Integer Ring Sieve (IRS) for Constructing Compact QC-LDPC Codes with Large Girth

Alireza Tasdighi, Emmanuel Boutillon

Integer Ring Sieve (IRS) for Constructing Compact QC-LDPC Codes with Large Girth

Alireza Tasdighi and Emmanuel Boutillon *Senior Member, IEEE*

Université de Bretagne-Sud

Lab-STICC, UMR 6285, CNRS – Lorient, France

alireza.tasdighi@univ-ubs.fr, emmanuel.boutillon@univ-ubs.fr

Abstract

This paper proposes a new method of construction of compact fully-connected Quasi-Cyclic Low Density Parity Check (QC-LDPC) code with girth $g = 10$ and $g = 12$. The originality of the proposed method is to impose constraint on the exponent matrix $\mathbf{P}$ to reduce the search space drastically. For a targeted expansion factor of N, the first step of the method is to sieve the integer ring Z_N to make a particular sub-group with specific properties to construct the second column of $\mathbf{P}$ (the first column being filled with zeros). The remaining columns of $\mathbf{P}$ are determined recursively as multiples of the second column thanks to an adaptation of the sequentially multiplied column (SMC) method where a controlled greedy search is applied at each step. The codes constructed with the proposed semi-algebraic method have lengths that can be significantly shorter than the best counterparts in the literature. To illustrate the great potential of the SMC method, we give the explicit construction of a rate 0.75 irregular LDPC code of size $65,220$ that allows a gain of 0.15 dB compared to the code of same rate and size 64,800 of the DVB-S2.

Index Terms

QC-LDPC Code Construction, Girth, Multiplicative Group, Cyclic Subgroup, Greedy Search Method.

I. Introduction

It has been more than two decades since the rediscovery of low-density parity-check (LDPC) codes as a class of modern channel coding [1]. LDPC codes can work close to the Shannon capacity with a low complexity message passing decoding algorithm. Moreover, Quasi-cyclic (QC)

LDPC code, a special class of LDPC codes, allows for efficient parallel hardware implementation and has been adopted in many communication standards. A few examples are WIFI standard [2], digital video broadcasting (DVB) standard [3], CCSDS standards [4], and more recently the 5G standard [5]. The promising coding techniques for communication systems beyond 5G are turbo codes, binary/nonbinary QC-LDPC codes [6], spatially coupled (SC) QC-LDPC codes [7], and polar codes. Assuming any scenario or application, constructing QC-LDPC codes with the smallest possible Tanner graph [8] of optimal cycle distribution free of short cycles has been a challenging issue within the past two decades. It has been shown that QC-LDPC code with a Tanner graph free of short cycles and free of some harmful combination of small cycles (known as "trapping sets") has better performance under iterative decoding algorithms. Many research works have been dedicated to study and construct such code [9], [10], [11], [12], [13], [14], [15], [16], [17], [18], [19], [20], [21], [22], [23]. One of the common methods to prevent harmful structures in Tanner graph of the code is increasing girth of the code's graph. In contrast with removing special trapping sets, which results in local improvement of performance of the code within specific SNR ranges, increasing the girth leads to a general improvement of the performance given any SNR regime. One of the main constraints of constructing a QC-LDPC code is keeping the length of the code as small as possible while preserving other good properties of that code. Considering some fixed conditions such as specific girth of the code and degree distribution of the exponent matrix, the QC-LDPC code with the shortest length can be more desirable in some cases due to easy encoding/decoding implementation, less required storage memory and low communication latency. In addition, it has recently been shown that by using some spreading techniques, a class of SC-QC-LDPC convolutional (C) codes with very low syndrome memory could be constructed based on QC-LDPC codes [21], [24], [25], [26], [27]. Specifically, [25] asserts that given fixed girth and degree distribution, the smaller the lifting degree of QC-LDPC code, the smaller the size of the syndrome memory of SC-QC-LDPCC code and thus the better performance of such code under windowed decoding. In this work we avoid the issue of SC-QC-LDPCC code and will concentrate fully on constructing short length QC-LDPC codes with girth $g = 10, 12$. However, we keep in mind SC-QC-LDPCC code is a potential candidate for beyond 5G applications, and good QC-LDPC code is the basis of good SC-QC-LDPC code.

QC-LDPC codes can be divided into two major classes: 1) random-like codes constructed by means of computer search under efficient algorithms and 2) structured codes constructed

based on algebraic tools [28]. These constructing methods all have deficiencies when considered individually. Search-based methods (even heuristic or exhaustive ones) require high search complexity but may find codes with shorter length than the ones obtained with algebraic methods. Algebraic based methods, on the other hand, will explicitly determine the code (like array code [28] of girth 6); however, so far algebraic methods are only known for the construction of small girth code, not high girth code. In fact, defining algebraic properties that are perfectly matched with high girth condition resulting in explicit construction of short length code is one of the main shortcomings of algebraic methods. In this paper we try to combine these two methods in order to construct large girth QC-LDPC code with short length in considerably lower search complexity. We take the search-based sequentially multiplied column (SMC) construction method [26] as our search algorithm and modifiy it by introducing an algebraic property for the second column of the exponent matrix of the code. The second column with the asserted algebraic property is found by an integer field sieve (IRS) method in a way that leads to search space reduction eventually. As a result, a semi algebraic fast search-based method of constructing high girth QC-LDPC code is proposed and many constructed codes of girth $g = 10, 12$ with different rates and degrees are reported. To the best of the authors' knowledge, all the constructed codes have lengths shorter (by up to 35%) or equal (for a small prototype matrix with $d_v = 3$ and $d_c \leq 8$) to their counterparts in the literature. For $d_v = 3$ and $g = 10$, the constructed codes have lengths equal, or very close, to the lower bound [29]. The paper also proposes matrices for values of d_v and d_c not yet reported in the literature. Moreover, an irregular QC-LDPC code of rate 0.75 and length 65220 bits (whose exponent matrix is locally optimized with the help of the presented SMC-structured codes) is constructed in Appdendix B. This is a counterpart code to DVB-S2 [30] code of rate 0.75 and length 64800 bits. Simulation results show the SMC-structured code outperforms by a few tenths dBs compared with rate 0.75, length 64800 DVB-S2 code. This further illustrates the usefulness of the presented high girth SMC-structured codes.

The rest of the paper is organized as follows: Section II presents the definitions and some earlier results on SMC construction based QC-LDPC codes as well as some group and number theory concepts, which will be used in later sections. Section III presents the building blocks of our proposed IRS technique. Necessary mathematical arguments, relevant greedy search algorithm, its extension for constructing the exponent matrices and the pertinent complexity analysis of the algorithm are provided in this section. Numerical results as well as simulation results are provided in Section IV. Finally, Section V concludes this paper.

II. PRELIMINARIES

In this section, we review the construction of a family of LDPC matrices well suited for hardware implementation called Quasi-Cyclic LDPC matrices. Then we discuss the conditions that result in QC-LDPC codes with good topological properties. Finally, we will give some notations and relations of group and number theories.

A. QC-LDPC block codes

Let us consider a *fully-connected* QC-LDPC block code in which the parity-check matrix is an $m \times n$ array of $N \times N$ circulant permutation matrices (CPMs), $\mathbf{I}(p_{ij})$, $0 \leq i \leq m-1$, $0 \leq j \leq n-1$, where N is the *lifting degree* of the code. $\mathbf{I}(p_{ij})$ is obtained from the identity matrix through a cyclic shift of its rows by p_{ij} positions, with $0 \leq p_{ij} \leq N-1$. The code length is $L = nN$, the column degree (i.e., the number of non-zero elements in each column) of the parity-check matrix is presented by m and the row degree (i.e., the number of non-zero elements in each row) of the parity-check matrix is presented by n[1]. The $m \times n$ matrix $\mathbf{P}$ having the integer values p_{ij} as its entries is referred to as the *exponent matrix* of the code. For such a QC-LDPC block code, a necessary and sufficient condition for the existence of a cycle of length $2k$ in its Tanner graph is

$$\sum_{i=0}^{k-1} \left(p_{m_i n_i} - p_{m_i n_{i+1}}\right) = 0 \mod N, \tag{1}$$

where $n_k = n_0$, $m_i \neq m_{i+1}$, $n_i \neq n_{i+1}$ [9].

To achieve a certain girth g, for given values of m and n, and for a fixed value of N, one has to find a matrix $\mathbf{P}$ whose entries do not satisfy (1) for any value of $k < g/2$, and any possible choice of the row and column indexes m_i and n_i. Starting from $\mathbf{P}$, the Tanner graph of the code can be easily obtained as it is unambiguously related to the values of p_{ij}.

We define a *structural cycle* in the Tanner graph of a CPM-based QC-LDPC block code as a cycle for which $\sum_{i=0}^{k-1} \left(p_{m_i n_i} - p_{m_i n_{i+1}}\right) = \beta N$, $\beta \in Z$. Indeed, this sum could be unequal to βN via altering p_{ij}s. In the face of a structural cycle, an *inevitable cycle* is defined as a cycle for which $\sum_{i=0}^{k-1} \left(p_{m_i n_i} - p_{m_i n_{i+1}}\right) = 0$, regardless of what the values of p_{ij}s are. In [9] it is shown that fully-connected CPM-based QC-LDPC codes always contain inevitable cycles of length 12, and thus their girth cannot be larger than 12.

[1]In the case that QC-LDPC code is not fully-connected, m and n are often noted by d_v and d_c in the literature, respectively

B. Code design via sequentially multiplied columns (SMC)

It is shown in [18] that the complexity of exhaustively checking equations of the type (1) goes high by increasing each one of the parameters m and n. Solutions with reduced complexity were proposed in [17] and [19], but the corresponding design methods result in girth $g = 8$. For constructing short codes with higher girths (i.e., $g = 10, 12$), many methods are developed. To the best of the authors' knowledge, the results in [26] for QC-LDPC codes with girth $g = 10, 12$ found by applying SMC construction technique are the shortest ones in the literature. Let us recall the basic assumptions of the design method proposed in [26]. The design of the parity-check matrix of a QC-LDPC block code with lifting degree N starts from an exponent matrix having the following form (SMC assumption)

$$\mathbf{P}^{\mathrm{SMC}}_{m\times n} = \left[\ \vec{0}\ \middle|\ \vec{P}_1\ \middle|\ \gamma_2 \otimes \vec{P}_1\ \middle|\ \gamma_3 \otimes \vec{P}_1\ \middle|\ \dots\ \middle|\ \gamma_{n-1} \otimes \vec{P}_1\ \right], \tag{2}$$

with m, n, $\in \mathbb{N}$, $m < n$, and $\vec{0}$ and $\vec{P}_1$ being column vectors with m entries in $\{0, \cdots, N-1\}$. The vector $\vec{0}$ is filled with all zero entries, while the entries of the vector $\vec{P}_1$ are chosen as follows: the first entry is zero, the second entry is one and the other entries are chosen in $\{2, \cdots, N-1\}$ in an increasing order. Then, the subsequent vectors have the form $\gamma_j \otimes \vec{P}_1$ $(j = 2, \cdots, n-1)$, where $\otimes$ denotes multiplication modulo N of each term of $\vec{P}_1$ with γ_j, and are computed from $\vec{P}_1$ through sequential multiplications by the coefficients $\gamma_j \in \{2, \cdots, N-1\}$ such that $\gamma_j < \gamma_{j+1}$. We now restate Proposition 1 of [26].

Proposition 2.1: Let $\mathbf{P}^{\mathrm{SMC}}_{m\times n}$ be the exponent matrix of a QC-LDPC block code C as defined in (2). Suppose that the Tanner graph associated with the sub-matrix $\left[\vec{0}\ \middle|\ \vec{P}_1\right]$ contains no inevitable cycles of lengths up to 10. Then, the Tanner graph of C has no inevitable cycle of length up to 10 for sufficiently large N and a proper choice of γ_js.

Proof: See Proposition 1 in [26]. □

Example 2.2: Let $m = 3$ and $n = 6$. Suppose that $\mathbf{P}^{\mathrm{SMC}}_{3\times 6}$ is the exponent matrix of a QC-LDPC block code C, as defined in (2), such that $\vec{P}_1 = (0, 1, 29)^T$. Considering (1), it is easy to check that the Tanner graph associated to $\left[\vec{0}\ \middle|\ \vec{P}_1\right]$ contains no inevitable cycles of length up to 10. Then, according to Proposition 2.1, the Tanner graph of C has no inevitable cycle of length up to 10 for sufficiently large N and a proper choice of γ_js. Choosing $\gamma_2 = 3$, $\gamma_3 = 7$, $\gamma_4 = 67$, and $\gamma_5 = 144$ and $N = 271$, it is easily verified that C has girth $g = 12$. The code length is $L = 1626$.

Indeed, proposition 2.1 guarantees that exponent matrices of type $\mathbf{P}_{m\times n}^{\mathrm{SMC}}$ can be avoided from having inevitable cycles of length up to 10. In order to do that, the authors of [26] established a recursive and greedy search algorithm (see algorithm 1 in [26]) to find a sufficiently large N with a proper ordered set of non-zero γ_js $(j = 2, \cdots, n-1)$ named $p_{1,j}$s as well as a proper ordered set of non-zero $p_{i,1}$s $(i = 1, \cdots, m-1)$ that do not comply with the constraint (1). It means that, with a given N, this search algorithm is supposed to find $n-2$ (resp., $m-1$) non-zero and distinct elements to be placed in the second row (resp., column) of $\mathbf{P}_{m\times n}^{\mathrm{SMC}}$. These elements vary from 1 to $N-1$, so in the worst case the overall possibilities are equal to $\binom{N-1}{n-2}\binom{N-1}{m-1}$. For high rate and high girth codes, the lifting degree is much bigger than m and n (i.e., $m, n \ll N$), so the whole search space is of $\mathcal{O}\left((N-1)^{m+n-3}\right)$. It has to be notified that if $g \in \{10, 12\}$ is our desired girth of the code, so, for each realization of the matrix $\mathbf{P}_{m\times n}^{\mathrm{SMC}}$, all the constraints of type (1) with $k < g/2$ have to be checked.

C. Some relations in Group and Number theory

Definition 2.3 (Prime factorization): Factorizing an integer composite number into a product of smaller integers is called *integer factorization*. If these integers are further restricted to prime powers, the process is called *prime factorization*.

Definition 2.4 (Co-prime integers): Two integers a and b are said to be *relatively prime* or *co-prime* if the only positive integer (factor) that divides both of them is 1. Consequently, no prime number can concurrently divide both of them. This is also equivalent to saying the Greatest Common Divisor (GCD) of a and b is 1. Standard notations for relatively prime integers a and b are $\mathrm{GCD}\,(a, b) = 1$ or $(a, b) = 1$.

If $c \geq 1$ divides a and b, we write $c \mid a$ and $c \mid b$. While c does not divide a (b) we write $c \nmid a$ ($c \nmid b$).

Definition 2.5 (Euler's totient function): Let N be a positive integer with prime factorization $N = {p_1}^{e_1} * \cdots * {p_N}^{e_N}$ $(e_i \geq 0,\ i = 1, \cdots, N)$. *Euler's totient function* counts the positive integers up to N that are relatively prime to N, and it is written as $\varphi(N)$ where, $\varphi(N) = N * (1 - 1/p_1) * ... * (1 - 1/p_N)$.

Theorem 2.6 (Euler's theorem): Suppose that N and a are co-prime positive integers. Then $a^{\varphi(N)} \equiv 1 \pmod{N}$.

Proof: See [31]. □

Definition 2.7 (Ring of integers modulo N): Ring of integers modulo N, which is written as $\mathbb{Z}_N$ (even as $\mathbb{Z}/N\mathbb{Z}$) is a set of numbers $\{0, 1, \cdots, N-1\}$ closed under two binary operations "$+$" and "$*$". Since any pair of elements in $\mathbb{Z}_N$ are commutative under operation "$+$" (resp., "$*$"), the group $(\mathbb{Z}_N, +)$ (resp., $(\mathbb{Z}_N \setminus \{0\}, *)$) is said to be *Abelian*.

It has to be understood that $(\mathbb{Z}_N \setminus \{0\}, *)$ is not a group evermore, as it has to satisfy *invertibility* condition. This condition, which certifies that every non-zero element of a group has to be invertible, is a necessary condition of the group. Furthermore, if $a, b \in \mathbb{Z}_N$, then we conventionally might use the notation ab to show $a * b$ when there is no ambiguity later.

Definition 2.8 (Multiplicative group modulo N): Let N be a positive integer. The integers co-prime (relatively prime) to N from the set $\{0, 1, \ldots, N-1\}$ of N non-negative integers form a group under multiplication modulo N, called the *multiplicative group of integers modulo* N. Another name for this group is *group of units*, and it is written as $\mathbb{Z}_N^{\times}$ (even as $(\mathbb{Z}/N\mathbb{Z})^{\times}$). Since $\varphi(N)$ counts the number of positive co-prime integers (less than N), $|\mathbb{Z}_N^{\times}| = \varphi(N)$.

Definition 2.9 (Cyclic group): A *cyclic group* G is a group that is generated by a single non identity element of this group a under group operation. Every element of this group is constructed by repeatedly applying the group operation to a or its inverse. If this group is finite with r elements, it is displayed as $\langle a \rangle = \{a^i | i = 1, 2, \cdots, r\}$.

Example 2.10 (Additive cyclic group): Let N be an arbitrary positive integer, $G = (\mathbb{Z}_N, +)$ and $a = 1$. So every element of G is generated by using repetitive summation of a modulo N.

Example 2.11 (Multiplicative cyclic group): Let $N_1 = 11$, $N_2 = 12$, $N_3 = 14$ and $N_4 = 17$. For each N_i $(i = 1, 2, 3, 4)$ we construct the corresponding multiplicative group $\mathbb{Z}_{N_i}^{\times}$, and from Definition 2.8 we know that $|\mathbb{Z}_{N_1}^{\times}| = 10$, $|\mathbb{Z}_{N_2}^{\times}| = 4$, $|\mathbb{Z}_{N_3}^{\times}| = 6$ and $|\mathbb{Z}_{N_4}^{\times}| = 16$. One can easily check that it is possible to generate all the elements in $\mathbb{Z}_{N_i}^{\times}$ $(i = 1, 3, 4)$ just by taking $a_1 = 2$ (resp., $a_3 = 2$ and $a_4 = 3$ are to be the generator element) and its repetitive multiplications modulo N. However, for the case $N_2 = 12$, there is no solo generator element for $\mathbb{Z}_{N_2}^{\times}$ thus, it is not cyclic.

Theorem 2.12: For any prime number p, $\mathbb{Z}_p^{\times}$ is always cyclic and there is a so-called generator $a \in \mathbb{Z}_p^{\times}$ (named as *primitive element* of $\mathbb{Z}_p^{\times}$) so that $\mathbb{Z}_p^{\times} = \{a^i | i = 1, 2, \cdots, p-1\}$.

Proof: See [31]. □

Note that Theorem 2.12 is not valid for an arbitrary integer value N. As we can see from Example 2.11, $\mathbb{Z}_{12}^{\times}$ is not cyclic but $\mathbb{Z}_{14}^{\times}$ is cyclic; however none of the integers 12 and 14 are prime numbers.

Definition 2.13 (Subgroup): Given a group G under a binary operation "$*$", a subset S of G is called a subgroup of G if S also forms a group under the operation "$*$". This is usually denoted by $S \leq G$ and read as "S is a subgroup of G".

Definition 2.14 (Order of an element): Let G be a finite group under a binary operation "$*$", $|G| = n$, $a \in G$, and e is the identity element of G. The smallest positive integer r ($1 \leq r \leq n$) for which $a^r = e$ is called the order of a (or simply $\mathrm{O}(a)$) where

$$a^r = \overbrace{a * a * \cdots * a}^{r \text{ times}}. \tag{3}$$

Definition 2.15 (Order of a group): The order of a finite group G is equal to the number of elements in G and is written as $\mathrm{O}(G)$.

If $G = \langle a \rangle$ is a cyclic group with generator a, then the order of G is equal to the order of its generator, i.e., $\mathrm{O}(a) = \mathrm{O}(\langle a \rangle)$.

Theorem 2.16 (Lagrange's theorem): For any finite group G, the order of every subgroup S of G divides the order of G. Thus, $\mathrm{GCD}(\mathrm{O}(S), \mathrm{O}(G)) = \mathrm{O}(S)$.

Proof: See [31]. □

Corollary 2.17: Let G be a finite group. For an arbitrary element $a \in G$, $\langle a \rangle = \{a^i | i = 1, 2, \cdots, \mathrm{O}(a)\}$ is a cyclic subgroup of G. In addition, $\mathrm{GCD}(\mathrm{O}(\langle a \rangle), \mathrm{O}(G)) = \mathrm{O}(\langle a \rangle)$.

