An Efficient Strategy to Count Cycles in the Tanner Graph of Quasi-Cyclic LDPC Codes

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

Abstract

In this paper, we present an efficient strategy to enumerate the number of k-cycles, $g \leq k < 2g$, in the Tanner graph of a quasi-cyclic low-density parity-check (QC-LDPC) code with girth g using its polynomial parity-check matrix H. This strategy works for both (d_v, d_c)-regular and irregular QC-LDPC codes. In this approach, we note that the mth power of the polynomial adjacency matrix can be used to describe walks of length m in the protograph and can therefore be sufficiently described by the matrices $B_m(H) \triangleq \left(HH^{\mathsf{T}}\right)^{\lfloor m/2 \rfloor} H^{(m \mod 2)}$, where $m \geq 0$. We provide formulas for the number of k-cycles, $\mathcal{N}_k$, by just taking into account repetitions in some multisets constructed from the matrices $B_m(H)$. This approach is shown to have low complexity. For example, in the case of QC-LDPC codes based on the $3 \times n_v$ fully-connected protograph, the complexity of determining $\mathcal{N}_k$, for $k = 4, 6, 8, 10$ and 12, is $O(n_v^2 \log(N))$, $O(n_v^2 \log(n_v) \log(N))$, $O(n_v^4 \log^4(n_v) \log(N))$, $O(n_v^4 \log(n_v) \log(N))$ and $O(n_v^6 \log^6(n_v) \log(N))$, respectively. The complexity, depending logarithmically on the lifting factor N, gives our approach, to the best of our knowledge, a significant advantage over previous works on the cycle distribution of QC-LDPC codes.

I. Introduction

Low-density parity-check (LDPC) codes form a class of error-correcting codes that were discovered by Gallager [1] in the early 1960s and that have been shown to be capacity-approaching. Because of this, members of this ensemble are now part of many industry standards, including

those developed by the Consultative Committee for Space Data System (CCSDS) [2]. The sub-ensemble of quasi-cyclic LDPC (QC-LDPC) codes is attractive for both implementation and analysis purposes since its members can be described in a compact and simple way [3], [4]. It is well-known that the structure of QC-LDPC codes, and the graph representation of an LDPC code in general, plays a fundamental role in determining the performance of the code under iterative decoding algorithms. In fact, the girth [5], together with the number of short cycles [6], and other graphical structures composed of short cycles, such as trapping sets [7], are important parameters to measure the iterative decoding performance of the code. As a consequence, researchers have been actively trying to find ways to not only reduce but eliminate, when possible, all the short cycles in a graph [8], and/or combinations of those cycles [7], [9], [10], in an attempt to improve the performance of the corresponding code.

It is well-known that enumerating the k-cycles in a general graph is hard [11], [12]. Consequently, a lot of effort has been dedicated to reduce the complexity of solving these problems. Several algorithms have been designed for cycle enumeration with complexities depending on the number of vertices, the number of edges, and the number of cycles. For a graph $G = (V, E)$ with set of vertices V and set of edges E, having cardinalities $|V|$ and $|E|$, respectively, there are some well-known algorithms designed to enumerate its cycles, including the Tarjan algorithm [13] and the Johnson algorithm [14]. The complexities of these algorithms are $O\left(|V||E|(c+1)\right)$ and $O\left((|V|+|E|)(c+1)\right)$, respectively, where c is the number of cycles. Other approaches, which will be elaborated upon below, focus on particular families of graphs and on specific members of these families, like the family of bipartite graphs and, some of its members, the Tanner graphs of QC-LDPC codes, for example.

The topic of enumerating cycles in a bipartite graph $G = (V, E)$, where $V = V_c \cup V_s$ is the set of vertices, V_c and V_s are the sets of check nodes and variable nodes, respectively, having cardinalities $|V_c|$ and $|V_s|$, respectively, has a rich literature. In [6], an algorithm is presented to count k-cycles, $k = g, g+2, g+4$, in a bipartite graph with complexity growing as $O\left(gn^3\right)$, where g is the girth of G (the length of a shortest cycle in G) and $n = \max\left(|V_c|, |V_s|\right)$. In [15], a message-passing algorithm for counting short cycles in a graph is presented. This algorithm is capable of counting k-cycles, with $g \leq k \leq 2g-2$, in the case of bipartite graphs, with complexity growing as $O\left(g|E|^2\right)$. In [16], a matrix of size $2|E| \times 2|E|$, called the directed edge matrix, is constructed and used to count the number of short cycles. This strategy requires

to calculate the trace of the kth power of this matrix or, equivalently, the eigenvalues of the kth power of the adjacency matrix. Such an approach has complexity $O\left(|E|^3\right)$ and becomes prohibitively high with an increase in the size of the Tanner graph.

In more recent works, a computational technique is presented in [8] to determine the numbers of g-cycles in a $(c+1, d+1)$-bi-regular bipartite graph from its adjacency matrix is given. These results were extended in [17], providing a strategy to compute the multiplicity of k-cycles, $g+2 \leq k \leq 2g-2$, in bi-regular bipartite graphs, as a function of the spectrum and the node degrees (the number of neighbors connected to the nodes). This work also contains closed form equations for the multiplicity of 4-cycles and 6-cycles in irregular bipartite graphs. In [18], a technique/algorithm based on a modified breadth-first search (BFS) algorithm, which establishes parent/child relationships between the nodes in the graph depending on their distance from the source node, is proposed to count the short cycles of a bipartite graph. This approach has a time complexity of $O\left(|V|^2\Delta\right)$ to count g-cycles and $(g+2)$-cycles, and a time complexity of $O\left(|V|^2\Delta^2\right)$ to count $(g+4)$-cycles, where Δ is the maximum node degree in the graph.

If a graph has a specific structure, such as a quasi-cyclic representation, then it is possible to reduce the complexity of enumerating their cycles by exploiting said structure. The directed edge matrix approach discussed in [16] was further analyzed in [19] in the case of QC-LDPC codes. In this approach, the authors proved that if the LDPC code is quasi-cyclic, then its directed edge matrix can be written as an array of circulant matrices. By exploiting the circulant structure to compute the eigenvalues as in [20], the complexity of this approach is reduced from $O\left(N^3|E_b|^3\right)$ to $O\left(N|E_b|^3\right)$, where N is the lifting factor and $|E_b|$ is the number of edges in the protograph.

In this paper, we present an efficient strategy to count the number of k-cycles, $k < 2g$, in the Tanner graph of QC-LDPC codes having girth g. This strategy, which works for both (d_v, d_c)-regular and irregular QC-LDPC codes, is formally analyzed from a complexity perspective in the case of the $3 \times n_v$ fully-connected (all-ones) protograph, and exemplified to count cycles using an irregular protograph used in the CCSDS standards [2]. Our approach has low complexity, shown to be depending logarithmically on the lifting factor N. Additionally, we illustrate how we can easily generalize the strategy for the $n_c \times n_v$ case, with $n_c > 3$, maintaining the same low complexity. To the best of our knowledge, no such approach has been presented with such low complexity, even though it is well known to use modulo operations to determine cycles in a QC-LDPC graph [21], [22]. Consequently, this gives our approach a significant advantage over

any previous work on the cycle distribution of QC-LDPC codes.

This paper is structured in the following way. In Section II, we introduce the necessary definitions, notation and background. In Section III, we define an equivalence of closed walks, that applies to TBC walks, to provide a general formula to count the number of k-cycles, $\mathcal{N}_k$, for $k < 2g$, in the Tanner graph of QC-LDPC codes. This formula works for both (d_v, d_c)-regular (where d_v and d_c are the variable node and check node degrees, respectively) and irregular protographs. We then present an efficient strategy to calculate $\mathcal{N}_k$ in Section IV where we restrict our attention to the fully-connected (all-ones) protograph and values $4 \leq k \leq 12$. The complexity of our approach is analyzed in Section V. In Section VI, we exemplify this strategy in an irregular protograph, and we conclude the paper with some remarks in Section VII.

II. Definitions, notation and background

Let $\mathcal{C}$ be a QC-LDPC code, either (d_v, d_c)-regular or irregular, with block length $n_v N$ based on the $n_c \times n_v$ protograph [23] described by the matrix $B = (b_{ij})_{n_c \times n_v}$, where b_{ij} is a nonnegative integer for $i \in [n_c]$ and $j \in [n_v]$, and where $[l] \triangleq \{0, 1, \ldots, l-1\}$. Then $\mathcal{C}$ can be described by a (scalar) parity-check matrix $H = (H_{ij})_{n_c \times n_v}$, where each H_{ij}, for $i \in [n_c]$ and $j \in [n_v]$, is a summation of b_{ij} $N \times N$ circulant permutation matrices if b_{ij} is nonzero, and the $N \times N$ all-zero matrix if $b_{ij} = 0$. Graphically, this operation is equivalent to taking an N-fold graph cover, or *lifting*, of the protograph. Here, N is called the lifting factor (lifting degree, or degree of the graph cover). Let x^r denote the $N \times N$ circulant permutation matrix obtained by circularly shifting to the left, by r positions modulo N, the entries of the $N \times N$ identity matrix I. For simplicity in the notation, let $p_{ij}(x)$ be the polynomial representation of H_{ij}, where $p_{ij}(x) = \sum_{l=0}^{N-1} a_l x^l$ and $a_l \in \{0, 1\}$ for all $l \in [N]$. Each polynomial $p_{ij}(x)$ has weight b_{ij}. Then we can rewrite the parity-check matrix H, using the polynomial representation, as $H = (p_{ij})_{n_c \times n_v}$.

From the parity-check matrix H, we construct a bipartite graph $G = (V, E)$, called a Tanner graph [24], by considering H as its biadjacency matrix. This bipartite graph represents the QC-LDPC code $\mathcal{C}$ obtained from H. The set V is the set of vertices (or nodes) and E is the set of edges, and their cardinalities are denoted by $|V|$ and $|E|$, respectively. Let denote the vertices of G by v_a, for $a = 0, 1, 2, \ldots, |V| - 1$, and the edges by e_b, for $b = 0, 1, 2, \ldots, |E| - 1$. Each edge e_b has the form $e_b = (v_a, v_c)$, for some $v_a, v_c \in V$, and the vertices v_a and v_c are called the endpoints of e. A (directed) walk W of length m in the graph G is an alternating

sequence $W = v_0e_1v_1e_2\cdots v_{m-1}e_mv_m$ of vertices and edges such that $e_l = (v_{l-1}, v_l) \in E$ for all $1 \leq l \leq m$. The first vertex appearing in the alternating sequence, v_0, is called the base point of W. A walk W is said to be closed if the two endpoints are the same, this is, when $v_0 = v_m$. A closed walk W is backtrackless if $e_l \neq e_{l+1}$ for all $l = 1, 2, \ldots, m-1$. A backtrackless closed walk W is tailless if $e_m \neq e_1$, and W is called, in this case, a TBC walk. A cycle is a closed walk W having distinct vertices and distinct edges, and if its alternating sequence has k edges in it, then we call W a k-cycle. The length of a shortest cycle is called the *girth* of the graph.

The adjacency matrix $A = (A_{ij})$ is the symmetric binary matrix with $A_{ij} = 1$ if $(v_i, v_j) \in E$, and $A_{ij} = 0$ otherwise. After some reordering of the vertices, if necessary, we can write A, for either the scalar or polynomial representation of H, in the compact expression

$$A = \begin{bmatrix} 0 & H \\ H^{\mathsf{T}} & 0 \end{bmatrix}, \tag{1}$$

where H^{T} denotes the transpose of H. The powers of A, and in particular the matrices

$$B_t(H) \triangleq \left(HH^{\mathsf{T}}\right)^{\lfloor t/2 \rfloor} H^{(t \mod 2)}, \quad t \geq 0, \tag{2}$$

give information about the walks [25]. It is not difficult to see that, for any nonnegative integer t, we have

$$A^{2t} = \begin{bmatrix} B_{2t}(H) & 0 \\ 0 & B_{2t}(H^{\mathsf{T}}) \end{bmatrix} \quad \text{and} \quad A^{2t+1} = \begin{bmatrix} 0 & B_{2t+1}(H) \\ B_{2t+1}(H^{\mathsf{T}}) & 0 \end{bmatrix}. \tag{3}$$

Since G is a bipartite graph, any k-cycle has even length, so $k = 2m$ for some m. We can form a walk of length k, or simply a k-walk, by taking the union of two walks of length m having the same two endpoints. If all the vertices and edges traversed in this k-walk are distinct, then the k-walk is a k-cycle. For example, if $k = 4$, then any 4-cycle is formed by the union of two different walks of length 2 having the same two endpoints. We can count the number of walks of length 2 between any two vertices by calculating the square of the adjacency matrix A. For $A^2 = ((A^2)_{ij})$, notice that

$$(A^2)_{ij} = \sum_{l=0}^{|V|-1} A_{il}A_{lj}. \tag{4}$$

The equation (4) gives the number of walks of length 2 between vertices v_i and v_j since we have two edges joining v_i to v_l to v_j whenever $A_{il} = A_{lj} = 1$. This argument was generalized in the following theorem.

Theorem 1 ([26]). *If $A^m = ((A^m)_{ij})$ is the mth power of the adjacency matrix A, then the entry $(A^m)_{ij}$ is equal to the number of walks of length m between the vertices v_i and v_j.*

The polynomial representation of QC-LDPC codes allows for a reduction in the complexity of our computations, so we will work with the polynomial parity-check matrix rather than with its scalar version. First, we consider the triangle operator $\triangle$ introduced in [25]. For two nonnegative integers e and f, define $d = e \triangle f \triangleq 1$ if $e \geq 2$ and $f = 0$, and $d = e \triangle f \triangleq 0$ otherwise. This definition can be extended to matrices. For two $s \times t$ matrices $E = (e_{ij})$ and $F = (f_{ij})$, we define the $s \times t$ matrix $D = (d_{ij}) \triangleq E \triangle F$ entry-wise, where $d_{ij} \triangleq e_{ij} \triangle f_{ij}$ for all pairs $(i, j) \in [s] \times [t]$. If $E(x)$ and $F(x)$ are the polynomial versions of E and F, respectively, then $D(x) \triangleq E(x) \triangle F(x)$, where $D(x)$ is the polynomial version of D.

