2022 IEEE International Symposium on Information Theory (ISIT) | 978-1-6654-2159-1/22/$31.00 ©2022 IEEE | DOI: 10.1109/ISIT50566.2022.9834862

Using Minors to Construct Generator Matrices for Quasi-Cyclic LDPC Codes

Roxana Smarandache*†, Anthony Gómez-Fonseca*, and David G. M. Mitchell‡

Departments of *Mathematics and †Electrical Engineering,
University of Notre Dame, Notre Dame, IN 46556, USA, {agomezfo, rsmarand}@nd.edu
‡Klipsch School of Electrical and Computer Engineering,
New Mexico State University, Las Cruces, NM 88003, USA, dgmm@nmsu.edu

***Abstract*—This paper gives a simple method to construct generator matrices with polynomial entries (and hence offers an alternative encoding method to the one commonly used) for all quasi-cyclic low-density parity-check (QC-LDPC) codes, even for those that are rank deficient. The approach is based on constructing a set of codewords with the desired total rank by using minors of the parity-check matrix. We exemplify the method on several well-known and standard codes. Moreover, we explore the connections between the minors of the parity-check matrix and the known upper bound on minimum distance and provide a method to compute the rank of any parity-check matrix representing a QC-LDPC code, and hence the dimension of the code, by using the minors of the corresponding polynomial parity-check matrix.**

I. Introduction

Quasi-cyclic LDPC (QC-LDPC) codes, are attractive for implementation purposes since they can be encoded with low complexity using simple feedback shift-registers [1] and their structure leads to efficiencies in decoder design [2]. Moreover, QC-LDPC codes can be shown to perform well compared to random LDPC codes for moderate block lengths [3], [4]. However, unlike typical members of an asymptotically good protograph-based LDPC code ensemble, the QC sub-ensemble does not have linear distance growth. Indeed, if the protograph base matrix consists of only ones and zeros, then the minimum Hamming distance is bounded above by $(n_c + 1)!$, where n_c is the number of check nodes in the protograph, regardless of the lifting factor N [5]. This result was extended to multi-edge protographs in [6]. Significant effort has been made in the coding theory community to design QC-LDPC code matrices with minimum distance and girth approaching these bounds, see [3], [4], [7]–[10] and references therein.

As a result of the rich structure of QC-LDPC codes, their matrix representations have been studied in a number of works. These include methods to construct a generator in standard form (e.g., [1]), which allows high throughput systematic encoding but the resulting generator matrix is typically dense. The sparse parity-check matrix is often represented as an array of circulant permutations, which facilitate efficient implementation, and will typically have a number of linearly dependent rows. Although Gaussian elimination can be employed to compute the rank with a complexity of $\mathcal{O}(n^3)$, it is desirable to have an analytic way to compute the rank, particularly for classes of algebraic QC-LDPC codes. Methods to compute the rank of QC-LDPC codes have been investigated, including approaches involving Fourier transforms [11], [12] and the matrix polynomial representation [13]. However, these approaches are limited to certain code parameters.

In this paper, we will use some previous results by Smarandache and Vontobel [6] to show how to construct polynomial generator matrices in various forms, including in standard form. The matrices are interesting from both the perspective of allowing for an encoding alternative to the methods in [1] as well as from the resulting codewords that are constructed from the method. In particular, the rows of the generator matrices we construct are codewords with relatively small weight, in some cases, equal to the minimum distance of the code. We exemplify these methods on some known codes. Our approach employs the minors of the polynomial matrix which also allow for a most general formula to compute the rank of any parity-check matrix representing a QC-LDPC code, and hence, the dimension of any QC-LDPC code.

II. Definitions, notations and background

We use the following notation. For any positive integer L, $[L]$ denotes the set $\{1, 2, \ldots, L\}$. For any matrix M, we let $M_{\mathcal{I},\mathcal{J}}$ be the sub-matrix of M that contains only the rows of M whose index appears in the set $\mathcal{I}$ and only the columns of M whose index appears in the set $\mathcal{J}$; if $\mathcal{I}$ equals the set of all row indices of M, we will simply write $M_{\mathcal{J}}$. We use the shorthand $M_{\mathcal{J}\setminus i}$ for $M_{\mathcal{J}\setminus\{i\}}$. If $\mathcal{I}$ and $\mathcal{J}$ have the same cardinality, we use $\Delta_{\mathcal{I},\mathcal{J}} = \det(H_{\mathcal{I},\mathcal{J}})$, and $\Delta_{\mathcal{J}} = \det(H_{[n_c],\mathcal{J}})$.

As usual, an LDPC code $\mathcal{C}$ is described as the null space of a parity-check matrix H to which we associate a Tanner graph [14] in the usual way. The girth of the Tanner graph, denoted by $\mathrm{girth}(H)$, is the length of its shortest cycle.

A protograph [15], [16] is a small bipartite graph represented by an $n_c \times n_v$ parity-check or *base* biadjacency matrix B with non-negative integer entries b_{ij}. The parity-check matrix H of a protograph-based LDPC block code can be created by replacing each non-zero entry b_{ij} by a sum of b_{ij} non-overlapping $N \times N$ permutation matrices and a zero entry by the $N \times N$ all-zero matrix. Graphically, this operation is equivalent to taking an N-fold graph cover, or "lifting", of the protograph. We denote the $N \times N$ circulant permutation matrix where the entries of the $N \times N$ identity matrix I are shifted to the left by r positions modulo N as I_r. A quasi-cyclic (QC) LDPC code of length $n = n_v N$ is a protograph-based LDPC code, for which the $N \times N$ lifting permutation matrices are

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

all circulant matrices I_r. Thus a QC code has an $n_cN \times n_vN$ parity-check matrix H of the form

$$H = \begin{bmatrix} H_{1,1} & H_{1,2} & \cdots & H_{1,n_v} \\ \vdots & \vdots & \ddots & \vdots \\ H_{n_c,1} & H_{n_c,2} & \cdots & H_{n_c,n_v} \end{bmatrix},$$

where the $N \times N$ sub-matrices $H_{i,j}$ are circulant; applying equal circular shifts to each length-N sub-blocks of a codeword results in a codeword.

