Necessary and Sufficient Girth Conditions for LDPC Tanner Graphs with Denser Protographs

Anthony Gómez-Fonseca*, Roxana Smarandache*†, and David G. M. Mitchell‡
Departments of *Mathematics and †Electrical Engineering, University of Notre Dame, Notre Dame, IN 46556, USA
{agomezfo, rsmarand}@nd.edu
‡Klipsch School of Electrical and Computer Engineering, New Mexico State University, Las Cruces, NM 88003, USA
dgmm@nmsu.edu

2021 11th International Symposium on Topics in Coding (ISTC) | 978-1-6654-0943-8/21/$31.00 ©2021 IEEE | DOI: 10.1109/ISTC49272.2021.9594176

***Abstract*—This paper gives necessary and sufficient conditions for the Tanner graph of a quasi-cyclic (QC) low-density parity-check (LDPC) code based on the all-one protograph to have girth 6, 8, 10, and 12, respectively, in the case of parity-check matrices with column weight 4. These results are a natural extension of the girth results of the already-studied cases of column weight 2 and 3, and it is based on the connection between the girth of a Tanner graph given by a parity-check matrix and the properties of powers of the product between the matrix and its transpose. The girth conditions can be easily incorporated into fast algorithms that construct codes of desired girth between 6 and 12; our own algorithms are presented for each girth, together with constructions obtained from them and corresponding computer simulations. More importantly, this paper emphasizes how the girth conditions of the Tanner graph corresponding to a parity-check matrix composed of circulants relate to the matrix obtained by adding (over the integers) the circulant columns of the parity-check matrix. In particular, we show that imposing girth conditions on a parity-check matrix is equivalent to imposing conditions on a square circulant submatrix obtained from it.**

I. Introduction

Optimized irregular quasi-cyclic (QC) low-density parity-check (LDPC) codes are attractive for implementation purposes due to their algebraic structure that allows for low complexity encoding [1] and leads to efficiencies in decoder design [2]. 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. 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., [3]). Therefore, codes with large girth are desirable for good performance (large minimum distance and low error floor). Although significant effort has been made to design QC-LDPC code matrices with large minimum distance and girth, e.g., [4]–[9], this can be particularly challenging for optimized protographs that contain dense subgraphs, such as those of the AR4JA codes [10] and 5G new radio LDPC codes [11], which contain a significant number of variable nodes with degree larger than 3.

In [12], [13], we have used some previous results 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 $B_t(H) \triangleq \left(HH^{\mathsf{T}}\right)^{\lfloor t/2 \rfloor} H^{(t \mod 2)}, t \geq 0$, to highlight the role that certain submatrices of HH^{T} play in the construction of codes of desired girth. In particular, we showed that the cycles in the Tanner graph of a $2N \times n_v N$ parity-check matrix H based on the $(2, n_v)$-regular fully connected (all-one) protograph, with lifting factor N, correspond one-to-one to the cycles in the Tanner graph of a $N \times N$ matrix, that we call C_{12}, obtained from H. Similarly, we show that imposing girth conditions on a $3N \times n_v N$ parity-check matrix is equivalent to imposing girth conditions on a $3N \times 3N$ submatrix of HH^{T}, which we call C_H.

In order to investigate large girth constructions from dense $n_c \times n_v$ protographs, where n_c is the number of check nodes and n_v is the number of variable nodes, this paper extends the results of [12] to the case $n_c = 4$ and shows how the girth conditions of a $4N \times n_v N$ parity-check matrix are reflected in the corresponding $4N \times 4N$ submatrix C_H of HH^{T}, and in particular, in a column of C_H given by the sum (over the integers) of the circulant columns of the parity-check matrix. Although we mostly assume the case of an $(4, n_v)$-regular fully connected protograph, the results can be used to analyze the girth of the Tanner graph of a parity-check matrix of zeros and ones. Throughout, we exemplify the techniques and related algorithms by constructing the Tanner graphs of $(4, 6)$-regular QC-LDPC codes with girths of 6, 8, 10, and 12, and we conclude the paper with computer simulations of some of the constructed codes with varying block lengths and girths, confirming the expected robust error control performance.

