bmatrix} 1+x & x & 0 \\ 0 & 1+x^{13} & x^2 \\ x & 0 & 1+x^7 \end{bmatrix},$$
$$P_2' = \begin{bmatrix} x & 0 & 0 \\ 0 & x^{13} & 0 \\ 0 & 0 & x^7 \end{bmatrix}, \; Q_2' = \begin{bmatrix} 0 & x & 0 \\ 0 & 0 & x^2 \\ x & 0 & 0 \end{bmatrix},$$

to obtain girth 8 for a circulant size $N = 11$, girth 10 if the size of the circulant is increased to $N = 31$, and girth 12 if the size is increased to $N = 41$. Therefore, the corresponding parity-check matrix H has girth 24 for $N = 41$.

Appendix C
Example 13 Revisited

We consider the $(3, 5)$-regular matrix $H_{3,g>8}$ from Example 13 of girth 10. To improve performance, we rewrite the

$$H_{3,g>8} = \left[\begin{array}{cc|cc|cc|cc|cc} 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ \hline 1 & 0 & 0 & x & 0 & x^4 & x^6 & 0 & x^{10} & 0 \\ 0 & 1 & 1 & 0 & x^3 & 0 & 0 & x^6 & 0 & x^{10} \\ \hline 1 & 0 & x^{33} & 0 & x^{53} & 0 & x^{122} & 0 & x^{97} & 0 \\ 0 & 1 & 0 & x^{33} & 0 & x^{53} & 0 & x^{122} & 0 & x^{97} \end{array}\right]. \quad (28)$$

$$H_{3,g>10} = \left[\begin{array}{cc|cc|cc|cc|cc} 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ \hline 1 & 0 & 0 & x & 0 & x^4 & x^6 & 0 & x^{10} & 0 \\ 0 & 1 & 1 & 0 & x^3 & 0 & 0 & x^6 & 0 & x^{10} \\ \hline 1 & 0 & x^{33} & 0 & x^{53} & 0 & x^{122} & 0 & x^{97} & 0 \\ 0 & 1 & 0 & x^{33} & 0 & x^{53} & 0 & x^{93} & 0 & x^{122} \end{array}\right]. \quad (29)$$

codes we constructed to display a pre-lifted protograph with $N_1 = 2$ as in (28), shown at the top of the page. The matrix (29), also shown at the top of the page, was modified in two entries, such that the 3×4 submatrices do not have all permutation matrices circulant (and hence commutative) and thus they can observe an increase in minimum distance and in girth. We need to modify at least one of every group of 4. The matrix shown in (29) has girth 10 for $N = 123$ and girth 12 for $N = 164$. Simulation results for the second code are provided in Section VII.

Appendix D
Substructures P_{2i} That Limit Girth to $2i$, $i \geq 6$, From [8]

We use the notation found in [8]. Let P_{2i} denote the incidence matrix of the subgraph of a protograph, which gives rise to an inevitable $2i$-cycle such that no inevitable cycles of length smaller than $2i$ are included in it. Therefore, if a protograph contains the submatrix P_{2i} or P_{2i}^{T}, for $i \geq 6$, then its protograph code cannot have girth larger than $2i$.

Lemma 25 [8]: The matrices P_{2i} are as follows:

$$P_{12} = \left\{ \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix} \right\}; P_{14} = \left\{ \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix} \right\};$$

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

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

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

References

[1] R. Smarandache and D. G. M. Mitchell, "Necessary and sufficient girth conditions for Tanner graphs of quasi-cyclic LDPC codes," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Melbourne, VIC, Australia, Jul. 2021, pp. 380–385.

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

[3] Z. Wang and Z. Cui, "A memory efficient partially parallel decoder architecture for quasi-cyclic LDPC codes," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 15, no. 4, pp. 483–488, Apr. 2007.

[4] T. J. Richardson and R. L. Urbanke, "Efficient encoding of low-density parity-check codes," *IEEE Trans. Inf. Theory*, vol. 47, no. 2, pp. 638–656, Feb. 2001.

[5] 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.

[6] 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.

[7] 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.

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

[9] H. Park, S. Hong, J.-S. No, and D.-J. Shin, "Design of multiple-edge protographs for QC LDPC codes avoiding short inevitable cycles," *IEEE Trans. Inf. Theory*, vol. 59, no. 7, pp. 4598–4614, Jul. 2013.

[10] M. Karimi and A. H. Banihashemi, "On the girth of quasi-cyclic protograph LDPC codes," *IEEE Trans. Inf. Theory*, vol. 59, no. 7, pp. 4542–4552, Jul. 2013.

[11] D. G. M. Mitchell, R. Smarandache, and D. J. Costello, Jr., "Quasi-cyclic LDPC codes based on pre-lifted protographs," *IEEE Trans. Inf. Theory*, vol. 60, no. 10, pp. 5856–5874, Oct. 2014.

[12] A. Tasdighi, A. H. Banihashemi, and M. R. Sadeghi, "Efficient search of girth-optimal QC-LDPC codes," *IEEE Trans. Inf. Theory*, vol. 62, no. 4, pp. 1552–1564, Apr. 2016.