With the help of the well-known isomorphism between the ring of circulant matrices over the binary field $\mathbb{F}_2$ and the ring $\mathbb{F}_2[x]/(x^N-1)$ of $\mathbb{F}_2$-polynomials modulo x^N-1 (see, *e.g.*, [17]), a QC LDPC code can also be described by an $n_c \times n_v$ polynomial parity-check matrix over $\mathbb{F}_2[x]/(x^N-1)$. In particular, with the $n_cN \times n_vN$ parity-check matrix H described above we associate the polynomial parity-check matrix

$$H(x) = \begin{bmatrix} h_{1,1}(x) & h_{1,2}(x) & \cdots & h_{1,n_v}(x) \\ \vdots & \vdots & \ddots & \vdots \\ h_{n_c,1}(x) & h_{n_c,2}(x) & \cdots & h_{n_c,n_v}(x) \end{bmatrix},$$

where $h_{i,j}(x) \in \mathbb{F}_2[x]/(x^N-1)$. Moreover, with any vector $\mathbf{c} = (c_{1,0}, \ldots, c_{1,N-1}, \ldots, c_{n_v,0}, \ldots, c_{n_v,N-1})$ in $\mathbb{F}_2^{n_vN}$, we associate the polynomial vector $\mathbf{c}(x) = \big(c_1(x), \ldots, c_{n_v}(x)\big)$ where $c_i(x) \triangleq \sum_{s=0}^{N-1} c_{i,s}x^s$. Then, the condition $H \cdot \mathbf{c}^{\mathsf{T}} = \mathbf{0}^{\mathsf{T}}$ (in $\mathbb{F}_2$) is equivalent to $H(x) \cdot \mathbf{c}(x)^{\mathsf{T}} = \mathbf{0}^{\mathsf{T}}$ in $\mathbb{F}_2[x]/(x^N-1)$.

We note the simple technique described in [6] to construct codewords of codes described by polynomial parity-check matrices, which extends a codeword construction technique by MacKay and Davey [5, Theorem 2].

Lemma 1. *Let $\mathcal{C}$ be the QC code defined by the $n_c \times n_v$ polynomial parity-check matrix $H(x)$ over $\mathbb{F}_2[x]/(x^N-1)$. Let $\mathcal{S}$ be an arbitrary size-(n_c+1) subset of $[n_v]$ and let $\mathbf{c}(x) = \big(c_1(x), c_2(x), \ldots, c_{n_v}(x)\big)$ be a length-n_v vector defined by*

$$c_i(x) \triangleq \begin{cases} \det{}^{\mathsf{T}}\left(H_{\mathcal{S}\setminus i}(x)\right) = \Delta_{\mathcal{S}\setminus i} & \text{if } i \in \mathcal{S} \\ 0 & \text{otherwise} \end{cases}.$$

Then $\mathbf{c}(x)$ is a codeword in $\mathcal{C}$.[1]

We also note the following bound from [6] based on the codewords created with Lemma 1:

$$d_{\min}(\mathcal{C}) \le \min_{\substack{\mathcal{S}\subseteq[n_v] \\ |\mathcal{S}|=n_c+1}}{}^{*} \sum_{i\in\mathcal{S}} \operatorname{wt} \Delta_{\mathcal{S}\setminus i} \tag{1}$$

where $\min^*$ takes the minimum positive value of a set.

III. A GENERATOR MATRIX FOR A QC CODE GIVEN BY H

This section, and the two theorems within, give an alternative approach to the method in [13] to compute the rank of H by computing full minors of the polynomial matrix $H(x)$. Moreover, it provides both a sparse generator matrix and a systematic generator matrix for the associated code $\mathcal{C}$. This method also yields the known upper bounds on the minimum distance of the code $\mathcal{C}$, see [6].

A. Case of $n_cN \times n_vN$ matrices H of full rank n_cN

Theorem 2. *Let H be the $n_cN \times n_vN$ parity-check matrix of a QC code $\mathcal{C}$ and let $H(x)$ be its corresponding polynomial parity-check matrix over $\mathbb{F}_2[x]/(x^N-1)$.*

If there exists a subset $\mathcal{S}$ of size n_c of $[n_v]$, and for simplicity and w.l.o.g. we assume that $\mathcal{S} = [n_c]$, such that $\Delta_{\mathcal{S}} = \det\big(H_{\mathcal{S}}(x)\big)$ is invertible in $\mathbb{F}_2[x]/(x^N-1)$, then

1) $\operatorname{rank}(H) = n_cN$, *i.e., H has full rank.*
2) *$H(x)$ is equivalent*[2] *to the $n_c \times n_v$ matrix*

$$\left[\begin{array}{c|ccc} \operatorname{diag}_{n_c}(\Delta_{\mathcal{S}}) & \Delta_{S_1\setminus 1} & \cdots & \Delta_{S_m\setminus 1} \\ & \vdots & & \vdots \\ & \Delta_{S_1\setminus n_c} & \cdots & \Delta_{S_m\setminus n_c} \end{array}\right] \sim$$

$$\left[\begin{array}{c|ccc} I_{n_c\times n_c} & \Delta_{S_1\setminus 1}\Delta_{\mathcal{S}}^{-1} & \cdots & \Delta_{S_m\setminus 1}\Delta_{\mathcal{S}}^{-1} \\ & \vdots & & \vdots \\ & \Delta_{S_1\setminus n_c}\Delta_{\mathcal{S}}^{-1} & \cdots & \Delta_{S_m\setminus n_c}\Delta_{\mathcal{S}}^{-1} \end{array}\right],$$

where $S_i = S \cup \{n_c+i\}$, for all $1 \le i \le m$, $m \triangleq n_v - n_c$, $\Delta_{S_i\setminus j} \triangleq \det\big(H_{S_i\setminus j}(x)\big)$, for all $1 \le j \le n_c$, the matrix $I_{n_c\times n_c}$ is the identity matrix of size $n_c \times n_c$, and $\operatorname{diag}_{n_c}(\Delta_{\mathcal{S}})$ is a diagonal $n_c \times n_c$ matrix with each diagonal entry equal to $\Delta_{\mathcal{S}}$.