We note that the motivation of the paper is not only to construct good $(4, n_v)$-regular QC-LDPC codes, rather we aim to demonstrate that the approach from [12] can be extended to higher column weights and that similar efficient algorithms can be used to construct denser graphs (or sub-graphs) with large girth. As mentioned above, this is particularly important since capacity approaching LDPC codes with irregular protographs often have dense sub-graphs [10]. The necessary and sufficient girth conditions we present here provide a unifying framework for a given girth to be achieved in which all constructions must fit. The proposed algorithms to choose lifting exponents are extremely fast, in fact they can be evaluated by hand, and can be used to obtain codes of a given girth for the smallest graph lifting factor N. We remark that the technique can be incorporated with other complementary design approaches, such as pre-lifting [9] and masking [4] to construct irregular LDPC codes that have low error floors from the (n_c, n_v)-regular protographs. Finally, note that the technique can also be modified to increase the minimum distance and/or minimum trapping/absorbing set size since cycles appear in the composition of these structures.

II. Definitions, notations and background

For any positive integer L, let $[L] = \{1, 2, \ldots, L\}$. An LDPC code $\mathcal{C}$ is defined as the null space of a parity-check matrix H, where $\mathcal{C} = \{c \mid Hc^\top = 0^\top\}$. We can associate a Tanner graph [16] to this matrix H in the usual way. Its girth, denoted $\mathrm{gir}(H)$, is defined as the length of a shortest cycle in the graph.

A protograph [10], [17] is a small bipartite graph that can be represented by an $n_c \times n_v$ parity-check or *base* biadjacency matrix $B = (b_{ij})$, where $b_{ij} > 0$ is an integer for each pair (i, j). The parity-check matrix H of a protograph-based LDPC block code can be constructed from B in the following way: each nonzero entry b_{ij} of B is replaced by a summation of b_{ij} non-overlapping permutation matrices of size $N \times N$, and each zero entry is replaced by the $N \times N$ all-zero matrix. In this case we write $H = B^{\uparrow N}$ and N is called the lifting factor. We denote the $N \times N$ circulant permutation matrix where the entries of the $N \times N$ identity matrix I are shifted (circularly) to the left by r positions modulo N, as x^r.

In this paper we use the triangle operator $\triangle$ introduced in [15]. For two nonnegative integers e and f, define

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

This definition can be extended to matrices. Let $E = (e_{ij})_{s\times t}$ and $F = (f_{ij})_{s\times t}$ be two $s \times t$ matrices. Then we define the $s \times t$ matrix $D = (d_{ij})_{s\times t} \triangleq E \triangle F$ entry-wise, where $d_{ij} \triangleq e_{ij} \triangle f_{ij}$ for all pairs $(i, j) \in [s] \times [t]$.

The following theorem found in [14] and [15] describes an important connection between $\mathrm{gir}(H)$ and matrices $B_t(H) \triangleq \left(HH^\mathsf{T}\right)^{\lfloor t/2 \rfloor} H^{(t \mod 2)}, t \geq 0$, and offers some insight on the inner structure of the Tanner graph which simplifies considerably the search for QC protograph-based codes with large girth and minimum distance.[1]

Theorem 1. *([14] and [15]) A Tanner graph of an LDPC code with parity-check matrix H has $\mathrm{gir}(H) > 2l$ if and only if $B_t(H) \triangle B_{t-2}(H) = 0, t = 2, 3, \ldots, l$.*

III. Constructing $4 \times n_v$ protograph-based QC codes of given girth $g \leq 12$

In this section, we will construct QC matrices by lifting a $4 \times n_v$ protograph. To do so, we derive the conditions required to obtain girth $6 \leq g \leq 12$ and provide algorithms to construct the codes.

Let H be the parity-check matrix of an $n_c N \times n_v N$, $n_c < n_v$, protograph-based LDPC code given by

$$H = \begin{pmatrix} I & I & \cdots & I \\ I & P_{22} & \cdots & P_{2n_v} \\ I & P_{32} & \cdots & P_{3n_v} \\ I & P_{42} & \cdots & P_{4n_v} \end{pmatrix}. \tag{1}$$

For each $i \in [4]$, $j \in [n_v]$, let $P_{i1} = P_{1j} = I$ and

$$C_{ij} = C_{ji}^\top \triangleq P_{i1}P_{j1}^\top + P_{i2}P_{j2}^\top + \cdots + P_{in_v}P_{jn_v}^\top \tag{2}$$

and define

$$C_H \triangleq \begin{pmatrix} 0 & C_{12} & C_{13} & C_{14} \\ C_{21} & 0 & C_{23} & C_{24} \\ C_{31} & C_{32} & 0 & C_{34} \\ C_{41} & C_{42} & C_{43} & 0 \end{pmatrix}. \tag{3}$$

The following theorem characterizes the connection between the matrix C_H and $\mathrm{gir}(H)$, derived from the relation established in Theorem 1 between $\mathrm{gir}(H)$ and the matrices $B_t(H)$.