Theorem 2 ([25], [26]). *A Tanner graph of an LDPC code with parity-check matrix H has girth$(H) > 2l$ if and only if $B_m(H) \triangle B_{m-2}(H) = 0$ for $2 \leq m \leq l$.*

The kth power of the scalar adjacency matrix A of the Tanner graph can be used to determine the number of k-walks between any two vertices, as we have seen in Theorem 1. The kth power of the polynomial version of the adjacency matrix, however, does not help us to count the number of k-walks between any two vertices of the Tanner graph, but, as we will see, it can be used to describe the edges traversed in a k-walk between any two vertices in the protograph. For example, if A is the polynomial version of the adjacency matrix (1), then

$$(A^2)_{ij}(x) = \sum_{l=0}^{n_c+n_v-1} A_{il}(x) A_{lj}(x), \tag{5}$$

and every term of the polynomial $(A^2)_{ij}(x)$ is a product of the form $x^{c_{il}} x^{c_{lj}} = x^{c_{il}+c_{lj}}$, where $x^{c_{il}}$ and $x^{c_{lj}}$ come from the polynomials $A_{il}(x)$ and $A_{lj}(x)$, respectively. Each one of the two circulants $x^{c_{il}}$ and $x^{c_{lj}}$ correspond to a unique edge in the protograph, and the order in which they appear in the product is the order used to traverse the walk in the protograph. The exponent $c_{il} + c_{lj}$, in consequence, corresponds to the two edges traversed from vertex v_i to vertex v_l to vertex v_j in the protograph. In the same way, every term of $(A^3)_{ij}(x)$ is a product of the form $x^{c_{il}} x^{c_{lk}} x^{c_{kj}} = x^{c_{il}+c_{lk}+c_{kj}}$, and the exponent $c_{il} + c_{lk} + c_{kj}$ corresponds to the three edges traversed in the protograph from vertex v_i to vertex v_l to vertex v_k to vertex v_j. In general, every term of $(A^m)_{ij}(x)$ is of the form $x^{c_{il_1}} x^{c_{l_1 l_2}} \cdots x^{c_{l_m j}} = x^{c_{il_1}+c_{l_1 l_2}+\cdots+c_{l_m j}}$, and each one of

them corresponds to a walk of length m and the specific order in which it is traversed, which is nicely described by the way the matrix multiplication in (3) is performed. This allows us to state a polynomial version of Theorem 1.

Theorem 3. *If $A^m = ((A^m)_{ij}(x))$ is the mth power of the polynomial adjacency matrix A, then every term of the polynomial $(A^m)_{ij}(x)$ is of the form $x^{c_{il_1}} x^{c_{l_1 l_2}} \cdots x^{c_{l_m j}}$ and corresponds to a walk of length m between the vertices v_i and v_j in the protograph.*

Definition 4. *The exponent $c_{il_1} + c_{l_1 l_2} + \cdots + c_{l_m j}$ corresponding to the product $x^{c_{il_1}} x^{c_{l_1 l_2}} \cdots x^{c_{l_m j}}$ in Theorem 3 is called a permutation shift.*

If $x^{c_{il_1}} x^{c_{l_1 l_2}} \cdots x^{c_{l_m j}}$ and $x^{c'_{il_1}} x^{c'_{l_1 l_2}} \cdots x^{c'_{l_m j}}$ are two terms of the polynomial $(A^m)_{ij}(x)$ describing two m-walks between vertices v_i and v_j in the protograph, then the combination

$$x^{c_{il_1}} x^{c_{l_1 l_2}} \cdots x^{c_{l_m j}} x^{-c'_{l_m j}} \cdots x^{-c'_{l_1 l_2}} x^{-c'_{il_1}}$$

of the first walk and the reversal of the second one describes a closed $(2m)$-walk that starts and ends at the vertex v_i, and that has the vertex v_j midway. Hence, the entries $(A^m)_{ij}(x)$ of the power A^m describe all the m-walks in the protograph and can be used to count certain cycles in the Tanner graph. The strategy of counting cycles in the Tanner graph presented in this paper requires to keep track of TBC walks in the protograph. This is why we are interested in analyzing the way each walk is traversed. First, we introduce some required concepts on graph covers.

At the beginning of this section, we explained the process to construct a Tanner graph from a protograph. In the sequel, we will need a little more mathematical accuracy, so we define the lifting process from a topological point of view. Let $G = (V, E)$ be a protograph described by matrix $B = (b_{ij})_{n_c \times n_v}$. Each row and each column of B corresponds to a check node and a variable node in the protograph, respectively. Once a lifting factor N is chosen, for each vertex $v \in V$ in the protograph, either a check node or a variable node, we create N copies of it and denote them by $\tilde{v}^l$, for $l \in [N]$. For each edge $e = (u, v) \in E$ in the protograph, there is, associated to it, a circulant permutation matrix x^a, where $a \in [N]$. Once the value for a is chosen, we create N copies of e and denote them by $\tilde{e}^l$, for $l \in [N]$. The vertices that are endpoints of these edges are permuted in such a way that we have $\tilde{e}^l = (u^l, v^{l-a \mod N})$. If we let $\tilde{V} = \{\tilde{v}^l \mid v \in V, l \in [N]\}$ and $\tilde{E} = \{\tilde{e}^l \mid e \in E, l \in [N]\}$, then the graph $\tilde{G} = (\tilde{V}, \tilde{E})$ is an

N-fold graph cover, or *lifting*, of the protograph, and we call it the Tanner graph. The process of creating the N copies $\tilde{v}^l$ of the vertex v and the N copies $\tilde{e}^l$ of the edge e induces a projection map $p : \tilde{G} \to G$, and we call p the natural projection map. The set of vertices $\left\{\tilde{v}^l \mid v \in V\right\}$ and the set of edges $\left\{\tilde{e}^l \mid e \in E\right\}$, denoted by $p^{-1}(v)$ and $p^{-1}(e)$, respectively, are called the fiber over the vertex v and the fiber over the edge e, respectively, under the natural projection map.

Lemmas 5 and 7, based on some results from [27], are useful to study both the images of cycles in the Tanner graph and the preimages of TBC walks in the protograph.

Lemma 5 ([28], [29])**.** *Let $\tilde{G}$ be an N-fold graph cover of the protograph G. Let W be a k-walk in G starting at vertex v and ending at vertex v', and having edge sequence $e_1, e_2, \ldots, e_k$ with associated circulant permutation matrices $x^{s_1}, x^{s_2}, \ldots, x^{s_k}$. Then the permutation shift s that maps $\tilde{v}$, the inverse image of v in $\tilde{G}$, to $\tilde{v}'$, the inverse image of v' in $\tilde{G}$, through the walk $\tilde{W}$ is given by*

$$s = \sum_{i=0}^{k-1} (-1)^i s_{i+1} \mod N. \tag{6}$$

Remark 6. If the walk W in Lemma 5 is traversed in the opposite direction starting at vertex v' and ending at vertex v, then its permutation shift is given by $s' = N - s \mod N$. □

We denote by $\mathbb{Z}_N$ the additive group of integers modulo N. For any element $a \in \mathbb{Z}_N$, the order of a is the smallest integer m such that $a^m = m \cdot a = 0$.

Lemma 7 ([28])**.** *Let $\tilde{G}$ be an N-fold graph cover of the protograph G and let W' be a k-cycle in $\tilde{G}$. Then W' is projected onto a TBC walk W of length k/m, where $m \geq 1$ is the order of the permutation shift of W in $\mathbb{Z}_N$.*

Remark 8. The order of a TBC walk W, which is referred to as the order of its permutation shift s in the previous lemmas when considered as an element of $\mathbb{Z}_N$, is given by $N/\gcd(N, s)$, where s is as in (6) and $\gcd$ denotes the greatest common divisor. □

We combine the following lemma with our analysis of TBC walk to count cycles in the Tanner graph.

Lemma 9 ([30])**.** *Let $\tilde{G}$ be an N-fold graph cover of the protograph G and let W be a closed k-walk in G. Then the inverse image of W in $\tilde{G}$ is the union of N/m closed (km)-walks, where*

$m \geq 1$ is the order of the permutation shift of W in $\mathbb{Z}_N$.

We extend the result in Lemma 9, stated for closed k-walks, to TBC walks of length k.

Theorem 10. *Let $\tilde{G}$ be an N-fold graph cover of the protograph G and let W be a TBC walk of length k in G. Then the inverse image of W in $\tilde{G}$ is the union of N/m TBC walks of length km, where $m \geq 1$ is the order of the permutation shift of W in $\mathbb{Z}_N$.*

Proof: By Lemma 9, the inverse image of W is the union of N/m closed (km)-walks, where $m \geq 1$ is the order of the permutation shift of W in $\mathbb{Z}_N$, since W is a closed walk. It remains to show that each element $\tilde{W}$ in the inverse image of W is backtrackless and tailless. Assume that $W = e_1 e_2 \cdots e_k$. The inverse image of a 2-walk $e_l e_{l+1}$ in W, for some l, gives a 2-walk $\tilde{e_{l'}} e_{\tilde{l'+1}}$ in $\tilde{W}$. If the two edges $\tilde{e_{l'}}$ and $e_{\tilde{l'+1}}$ are equal, meaning that the same edge is being traversed consecutively in a row in opposite directions, their projection onto G will give the same edge, contradicting the assumption that W backtrackless. Similarly, if the edges $\tilde{e_1}$ and $e_{\tilde{km}}$, which are consecutive edges in $\tilde{W}$, are equal, then their projection onto G will give the same edge, again contradicting the assumption that W is backtrackless. This concludes the proof. ■

The following lemma explain why we restrict our analysis to k-cycles with $k < 2g$, where g is the girth of the Tanner graph.

Lemma 11 ([15])**.** *Let G be a graph with girth g. Then the set of TBC walks of length k coincides with the set of k-cycles if $k < 2g$.*

Notice that the set of TBC walks of length k and the set of k-cycles are not equal if $k \geq 2g$. For the case when $k = 2g$, let W be a g-cycle. The double traversal of W, denoted by W^2, is a TBC walk of length $2g$, but it is not a $(2g)$-cycle because the intermediate vertices are not distinct. For $k > 2g$, a similar argument is used.

Remark 12. As a direct consequence of Lemmas 7 and 11, and Theorem 10, the TBC walks in the protograph of a QC-LDPC code are the necessary and sufficient structures needed to describe all the k-cycles, $k < 2g$, in the Tanner graph. □

III. Counting cycles: a general protograph

The equivalence of closed walks is an important notion in this work.

Definition 13. *Two closed walks W_1 and W_2 are said to be equivalent if one can be obtained from the other by a change of base point, a change in direction, or both.*

If W is a closed walk of length k, then there are $2k$ equivalent closed walks to W. In the following definition, we introduce a set whose cardinality is used in the formulas for the number of k-cycles, $\mathcal{N}_k$, in the Tanner graph.

Definition 14. *Let H be a polynomial parity-check matrix and let N be the lifting factor. For integers $d \geq 0$ and $f \geq 1$, the set $W(d, f)$ is defined as the collection of all nonequivalent TBC walks of length d in the protograph having permutation shift of order f in $\mathbb{Z}_N$.*

Remark 15. Notice that the construction of the set $W(d, f)$ in Definition 14 depends on both the protograph and the lifting factor N. In algebra, the additive group $\mathbb{Z}_N$ has order N and the order of every element is a divisor of N. Hence, if s is not a divisor of N, the set $W(d, f)$ is empty independently of the selection of the length d. For example, if $N = 4$, no element in $\mathbb{Z}_4$ has order 3 because 3 does not divide 4, so the set $W(d, 3)$ is empty for any value of d. However, even if f does divide N, there are instances where the set $W(d, f)$ is automatically empty. If the protograph is the $n_c \times n_v$ fully-connected (all-ones), it is not possible to obtain a TBC walk of length 4 from the double traversal of a walk of length 2, forcing $W(2, f)$ to be empty. If the protograph is a multiedge graph, as we will discuss later, then it is possible to have a nonempty set $W(2, f)$. □

The following theorem gives the number of k-cycles in the Tanner graph using the walks described by the entries of the polynomial parity-check matrix H.

Theorem 16. *Let H be the polynomial parity-check matrix of a protograph-based QC-LDPC code with girth g, and let k be an even integer with $2 \leq k < 2g$. Let*

$$D(k) = \{d \mid d \text{ divides } k, d \geq 2, d \text{ even}\}$$

and, for any $d \in D(k)$, let $W(d, k/d)$ denote the set of nonequivalent TBC walks of length d having permutation shift of order k/d in $\mathbb{Z}_N$. Then the number $\mathcal{N}_k$ of k-cycles, $k < 2g$, in the

corresponding Tanner graph G with parity-check matrix H is given by

$$\mathcal{N}_k = \sum_{d \in D(k)} \left(|W(d, k/d)| - \sum_{\substack{d' \in D(k) \\ d' | d,\ d' < d}} |W(d', k/d')| \right) \cdot \frac{N}{k/d}, \tag{7}$$

where N is the lifting factor.

Proof: Suppose that H has girth g. By Lemma 7, any k-cycle $\tilde{W}$ in the Tanner graph projects onto a (naturally shortest) TBC walk W of length d' having permutation shift of order k/d' in $\mathbb{Z}_N$. Hence, to count the number of k-cycles in the Tanner graph, it is enough to count the TBC walks that will be lifted to k-cycles.

