Spectral Graph Analysis of Quasi-Cyclic Codes

Roxana Smarandache
Department of Mathematics and Statistics
San Diego State University
San Diego, CA 92182, USA
Email: rsmarand@sciences.sdsu.edu

Mark F. Flanagan
Department of Electronic Engineering
University College Dublin
Belfield, Dublin 4, Ireland
Email: mark.flanagan@ieee.org

***Abstract*—In this paper we analyze the bound on the additive white Gaussian noise channel (AWGNC) pseudo-weight of a (c, d)-regular linear block code based on the two largest values $\lambda_1 > \lambda_2$ of the eigenvalues of $\mathbf{H}^\mathsf{T}\mathbf{H}$: $w_\mathrm{p}^{\min}(\mathbf{H}) \geqslant n\frac{2c-\lambda_2}{\lambda_1-\lambda_2}$. [6]. In particular, we analyze (c, d)-regular quasi-cyclic (QC) codes of length rL described by $J \times L$ block parity-check matrices with circulant block entries of size $r \times r$. We proceed by showing how the problem of computing the eigenvalues of the $rL \times rL$ matrix $\mathbf{H}^\mathsf{T}\mathbf{H}$ can be reduced to the problem of computing eigenvalues for r matrices of size $L \times L$. We also give a necessary condition for the bound to be attained for a circulant matrix H and show a few classes of cyclic codes satisfying this criterion.**

***Index Terms*—Low-density parity-check codes, pseudo-codewords, pseudo-weights, eigenvalues, eigenvectors.**

I. Introduction

Low-density parity-check (LDPC) codes offer excellent tradeoffs between performance and complexity for error correction in communication systems. Quasi-cyclic (QC) LDPC codes in particular have proved extremely attractive due to their implementation advantages, both in encoding and decoding [1], [2], [3]. Many analyses of QC-LDPC codes have been carried out based on optimization of parameters such as the minimum Hamming distance of the code or the girth of the Tanner graph. However, it has been shown that an excellent first-order measure of performance over the AWGNC is the minimum *pseudo-weight* of the code [4]. So far, few results exist in the literature on the minimum pseudo-weight of QC-LDPC and related codes.

Spectral graph analysis was used in [5], and more recently, in [6], to obtain bounds on the minimum Hamming weight, and minimum AWGNC pseudo-weight, respectively, of a length-n (c, d)-regular code $\mathcal{C}$ over the binary field $\mathbb{F}_2$:

$$d_{\min} \geqslant w_\mathrm{p}^{\min}(\mathbf{H}) \geqslant n\frac{2c-\lambda_2}{\lambda_1-\lambda_2}; d_{\min} \geqslant n\frac{2}{d}\frac{2c+d-2-\lambda_2}{\lambda_1-\lambda_2},$$

with $\lambda_1 > \cdots > \lambda_s$ being the distinct ordered eigenvalues of $\mathbf{H}^\mathsf{T}\mathbf{H} \in \mathbb{R}^{n\times n}$ (where $\mathbf{H}$ is viewed as a matrix in $\mathbb{R}^{m\times n}$). These bounds are, for most codes, loose. However, in particular cases, like the projective geometry codes [7], [8], [9], they are attained. A current problem with these bounds is that for most LDPC codes, it is not practical to evaluate the eigenvalues λ_1, λ_2 due to the size of the matrix $\mathbf{H}^\mathsf{T}\mathbf{H}$.

In this paper we show how to compute the AWGN pseudo-weight lower bound for quasi-cyclic (QC) and related codes by utilizing the $\mathcal{A}$-submodule structure of quasi-cyclic codes, $\mathcal{A} = \mathbb{R}[X]/(X^r - 1)$ [10], [11], [12]. In particular, we begin by showing how the polynomial parity-check matrix that describes a cyclic code can be used to compute the required eigenvalues, and then generalize this approach to compute the required eigenvalues for QC codes. We also define the class of "nested circulant" matrices, and show that these have eigenvalues which are given by evaluating a multivariate associated polynomial at points whose coordinates are particular roots of unity. Finally, we give a necessary condition for the pseudo-weight lower bound to be attained when $\mathbf{H}$ is circulant and show a few classes of cyclic codes satisfying this criterion.