Theorem 2. *Let H, C_{ij} and C_H be defined as in* (1)*,* (2) *and* (3)*, respectively. Then*[2]

$$\begin{aligned}
&\mathrm{gir}(H) > 4 \;\Leftrightarrow C_H \triangle 0 = 0, \\
&\mathrm{gir}(H) > 6 \;\Leftrightarrow C_H \triangle 0 = 0 \;\; \& \; C_H H \triangle H = 0, \\
&\mathrm{gir}(H) > 8 \;\Leftrightarrow C_H \triangle 0 = 0 \;\; \& \; C_H^2 \triangle (I + C_H) = 0, \\
&\mathrm{gir}(H) > 10 \Leftrightarrow \mathrm{gir}(H) > 8 \;\; \& \; C_H^2 H \triangle (H + C_H H) = 0, \\
&\mathrm{gir}(H) > 12 \Leftrightarrow \mathrm{gir}(H) > 10 \; \& \; C_H^3 \triangle (I + C_H + C_H^2) = 0.
\end{aligned}$$

Proof: Note that

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

We obtain the following equivalences, completing the proof:

$$\begin{aligned}
&B_2(H) \triangle I = 0 \Leftrightarrow C_H \triangle 0 = 0; \\
&B_3(H) \triangle B_1(H) = 0 \Leftrightarrow C_H H \triangle H = 0; \\
&B_4(H) \triangle B_2(H) = 0 \Leftrightarrow (n_v I + C_H)^2 \triangle (n_v I + C_H) = 0 \\
&\quad \Leftrightarrow C_H^2 \triangle (I + C_H) = 0; \\
&B_5(H) \triangle B_3(H) = 0 \Leftrightarrow (n_v I + C_H)^2 H \triangle (n_v I + C_H) H = 0 \\
&\quad \Leftrightarrow C_H^2 H \triangle (H + C_H H) = 0; \\
&B_6(H) \triangle B_4(H) = 0 \Leftrightarrow (n_v I + C_H)^3 \triangle (n_v I + C_H)^2 = 0 \\
&\quad \Leftrightarrow C_H^3 \triangle (I + C_H + C_H^2) = 0.
\end{aligned}$$

■

Remark 3. Note that, for practical implementation, it is desirable to take each P_{ij} to be a circulant x^l, for some l, or a permutation matrix lifted to some circulants. In the remainder of the paper, we consider the first case. The second case was investigated in the case of $n_c = 3$ in [9], [12] and is left to future work for $n_c > 3$. □

Suppose that each matrix P_{ij} is a circulant permutation matrix, that is $P_{2l} = x^{i_l}, P_{3l} = x^{j_l}, P_{4l} = x^{k_l}$, for all $l \in [n_v]$, with $i_1 = j_1 = k_1 = 0$ and $P_{1l} = 1$ for all $l \in [n_v]$. The associated matrix H is then[3]

$$H = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ 1 & x^{i_2} & \cdots & x^{i_{n_v}} \\ 1 & x^{j_2} & \cdots & x^{j_{n_v}} \\ 1 & x^{k_2} & \cdots & x^{k_{n_v}} \end{pmatrix}. \tag{4}$$

[1] Please note the notational distinction between the protograph base matrix B and the matrices $B_t(H)$ defined here.

[2] We write the conditions for $\mathrm{gir}(H) > 2l$, $l = 5, 6$, as the conditions for $\mathrm{gir}(H) > 2l - 2$, which preclude the cycles of length smaller than $2l$, along with the additional necessary conditions to preclude cycles of length $2l$.

[3] Note that 0 and $1 = x^0$ correspond to the all-zero and identity matrices, respectively, where the dimensions are implied by the context.