Let $\tilde{W}$ be a k-cycle in the Tanner graph and let W be its projection, a TBC walk of length d' having permutation shift of order k/d' in $\mathbb{Z}_N$. Let $p_{\text{shift}}(W)$ be the permutation shift of W. Since $W \in W(d', k/d')$, we have $(k/d') \cdot p_{\text{shift}}(W) = 0$ in $\mathbb{Z}_N$ and, in particular, d' is the smallest positive integer satisfying this equation. For any $d \in D(k)$ such that d' divides d and $d' < d$, traversing W d/d' times gives us a TBC walk of length d. We denote the traversal by $W^{d/d'}$, and its permutation shift, $p_{\text{shift}}(W^{d/d'})$, is 0 in $\mathbb{Z}_N$. The inverse image of $W^{d/d'}$ is, then, a collection of TBC walks that are not cycles in the Tanner graph since they are the cycles in the inverse image of W, but traversed d/d' times. Hence, the only elements in $W(d, k/d)$ that contribute to the number of cycles in the Tanner graph are those TBC walks that are not a multiple traversal of shorter TBC walks having permutation shift of order smaller than k/d in $\mathbb{Z}_N$. Rewriting this in symbols, the number of TBC walks satisfying this property is $\mu(d, k) = |W(d, k/d)| - \sum_{\substack{d' \in D(k) \\ d' | d,\ d' < d}} |W(d', k/d')|$ and, by Theorem 10, the number of k-cycles that each one of them contribute is $N/(k/d)$. Taking the sum of $\mu(d, k) \cdot N/(k/d)$ over all $d \in D(k)$ gives equation (7). ■

IV. Counting cycles: binary protographs

The equation (7) in Theorem 16 gives the number of k-cycles in the Tanner graph of an arbitrary QC-LDPC code. Since the Tanner graph is a graph cover of the protograph, and $N \geq 1$, the former has, at least, the same number of vertices and edges as the latter. In practice, we restrict $N > 1$, so counting TBC walks in the protograph, instead of directly counting cycles in the Tanner graph, represents a reduction in the number of computations required to determine

$\mathcal{N}_k$. In this section, we focus on the fully-connected (all-ones) protograph and discuss how to determine $\mathcal{N}_k$ with a strategy that has complexity logarithmic on the lifting factor N. We show that this involves determining the cardinality of the sets $W(d, f)$, for integers $d \geq 0$ and $f \geq 1$, in a simple way. We note that, by studying the all-ones protograph, we also have the framework for any binary (regular or irregular) protograph because "masking" (replacing ones with zeros) [31] makes the problem simpler since various exponents are removed from the calculation. In Section VI, we show how to extend the approach to general (non-binary) protographs.

Let $\mathcal{C}$ be a QC-LDPC code with parity check matrix H given by

$$H = \begin{bmatrix} x^{l_{0,0}} & x^{l_{0,1}} & \dots & x^{l_{0,n_v-1}} \\ x^{l_{1,0}} & x^{l_{1,1}} & \dots & x^{l_{1,n_v-1}} \\ \vdots & \vdots & \ddots & \vdots \\ x^{l_{n_c-1,0}} & x^{l_{n_c-1,1}} & \dots & x^{l_{n_c-1,n_v-1}} \end{bmatrix}, \tag{8}$$

where $l_{ij} \in [N]$ for $i \in [n_c]$ and $j \in [n_v]$. In numerical examples, we can assume, without loss of generality, that $l_{0,j} = l_{i,0} = 0$ for $i \in [n_c]$ and $j \in [n_v]$, as a way to reduce the complexity of the computations. In the theoretical results, however, we do not automatically set them to 0 in order to analyze TBC walk patterns in detail.

Consider the following definition.

Definition 17. *A multiset (shortened to mset) is a collection of elements in which elements are allowed to repeat. The number of times an element occurs in a multiset is called its multiplicity. The cardinality of a multiset is the sum of the multiplicities of its elements.*

By Theorem 2, following the discussion in [32], girth$(H) > 4$ if and only if each one of the $\binom{n_c}{2}$ msets $\{l_{i,m} - l_{i',m} \mid m \in [n_v]\}$, for $i < i'$, contains distinct elements in $\mathbb{Z}_N$. If one of these msets has a repeated element (a *repetition*), some 4-cycles appears in the Tanner graph and the exact amount of them is calculated in the following theorem.

Theorem 18. *Let H be as in* (8)*. A repetition in any of the following $\binom{n_c}{2}$ msets*

$$A_{i,i'} = \{l_{i,m} - l_{i',m} \mid m \in [n_v]\}, \quad i < i',$$

lifts to exactly N 4-cycles in the Tanner graph. The total number of 4-cycles in the Tanner graph, $\mathcal{N}_4$, is given by

$$\mathcal{N}_4 = |W(4, 1)| \cdot N, \tag{9}$$

where $W(4,1)$ is the set of all nonequivalent TBC walks associated to the repetitions in the msets above.

Proof: The msets $A_{i,i'} = \{l_{i,m} - l_{i',m} \mid m \in [n_v]\}$, $i < i'$, describe all nonequivalent walks of length 2 in the matrix H. A repetition in any of the msets gives a TBC walk of length 4 with permutation shift $l_{i,m} - l_{i',m} - l_{i',m'} + l_{i,m'} = 0$ in $\mathbb{Z}_N$ if $m \neq m'$. By Theorem 10, this TBC walk lifts to N 4-cycles. The same approach works for all the other msets and, by letting $W(4,1)$ be the set of all nonequivalent TBC walks associated to the repetitions, the result follows. ■

Example 19. Let H be the polynomial parity-check matrix given by

$$H = \begin{bmatrix} x^{h_0} & x^{h_1} & x^{h_2} & x^{h_3} & x^{h_4} \\ x^{i_0} & x^{i_1} & x^{i_2} & x^{i_3} & x^{i_4} \\ x^{j_0} & x^{j_1} & x^{j_2} & x^{j_3} & x^{j_4} \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & x & x^2 & x^3 & x^4 \\ 1 & x^2 & x & x^5 & x^7 \end{bmatrix}.$$

This matrix has girth 4 for lifting factor $N = 5$. Calculating the three msets in Theorem 18 over $\mathbb{Z}_5$, we obtain $A_{0,1} = \{0,4,3,2,1\}$, $A_{0,2} = \{0,3,4,0,3\}$, and $A_{1,2} = \{0,4,1,3,2\}$. Notice that there are two repetitions in the second mset, so there are two elements in $W(4,1)$, specifically $W(4,1) = \{h_0 - j_0 + j_3 - h_3, h_1 - j_1 + j_4 - h_4\}$. Hence, the number of 4-cycles $\mathcal{N}_4$ in the Tanner graph is $\mathcal{N}_4 = |W(4,1)| \cdot N = 2 \cdot 5 = 10$. If we take $N = 10$, then the parity-check matrix H has girth 6. To confirm that there is no 4-cycle in H, we calculate the three msets in Theorem 18 over $\mathbb{Z}_{10}$ and we obtain $A_{0,1} = \{0,9,8,7,6\}$, $A_{0,2} = \{0,8,9,5,3\}$, and $A_{1,2} = \{0,9,1,8,7\}$. Since there is no repetition in these msets, we conclude that $\mathcal{N}_4 = 0$. □

Remark 20. Theorem 18 was used to calculate the number of elements in $W(4,1)$, but the strategy can be modified in a straightforward way to count the number of elements in $W(4,2)$. In this case, we are not simply targeting repetitions in the msets $A_{i,i'}$. Instead, we are looking for two elements α_l and $\alpha_{l'}$ with $\alpha_l \neq \alpha_{l'}$, coming from the same mset, such that $2 \cdot (\alpha_l - \alpha_{l'}) = 0$ in $\mathbb{Z}_N$. The double traversal of the TBC walk that corresponds to the permutation shift $\alpha_l - \alpha_{l'}$ is an element of $W(4,2)$. This approach is used to compute $W(4,s)$, for any s, by requiring $s \cdot (\alpha_l - \alpha_{l'}) = 0$ and $t \cdot (\alpha_l - \alpha_{l'}) \neq 0$, $t \in [s] \backslash \{0\}$, in $\mathbb{Z}_N$. □

In the rest of the section, for space constraints, we will take $n_c = 3$ in (8), so H is given by

$$H = \begin{bmatrix} x^{h_0} & x^{h_1} & \cdots & x^{h_{n_v-1}} \\ x^{i_0} & x^{i_1} & \cdots & x^{i_{n_v-1}} \\ x^{j_0} & x^{j_1} & \cdots & x^{j_{n_v-1}} \end{bmatrix}. \tag{10}$$

By Theorem 2, as discussed in [32], girth$(H) > 6$ if and only if, for $m \in [n_v]$ and $l \in [n_v]\backslash\{m\}$, all the elements in each one of the msets

$$\{h_l - i_l + i_m, h_l - j_l + j_m\}, \qquad \{i_l - h_l + h_m, i_l - j_l + j_m\}, \qquad \{j_l - h_l + h_m, j_l - i_l + i_m\},$$

are distinct. In the following theorem, we rewrite these conditions in a way that is helpful to count 6-cycles in the Tanner graph.

Theorem 21. *Let H be as in* (10) *and, for $m \in [n_v]$, consider the following msets*

$$A_{1,m} = \{(l, h_l - i_l + i_m) \mid l \in [n_v], l \neq m\}, \qquad B_{2,m} = \{(l, i_l - j_l + j_m) \mid l \in [n_v], l \neq m\},$$
$$A_{2,m} = \{(l, h_l - j_l + j_m) \mid l \in [n_v], l \neq m\}, \qquad C_{1,m} = \{(l, j_l - h_l + h_m) \mid l \in [n_v], l \neq m\},$$
$$B_{1,m} = \{(l, i_l - h_l + h_m) \mid l \in [n_v], l \neq m\}, \qquad C_{2,m} = \{(l, j_l - i_l + i_m) \mid l \in [n_v], l \neq m\}.$$

For $l, l' \in [n_v]$, let $(l, \alpha_l) \in A_{1,m}$ and $(l', \alpha_{l'}) \in A_{2,m}$ be such that $\alpha_l = \alpha_{l'}$. Then the repetition $\alpha_l = \alpha_{l'}$ lifts to exactly N 6-cycles in the Tanner graph if $l \neq l'$. The same result follows if the pair $A_{1,m}, A_{2,m}$ is replaced by any of the pairs $B_{1,m}, B_{2,m}$ and $C_{1,m}, C_{2,m}$. Moreover, one of these pairs, running over all $m \in [n_v]$, is sufficient to describe all 6-cycles in H. Hence, the total number of 6-cycles in the Tanner graph, $\mathcal{N}_6$, is given by

$$\mathcal{N}_6 = |W(6,1)| \cdot N, \tag{11}$$

where $W(6,1)$ is the set of all nonequivalent TBC walks associated to the repetitions in one of the pairs above, and

$$|W(6,1)| = \sum_{m \in [n_v]} \mathcal{R}_{A_{1,m}, A_{2,m}}, \tag{12}$$

where $\mathcal{R}_{A_{1,m}, A_{2,m}}$ is the number of repetitions $\alpha_l = \alpha_{l'}$ between the msets $A_{1,m}$ and $A_{2,m}$.

Proof: Suppose that there is a repetition in the pair $A_{1,m}, A_{2,m}$ as in the statement. Then, for $l, l' \in [n_v]$, there are $\alpha_l = h_l - i_l + i_m$ and $\alpha_{l'} = h_{l'} - j_{l'} + j_m$ with $\alpha_l = \alpha_{l'}$ in $\mathbb{Z}_N$. This implies

that $h_l - i_l + i_m = h_{l'} - j_{l'} + j_m$ in $\mathbb{Z}_N$, which is equivalent to have $h_l - i_l + i_m - j_m + j_{l'} - h_{l'} = 0$ in $\mathbb{Z}_N$. If $l \neq l'$, then this permutation shift describes a TBC walk of length 6 and, by Theorem 10, it lifts to exactly N 6-cycles in the Tanner graph. If the repetition happens in the pair $B_{1,m}, B_{2,m}$, then for $l, l' \in [n_v]$, there are $\beta_l = i_l - h_l + h_m$ and $\beta_{l'} = i_{l'} - j_{l'} + j_m$ with $\beta_l = \beta_{l'}$ in $\mathbb{Z}_N$. This implies that $i_l - h_l + h_m - j_m + j_{l'} - i_{l'} = 0$ in $\mathbb{Z}_N$. If $l \neq l'$, then this permutation shift describes a TBC walk of length 6 and, by Theorem 10, it lifts to exactly N 6-cycles in the Tanner graph. If the repetition happens in the pair $C_{1,m}, C_{2,m}$, then we obtain, following the same idea as before, $j_l - h_l + h_m - i_m + i_{l'} - j_{l'} = 0$ in $\mathbb{Z}_N$, for $l, l' \in [n_v]$. If $l \neq l'$, then the corresponding TBC walk of length 6 lifts to exactly N 6-cycles in the Tanner graph by Theorem 10.

To show that only one of these pairs, running over all $m \in [n_v]$, is sufficient to describe all 6-cycles, it is enough to consider the TBC walks that they describe and apply a change of base point or direction, or both. First, we show that any TBC walk constructed from the pair $B_{1,m}, B_{2,m}$ is equivalent to some TBC walk described in the pair $A_{1,m}, A_{2,m}$. A TBC walk constructed from the pair $B_{1,m}, B_{2,m}$ involves a permutation shift of the form $i_l - h_l + h_m - j_m + j_{l'} - i_{l'}$. If h_l becomes the base point and we reverse the direction of the TBC walk, then we obtain the expression $-(h_l - i_l + i_{l'} - j_{l'} + j_m - h_m)$. The assignment

$$l \leftarrow l, \quad m \leftarrow l' \quad \text{and} \quad l' \leftarrow m$$

gives the corresponding TBC walk described in the pair $A_{1,m}, A_{2,m}$. Similarly, a TBC walk constructed from the pair $C_{1,m}, C_{2,m}$ involves a permutation shift of the form $j_l - h_l + h_m - i_m + i_{l'} - j_{l'}$. If h_m becomes the base point and we maintain the direction of the TBC walk, then we obtain the expression $h_m - i_m + i_{l'} - j_{l'} + j_l - h_l$. The assignment

$$l \leftarrow m, \quad m \leftarrow l' \quad \text{and} \quad l' \leftarrow l$$

gives the corresponding TBC walk described in the pair $A_{1,m}, A_{2,m}$.