3) *The $(n_v - n_c) \times n_v$ matrices $G(x)$ below are two equivalent generator polynomial matrices for $\mathcal{C}$:*

$$\left[\begin{array}{ccc|c} (\Delta_{S_1\setminus 1})^{\mathsf{T}} & \cdots & (\Delta_{S_1\setminus n_c})^{\mathsf{T}} & \\ \vdots & & \vdots & \operatorname{diag}_m(\Delta_{\mathcal{S}}) \\ (\Delta_{S_m\setminus 1})^{\mathsf{T}} & \cdots & (\Delta_{S_m\setminus n_c})^{\mathsf{T}} & \end{array}\right] \sim$$

$$\left[\begin{array}{ccc|c} (\Delta_{S_1\setminus 1}\Delta_{\mathcal{S}}^{-1})^{\mathsf{T}} & \cdots & (\Delta_{S_1\setminus n_c}\Delta_{\mathcal{S}}^{-1})^{\mathsf{T}} & \\ \vdots & & \vdots & I_{m\times m} \\ (\Delta_{S_m\setminus 1}\Delta_{\mathcal{S}}^{-1})^{\mathsf{T}} & \cdots & (\Delta_{S_m\setminus n_c}\Delta_{\mathcal{S}}^{-1})^{\mathsf{T}} & \end{array}\right],$$

with notation as above, and where the matrix $I_{m\times m}$ is the identity matrix of size $(n_v - n_c) \times (n_v - n_c)$, and $\operatorname{diag}_m(\Delta_{\mathcal{S}})$ is a diagonal $(n_v - n_c) \times (n_v - n_c)$ matrix with each diagonal entry equal to $\Delta_{\mathcal{S}}$.

Proof: The proof is a relatively straightforward consequence of Lemma 1 and is omitted for space constraints. ■

Remark 3. In Theorem 2, we give two (new) equivalent representations for both $H(x)$ and $G(x)$, the first one both matrices are sparse, while the second, is a systematic representation, both of which could be of interest to design efficient encoding and decoding algorithms. Note that the first representation of $G(x)$ contains the codewords from which the upper bound (1) can be deduced, see also [6], and hence provides a sparse representation that would be amenable to high throughput

[1] The determinant of an $m \times m$-polynomial matrix $B = [b_{j,i}(x)]_{j,i}$ over $\mathbb{F}_2[x]$ is $\det(B) = \sum_\sigma \prod_{j\in[m]} b_{j,\sigma(j)}(x)$, where the summation is over all $m!$ permutations of the set $[m]$. Then $\det^{\mathsf{T}}$ transposes the polynomials, i.e., the exponents are taken with the negative sign modulo N.

[2] By equivalent, we mean that a matrix can be obtained from an equivalent matrix by applying elementary row operations (we call them row equivalent), which would not change its row space nor its null space, and column permutations, which might change these both, leaving invariant all the important parameters of the corresponding code and its Tanner graph.

encoding following approaches such as [1]. The systematic version, as is typical, is not as sparse and, in most cases, the row codewords have weight larger than this upper bound. However, the systematic form may also be of interest, e.g., to avoid the need for encoder inverse operations. □

In the following we give two examples and show how this method of creating sets of codewords based on the full size minors of a $n_c \times (n_c+1)$ submatrix of $H(x)$ can also display codewords of the weight equal to the minimum distance. The upper bound (1) on the minimum distance given by the minimum of the weights of these codewords is relevant because it is shown to be tight.

Example 4. (AR4JA codes) Let $H(x)$ be the polynomial parity-check matrix given by

$$H(x) = \begin{bmatrix} 0 & 0 & 1 & 0 & 1+x \\ 1 & 1 & 0 & 1 & x+x^2+x^3 \\ 1 & x+x^2 & 0 & 1+x^3 & 1 \end{bmatrix}$$

with $N = 4$. The rows of the matrix $G(x)$ below are linearly independent codewords for the code $\mathcal{C}$ given by H, and since $\Delta_{123} = \det(H_{123}) = x^2+x+1$ is irreducible in $\mathbb{F}_2[x]/(x^4+1)$, the matrix $G(x)$ has rank $2N = 8$ and thus, forms a generator matrix for the code $\mathcal{C}$:

$$G(x) = \begin{bmatrix} \Delta_{234}^{\mathsf{T}} & \Delta_{134}^{\mathsf{T}} & \Delta_{124}^{\mathsf{T}} & \Delta_{123}^{\mathsf{T}} & 0 \\ \Delta_{235}^{\mathsf{T}} & \Delta_{135}^{\mathsf{T}} & \Delta_{125}^{\mathsf{T}} & 0 & \Delta_{123}^{\mathsf{T}} \end{bmatrix} =$$

$$\begin{bmatrix} (x+1)^3 & x & 0 & x^3+x^2+1 & 0 \\ x^3+x^2+1 & (x+1)^3 & x+1 & 0 & x^3+x^2+1 \end{bmatrix}.$$

Note that the vectors $(\Delta_{245}^{\mathsf{T}}, \Delta_{145}^{\mathsf{T}}, 0, \Delta_{125}^{\mathsf{T}}, \Delta_{124}^{\mathsf{T}})$, $(\Delta_{345}^{\mathsf{T}}, 0, \Delta_{145}^{\mathsf{T}}, \Delta_{135}^{\mathsf{T}}, \Delta_{134}^{\mathsf{T}})$, $(0, \Delta_{345}^{\mathsf{T}}, \Delta_{245}^{\mathsf{T}}, \Delta_{235}^{\mathsf{T}}, \Delta_{234}^{\mathsf{T}})$, are also codewords, where $\Delta_{145} = \det(H_{145}) = x+1$, $\Delta_{245} = \det(H_{245}) = 0$, and $\Delta_{345} = \det(H_{345}) = x$, but they are linear combinations of the ones displayed in the matrix $G(x)$, so they are not needed for the generator matrix. Displaying them is useful, however, since the nonzero minimum of the weights of the five codewords gives an upper bound on the minimum distance of the code (see (1)), in this case, the codeword $(\Delta_{245}^{\mathsf{T}}, \Delta_{145}^{\mathsf{T}}, 0, \Delta_{125}^{\mathsf{T}}, \Delta_{124}^{\mathsf{T}}) = (0, x+1, 0, x+1, 0)$ has weight 4, which is in fact the minimum distance of the code; this code has parameters $[20, 8, 4]$.