Proof: The result is a direct conclusion of Definition 2.9 and of Theorem 2.16. □

Suppose that N ($N > 1$) is an integer number, $a, b \in \mathbb{Z}_N$ and $a \neq 0$. In the upcoming sections, it is needed to find the solution of equation $a\mathrm{x} = b$, and under which circumstances b is dividable by a. The next proposition determines this condition.

Proposition 2.18: Let N ($N > 1$) be an integer number, $a, b \in \mathbb{Z}_N$, and $a \neq 0$. Also let d be equal to $d = \mathrm{GCD}(a, N)$. Equation $ax \equiv b \mod N$ has no solution if $d \nmid b$, and it has d different solutions if $d|b$. In addition, let x_0 be the only solution of the equation $(a/d)\, x \equiv (b/d) \mod (N/d)$. So, d different solutions of the primary equation are $x_i = x_0 + (i * (N/d))$ ($i = 0, 1, \cdots, d-1$).

Proof: See [31]. □

Example 2.19: Let $N = 18$, $a = 14$, and $b = 12$. So, $d = \mathrm{GCD}(14, 18) = 2$ and $d|b$. In this case, we solve the equation $(14/2)\, x \equiv (12/2) \mod (18/2)$, and $x_0 = 6$ is the solution. Since $d = 2$, the equation $14x \equiv 12 \mod 18$ has two different solutions: $x_0 = 6$ and $x_1 = 6 + (1 * (18/2)) = 15$.

In the next section, our method of sieving integer ring as well as a controlled greedy search algorithm for implementing this method is fully explained.

III. Integer Ring Sieve to find permissible elements for the vector $\vec{P}_1$

This section is divided into four parts. In Part A, we propose our definition of *equivalent* relations of type (1) (i.e., equivalent cycles) in an exponent matrix (Tanner graph) of a fully-connected QC-LDPC code as well as give a theorem for counting all classes of cycles under this equivalent relation, i.e., the number of *nonequivalent* cycles of length $2k$ ($k = 2, 3, 4, 5$) in this matrix (graph). In Part B, several properties for selecting the second column of matrix $\mathbf{P}^{\mathrm{SMC}}_{m\times n}$ (i.e., $\vec{P}_1$) are suggested. Indeed, depending on the size of d_v, we propose a specific property for the elements in $\vec{P}_1$ in a way that we can reduce the number of "potential but nonequivalent" cycles by a factor of 3 when $d_v = 3$ and a factor of $d_v - 1$ if $d_v > 3$. In Part C, some arguments and statistics in existence of proper sieve occurrences that can meet properties suggested in Part B are provided. Our greedy search algorithm is explained in Part D with pseudo code. Complexity analyses for highlighting the important role of our sieving method in reducing the search space are also provided in this final part.

A. Counting nonequivalent relations of type (1) corresponding to nonequivalent potential cycles of Tanner graph of a fully-connected QC-LDPC code

Definition 3.1 (Potential cycle): Let $\mathbf{P}$, N, k and $p_{m_i n_i}, p_{m_i n_{i+1}} \in \mathbf{P}$ $(0 \le i \le k-1)$ be the parameters in relation (1). To address any set of $2k$ elements $p_{m_i n_i}$ that meets the conditions $n_0 = n_k$, $m_i \neq m_{i+1}$, and $n_i \neq n_{i+1}$, we consider its corresponding summation, name it as *potential* cycle $\mathcal{C}_{2k}$ of $\mathbf{P}$, and display it as

$$\mathcal{C}_{2k} : \sum_{i=0}^{k-1} \left(p_{m_i n_i} - p_{m_i n_{i+1}}\right). \tag{4}$$

In fact, as long as the elements p_{ij}s are considered as symbolic within this summation and are not assigned with some integers, we call this cycle potential. When all the elements within this summation are assigned with integers and the summation is equal to zero modulo N, then $\mathcal{C}_{2k}$ is an *activated* cycle.

Simply, any activated cycle is considered a realization of a potential cycle. In other words, a potential cycle $\mathcal{C}_{2k}$ is a symbolic presentation of its corresponding activated cycle. So, if girth of QC-LDPC code C is g it means 1) none of its potential cycles of length $2k$ ($k < g/2$) are

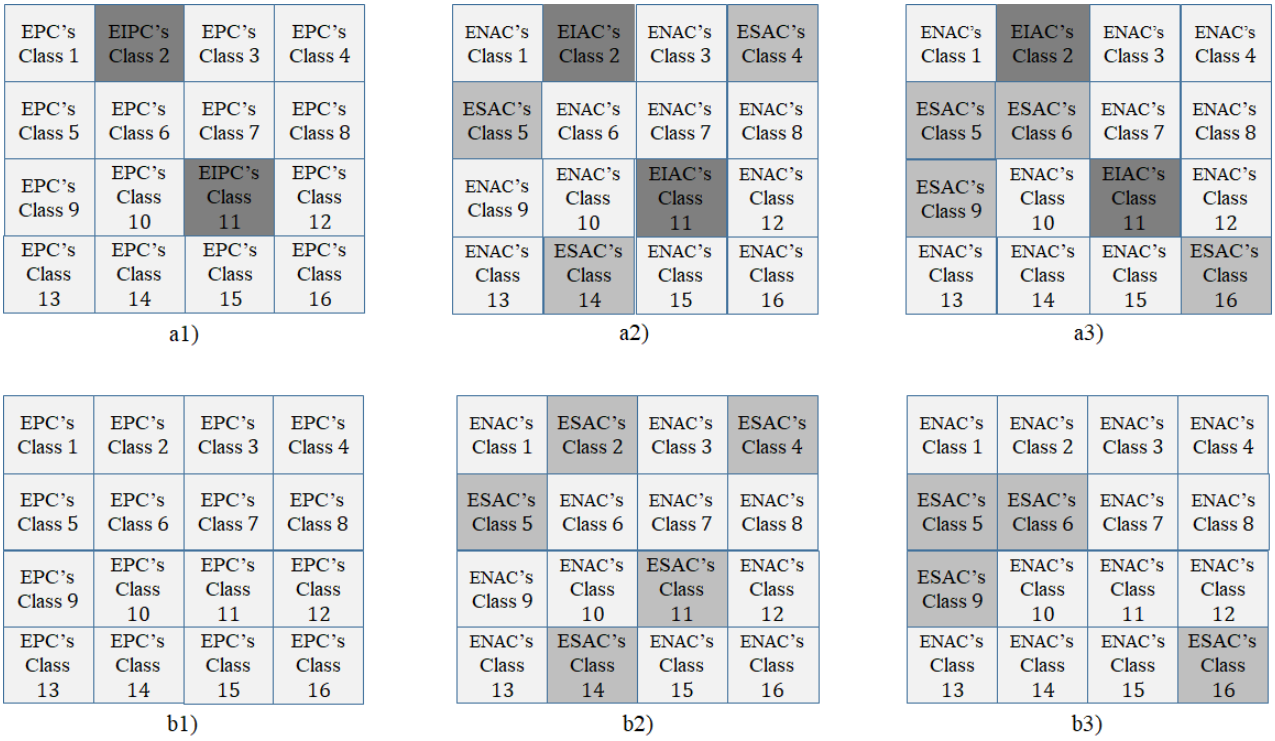

Fig. 1. Nexus of different categorizing of cycles. (a1) and (b1) are diagrams to different classes of equivalent cycles of length $2k$ before assigning p_{ij} values. (a2) and (a3) are different realizations of (a1), and, (b2) and (b3) are different realizations of (b1) after assigning p_{ij} values.

activated after assigning values to p_{ij}s and 2) there is no inevitable (potential or activated) cycle of length $2k$ ($k < g/2$) in code C[2].

Definition 3.2 (Equivalent cycles): Let $\mathcal{C}_{2k}$ be a potential cycle defined in 3.1. Potential cycle $\mathcal{C}'_{2k}$ with corresponding summation $\sum_{i=0}^{k-1}(p_{m'_i n'_i} - p_{m'_i n'_{i+1}})$ is *equivalent* to the cycle $\mathcal{C}_{2k}$, if and only if, $n'_0 = n'_k$, $m'_i \neq m'_{i+1}$, $n'_i \neq n'_{i+1}$, $\bigcup_{i=0}^{k-1}\{(m'_i, n'_i), (m'_i, n'_{i+1})\} = \bigcup_{i=0}^{k-1}\{(m_i, n_i), (m_i, n_{i+1})\}$ and $|\sum_{i=0}^{k-1}(p_{m'_i n'_i} - p_{m'_i n'_{i+1}})| = |\sum_{i=0}^{k-1}(p_{m_i n_i} - p_{m_i n_{i+1}})|$. In other words, $\mathcal{C}'_{2k}$ is derived by specifically reordering the terms of summation $\sum_{i=0}^{k-1}(p_{m_i n_i} - p_{m_i n_{i+1}})$ or by the additive inverse of it.

Note that with our definition of equivalent cycles $\mathcal{C}_{2k}$ and $\mathcal{C}'_{2k}$, one can imagine that $\mathcal{C}_{2k}$ is an activated cycle if and only if $\mathcal{C}'_{2k}$ is. Moreover, equivalent cycles are involved in the same rows,

[2]Note that in this context an inevitable cycle could be considered both as potential and activated. In fact, before assigning values to the elements of $\mathbf{P}$ an inevitable cycle is called Inevitable Potential Cycle (IPC) while it is called Inevitable Activated Cycle (IAC) afterward.

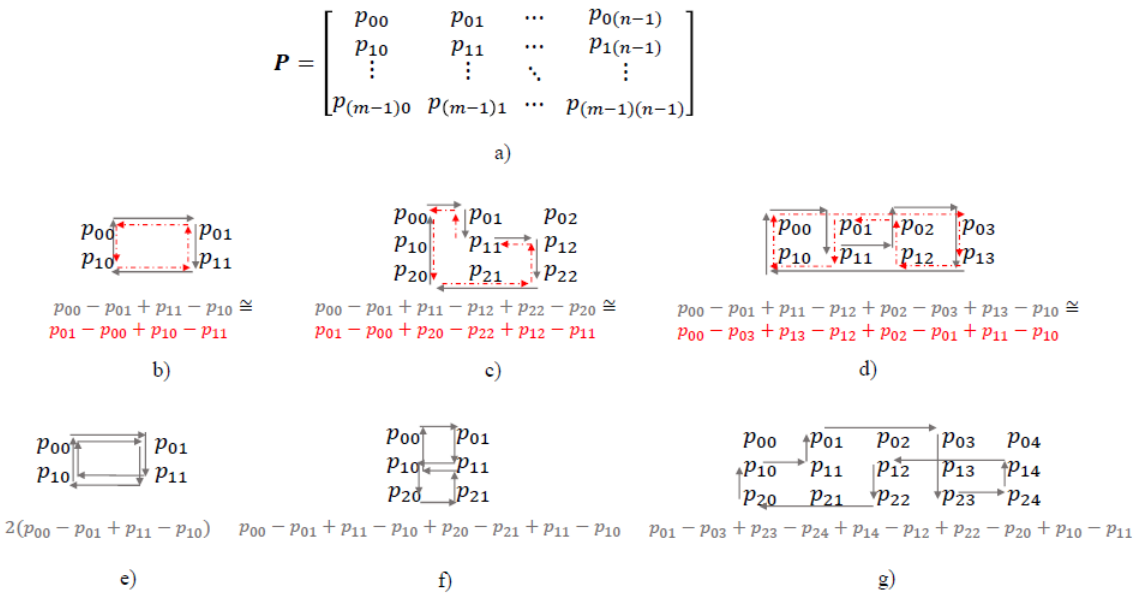

Fig. 2. Sample paths for cycles of length between 4 and 10 involved in exponent matrix $\mathbf{P}$: a) exponent matrix of size $m \times n$. b) paths of length 4 equivalent cycles. c) paths of length 6 equivalent cycles. d) paths of length 8 equivalent cycles. e) path of a length 8 cycle nonequivalent to (d). f) another path of a length 8 cycle nonequivalent to the paths (d) and (e). g) path of a length 10 cycle.

the same columns, and even in the same elements of $\mathbf{P}$.

To further address the nexus of our various categorizing of cycles, we consider a formal cycle $\mathcal{C}_{2k}$ in $\mathbf{P}$ with two scenarios: 1) $\mathbf{P}$ contains several nonequivalent classes of potential cycles of length $2k$ where some of them are inevitable cycles and 2) $\mathbf{P}$ contains several nonequivalent classes of potential cycles of length $2k$ with no inevitable cycle. (a1) and (b1) in Fig.1 depict a diagram with 16 nonequivalent classes of potential cycles of length $2k$ respectively for scenario 1 and 2. In scenario 1, we see two classes of Equivalent Inevitable Potential Cycles (EIPC's). (a2) and (a3) in Fig.1 are two different realizations of (a1) related to two different assignments of p_{ij}s. As can be seen, there are three types of equivalent classes in (a2) and (a3). The first one is Equivalent Not-Activated Cycles (ENAC's), second one is Equivalent Structurally Activated Cycles (ESAC's), and the last one is Equivalent Inevitably Activated Cycles (EIAC's). (b2) and (b3) in Fig.1 are also two different realizations of (b1) related to two different assignments of p_{ij}s. As can be seen, there are no EIACs in these diagrams because there were no EIPCs in (b1). In this work we follow scenario 2 and will try to find the optimal assignment in order to keep all the potential cycles of length $2k$ ($k = 2, 3, 4, 5$) inactivated, as there is no inevitable

cycle of length $2k$ ($k = 2, 3, 4, 5$) in the exponent matrix of a fully-connected QC-LDPC code. The following example also further illustrates the perception of equivalent potential cycles.

Example 3.3: Suppose that $\mathbf{P}$ is the exponent matrix in Fig. 2 (a). Cycles $\mathcal{C}_4$, $\mathcal{C}_6$, and $\mathcal{C}_8$, which are depicted with continuous arrows respectively in Fig. 2 (b), (c) and (d), are considered potential cycles. Indeed, depending on the values of p_{ij}, which are taken from the set $\{0, 1, \cdots, N-1\}$, their corresponding summations may (or may not) be equal to zero modulo N. However, regardless of the amount of their summation, each one of these cycles has some other equivalent representation in matrix $\mathbf{P}$. For instance, dash-dot arrows in Fig. 2 (b) and (c) respectively show another equivalent representation (i.e. additive inverse) of $\mathcal{C}_4$ and $\mathcal{C}_6$. Also, the dash-dot arrows in part (d) display a rearrangement of the summation corresponding to $\mathcal{C}_8$ and thus presents an equivalent cycle of $\mathcal{C}_8$.

The definition of equivalent classes of cycles reduces the number of equations to be verified in constructing QC-LDPC code of given girth, so it accelerates the search process. We will argue this method further in the following sections when we try to explain our search algorithm. However, before that we provide a definition and a theorem here to count nonequivalent potential cycles of length less than or equal to 10 in an exponent matrix $\mathbf{P}$ of size $m \times n$ where $m, n \geq 2$.

Definition 3.4 (Cycle's tracking matrix of order $2k$): Cycle's tracking matrix of order $2k$ is a square matrix of size k ($k = 2, 3, \cdots$) where its (i-j)$^{\text{th}}$ component counts the number of non-equivalent potential cycles of length $2k$ that involve all rows and columns of a matrix of size $i \times j$. This matrix is written as $T^{\mathcal{C}_{2k}}$.

It has to be noted that $T^{\mathcal{C}_{2k}}$ is symmetrical (i.e., $T^{\mathcal{C}_{2k}} = \left(T^{\mathcal{C}_{2k}}\right)^T$) as the number of potential cycles involved in a $i \times j$ matrix is equal to the number of such cycles involved in matrix of size $j \times i$.

Theorem 3.5: Let $\mathbf{P}_{m\times n}$ be an exponent matrix of a fully-connected QC-LDPC code with $m \geq 2$ and $n \geq 2$ and $\#\mathcal{C}_{2k}^{m,n}$ be the number of nonequivalent potential cycles of length $2k$ ($k = 2, 3, 4, 5$) involved in $\mathbf{P}_{m\times n}$. So

$$\#\mathcal{C}_{2k}^{m,n} = \sum_{i=2}^{\min\{k,m\}} \sum_{j=2}^{\min\{k,n\}} t_{ij}^{\mathcal{C}_{2k}} \binom{m}{i} \binom{n}{j}, \tag{5}$$

where $t_{ij}^{\mathcal{C}_{2k}}$ is the $(i\text{-}j)^{\text{th}}$ component of cycle's tracking matrix $T^{\mathcal{C}_{2k}}$ $(k=2,3,4,5)$ below

$$T^{\mathcal{C}_4}=\begin{bmatrix}0&0\\0&1\end{bmatrix},\ T^{\mathcal{C}_6}=\begin{bmatrix}0&0&0\\0&0&0\\0&0&6\end{bmatrix},\ T^{\mathcal{C}_8}=\begin{bmatrix}0&0&0&0\\0&1&3&3\\0&3&18&36\\0&3&36&72\end{bmatrix},\ T^{\mathcal{C}_{10}}=\begin{bmatrix}0&0&0&0&0\\0&0&0&0&0\\0&0&60&180&180\\0&0&180&900&1440\\0&0&180&1440&1440\end{bmatrix}$$

and $\binom{n}{r}$ is equal to $\frac{n!}{r!(n-r)!}$ when $r\leq n$ and 0 otherwise.

Proof: First we notice that based on relation (1) a potential cycle $\mathcal{C}_{2k}$ of length $2k$ $(k\geq 2)$ is involved in at most k rows as well as k columns of matrix $\mathbf{P}_{m\times n}$. Secondly, for constitution of a cycle of length $2k$, the minimum required number of columns (rows) of $\mathbf{P}_{m\times n}$ is 2 when k is an even number and 3 otherwise. So the term $\binom{m}{i}\binom{n}{j}$ in relation (5) enumerates all the sub-matrices of size $i\times j$ of a matrix of size $m\times n$ where $2\leq i\leq \min\{k,m\}$ and $2\leq j\leq \min\{k,n\}$. For each one of such sub-matrices, $t_{ij}^{\mathcal{C}_{2k}}$ counts the number of nonequivalent potential cycles that are involved in a sub-matrix of size $i\times j$. By computer programming it is possible to enumerate all such cycles of length $2k$ $(k=2,3,4,5)$ which occupy i rows and j columns. For example, parts (d), (e), (f), and (g) of Fig. 2 are certain samples of potential cycles respectively of size 8, 8, 8, and 10 occupying all rows and columns of sub-matrices of dimension 2×4, 2×2, 3×2, and 3×5. We used computer programming, and the derived results are summarized in tracking matrices $T^{\mathcal{C}_{2k}}$ $(k=2,3,4,5)$. In summary, relation (5) considers multiplicities of sub-matrices of size $i\times j$ multiplied by nonequivalent potential cycles of length $2k$ that are involved in such matrices. □

Given that g is our desired girth of a code with exponent matrix $\mathbf{P}$ of size $m\times n$, one quick impression of Theorem 3.5 is the verification algorithm[3] has to make sure that none of the nonequivalent cycles of length $2k$ $(k<g/2)$ is activated. Table I contains multiplicities of such cycles for certain sizes of m, and n. For instance, if $g=12$, $m=3$ and $n=10$, then the verification algorithm is supposed to check $\#\mathcal{C}_4^{3,10}+\#\mathcal{C}_6^{3,10}+\#\mathcal{C}_8^{3,10}+\#\mathcal{C}_{10}^{3,10}=135+720+12960+90360=104175$ nonequivalent cycles of lengths 4 to 10 are not activated. In addition, with some modifications we are still able to further reduce the number of these

[3]We recall that greedy search algorithm in [26] consists of two main parts: 1) picking proper elements from the set $\{1,\cdots,N-1\}$ to be placed as components of sequential rows (columns) of $\mathbf{P}$ 2) verifying if every cycle of length less than g remains potential for the assigned $\mathbf{P}$ or not. A proper selection (part (1)) along with a valid verification (part (2)) will terminate this algorithm successfully.

TABLE I

NUMBER OF NONEQUIVALENT POTENTIAL CYCLES OF SIZE $2k$ ($k = 2, 3, 4, 5$) WHICH ARE INVOLVED IN MATRIX $\mathbf{P}_{m\times n}$, WHEN, $2 \leq m \leq 5$ AND $2 \leq n \leq 10$.