The formula for $\mathcal{N}_6$ in (11) follows from equation (7) in Theorem 16. It remains to show that $|W(6,1)|$ is given by (12). Since the pair $A_{1,m}, A_{2,m}$, running over all $m \in [n_v]$, is sufficient to describe all the TBC walks of length 6, we use the unique TBC walk pattern $h_l - i_l + i_m - j_m + j_{l'} - h_{l'}$ and constructed all its equivalent walks. It turns out that no equivalent walk has the same TBC walk pattern, so each repetition is counted exactly once, and we conclude the proof. ■

Example 22. Let H be as in Example 19 and take $N = 5$. Since H has girth 4, we can also use our strategy to calculate 6-cycles in the Tanner graph. Following Theorem 21, we should construct, for each $m \in [n_v]$, the pair of msets $A_{1,m}, A_{2,m}$ (since only one of the three pairs is sufficient). Some computations show that

$$A_{1,0} = \{(1,4),(2,3),(3,2),(4,1)\}, \quad A_{1,2} = \{(0,2),(1,1),(3,4),(4,3)\}, \quad A_{1,4} = \{(0,4),(1,3),(2,2),(3,1)\},$$
$$A_{2,0} = \{(1,3),(2,4),(3,0),(4,3)\}, \quad A_{2,2} = \{(0,1),(1,4),(3,1),(4,4)\}, \quad A_{2,4} = \{(0,2),(1,0),(2,1),(3,2)\}.$$
$$A_{1,1} = \{(0,1),(2,4),(3,3),(4,2)\}, \quad A_{1,3} = \{(0,3),(1,2),(2,1),(4,4)\},$$
$$A_{2,1} = \{(0,2),(2,1),(3,2),(4,0)\}, \quad A_{2,3} = \{(0,0),(1,3),(2,4),(4,3)\},$$

Once all the pairs $A_{1,m}, A_{2,m}$, for $m \in [n_v]$, are constructed, we analyze each one separately. For example, if $m = 0$, notice that $(1,4) \in A_{1,0}$ and $(2,4) \in A_{2,0}$. Since there is a repetition in the second coordinate of these two elements and they differ in the first coordinate, then this contributes one TBC walk of length 6 to the set $W(6,1)$. Hence, after applying the same strategy for the other pairs, we obtain $|W(6,1)| = 16$, so $\mathcal{N}_6 = |W(6,1)| \cdot N = 16 \cdot 5 = 80$. □

In the Appendix, we provide an algorithm to count 6-cycles based on Theorem 21.

Definition 23. *Let W be a walk in the $n_c \times n_v$ fully-connected (all-ones) protograph. If W has length $k = 2m$ and its permutation shift is given by*

$$h_{\alpha_1\beta_1} - h_{\alpha_2\beta_1} + h_{\alpha_3\beta_2} - h_{\alpha_4\beta_2} + \cdots + h_{\alpha_{k-1}\beta_m} - h_{\alpha_k\beta_m}, \tag{13}$$

we use the shorthand $[h_{\alpha_1}, h_{\alpha_2}, \ldots, h_{\alpha_k}]_{\beta_1,\beta_2,\ldots,\beta_m}$. If W has length $k = 2m+1$ and its permutation shift is given by

$$h_{\alpha_1\beta_1} - h_{\alpha_2\beta_1} + h_{\alpha_3\beta_2} - h_{\alpha_4\beta_2} + \cdots + h_{\alpha_{k-1}\beta_m} - h_{\alpha_k\beta_m} + h_{\alpha_{k+1}\beta_{m+1}}, \tag{14}$$

we use the shorthand $[h_{\alpha_1}, h_{\alpha_2}, \ldots, h_{\alpha_k} | h_{\alpha_{k+1}}]_{\beta_1,\beta_2,\ldots,\beta_m|\beta_{m+1}}$

By Theorem 2, as discussed in [32], girth$(H) > 8$ if and only if the following nine equations are satisfied:

$$\sum_{u,v\in[n_v]} x^{[h,i,i,h]_{u,v}} + x^{[h,j,j,h]_{u,v}} \triangle 1 = 0, \quad \sum_{u,v\in[n_v]} x^{[j,h,h,j]_{u,v}} + x^{[j,i,i,j]_{u,v}} \triangle 1 = 0, \quad \sum_{u,v\in[n_v]} x^{[h,i,i,j]_{u,v}} \triangle 0 = 0,$$
$$\sum_{u,v\in[n_v]} x^{[i,h,h,i]_{u,v}} + x^{[i,j,j,i]_{u,v}} \triangle 1 = 0, \quad \sum_{u,v\in[n_v]} x^{[h,j,j,i]_{u,v}} \triangle 0 = 0, \quad \sum_{u,v\in[n_v]} x^{[i,h,h,j]_{u,v}} \triangle 0 = 0,$$

$$\sum_{u,v\in[n_v]} x^{[i,j,j,h]_{u,v}} \triangle 0 = 0, \qquad \sum_{u,v\in[n_v]} x^{[j,i,i,h]_{u,v}} \triangle 0 = 0, \qquad \sum_{u,v\in[n_v]} x^{[j,h,h,i]_{u,v}} \triangle 0 = 0.$$

The exponents of the circulants in each one of these equations describe the walks of length 4 in the protograph, and these are the walks that we study to form the TBC walks of length 8 that can lift to 8-cycles in the Tanner graph. For example, there are two exponents in the first equation, namely $[h,i,i,h]_{u,v}$ and $[h,j,j,h]_{u,v}$, and they give three possible TBC walk patterns:

$$[h,i,i,h,h,i,i,h]_{u,v,v',u'}, \qquad [h,i,i,h,h,j,j,h]_{u,v,v',u'}, \qquad [h,j,j,h,h,j,j,h]_{u,v,v',u'}.$$

Notice that each of these three 8-walks is a TBC walk if the conditions $u \neq v$, $v \neq v'$, $v' \neq u'$ and $u' \neq u$ are satisfied. Once all the TBC walk patterns have been constructed, from all the nine equations above, the next task is to eliminate duplicates. The following list contains all 6 nonequivalent TBC walk patterns obtained from the equations above:

$$[h,i,i,h,h,i,i,h]_{u,v,v',u'}, \qquad [h,j,j,h,h,j,j,h]_{u,v,v',u'}, \qquad [h,i,i,j,j,i,i,h]_{u,v,v',u'},$$
$$[h,i,i,h,h,j,j,h]_{u,v,v',u'}, \qquad [h,j,j,i,i,j,j,h]_{u,v,v',u'}, \qquad [i,j,j,i,i,j,j,i]_{u,v,v',u'}.$$

In the following theorem, we rewrite these conditions in a way that is helpful to count 8-cycles in the Tanner graph.

Theorem 24. *Let H be as in* (10) *and, for $u,v \in [n_v]$ with $u \neq v$, consider the following msets*

$$A_{1,1} = \{(u,v,[h,i,i,h]_{u,v})\}, \qquad A_{3,1} = \{(u,v,[h,j,j,h]_{u,v})\}, \qquad A_{5,1} = \{(u,v,[h,i,i,j]_{u,v})\},$$
$$A_{1,2} = \{(u,v,[h,i,i,h]_{u,v})\}, \qquad A_{3,2} = \{(u,v,[h,j,j,h]_{u,v})\}, \qquad A_{5,2} = \{(u,v,[h,i,i,j]_{u,v})\},$$
$$A_{2,1} = \{(u,v,[h,i,i,h]_{u,v})\}, \qquad A_{4,1} = \{(u,v,[h,j,j,i]_{u,v})\}, \qquad A_{6,1} = \{(u,v,[i,j,j,i]_{u,v})\},$$
$$A_{2,2} = \{(u,v,[h,j,j,h]_{u,v})\}, \qquad A_{4,2} = \{(u,v,[h,j,j,i]_{u,v})\}, \qquad A_{6,2} = \{(u,v,[i,j,j,i]_{u,v})\},$$

For $u,v,u',v' \in [n_v]$, let $(u,v,\alpha_{u,v}) \in A_{1,1}$ and $(u',v',\alpha_{u',v'}) \in A_{1,2}$ be such that $\alpha_{u,v} = \alpha_{u',v'}$. Then this repetition $\alpha_{u,v} = \alpha_{u',v'}$ lifts to a collection of 8-cycles in the Tanner graph if $u \neq u'$ and $v \neq v'$. The same result follows if the pair $A_{1,1}, A_{1,2}$ is replaced by any of the other five pairs. Moreover, these six pairs are sufficient to describe all 8-cycles. The total number of 8-cycles in the Tanner graph, $\mathcal{N}_8$, is given by

$$\mathcal{N}_8 = |W(4,2)| \cdot N/2 + (|W(8,1)| - |W(4,2)|) \cdot N, \tag{15}$$

where $W(8,1)$ is the set of all nonequivalent TBC walks associated to the repetitions in the msets above and $W(4,2)$ is the set of all nonequivalent TBC walks of length 4 having permutation shift of order 2 in $\mathbb{Z}_N$. The cardinality of $W(8,1)$ is given by

$$|W(8,1)| = \mathcal{R}^*_{A_{1,1},A_{1,2}} + \frac{1}{2}\mathcal{R}_{A_{2,1},A_{2,2}} + \mathcal{R}^*_{A_{3,1},A_{3,2}} + \frac{1}{2}\mathcal{R}_{A_{4,1},A_{4,2}} + \frac{1}{2}\mathcal{R}_{A_{5,1},A_{5,2}} + \mathcal{R}^*_{A_{6,1},A_{6,2}}, \quad (16)$$

where $\mathcal{R}_{X_1,X_2}$ is the number of repetitions $\alpha_{u,v} = \alpha_{u',v'}$ between the msets X_1 and X_2, the coefficient of each $\mathcal{R}_{X_1,X_2}$ is coming from the number of equivalent walks for the corresponding TBC walk pattern, $\mathcal{R}^*_{X_1,X_2}$ is given by

$$\mathcal{R}^*_{X_1,X_2} = \frac{1}{2}\mathcal{R}^{*c}_{X_1,X_2} + \frac{1}{4}\mathcal{R}^{*nc}_{X_1,X_2}, \quad (17)$$

and $\mathcal{R}^{*c}_{X_1,X_2}$ and $\mathcal{R}^{*nc}_{X_1,X_2}$ are the numbers of repetitions $\alpha_{u,v} = \alpha_{u',v'}$ between the msets X_1 and X_2 satisfying and not satisfying the conditions $u' = v$ and $v' = u$, respectively.

Proof: To show that a repetition in any of these pairs lifts to a collection of 8-cycles in the Tanner graph, we proceed as before. Consider a repetition in the pair $A_{1,1}, A_{1,2}$, so there are $u, v, u', v' \in [n_v]$ such that $\alpha_{u,v} = [h,i,i,h]_{u,v}$, $\alpha_{u',v'} = [h,i,i,h]_{u',v'}$ and $\alpha_{u,v} = \alpha_{u',v'}$ in $\mathbb{Z}_N$. Then this is equivalent to $[h,i,i,h,h,i,i,h]_{u,v,v',u'} = 0$ in $\mathbb{Z}_N$. To guarantee that this permutation shift represents a TBC walk, in addition to the conditions $u \neq v$ and $u' \neq v'$ required in the construction of the msets $A_{1,1}$ and $A_{1,2}$, respectively, we need to ensure that $u \neq u'$ and $v \neq v'$. By Theorem 10, this TBC walk lifts to a collection of 8-cycles. The same approach works for the remaining pairs. The proof that these msets are sufficient to describe all 8-cycles was addressed before the statement of the theorem.

The formula for $\mathcal{N}_8$ in (15) follows from equation (7) in Theorem 16. It remains to show that $|W(8,1)|$ is given by (16). Once a TBC walk pattern is fixed, say $[h,i,i,h,h,j,j,h]_{u,v,v',u'}$ for some $u, v, u', v' \in [n_v]$, it is possible that at least one of its equivalent walks has the same pattern. In this case, there is only one equivalent walk with the same TBC walk pattern and it has permutation shift $[h,i,i,h,h,j,j,h]_{v,u,u',v'}$. Hence, when analyzing the contribution of the repetitions in the pair $A_{2,1}, A_{2,2}$ to the set $W(8,1)$, we have to divide the total number of repetitions by the number of equivalent expressions for the TBC walk pattern, which is 2 in this case. This is due to the fact that the tuples (u, v, v', u') and (v, u, u', v') are always distinct since we require $u \neq v, v \neq v', v' \neq u'$ and $u' \neq u$. If we do the same for all the nonequivalent TBC

walk patterns, we obtain the following equivalent walks:

$$[h,i,i,h,h,i,i,h]_\beta,\ \beta\in\{(u,v,v',u'),(v',u',u,v),(v,u,u',v'),(u',v',v,u)\};$$
$$[h,i,i,h,h,j,j,h]_\beta,\ \beta\in\{(u,v,v',u'),(v,u,u',v')\};$$
$$[h,j,j,h,h,j,j,h]_\beta,\ \beta\in\{(u,v,v',u'),(v',u',u,v),(v,u,u',v'),(u',v',v,u)\};$$
$$[h,j,j,i,i,j,j,h]_\beta,\ \beta\in\{(u,v,v',u'),(u',v',v,u)\};$$
$$[h,i,i,j,j,i,i,h]_\beta,\ \beta\in\{(u,v,v',u'),(u',v',v,u)\};$$
$$[i,j,j,i,i,j,j,i]_\beta,\ \beta\in\{(u,v,v',u'),(v',u',u,v),(v,u,u',v'),(u',v',v,u)\}.$$

In the case of the pairs $A_{4,1},A_{4,2}$ and $A_{5,1},A_{5,2}$, the tuples (u,v,v',u') and (u',v',v,u) are always distinct by the same reason as for the pair $A_{2,1},A_{2,2}$. The case is different for the pairs $A_{1,1},A_{1,2}$ and $A_{3,1},A_{3,2}$ and $A_{6,1},A_{6,2}$. The four tuples (u,v,v',u'), (v',u',u,v), (v,u,u',v') and (u',v',v,u) are not necessarily distinct. In fact, there are two possible scenarios: either $u'=v$ and $v'=u$, which gives only two distinct tuples, or the four tuples are all distinct. The total contribution coming from the first scenario should be divided by 2, and the total contribution coming from the second scenario should be divided by 4. This analysis concludes the proof. ■