Multiplying the two rows of G by $(x^3+x^2+1)^{-1} = x^2+x+1$ gives a generator matrix in standard form,

$$G(x) = \begin{bmatrix} x^3+x^2+x+1 & x^3+x^2+x & 0 & 1 & 0 \\ 1 & x^3+x^2+x+1 & x^3+1 & 0 & 1 \end{bmatrix},$$

while

$$H(x) = \begin{bmatrix} 1 & 0 & 0 & x^3+x^2+x+1 & 1 \\ 0 & 1 & 0 & x+x^2+x^3 & x^3+x^2+x+1 \\ 0 & 0 & 1 & 0 & x+1 \end{bmatrix}$$

is a polynomial parity-check matrix in systematic form. □

We exemplify the method also on a $4N \times 8N$, $N = 16$, irregular matrix.

Example 5. Let $H_{(128,64)}$, shown below, be the $4N \times 8N$, $N = 16$, protograph-based matrix of the $[128, 64, 14]$ irregular, multi-edge protograph specified by the NASA Consultative Committee for Space Data Systems (CCSDS) [16], [18]:

$$\left[\begin{array}{cccc|cccc} 1+x^7 & x^2 & x^{14} & x^6 & 0 & 1 & x^{13} & 1 \\ x^6 & 1+x^{15} & 1 & x & 1 & 0 & 1 & x^7 \\ x^4 & x & 1+x^{15} & x^{14} & x^{11} & 1 & 0 & x^3 \\ 1 & x & x^9 & 1+x^{13} & x^{14} & x & 1 & 0 \end{array}\right],$$

Let $\mathcal{S} = \{5, 6, 7, 8\}$. We use the notation $\Delta_{abcd} = \det(H_{\{a,b,c,d\}})$ and compute $\Delta_{5678} = x^{14}+x^{12}+x^3$, which is invertible in $\mathbb{F}_2[x]/(x^{16}+1)$, since $x^{16}+1 = (x+1)^{16}$ has only $(x+1)$ as irreducible factor in $\mathbb{F}_2[x]$. We compute $\Delta_{5678}^{-1} = (x^{14}+x^{12}+x^3)^{-1} = x^{13}+x^{12}+x^{11}+x^{10}+x^9+x^8+x^7+x+1$, so that we can compute the values $\delta_{abcd} \triangleq \Delta_{abcd}(\Delta_{\mathcal{S}})^{-1}$ that appear in the the systematic parity-check matrix $H'(x)$ and the systematic generator matrix $G(x)$ given as

$$H'(x) \triangleq \left[\begin{array}{cccc|c} \delta_{1678} & \delta_{2678} & \delta_{3678} & \delta_{4678} & \\ \delta_{1578} & \delta_{2578} & \delta_{3578} & \delta_{4578} & I_{4\times 4} \\ \delta_{1568} & \delta_{2568} & \delta_{3568} & \delta_{4568} & \\ \delta_{1567} & \delta_{2567} & \delta_{3567} & \delta_{4567} & \end{array}\right],$$

$$G(x) \triangleq \left[\begin{array}{c|cccc} & \delta_{1678}^{\mathsf{T}} & \delta_{1578}^{\mathsf{T}} & \delta_{1568}^{\mathsf{T}} & \delta_{1567}^{\mathsf{T}} \\ & \delta_{2678}^{\mathsf{T}} & \delta_{2578}^{\mathsf{T}} & \delta_{2568}^{\mathsf{T}} & \delta_{2567}^{\mathsf{T}} \\ I_{4\times 4} & \delta_{3678}^{\mathsf{T}} & \delta_{3578}^{\mathsf{T}} & \delta_{3568}^{\mathsf{T}} & \delta_{3567}^{\mathsf{T}} \\ & \delta_{4678}^{\mathsf{T}} & \delta_{4578}^{\mathsf{T}} & \delta_{4568}^{\mathsf{T}} & \delta_{4567}^{\mathsf{T}} \end{array}\right],$$

$$\begin{aligned}
\delta_{1678} &= x^{12}+x^{11}+x^{10}+x^7+x^6+x^4+x, \\
\delta_{1578} &= x^{13}+x^{11}+x^{10}+x^7+x^6+x^4+x^2+x, \\
\delta_{1568} &= (x+1)(x^{14}+x^{11}+x^9)+(x^4+1)(x^3+1), \\
\delta_{1567} &= x^{12}+x^{10}+x^9+x^8+x^7+x^2, \\
\delta_{2678} &= (x+1)(x^{14}+x^{12}+x^{11}+x^9+x^6+x^2), \\
\delta_{2578} &= x^{13}+x^{10}+x^9+x^7+x^6+x^5+x^4+x^3+x^2, \\
\delta_{2568} &= x^{14}+x^{13}+x^{12}+x^{10}+x^9+x^6+x^3+1, \\
\delta_{2567} &= x^{11}+x^5+x^4+1, \ \delta_{3678} = x^{15}+x^{11}+x^8+1, \\
\delta_{3578} &= (x+1)(x^{14}+x^{12}+x^{10}+x^7+x^6+x^4+1), \\
\delta_{3568} &= x^{15}+x^{12}+x^{11}+x^9+x^7+x^5+x^2+x+1, \\
\delta_{3567} &= x^{14}+x^{11}+x^{10}+x^9+x^5+x^2+x+1, \\
\delta_{4678} &= x^{15}+x^{12}+x^{11}+x^{10}+x^8+x^6+x^4+x^2, \\
\delta_{4578} &= x^{14}+x^{10}+x^8+x^7+x^6+x^5+x^4+x^2, \\
\delta_{4568} &= x^{15}+x^{11}+x^{10}+x^7+x^5+x^4+x^3+x^2, \\
\delta_{4567} &= x^{15}+x^{14}+x^{12}+x^{10}+x^5+x+1,
\end{aligned}$$

where $\delta_{abcd}^{\mathsf{T}}$ is the transpose of δ_{abcd}, which changes the exponents to their negatives modulo N.