[13] M. Battaglioni, M. Baldi, and G. Cancellieri, "Improving the minimum distance of QC-LDPC codes by removing cycles," in *Proc. AEIT Int. Annu. Conf. (AEIT)*, Sep. 2020, pp. 1–5.

[14] J. A. McGowan and R. C. Williamson, "Loop removal from LDPC codes," in *Proc. IEEE Inf. Theory Workshop*, Paris, France, Mar./Apr. 2003, pp. 230–233.

[15] X. Wu, X. You, and C. Zhao, "A necessary and sufficient condition for determining the girth of quasi-cyclic LDPC codes," *IEEE Trans. Commun.*, vol. 56, no. 6, pp. 854–857, Jun. 2008.

[16] S. Lin, Y. Kou, and M. P. C. Fossorier, "Finite geometry low density parity-check codes: Construction, structure, and decoding," in *Codes, Graphs, and Systems* (The Kluwer International Series in Engineering and Computer Science), R. Blahut and R. Koetter, Eds. Boston, MA, USA: Springer, 2002, vol. 670.

[17] R. Smarandache and P. O. Vontobel, "Pseudo-codeword analysis of Tanner graphs from projective and Euclidean planes," *IEEE Trans. Inf. Theory*, vol. 53, no. 7, pp. 2376–2393, Jul. 2007.

[18] *Short Blocklength LDPC Codes for TC Synchronization and Channel Coding*, Consutlative Committee Space Datas Syst. Orange Book, 2012.

[19] D. Divsalar, S. Dolinar, C. R. Jones, and K. Andrews, "Capacity-approaching protograph codes," *IEEE J. Sel. Areas Commun.*, vol. 27, no. 6, pp. 876–888, Aug. 2009.

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

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

[22] M. Fujisawa and S. Sakata, "A class of quasi-cyclic regular LDPC codes from cyclic difference families with girth 8," in *Proc. Int. Symp. Inf. Theory (ISIT)*, 2005, pp. 2290–2294.

[23] M. Esmaeili and M. Javedankherad, "4-cycle free LDPC codes based on difference sets," *IEEE Trans. Commun.*, vol. 60, no. 12, pp. 3579–3586, Dec. 2012.

[24] P. Daqin, Z. Shumin, and S. Jing, "A novel construction of QC-LDPC codes based on combinatorial mathematics," *Proc. Comput. Sci.*, vol. 131, pp. 786–792, Jan. 2018.

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

[26] J. Thorpe, "Low-density parity-check (LDPC) codes constructed from protographs," Jet Propuls. Lab., Pasadena, CA, USA, INP Prog. Rep. 42-154, Aug. 2003.

[27] R. Smarandache, D. G. M. Mitchell, and D. J. Costello, "Partially quasi-cyclic protograph-based LDPC codes," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Kyoto, Japan, Jun. 2011, pp. 1–5.

[28] D. G. M. Mitchell, R. Smarandache, and D. J. Costello, "Constructing good QC-LDPC codes by pre-lifting protographs," in *Proc. IEEE Inf. Theory Workshop (ITW)*, Lausanne, Switzerland, Sep. 2012, pp. 202–206.

[29] A. Gomez-Fonseca, R. Smarandache, and D. G. M. Mitchell, "Necessary and sufficient girth conditions for LDPC Tanner graphs with denser protographs," in *Proc. 11th Int. Symp. Topics Coding (ISTC)*, Montreal, QC, Canada, Aug. 2021, pp. 1–5.

[30] T. J. Richardson and R. L. Urbanke, *Modern Coding Theory*. Cambridge, U.K.: Cambridge Univ. Press, 2008.

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

Roxana Smarandache (Senior Member, IEEE) received the B.S. degree in mathematics with a thesis in number theory from the University of Bucharest in 1996, the M.Sc. degree in 1997, and the Ph.D. degree in mathematics with a thesis in coding theory from the University of Notre Dame, IN, USA, in 2001.

After spending 11 years on the Faculty of San Diego State University, she joined the University of Notre Dame in 2012, where she is a Professor of mathematics and electrical engineering. From 2021 to 2022, she is on a Sabbatical Leave at the Swiss Federal Institute of Technology in Zürich, Switzerland (ETHZ). Her research interests are in coding theory, combinatorics, and graph theory. In particular, she focuses on low-density parity check codes, iterative and linear programming decoding, and convolutional codes.

Dr. Smarandache was an Associate Editor of the *Advances in Mathematics of Communications* (AMC) journal from 2013 to 2014 and the IEEE TRANSACTIONS ON INFORMATION THEORY from 2014 to 2017.

David G. M. Mitchell (Senior Member, IEEE) received the Ph.D. degree in electrical engineering from the University of Edinburgh, U.K., in 2009. From 2009 to 2015, he held Post-Doctoral Research Associate and Visiting Assistant Professor positions with the Department of Electrical Engineering, University of Notre Dame, USA. Since 2015, he has been an Assistant Professor with the Klipsch School of Electrical and Computer Engineering, New Mexico State University, USA. His research interests include digital communications, with emphasis on error control coding and information theory. He was a recipient of the National Science Foundation Faculty Early Career Award in 2022. He currently serves as an Associate Editor for the IEEE TRANSACTIONS ON INFORMATION THEORY.