Example 25. Let H be the parity-check matrix of the $[155,64,20]$ Tanner code given by

$$H=\begin{bmatrix} x & x^2 & x^4 & x^8 & x^{16}\\ x^5 & x^{10} & x^{20} & x^9 & x^{18}\\ x^{25} & x^{19} & x^7 & x^{14} & x^{28}\end{bmatrix}. \tag{18}$$

Then H has girth 8 for $N=31$. We use Theorem 24 to count the number of 8-cycles, $\mathcal{N}_8$, in the Tanner graph. Some computations show that $\mathcal{R}^*_{A_{1,1},A_{1,2}}=\frac{1}{2}(0)+\frac{1}{4}(0)=0$, $\mathcal{R}_{A_{2,1},A_{2,2}}=10$, $\mathcal{R}^*_{A_{3,1},A_{3,2}}=\frac{1}{2}(0)+\frac{1}{4}(0)=0$, $\mathcal{R}_{A_{4,1},A_{4,2}}=10$, $\mathcal{R}_{A_{5,1},A_{5,2}}=10$, and $\mathcal{R}^*_{A_{6,1},A_{6,2}}=\frac{1}{2}(0)+\frac{1}{4}(0)=0$, so $|W(8,1)|=0+\frac{1}{2}(10)+0+\frac{1}{2}(10)+\frac{1}{2}(10)+0=15$ and $\mathcal{N}_8=|W(8,1)|\cdot N=15\cdot 31=465$. □

By Theorem 2, girth$(H)>10$ if and only if, for each $m\in[n_v]$, all the elements in each one of the msets

$$\{[h,i,i,h|h]_{u,v|m},[h,j,j,h|h]_{u,v|m},[h,j,j,i|i]_{u,v|m},[h,i,i,j|j]_{u,v|m}\mid u,v\in[n_v],u\neq v,v\neq m\},$$
$$\{[i,j,j,h|h]_{u,v|m},[i,h,h,i|i]_{u,v|m},[i,j,j,i|i]_{u,v|m},[i,h,h,j|j]_{u,v|m}\mid u,v\in[n_v],u\neq v,v\neq m\},$$

$$\{[j,i,i,h|h]_{u,v|m}, [j,h,h,i|i]_{u,v|m}, [j,h,h,j|j]_{u,v|m}, [j,i,i,j|j]_{u,v|m} \mid u,v \in [n_v], u \neq v, v \neq m\},$$

are distinct. Following the strategy used before, the elements in each one of these msets describe the walks of length 5 in the protograph, and these are the walks that we study to form the TBC walks of length 10 that can lift to 10-cycles in the Tanner graph. In the following theorem, we rewrite these conditions in a way that is helpful to count 10-cycles in the Tanner graph.

Theorem 26. *Let H be as in* (10) *and, for $u, v \in [n_v]$, with $u \neq v$ and $v \neq m$, consider the following msets*

$$A_{1,m} = \{(u, [h,i,i,h|h]_{u,v|m})\}, \quad B_{1,m} = \{(u, [h,j,j,h|h]_{u,v|m})\}, \quad C_{1,m} = \{(u, [h,j,j,i|i]_{u,v|m})\},$$
$$A_{2,m} = \{(u, [h,j,j,i|i]_{u,v|m})\}, \quad B_{2,m} = \{(u, [h,j,j,i|i]_{u,v|m})\}, \quad C_{2,m} = \{(u, [h,i,i,j|j]_{u,v|m})\}.$$

For $u, u' \in [n_v]$, let $(u, \alpha_u) \in A_{1,m}$ and $(u', \alpha_{u'}) \in A_{2,m}$ be such that $\alpha_u = \alpha_{u'}$. Then this repetition $\alpha_u = \alpha_{u'}$ lifts to a collection of 10-cycles in the Tanner graph if $u \neq u'$. The same result follows if the pair $A_{1,m}, A_{2,m}$ is replaced by any of the pairs $B_{1,m}, B_{2,m}$ and $C_{1,m}, C_{2,m}$. Moreover, these msets, running over all $m \in [n_v]$, are sufficient to describe all 10-cycles. The total number of 10-cycles in the Tanner graph, $\mathcal{N}_{10}$, is given by

$$\mathcal{N}_{10} = |W(10,1)| \cdot N, \tag{19}$$

where $W(10,1)$ is the set of all TBC walks associated to the repetitions in the msets above, and

$$|W(10,1)| = \sum_{m \in [n_v]} \mathcal{R}_{A_{1,m},A_{2,m}} + \mathcal{R}_{B_{1,m},B_{2,m}} + \mathcal{R}_{C_{1,m},C_{2,m}}, \tag{20}$$

where $\mathcal{R}_{X_{1,m},X_{2,m}}$ is the number of repetitions $\alpha_u = \alpha_{u'}$ between the msets $X_{1,m}$ and $X_{2,m}$.

Proof: To show that a repetition in any of these msets lifts to a collection of 10-cycles in the Tanner graph, we proceed as before. Consider a repetition in the pair $A_{1,m}, A_{2,m}$, so there are $u, v, u', v' \in [n_v]$ such that $\alpha_u = [h,i,i,h|h]_{u,v|m}$, $\alpha_{u'} = [h,j,j,i|i]_{u',v'|m}$ and $\alpha_u = \alpha_{u'}$ in $\mathbb{Z}_N$. This is equivalent to $[h,i,i,h,h,i,i,j,j,h]_{u,v,m,v',u'} = 0$ in $\mathbb{Z}_N$. To guarantee that this permutation shift represents a TBC walk, additionally to the conditions $u \neq v, v \neq m$ and $u' \neq v', v' \neq m$ required in the construction of the msets $A_{1,m}$ and $A_{2,m}$, respectively, we need to ensure that $u \neq u'$. By Theorem 10, this TBC walk lifts to a collection of N 10-cycles. The same approach works for the pairs $B_{1,m}, B_{2,m}$ and $C_{1,m}, C_{2,m}$.

To prove that these pairs are sufficient to describe all 10-cycles in the Tanner graph, it is enough to analyze the three msets described in the calculation of the conditions. From the first mset $\{[h,i,i,h|h]_{u,v|m}, [h,j,j,h|h]_{u,v|m}, [h,j,j,i|i]_{u,v|m}, [h,i,i,j|j]_{u,v|m} \mid u,v \in [n_v], u \neq v, v \neq m\}$, there are only 5 ways to form a TBC walk and these are given by the following TBC walk patterns:

$$[h,i,i,h,h,i,i,j,j,h]_{u,v,m,v',u'}, \quad [h,j,j,h,h,i,i,j,j,h]_{u,v,m,v',u'}, \quad [h,j,j,i,i,j,j,i,i,h]_{u,v,m,v',u'}.$$
$$[h,i,i,h,h,j,j,i,i,h]_{u,v,m,v',u'}, \quad [h,j,j,h,h,j,j,i,i,h]_{u,v,m,v',u'},$$

The second pattern is equivalent to the first one by considering the assignment given by

$$u \leftarrow v, \quad v \leftarrow u, \quad m \leftarrow u', \quad v' \leftarrow v', \quad \text{and} \quad u' \leftarrow m.$$

The third pattern is not equivalent to the first one, and it is not difficult to see that since the circulants x^{i_l} and x^{j_l} are visited a different amount of times. The fourth pattern is equivalent to the first one by considering the assignment (as before) given by

$$u \leftarrow v, \quad v \leftarrow u, \quad m \leftarrow u', \quad v' \leftarrow v', \quad \text{and} \quad u' \leftarrow m.$$

The fifth pattern is not equivalent to the first one nor to the third one since the circulants x^{h_l} and x^{j_l}, and x^{h_l} and x^{i_l}, respectively, are visited a different amount of times. The same strategy is used to show that each TBC walk pattern described by the other two msets is equivalent to one of the three nonequivalent patterns described here. Hence, these three pairs, running over all $m \in [n_v]$, are sufficient to describe all 10-cycles.

The formula for $\mathcal{N}_{10}$ in (19) follows from equation (7) in Theorem 16. It remains to show that $|W(10,1)|$ is given by (20). Since the pairs $X_{1,m}, X_{2,m}$, with $X \in \{A,B,C\}$ and running over all $m \in [n_v]$, are sufficient to describe all the TBC walks of length 10, we used the three TBC walk patterns $[h,i,i,h,h,i,i,j,j,h]_{u,v,m,v',u'}$, $[h,j,j,h,h,i,i,j,j,h]_{u,v,m,v',u'}$, and $[h,j,j,i,i,j,j,i,i,h]_{u,v,m,v',u'}$ to construct all their equivalent walks. It turns out that none of the corresponding equivalent walks has any of this three TBC walk patterns, so each repetition is counted exactly once, and we conclude the proof. ■

Example 27. Let H be the parity-check matrix of the $[155, 64, 20]$ Tanner code given by (18) in Example 25. We use Theorem 26 to count the number of 10-cycles in the Tanner graph. For each

$m \in [5]$, we need to construct the three pairs $A_{1,m}, A_{2,m}$, $B_{1,m}, B_{2,m}$ and $C_{1,m}, C_{2,m}$. By Theorem 26, for each pair $X_{1,m}, X_{2,m}$, $X \in \{A, B, C\}$ and $m \in [5]$, we need to find $(u, \alpha_u) \in X_{1,m}$ and $(u', \alpha_{u'}) \in X_{2,m}$ such that $\alpha_u = \alpha_{u'}$ and $u \neq u'$ for some $u, u' \in [5]$. A careful analysis of these msets shows that, for each pair, we obtain 8 repetitions of this type. This implies that $|W(10,1)| = 3 \cdot 5 \cdot 8 = 120$. Therefore, $\mathcal{N}_{10} = |W(10,1)| \cdot N = 120 \cdot 31 = 3720$. □

It is well known that the girth of a QC-LDPC code based on the fully-connected (all-ones) protograph is upper bounded by 12 [33], meaning that the existence of an inevitable cycle of length 12 is independent on the selection of circulants. Following the same strategy as before, we obtain the following list contains all 13 nonequivalent TBC walk patterns, with indices $[\cdot]_\beta = [\cdot]_{u,v,w,w',v',u'}$:

$$[h,j,j,i,i,h,h,i,i,j,j,h]_\beta, \quad [h,j,j,h,h,i,i,h,h,j,j,h]_\beta, \quad [h,j,j,h,h,j,j,i,i,j,j,h]_\beta,$$
$$[h,j,j,i,i,h,h,j,j,i,i,h]_\beta, \quad [h,j,j,h,h,i,i,j,j,i,i,h]_\beta, \quad [h,j,j,i,i,j,j,i,i,j,j,h]_\beta,$$
$$[h,i,i,h,h,i,i,h,h,i,i,h]_\beta, \quad [h,i,i,j,j,i,i,j,j,i,i,h]_\beta, \quad [i,j,j,i,i,j,j,i,i,j,j,i]_\beta.$$
$$[h,i,i,h,h,i,i,h,h,j,j,h]_\beta, \quad [h,i,i,h,h,j,j,i,i,j,j,h]_\beta,$$
$$[h,i,i,h,h,i,i,j,j,i,i,h]_\beta, \quad [h,j,j,h,h,j,j,h,h,j,j,h]_\beta,$$

In the following theorem, we rewrite these conditions in a way that is helpful to count 12-cycles in the Tanner graph.

Theorem 28. *Let H be as in* (10) *and, for $u, v, w \in [n_v]$ with $u \neq v$, $v \neq w$, consider the following msets*

$$A_{1,1} = \{(u,v,w,[h,j,j,i,i,h]_{u,v,w})\}, \quad A_{5,2} = \{(u,v,w,[h,i,i,j,j,i]_{u,v,w})\}, \quad A_{10,1} = \{(u,v,w,[h,j,j,h,h,j]_{u,v,w})\},$$
$$A_{1,2} = \{(u,v,w,[h,j,j,i,i,h]_{u,v,w})\}, \quad A_{6,1} = \{(u,v,w,[h,j,j,h,h,i]_{u,v,w})\}, \quad A_{10,2} = \{(u,v,w,[h,j,j,h,h,j]_{u,v,w})\},$$
$$A_{2,1} = \{(u,v,w,[h,j,j,i,i,h]_{u,v,w})\}, \quad A_{6,2} = \{(u,v,w,[h,j,j,h,h,i]_{u,v,w})\}, \quad A_{11,1} = \{(u,v,w,[h,j,j,h,h,j]_{u,v,w})\},$$
$$A_{2,2} = \{(u,v,w,[h,i,i,j,j,h]_{u,v,w})\}, \quad A_{7,1} = \{(u,v,w,[h,j,j,h,h,i]_{u,v,w})\}, \quad A_{11,2} = \{(u,v,w,[h,j,j,i,i,j]_{u,v,w})\},$$
$$A_{3,1} = \{(u,v,w,[h,i,i,h,h,i]_{u,v,w})\}, \quad A_{7,2} = \{(u,v,w,[h,i,i,j,j,i]_{u,v,w})\}, \quad A_{12,1} = \{(u,v,w,[h,j,j,i,i,j]_{u,v,w})\},$$
$$A_{3,2} = \{(u,v,w,[h,i,i,h,h,i]_{u,v,w})\}, \quad A_{8,1} = \{(u,v,w,[h,i,i,j,j,i]_{u,v,w})\}, \quad A_{12,2} = \{(u,v,w,[h,j,j,i,i,j]_{u,v,w})\},$$
$$A_{4,1} = \{(u,v,w,[h,i,i,h,h,i]_{u,v,w})\}, \quad A_{8,2} = \{(u,v,w,[h,i,i,j,j,i]_{u,v,w})\}, \quad A_{13,1} = \{(u,v,w,[i,j,j,i,i,j]_{u,v,w})\},$$
$$A_{4,2} = \{(u,v,w,[h,j,j,h,h,i]_{u,v,w})\}, \quad A_{9,1} = \{(u,v,w,[h,i,i,h,h,j]_{u,v,w})\}, \quad A_{13,2} = \{(u,v,w,[i,j,j,i,i,j]_{u,v,w})\}.$$
$$A_{5,1} = \{(u,v,w,[h,i,i,h,h,i]_{u,v,w})\}, \quad A_{9,2} = \{(u,v,w,[h,j,j,i,i,j]_{u,v,w})\},$$