A sparser but "systematic-like" generator matrix is, however, the following,

$$G' \triangleq \left[\begin{array}{c|cccc} & \Delta_{1678}^{\mathsf{T}} & \Delta_{1578}^{\mathsf{T}} & \Delta_{1568}^{\mathsf{T}} & \Delta_{1567}^{\mathsf{T}} \\ & \Delta_{2678}^{\mathsf{T}} & \Delta_{2578}^{\mathsf{T}} & \Delta_{2568}^{\mathsf{T}} & \Delta_{2567}^{\mathsf{T}} \\ \mathrm{diag}_4(\Delta_{5678}^{\mathsf{T}}) & \Delta_{3678}^{\mathsf{T}} & \Delta_{3578}^{\mathsf{T}} & \Delta_{3568}^{\mathsf{T}} & \Delta_{3567}^{\mathsf{T}} \\ & \Delta_{4678}^{\mathsf{T}} & \Delta_{4578}^{\mathsf{T}} & \Delta_{4568}^{\mathsf{T}} & \Delta_{4567}^{\mathsf{T}} \end{array}\right],$$

with a corresponding "systematic-like" parity-check matrix

$$H'' \triangleq \left[\begin{array}{cccc|c} \Delta_{1678} & \Delta_{2678} & \Delta_{3678} & \Delta_{4678} & \\ \Delta_{1578} & \Delta_{2578} & \Delta_{3578} & \Delta_{4578} & \mathrm{diag}_4(\Delta_{5678}) \\ \Delta_{1568} & \Delta_{2568} & \Delta_{3568} & \Delta_{4568} & \\ \Delta_{1567} & \Delta_{2567} & \Delta_{3567} & \Delta_{4567} & \end{array}\right],$$

$$\begin{aligned}
\Delta_{5678} &= x^{14}+x^{12}+x^3, \quad \Delta_{1678} = x^{14}+x^6+x^5+x^3+1, \\
\Delta_{1578} &= x^{15}+x^{11}+x^{10}+x^9+x^8+x^6+x^3+1, \\
\Delta_{1568} &= x^{12}+x^{11}+x^{10}+x^9+x^7+1, \\
\Delta_{1567} &= (x+1)(x^{14}+x^{12}+x^4)+x^{11}+x^7+x^3+1, \\
\Delta_{2678} &= x^{15}+x^9+x^8+x^5+x^4+x^3,
\end{aligned}$$

$$\Delta_{2578} = (x+1)(x^{14}+x^{12}+x^{10}+x^4)+1,$$
$$\Delta_{2568} = (x^2+1)(x^{12}+x^{11}+x^5+x^2+x)+x+1,$$
$$\Delta_{2567} = x^{12}+x^9+x^8+x^2+x+1,$$
$$\Delta_{3678} = x^{13}+x^{12}+x^9+x^7+x^6+x^4+x^3+x^2,$$
$$\Delta_{3578} = x^{13}+x^{11}+x^9+x^8+x^4+x^2,$$
$$\Delta_{3568} = x^{14}+x^{11}+x^9+(x+1)(x^4+x^2+1),$$
$$\Delta_{3567} = x^{15}+x^{14}+x^{12}+x^{10}+x^9+x^6+x^4+1,$$
$$\Delta_{4678} = x^{15}+x^{10}+x^5+x^2, \Delta_{4568} = x^{15}+x^{11}+x^{10}+x^9,$$
$$\Delta_{4578} = x^{14}+x^{13}+x^{12}+x^{11}+x^9+x^7,$$
$$\Delta_{4567} = x^{14}+x^{13}+x^{11}+x^8+x^6+x^4+x^2.$$

The rows of the matrix $G'(x)$ represent codewords of weight that equal the upper bound on the minimum distance from (1). The last row, for example, gives $d_{\min}(\mathcal{C}) \leq 24$.

If instead we take $\mathcal{S} = \{1,5,6,8\}$, the polynomial $\Delta_{1578} = x^{15}+x^{11}+x^{10}+x^9+x^8+x^6+x^3+1$ is not invertible in $\mathbb{F}_2[x]/(x^{16}+1)$, so we cannot obtain the identity matrix. □

B. Case of $n_cN \times n_vN$ rank deficient matrices H

This section considers the case in which, for any subset $\mathcal{S}$ of size n_c of $[n_v]$, $\Delta_{\mathcal{S}} \triangleq \det\big(H_{\mathcal{S}}(x)\big)$ is not invertible. Let $\mathcal{S}$ be a subset of size n_c of $[n_v]$ such that $\gcd\big(\Delta_{\mathcal{S}}, x^N+1\big) = d(x) \neq 1$ in $\mathbb{F}_2[x]$ and supposed that $d(x)$ divides $\Delta_{\mathcal{T}}$ for all subsets $\mathcal{T}$ of size n_c of $[n_v]$. For simplicity and w.l.o.g., we assume that $\mathcal{S} = [n_c]$.