The matrices C_{ij} and C_H are given as

$$\begin{cases} C_{21} = \sum_{l=1}^{n_v} x^{i_l}, C_{31} = \sum_{l=1}^{n_v} x^{j_l}, C_{41} = \sum_{l=1}^{n_v} x^{k_l}, \\ C_{32} = \sum_{l=1}^{n_v} x^{j_l - i_l}, C_{42} = \sum_{l=1}^{n_v} x^{k_l - i_l}, C_{43} = \sum_{l=1}^{n_v} x^{k_l - j_l}. \end{cases} \tag{5}$$

Remark 4. Note that the transpose of the matrix

$$\begin{bmatrix} n_v I & C_{12} & C_{13} & C_{14} \end{bmatrix}$$

is equal to the sum of the n_v circulant columns of H and has an important role in the girth, as we see in Theorem 2. □

Theorem 5. *Let H and C_H be defined as in* (4) *and* (3)*, respectively. Then* $\mathrm{gir}(H) > 4$ *if and only if each one of the six sets* $\{i_1, i_2, \ldots, i_{n_v}\}$, $\{j_1, j_2, \ldots, j_{n_v}\}$, $\{k_1, k_2, \ldots, k_{n_v}\}$, $\{i_1 - j_1, i_2 - j_2, \ldots, i_{n_v} - j_{n_v}\}$, $\{i_1 - k_1, i_2 - k_2, \ldots, i_{n_v} - k_{n_v}\}$ *and* $\{j_1 - k_1, j_2 - k_2, \ldots, j_{n_v} - k_{n_v}\}$ *contains exactly n_v distinct elements.*

Proof: By Theorem 2, $\mathrm{gir}(H) > 4$ if and only if $C_H \triangle 0 = 0$. This is equivalent to $C_{ij} \triangle 0 = 0$ for all $1 \le i < j \le 4$. Expanding each of these equations, we obtain

$$\sum_{l=1}^{n_v} x^{i_l} \triangle 0 = 0, \quad \sum_{l=1}^{n_v} x^{j_l} \triangle 0 = 0, \quad \sum_{l=1}^{n_v} x^{k_l} \triangle 0 = 0,$$

$$\sum_{l=1}^{n_v} x^{i_l - j_l} \triangle 0 = 0, \quad \sum_{l=1}^{n_v} x^{i_l - k_l} \triangle 0 = 0, \quad \sum_{l=1}^{n_v} x^{j_l - k_l} \triangle 0 = 0.$$

By using the definition of the triangle operator $\triangle$, we conclude that, for each equation, the exponents should be distinct and the claim follows. ■

To choose the exponents i_l, j_l, and k_l satisfying the conditions in Theorem 5, we provide the following algorithm to construct a $(4, n_v)$-regular graph with $g > 4$. In this algorithm, we first choose i_1, j_1, k_1 such that they are not in the specified *forbidden sets*, i.e., sets of values that would create a cycle of size below the desired girth, then we choose i_2, j_2, k_2, then we choose i_3, j_3, k_3, and so on.

Algorithm 6. *(Construct $(4, n_v)$-regular graph with $g > 4$)*
Step 1: Set $i_1 = 0$, $j_1 = 0$ and $k_1 = 0$. Set $l = 1$.
Step 2: Let $l := l + 1$. Choose
$i_l \notin \{i_m \mid 1 \le m \le l-1\}$
$j_l \notin \{j_m, i_l + (j_m - i_m) \mid 1 \le m \le l-1\}$
$k_l \notin \{k_m, i_l + (k_m - i_m), j_l + (k_m - j_m) \mid 1 \le m \le l-1\}$
Step 3: If $l = n_v$ stop; otherwise go to Step 2.

Example 7. In this example, we construct a 4×6 protograph-based matrix using Algorithm 6. In each iteration l, $2 \le l \le n_v$, we choose the smallest positive value for each of i_l, j_l, and k_l. We obtain

$$H = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & x & x^2 & x^3 & x^4 & x^5 \\ 1 & x^2 & x & x^5 & x^7 & x^3 \\ 1 & x^3 & x^5 & x & x^9 & x^2 \end{pmatrix}.$$

If we choose lifting factor $N = \left(\max_{1 \le l \le 6} \{i_l, j_l, k_l\} \right) + 1 = 10$, then H has girth 6. □

Example 8. Using Algorithm 6, we construct a protograph-based matrix as in Example 7. In each iteration l, $2 \le l \le n_v$, however, we choose each of i_l, j_l, and k_l to be one more than the maximum value in their corresponding forbidden sets. We obtain

$$H = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & x & x^2 & x^3 & x^4 & x^5 \\ 1 & x^2 & x^4 & x^6 & x^8 & x^{10} \\ 1 & x^3 & x^6 & x^9 & x^{12} & x^{15} \end{pmatrix}. \tag{6}$$