Let $(u, v, w, \alpha_{u,v,w}) \in A_{1,1}$ *and* $(u', v', w', \alpha_{u',v',w'}) \in A_{1,2}$ *be such that* $\alpha_{u,v,w} = \alpha_{u',v',w'}$*. Then this repetition* $\alpha_{u,v,w} = \alpha_{u',v',w'}$ *lifts to a collection of 12-cycles in the Tanner graph if* $u \neq u'$ *and* $w \neq w'$*. The same result follows if the pair* $A_{1,1}, A_{1,2}$ *is replaced by any of the other pairs. Moreover, these pairs are sufficient to describe all 12-cycles. The total number of 12-cycles in the Tanner graph,* $\mathcal{N}_{12}$*, is given by*

$$\mathcal{N}_{12} = |W(4,3)| \cdot N/3 + |W(6,2)| \cdot N/2 + (|W(12,1)| - |W(4,3)| - |W(6,2)|) \cdot N, \quad (21)$$

where $W(12,1)$ *is the set of all nonequivalent TBC walks associated to the repetitions in the msets above, and* $W(4,3)$ *and* $W(6,2)$ *are the sets of all nonequivalent TBC walks of length 4 and 6, respectively, having permutation shift of order 3 and 2 in* $\mathbb{Z}_N$*, respectively. The cardinality of* $W(12,1)$ *is given by*

$$\begin{aligned} |W(12,1)| = {} & \frac{1}{2}\mathcal{R}_{A_{1,1},A_{1,2}} + \mathcal{R}^{*}_{A_{2,1},A_{2,2}} + \mathcal{R}^{**}_{A_{3,1},A_{3,2}} + \frac{1}{2}\mathcal{R}_{A_{4,1},A_{4,2}} + \frac{1}{2}\mathcal{R}_{A_{5,1},A_{5,2}} + \frac{1}{2}\mathcal{R}_{A_{6,1},A_{6,2}} + \frac{1}{2}\mathcal{R}_{A_{7,1},A_{7,2}} \\ & + \frac{1}{2}\mathcal{R}_{A_{8,1},A_{8,2}} + \frac{1}{2}\mathcal{R}_{A_{9,1},A_{9,2}} + \mathcal{R}^{**}_{A_{10,1},A_{10,2}} + \frac{1}{2}\mathcal{R}_{A_{11,1},A_{11,2}} + \frac{1}{2}\mathcal{R}_{A_{12,1},A_{12,2}} + \mathcal{R}^{**}_{A_{13,1},A_{13,2}}, \end{aligned} \quad (22)$$

where $\mathcal{R}_{X_1,X_2}$ *is the number of repetitions* $\alpha_{u,v,w} = \alpha_{u',v',w'}$ *between the msets* X_1 *and* X_2*, the coefficient of each* $\mathcal{R}_{X_1,X_2}$ *is coming from the number of equivalent walks for the corresponding TBC walk pattern,* $\mathcal{R}^{*}_{A_{2,1},A_{2,2}}$ *is given by*

$$\mathcal{R}^{*}_{A_{2,1},A_{2,2}} = \mathcal{R}^{*c}_{A_{2,1},A_{2,2}} + \frac{1}{2}\mathcal{R}^{*nc}_{A_{2,1},A_{2,2}}, \quad (23)$$

$\mathcal{R}^{*c}_{A_{2,1},A_{2,2}}$ *and* $\mathcal{R}^{*nc}_{A_{2,1},A_{2,2}}$ *are the numbers of repetitions* $\alpha_{u,v,w} = \alpha_{u',v',w'}$ *between the msets* $A_{2,1}$ *and* $A_{2,2}$ *satisfying, and not satisfying, the conditions* $u' = w$*,* $v' = v$ *and* $w' = u$*, respectively,* $\mathcal{R}^{**}_{X_1,X_2}$ *is given by*

$$\mathcal{R}^{**}_{X_1,X_2} = \frac{1}{2}\mathcal{R}^{**c}_{X_1,X_2} + \frac{1}{6}\mathcal{R}^{**nc}_{X_1,X_2}, \quad (24)$$

and, $\mathcal{R}^{**c}_{X_1,X_2}$ *and* $\mathcal{R}^{**nc}_{X_1,X_2}$ *are the numbers of repetitions* $\alpha_{u,v,w} = \alpha_{u',v',w'}$ *between the msets* X_1 *and* X_2 *satisfying, and not satisfying, the conditions* $u' = v$*,* $v' = u = w$ *and* $w' = v$*, respectively.*

Proof: To show that a repetition in any of these pairs lifts to a collection of 12-cycles in the Tanner graph, we proceed as before. Consider a repetition in the pair $A_{1,1}, A_{1,2}$, so there are $u, v, w, u', v', w' \in [n_v]$ such that $\alpha_{u,v,w} = [h, j, j, i, i, h]_{u,v,w}$, $\alpha_{u',v',w'} = [h, j, j, i, i, h]_{u',v',w'}$ and

$\alpha_{u,v,w} = \alpha_{u',v',w'}$ in $\mathbb{Z}_N$. Then this is equivalent to $[h,j,j,i,i,h,h,i,i,j,j,h]_{u,v,w,w',v',u'} = 0$ in $\mathbb{Z}_N$. To guarantee that this permutation shift represents a TBC walk, additionally to the conditions $u \neq v$ and $v \neq w$, and $u' \neq v'$ and $v' \neq w'$ required in the construction of the msets $A_{1,1}$ and $A_{1,2}$, respectively, we need to ensure that $u \neq u'$ and $w \neq w'$. By Theorem 10, this TBC walk lifts to a collection of 12-cycles. The same approach works for the remaining pairs. The proof that these msets are sufficient to describe all 12-cycles was addressed before the statement of the theorem.

The formula for $\mathcal{N}_{12}$ in (21) follows from equation (7) in Theorem 16. It remains to show that $|W(12,1)|$ is given by (22). If for each nonequivalent TBC walk pattern we find the equivalent walks, then we obtain the following:

$$
\begin{aligned}
&[h,j,j,i,i,h,h,i,i,j,j,h]_\beta,\ \beta \in \{(u,v,w,w',v',u'),(u',v',w',w,v,u)\};\\
&[h,j,j,i,i,h,h,j,j,i,i,h]_\beta,\ \beta \in \{(u,v,w,w',v',u'),(w',v',u',u,v,w)\};\\
&[h,i,i,h,h,i,i,h,h,i,i,h]_\beta,\ \beta \in \{(u,v,w,w',v',u'),(w,w',v',u',u,v),(v',u',u,v,w,w'),\\
&\qquad\qquad (v,u,u',v',w',w),(w',w,v,u,u',v'),(u',v',w',w,v,u)\};\\
&[h,i,i,h,h,i,i,h,h,j,j,h]_\beta,\ \beta \in \{(u,v,w,w',v',u'),(w',w,v,u,u',v')\};\\
&[h,i,i,h,h,i,i,j,j,i,i,h]_\beta,\ \beta \in \{(u,v,w,w',v',u'),(v,u,u',v',w',w)\};\\
&[h,j,j,h,h,i,i,h,h,j,j,h]_\beta,\ \beta \in \{(u,v,w,w',v',u'),(u',v',w',w,v,u)\};\\
&[h,j,j,h,h,i,i,j,j,i,i,h]_\beta,\ \beta \in \{(u,v,w,w',v',u'),(v,u,u',v',w',w)\};\\
&[h,i,i,j,j,i,i,j,j,i,i,h]_\beta,\ \beta \in \{(u,v,w,w',v',u'),(u',v',w',w,v,u)\};\\
&[h,i,i,h,h,j,j,i,i,j,j,h]_\beta,\ \beta \in \{(u,v,w,w',v',u'),(v,u,u',v',w',w)\};\\
&[h,j,j,h,h,j,j,h,h,j,j,h]_\beta,\ \beta \in \{(u,v,w,w',v',u'),(w,w',v',u',u,v),(v',u',u,v,w,w'),\\
&\qquad\qquad (v,u,u',v',w',w),(w',w,v,u,u',v'),(u',v',w',w,v,u)\};\\
&[h,j,j,h,h,j,j,i,i,j,j,h]_\beta,\ \beta \in \{(u,v,w,w',v',u'),(v,u,u',v',w',w)\};\\
&[h,j,j,i,i,j,j,i,i,j,j,h]_\beta,\ \beta \in \{(u,v,w,w',v',u'),(u',v',w',w,v,u)\};\\
&[i,j,j,i,i,j,j,i,i,j,j,i]_\beta,\ \beta \in \{(u,v,w,w',v',u'),(w,w',v',u',u,v),(v',u',u,v,w,w');\\
&\qquad\qquad (v,u,u',v',w',w),(w',w,v,u,u',v'),(u',v',w',w,v,u)\}.
\end{aligned}
$$

Recall that once we choose a TBC walk pattern W having permutation shift $[W]_{u,v,w,w',v',u'}$, we need to impose the conditions $u \neq v$, $v \neq w$, $w \neq w'$, $w' \neq v'$, $v' \neq u'$, and $u' \neq u$ to make it a TBC walk. For the pair $A_{m,1}, A_{m,2}$ with $m \in \{1, 6, 8, 12\}$, the two tuples of indices (u, v, w, w', v', u') and (u', v', w', w, v, u) are always distinct, otherwise we will have $u' = u$ and $w' = w$. Hence, every TBC walk having this TBC walk pattern is always counted twice. The same situation happens in the following pairs and tuples of indices:

- pair $A_{4,1}, A_{4,2}$ and tuples of indices $(u, v, w, w', v', u'), (w', w, v, u, u', v')$; and
- pair $A_{m,1}, A_{m,2}$ with $m \in \{5, 7, 9, 11\}$ and tuples of indices $(u, v, w, w', v', u'), (v, u, u', v', w', w)$.

For the pair $A_{2,1}, A_{2,2}$, the two tuples of indices (u, v, w, w', v', u') and (w', v', u', u, v, w) are not always distinct. There are two possible scenarios: either $u' = w$, $v' = v$ and $w' = u$, which gives only one distinct tuple, or the two tuples are distinct. The total contribution coming from the first scenario is taken as it is, and the total contribution coming from the second scenario should be divided by 2. The case is different for the pairs $A_{3,1}, A_{3,2}$, $A_{10,1}, A_{10,2}$ and $A_{13,1}, A_{13,2}$. The six tuples (u, v, w, w', v', u'), (w, w', v', u', u, v), (v', u', u, v, w, w'), (v, u, u', v', w', w), (w', w, v, u, u', v') and (u', v', w', w, v, u) are not necessarily distinct. In fact, there are two possible scenarios: either $u' = v$, $v' = u = w$ and $w' = v$, which gives only two distinct tuples, or the six tuples are all distinct. The total contribution coming from the first scenario should be divided by 2, and the total contribution coming from the second scenario should be divided by 6. This analysis concludes the proof. ■

Example 29. Let H be the parity-check matrix of the $[155, 64, 20]$ Tanner code given by (18) in Example 25. We use Theorem 28 to count the number of 12-cycles in the Tanner graph. Our computations show that $\mathcal{R}_{A_{1,1},A_{1,2}} = 110$, $\mathcal{R}^{*}_{A_{2,1},A_{2,2}} = 0 + \frac{1}{2}(110) = 55$, $\mathcal{R}^{**}_{A_{3,1},A_{3,2}} = \frac{1}{2}(0) + \frac{1}{6}(180) = 30$, $\mathcal{R}_{A_{4,1},A_{4,2}} = 130$, $\mathcal{R}_{A_{5,1},A_{5,2}} = 150$, $\mathcal{R}_{A_{6,1},A_{6,2}} = 150$, $\mathcal{R}_{A_{7,1},A_{7,2}} = 110$, $\mathcal{R}_{A_{8,1},A_{8,2}} = 130$, $\mathcal{R}_{A_{9,1},A_{9,2}} = 110$, $\mathcal{R}^{**}_{A_{10,1},A_{10,2}} = \frac{1}{2}(0) + \frac{1}{6}(180) = 30$, $\mathcal{R}_{A_{11,1},A_{11,2}} = 130$, $\mathcal{R}_{A_{12,1},A_{12,2}} = 150$, $\mathcal{R}^{**}_{A_{13,1},A_{13,2}} = \frac{1}{2}(0) + \frac{1}{6}(180) = 30$. Hence, $|W(12, 1)| = \frac{1}{2}(110) + 55 + 30 + \frac{1}{2}(130) + \frac{1}{2}(150) + \frac{1}{2}(150) + \frac{1}{2}(110) + \frac{1}{2}(130) + \frac{1}{2}(110) + 30 + \frac{1}{2}(130) + \frac{1}{2}(150) + 30 = 730$. Therefore, $\mathcal{N}_{12} = |W(12, 1)| \cdot N = 730 \cdot 31 = 22630$. □

Remark 30. The Tanner graph of a QC-LDPC code based on the $n_c \times n_v$ fully-connected protograph, with $2 \leq n_c < n_v$, has girth at most 12 [33]. Hence, equation (7) can be used to count cycles of length up to 22. For space constraints, we are not including the analysis to

determine $\mathcal{N}_k$ with $k = 14, 16, 18, 20, 22$, although similar expressions and algorithms can be obtained in the same way. □

V. Complexity

In this section, we determine the complexity of our approach and compare it to other results in the literature. Let H be the parity-check matrix of a QC-LDPC code given in (10) and let N be the lifting factor. The following analysis is performed for the $3 \times n_v$ fully-connected protograph, but it is not difficult to see that a generalization of our strategy for the $n_c \times n_v$ fully-connected protograph, with $n_c > 3$, having Theorem 18 as a reference, involves the same complexity, with the exception that more msets should be calculated.