In this case, we can still construct the matrix G_1 of codewords similar to the one formed in Section III-A:

$$G_1 \triangleq \left[\begin{array}{ccc|c} \Delta^{\mathsf{T}}_{S_1\setminus 1} & \Delta^{\mathsf{T}}_{S_1\setminus 2} & \cdots & \Delta^{\mathsf{T}}_{S_1\setminus n_c} \\ \vdots & \vdots & & \vdots \\ \Delta^{\mathsf{T}}_{S_m\setminus 1} & \Delta^{\mathsf{T}}_{S_m\setminus 2} & \cdots & \Delta^{\mathsf{T}}_{S_m\setminus n_c} \end{array} \middle| \; \operatorname{diag}(\Delta^{\mathsf{T}}_{\mathcal{S}}) \right].$$

However, unlike the case in which $\Delta_{\mathcal{S}}$ is invertible, this matrix does not generate the entire code $\mathcal{C}$, but only a subcode of $\mathcal{C}$ because its rank is lower that the dimension of the code. In this case, we will need to add to this matrix a few rows of "obvious" codewords to increase the rank. We exemplify this on the famous $[155, 64, 20]$ Tanner code below.

Example 6. ($[155, 64, 20]$ Tanner code) Let

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

All 3×3 minors and $X^{31}+1$ have common factor $(x+1)$, so $H(x)$ does not have any irreducible 3×3 submatrix $H_{\mathcal{S}}$.

Let $\mathcal{S} = \{1,2,3\}$, and $\Delta_{123} \triangleq \det(H_{123}) = x^{28}+x^{18}+x^{16}+x^{14}+x^9+x^8$. The matrix

$$\begin{bmatrix} \Delta_{234} & \Delta_{134} & \Delta_{124} & \Delta_{123} & 0 \\ \Delta_{235} & \Delta_{135} & \Delta_{125} & 0 & \Delta_{123} \end{bmatrix},$$

$$\Delta_{234} = \det(S_{234}) = x^{28}+x^{25}+x^{18}+x^{16}+x^5+x,$$
$$\Delta_{134} = \det(S_{134}) = x^{23}+x^{22}+x^{20}+x^{17}+x^7+x^4,$$
$$\Delta_{124} = \det(S_{124}) = x^{29}+x^{25}+x^{21}+x^{12}+x^5+x,$$
$$\Delta_{123} = \det(S_{123}) = x^{28}+x^{18}+x^{16}+x^{14}+x^9+x^8,$$
$$\Delta_{235} = \det(S_{235}) = x^{27}+x^{24}+x^{19}+x^{11}+x^{10}+x^2,$$
$$\Delta_{135} = \det(S_{135}) = x^{30}+x^{28}+x^{26}+x^{18}+x^{16}+x^6,$$
$$\Delta_{125} = \det(S_{125}) = x^{20}+x^{14}+x^9+x^8+x^7+x^4,$$

is a matrix of two codewords. It has rank 60, so it only generates a subcode of $\mathcal{C}$ (of the same minimum distance 20). To increase its rank and, thus, obtain a full generator matrix, we need to add some linearly independent codewords to this matrix. One would hope that the entire matrix of codewords

$$\begin{bmatrix} \Delta_{234} & \Delta_{134} & \Delta_{124} & \Delta_{123} & 0 \\ \Delta_{235} & \Delta_{135} & \Delta_{125} & 0 & \Delta_{123} \\ \Delta_{245} & \Delta_{145} & 0 & \Delta_{125} & \Delta_{124} \\ \Delta_{345} & 0 & \Delta_{145} & \Delta_{135} & \Delta_{134} \\ 0 & \Delta_{345} & \Delta_{245} & \Delta_{235} & \Delta_{234} \end{bmatrix},$$

$$\Delta_{245} = \det(S_{245}) = x^{15}+x^{14}+x^{13}+x^9+x^8+x^3,$$
$$\Delta_{145} = \det(S_{145}) = x^{20}+x^{19}+x^{10}+x^7+x^4+x^2,$$
$$\Delta_{345} = \det(S_{345}) = x^{25}+x^{19}+x^{10}+x^5+x^2+x,$$

has the correct rank, but this is not the case since three of the 5 codewords above are linear combinations of the remaining two, and the rank of the matrix above is still 60 over $\mathbb{F}_2$. Although these 3 codewords are not necessary to construct a generator matrix, displaying them is useful, nonetheless, since they give the known upper bound on the minimum distance (1), $d_{\min}(C) \leq 4\cdot 6 = 24$, see [6].

However, the matrix

$$G = \begin{bmatrix} \Delta_{234} & \Delta_{134} & \Delta_{124} & \Delta_{123} & 0 \\ \Delta_{235} & \Delta_{135} & \Delta_{125} & 0 & \Delta_{123} \\ f & f & 0 & 0 & 0 \\ f & 0 & f & 0 & 0 \\ f & 0 & 0 & f & 0 \\ f & 0 & 0 & 0 & f \end{bmatrix},$$

where $f = 1+x+x^2+\cdots+x^{30}$, has the correct rank 64, and its rows are codewords for the code given by H. Therefore, it is a generator matrix for the $[155, 64, 20]$ Tanner code.

This generator matrix is sparse and in "systematic-like" form. We can make it more systematic in the following way. Since $\gcd(\Delta_{123}, f) = 1$, over the polynomial ring $\mathbb{F}_2[x]$, there exist $A(x), B(x) \in \mathbb{F}_2[x]$,

$$A = (x^3+1)(x^{25}+x^5)+(x+1)(x^{18}+x^{15}+x^{14}+x^9+x)$$
$$B = (x+1)(x^{25}+x^{22}+x^{16}+x^{12}+x^{10}+1)+x^9,$$

such that $A(x)\cdot\Delta_{123} + B(x)\cdot f = \gcd(\Delta_{123}, f) = 1$.