–	m=2				m=3				m=4				m=5			
–	$\#\mathcal{C}_4^{2,n}$	$\#\mathcal{C}_6^{2,n}$	$\#\mathcal{C}_8^{2,n}$	$\#\mathcal{C}_{10}^{2,n}$	$\#\mathcal{C}_4^{3,n}$	$\#\mathcal{C}_6^{3,n}$	$\#\mathcal{C}_8^{3,n}$	$\#\mathcal{C}_{10}^{3,n}$	$\#\mathcal{C}_4^{4,n}$	$\#\mathcal{C}_6^{4,n}$	$\#\mathcal{C}_8^{4,n}$	$\#\mathcal{C}_{10}^{4,n}$	$\#\mathcal{C}_4^{5,n}$	$\#\mathcal{C}_6^{5,n}$	$\#\mathcal{C}_8^{5,n}$	$\#\mathcal{C}_{10}^{5,n}$
$n=2$	1	0	1	0	3	0	6	0	6	0	21	0	10	0	55	0
$n=3$	3	0	6	0	9	6	45	60	18	24	189	420	30	60	555	1680
$n=4$	6	0	21	0	18	24	189	420	36	96	864	3300	60	240	2640	14460
$n=5$	10	0	55	0	30	60	555	1680	60	240	2640	14460	100	600	8200	65940
$n=6$	15	0	120	0	45	120	1305	4980	90	480	6345	45660	150	1200	19875	212340
$n=7$	21	0	231	0	63	210	2646	12180	126	840	13041	116760	210	2100	41055	548940
$n=8$	28	0	406	0	84	336	4830	26040	168	1344	24024	257880	280	3360	75880	1220520
$n=9$	36	0	666	0	108	504	8154	50400	216	2016	40824	511560	360	5040	129240	2431800
$n=10$	45	0	1035	0	135	720	12960	90360	270	2880	65205	934920	450	7200	206775	4457880

nonequivalent cycles. To this end, a special class of exponent matrices with SMC assumption and a predetermined column is considered in the following part.

B. Designing $\vec{P}_1$ using cyclic subgroups of multiplicative group $\mathbb{Z}_N^\times$

Let $\vec{P}_1$ be the second column of exponent matrix $\mathbf{P}_{m\times n}^{\mathrm{SMC}}$ that is introduced in relation (2). In this part we try to pick the non-zero elements of $\vec{P}_1$ from a specific cyclic subgroup of $\mathbb{Z}_N^\times$. Depending on the value of d_v (i.e., value of m), we consider a specific cyclic subgroup and then propose allocating some or all of the elements in this subgroup to p_{1j} ($1 \leq j \leq m-1$). The main reason behind such allocation is reducing the number of nonequivalent potential cycles to some extent, and thus accelerating our verification algorithm. We select our candidate subgroup in a way that it can impose equivalent potential cycles to $\mathbf{P}_{m\times n}^{\mathrm{SMC}}$, as much as possible. These extra equivalent cycles are some of those nonequivalent cycles that are enumerated in Theorem 3.5 in general, but here they could be considered as equivalent due to the property of our selected subgroup. Furthermore, by following this approach we have two other important properties. Firstly, by forcing some counted nonequivalent cycles in Theorem 3.5 to be in pre-known equivalent classes, we not only can reduce the search space, but also increase the chance of finding codes with an assumed girth. Secondly, since our designation of $\vec{P}_1$ is done *a priori* and definite, the elements in $\vec{P}_1$ would not be variables anymore. The search complexity is reduced to determining elements γ_j ($j = 2, 3, \cdots, n-1$), only.

We pass further discussions to the next sections and will focus on two specific lemmas. These lemmas elucidate both the selecting of cyclic subgroups and the role of these subgroups in reducing nonequivalent potential cycles.

Lemma 3.6: Suppose that $\mathbf{P}_{3\times n}^{\mathrm{SMC}}$ is an exponent matrix of form (2) with lifting degree N and $\vec{P}_1 = [0, 1, a]^T$ is the second column of $\mathbf{P}_{3\times n}^{\mathrm{SMC}}$ where a is a non-identity element in multiplicative group $\mathbb{Z}_N^{\times}$ with property $a * (1-a) = 1$ and superscript "T" stands for vector transpose. Thus, $O(\langle a\rangle) = 6$ and

$$\#\mathcal{C}_{2k,a}^{3,n} \leq \frac{\#\mathcal{C}_{2k}^{3,n}}{3}$$

where $\#\mathcal{C}_{2k,a}^{3,n}$ is the number of nonequivalent potential cycles of length $2k$ ($k = 2, 3, 4, 5$) pertaining to $\mathbf{P}_{3\times n}^{\mathrm{SMC}}$ with the second column $\vec{P}_1$, and $\#\mathcal{C}_{2k}^{3,n}$ is introduced in Theorem 3.5 for the general case of an exponent matrix $\mathbf{P}_{3\times n}$ with three rows.

Proof: To show that $O(\langle a\rangle)$ is 6 we need to show that $O(a) = 6$. To this end, we consider the assumption $a * (1-a) = a - a^2 = 1$ and repeatedly apply the group operation to a as follows:

$$a^2 = a * a = a - 1, \;\; a^3 = a * a^2 = a^2 - a = -1, \;\; a^4 = a * a^3 = -a,$$
$$a^5 = a * a^4 = 1 - a, \;\; a^6 = a * a^5 = a - a^2 = 1.$$

To prove $\#\mathcal{C}_{2k,a}^{3,n} \leq \frac{\#\mathcal{C}_{2k}^{3,n}}{3}$, we show that for any potential cycle $\mathcal{C}_{2k}$: $\sum_{i=0}^{k-1}(p_{m_i n_i} - p_{m_i n_{i+1}})$ in matrix $\mathbf{P}_{3\times n}^{\mathrm{SMC}}$ below

$$\begin{bmatrix} 0 & 0 & 0 & \cdots & 0 \\ 0 & 1 & \gamma_2 & \cdots & \gamma_n \\ 0 & a & a\gamma_2 & \cdots & a\gamma_n \end{bmatrix}, \tag{6}$$

there are at least two corresponding and avoidable cycles $a\mathcal{C}_{2k}$: $\sum_{i=0}^{k-1}\left(ap_{m_i n_i} - ap_{m_i n_{i+1}}\right)$ and $(1-a)\,\mathcal{C}_{2k}$: $\sum_{i=0}^{k-1}\left((1-a)\,p_{m_i n_i} - (1-a)\,p_{m_i n_{i+1}}\right)$ in this matrix that have the same length as $\mathcal{C}_{2k}$ but are located in different positions (with partly different elements) of $\mathbf{P}_{3\times n}^{\mathrm{SMC}}$ compared with $\mathcal{C}_{2k}$. Note that in Definition 3.2 it was emphasized that equivalent potential cycles will occupy exactly the same elements, rows and columns of matrix $\mathbf{P}$, so in the context of Definition 3.2, potential cycles $\mathcal{C}_{2k}$, $a\mathcal{C}_{2k}$ and $(1-a)\mathcal{C}_{2k}$ are nonequivalent. However, as it will be shown later, $\mathcal{C}_{2k}$ is an activated cycle if and only if $a\mathcal{C}_{2k}$ ($(1-a)\,\mathcal{C}_{2k}$) is activated. Thus, we consider them as equivalent cycles. In other words, by verifying one, the other two will be verified. Before continuing, we need to establish a fact regarding isomorphic exponent matrices.

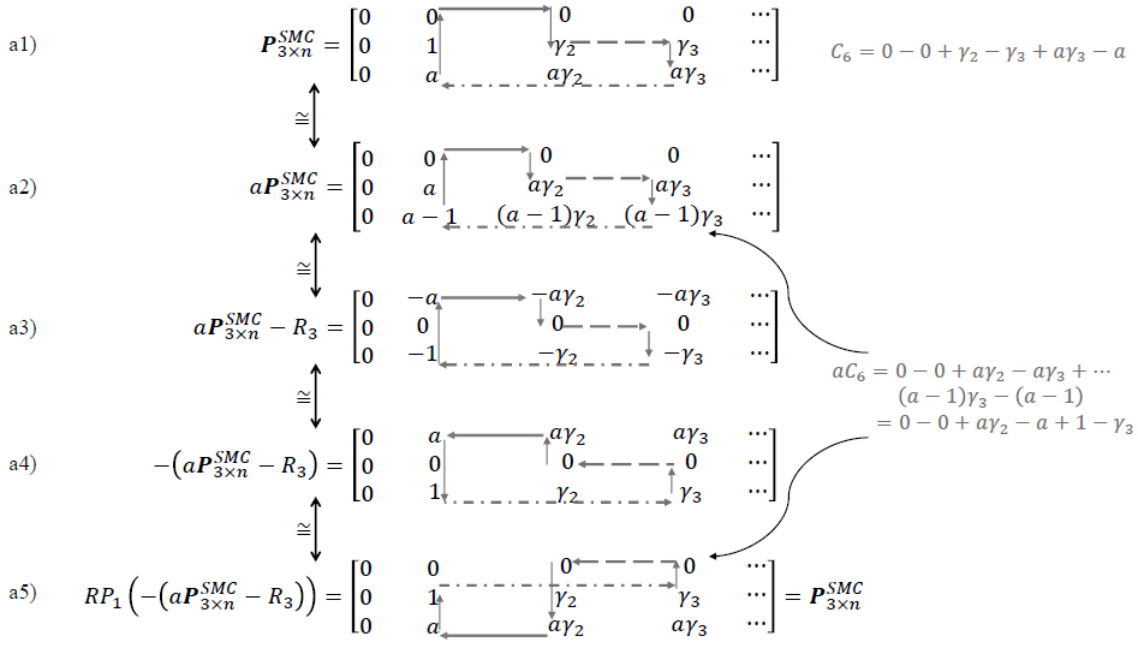

Fig. 3. Isomorphic forms of exponent matrix $\mathbf{P}^{\mathrm{SMC}}_{3\times n}$ under transformation $RP_1\left(-\left(aX - R_3\right)\right)$: parts (a1) to (a5) clarify the stepwise impact of transformation $RP_1\left(-\left(aX - R_3\right)\right)$ on both $\mathbf{P}^{\mathrm{SMC}}_{3\times n}$ and the sample path of a potential cycle $\mathcal{C}_6$.

Let $N \in \mathbb{N}$, $a \in \mathbb{Z}_N^{\times}$, and $\mathbf{P}_1$ (resp., $\mathbf{P}_2$) be an exponent matrix of code C_1 (resp., C_2) with lifting degree N. It is shown [18] that $\mathbf{P}_2$ (or the equivalent Tanner graph of C_2) is isomorphic to $\mathbf{P}_1$ (Tanner graph of C_1) if it is constructed by row (column) permutation of $\mathbf{P}_1$ and/or by adding a constant to each row (column) of $\mathbf{P}_1$ and/or by multiplying a to $\mathbf{P}_1$. Given this fact and considering $\mathrm{GCD}\left(a, N\right) = \mathrm{GCD}\left(1-a, N\right) = 1$, we have $\mathbf{P}^{\mathrm{SMC}}_{3\times n} \cong a\mathbf{P}^{\mathrm{SMC}}_{3\times n} \cong (1-a)\,\mathbf{P}^{\mathrm{SMC}}_{3\times n}$ where "$\cong$" stands for isomorphic relation. $\mathcal{C}_{2k}$ is also an activated cycle (i.e., its summation is equal to zero modulo N) if and only if $a\mathcal{C}_{2k}$ ($(1-a)\mathcal{C}_{2k}$) is activated. Now consider the cycle-path $\mathcal{C}_{2k}$ ($k = 2, 3, 4, 5$) in matrix $\mathbf{P}^{\mathrm{SMC}}_{3\times n}$ (see Fig. 3 (a1) or Fig. 4 (a1) for a sample cycle of length six). Additionally, consider the cycle-paths of $a\mathcal{C}_{2k}$ and $(1-a)\mathcal{C}_{2k}$, respectively, in $a\mathbf{P}^{\mathrm{SMC}}_{3\times n}$ and $(1-a)\mathbf{P}^{\mathrm{SMC}}_{3\times n}$ (see Fig. 3 (a2) or Fig. 4 (a2) for the cycle of length six). In the sequel, we attempt to illustrate the cycle-path $a\mathcal{C}_{2k}$ (resp., $(1-a)\mathcal{C}_{2k}$) in matrix $a\mathbf{P}^{\mathrm{SMC}}_{3\times n}$ (resp., $(1-a)\mathbf{P}^{\mathrm{SMC}}_{3\times n}$) has an isomorphic form in matrix $\mathbf{P}^{\mathrm{SMC}}_{3\times n}$.

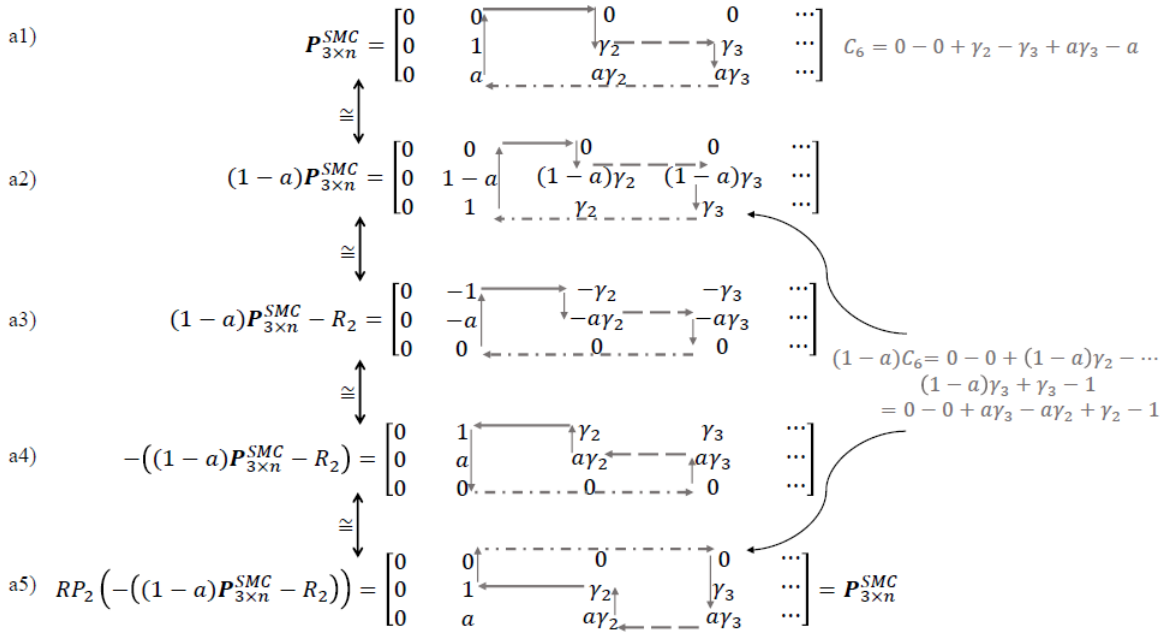

Fig. 4. Isomorphic forms of exponent matrix $\mathbf{P}_{3\times n}^{\mathrm{SMC}}$ under transformation $RP_2\left(-\left(\left(1-a\right)X - R_2\right)\right)$: parts (a1) to (a5) clarify the stepwise impact of transformation $RP_2\left(-\left(\left(1-a\right)X - R_2\right)\right)$ on both $\mathbf{P}_{3\times n}^{\mathrm{SMC}}$ and the sample path of a potential cycle $\mathcal{C}_6$.

Assume that matrices R_2, R_3, RP_1 and RP_2 are defined as follows:

$$R_2 = \begin{bmatrix} 0 & 1 & \gamma_2 & \cdots & \gamma_n \\ 0 & 1 & \gamma_2 & \cdots & \gamma_n \\ 0 & 1 & \gamma_2 & \cdots & \gamma_n \end{bmatrix}, R_3 = \begin{bmatrix} 0 & a & a\gamma_2 & \cdots & a\gamma_n \\ 0 & a & a\gamma_2 & \cdots & a\gamma_n \\ 0 & a & a\gamma_2 & \cdots & a\gamma_n \end{bmatrix}, RP_1 = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}, RP_2 = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}, \tag{7}$$

where R_i $(i = 2, 3)$ is constructed from the i^{th} row of matrix $\mathbf{P}_{3\times n}^{\mathrm{SMC}}$ and RP_i $(i = 1, 2)$ is a row permutation matrix to be applied on $\mathbf{P}_{3\times n}^{\mathrm{SMC}}$. So, matrix $RP_1\left(-\left(a\mathbf{P}_{3\times n}^{\mathrm{SMC}} - R_3\right)\right)$, which is constructed by applying linear transformations as well as row permutation matrix RP_1 on $a\mathbf{P}_{3\times n}^{\mathrm{SMC}}$ (see Fig. 3 parts (a3) to (a5)), has a form exactly like matrix $\mathbf{P}_{3\times n}^{\mathrm{SMC}}$. Furthermore, the cycle $a\mathcal{C}_{2k}$ has a new path in the resulting matrix and, at the same time, is isomorphic to the cycle in matrix $a\mathbf{P}_{3\times n}^{\mathrm{SMC}}$ (Fig.3 part (a2)). Similarly, matrix $RP_2\left(-\left(\left(1-a\right)\mathbf{P}_{3\times n}^{\mathrm{SMC}} - R_2\right)\right)$ is constructed by applying linear transformations as well as row permutation RP_2 on $(1-a)\mathbf{P}_{3\times n}^{\mathrm{SMC}}$ (see Fig. 4 parts (a3) to (a5)), and it has a form exactly like matrix $\mathbf{P}_{3\times n}^{\mathrm{SMC}}$, too. Also, the cycle $(1-a)\mathcal{C}_{2k}$ has a new path in the resulting matrix and, at the same time, is isomorphic to the cycle in matrix $(1-a)\mathbf{P}_{3\times n}^{\mathrm{SMC}}$ (Fig.4 part (a2)). As the permutation matrices RP_1 and RP_2 will entirely permute the rows of a matrix and, at the same time, are different from each other, so the new

path of cycle $a\mathcal{C}_{2k}$ (resp., $(1-a)\mathcal{C}_{2k}$) in the resulting matrix (i.e., matrix in part (a5)) would be different from the path of cycle $\mathcal{C}_{2k}$ (in matrix part (a1)) and different from $(1-a)\mathcal{C}_{2k}$ (resp., $a\mathcal{C}_{2k}$). To summarize, for an arbitrary potential cycle $\mathcal{C}_{2k}$, there are two other different potential cycles $a\mathcal{C}_{2k}$ and $(1-a)\mathcal{C}_{2k}$ with the same length as $\mathcal{C}_{2k}$, and the verification algorithm needs to check only one of them. Since $a\mathcal{C}_{2k}$ and $(1-a)\mathcal{C}_{2k}$ have cycle-paths in $\mathbf{P}^{\mathrm{SMC}}_{3\times n}$ different from $\mathcal{C}_{2k}$, $\#\mathcal{C}^{3,n}_{2k,a} \leq \frac{\#\mathcal{C}^{3,n}_{2k}}{3}$. □

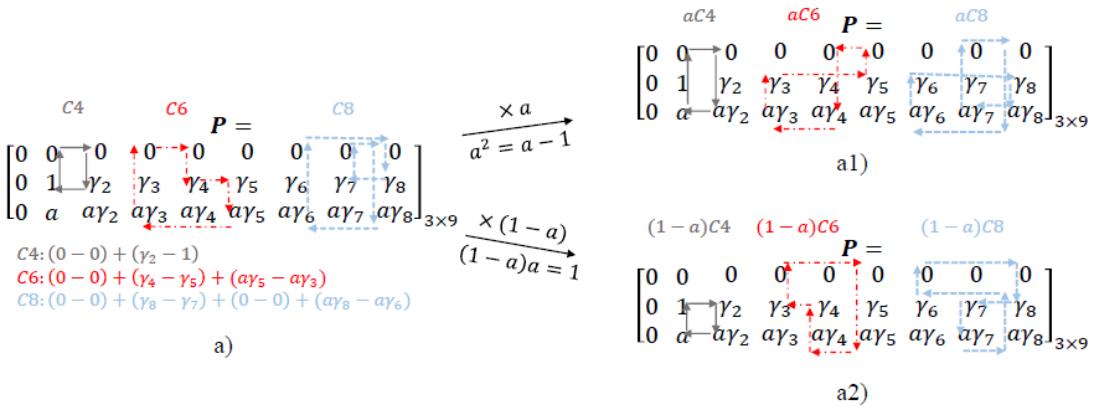

Fig. 5. Samples of isomorphic paths of cycles with different length in $\mathbf{P}^{\mathrm{SMC}}_{3\times 9}$: a) primary underlined paths for cycles $\mathcal{C}_4$, $\mathcal{C}_6$ and $\mathcal{C}_8$. a1) isomorphic paths for the considered primary paths in part (a) derived from transformation $\mathbf{t}_1$. a2) isomorphic paths for the considered primary paths in part (a) derived from transformation $\mathbf{t}_2$.