In Theorem 18, to count the number of 4-cycles in the Tanner graph, we need to construct the $\binom{n_c}{2} = \frac{n_c(n_c-1)}{2}$ msets $A_{i,i'} = \{l_{i,m} - l_{i',m} \mid m \in [n_v]\}$, $i < i'$, and check for repetitions in each one of them. Since each mset has n_v elements, it is sufficient to do $\frac{(n_v-1)n_v}{2}$ comparisons in each one of them. This implies that the complexity of determining $\mathcal{N}_4$ is $O(n_v^2 \log(N))$.

To count the number of 6-cycles in the Tanner graph using Theorem 21, we need to construct one pair of msets $A_{1,m} = \{(l, h_l - i_l + i_m) \mid l \in [n_v], l \neq m\}$ and $A_{2,m} = \{(l, h_l - j_l + j_m) \mid l \in [n_v], l \neq m\}$, for each $m \in [n_v]$. Both msets $A_{1,m}$ and $A_{2,m}$ have $n_v - 1$ elements. If $(l, \alpha_l) \in A_{1,m}$ and $(l', \alpha_{l'}) \in A_{2,m}$ for some $l, l' \in [n_v]$, we are interested in repetitions $\alpha_l = \alpha_{l'}$ such that $l \neq l'$. This implies that the complexity of determining $\mathcal{N}_6$ is $O(n_v^2 \log(n_v) \log(N))$.

To determine the complexity of counting 8-cycles in the Tanner graph, we proceed as before and use Theorem 24 and, in particular, equations (15) and (16). In this case, we need to construct the six pairs X_1, X_2 in Theorem 24. Each one of these msets has $n_v(n_v - 1)$ elements. If $(u, v, \alpha_{u,v}) \in X_1$ and $(u', v', \alpha_{u',v'}) \in X_2$ for some $u, v, u', v' \in [n_v]$ with $u \neq v$ and $u' \neq v'$, we are interested in repetitions $\alpha_{u,v} = \alpha_{u',v'}$ such that $u \neq u'$ and $v \neq v'$. The equation in (16) impose the additional requirement to verify, in the worst case scenario, whether $u' = v$ and $v' = u$ is true or false. Combining all of this, the complexity of determining $\mathcal{N}_8$ is $O(n_v^4 \log^4(n_v) \log(N))$.

To count the number of 10-cycles in the Tanner graph, we use Theorem 26. In this theorem, we need to construct three pairs $X_{1,m}, X_{2,m}$, with $X \in \{A, B, C\}$, running over $m \in [n_v]$, and check whether for elements $(u, \alpha_u) \in X_{1,m}$ and $(u', \alpha_{u'}) \in X_{2,m}$, with $u, u' \in [n_v]$, we have that $u \neq u'$ and $\alpha_u = \alpha_{u'}$. Once a value for m is chosen, there are two indices required to construct both α_u and $\alpha_{u'}$. The complexity of determining $\mathcal{N}_{10}$ is, in consequence, $O(n_v^4 \log(n_v) \log(N))$.

Theorem 28 and, in particular, equations (21) and (22), are used to count the number of 12-cycles in the Tanner graph. In this case, we need to construct the thirteen pairs of msets X_1, X_2 given in the statement of the theorem. For $u, v, w, u', v', w' \in [n_v]$, we want to identify tuples $(u, v, w, \alpha_{u,v,w}) \in X_1$ and $(u', v', w', \alpha_{u',v',w'}) \in X_2$ such that $u \neq v$, $v \neq w, u' \neq v'$, $v' \neq w'$ and $\alpha_{u,v,w} = \alpha_{u',v',w'}$. To construct each $\alpha_{u,v,w}$ and $\alpha_{u',v',w'}$, we need to choose three indices. The worst case scenario happens when determining the value $\mathcal{R}^{**}_{X_1,X_2}$ in equation (22), where we need to check whether $u' = v$, $v' = u = w$, and $w' = v$ is true or false. When combined, this has complexity $O(n_v^6 \log^6(n_v) \log(N))$.

Although omitted for space constraints, an argument similar to the analysis above can be used to conclude that the complexity of determining $\mathcal{N}_k$ is upper-bounded by $O(n_v^{k/2-1} \log(n_v) \log(N))$ if $k = 14, 18$ and 22, and $O(n_v^{k/2} \log^{k/2}(n_v) \log(N))$ if $k = 16$ and 20. We recall that the reason to limit our analysis to $k \leq 22$, in the case of the fully-connected protograph, follows from Lemma 11 and Remark 30. For the general case, if the protograph is any graph described by the base matrix $B = (b_{ij})_{n_c \times n_v}$, where we allow the protograph to be a multi-edge graph, a similar analysis can be used. The weight of the ith row of B, denoted by $B_{\text{row}(i)}$, is given by $B_{\text{row}(i)} = \sum_{j \in [n_v]} b_{ij}$. Let w_{row} denote the maximum row weight of B, so $w_{\text{row}} = \max_{i \in [n_c]} \left\{ B_{\text{row}(i)} \right\}$. In the worst-case scenario, the complexity of determining $\mathcal{N}_k$, $k < 2g$, is given by $O(w_{\text{row}}^{k/2} \log^{k/2}(w_{\text{row}}) \log(N))$.

To show how fast we can calculate the number of k-cycles, $\mathcal{N}_k$, in the Tanner graph of a QC-LDPC code, we include some tables. Table I shows the number of k-cycles for the parity-check matrix H in Example 25 for lifting factor N. For the same parity-check matrix H, in Table II, we provide the time taken to count the number of k-cycles using our algorithms. The computations were done using SageMath [34] in a MacBook Pro (13-inch, 2018, Four Thunderbolt 3 Ports) with a 2.3 GHz Quad-Core Intel Core i5 processor and 16 GB 2133 MHz LPDDR3 of memory.

VI. Counting cycles: a multi-edge protograph

In Section IV, we analyzed how to count the number of k-cycles, $4 \leq k \leq 12$, in a Tanner graph lifted from the fully-connected (all-ones) protograph using a description of the TBC walks in the protograph. The strategy of using the TBC walks to count k-cycles in the Tanner graph only works when $k < 2g$. In this section, we apply this strategy to an irregular protograph.

TABLE I

NUMBER OF k-CYCLES, $\mathcal{N}_k$, FOR H IN EXAMPLE 25 FOR LIFTING FACTOR N.

N	k				
	4	6	8	10	12
5	25	55	–	–	–
10	10	50	–	–	–
15	30	45	–	–	–
20	0	20	630	3540	–
25	0	25	600	3575	–
31	0	0	465	3720	22630
50	0	0	550	3600	22275
75	0	0	825	4650	26475
100	0	0	1100	6200	35100
125	0	0	1375	7750	43875
150	0	0	1650	9300	52650
175	0	0	1925	10850	61425
200	0	0	2200	12400	70200
500	0	0	5500	31000	175500
1000	0	0	11000	62000	351000

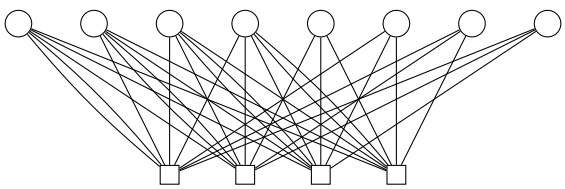

Fig. 1. Irregular protograph in the CCSDS standards.

Consider the QC-LDPC code having parity-check matrix H given by

$$H = \begin{bmatrix} 1+x^7 & x^2 & x^{14} & x^6 & 0 & 1 & x^{13} & 1 \\ x^6 & 1+x^{15} & 1 & x & 1 & 0 & 1 & x^7 \\ x^4 & x & 1+x^{15} & x^{14} & x^{11} & 1 & 0 & x^3 \\ 1 & x & x^9 & 1+x^{13} & x^{14} & x & 1 & 0 \end{bmatrix}, \tag{25}$$

and lifting factor $N = 16$. This code has parameters $[128, 64, 14]$ and is obtained by lifting the irregular protograph in Figure 1. It is part of the Consultative Committee for Space Data Systems

TABLE II

TIME TAKEN TO COUNT THE NUMBER OF k-CYCLES, $\mathcal{N}_k$, FOR H IN EXAMPLE 25 FOR LIFTING FACTOR N USING OUR APPROACH.

N	k				
	4	6	8	10	12
5	84.4 μs	252 μs	–	–	–
10	83.4 μs	244 μs	–	–	–
15	86.6 μs	246 μs	–	–	–
20	86.0 μs	247 μs	2.85 ms	5.01 ms	–
25	86.8 μs	246 μs	2.78 ms	4.96 ms	–
31	85.5 μs	246 μs	2.77 ms	5.18 ms	63.1 ms
50	85.8 μs	244 μs	2.97 ms	5.06 ms	64.2 ms
75	85.1 μs	247 μs	2.57 ms	5.08 ms	64.4 ms
100	84.6 μs	252 μs	2.82 ms	5.02 ms	65.0 ms
125	85.7 μs	246 μs	2.77 ms	4.97 ms	64.3 ms
150	86.7 μs	244 μs	2.97 ms	5.02 ms	64.6 ms
175	83.1 μs	244 μs	2.88 ms	5.03 ms	63.9 ms
200	87.7 μs	247 μs	2.93 ms	5.06 ms	64.1 ms
500	88.0 μs	254 μs	3.03 ms	5.25 ms	65.5 ms
1000	87.5 μs	257 μs	3.04 ms	5.16 ms	65.0 ms

(CCSDS) standards [2]. We can write a general version for the parity-check matrix H in the following way

$$H = \begin{bmatrix} x^{h_1} + x^{h_2} & x^{h_3} & x^{h_4} & x^{h_5} & 0 & x^{h_6} & x^{h_7} & x^{h_8} \\ x^{i_1} & x^{i_2} + x^{i_3} & x^{i_4} & x^{i_5} & x^{i_6} & 0 & x^{i_7} & x^{i_8} \\ x^{j_1} & x^{j_2} & x^{j_3} + x^{j_4} & x^{j_5} & x^{j_6} & x^{j_7} & 0 & x^{j_8} \\ x^{k_1} & x^{k_2} & x^{k_3} & x^{k_4} + x^{k_5} & x^{k_6} & x^{k_7} & x^{k_8} & 0 \end{bmatrix}. \tag{26}$$

Since we are interested in studying the cycle structure of this protograph, we will apply the same strategy used in Section IV. To do this, we use again Theorem 2 and the product HH^{T}. Notice that $HH^{\mathsf{T}} = 8I + C_H$, where the entries $(C_H)_{ij}$ of the matrix C_H are given by

$$(C_H)_{11} = x^{h_1-h_2} + x^{h_2-h_1},$$

$$(C_H)_{12} = (C_H)_{21}^{\mathsf{T}} = x^{h_1-i_1} + x^{h_2-i_1} + x^{h_3-i_2} + x^{h_3-i_3} + x^{h_4-i_4} + x^{h_5-i_5} + x^{h_7-i_7} + x^{h_8-i_8},$$

$$(C_H)_{13} = (C_H)_{31}^{\mathsf{T}} = x^{h_1-j_1} + x^{h_2-j_1} + x^{h_3-j_2} + x^{h_4-j_3} + x^{h_4-j_4} + x^{h_5-j_5} + x^{h_6-j_7} + x^{h_8-j_8},$$

$$(C_H)_{14} = (C_H)_{41}^{\mathsf{T}} = x^{h_1-k_1} + x^{h_2-k_1} + x^{h_3-k_2} + x^{h_4-k_3} + x^{h_5-k_4} + x^{h_5-k_5} + x^{h_6-k_7} + x^{h_7-k_8},$$

$$(C_H)_{22} = x^{i_2-i_3} + x^{i_3-i_2},$$

$$(C_H)_{23} = (C_H)_{32}^{\mathsf{T}} = x^{i_1-j_1} + x^{i_2-j_2} + x^{i_3-j_2} + x^{i_4-j_3} + x^{i_4-j_4} + x^{i_5-j_5} + x^{i_6-j_6} + x^{i_8-j_8},$$

$$(C_H)_{24} = (C_H)_{42}^{\mathsf{T}} = x^{i_1-k_1} + x^{i_2-k_2} + x^{i_3-k_2} + x^{i_4-k_3} + x^{i_5-k_4} + x^{i_5-k_5} + x^{i_6-k_6} + x^{i_7-k_8},$$

$$(C_H)_{33} = x^{j_3-j_4} + x^{j_4-j_3},$$

$$(C_H)_{34} = (C_H)_{43}^{\mathsf{T}} = x^{j_1-k_1} + x^{j_2-k_2} + x^{j_3-k_3} + x^{j_4-k_3} + x^{j_5-k_4} + x^{j_5-k_5} + x^{j_6-k_6} + x^{j_7-k_7},$$

$$(C_H)_{44} = x^{k_4-k_5} + x^{k_5-k_4}.$$

As we discussed before, girth$(H) > 4$ if and only if $HH^{\mathsf{T}} \triangle I = 0$. If there is a repetition in one of the msets of exponents of C_{ij}, some 4-cycles may appear in the Tanner graph depending on where the repetitions are coming from. For example, in entry $(C_H)_{11}$ there are two exponents describing two walks, $h_1 - h_2$ and $h_2 - h_1$, so we obtain only one possible TBC walk of length 4 (formed by combining the first walk and the reversal of the second one) having permutation shift given by $h_1 - h_2 + h_1 - h_2$. If we consider the entry $(C_H)_{12}$, it has eight exponents, $h_1 - i_1$, $h_2 - i_1$, $h_3 - i_2$, $h_3 - i_3$, $h_4 - i_4$, $h_5 - i_5$, $h_7 - i_7$ and $h_8 - i_8$. However, the combination of two of them does not guarantee the appearance of 4-cycles in the Tanner because they may not be describing a TBC walk in the protograph. For example, combining $h_1 - i_1$ and $h_2 - i_1$ gives a walk of length 4 having permutation shift $h_1 - i_1 + i_1 - h_2$, which is not a TBC walk because the circulant x^{i_1} is traversed twice (in opposite directions) consecutively in a row. If the second walk is $h_3 - i_2$ instead, then we have a TBC walk with permutation shift $h_1 - i_1 + i_2 - h_3$ that lifts to a collection of 4-cycles in the Tanner graph if its value is 0 in $\mathbb{Z}_N$. There are 160 nonequivalent TBC walks obtained in this fashion and we use them to count 4-cycles in the Tanner graph.