Adding the first row of G multiplied by A with the fifth row of G, and adding the second row of G multiplied by A with the sixth row of G, we obtain

$$G_1 \triangleq \begin{bmatrix} A_{11} & A_{12} & A_{13} & 1 & 0 \\ A_{21} & A_{22} & A_{23} & 0 & 1 \\ f & f & 0 & 0 & 0 \\ f & 0 & f & 0 & 0 \end{bmatrix}, \text{ where}$$

$$A_{11} = x^{28}+x^{18}+x^{16}+x^{14}+x^9+x^8,$$
$$A_{12} = (x+1)(x^{22}+x^{16}+x^{15}+x^{13}+x^8+x^2+x+1),$$
$$A_{13} = x^{29}+x^{25}+x^{21}+x^{20}+x^{12}+x^7+x^5+x^4+x,$$
$$A_{21} = x^{30}+x^{13}+x^{10}+(x+1)[(x^6+1)(x^{19}+x^{16}+1)+x^{15}],$$
$$A_{22} = x^{29}+x^{27}+x^{25}+x^{24}+x^{21}+x^{20}+x^{19}+x^{12}+x^{11}+$$
$$x^{10}+x^7+x^5+x^4+x^2+x+1,$$
$$A_{23} = (x^3+1)(x^{25}+x^5+x)+(x^2+1)(x^{18}+x^{14}+x^7).$$

□

The following theorem gives the formula for the rank over $\mathbb{F}_2$ of a scalar matrix using the computation of the degree of the minors of the corresponding polynomial matrix.

Theorem 7. *Let H be a $n_cN \times n_vN$ matrix over $\mathbb{F}_2$ and $H(x)$ be the corresponding $n_c \times n_v$ polynomial matrix. For all $i \in [n_c]$, we define the following in $\mathbb{F}_2[x]$:*

$$\gamma_i(x) \triangleq \gcd\{\Delta_{\mathcal{I},\mathcal{J}}(H(x) \mid |\mathcal{I}| = |\mathcal{J}| = i\}, \gamma_0 \triangleq 1,$$
$$d_i(x) \triangleq \gcd(\gamma_i/\gamma_{i-1}, x^N + 1), \text{ where}$$
$$\gcd(0/0, x^N + 1) \triangleq \gcd(0, x^N + 1) = x^N + 1. \text{ Then,}$$
$$\operatorname{rank}_{\mathbb{F}_2}(H) = n_c \cdot N - \sum_{i=1}^{n_c} \deg d_i(x) \Rightarrow$$
$$\dim(\mathcal{C}) = (n_v - n_c) \cdot N + \sum_{i=1}^{n_c} \deg d_i(x).$$

Proof: In $\mathbb{F}_2[x]$, $H(x)$ is equivalent (after elementary row and column operations that leave its rank invariant) to its Smith normal form

$$\left[\begin{array}{c|c} \operatorname{diag}(\frac{\gamma_1}{\gamma_0}(x), \frac{\gamma_2}{\gamma_1}(x), \ldots, \frac{\gamma_{n_c}}{\gamma_{n_c-1}}(x)) & 0_{n_c \times (n_v - n_c)} \end{array} \right].$$

Taking the gcd of the entries with (x^N+1), we obtain a matrix equivalent to $H(x)$ in $\mathbb{F}_2[x]/(x^N+1)$, therefore, the rank over $\mathbb{F}_2$ of the $n_cN \times n_vN$ matrix H is equal to the sum of the ranks of the circulant matrices associated to $d_i(x)$. ∎

Example 8. Let $H(x) \triangleq$

$$\begin{bmatrix} 1+x^2 & 1+x^4 & 1+x^6 & 1+x^8 & 1+x^{16} \\ x^4+x^{12} & x^{20}+x^{22} & x^{30}+x^{42} & x^{40}+x^{14} & 1+x^{50} \\ 1+x^4 & x^{30}+x^{24} & x^{12}+x^{14} & x^3+x^{13} & x+x^9 \end{bmatrix}$$

be a 3×5 polynomial matrix in $\mathbb{F}_2[x]$. Depending on N, its Tanner graph can have girth 6. We will keep N variable, and compute the rank of the $3N \times 5N$ matrix H obtained from $H(x)$ in the ring $\mathbb{F}_2[x]/(x^N + 1)$. We obtain (the following include relevant Magma commands):

$$\gamma_i \triangleq \text{GCD}(\text{Minors}(H, i)), \text{ in } \mathbb{F}_2[x],$$
$$\gamma_0 \triangleq 1, \gamma_1 = (x+1)^2, \gamma_2 = (x+1)^4, \gamma_3 = (x+1)^6,$$
$$\frac{\gamma_1}{\gamma_0} = \frac{\gamma_2}{\gamma_1} = \frac{\gamma_3}{\gamma_2} = x^2 + 1, \text{ so, for all } 1 \le i \le 3,$$
$$d_i = \gcd(x^2+1, x^N+1) = \begin{cases} x^2+1 & \text{if } N \text{ even} \\ x+1 & \text{if } N \text{ odd} \end{cases} \Longrightarrow$$
$$\operatorname{rank}(H) = 3(N - \deg(d_i)) = \begin{cases} 3N-6 & \text{if } N \text{ even} \\ 3N-3 & \text{if } N \text{ odd} \end{cases}.$$

Therefore, the same matrix gives a code of larger dimension if N is even. For example, $N = 44$, gives H of rank 128, and the code of dimension 92, while $N = 45$ gives a slightly longer code that has the same dimension 92. □

We end with a theorem that shows how to obtain an equivalent upper triangular form for $H(x)$ and thus, to provide an alternative proof to Theorem 7.[3] The proof is based on simple computations of determinants.

Theorem 9. *Let $H(x) = (h_{ij})_{i,j}$ by an $n_c \times n_v$ polynomial matrix. We assume, w.l.o.g, that $\gcd(\frac{\Delta_{[i],[i]}}{\gamma_i}, x^N + 1) = 1$, for all $i \in [n_c]$.[4] Then, $H(x)$ is equivalent to the upper triangular matrix*

$$\begin{bmatrix} h_{11} & h_{12} & \cdots & h_{1n_c} & \cdots & h_{1n_v} \\ 0 & \frac{\Delta_{[2],[2]}}{\gamma_1} & \cdots & \frac{\Delta_{[2],1n_c}}{\gamma_1} & \cdots & \frac{\Delta_{[2],1n_v}}{\gamma_1} \\ 0 & 0 & \cdots & \frac{\Delta_{[3],12n_c}}{\gamma_2} & \cdots & \frac{\Delta_{[3],12n_v}}{\gamma_2} \\ \vdots & \vdots & & \vdots & & \vdots \\ 0 & 0 & \cdots & \frac{\Delta_{[n_c],[n_c]}}{\gamma_{n_c-1}} & \cdots & \frac{\Delta_{[n_c],[n_c-1]\cup n_v}}{\gamma_{n_c-1}} \end{bmatrix},$$

where the determinants and the divisions are performed in $\mathbb{F}_2[x]$ first, followed by the modular operation $\mod (x^N+1)$.