Example 3.7: Suppose that $\mathbf{P}^{\mathrm{SMC}}_{3\times 9}$ is the exponent matrix in Fig. 5 (a), and cycles $\mathcal{C}_{2k}$ ($k = 2,3,4$) are the potential cycles with the path depicted in Fig. 5 (a). Following the procedure described in the proof of Lemma 3.6, we can find at least two other isomorphic paths to the cycle $\mathcal{C}_{2k}$ named $a\mathcal{C}_{2k}$ (Fig. 5 (a1)) and $(1-a)\mathcal{C}_{2k}$ (Fig. 5 (a2)). To this end, we consider the transformations $\mathbf{t}_1(X) = RP_1(-(aX - R_3))$ and $\mathbf{t}_2(X) = RP_2(-((1-a)X - R_2))$ where parameter a, matrix RP_i ($i = 1,2$), and matrix R_i ($i = 2,3$) were introduced in the proof of Lemma 3.6. As it was explained in this lemma, $\mathbf{t}_1\left(\mathbf{P}^{\mathrm{SMC}}_{3\times 9}\right) = \mathbf{t}_2\left(\mathbf{P}^{\mathrm{SMC}}_{3\times 9}\right) = \mathbf{P}^{\mathrm{SMC}}_{3\times 9}$. However, the path of cycle $a\mathcal{C}_{2k}$ (resp., $(1-a)\mathcal{C}_{2k}$) in matrix $a\mathbf{P}^{\mathrm{SMC}}_{3\times 9}$ (resp., $(1-a)\mathbf{P}^{\mathrm{SMC}}_{3\times 9}$) is transformed to a path in matrix $\mathbf{P}^{\mathrm{SMC}}_{3\times 9}$ which is different from the path of cycle $\mathcal{C}_{2k}$ in this matrix.

Lemma 3.8: Suppose that $\mathbf{P}^{\mathrm{SMC}}_{4\times n}$ is an exponent matrix of form (2) with lifting degree N and $\vec{P}_1 = [0,1,a,a^2]^T$ is the second column of $\mathbf{P}^{\mathrm{SMC}}_{4\times n}$ where a is a non-identity element in multiplicative group $\mathbb{Z}^{\times}_N$ with property $a^3 = 1$. Thus

$$\#\mathcal{C}^{4,n}_{2k,a} \leq \frac{\#\mathcal{C}^{4,n}_{2k}}{3},$$

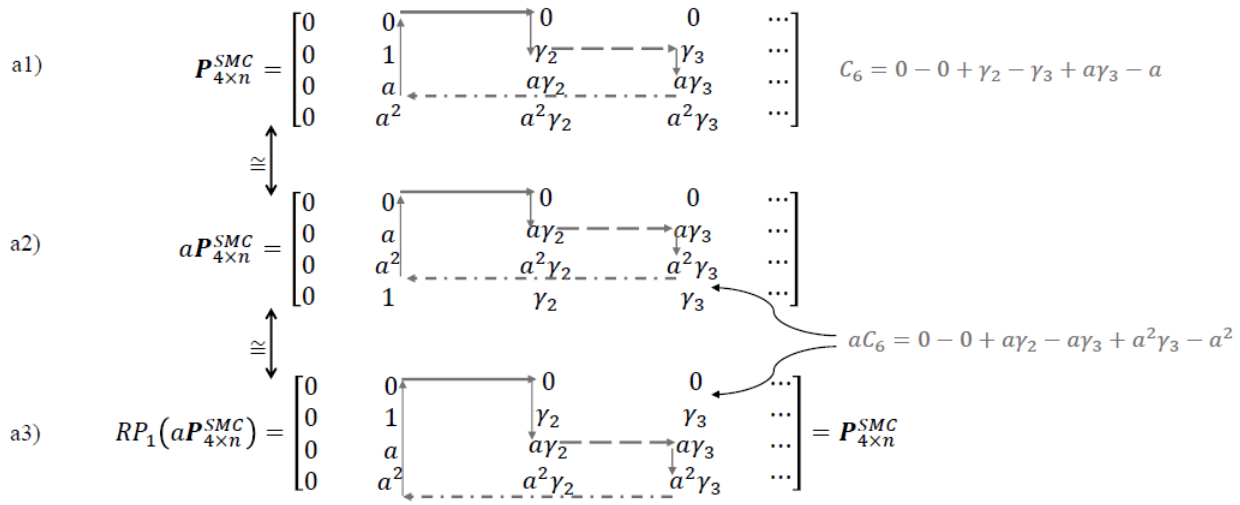

Fig. 6. Isomorphic forms of exponent matrix $\mathbf{P}_{4\times n}^{\mathrm{SMC}}$ under transformation $RP_1(aX)$: parts (a1) to (a3) clarify the stepwise impact of transformation $RP_1(aX)$ on both $\mathbf{P}_{4\times n}^{\mathrm{SMC}}$ and the sample path of a potential cycle $\mathcal{C}_6$.

where $\#\mathcal{C}_{2k,a}^{4,n}$ is the number of nonequivalent potential cycles of $\mathbf{P}_{4\times n}^{\mathrm{SMC}}$ of length $2k$ ($k = 2, 3, 4, 5$) and $\#\mathcal{C}_{2k}^{4,n}$ is introduced in Theorem 3.5 for the general case of an exponent matrix $\mathbf{P}_{4\times n}$ with four rows.

Proof: Before starting the proof, note that $\langle a \rangle$ is a cyclic subgroup of $\mathbb{Z}_N^{\times}$ of order 3 as a is not an identity element and $a^3 = 1$.

As pointed out in the proof of Lemma 3.6, we ought to show that for any potential cycle $\mathcal{C}_{2k}$: $\sum_{i=0}^{k-1}(p_{m_i n_i} - p_{m_i n_{i+1}})$ in matrix $\mathbf{P}_{4\times n}^{\mathrm{SMC}}$ below

$$\begin{bmatrix} 0 & 0 & 0 & \cdots & 0 \\ 0 & 1 & \gamma_2 & \cdots & \gamma_n \\ 0 & a & a\gamma_2 & \cdots & a\gamma_n \\ 0 & a^2 & a^2\gamma_2 & \cdots & a^2\gamma_n \end{bmatrix}, \tag{8}$$

there are at least two corresponding and ignorable cycles $a\mathcal{C}_{2k}$: $\sum_{i=0}^{k-1}\left(ap_{m_i n_i} - ap_{m_i n_{i+1}}\right)$ and $a^2\mathcal{C}_{2k}$: $\sum_{i=0}^{k-1}\left(a^2 p_{m_i n_i} - a^2 p_{m_i n_{i+1}}\right)$ in this matrix which have the same length as $\mathcal{C}_{2k}$ but are located in different positions (with partly different elements) of $\mathbf{P}_{4\times n}^{\mathrm{SMC}}$ compared with $\mathcal{C}_{2k}$. Similar to the proof of Lemma 3.6, we recall that since a (resp., a^2) is invertible, $\mathcal{C}_{2k}$ is an activated cycle if and only if $a\mathcal{C}_{2k}$ ($a^2\mathcal{C}_{2k}$) is activated. Thus, we consider $\mathcal{C}_{2k}$, $a\mathcal{C}_{2k}$, and $a^2\mathcal{C}_{2k}$ to be equivalent cycles even though this characteristic is not compatible with the Definition 3.2. Now let $N \in \mathbb{N}$, $a \in \mathbb{Z}_N^{\times}$ and $\mathbf{P}_1$ (resp., $\mathbf{P}_2$) be exponent matrix of code C_1 (resp., C_2) with lifting degree N. It is shown [18] that $\mathbf{P}_2$ (or the equivalent Tanner graph of C_2) is isomorphic to $\mathbf{P}_1$ (Tanner graph of

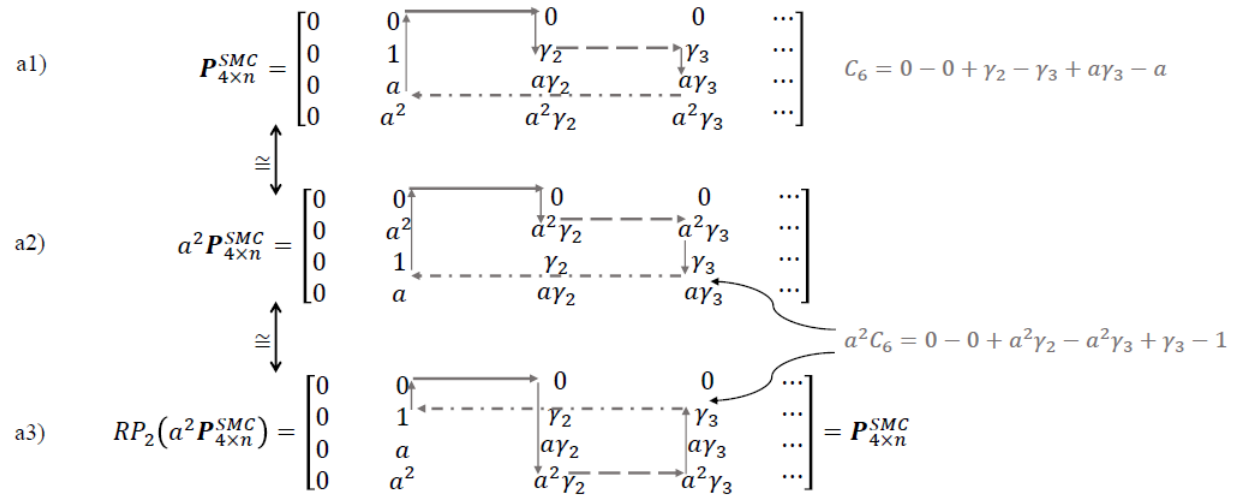

Fig. 7. Isomorphic forms of exponent matrix $\mathbf{P}_{4\times n}^{\mathrm{SMC}}$ under transformation $RP_2\left(a^2X\right)$: parts (a1) to (a3) clarify the stepwise impact of transformation $RP_2\left(a^2X\right)$ on both $\mathbf{P}_{4\times n}^{\mathrm{SMC}}$ and the sample path of a potential cycle $\mathcal{C}_6$

C_1) if it is constructed by row (column) permutation of $\mathbf{P}_1$ and/or by adding a constant to each row (column) of $\mathbf{P}_1$ and/or by multiplying a to $\mathbf{P}_1$. Given this fact $\mathbf{P}_{4\times n}^{\mathrm{SMC}} \cong a\mathbf{P}_{4\times n}^{\mathrm{SMC}} \cong a^2\mathbf{P}_{4\times n}^{\mathrm{SMC}}$. Moreover, consider the cycle-path $\mathcal{C}_{2k}$ $(k = 2, 3, 4, 5)$ in matrix $\mathbf{P}_{4\times n}^{\mathrm{SMC}}$ (see Fig. 6 (a1) or Fig. 7 (a1) for a sample cycle of length six). Additionally, consider the cycle-paths of $a\mathcal{C}_{2k}$ and $a^2\mathcal{C}_{2k}$ in $a\mathbf{P}_{4\times n}^{\mathrm{SMC}}$ and $a^2\mathbf{P}_{4\times n}^{\mathrm{SMC}}$ (see Fig. 6 (a2) or Fig. 7 (a2) for the cycle of length six), respectively. In the sequel, we attempt to illustrate the cycle-path $a\mathcal{C}_{2k}$ (resp., $a^2\mathcal{C}_{2k}$) in matrix $a\mathbf{P}_{4\times n}^{\mathrm{SMC}}$ (resp., $a^2\mathbf{P}_{4\times n}^{\mathrm{SMC}}$) has an isomorphic form in matrix $\mathbf{P}_{4\times n}^{\mathrm{SMC}}$.

Assume that matrices RP_1 and RP_2 are defined as follows:

$$RP_1 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix}, RP_2 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{bmatrix}, \tag{9}$$

where RP_i $(i = 1, 2)$ is a row permutation matrix to be applied on $\mathbf{P}_{4\times n}^{\mathrm{SMC}}$. So matrix $RP_1\left(a\mathbf{P}_{4\times n}^{\mathrm{SMC}}\right)$, which is constructed by applying row permutation matrix RP_1 on $a\mathbf{P}_{4\times n}^{\mathrm{SMC}}$ (see Fig. 6 parts (a2) to (a3)), has a form exactly like matrix $\mathbf{P}_{4\times n}^{\mathrm{SMC}}$. Furthermore, the cycle $a\mathcal{C}_{2k}$ has a new path in the resulting matrix, and at the same time it is isomorphic to the cycle in matrix $a\mathbf{P}_{4\times n}^{\mathrm{SMC}}$ (Fig.6 part (a2)). Similarly, matrix $RP_2\left(a^2\mathbf{P}_{4\times n}^{\mathrm{SMC}}\right)$) is constructed by applying row permutation matrix RP_2 on $a^2\mathbf{P}_{4\times n}^{\mathrm{SMC}}$ (see Fig. 7 parts (a2) to (a3)), and it has a form exactly like matrix $\mathbf{P}_{4\times n}^{\mathrm{SMC}}$, too. Also, the cycle $a^2\mathcal{C}_{2k}$ has a new path in the resulting matrix, and at the same time it is isomorphic to

the cycle in matrix $a^2\mathbf{P}^{\mathrm{SMC}}_{4\times n}$ (Fig.7 part (a2)). Permutation matrices RP_1 and RP_2 will entirely permute the rows of matrices except the first row, which is intact. Since these permutations are different from each other, the new path of cycle $a\mathcal{C}_{2k}$ (resp., $a^2\mathcal{C}_{2k}$) in the resulting matrix (i.e., matrix in part (a3)) would be different from the path of cycle $\mathcal{C}_{2k}$ (in matrix part (a1)) and different from $a^2\mathcal{C}_{2k}$ (resp., $a\mathcal{C}_{2k}$). To summarize, for an arbitrary potential cycle $\mathcal{C}_{2k}$ there are two other different potential cycles $a\mathcal{C}_{2k}$ and $a^2\mathcal{C}_{2k}$ with the same length as $\mathcal{C}_{2k}$, and the verification algorithm needs to check only one of them. Since $a\mathcal{C}_{2k}$ and $a^2\mathcal{C}_{2k}$ have cycle-paths in $\mathbf{P}^{\mathrm{SMC}}_{4\times n}$ different from $\mathcal{C}_{2k}$, $\#\mathcal{C}^{4,n}_{2k,a} \leq \frac{\#\mathcal{C}^{4,n}_{2k}}{3}$. □

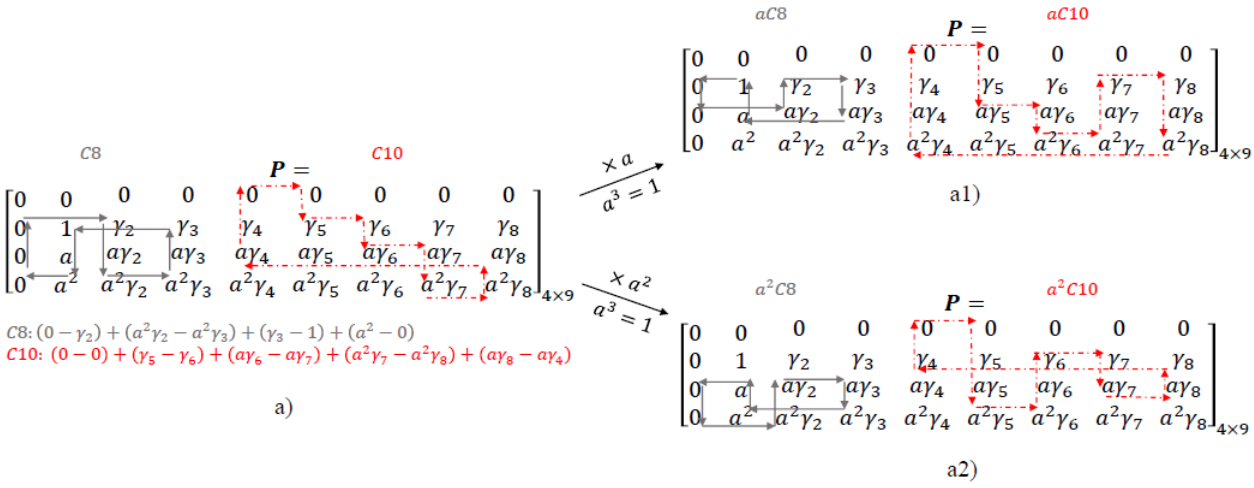

Fig. 8. Samples of isomorphic paths of cycles with different length in $\mathbf{P}^{\mathrm{SMC}}_{4\times 9}$: a) primary underlined paths for cycles $\mathcal{C}_8$ and $\mathcal{C}_{10}$. a1) isomorphic paths for the considered primary paths in part (a) derived from transformation $\mathbf{t}_1$. a2) isomorphic paths for the considered primary paths in part (a) derived from transformation $\mathbf{t}_2$.

Example 3.9: Suppose that $\mathbf{P}^{\mathrm{SMC}}_{4\times 9}$ is the exponent matrix in Fig. 8 (a), and cycles $\mathcal{C}_{2k}$ $(k = 4, 5)$ are the potential cycles with the path depicted in Fig. 8 (a). Following the procedure described in the proof of Lemma 3.8, we can find at least two other isomorphic paths to the cycle $\mathcal{C}_{2k}$ named $a\mathcal{C}_{2k}$ (Fig. 8 (a1)) and $a^2\mathcal{C}_{2k}$ (Fig. 8 (a2)). To this end, we consider the transformations $\mathbf{t}_1(X) = RP_1(aX)$ and $\mathbf{t}_2(X) = RP_2(a^2X)$ where parameter a and matrix RP_i $(i = 1, 2)$ were introduced in the proof of Lemma 3.8. As was explained in this lemma, $\mathbf{t}_1\left(\mathbf{P}^{\mathrm{SMC}}_{4\times 9}\right) = \mathbf{t}_2\left(\mathbf{P}^{\mathrm{SMC}}_{4\times 9}\right) = \mathbf{P}^{\mathrm{SMC}}_{4\times 9}$. However, path of cycle $a\mathcal{C}_{2k}$ (resp., $a^2\mathcal{C}_{2k}$) in matrix $a\mathbf{P}^{\mathrm{SMC}}_{4\times 9}$ (resp., $a^2\mathbf{P}^{\mathrm{SMC}}_{4\times 9}$) is transformed to a path in matrix $\mathbf{P}^{\mathrm{SMC}}_{4\times 9}$, which is different from the path of cycle $\mathcal{C}_{2k}$ in this matrix.

Note that we have tried to intuitively reason lemmas 3.6 and 3.8 to make them easier to

understand. However, an algebraic proof method to these lemmas is presented in Appendix A. In addition, a general formulation of these lemmas is presented in the following theorem.

Theorem 3.10: Suppose that $\mathbf{P}^{\mathrm{SMC}}_{m\times n}$ is an exponent matrix of form (2) with lifting degree N and $\left[0,1,a,a^2,\cdots a^{m-2}\right]^T$ is the second column of $\mathbf{P}^{\mathrm{SMC}}_{m\times n}$ $(m,n\geq 3)$ where a is a non-identity element in multiplicative group $\mathbb{Z}_N^{\times}$ with property $a*(1-a)=1$ (resp., $O(a)=m-1$) when $m=3$ (resp., $m\geq 4$). Thus

$$\#\mathcal{C}^{m,n}_{2k,a}\leq \frac{\#\mathcal{C}^{m,n}_{2k}}{3} \ \text{(resp., } \#\mathcal{C}^{m,n}_{2k,a}\leq \frac{\#\mathcal{C}^{m,n}_{2k}}{m-1}\text{)}$$

where $m=3$ (resp., $m\geq 4$), $\#\mathcal{C}^{m,n}_{2k,a}$ is the number of nonequivalent potential cycles of $\mathbf{P}^{\mathrm{SMC}}_{m\times n}$ of length $2k$ $(k=2,3,4,5)$ and $\#\mathcal{C}^{m,n}_{2k}$ is from Theorem 3.5 for the general case of an exponent matrix $\mathbf{P}_{m\times n}$ with m rows.