Theorem 31. *Let H be as in* (26)*. Then there are 160 nonequivalent TBC walks of length 4. These TBC walks are sufficient to describe all 4-cycles in H. The set $W(4,1)$ is the collection of those TBC walks α in this list with $\alpha = 0$ in $\mathbb{Z}_N$. Hence, the total number of 4-cycles in the Tanner graph, $\mathcal{N}_4$, is given by*

$$\mathcal{N}_4 = |W(2,2)| \cdot N/2 + (|W(4,1)| - |W(2,2)|) \cdot N. \tag{27}$$

Proof: The 160 nonequivalent TBC walks of length 4 are easily obtained by combining

exponents in the entries $(C_H)_{ij}$ above. The facts that these TBC walks are sufficient to describe all 4-cycles in H and that any of them being 0 lifts to a collection of 4-cycles in the Tanner graph follows from the strategy used in Section IV. The formula for $\mathcal{N}_4$ in (27) follows from equation (7) in Theorem 16, and we conclude the proof. ■

Remark 32. There is a noticeable difference between the formulas in (9) and (27) for the number of 4-cycles, $\mathcal{N}_4$, in the cases of the fully-connected (all-ones) protograph and the irregular protograph in this section, respectively. In the first case, we cannot have a TBC walk of length 2 in the protograph because any pair of check and variable nodes have at most one edge joining them. This requires any TBC walk to have length at least 4 taking into account that the protograph is a bipartite graph. In the second case, it is possible to have a TBC walk of length 2 since there are some pairs of check and variable nodes with two edges joining them. □

Example 33. Let H be as in (25) and let the lifting factor be $N = 16$. Then H has girth 6, so the number of 4-cycles, $\mathcal{N}_4$, is 0 and we can verify this in the following way. Some computations show that there are no TBC walk of length 2 having permutation shift of order 2 in $\mathbb{Z}_{16}$, and that none of the TBC walks of length 4 described in Theorem 31 have permutation shift 0 in $\mathbb{Z}_{16}$. Hence, the number of 4-cycles, $\mathcal{N}_4$, in the Tanner graph is $\mathcal{N}_4 = |W(2,2)| \cdot 16/2 + (|W(4,1)| - |W(2,2)|) \cdot 16 = 0 \cdot 16/2 + (0-0) \cdot 16 = 0$. □

In the following example, we apply the strategy used before to count k-cycles, $k > 4$, in another parity-check matrix H based on (26). The formulas for $\mathcal{N}_k$ should be adapted for the irregular protograph as we did in (27).

Example 34. For lifting factor $N = 64$, consider the parity-check matrix H given by

$$H = \begin{bmatrix} 1+x^{63} & x^{30} & x^{50} & x^{25} & 0 & x^{43} & x^{62} & 1 \\ x^{56} & 1+x^{61} & x^{50} & x^{23} & 1 & 0 & x^{37} & x^{26} \\ x^{16} & 1 & 1+x^{55} & x^{27} & x^{56} & 1 & 0 & x^{43} \\ x^{35} & x^{56} & x^{62} & 1+x^{11} & x^{58} & x^{3} & 1 & 0 \end{bmatrix}.$$

This matrix has girth 6 and we use the strategy used before to count the number of k-cycles, $6 \leq k < 12$, in the associated Tanner graph. To count 6-cycles, it is enough to count the number of TBC walks of length 6 having permutation shift 0 in $\mathbb{Z}_{64}$. The permutation shifts of these TBC walks are:

$$h_4 - j_4 + j_1 - k_1 + k_7 - h_6, \quad h_8 - j_8 + j_4 - k_3 + k_5 - h_5, \quad h_3 - j_2 + j_6 - k_6 + k_1 - h_2, \quad i_6 - j_6 + j_7 - k_7 + k_2 - i_3,$$
$$h_8 - j_8 + j_2 - k_2 + k_1 - h_1, \quad h_7 - i_7 + i_5 - j_5 + j_8 - h_8, \quad h_4 - i_4 + i_8 - j_8 + j_1 - h_2, \quad j_2 - k_2 + k_4 - k_5 + k_7 - j_7.$$
$$h_2 - j_1 + j_4 - k_3 + k_7 - h_6, \quad h_1 - k_1 + k_5 - k_4 + k_7 - h_6, \quad i_3 - i_2 + i_4 - j_3 + j_8 - i_8,$$
$$h_3 - j_2 + j_4 - j_3 + j_8 - h_8, \quad h_1 - i_1 + i_6 - k_6 + k_5 - h_5, \quad i_1 - j_1 + j_7 - k_7 + k_8 - i_7,$$

Since these expressions are congruent to 0 modulo 64, and there are 14 of them, then there are $\mathcal{N}_6 = 14 \cdot 64/1 = 896$ 6-cycles in the Tanner graph.

An 8-cycle in the Tanner graph projects onto a TBC walk of length 2 with permutation shift of order 4 in $\mathbb{Z}_{64}$ (traversed four times), onto a TBC walk of length 4 with permutation shift of order 2 in $\mathbb{Z}_{64}$ (traversed twice) or onto a TBC walk of length 8 with permutation shift 0 having no subgraph of smaller length with permutation shift 0. There is no TBC walk of length 2 with permutation shift of order 4 in $\mathbb{Z}_{64}$. There are three TBC walks of length 4 with permutation shift of order 2, and these are $h_3 - j_2 + j_5 - h_5$, $i_1 - j_1 + j_6 - i_6$ and $i_3 - k_2 + k_8 - i_7$. These TBC walks contribute $3 \cdot 64/2 = 96$ 8-cycles in the Tanner graph. There are 539 TBC walks of length 8 with permutation shift 0, including the double traversal of the three TBC walks of length 4, so there are 536 TBC walks contributing $(539 - 3) \cdot 64/1 = 34304$ 8-cycles in the Tanner graph. Hence, the total number of 8-cycles in the Tanner graph is $\mathcal{N}_8 = 96 + 34304 = 34400$.

A 10-cycle in the Tanner graph can only project onto a TBC walk of length 10 with permutation shift 0. There are 9142 of these TBC walks, so the total number of 10-cycles in the Tanner graph is $\mathcal{N}_{10} = 9142 \cdot 64/1 = 585088$. □

VII. Concluding remarks

This paper discusses an efficient strategy to count cycles in the Tanner graph of arbitrary QC-LDPC codes. We use some results on graph covers involving the images of cycles in the Tanner graph and the preimages of tailless backtrackless closed walks in the protograph to provide closed formulas for the number of k-cycles, $\mathcal{N}_k$, by just taking into account repetitions in some msets constructed from the matrices $B_m(H)$. Our strategy has been shown to reduce the complexity of determining $\mathcal{N}_k$, giving our approach a significant advantage over previous works on the cycle distribution of QC-LDPC codes.

ACKNOWLEDGEMENTS

This material is based upon work supported by the National Science Foundation under Grant Nos. CCF-2145917, CNS-2148358, HRD-1914635, and OIA-1757207. A. G. F. thanks the support of the GFSD (formerly NPSC) and Kinesis-Fernández Richards fellowships.

APPENDIX

Algorithm 1 shows how we use Theorem 21 to count 6-cycles in the Tanner graph of QC-LDPC codes based on the $3 \times n_v$ fully-connected protograph. Let $V[k]$ denote the kth element in the list, set or tuple V. Indexing starts with 0.

Algorithm 1 Counting 6-cycles

Input: Exponents in polynomial parity-check matrix (10), n_v, N.

Initialize $W_{6,1} = 0$.

for $m = 0$ to $n_v - 1$ **do**

  $A_{1,m} \leftarrow \{(l, h_l - i_l + i_m) \mid l \in [n_v], l \neq m\}$

  $A_{2,m} \leftarrow \{(l, h_l - j_l + j_m) \mid l \in [n_v], l \neq m\}$

  for $\alpha = 0$ to $n_v - 1$ **do**

    for $\beta = 0$ to $n_v - 1$ **do**

      if $\alpha \neq \beta$ and $A_{1,m}[\alpha][1] == A_{2,m}[\beta][1]$ **then**

        $W_{6,1} += 1$

      else

        continue

return $W_{6,1} \cdot N$

This algorithm can be easily adapted to count longer cycles using the results of this paper. We do not include them for space constraints.

REFERENCES

[1] R. G. Gallager, "Low-density parity-check codes," *IRE Transactions on Information Theory*, vol. 8, pp. 21–28, 1962.

[2] CCSDS, "TC Synchronization and Channel Coding. Issue 4. Recommendation for Space Data System Standards (Blue Book), CCSDS 231.0-B-4. Washington, D.C.: CCSDS," July 2021.

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

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

[5] Y. Mao and A. H. Banihashemi, "A heuristic search for good low-density parity-check codes at short block lengths," *IEEE International Conference on Communications Proceedings*, vol. 1, pp. 41–44, June 2001.

[6] T. R. Halford and K. M. Chugg, "An algorithm for counting short cycles in bipartite graphs," *IEEE Transactions on Information Theory*, vol. 52, no. 1, pp. 287–292, Jan. 2006.

[7] M. Karimi and A. H. Banihashemi, "Efficient algorithm for finding dominant trapping sets of LDPC codes," *IEEE Transactions on Information Theory*, vol. 58, no. 11, pp. 6942–6958, Nov. 2012.

[8] I. F. Blake and S. Lin, "On short cycle enumeration in biregular bipartite graphs," *IEEE Transactions on Information Theory*, vol. 64, no. 10, pp. 6526–6535, Oct. 2018.

[9] M. Battaglioni, F. Chiaraluce, M. Baldi, M. Pacenti, and D. G. M. Mitchell, "Optimizing quasi-cyclic spatially coupled LDPC codes by eliminating harmful objects," *EURASIP Journal on Wireless Communications and Networking*, vol. 63, pp. 1–29, July 2023.

[10] H. Esfahanizadeh, A. Hareedy, and L. Dolecek, "Finite-length construction of high performance spatially-coupled codes via optimized partitioning and lifting," *IEEE Transactions on Communications*, vol. 67, no. 1, pp. 3–16, 2019.

[11] J. Flum and M. Grohe, "The parameterized complexity of counting problems," *IEEE Symposium on Foundations of Computer Science Proceedings*, pp. 538–547, 2002.

[12] ——, "The parameterized complexity of counting problems," *SIAM Journal on Computing*, vol. 33, no. 4, pp. 892–922, 2004.

[13] R. Tarjan, "Enumeration of the elementary circuits of a directed graph," *SIAM Journal on Computing*, vol. 2, pp. 211–216, 1973.

[14] D. B. Johnson, "Finding all the elementary circuits of a directed graph," *SIAM Journal on Computing*, vol. 4, pp. 77–84, 1975.

[15] M. Karimi and A. H. Banihashemi, "Message-passing algorithms for counting short cycles in a graph," *IEEE Transactions on Communications*, vol. 61, no. 2, pp. 485–495, Feb. 2013.

[16] H. M. Stark and A. A. Terras, "Zeta functions of finite graphs and coverings," *Advances in Mathematics*, vol. 121, pp. 124–165, 1996.

[17] A. Dehghan and A. H. Banihashemi, "On computing the multiplicity of cycles in bipartite graphs using the degree distribution and the spectrum of the graph," *IEEE Transactions on Information Theory*, vol. 65, no. 6, June 2019.

[18] ——, "Counting short cycles in bipartite graphs: A fast technique/algorithm and a hardness result," *IEEE Transactions on Communications*, vol. 68, no. 3, pp. 1378–1390, Mar. 2020.

[19] M. Karimi and A. H. Banihashemi, "Counting short cycles of quasi cyclic protograph LDPC codes," *IEEE Communications Letters*, vol. 16, no. 3, pp. 400–403, Mar. 2012.

[20] G. J. Tee, "Eigenvectors of block circulant and alternating circulant matrices," *Research Letters in the Information and Mathematical Sciences*, vol. 8, pp. 123–142, 2005.

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

[22] Y. Wang, S. C. Draper, and J. S. Yedidia, "Hierarchical and high-girth QC LDPC codes," *IEEE Transactions on Information Theory*, vol. 59, no. 7, pp. 4553–4583, July 2013.

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

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

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

[26] J. McGowan and R. Williamson, "Loop removal from LDPC codes," *IEEE Information Theory Workshop Proceedings*, pp. 230–233, 2003.

[27] J. L. Gross and T. W. Tucker, *Topological Graph Theory*. New York: Wiley, 1987.

[28] R. Asvadi, A. H. Banihashemi, and M. Ahmadian-Attari, "Design of irregular quasi-cyclic protograph codes with low error floors," *IEEE International Symposium on Information Theory Proceedings*, pp. 908–912, 2011.

[29] ——, "Lowering the error floor of LDPC codes using cyclic liftings," *IEEE Transactions on Information Theory*, vol. 57, no. 4, pp. 2213–2224, Apr. 2011.

[30] C. A. Kelley, "On codes designed via algebraic lifts of graphs," *2008 46th Annual Allerton Conference on Communication, Control, and Computing*, pp. 1254–1261, 2008.

[31] J. Xu, L. Chen, I. Djurdjevic, S. Lin, and K. Abdel-Ghaffar, "Construction of regular and irregular LDPC codes: Geometry decomposition and masking," *IEEE Transactions on Information Theory*, vol. 53, no. 1, pp. 121–134, Jan. 2007.

[32] R. Smarandache and D. G. M. Mitchell, "A unifying framework to construct QC-LDPC tanner graphs of desired girth," *IEEE Transactions on Information Theory*, vol. 68, no. 9, pp. 5802–5822, Sept. 2022.

[33] R. Smarandache and P. O. Vontobel, "Quasi-cyclic LDPC codes: Influence of proto- and Tanner-graph structure on minimum Hamming distance upper bounds," *IEEE Transactions on Information Theory*, vol. 58, no. 2, pp. 585–607, Feb. 2012.

[34] The Sage Developers, "SageMath, the Sage Mathematics Software System," 2018. [Online]. Available: https://www.sagemath.org