Example 10. Let $H(x)$ be the polynomial parity-check matrix of Example 6. We compute $\gamma_1 = 1$, $d_1 = 1$, and $d_2 = d_3 = x + 1$, so the rank over $\mathbb{F}_2$ of H is 91. The matrix $H_1(x)$ below gives the same $[155, 64, 20]$ code as $H(x)$:[5]

$$H_1(x) \triangleq \begin{bmatrix} x & x^2 & x^4 & x^8 & x^{16} \\ 0 & x^{10}+x^6 & x^{20}+x^8 & x^{12}+x^9 & x^{20}+x^{18} \\ 0 & 0 & \frac{\Delta_{[3],123}}{x+1} & \frac{\Delta_{[3],124}}{x+1} & \frac{\Delta_{[3],125}}{x+1} \end{bmatrix},$$
$$\Delta_{[3],123} = x^{47} + x^{40} + x^{39} + x^{28} + x^{18} + x^{14},$$
$$\Delta_{[3],124} = x^{43} + x^{36} + x^{32} + x^{29} + x^{25} + x^{21},$$
$$\Delta_{[3],125} = x^{51} + x^{45} + x^{40} + x^{39} + x^{38} + x^{35},$$
$$\frac{\Delta_{[3],123}}{x+1} \bmod x^{31} + 1 = x^{30} + x^{29} + x^{28} + x^{17} + x^{16} + x^{13} +$$
$$x^{12} + x^{11} + x^{10} + x^9 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1,$$
$$\frac{\Delta_{[3],124}}{x+1} \bmod x^{31} + 1 = x^{30} + x^{29} + x^{24} + x^{23} + x^{22} + x^{21} +$$
$$x^{11} + x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + 1,$$
$$\frac{\Delta_{[3],125}}{x+1} \bmod x^{31} + 1 = x^{19} + x^{18} + x^{17} + x^{16} + x^{15} + x^{14} +$$
$$x^8 + x^6 + x^5 + x^4.$$

Note that there could be N for which simpler equivalent triangular forms can be obtained. For values N for which

$$\gcd\left(\frac{\Delta_{[i],[i]}}{\gamma_{i-1}}, x^N + 1\right) = \gcd\left(\delta_{[i],[i]}, x^N + 1\right),$$

where $\delta_{\mathcal{I},\mathcal{J}} \triangleq \Delta_{\mathcal{I},\mathcal{J}} \mod x^N+1$, the denominator γ_{i-1} can be dropped in Theorem 9. For example, the matrix $H_2(x)$ below gives also the same $[155, 64, 20]$ code as $H(x)$, for $N = 31$:

$$H_2(x) \triangleq \begin{bmatrix} x & x^2 & x^4 & x^8 & x^{16} \\ 0 & x^{10}+x^6 & x^{20}+x^8 & x^{12}+x^9 & x^{20}+x^{18} \\ 0 & 0 & \delta_{[3],123} & \delta_{[3],124} & \delta_{[3],125} \end{bmatrix},$$

where $\delta_{[3],12i} \triangleq \Delta_{[3],12i} \mod x^{31} + 1$ for all $i \in \{3, 4, 5\}$. □

IV. Concluding remarks

This paper shows how to obtain a generator matrix for an LDPC code using minors of the polynomial parity-check matrix. The resulting matrices can be presented in several forms that may facilitate efficient encoder implementation as well as minimum distance analysis. Moreover, the approach was shown to provide a formula for the dimension of any QC-LDPC code based on the minors of its polynomial parity-check matrix.

[3] Note that [13] only addresses the $n_c = 3$ case.

[4] We perform elementary row and column permutations to obtain this form.

[5] Note that we can also compute the rank over $\mathbb{F}_2$ of H from the equivalent form H_1.

REFERENCES

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

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

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

[4] R. M. Tanner, D. Sridhara, A. Sridharan, T. E. Fuja, and D. J. Costello, Jr., "LDPC block and convolutional codes based on circulant matrices," *IEEE Transactions on Information Theory*, vol. 50, no. 12, pp. 2966–2984, Dec. 2004.

[5] D. J. C. MacKay and M. C. Davey, "Evaluation of Gallager codes for short block length and high rate applications," in *IMA Volumes in Mathematics and its Applications, Vol. 123: Codes, Systems, and Graphical Models*. Springer-Verlag, 2001, pp. 113–130.

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

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

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

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

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

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

[12] K. Liu, Q. Huang, S. Lin, and K. Abdel-Ghaffar, "Quasi-cyclic LDPC codes: Construction and rank analysis of their parity-check matrices," in *2012 Information Theory and Applications Workshop*, 2012, pp. 227–233.

[13] P.-C. Yang, C.-H. Wang, and C.-C. Chao, "Rank analysis of parity-check matrices for quasi-cyclic ldpc codes," in *2018 IEEE International Symposium on Information Theory (ISIT)*, 2018, pp. 491–495.

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

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

[16] D. Divsalar, S. Dolinar, C. Jones, and K. Andrews, "Capacity-approaching protograph codes," *IEEE Journal on Selected Areas in Communications*, vol. 27, no. 6, pp. 876–888, Aug. 2009.

[17] K. Lally and P. Fitzpatrick, "Algebraic structure of quasicyclic codes," *Disc. Appl. Math. Trans. Inform. Theory*, vol. 111, pp. 157–175, 2001.

[18] *Short blocklength LDPC codes for TC synchronization and channel coding*, The Consultative Committee for Space Data Systems Orange Book, 2012.