II. Basic Notation and Definitions

All codes in this paper will be binary linear codes of a certain length n specified through a (scalar) parity-check matrix $\mathbf{H} = (h_{j,i}) \in \mathbb{F}_2^{m\times n}$ as the set of all vectors $\mathbf{c} \in \mathbb{F}_2^n$ such that $\mathbf{H} \cdot \mathbf{c}^\mathsf{T} = \mathbf{0}^\mathsf{T}$, where $^\mathsf{T}$ denotes transposition. The minimum Hamming distance of a code $\mathcal{C}$ will be denoted by $d_{\min}(\mathcal{C})$. The fundamental cone $\mathcal{K}(\mathbf{H})$ of $\mathbf{H}$ is the set of all vectors $\boldsymbol{\omega} \in \mathbb{R}^n$ that satisfy

$$\omega_i \geqslant 0 \qquad \text{for all } i \in \mathcal{I}(\mathbf{H}) , \tag{1}$$

$$\omega_i \leqslant \sum_{i' \in \mathcal{I}_j(\mathbf{H})\setminus i} \omega_{i'} \text{ for all } j \in \mathcal{J}(\mathbf{H}),\ \ i \in \mathcal{I}_j(\mathbf{H}) , \tag{2}$$

where $\mathcal{J}(\mathbf{H})$ and $\mathcal{I}(\mathbf{H})$ denote the sets of row and column indices of $\mathbf{H}$ respectively, and $\mathcal{I}_j(\mathbf{H}) \triangleq \{i \in \mathcal{I} \mid h_{j,i} = 1\}$ for each $j \in \mathcal{J}(\mathbf{H})$. A vector $\boldsymbol{\omega} \in \mathcal{K}(\mathbf{H})$ is called a *pseudo-codeword*. The AWGNC *pseudo-weight* of a pseudo-codeword $\boldsymbol{\omega}$ is defined to be $w_\mathrm{p}(\boldsymbol{\omega}) = w_\mathrm{p}^{\mathrm{AWGNC}}(\boldsymbol{\omega}) \triangleq \|\boldsymbol{\omega}\|_1^2/\|\boldsymbol{\omega}\|_2^2$. (For a motivation of these definitions, see [14], [15]). The minimum of the AWGNC pseudo-weight over all nonzero pseudo-codewords is called the minimum AWGNC pseudo-weight and is denoted by $w_\mathrm{p}^{\min}(\mathbf{H})$.

For any integer $s \geq 1$, let $R_s = \{\exp(\imath 2\pi r/s) \ :\ 0 \leq r < s\}$ denote the set of complex s-th roots of unity, and let $R_s^- = R_s \setminus \{1\}$. The symbol * denotes complex conjugation. Also, an $r \times r$ circulant matrix $\mathbf{B}$, whose entries are square $L \times L$ matrices, will be called an *L-block circulant* matrix; we shall denote this by

$$\mathbf{B} = \mathrm{circ}(\mathbf{b}_0, \mathbf{b}_1, \cdots, \mathbf{b}_{r-1})$$

where the (square $L \times L$ matrix) entries in the first column of $\mathbf{B}$ are $\mathbf{b}_0$, $\mathbf{b}_1$, ... , $\mathbf{b}_{r-1}$ respectively.

978-1-4244-4148-8/09/$25.00 ©2009
This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE "GLOBECOM" 2009 proceedings.

Finally, $\mathbb{Z}$, $\mathbb{R}$, $\mathbb{C}$, and $\mathbb{F}_2$ will be the ring of integers, the field of real numbers, the complex field, and the finite field of size 2, respectively. For a positive integer L, $[L]$ will denote the set of nonnegative integers smaller than L: $[L] = \{0, 1, \ldots, L-1\}$.

III. Computing the Eigenvalues of $\mathbf{H}^\mathsf{T}\mathbf{H}$ for a QC Code

In this section we will show that the polynomial representation of a QC code will prove very helpful in computing the eigenvalues of the large matrix $\mathbf{H}^\mathsf{T}\mathbf{H}$, easing in this way the computation of the lower bound

$$d_{\min} \geqslant w_{\mathrm{p}}^{\min}(\mathbf{H}) \geqslant n\frac{2c-\lambda_2}{\lambda_1-\lambda_2}. \tag{3}$$

This section is organized in three subsections. In Sec. III-A and III-B we provide some background on circulant matrices and QC codes. Section III-C will contain the main result on the eigenvalues of $\mathbf{H}^\mathsf{T}\mathbf{H}$, where $\mathbf{H}$ is the parity-check matrix of a QC code.