Proof: For the cases $m=3$ and $m=4$ we refer them to the lemmas 3.6 and 3.8, respectively. For the case $m\geq 5$ the argument is exactly the same as the case $m=4$. This means that tailored to the order of non-identity element $a\in\mathbb{Z}_N^{\times}$ and any potential cycle $\mathcal{C}_{2k}\in\mathcal{C}^{m,n}_{2k}$ $(k=2,3,4,5)$, it must be shown that there are $m-2$ other isomorphically equivalent cycles $a^i\mathcal{C}_{2k}$ $(i=1,\cdots,m-2)$ that all have the same length as the cycle $\mathcal{C}_{2k}$ but with different paths in matrix $\mathbf{P}^{\mathrm{SMC}}_{m\times n}$ of form (2) that has $\left[0,1,a,a^2,\cdots a^{m-2}\right]^T$ as its second column. To show this fact, we consider below a row permutation matrix of size m

$$RP_i=\left(\begin{bmatrix} 1 & 0 & 0 & 0 & \cdots & 0 & 0\\ 0 & 0 & 0 & 0 & \cdots & 0 & 1\\ 0 & 1 & 0 & 0 & \cdots & 0 & 0\\ 0 & 0 & 1 & 0 & \cdots & 0 & 0\\ 0 & 0 & 0 & 1 & \cdots & 0 & 0\\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \\ 0 & 0 & 0 & 0 & \cdots & 1 & 0 \end{bmatrix}_{m\times m}\right)^i,\quad i=1,2,\cdots,m-2 \tag{10}$$

and apply it on the left side of matrix $a^i\mathbf{P}^{\mathrm{SMC}}_{m\times n}$. Following the steps of the presented argument in Lemma 3.8, this action will translate the potential cycle $\mathcal{C}_{2k}$ to $m-2$ other isomorphic cycles $a^i\mathcal{C}_{2k}$ that all have the same size as $\mathcal{C}_{2k}$ but with completely different paths in $\mathbf{P}^{\mathrm{SMC}}_{m\times n}$. □

Here it should be noted that using the constraint $a(1-a)=1$ for the case $m=3$ is more efficient than using $a^2=1$. This is because the former constraint will reduce the equivalent cycles by a factor of 3 while the later constraint will reduce it by a factor of 2.

C. IRS technique as an A priori step of greedy search algorithm

In Theorem 3.10 it was shown that by tailoring to the column degree $d_v = m$ of exponent matrix $\mathbf{P}^{\mathrm{SMC}}_{m\times n}$, there might exist a proper cyclic subgroup $\langle a\rangle$ of multiplicative group $\mathbb{Z}_N^{\times}$ from which we can pick non-zero components of $\vec{P}_1$. Specifically, this theorem asserts that $\vec{P}_1 = [0, 1, a, a^2, \cdots a^{m-2}]^T$. The essence of Theorem 3.10 is determining $\vec{P}_1$ a priori in a way that 1) the number of nonequivalent potential cycles is reduced by a certain factor and 2) the greedy search algorithm does not need to search components of $\vec{P}_1$ anymore. Then, after determining a suitable $\vec{P}_1$ that meets the condition of Theorem 3.10, the search algorithm will take the sub-matrix $\left[\vec{0} \;\middle|\; \vec{P}_1\right]$ as a base and try to find proper values of γ_js in order for $\mathbf{P}^{\mathrm{SMC}}_{m\times n}$ to meet the girth condition. Nevertheless, it has to be noted that Theorem 3.10 does not guarantee that sub-matrix $\left[\vec{0} \;\middle|\; \vec{P}_1\right]$ meets the girth condition itself. So given the desired girth $g = 2k$ ($k = 5, 6$), the questions are "does every candidate $\vec{P}_1$ result in a sub-matrix $\left[\vec{0} \;\middle|\; \vec{P}_1\right]$ with desired girth g? If not, what is the portion of $\mathbb{Z}_N^{\times}$s (accordingly, what is the portion of Ns) holding at least one cyclic subgroup $\langle a\rangle$ that meets the condition of Theorem 3.10, and at the same time $\left[\vec{0} \;\middle|\; \vec{P}_1\right]$ meets the girth condition?" To answer the first question, we provide a proposition for the case $d_v = 3$ and a counterexample for the case $d_v \geq 4$. To address the second question, some statistics are provided.

Proposition 3.11: Suppose that $N \in \mathbb{N}$, $N \geq 7$ and $\vec{P}_1 = [0, 1, a]^T$ where, a is a non-identity element of multiplicative group $\mathbb{Z}_N^{\times}$ with property $a * (1 - a) = 1$. Then, QC-LDPC code with exponent matrix $\left[\vec{0} \;\middle|\; \vec{P}_1\right]$ has girth equal to 12.

Proof: Based on Theorem 3.5, we recognize that $\left[\vec{0} \;\middle|\; \vec{P}_1\right]$ has no potential cycle of length 6 and 10, as it has only two columns. Furthermore, based on the results of Lemma 3.6, the number of nonequivalent potential cycles of length 4 (resp., 8) that we need to check is $\#\mathcal{C}^{3,2}_{4,a} = 1$ (resp., $\#\mathcal{C}^{3,2}_{8,a} = 2$). The paths of nonequivalent potential cycles of length 4 and 8, which are involved in the first two columns of exponent matrix $\mathbf{P}$ are depicted in parts (b), (e), and (f) of Fig. 2, respectively. Given that $p_{00} = p_{10} = p_{20} = p_{01} = 0$, $p_{11} = 1$, and $p_{21} = a$, we have:

cycle $\mathcal{C}_4$ in part (b) : $p_{00} - p_{01} + p_{11} - p_{10} = 1 \neq 0 \mod N$,

cycle $\mathcal{C}_8$ in part (e) : $2\,(p_{00} - p_{01} + p_{11} - p_{10}) = 2 \neq 0 \mod N$,

cycle $\mathcal{C}_8$ in part (f) : $p_{00} - p_{01} + p_{11} - p_{10} + p_{20} - p_{21} + p_{11} - p_{10} = 2 - a \neq 0 \mod N$.

Note that since $a * (1 - a) = a - a^2 = 1$, $a^2 = a - 1$. Considering that GCD $(a, N) = 1$, if $2 - a = 0 \mod N$, then $2a = a^2 \mod N$. Thus, $2a = a - 1 \mod N$. This means that $a = -1$

$\mod N$. But there is a contradiction as $a = -1 \mod N$ and at the same time $a = 2 \mod N$. □

In the following we bring a counterexample that shows every a value that meets the condition $a^{d_v-1} = 1$ ($d_v \geq 4$) would not necessarily be a proper candidate for constructing the sub-matrix $\left[\vec{0} \;\middle|\; \vec{P}_1\right]$ with girth 12.

Example 3.12: Let $N_1 = 41$, $N_2 = 239$, $N_3 = 639$, $N_4 = 1443$, and correspondingly consider multiplicative groups $\mathbb{Z}_{N_i}^{\times}$ ($i = 1, 2, 3, 4$) where $|\mathbb{Z}_{N_1}^{\times}| = 40$, $|\mathbb{Z}_{N_2}^{\times}| = 238$, $|\mathbb{Z}_{N_3}^{\times}| = 420$, and $|\mathbb{Z}_{N_4}^{\times}| = 864$. Conventionally suppose that an element $a \in \mathbb{Z}_N^{\times}$ has property $\mathfrak{I}$ when $a*(1-a) = 1$, has property $\mathfrak{II}$ when $O(a) = 3$, and has property $\mathfrak{III}$ when $O(a) = 4$. So none of the elements of $\mathbb{Z}_{N_1}^{\times}$ holds properties $\mathfrak{I}$ and $\mathfrak{II}$, while there are two elements $a = 9, 32$ in this group that meet the property $\mathfrak{III}$. Nevertheless, neither $a = 9$ nor $a = 32$ are proper candidates for constructing vector $\vec{P}_1 = [0, 1, a, a^2, a^3]^T$ as they will result in matrix $\left[\vec{0} \;\middle|\; \vec{P}_1\right]$ with girth less than or equal to 8. For the value N_2, none of the elements of $\mathbb{Z}_{N_2}^{\times}$ holds properties $\mathfrak{I}$ to $\mathfrak{III}$. For $\mathbb{Z}_{N_3}^{\times}$, there is no element with property $\mathfrak{I}$ and $\mathfrak{III}$, but only two elements $a = 214, 427$ hold the property $\mathfrak{II}$. However, neither $a = 214$ nor $a = 427$ are proper candidates for constructing vector $\vec{P}_1 = [0, 1, a, a^2]^T$ as they will result in matrix $\left[\vec{0} \;\middle|\; \vec{P}_1\right]$ with girth less than or equal to 8. Eventually, $\mathbb{Z}_{N_4}^{\times}$ possesses four elements $a = 101, 212, 1232, 1343$ that have property $\mathfrak{I}$ and all of them are suitable choices for constructing $\vec{P}_1 = [0, 1, a]$. This is because, based on proposition 3.11, $\vec{P}_1 = [0, 1, a]$ with property $\mathfrak{I}$ always constitutes a two-column matrix with girth 12. Moreover, $\mathbb{Z}_{N_4}^{\times}$ has 8 elements $a = 100, 211, 334, 445, 898, 1210, 1231, 1342$ with property $\mathfrak{II}$, and all of them are suitable candidates for constructing $\vec{P}_1$. Also, there are 24 elements in $\mathbb{Z}_{N_4}^{\times}$ that have property $\mathfrak{III}$, and among them, 16 are good candidate for constructing $\vec{P}_1$, which are $a = 73, 142, 376, 512, 554, 593, 623, 746, 850, 857, 1067, 1178, 1301, 1331, 1370, 1412$.

TABLE II

RATIO OF PERMISSIBLE VALUES OF N BELONG TO THE SET $\{37, 38, \cdots, 7400\}$ AND THE AVERAGE NUMBER $\bar{a}$ OF PERMISSIBLE a'S PER PERMISSIBLE $\mathbb{Z}_N^{\times}$. PERMISSIBLE a IN $\mathbb{Z}_N^{\times}$ IS THE VALUE FOR WHICH $\left[\vec{0}|\vec{P}_1\right]$ HAS GIRTH GREATER THAN 8.

–	$a(1-a) = 1$	$a^3 = 1$	$a^4 = 1$	$a^5 = 1$
Ratio of permissible N's	13%	60%	51%	24%
$\bar{a}$'s per permissible N	2.72	3.63	8.46	5.75

Although Example 3.12 highlights there probably is not a general and explicit way for finding

cyclic subgroups that are suitable for launching a greedy search algorithm, there still is a reliable trend to ensure that suitable candidates of cyclic subgroups are available even with a large size. To address this issue we bring some statistics in Table II and Fig. 9. The first row of Table II indicates the property of each cyclic subgroup. The second row of this table contains the proportion (or ratio) of those integer number Ns, which for that $\mathbb{Z}_N^{\times}$ possesses at least one suitable cyclic subgroup of indicated order. The variation range of N is between 37 and 7400, which is high enough for our investigation and inference. As can be seen in Table II this ratio is always greater than 10%. The third row of Table II accommodates the average number of suitable candidates of value a that exist in each suitable multiplicative group $\mathbb{Z}_N^{\times}$. For instance, if the ultimate goal is using SMC technique for constructing a fully-connected QC-LDPC code with $d_v = 4$ and girth at least 10, one can consider a fixed $N \in \mathbb{N}$ as a lifting degree and hope that they have a 60% chance (for this specific N) to find a proper cyclic subgroup of order 3 to make $\vec{P}_1$. In addition, for each N, $\mathbb{Z}_N^{\times}$ possesses more than three a values (on average) that we can make use to form vector $\vec{P}_1 = [0, 1, a, a^2]^T$. Fig. 9 helps us to have a conception of piecewise trends of existence cyclic subgroups while N is gradually increased. This figure consists of four parts; each one displays a screenshot of size 10 of a 3-dimensional histogram. These small histograms show the multiplicities of suitable a values (as $\mathbf{z}$ axis) of $\mathbb{Z}_N^{\times}$ considering N (as $\mathbf{x}$ axis). The notable thing is these screenshots are selected from different parts of the general histogram. The results of this figure ensure that we have a chance to find a suitable cyclic subgroup of $\mathbb{Z}_N^{\times}$ even when N belongs to the small intervals who are picked from different parts of the integer ring[4].

Before concluding this part, there are three important relevant facts. First, Lagrange's theorem 2.16 is a primary criterion to verify if $\mathbb{Z}_N^{\times}$ has at least one cyclic subgroup of our desired order or not. However, this theorem proposes a necessary but not sufficient condition. For example, $|\mathbb{Z}_{240}^{\times}| = \varphi(240) = 64$ and $\text{GCD}(8, 64) = 8$, but $\mathbb{Z}_{240}^{\times}$ has no element of order greater than 4. So it is impossible to construct $\vec{P}_1 = [0, 1, a, \cdots, a^{m-1}]^T$ when $N = 240$ and $m = 8$.

[4]The authors seize this opportunity to highlight another capability of IRS method which is beyond the scope of this paper but could be considered as future work. Indeed, if N is a prime number and non-zero components of $\vec{P}_1$ constitute a cyclic subgroup of $\mathbb{Z}_N^{\times}$, then the set of non-zero elements of $\vec{P}_j$ ($j = 2, \cdots, n-1$) is a *co-set* of this subgroup. In other words, exponent matrix $\mathbf{P}_{m\times n}^{\text{SMC}}$ is made of a specific cyclic subgroup of multiplicative group $\mathbb{Z}_N^{\times}$ and some of its co-sets. Investigation of the relation between these co-sets and the girth of SMC constructing based QC-LDPC codes could be considered as future studies.

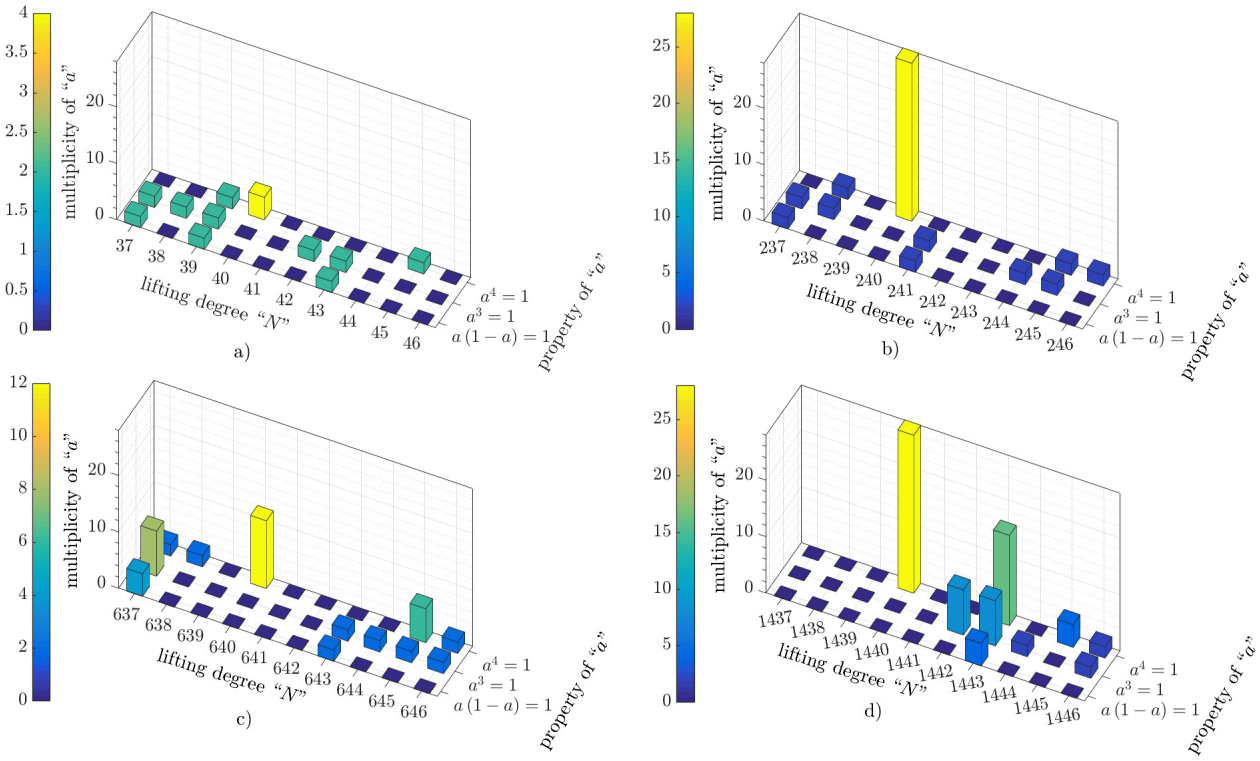

Fig. 9. 3-Dimensional histograms that pick **z** axis to show the abundance of "a" values with properties "$a(1-a) = 1$", "$a^3 = 1$" and "$a^4 = 1$" which are in $\mathbb{Z}_N^{\times}$, where, $N \in \{i+37, i+38, \cdots, i+46\}(i = 0, 200, 600, 1400)$: a) screenshot of size 10 when $i = 0$. b) screenshot of size 10 when $i = 200$. c) screenshot of size 10 when $i = 600$. d) screenshot of size 10 when $i = 1400$.

Second, checking for the existence of a proper N and, accordingly, the existence of a suitable cyclic subgroup that results in $\vec{P}_1$ is not time-consuming. Given a fixed m, it will take few milliseconds for MATLAB software to check if $\mathbb{Z}_N^{\times}$ is a proper candidate or not. Third, the following proposition, "the search algorithm will need to investigate only one permissible a per each permissible cyclic subgroup of $\mathbb{Z}_N^{\times}$ that meets the girth condition." In other words, if there is more than one generator for permissible cyclic subgroup S ($S \leq \mathbb{Z}_N^{\times}$), then it is sufficient to check only one of them.

Proposition 3.13: Let $N \geq 6$, a, b be two different elements of $\mathbb{Z}_N^{\times}$ which satisfy the constraint in Theorem 3.10 and $\langle a \rangle = \langle b \rangle = S$. The Tanner graph of constructed matrix $\mathbf{P}_{m\times n}^{\mathrm{SMC}}$ with second column $[0, 1, a, \cdots, a^{m-2}]^T$ has the same girth as the Tanner graph of matrix $\mathbf{P}_{m\times n}^{\mathrm{SMC}}$ with second column $[0, 1, b, \cdots, b^{m-2}]^T$.

Proof: It is shown [18] that if $d \in \mathbb{Z}_N^{\times}$ then the Tanner graph of code with exponent matrix

$\mathbf{P}$ is isomorphic to the Tanner graph of code with exponent matrix $d\mathbf{P}$. Since a and b are in $\mathbb{Z}_N^{\times}$ so both of them are invertible and $\text{GCD}\,(a, N) = \text{GCD}\,(b, N) = 1$. Given this fact we consider two cases:

Case I ($d_v = m = 3$): In this case, a and b have the property $a\,(1-a) = 1 = b\,(1-b)$ and based on Lemma 3.6, $O\,(\langle a\rangle) = O\,(\langle b\rangle) = 6$. Since a necessary and sufficient condition for non-identity element $z = x^y$ ($\langle x\rangle = S,\ y \in \mathbb{N}$) to be a generator of S is $\text{GCD}\,(y, O(S)) = 1$, it is easy to see that a and $b = a^5$ are the only generators of S. If $\mathbf{P}_{3\times n}^{\text{SMC}}$ has $[0, 1, a]^T$ as its second column, then $a^5\mathbf{P}_{3\times n}^{\text{SMC}}$ preserves SMC property, and it has $[0, a^5, 1]^T$ as its second column. Swapping the second and the third rows of $a^5\mathbf{P}_{3\times n}^{\text{SMC}}$ also does not affect the girth but gives $[0, 1, a^5]^T = [0, 1, b]^T$ as the second column.

Case II ($d_v = m \geq 4$): In this case a and b have the property $a^{m-1} = 1 = b^{m-1}$ and $O(S) = m - 1$. So, as in case I, b has a form like $b = a^y$ where $y \in \mathbb{N}$ ($1 \leq y \leq m - 2$) and $\text{GCD}\,(y, m-1) = 1$. If $\mathbf{P}_{m\times n}^{\text{SMC}}$ has $[0, 1, a, \cdots, a^{m-1-y}, a^{m-1-y+1}, \cdots, a^{m-2}]^T$ as its second column, then $a^y\mathbf{P}_{m\times n}^{\text{SMC}}$ has $[0, a^y, a^{y+1}, \cdots, 1, a, \cdots, a^{y-1}]^T$ as its second column while preserving the SMC constraint. Permuting the rows of $a^y\mathbf{P}_{m\times n}^{\text{SMC}}$ does not affect the girth but gives $\left[0, 1, a^y, a^{2y}, \cdots, a^{(m-2)y}\right]^T = [0, 1, b, b^2, \cdots, b^{m-2}]^T$ as the second column of $a^y\mathbf{P}_{m\times n}^{\text{SMC}}$. □

In Summary, the search algorithm will test one permissible generator per each permissible cyclic subgroup S to find exponent matrix $\mathbf{P}_{m\times n}^{\text{SMC}}$ of code with girth g ($g = 10, 12$). The final point is there might be more than one permissible cyclic subgroup of $\mathbb{Z}_N^{\times}$ that meet the conditions in Theorem 3.10; however, not all of them would necessarily result in matrix $\mathbf{P}_{m\times n}^{\text{SMC}}$ with girth g ($g = 10, 12$) for the given N. For example $\mathbb{Z}_{301}^{\times}$ has two distinct permissible cyclic subgroups $S_1 = \langle 80\rangle$ and $S_2 = \langle 136\rangle$ of order 6 where their generators satisfy the property $a\,(1-a) = 1$ as well as the girth conditions. We will see in Section IV that search algorithm is able to find exponent matrix $\mathbf{P}_{3\times 10}^{\text{SMC}}$ with second column $[0, 1, 80]^T$ for code with girth 10 while it is impossible to find girth 10 code with exponent matrix $\mathbf{P}_{3\times 10}^{\text{SMC}}$ and second column $[0, 1, 136]^T$.