If we let $N = \left(\max_{1 \le l \le 6} \{i_l, j_l, k_l\} \right) + 1 = 16$, then the girth of H is 6. Notice that $N = 16$ is not the smallest positive value for which $\mathrm{gir}(H) > 4$. If we choose $N = 7$, then $\mathrm{gir}(H) = 6$. We note that (6) is a shortened version of Fan's array construction [18] that gives $g = 6$ for $N = 7$. □

Remark 9. We note that, given a set of exponents that meet the conditions of the corresponding theorem, the algorithms can be modified to produce a list of all lifting factors N that achieve girth at least as large as that specified by the algorithm. Such a modification is detailed in [12], [13]. □

Theorem 10. *Let H and C_H be defined as in equations* (4) *and* (3)*, respectively. Then* $\mathrm{gir}(H) > 6$ *if and only if, for any $m \in [n_v]$, each one of these four sets is of maximal size*[4]*:*

$\{i_m - i_n, j_m - j_n, k_m - k_n \mid n \in [n_v], n \ne m\}$,

$\{i_n, i_n - j_n + j_m, i_n - k_n + k_m, i_p + (j_n - j_m) + (k_m - k_p) \mid n, p \in [n_v], p \ne m, n \ne m\}$,

$\{j_n, j_n - i_n + i_m, j_n - k_n + k_m, j_p + (i_n - i_m) + (k_m - k_p) \mid n, p \in [n_v], p \ne m, n \ne m\}$,

$\{k_n, k_n - i_n + i_m, k_n - j_n + j_m, k_p + (i_n - i_m) + (j_m - j_p) \mid n, p \in [n_v], p \ne m, n \ne m\}$.

Algorithm 11. *(Construct $(4, n_v)$-regular graph with $g > 6$)*
Step 1: Set $i_1 = 0$, $j_1 = 0$ and $k_1 = 0$. Set $l = 1$.
Step 2: Let $l := l + 1$. Choose
$i_l \notin \{i_m, (i_m - j_m) + j_n, (j_m - k_m) + (k_n - j_n) + i_p, (i_m - k_m) + k_n, (k_m - j_m) + (j_n - k_n) + i_p \mid 1 \le m, n, p \le l-1\}$
$j_l \notin \{j_m, i_l + j_m - i_n, i_m + (j_n - i_n), (i_m - k_m) + (k_n - i_n) + j_p, i_l + (k_m - i_m) + (j_n - k_n), (j_m - k_m) + k_n, i_l + (j_m - k_m) + k_n - i_p, 2i_l + (k_m - i_m) + (j_n - k_n) - i_p \mid 1 \le m, n, p \le l-1\}$
$k_l \notin \{k_m, j_l + k_m - j_n, i_l + k_m - i_n, j_l + (i_m - j_m) + (i_n - k_n), i_m + (k_n - i_n), j_l + i_m - j_n + (k_p - i_p), 2j_l + (i_m - j_m) + (k_n - i_n) - j_p, (k_m - j_m) + j_n, i_l + (j_m - i_m) + (k_n - j_n), i_l + (k_m - j_m) + j_n - i_p, 2i_l + (j_m - i_m) + (k_n - j_n) - i_p \mid 1 \le m, n, p \le l-1\}$
Step 3: If $l = n_v$ stop; otherwise go to Step 2.

Example 12. In this example, we construct a 4×6 protograph-based matrix using Algorithm 11. In each iteration l, $2 \le l \le n_v$, we choose the smallest positive value for each of i_l, j_l, and k_l as we did in Example 7. We obtain

[4]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.

$$H = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & x & x^5 & x^8 & x^{10} & x^{25} \\ 1 & x^3 & x^{14} & x^{29} & x^{49} & x^{96} \\ 1 & x^4 & x^2 & x^{36} & x^{55} & x^{108} \end{pmatrix}. \quad (7)$$

If we choose lifting factor $N = \left(\max_{1\leq l\leq 6}\{i_l, j_l, k_l\}\right)+1 = 109$, then H has girth 8. The smallest positive integer N required to obtain $\mathrm{gir}(H) > 6$ is $N = 85$. Simulation results are provided for codes obtained from (7) with $N = 85$ and $N = 347$ in Section IV. □