A. Eigenvalues of a Circulant Matrix

The eigenvalues of a square circulant matrix are well known [16]. If $\mathbf{B} \in \mathbb{C}^{n\times n}$ is a circulant matrix and $w(X) = b_0 + b_1 X + \ldots + b_{n-1}X^{n-1}$ its (column) associated polynomial, then the eigenvalues of $\mathbf{B}$ are given by this polynomial's evaluation at the complex n-th roots of unity, i.e. $w(x)$ for all $x \in R_n$.

The following gives a proof of this result based on the polynomial representation of a circulant matrix. It may be seen as a special case of the method we present later for QC codes.

Let λ be an eigenvalue of $\mathbf{B}$. Then there exists a nonzero vector $\mathbf{v} = (v_0, \ldots, v_{n-1})^\mathsf{T} \in \mathbb{C}^n$ such that

$$\mathbf{B}\mathbf{v} = \lambda\mathbf{v}.$$

In polynomial form, this equation is equivalent to (here $v(X) = v_0 + v_1 X + \ldots + v_{n-1}X^{n-1}$):

$$\begin{aligned} & w(X)v(X) = \lambda v(X) \mod (X^n - 1) \text{ iff} \\ & X^n - 1 \mid w(X)v(X) - \lambda v(X) \text{ in } \mathbb{C} \text{ iff} \\ & w(x)v(x) = \lambda v(x), \forall x \in R_n \text{ iff} \\ & (w(x) - \lambda)v(x) = 0, \forall x \in R_n\ . \end{aligned}$$

For each $x \in R_n$, $\lambda = w(x)$ is a solution of the above equation, and therefore it is an eigenvalue for the matrix $\mathbf{B}$. There are n such solutions, therefore, these are all possible eigenvalues of $\mathbf{B}$.

In the next theorem we will consider an *L-block circulant* matrix instead of a circulant matrix. This theorem may be found in [17]; we provide here an alternative proof based on the polynomial representation.

Theorem 1 *Let $\mathbf{B} = \mathrm{circ}(\mathbf{b}_0, \mathbf{b}_1, \cdots, \mathbf{b}_{r-1}) \in \mathbb{C}^{rL\times rL}$ be an L-block circulant matrix. Let $\mathbf{W}(X) = \mathbf{b}_0 + \mathbf{b}_1 X + \ldots + \mathbf{b}_{r-1}X^{r-1}$ its (column) associated matrix polynomial. Then the eigenvalues of $\mathbf{B}$ are given by the union of the eigenvalues of the $L \times L$ matrices $\mathbf{W}(x)$, for all $x \in R_r$.*

Proof: The proof follows the reasoning in the theorem above.

Let λ be an eigenvalue of $\mathbf{B}$. Then there exists a nonzero vector $\mathbf{v} \triangleq (v_0, \ldots, v_{rL-1})^\mathsf{T} \in \mathbb{C}^{rL}$ such that

$$\mathbf{B}\mathbf{v} = \lambda\mathbf{v}. \tag{4}$$

Let $\mathbf{p}(X) \in \mathbb{C}^L[X]$ given by $\mathbf{p}(X) = (v_0, \ldots, v_{L-1})^\mathsf{T} + (v_L, \ldots, v_{2L-1})^\mathsf{T} X + \ldots + (v_{r(L-1)}, \ldots, v_{rL-1})^\mathsf{T} X^{r-1}$. In polynomial form, equation (4) is equivalent to:

$$\begin{aligned} & \mathbf{B}(X)\mathbf{p}(X) = \lambda\mathbf{p}(X) \mod (X^r - 1) \text{ iff} \\ & X^r - 1 \mid \mathbf{B}(X)\mathbf{p}(X) - \lambda\mathbf{p}(X) \text{ in } \mathbb{C} \text{ iff} \\ & \mathbf{B}(x)\mathbf{p}(x) = \lambda\mathbf{p}(x), \forall x \in R_r. \end{aligned}$$

The last equation is the equation for the eigenvalues of the matrix $\mathbf{B}(x)$. Each such matrix has L eigenvalues, counting multiplicities, and there are r distinct complex numbers in R_r; this accounts for the total number rL of eigenvalues of $\mathbf{B}$. The eigenvectors can also be deduced from the above.