D. Controlled greedy search algorithm

In this section, we present a new controlled greedy search algorithm that uses the SMC technique [26]. In the proposed algorithm, the complexity of the "verification" phase is considerably reduced thanks to the considered IRS technique. Moreover, the behavior of the "assigning" phase is optimized and controlled based on the available information at each step. In the following, the proposed version of this algorithm along with a complementary explanation are presented.

Algorithm 1 Controlled greedy search algorithm for $m \geq 3$

Input: Parameters n, m, N of the code, targeted girth g, vector G of size n to control the greedy search effort.

Output: Eventually, set of coefficients Γ_n of size n if success, empty set otherwise.

- - - - - - - - - - - - - - - - - - - primary step - - - - - - - - - - - - - - - - - - -

$\mathcal{A} = \{2, 3, \ldots, N-1\}$, $\Gamma_n = \varnothing$, $\Gamma_1 = \{0\}$
while $\mathcal{A} \neq \varnothing$ and $\Gamma_n = \varnothing$ **do**
    Extract an element a of $\mathcal{A}$.
    $\mathcal{A} = \mathcal{A} \setminus \{a\}$
    if $O(a) = m - 1$ **then**
        Set $\vec{P}_1 = (0, 1, a, a^2, \ldots, a^{m-2})^T$
        $\mathcal{A} = \mathcal{A} \setminus \{a^k\}_{k=2,\ldots,m-2}$
        $\mathcal{S} = \Phi_g(\Gamma_1, \vec{P}_1, N)$
        $\Gamma_n =$ **search** $(\Gamma_1, \mathcal{S}, N, n, \vec{P}_1, G)$

- - - - - - - - - - - - - - - - - - - **search** function - - - - - - - - - - - - - - - - - - -

$\Gamma_n =$ **search** $(\Gamma, \mathcal{S}, N, n, \vec{P}_1, G)$
$\Gamma_n = \Gamma$
if $|\Gamma_n| = n$ **then** Return Γ_n
else
    for $i = 1$ to $|\mathcal{S}|$ **do**
        $s(i) = |\mathcal{S} \cap \Phi_g(\Gamma \cup \mathcal{S}(i), \vec{P}_1, N)|$ (note: s is a vector).
    $I =$ **sort _index** (s) (note: $s(I(1)) \geq s(I(2)) \geq \ldots \geq s(I(|\mathcal{S}|))$).
    for $j = 1$ to **min** $(|\mathcal{S}|, G(|\Gamma|))$ **do**
        if $|\Gamma_n| = n$ **then** Return Γ_n
        else
            $\Gamma_k = \Gamma \cup \{\mathcal{S}(I(j))\}$
            $\mathcal{S} = \mathcal{S} \setminus \{\mathcal{S}(I(j))\}$
            $\mathcal{S}_k = \mathcal{S} \cap \Phi_g(\Gamma_k, \vec{P}_1, N)$
            if $|\Gamma_k| + |\mathcal{S}_k| \geq n$ **then**
                $\Gamma_n =$ **search** $(\Gamma_k, \mathcal{S}_k, N, n, \vec{P}_1, G)$
            else
                Return $\varnothing$

Let $\Gamma_k = \{0, 1, \gamma_2, \ldots, \gamma_{k-1}\}$ be a set of size k of elements of $\mathbb{Z}_N^\times$. The property $\rho_g(\Gamma_k, \vec{P}_1, N)$ is true if and only if the exponent matrix $\left[\ \vec{0}\ \middle|\ \vec{P}_1\ \middle|\ \gamma_2 \otimes \vec{P}_1\ \middle|\ \ldots\ \middle|\ \gamma_{k-1} \otimes \vec{P}_1\ \right]$ gives a matrix with a girth greater than or equal to g when expanded by a factor of N. We call $\Phi_g(\Gamma_k, \vec{P}_1, N)$ the ordered set of coefficients of $\mathbb{Z}_N$ so that a vector Γ_{k+1} of size $k+1$ constructed by the concatenation of Γ_k and any coefficient of $\Phi_g(\Gamma_k, \vec{P}_1, N)$ also gives an exponent matrix of girth g. In a more formal way

$$\beta \in \Phi_g(\Gamma_k, \vec{P}_1, N) \iff \rho_g(\Gamma_k \cup \{\beta\}, \vec{P}_1, N) \text{ is true.} \tag{11}$$

The search of a solution of degree (m, n) for a given expansion factor N is done in two steps. The first step consists of the enumeration of a single element per class of the a values verifying the condition of Theorem 3.10. This step is described in Algorithm 1 part 1 for $m > 3$. To do so, the set of values $\mathcal{A}$ is initialized as $\mathcal{A} = \{2, 3, \ldots, N-1\}$. The values of $\mathcal{A}$ are extracted one by one. Each time an extracted value a fulfills the condition of theorem 3.10, the function **search** is launched to try to find a solution Γ_n. In case of success, the algorithm is successful and stops. Otherwise, the elements of $\langle a \rangle$ are suppressed from the search space $\mathcal{A}$. The process continues until no more values remain in $\mathcal{A}$. In this case, the search is unsuccessful. Note that for $m = 3$, the condition $O(a) = m - 1$ of line 5 should be replaced by the condition $a(1-a) = 1 \mod N$, and line 7 should be replaced by the instruction $\mathcal{A} = \mathcal{A} \setminus \{a^k\}_{k=2,\ldots,5}$.

The **search** function is described in Algorithm 1, part 2. It is a recursive function that tries to increase recursively the size of Γ until it reaches a size of n. The arguments of the **search** function are Γ, $\mathcal{S}$, N, n, $\vec{P}_1$, and a vector G of size n that controls the processing effort. Let us describe the processing during the first call of the function in line 9. The arguments of this first call are $\Gamma_1 = \{0\}$ and $\mathcal{S}$ (defined in line 8), the set of values compatible with Γ_1 (see (11)). Lines 14 and 15 set up the greedy search. For $i = 1, \ldots, |\mathcal{S}|$, the number $s(i)$ of triplets $\Gamma_3 = \{0, \mathcal{S}(i), \mu\}$, $\mu \in \mathcal{S}$ verifying the condition $\rho(\Gamma_3, \vec{P}_1, N)$ is computed (note that $s(i) < |\mathcal{S}|$). The $s(i)$ are thus sorted in decreasing order (line 16), and the first $G(|\Gamma|) = G(1)$ elements of $\mathcal{S}$ (line 17) associated to the highest values of vector s are tested. For each tested value, a vector Γ_k of size 2 is generated (line 18). The tested value is suppressed from the set $\mathcal{S}$ (line 19), and then the subset $\mathcal{S}_k$ of $\mathcal{S}$ of values compatible with Γ_k is created (line 20). If the size of $\mathcal{S}_k$ plus the size of Γ_k is greater than or equal to n, or, if there is still the possibility to generate a Γ vector of length n, then the search function is called again with a Γ set of size 2. The process is recursively reiterated until a length n Γ vector is found or until no more possibility remains to

be explored. The complexity of the search is controlled by a vector G of size n. The k^{th} value $G(k)$ of G indicates that only the most "promising" $G(k)$ branches will be explored inside each depth k recursive call of the search function. Note that when all the values of G are equal to N the search algorithm is exhaustive. It can be done in a limited time (less than a few days) only for low values of n. For large n, the first values of G are set to 1 or 2 for reducing the search space to a reasonable size. Note that $|X|$ represents the cardinal of the set X.

TABLE III

COMPARISON OF THE COMPLEXITIES: EXHAUSTIVE SEARCH VERSUS NEW PROPOSED SEARCH METHOD ($\bar{m} = \min\{k, m\}$ AND $\bar{n} = \min\{k, n\}$)

–	"verification" search space		"assigning" search space		overall complexity	
–	SMC & IRS	exhaustive	SMC & IRS	exhaustive	SMC & IRS	exhaustive
$m = 3$	$\frac{\sum_{i=2}^{\bar{m}} \sum_{j=2}^{\bar{n}} t_{ij}^{\mathcal{C}_{2k}} \binom{3}{i}\binom{n}{j}}{3}$	$\sum_{i=2}^{\bar{m}} \sum_{j=2}^{\bar{n}} t_{ij}^{\mathcal{C}_{2k}} \binom{3}{i}\binom{n}{j}$	$(N-3)^{n-2}$	$(N-1)^{2(n-1)}$	$\mathcal{O}\left((N-3)^{(n-2)}\right)$	$\mathcal{O}\left((N-1)^{2(n-1)}\right)$
$m \geq 4$	$\frac{\sum_{i=2}^{\bar{m}} \sum_{j=2}^{\bar{n}} t_{ij}^{\mathcal{C}_{2k}} \binom{m}{i}\binom{n}{j}}{m-1}$	$\sum_{i=2}^{\bar{m}} \sum_{j=2}^{\bar{n}} t_{ij}^{\mathcal{C}_{2k}} \binom{m}{i}\binom{n}{j}$	$(N-m)^{n-2}$	$(N-1)^{(m-1)(n-1)}$	$\mathcal{O}\left((N-m)^{(n-2)}\right)$	$\mathcal{O}\left((N-1)^{(m-1)(n-1)}\right)$

At the end of this discussion, we compare the complexity of our proposed search method that uses IRS technique with an exhaustive search in terms of: 1) mitigating the verification phase by reducing nonequivalent potential cycles and 2) mitigating the assigning phase by reducing the number of undetermined components of exponent matrix $\mathbf{P}$. These two types of simplification are logically accurate even for $g = 10$ or 12. Table III summarizes these results. The first column of this table shows the column degree $d_v = m$ of our constructed QC-LDPC codes. Without loss of generality we assume $n >> m$ due to the fact that studying the complexity of our search method would be important when the rate of the codes is high. In other words, if one intends to find fully-connected QC-LDPC code of different rates, the dominant variable is row weight $d_c = n$. The second column of the table presents the necessary search space for the verification phase. As was shown in Theorems 3.5 and 3.10, this space is equal to $\sum_{i=2}^{\min\{k,m\}} \sum_{j=2}^{\min\{k,n\}} t_{ij}^{\mathcal{C}_{2k}} \binom{m}{i}\binom{n}{j}$ and $\left(\sum_{i=2}^{\min\{k,m\}} \sum_{j=2}^{\min\{k,n\}} t_{ij}^{\mathcal{C}_{2k}} \binom{m}{i}\binom{n}{j}\right)/(m-1)$ respectively for an exhaustive search and our IRS method combined with the SMC technique. Considering that girth of the code is less than or equal to $2k = 12$ (i.e., $k \leq 6$), $m \ll n$ and the parameter $t_{ij}^{\mathcal{C}_{2k}}$ is always less than or equal to 1440 (see tracking matrix $T^{\mathcal{C}_{10}}$ in Theorem 3.5), it can be concluded that the dominant term in any of previous summations is $\binom{n}{k}$. Since in the worst case the complexity of $\binom{n}{k}$ is of $\mathcal{O}\left(n^k\right)$ and the

summation is finite, the overall complexity of the verification phase is of polynomial order and equal to $\mathcal{O}\left(n^k\right)$. This means that even with or without applying the IRS approach the complexity of verification phase is polynomial. However, by applying the IRS approach the complexity is reduced as a factor of $m-1$, which is slightly lower. The third column of the table counts the number of candidate values among $\mathbb{Z}_N$ that can be assigned to each non-zero component of the exponent matrix. Given that the exponent matrix $\mathbf{P}$ is of size $m \times n$ with all zero first row and all zero first column, in an exhaustive search case, $(m-1)(n-1)$ remaining components of $\mathbf{P}$ have to be assigned. None of these remaining components has to be zero, otherwise the girth is 4. So the number of such possibilities is equal to $(N-1)^{(m-1)(n-1)}$. On the other hand, when the IRS method is considered, the second column is assigned a priori. So the remaining components of $\mathbf{P}$ are those in column 3 to n. When SMC technique is considered concurrently with IRS, we need to assign one component γ_j per j^{th} column. So $n-2$ components need to be assigned. Knowing the fact that "when $\mathbf{P}$ has all zero first row and all zero first column and its girth is greater than 6, all the non-zero elements of $\mathbf{P}$ have to be distinct ([18])", so each one of the $n-2$ components has to be different from the elements in the second column, i.e., $\gamma_j \in \mathbb{Z}_N \backslash \{0, 1, a, \cdots, a^{m-2}\}$. So the number of such possibilities is $(N-m)^{n-2}$. Finally, the fourth column proposes the overall complexity of the search method. Given the fact that for high girth code, $N >> n$, and the verification search has polynomial complexity, one can easily conclude that the overall complexity of both phases is dominated by the assigning phase equal to $\mathcal{O}\left((N-1)^{(m-1)(n-1)}\right)$ and $\mathcal{O}\left((N-m)^{(n-2)}\right)$, respectively, for exhaustive search and our proposed search method.

In general cases, by considering the number of nonequivalent cycles in relation (5) as the verification search space and noticing that $(N-1)^{(m-1)(n-1)}$ is the general assigning search space, one can figure out that the complexity of both verification and assigning phases of an exhaustive search are instinctively exponential. Information in the last column of Table III shows that even when combining SMC approach with IRS technique the complexity remains exponential. However, privileges of the aforementioned combination are that not only does it considerably reduce both of the search spaces, but by this synchronous combination, we are also still able to find lifting degrees very close to the lower bound even for large values of d_cs. In the next section we will investigate the outcomes of our greedy search algorithm. These results demonstrate that combining SMC with IRS for finding QC-LDPC code with large girth and short length is a practical tool.

IV. Numerical Results

To present our results in comparison with the state-of-the-art, we have performed the following experiment: Given a fixed girth g ($g = 10, 12$), for each size $m \times n$ of the exponent matrix, we start by the smallest value of N reported in the literature as providing for a QC-LDPC code obtained from a cyclic lifting of degree N of the fully-connected $m \times n$ exponent matrix. For this value of N, we apply the proposed search algorithm to see if we can find an exponent matrix of the form (2) for a QC-LDPC code of girth g. If we succeed, we then reduce the value of N into the nearest smaller integer value for which $\mathbb{Z}_N^{\times}$ contains at least one eligible cyclic subgroup to form $\vec{P}_1$, and repeat the same experiment. We continue until the proposed algorithm fails to provide an answer. At that point, we report the previous value of N along with the corresponding exponent matrix found by the algorithm. These results are presented in Tables IV-VII for values of $(m, g) = (3, 10),\ (3, 12),\ (4, 10),$ and $(4, 12)$, respectively. To present the exponent matrices, we have only provided the second row along with the generator element a of the corresponding cyclic subgroup. In the tables, we have also reported the $d_c = n$, rate and the minimum found lifting degree N. Although our proposed algorithm has the capability to find very high rate codes with girth $g = 10, 12$, Tables IV-VII contain the codes with lengths below $100K$ bits. This is because most of the implemented LDPC code in the literature have lengths below $100K$ bits. In the tables, we have additionally provided the best available results (in terms of minimum N) in the literature even for the search-based results or the explicit (i.e., deterministic) constructions for comparison. Note that, due to the lack of published results for exponent matrices with a large row degree d_c, we apply search algorithm 1 either by considering some proposed lower bounds (of lifting degree N) in the literature or with our conjecture of lifting degree N as a primary input of this algorithm. If input parameter N is considered as a lower bound then algorithm 1 has to test N every time and moves upward up to the point that it achieves the first success. Otherwise (i.e., if there is no lower bound or upper bound), we need to guess the starting point of N. This conjecture of N comes from studying the general trend of the lifting degree growth rate of previous Ns of smaller exponent matrices with the same girth. Here we used nonlinear regression to predict the new input values of N where "cubic polynomial" is considered as to be the regressions model (RM). As an example of former situation with a lower bound, we can look at girth $g = 10$ exponent matrices. When $g = 10$ and the exponent matrix is of size $m \times n$, there is a lower bound equal to $\frac{(m^2-m)(n^2-n)}{2} + 1$ for the lifting degree

TABLE IV

EXPONENT MATRICES OF THE SHORTEST QC-LDPC CODES WITH GIRTH 10, CONSTRUCTED FROM A $3 \times n$ FULLY-CONNECTED BASE GRAPH CONSIDERING COMBINATION OF SMC AND IRS METHODS (N_{min} IS THE SMALLEST LIFTING DEGREE. a IS THE GENERATOR OF CYCLIC SUBGROUP $\langle a \rangle$ OF $\mathbb{Z}_N^{\times}$. THE LIFTING DEGREE OF THE SHORTEST EXISTING CODES IS GIVEN BETWEEN BRACKETS. ONLY THE SECOND ROW OF THE EXPONENT MATRIX ARE LISTED)

n	Rate	N_{min}	a	Second Row of Exponent Matrix
4	0.263	37 (37 [14], [18])	27	$0, 1, 3, 24$
5	0.406	61 (61 [14], [18])	48	$0, 1, 3, 7, 12$
6	0.503	91 (91 [18])	17	$0, 1, 3, 7, 25, 38$
7	0.573	129 (139 [21])	80	$0, 1, 3, 7, 16, 41, 84$
8	0.626	181 (181 [21])	133	$0, 1, 3, 69, 120, 129, 141, 156$
9	0.667	237 (241 [21])	182	$0, 1, 3, 7, 37, 65, 80, 133, 196$
10	0.700	301 (313 [21])	80	$0, 1, 3, 7, 33, 73, 117, 140, 208, 226$
11	0.727	373 (397 [21])	285	$0, 1, 3, 35, 50, 73, 95, 170, 180, 221, 235$
12	0.750	463 (523 [21])	442	$0, 1, 3, 9, 29, 116, 148, 219, 260, 329, 388, 418$
13	0.769	571 (815 [32])	662	$0, 1, 3, 9, 91, 120, 140, 217, 375, 398, 511, 516, 561$
14	0.785	727 (1050 [32])	446	$0, 1, 3, 7, 12, 35, 105, 192, 213, 352, 442, 472, 653, 714$
15	0.80	877 (1235 [32])	595	$0, 1, 3, 7, 12, 22, 47, 114, 247, 390, 423, 431, 639, 692, 755$
16	0.812	1039 (1550 [32])	899	$0, 1, 3, 7, 12, 20, 36, 183, 396, 462, 674716, 798, 823, 967, 982$
17	0.823	1231 (1810 [32])	1105	$0, 1, 3, 7, 12, 20, 34, 106, 132, 374, 402, 450, 519, 737, 1010, 1061, 1071$
18	0.833	1453 (2100 [32])	760	$0, 1, 3, 7, 12, 20, 30, 46, 132, 184, 239, 320, 418, 867, 951, 1015, 1100, 1382$
19	0.842	1723 (2500 [32])	1682	$0, 1, 3, 7, 12, 20, 30, 46, 67, 99, 248, 605, 693, 793, 831, 975, 1105, \ldots$ $1271, 1381$
20	0.850	2089 (2875 [32])	1263	$0, 1, 3, 7, 12, 20, 30, 45, 61, 85, 107, 249, 510, 602, 970, 1022, 1297, \ldots$ $1481, 1635, 1987$
21	0.857	2197 (3300 [32])	1161	$0, 1, 125, 122, 251, 1533, 493, 2191, 1416, 867, 2083, 877, 1794, 413, \ldots$ $303, 811, 846, 1262, 1438, 1739, 2109$
22	0.863	2689	2298	$0, 1, 196, 66, 522, 1998, 524, 1109, 1343, 1217, 432, 39, 2255, 1257, \ldots$ $17, 466, 1596, 1788, 2346, 2504, 2524, 2618$
23	0.869	3049	2517	$0, 1, 267, 89, 710, 2145, 726, 2338, 639, 1971, 2886, 2445, 2077, 1424, \ldots$ $1821, 414, 586, 612, 1002, 1373, 1504, 1573, 2646$
24	0.875	3331	1868	$0, 1, 404, 407, 2676, 1209, 399, 557, 1623, 2013, 3231, 1878, 2436, 716, \ldots$ $242, 916, 31, 1843, 1941, 1998, 2229, 2318, 2618, 3139$
25	0.880	3577	1452	$0, 1, 674, 677, 1346, 571, 2700, 7, 3467, 580, 2895, 1657, 2916, \ldots$ $2443, 91, 3204, 1033, 3049, 3523, 164, 1070, 2651, 2772, 2931, 3144$