Example 13. If we choose values of i_l, j_l, and k_l one more than the maximum value in their corresponding forbidden sets (instead of choosing the smallest positive value for each of i_l, j_l, and k_l, as in Example 12) we obtain the following matrix

$$H = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & x & x^8 & x^{54} & x^{355} & x^{2324} \\ 1 & x^3 & x^{23} & x^{154} & x^{1011} & x^{6617} \\ 1 & x^7 & x^{53} & x^{354} & x^{2323} & x^{15203} \end{pmatrix}.$$

For these circulants, $N = 111$ is the smallest value that can obtain this girth.

Reducing the exponents modulo 111, we obtain

$$H = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & x & x^8 & x^{54} & x^{22} & x^{104} \\ 1 & x^3 & x^{23} & x^{43} & x^{12} & x^{68} \\ 1 & x^7 & x^{53} & x^{21} & x^{103} & x^{107} \end{pmatrix}, \quad (8)$$

which also has girth 8 for $N = 111$. Note that the smallest positive integer to obtain girth 8 in (8) is now $N = 105$. Simulation results are provided for codes obtained from (8) with $N = 111$ and $N = 347$ in Section IV. □

Theorem 14. *Let H and C_H be defined as in* (4) *and* (3)*, respectively. Then* $\mathrm{gir}(H) > 8$ *if and only if* $\mathrm{gir}(H) > 4$ *and each one of these sixteen sets is of maximal size for all* $u, w \in [n_v], u \neq w$*:*

$\{(i_u-j_u)+j_w, (i_u-k_u)+k_w\}, \{(j_u-i_u)+i_w, (j_u-k_u)+k_w\}$,
$\{(k_u-i_u)+i_w, (k_u-j_u)+j_w\}, \{(j_u-i_u)-j_w, (k_u-i_u)-k_w\}$,
$\{j_u-i_w, (j_u-k_u)-(i_w-k_w)\}, \{k_u-i_w, (k_u-j_u)-(i_w-j_w)\}$,
$\{(i_u-j_u)-i_w, (k_u-j_u)-k_w\}, \{i_u-j_w, (i_u-k_u)-(j_w-k_w)\}$,
$\{k_u-j_w, (k_u-i_u)-(j_w-i_w)\}, \{(i_u-k_u)-i_w, (j_u-k_u)-j_w\}$,
$\{i_u-k_w, (i_u-j_u)-(k_w-j_w)\}, \{i_u-i_w, j_u-j_w, k_u-k_w\}$,
$\{j_u-j_w, (i_u-j_u)-(i_w-j_w), (j_u-k_u)-(j_w-k_w)\}$,
$\{k_u-k_w, (i_u-k_u)-(i_w-k_w), (j_u-k_u)-(j_w-k_w)\}$,
$\{i_u-i_w, (i_u-j_u)-(i_w-j_w), (i_u-k_u)-(i_w-k_w)\}$,
$\{j_u-k_w, (j_u-i_u)-(k_w-i_w)\}$.

Example 15. We construct a 4×6 matrix H using an algorithm derived from Theorem 14, where, at each iteration l, $l \in [n_v]$, we choose the smallest possible positive value for each of i_l, j_l, k_l, as we did in Examples 7 and 12.[5] We obtain

$$H = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & x & x^9 & x^{28} & x^{41} & x^{75} \\ 1 & x^3 & x^{21} & x^{54} & x^{98} & x^{180} \\ 1 & x^7 & x^{38} & x^{93} & x^{162} & x^{297} \end{pmatrix}.$$

[5]Due to space constraints, we omit algorithms corresponding to Theorems 13 and 15; they can be written in the same way as Algorithms 6 and 10.