B. Definition and Properties of QC Codes

A linear QC-LDPC code $\mathcal{C}_{\mathrm{QC}} \triangleq \mathcal{C}_{\mathrm{QC}}^{(r)}$ of length $n = rL$ can be described by an $rJ \times rL$ (scalar) parity-check matrix $\bar{\mathbf{H}}_{\mathrm{QC}}^{(r)} \triangleq \bar{\mathbf{H}}$ that is formed by a $J \times L$ array of $r \times r$ circulant matrices.

$$\bar{\mathbf{H}} = \begin{bmatrix} \mathbf{P}_{1,1} & \mathbf{P}_{1,2} & \ldots & \mathbf{P}_{1,L} \\ \mathbf{P}_{2,1} & \mathbf{P}_{2,2} & \ldots & \mathbf{P}_{2,L} \\ \vdots & \vdots & \ldots & \vdots \\ \mathbf{P}_{J,1} & \mathbf{P}_{J,2} & \ldots & \mathbf{P}_{J,L} \end{bmatrix}, \tag{5}$$

where the entries $\mathbf{P}_{i,j}$ are $r \times r$ circulant matrices. Clearly, by choosing these circulant matrices to be low-density, the parity-check matrix will also be low-density.

With the help of the well-known isomorphism between the ring of $r \times r$ circulant matrices and the ring of polynomials modulo $X^r - 1$, to each matrix $\mathbf{P}_{i,j}$ we can associate a polynomial $p_{i,j}(X)$, and thus a QC-LDPC code can equivalently be described by a polynomial parity-check matrix $\mathbf{P}(X)$ of size $J \times L$, with polynomial operations performed modulo $X^r - 1$:

$$\mathbf{P}(X) = \begin{bmatrix} p_{1,1}(X) & p_{1,2}(X) & \ldots & p_{1,L}(X) \\ p_{2,1}(X) & p_{2,2}(X) & \ldots & p_{2,L}(X) \\ \vdots & \vdots & \ldots & \vdots \\ p_{J,1}(X) & p_{J,2}(X) & \ldots & p_{J,L}(X) \end{bmatrix}. \tag{6}$$

By permuting the rows and columns of the scalar parity-check matrix $\bar{\mathbf{H}}$,[1] we obtain an equivalent parity-check matrix representation $\mathbf{H}$ for the QC code $\mathcal{C}_{\mathrm{QC}}^{(r)}$,

$$\mathbf{H} \triangleq \begin{bmatrix} \mathbf{H}_0 & \mathbf{H}_{r-1} & \cdots & \mathbf{H}_1 \\ \mathbf{H}_1 & \mathbf{H}_0 & \cdots & \mathbf{H}_2 \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{H}_{r-1} & \mathbf{H}_{r-2} & \cdots & \mathbf{H}_0 \end{bmatrix}. \tag{7}$$

[1] i.e., by taking the first row in the first block of r rows, the first row in the second block of r rows, etc., then the second row in the first block, the second row in the second block, etc., and similarly for the columns.

978-1-4244-4148-8/09/$25.00 ©2009
This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE "GLOBECOM" 2009 proceedings.

where $\mathbf{H}_0, \mathbf{H}_1, \ldots, \mathbf{H}_{r-1}$ are scalar $J \times L$ matrices. The connection between the two representations is

$$\mathbf{H}_0 + \mathbf{H}_1 X + \cdots + \mathbf{H}_{r-1} X^{r-1} = \mathbf{P}(X). \quad (8)$$

C. The Eigenvalues of the Matrix $\mathbf{H}^\mathsf{T} \cdot \mathbf{H}$ of a QC Code

Note that for a fixed value of $r \geq 1$, (8) provides a simple bijective correspondence between the set of polynomial matrices $\mathbf{P}(X) \in (\mathbb{R}[X]/(X^r - 1))^{J \times L}$ and the set of parity-check matrices of the form (7). Furthermore, the product of two such polynomial matrices, where defined, yields another which corresponds via this bijection with the product of the corresponding parity-check matrices in the form (7). Also note that transposition of a polynomial matrix in the form (8) corresponds to transposition of the corresponding parity-check matrix in the form (7), under this bijection.

It follows that $\mathbf{H}^\mathsf{T} \cdot \mathbf{H}$ is an L-block circulant matrix; applying Theorem 1 to this matrix yields the following corollary.