TABLE V

EXPONENT MATRICES OF THE SHORTEST QC-LDPC CODES WITH GIRTH 12, CONSTRUCTED FROM A $3 \times n$ FULLY-CONNECTED BASE GRAPH CONSIDERING COMBINATION OF SMC AND IRS METHODS (N_{min} IS THE SMALLEST LIFTING DEGREE. a IS THE GENERATOR OF CYCLIC SUBGROUP $\langle a \rangle$ OF $\mathbb{Z}_N^{\times}$. THE LIFTING DEGREE OF THE SHORTEST EXISTING CODES IS GIVEN BETWEEN BRACKETS. ONLY THE SECOND ROW OF THE EXPONENT MATRIX ARE LISTED)

n	Rate	N_{min}	a	Second Row of Exponent Matrix
4	0.263	73 (73 [14], [18])	9	$0, 1, 3, 13$
5	0.406	151 (151 [21])	119	$0, 1, 3, 108, 139$
6	0.503	271 (271 [21])	29	$0, 1, 3, 7, 67, 144$
7	0.573	427 (457 [21])	136	$0, 1, 3, 18, 209, 300, 388$
8	0.626	619 (691 [21])	367	$0, 1, 3, 216, 312, 318, 462, 529$
9	0.667	921 (991 [21])	632	$0, 1, 3, 84, 224, 361, 410, 849, 916$
10	0.700	1303 (1447 [21])	1208	$0, 1, 14, 5, 89, 349, 383, 562, 1130, 1152$
11	0.727	2011 (2161 [21])	1806	$0, 1, 30, 10, 3, 122, 454, 654, 937, 1095, 1699$
12	0.750	2883 (4730 [14])	2444	$0, 1, 522, 442, 965, 11, 902, 1145, 1857, 2091, 2632, 2775$
13	0.769	3769 (5851 [33])	3306	$0, 1, 154, 1257, 2564, 3099, 1636, 19, 1539, 2519, 2855, 3111, 3250$
14	0.785	4953	1544	$0, 1, 108, 1546, 1331, 4308, 3839, 4746, 2558, 457, 486, 1252, 4262, 4911$
15	0.80	6321	2273	$0, 1, 4380, 4051, 1613, 5328, 827, 3891, 5171, 4342, 1637, 2135, 4082, \ldots$ $4694, 5905$

N [29], [34]. So for the code with $d_c = n > 21$ (see Table IV) where there is no reported value, we use this lower bound as the input value of N within algorithm 1. The lower bound of N for the case $(m, n) = (3, 22)$ is 1387, and algorithm 1 takes this as an input and increases N up to the point that it encounters first success. We limited the running time of our search program to 72 hours, and the smallest successful lifting degree was $N = 2689$ using a core i7 desktop computer with a 3.5 GHz CPU and 8 GB RAM running in parallel. As an example of the later situation where there is no bound for N we can look at girth $g = 12$ exponent matrices. We performed cubic regression for both of the cases $d_v = m = 3, 4$. Regression models $\mathrm{RM}_{m=3}^{g=12}$ and $\mathrm{RM}_{m=4}^{g=12}$ presented below are respectively derived for the cases $m = 3$ ($4 \leq n \leq 13$) and $m = 4$ ($5 \leq n \leq 9$).

$$\mathrm{RM}_{m=3}^{g=12}(n) = 4.422299611n^3 - 55.13985257n^2 + 303.524031n - 535.7821601$$
$$\mathrm{RM}_{m=4}^{g=12}(n) = 132.6276493n^3 - 2135.788568n^2 + 11973.00351n - 22484.20244$$

TABLE VI

EXPONENT MATRICES OF THE SHORTEST QC-LDPC CODES WITH GIRTH 10, CONSTRUCTED FROM A $4 \times n$ FULLY-CONNECTED BASE GRAPH CONSIDERING COMBINATION OF SMC AND IRS METHODS (N_{min} IS THE SMALLEST LIFTING DEGREE. a IS THE GENERATOR OF CYCLIC SUBGROUP $\langle a \rangle$ OF $\mathbb{Z}_N^{\times}$. THE LIFTING DEGREE OF THE SHORTEST EXISTING CODES IS GIVEN BETWEEN BRACKETS. ONLY THE SECOND ROW OF THE EXPONENT MATRIX ARE LISTED)

n	Rate	N_{min}	a	Second Row of Exponent Matrix
5	0.200	133 (139 [21])	11	$0, 1, 5, 21, 54$
6	0.333	223 (241 [21])	39	$0, 1, 3, 9, 45, 59$
7	0.428	271 (307 [21])	28	$0, 1, 3, 7, 141, 221, 255$
8	0.500	403 (409 [21])	87	$0, 1, 3, 7, 111, 159, 233, 303$
9	0.555	541 (577 [21])	129	$0, 1, 3, 99, 264, 314, 353, 401, 423$
10	0.600	703 (787 [21])	26	$0, 1, 9, 123, 353, 443, 498, 501, 609, 663$
11	0.636	919 (1039 [21])	52	$0, 1, 3, 158, 113, 349, 509, 677, 702, 725, 772$
12	0.666	1213 (1381 [21])	217	$0, 1, 3, 653, 1088, 798, 29, 195, 370, 476, 574, 713$
13	0.692	1459	339	$0, 1, 487, 1313, 1053, 740, 533, 398, 504, 662, 664, 685, 970$
14	0.714	1939	1822	$0, 1, 3, 1590, 1357, 112, 579, 152, 254, 323, 417, 848, 975, 1863$
15	0.733	2539	2232	$0, 1, 3, 920, 1533, 278, 2515, 1504, 333, 538, 317, 404, 769, 1437, 2383$
16	0.750	3991	3701	$0, 1, 3, 869, 1448, 1062, 777, 2220, 3507, 10, 30, 41, 164, 845, 1632, 1808$
17	0.764	4909	4335	$0, 1, 3, 1721, 2868, 467, 4807, 2761, 679, 792, 675, 1916, 4687, 32, 50, \ldots$ $3314, 3559$

TABLE VII

EXPONENT MATRICES OF THE SHORTEST QC-LDPC CODES WITH GIRTH 12, CONSTRUCTED FROM A $4 \times n$ FULLY-CONNECTED BASE GRAPH CONSIDERING COMBINATION OF SMC AND IRS METHODS (N_{min} IS THE SMALLEST LIFTING DEGREE. a IS THE GENERATOR OF CYCLIC SUBGROUP $\langle a \rangle$ OF $\mathbb{Z}_N^{\times}$. THE LIFTING DEGREE OF THE SHORTEST EXISTING CODES IS GIVEN BETWEEN BRACKETS. ONLY THE SECOND ROW OF THE EXPONENT MATRIX ARE LISTED)

n	Rate	N_{min}	a	Second Row of Exponent Matrix
5	0.200	571 (607 [21])	461	$0, 1, 17, 184, 482$
6	0.333	1087 (1201 [21])	829	$0, 1, 4, 142, 1018, 1055$
7	0.428	2203 (2371 [21])	1917	$0, 1, 4, 130, 443, 1082, 1397$
8	0.500	4489 (6607 [10])	3789	$0, 1, 942, 1062, 1547, 2202, 1312, 3692$
9	0.555	8966 (12071 [10])	3977	$0, 1, 4987, 6942, 11, 17, 1158, 2049, 3754$

So, if our underlined exponent matrix is of size $3 \times n$ (resp., $4 \times n$) and there is no bound for the size of N, we estimate it with $N \simeq \lfloor \mathrm{RM}_{m=3}^{g=12}(n) \rfloor$ (resp., $N \simeq \lfloor \mathrm{RM}_{m=4}^{g=12}(n) \rfloor$). As we are not sure if this approximated value of N is a lower bound or upper bound, our search program would be run for two cases in parallel: 1) upward check and 2) downward check. During this process and at a time when the program sees a success by decreasing N, it will terminate the upward manner and will focus only on downward movement. This process is continued until the processing time is over. As a result, for a girth 12 exponent matrix of size $(m, n) = (3, 14)$, we could not find an accurate bound for its lifting degree (see Table V); however, we estimated it as $N \simeq \lfloor \mathrm{RM}_{m=3}^{g=12}(14) \rfloor = 5040$. We ran our search program for it, and after 24 hours of running, the smallest successful N was 4953. The point-to-point growth rate curves to all the values of N found by our search program, by proposed bounds, and by estimations are included in Fig. 10 for further comparison and investigation.

As pointed out in the introduction, the exponent matrices of fully-connected codes reported in Tables IV to VII can be used to construct other practical LDPC codes (regular or irregular). As an example of such construction methods, we considered the $(64800, 48600)$ DVB-S2 standard code [30] as a reference code and tried to design a similar code in length and rate using the proposed SMC-structured QC-LDPC codes. To this end, we started from a base-matrix of dimension 15×60 and lifting degree $N = 1087$ to define a rate 3/4 $(65220, 48915)$ fully-connected QC-LDPC code $C_{\textbf{full}}$ with Tanner graph $T_{\textbf{full}}$. The overall girth is 6 but the Tanner graph contains several distinct and large sub-graphs of girth 12. To mimic the edge distribution of the DVB-S2 code, parts of the exponent matrix are suppressed from $C_{\textbf{full}}$ to generate an irregular QC-LDPC code $C_{\textbf{masked}}$. The details on the construction of $C_{\textbf{masked}}$ are given in Appendix B. Finally, performances of both $C_{\textbf{masked}}$ and DVB-S2 codes were evaluated under Additive White Gaussian Noise (AWGN) channel with Sum-Product (SP) algorithm by AFF3CT software [35]. Fig. 11 depicts the Frame Error Rate (FER) as well as the Bit Error Rate (BER) performances of these codes. As it can be seen from this figure, $C_{\textbf{masked}}$ has better performance in waterfall region and it gains 0.15 dB at FER$= 10^{-5}$ under SP decoder with 50 decoding iterations.

V. Conclusion

We have proposed a search-based method for the construction of fully-connected QC-LDPC block codes capable of achieving girths $g = 10,\ 12$ with lengths close to the lower bounds. To ease the search, we sieved through the multiplicative ring of integers. We showed that by

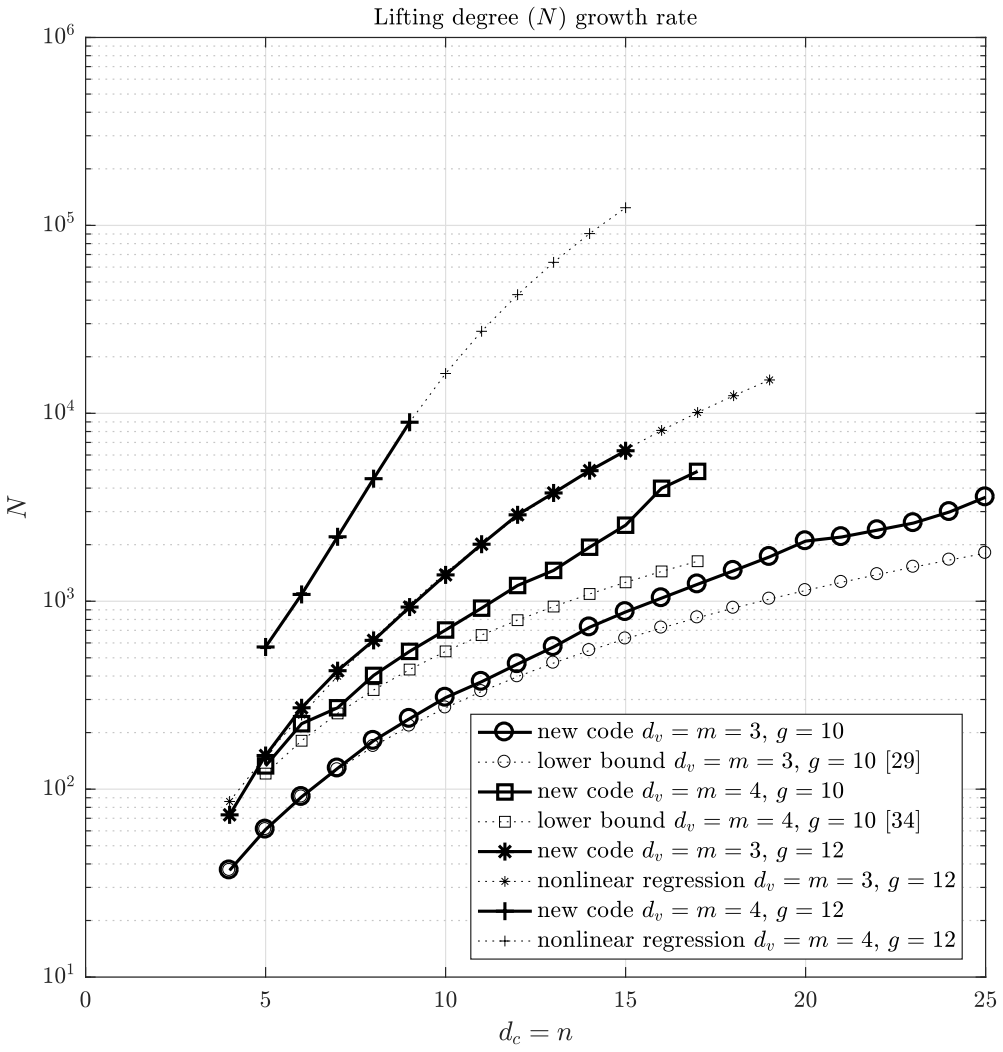

Fig. 10. Minimum lifting degree N growth rate of new constructed codes versus $d_c = n$ for $d_v = m = 3, 4$.

smartly selecting elements of exponent matrix's second column of the code from this ring, it is possible to further reduce the search space and still find high girth QC-LDPC codes with lengths very close to the lower bound. Pseudo code of our proposed search algorithm was presented and as a result of our method, a variety of fully-connected QC-LDPC codes with different rates and small lengths were provided in tables. Furthermore, small length counterpart codes were addressed within the tables for comparison, and in most of the cases the new codes have lengths smaller than the available state of the art. In the end, capability of the proposed method in constructing practical irregular QC-LDPC codes was illustrated, and their good performances were compared with the standard codes.

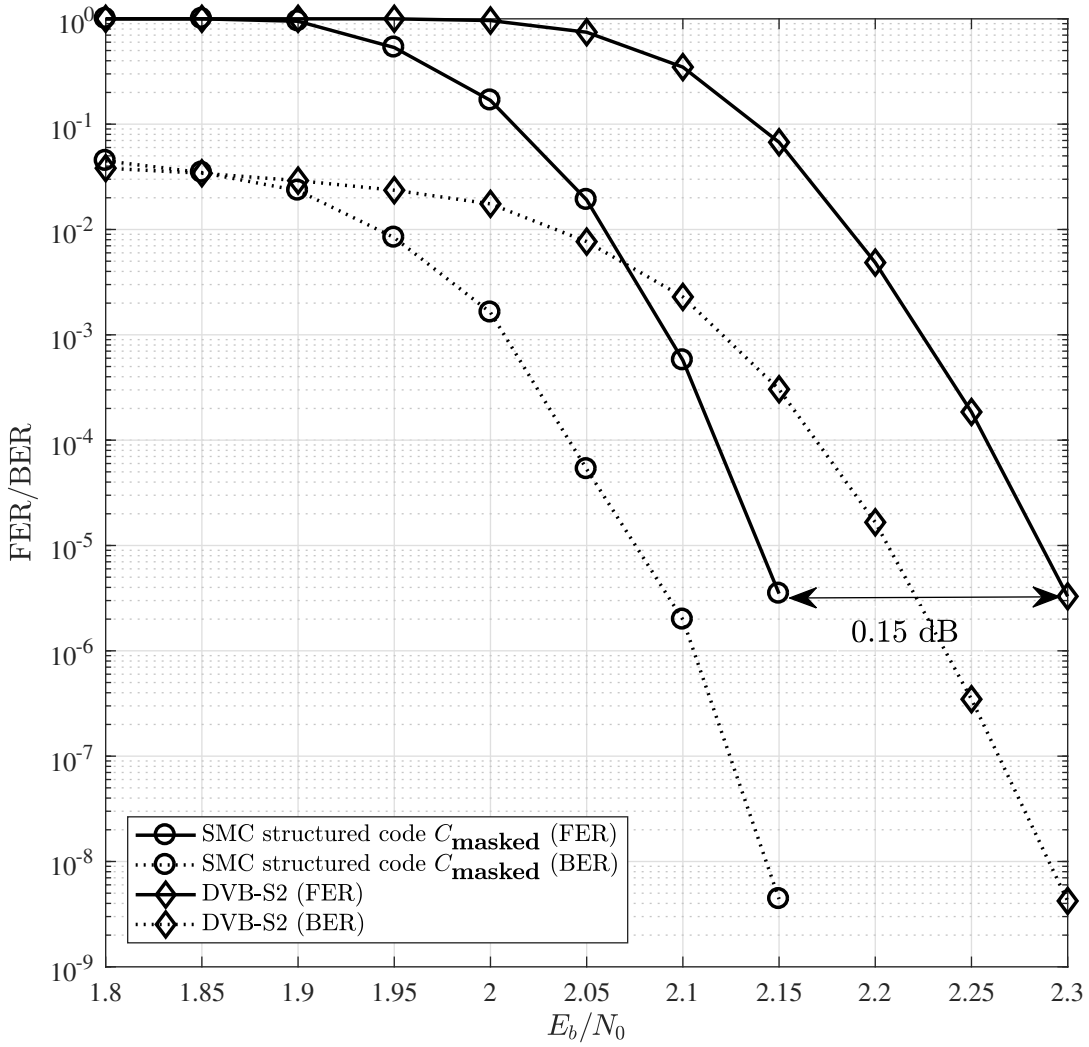

Fig. 11. Performance comparison of a $(65220, 48915)$ SMC-structured QC-LDPC code, constructed by cyclic lifting of a masked 15×60 fully-connected base graph and lifting degree $N = 1087$, with a $(64800, 48600)$ DVB-S2 code [30].

APPENDIX

A. An algebraic proof to lemmas 3.6 and 3.8.

Let $\mathcal{C}_{2k}^{m,n}$ be a potential cycle of length $2k$ in $\mathbf{P}_{m\times n}^{\mathrm{SMC}}$ with summation $\sum_{i=0}^{k-1}\left(p_{m_i n_i} - p_{m_i n_{i+1}}\right)$ where $n_k = n_0$, $m_i \neq m_{i+1}$ and $n_i \neq n_{i+1}$. Without loss of generality we can rewrite this summation as $\sum_{i=0}^{k-1}\left(p_{m_i n_i} - p_{m_{i+1} n_i}\right)$ where $m_k = m_0$, $m_i \neq m_{i+1}$ and $n_i \neq n_{i+1}$. Since the second column of $\mathbf{P}_{m\times n}^{\mathrm{SMC}}$ is $\vec{P}_1 = [0, 1, a, a^2, \cdots, a^{m-2}]^T$, the later summation could be written

as $\sum_{i=0}^{k-1}\gamma_{n_i}\left(\delta\left(m_i\right)-\delta\left(m_{i+1}\right)\right)$ where $m_i \in \{0,1,2,\cdots,m-1\}$, $n_i \in \{0,1,2,\cdots,n-1\}$, $\delta\left(m_i\right)=\vec{P}_1\left(m_i\right)$, $\gamma_0=0$, $\gamma_1=1$, and γ_{n_i} $(2\leq n_i)$ is the coefficient of column $\vec{P}_{n_i}=\gamma_{n_i}\vec{P}_1$. Assuming $\Delta\left(m_i\right)=\delta\left(m_i\right)-\delta\left(m_{i+1}\right)$, the summation of $\mathcal{C}_{2k}^{m,n}$ could be written as $\sum_{i=0}^{k-1}\gamma_{n_i}\Delta\left(m_i\right)$. Let us first consider the case $m=3$ and $a(1-a)=1$, where $a\in\mathbb{Z}_N^{\times}$. Since $\text{GCD}(a,N)=\text{GCD}((1-a),N)=1$, $\sum_{i=0}^{k-1}\gamma_{n_i}\Delta\left(m_i\right)=0 \mod N$ if and only if $\sum_{i=0}^{k-1}\gamma_{n_i}a\Delta\left(m_i\right)=0 \mod N$ if and only if $\sum_{i=0}^{k-1}\gamma_{n_i}(1-a)\Delta\left(m_i\right)=0 \mod N$. In other words, $\mathcal{C}_{2k}^{m,n}$ is activated if and only if $a\mathcal{C}_{2k}^{m,n}$ is activated if and only if $(1-a)\mathcal{C}_{2k}^{m,n}$ is. On the other hand, it is easy to check that $\Delta\left(m_i\right),\ a\Delta\left(m_i\right),\ (1-a)\Delta\left(m_i\right)\in\{\pm1,\pm a,\pm(1-a)\}$ (see Table VIII). In fact for every index m_i, each of the differences $\Delta\left(m_i\right),\ a\Delta\left(m_i\right)$, and $(1-a)\Delta\left(m_i\right)$ is calculated by considering elements in the same column but different pairs of rows of $\mathbf{P}_{3\times n}^{\text{SMC}}$. As a result, potential cycles $\mathcal{C}_{2k}^{m,n}$, $a\mathcal{C}_{2k}^{m,n}$, and $(1-a)\mathcal{C}_{2k}^{m,n}$ have the same length but different paths in $\mathbf{P}_{3\times n}^{\text{SMC}}$ and they concurrently are either activated or not-activated. So $\#\mathcal{C}_{2k,a}^{3,n}\leq\frac{\#\mathcal{C}_{2k}^{3,n}}{3}$. For the case $m=4$ and $a^3=1$, where $a\in\mathbb{Z}_N^{\times}$, one can also follow the same argument by considering the values in Table IX. As result $\#\mathcal{C}_{2k,a}^{4,n}\leq\frac{\#\mathcal{C}_{2k}^{4,n}}{3}$.