If we choose $N = 2\left(\max_{1\leq l\leq 6}\{i_l, j_l, k_l\}\right) + 1 = 595$, then H has girth 10. The smallest N required to obtain $\mathrm{gir}(H) > 8$ is $N = 347$. The resulting code is simulated in Section IV.□

Theorem 16. *Let H and C_H be defined as in equations* (4) *and* (3)*, respectively. Then* $\mathrm{gir}(H) > 10$ *if and only if* $\mathrm{gir}(H) > 8$ *and, for any $l \in [n_v]$, each one of these four sets is of maximal size:*

$\{i_u - i_w, j_u - j_w, k_u - k_w, i_l + (j_u - i_u) - j_w, i_l + (k_u - i_u) - k_w, j_l + (i_u - j_u) - i_w, j_l + (k_u - j_u) - k_w, k_l + (i_u - k_u) - i_w, k_l + (j_u - k_u) - j_w \mid u, w \in [n_v], u \neq w, u \neq l\}$,

$\{(i_u - j_u) + j_w, (i_u - k_u) + k_w, i_l + i_u - i_w, i_l + (i_u - j_u) - (i_w - j_w), i_l + (i_u - k_u) - (i_w - k_w), j_l + i_u - j_w, j_l + (i_u - k_u) - (j_w - k_w), k_l + i_u - k_w, k_l + (i_u - j_u) - (k_w - j_w) \mid u, w \in [n_v], u \neq w, w \neq l\}$,

$\{(j_u - i_u) + i_w, (j_u - k_u) + k_w, i_l + j_u - i_w, i_l + (j_u - k_u) - (i_w - k_w), j_l + j_u - j_w, j_l + (i_w - j_w) - (i_u - j_u), j_l + (j_u - k_u) - (j_w - k_w), k_l + j_u - k_w, k_l + (j_u - i_u) - (k_w - i_w) \mid u, w \in [n_v], u \neq w, w \neq l\}$,

$\{(k_u - i_u) + i_w, (k_u - j_u) + j_w, i_l + k_u - i_w, i_l + (k_u - j_u) - (i_w - j_w), j_l + k_u - j_w, j_l + (k_u - i_u) - (j_w - i_w), k_l + k_u - k_w, k_l + (i_w - k_w) - (i_u - k_u), k_l + (j_w - k_w) - (j_u - k_u) \mid u, w \in [n_v], u \neq w, w \neq l\}$.

Example 17. In this example, we construct a 4×6 protograph-based matrix using an algorithm derived from Theorem 16. In each iteration l, $2 \leq l \leq n_v$, we choose the smallest positive value for each of i_l, j_l and k_l. We obtain

$$H = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & x & x^{12} & x^{45} & x^{147} & x^{445} \\ 1 & x^3 & x^{31} & x^{126} & x^{320} & x^{980} \\ 1 & x^7 & x^{67} & x^{231} & x^{636} & x^{1626} \end{pmatrix}.$$

If we choose $N = 2\left(\max_{1\leq l\leq 6}\{i_l, j_l, k_l\}\right) + 1 = 3253$, then H has girth 12, however, the smallest N required to obtain $\mathrm{gir}(H) > 10$ is $N = 1881$. The resulting code is simulated in Section IV. □

Remark 18. We note that we could also use a computer to search for the possible values in the same way, one by one, with techniques such as progressive edge growth (PEG) [19], but the last values in the matrix are hard to obtain, particularly as the density of the protograph increases. However, the proposed algorithms immediately give the next possible value and can be modified to return the size N needed in a similar way to the formulation in [12]. The algorithms can also be modified so that a random value among the possible is chosen at each time in order to optimize the performance. Or it can be chosen such that the smallest possible value can be taken at each point so that the smallest N is obtained. If a choice is not possible at some point for a desired N, backtracking can be added to pick a different value at a previous step, until a value is available at the current step. Finally, we note that

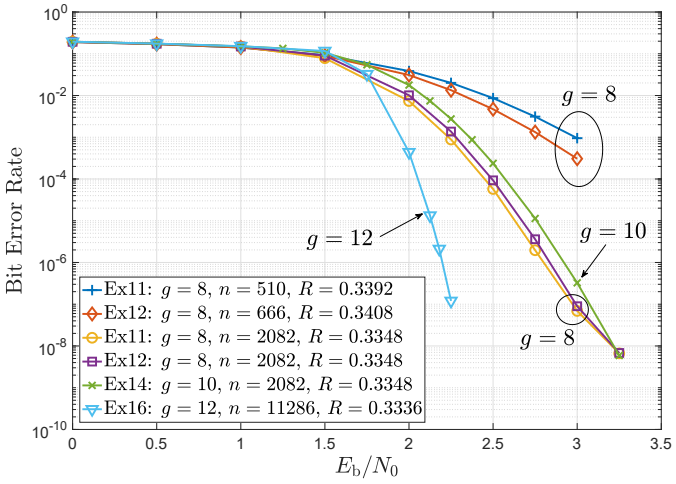

Fig. 1. Simulated decoding performance in terms of BER for the $R \approx 1/3$, $(4, 6)$-regular QC-LDPC codes from Examples 11-16.