TABLE VIII

LOOKUP TABLE TO $\Delta\left(m_i\right)$, $a\Delta\left(m_i\right)$ AND $(1-a)\Delta\left(m_i\right)$ WHEN SECOND COLUMN OF $\mathbf{P}_{3\times n}^{\text{SMC}}$ IS $\vec{P}_1=[0,1,a]^T$.

$\Delta\left(m_i\right)$	1	a	$1-a$	-1	$-a$	$-1+a$
$a\Delta\left(m_i\right)$	a	$-1+a$	1	$-a$	$1-a$	-1
$(1-a)\,\Delta\left(m_i\right)$	$1-a$	-1	$-a$	$-1+a$	1	a

TABLE IX

LOOKUP TABLE TO $\Delta\left(m_i\right)$, $a\Delta\left(m_i\right)$ AND $a^2\Delta\left(m_i\right)$ WHEN SECOND COLUMN OF $\mathbf{P}_{4\times n}^{\text{SMC}}$ IS $\vec{P}_1=\left[0,1,a,a^2\right]^T$.

$\Delta\left(m_i\right)$	1	a	a^2	$1-a$	$1-a^2$	$a-a^2$	-1	$-a$	$-a^2$	$-1+a$	$-1+a^2$	$-a+a^2$
$a\Delta\left(m_i\right)$	a	a^2	1	$a-a^2$	$-1+a$	$-1+a^2$	$-a$	$-a^2$	-1	$-a+a^2$	$1-a$	$1-a^2$
$a^2\Delta\left(m_i\right)$	a^2	1	a	$-1+a^2$	$-a+a^2$	$1-a$	$-a^2$	-1	$-a$	$1-a^2$	$a-a^2$	$-1+a$

B. DVB-S2 like code construction

The array displayed in (13) is a vertical display of an exponent matrix $\mathbf{P}_{15\times 60}^{\text{SMC}}$ with lifting degree 1087, which is *masked* [5] in a way that its row (resp., column) degree distribution is

[5]See section 7 of [28] for masking technique.

$\rho(x) = 0.8666x^{15} + 0.1334x^{16}$ (resp., $\lambda(x) = 0.25x + 0.55x^2 + 0.0666x^3 + 0.0834x^{10} + 0.05x^{13}$). Thus, the resulting code of (13) would be an irregular QC-LDPC code that we call $C_{\textbf{masked}}$. Before the masking operation, $\mathbf{P}^{\mathrm{SMC}}_{15\times 60}$ is an exponent matrix of a girth $g = 6$ fully-connected QC-LDPC code $C_{\textbf{full}}$ of length $60 * 1087 = 65220$ and rate $\frac{60-15}{60} = 0.75$ that preserves SMC property. Although the Tanner graph $T_{\textbf{full}}$ of code $C_{\textbf{full}}$ is of girth 6, it is locally optimized so that it has several distinct and large sub-graphs each of girth 12. To impose this property to $T_{\textbf{full}}$, $\mathbf{P}^{\mathrm{SMC}}_{15\times 60}$ is constructed as follows:

$$\mathbf{P}^{\mathrm{SMC}}_{15\times 60} = \left[\begin{array}{c|c|c|c} & 0 & \cdots & 0 \\ A^T & \gamma_4 & \cdots & \gamma_{59} \\ \hline A_1 & p_{3,2}\gamma_4 & \cdots & p_{3,2}\gamma_{59} \\ \hline A_2 & \vdots & \ddots & \vdots \\ & p_{15,2}\gamma_4 & \cdots & p_{15,2}\gamma_{59} \end{array}\right], \tag{12}$$

where matrix A is the matrix of dimension 4×6 defined in Table VII for rate $1/3$ (fully-connected QC-LDPC code with $m = 4$, $n = 6$, and $N_{min} = 1087$), thus A^T is of dimension 6×4. Matrix A_1 is the matrix of dimension 5×4 generated with the 5 last rows of A^T multiplied by the factor 139, i.e., $A_1(i,j) = 139 * A^T(i+1,j) \pmod{1087}$ ($i = 1,\ldots,5; j = 1,\ldots,4$). Matrix A_2 is the matrix of dimension 4×4 generated with the rows 2 to 5 of A^T multiplied by the factor 719, i.e., $A_2(i,j) = 719 * A^T(i+1,j) \pmod{1087}$ ($i = 1,\ldots,4; j = 1,\ldots,4$). Since 1087 is a prime number, $\mathrm{GCD}(139, 1087) = \mathrm{GCD}(719, 1087) = 1$, and thus A_1 and A_2 are also of girth 12 (lemma 3 of [18]). As shown in (12), the first four columns of $\mathbf{P}^{\mathrm{SMC}}_{15\times 60}$ are made of the vertical concatenation of A^T, A_1, and A_2. This left part of matrix $\mathbf{P}^{\mathrm{SMC}}_{15\times 60}$ is intentionally constructed with high girth sub-matrices as it will be only lightly masked. The rest of the columns of $\mathbf{P}^{\mathrm{SMC}}_{15\times 60}$ still apply to SMC property, where $p_{j,2}$'s ($j = 3, \cdots, 15$) are components of the second column of $\mathbf{P}^{\mathrm{SMC}}_{15\times 60}$, coefficients γ_i's ($4 \le i \le 59$) are selected in a way that $\mathbf{P}^{\mathrm{SMC}}_{15\times 60}$ respects girth-6 constraint, and $p_{j,2}\gamma_i$ is calculated modulo 1087.

	r_1	r_2	r_3	r_4	r_5	r_6	r_7	r_8	r_9	r_{10}	r_{11}	r_{12}	r_{13}	r_{14}	r_{15}
c_1	−1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
c_2	−1	1	4	142	1018	1055	139	556	172	192	987	719	702	1007	391
c_3	0	829	55	322	410	647	9	36	−1	466	799	375	413	1074	213
c_4	0	−1	1028	623	−1	472	939	495	−1	429	388	1080	1059	−1	483
c_5	0	9	36	191	466	−1	−1	656	461	−1	187	1036	883	367	−1
c_6	0	837	−1	371	945	391	34	136	480	915	−1	−1	−1	434	80
c_7	−1	265	1060	−1	194	216	964	−1	1013	878	675	310	153	−1	350
c_8	0	43	172	671	294	−1	542	1081	874	−1	48	−1	837	908	−1
c_9	0	−1	−1	−1	−1	−1	−1	−1	893	921	−1	−1	548	−1	−1
c_{10}	−1	−1	109	−1	−1	215	−1	−1	−1	−1	−1	842	−1	1081	−1
c_{11}	−1	70	−1	−1	605	−1	1034	−1	−1	−1	−1	−1	−1	−1	195
c_{12}	0	−1	−1	337	−1	−1	−1	355	−1	−1	421	−1	−1	−1	−1
c_{13}	−1	−1	−1	−1	−1	438	747	−1	635	−1	−1	−1	−1	−1	−1
c_{14}	−1	106	−1	−1	−1	956	−1	−1	−1	−1	−1	124	−1	−1	−1
c_{15}	0	−1	−1	−1	−1	−1	−1	−1	−1	1060	82	−1	−1	−1	−1
c_{16}	−1	−1	−1	−1	23	−1	−1	−1	305	−1	−1	−1	−1	−1	232
c_{17}	−1	−1	−1	−1	278	−1	−1	438	−1	−1	−1	−1	−1	23	−1
c_{18}	−1	−1	−1	112	−1	−1	523	−1	−1	−1	−1	−1	569	−1	−1
c_{19}	−1	−1	425	−1	6	−1	−1	−1	−1	834	−1	−1	−1	−1	−1
c_{20}	−1	−1	496	−1	−1	380	−1	−1	−1	−1	−1	22	−1	−1	−1
c_{21}	−1	952	−1	−1	−1	−1	−1	−1	−1	168	456	−1	−1	−1	−1
c_{22}	−1	380	−1	697	−1	−1	−1	−1	−1	−1	−1	−1	−1	36	−1
c_{23}	0	−1	−1	−1	−1	−1	−1	−1	276	−1	−1	−1	−1	−1	46
c_{24}	−1	−1	−1	−1	343	−1	270	−1	−1	−1	−1	−1	433	−1	−1
c_{25}	−1	−1	−1	178	−1	−1	−1	−1	−1	−1	−1	1085	−1	−1	138
c_{26}	−1	−1	−1	838	−1	347	−1	−1	−1	−1	−1	186	−1	−1	−1
c_{27}	−1	−1	687	−1	−1	−1	−1	−1	−1	366	217	−1	−1	−1	−1
c_{28}	0	−1	−1	−1	−1	−1	−1	296	−1	−1	−1	−1	−1	−1	302
c_{29}	−1	179	−1	−1	−1	−1	−1	−1	352	−1	−1	−1	−1	−1	421
c_{30}	0	−1	−1	−1	−1	−1	−1	87	−1	−1	−1	−1	−1	965	−1
c_{31}	−1	435	−1	−1	−1	211	−1	−1	−1	908	−1	−1	−1	−1	−1
c_{32}	−1	−1	−1	−1	55	1081	−1	−1	−1	−1	−1	1018	−1	−1	−1
c_{33}	−1	−1	−1	886	−1	−1	−1	−1	−1	310	65	−1	−1	−1	−1
c_{34}	−1	−1	−1	100	−1	−1	−1	315	−1	−1	−1	−1	−1	158	−1
c_{35}	−1	−1	892	−1	−1	−1	−1	−1	311	−1	−1	−1	−1	−1	233
c_{36}	−1	1051	−1	−1	−1	−1	−1	637	−1	−1	−1	−1	−1	706	−1
c_{37}	0	−1	−1	−1	−1	−1	−1	−1	863	−1	−1	−1	−1	812	−1
c_{38}	0	−1	−1	−1	−1	−1	383	−1	−1	−1	−1	−1	425	−1	−1
c_{39}	−1	−1	−1	−1	−1	−1	−1	−1	−1	−1	600	34	136	−1	−1
c_{40}	−1	−1	−1	−1	750	−1	−1	−1	−1	985	−1	−1	−1	−1	98
c_{41}	−1	−1	−1	388	−1	−1	−1	−1	669	−1	−1	−1	−1	700	−1
c_{42}	−1	−1	16	−1	−1	−1	556	−1	−1	−1	−1	−1	634	−1	−1
c_{43}	−1	−1	989	−1	−1	−1	−1	509	−1	−1	−1	−1	193	−1	−1
c_{44}	−1	270	−1	−1	−1	−1	572	−1	−1	−1	−1	644	−1	−1	−1
c_{45}	0	−1	−1	−1	−1	735	−1	−1	−1	−1	1074	−1	−1	−1	−1
c_{46}	0	−1	−1	−1	−1	−1	−1	−1	−1	−1	−1	−1	−1	−1	223
c_{47}	0	291	−1	−1	−1	−1	−1	−1	−1	−1	−1	−1	−1	−1	−1
c_{48}	−1	32	128	−1	−1	−1	−1	−1	−1	−1	−1	−1	−1	−1	−1
c_{49}	−1	−1	14	497	−1	−1	−1	−1	−1	−1	−1	−1	−1	−1	−1
c_{50}	−1	−1	−1	119	57	−1	−1	−1	−1	−1	−1	−1	−1	−1	−1
c_{51}	−1	−1	−1	−1	536	989	−1	−1	−1	−1	−1	−1	−1	−1	−1
c_{52}	−1	−1	−1	−1	−1	814	1016	−1	−1	−1	−1	−1	−1	−1	−1
c_{53}	−1	−1	−1	−1	−1	−1	658	458	−1	−1	−1	−1	−1	−1	−1
c_{54}	−1	−1	−1	−1	−1	−1	−1	1025	1060	−1	−1	−1	−1	−1	−1
c_{55}	−1	−1	−1	−1	−1	−1	−1	−1	506	489	−1	−1	−1	−1	−1
c_{56}	−1	−1	−1	−1	−1	−1	−1	−1	−1	382	571	−1	−1	−1	−1
c_{57}	−1	−1	−1	−1	−1	−1	−1	−1	−1	−1	383	192	−1	−1	−1
c_{58}	−1	−1	−1	−1	−1	−1	−1	−1	−1	−1	−1	897	327	−1	−1
c_{59}	−1	−1	−1	−1	−1	−1	−1	−1	−1	−1	−1	−1	989	869	−1
c_{60}	−1	−1	−1	−1	−1	−1	−1	−1	−1	−1	−1	−1	−1	936	969

(13)

REFERENCES

[1] D. J. C. MacKay, "Good error-correcting codes based on very sparse matrices," *IEEE Transactions on Information Theory*, vol. 45, no. 2, pp. 399–431, Mar. 1999.

[2] "IEEE Draft Standard for Air Interface for Broadband Wireless Access Systems," *IEEE P802.16/D4, September 2017 (Revision of IEEE Std 802.16-2012)*, pp. 1–2764, Sept. 2017.

[3] ETSI, "Digital Video Broadcasting (DVB)," *European Telecommunications Standards Institute, Sophia Antipolis, France*, pp. 1–78, Apr. 2009.

[4] CCSDS, "Short Blocklength LDPC codes for TC synchronization and channel coding," *CCSDS 231.1-O-1*, 2015.

[5] https://www.3gpp.org/ftp/tsg_ran/WG1_RL1/.

[6] H. Li, B. Bai, X. Mu, J. Zhang, and H. Xu, "Algebra-assisted construction of quasi-cyclic LDPC codes for 5g new radio," *IEEE Access*, vol. 6, pp. 50 229–50 244, Sept. 2018.

[7] M. Zhang, Z. Wang, Q. Huang, and S. Wang, "Time-invariant quasi-cyclic spatially coupled LDPC codes based on packings," *IEEE Transactions on Communications*, vol. 64, no. 12, pp. 4936–4945, 2016.

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

[9] 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.

[10] M. E. O'Sullivan, "Algebraic construction of sparse matrices with large girth," *IEEE Transactions on Information Theory*, vol. 52, no. 2, pp. 718–727, Feb. 2006.

[11] Yige Wang, J. S. Yedidia, and S. C. Draper, "Construction of high-girth QC-LDPC codes," in *2008 5th International Symposium on Turbo Codes and Related Topics*, Sep. 2008, pp. 180–185.

[12] R. Asvadi, A. H. Banihashemi, and M. Ahmadian-Attari, "Lowering the Error Floor of LDPC Codes Using Cyclic Liftings," *IEEE Transactions on Information Theory*, vol. 57, no. 4, pp. 2213–2224, Apr. 2011.

[13] D. V. Nguyen, S. K. Chilappagari, M. W. Marcellin, and B. Vasic, "On the Construction of Structured LDPC Codes Free of Small Trapping Sets," *IEEE Transactions on Information Theory*, vol. 58, no. 4, pp. 2280–2302, Apr. 2012.

[14] I. E. Bocharova, F. Hug, R. Johannesson, B. D. Kudryashov, and R. V. Satyukov, "Searching for Voltage Graph-Based LDPC Tailbiting Codes With Large Girth," *IEEE Transactions on Information Theory*, vol. 58, no. 4, pp. 2265–2279, Apr. 2012.

[15] J. Wang, L. Dolecek, and R. D. Wesel, "The Cycle Consistency Matrix Approach to Absorbing Sets in Separable Circulant-Based LDPC Codes," *IEEE Transactions on Information Theory*, vol. 59, no. 4, pp. 2293–2314, Apr. 2013.

[16] M. Diouf, D. Declercq, S. Ouya, and B. Vasic, "A PEG-like LDPC code design avoiding short trapping sets," in *2015 IEEE International Symposium on Information Theory (ISIT)*, Jun. 2015, pp. 1079–1083.

[17] M. Gholami and Z. Gholami, "An explicit method to generate some QC-LDPC codes with girth 8," *Iranian Journal of Science and Transactions A: Science*, vol. 40, no. 2, pp. 145–149, Jun. 2016.

[18] A. Tasdighi, A. H. Banihashemi, and M. Sadeghi, "Efficient Search of Girth-Optimal QC-LDPC Codes," *IEEE Transactions on Information Theory*, vol. 62, no. 4, pp. 1552–1564, Apr. 2016.

[19] ——, "Symmetrical Constructions for Regular Girth-8 QC-LDPC Codes," *IEEE Transactions on Communications*, vol. 65, no. 1, pp. 14–22, Jan. 2017.

[20] X. Tao, Y. Li, Y. Liu, and Z. Hu, "On the Construction of LDPC Codes Free of Small Trapping Sets by Controlling Cycles," *IEEE Communications Letters*, vol. 22, no. 1, pp. 9–12, Jan. 2018.

[21] M. Battaglioni, A. Tasdighi, M. Baldi, M. H. Tadayon, and F. Chiaraluce, "Compact QC-LDPC Block and SC-LDPC Convolutional Codes for Low-Latency Communications," in *2018 IEEE 29th Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*, Sep. 2018, pp. 1–5.

[22] A. Derrien, E. Boutillon, and A. Cerqueus, "Additive, Structural, and Multiplicative Transformations for the Construction of Quasi-Cyclic LDPC Matrices," *IEEE Transactions on Communications*, vol. 67, no. 4, pp. 2647–2659, Apr. 2019.

[23] S. Naseri and A. H. Banihashemi, "Construction of Girth-8 QC-LDPC Codes Free of Small Trapping Sets," *IEEE Communications Letters*, vol. 23, no. 11, pp. 1904–1908, Nov. 2019.

[24] A. Jimenez Felstrom and K. S. Zigangirov, "Time-varying periodic convolutional codes with low-density parity-check matrix," *IEEE Transactions on Information Theory*, vol. 45, no. 6, pp. 2181–2191, Sep. 1999.

[25] M. Battaglioni, A. Tasdighi, G. Cancellieri, F. Chiaraluce, and M. Baldi, "Design and Analysis of Time-Invariant SC-LDPC Convolutional Codes With Small Constraint Length," *IEEE Transactions on Communications*, vol. 66, no. 3, pp. 918–931, Mar. 2018.

[26] M. H. Tadayon, A. Tasdighi, M. Battaglioni, M. Baldi, and F. Chiaraluce, "Efficient Search of Compact QC-LDPC and SC-LDPC Convolutional Codes With Large Girth," *IEEE Communications Letters*, vol. 22, no. 6, pp. 1156–1159, Jun. 2018.

[27] M. Battaglioni, M. Baldi, F. Chiaraluce, and M. Lentmaier, "Girth Properties of Time-Varying SC-LDPC Convolutional Codes," in *2019 IEEE International Symposium on Information Theory (ISIT)*, Jul. 2019, pp. 2599–2603.

[28] J. Li, S. Lin, K. Abdel-Ghaffar, D. J. Costello Jr, and W. E. Ryan, *LDPC code designs, constructions, and unification*. Cambridge University Press, 2016.

[29] M. Karimi and A. H. Banihashemi, "On the Girth of Quasi-Cyclic Protograph LDPC Codes," *IEEE Transactions on Information Theory*, vol. 59, no. 7, pp. 4542–4552, Jul. 2013.

[30] https://www.etsi.org/deliver/etsi_en/302300_302399/30230701/01.04.01_60/en_30230701v010401p.pdf.

[31] H. Riesel, *Prime numbers and computer methods for factorization*. Springer Science & Business Media, 2012, vol. 126.

[32] http://www-labsticc.univ-ubs.fr/~boutillon/ldpc/ldpc.htm.

[33] H. Xu, H. Li, D. Feng, B. Zhang, and H. Zhu, "On the Girth of Tanner (3,13) Quasi-Cyclic LDPC Codes," *IEEE Access*, vol. 7, pp. 5153–5179, 2019.

[34] F. Amirzade and M. Sadeghi, "Lower Bounds on the Lifting Degree of QC-LDPC Codes by Difference Matrices," *IEEE Access*, vol. 6, pp. 23 688–23 700, 2018.

[35] https://aff3ct.github.io/.