the algorithm can also be modified to increase the minimum distance and/or minimum trapping/absorbing set size since cycles appear in the composition of these structures. □

IV. Simulation Results

To verify the performance of the constructed codes, computer simulations were performed assuming binary phase shift keyed (BPSK) modulation and an 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 several $R \approx 1/3$ $(4, 6)$-regular QC-LDPC codes from Examples 11-16 with varying code lengths and girth. For comparison, we selected a larger lifting factor than the minimum for the codes from Examples 11 and 12 with ($N = 347$ corresponding to block length $n = 2082$, both codes retain $g = 8$) to match the block length of the $g = 10$ code from Example 14. We note that the girth $g = 8$ codes have similar performance, and a slightly better waterfall, than the girth 10 code, but they also display the beginning of an error floor at 3.25dB. The Example 14 and 16 codes with girth $g = 10$ and $g = 12$, respectively, display no indication of an error-floor, at least down to respective BERs of 10^{-8} and 10^{-7}. The Example 16 code with $g = 12$ has a larger lifting factor $N = 1881$ and the resulting code with block length $n = 11286$ shows a waterfall approximately 0.58dB from the iterative decoding threshold (1.67dB) for $(4, 6)$-regular LDPC codes [20] at a BER of 10^{-7}.

V. Concluding Remarks

In this paper we gave necessary and sufficient conditions for the Tanner graph of a protograph-based QC-LDPC code with column weight 4 to have girth $6 \leq g \leq 12$, successfully extending the approach of [12] to denser protographs. The girth conditions were used to write fast algorithms which were exemplified by constructing the Tanner graphs of $(4, 6)$-regular QC-LDPC codes with girths of 6, 8, 10, and 12. The necessary and sufficient girth conditions we presented provide a unifying framework for a given girth to be achieved in which all constructions must fit. Obtaining large girth for relatively dense graphs is a challenging and important topic since capacity approaching irregular LDPC codes often have such sub-graphs in the protograph. Future work involves extending the techniques in this paper to optimized irregular protographs to achieve large girth and low error floors.

Acknowledgements

This material is based upon work supported by the National Science Foundation under Grant Nos. OIA-1757207 and HRD-1914635. A. G. F. thanks the support of the GFSD (formerly NPSC) and Kinesis-Fernández Richards fellowships.

References

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

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

[3] 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.

[4] J. Xu, L. Chen, I. Djurdjevic, S. Lin, and K. A. S. Abdel-Ghaffar, "Construction of regular and irregular LDPC codes: Geometry decomposition and masking," *IEEE Trans. Inf. Theory*, vol. 54, no. 1, pp. 121–134, Jan. 2007.

[5] 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.

[6] 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.

[7] 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, July 2013.

[8] M. Karimi and A. H. Banihashemi, "On the girth of quasi-cyclic protograph LDPC codes," *IEEE Trans. Inf. Theory*, vol. 59, pp. 4542–4552, 2013.

[9] 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.

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

[11] T. Richardson and S. Kudekar, "Design of low-density parity check codes for 5G new radio," *IEEE Comm. Magazine*, vol. 56, no. 3, pp. 28–34, 2018.

[12] R. Smarandache and D. G. M. Mitchell, "Necessary and sufficient girth conditions for Tanner graphs of quasi-cyclic LDPC codes," *Proc. IEEE Int. Symp. Inf. Theory*, pp. 380–385, July 2021.

[13] R. Smarandache and D. G. M. Mitchell, "A Unifying Framework to Construct QC-LDPC Tanner Graphs of Desired Girth," *submitted to IEEE Trans. Inf. Theory*, 2021. Online: https://arxiv.org/abs/2108.01637

[14] J. McGowan and R. Williamson, "Loop removal from LDPC codes," in *Proc. IEEE Inf. Theory Workshop*, Paris, France, 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. Comm.*, vol. 56, pp. 854–857, 2008.

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

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

[18] J. L. Fan, "Array codes as low-density parity-check codes," *Proc. Int. Symp. on Turbo Codes and Related Topics*, Brest, France, Sept. 2000.

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

[20] T. J. Richardson and R. L. Urbanke, *Modern coding theory*. Cambridge University Press, 2008.