Corollary 2 *The eigenvalues of $\mathbf{H}^\mathsf{T} \cdot \mathbf{H}$ are given by the union of the eigenvalues of the $L \times L$ matrices $\mathbf{P}^\mathsf{T}(x^*) \cdot \mathbf{P}(x)$, for $x \in R_r$.*

Proof: We apply Theorem 1 to the L-block circulant matrix $\mathbf{H}^\mathsf{T} \cdot \mathbf{H} \triangleq \mathrm{circ}(\mathbf{b}_0, \mathbf{b}_1, \cdots, \mathbf{b}_{r-1}) \in \mathbb{C}^{rL \times rL}$ and form the matrix $\mathbf{W}(X) = \mathbf{b}_0 + \mathbf{b}_1 X + \ldots + \mathbf{b}_{r-1} X^{r-1}$. This is equal to the product of the two matrix polynomials of $\mathbf{H}^\mathsf{T}$ and $\mathbf{H}$, which are $\mathbf{H}_0^\mathsf{T} + \mathbf{H}_{r-1}^\mathsf{T} X + \cdots + \mathbf{H}_1^\mathsf{T} X^{r-1} = X^r \mathbf{P}^\mathsf{T}(1/X)$ and $\mathbf{H}_0 + \mathbf{H}_1 X + \cdots + \mathbf{H}_{r-1} X^{r-1} = \mathbf{P}(X)$, respectively. Therefore $\mathbf{W}(X) = (X^r \mathbf{P}^\mathsf{T}(1/X)) \cdot \mathbf{P}(X)$ and so the eigenvalues of $\mathbf{H}^\mathsf{T} \cdot \mathbf{H}$ are the eigenvalues of $\mathbf{P}^\mathsf{T}(1/x) \cdot \mathbf{P}(x)$, for all $x \in R_r$; these are then equal to the eigenvalues of $\mathbf{P}^\mathsf{T}(x^*) \cdot \mathbf{P}(x)$, for all $x \in R_r$ (as $x^* = 1/x$ for all such x).

Example 3 Let $r = 31$ and consider the $(3,5)$-regular QC-LDPC code given by the scalar 93×155 matrix[2]

$$\bar{\mathbf{H}} = \begin{bmatrix} \mathbf{I}_1 & \mathbf{I}_2 & \mathbf{I}_4 & \mathbf{I}_8 & \mathbf{I}_{16} \\ \mathbf{I}_5 & \mathbf{I}_{10} & \mathbf{I}_{20} & \mathbf{I}_9 & \mathbf{I}_{18} \\ \mathbf{I}_{25} & \mathbf{I}_{19} & \mathbf{I}_7 & \mathbf{I}_{14} & \mathbf{I}_{28} \end{bmatrix}.$$

The polynomial parity-check matrix $\mathbf{P}(X) \in (\mathbb{R}[X]/(X^r - 1))^{3 \times 5}$ is

$$\mathbf{P}(X) = \begin{bmatrix} X & X^2 & X^4 & X^8 & X^{16} \\ X^5 & X^{10} & X^{20} & X^9 & X^{18} \\ X^{25} & X^{19} & X^7 & X^{14} & X^{28} \end{bmatrix}.$$

This code is the famous $(3,5)$-regular QC-LDPC code of length 155 presented in [18]. Note that the code parameters are $[155, 64, 20]$. The corresponding matrix $\mathbf{H}$ in the form (7) is a 31×31 matrix with block entries $\mathbf{H}_i$, $i \in [31]$ obtained by decomposing $\mathbf{P}(X)$ according to the powers of X:

$$\mathbf{P}(X) = \mathbf{H}_0 + \mathbf{H}_1 X + \cdots + \mathbf{H}_{30} X^{30}. \quad (9)$$

Obviously only 15 matrices among the $\mathbf{H}_i$ are nonzero, and all of these contain only one 1, the other entries being zero.

[2]Here $\mathbf{I}_\ell$ denotes the 31×31 identity matrix with rows shifted cyclically to the left by ℓ positions.

The matrix $\mathbf{H}^\mathsf{T} \cdot \mathbf{H}$ is a 5-block circulant matrix. Corollary 2 above tells us that in order to compute its eigenvalues, we need to form the matrices $\mathbf{P}^\mathsf{T}(\rho^{-i}) \cdot \mathbf{P}(\rho^i)$, for all $i \in [31]$ (here ρ denotes a primitive complex 31-th root of unity). We have that

$$\mathbf{P}^\mathsf{T}(1/x) = \begin{bmatrix} x^{30} & x^{29} & x^{27} & x^{23} & x^{15} \\ x^{26} & x^{21} & x^{11} & x^{22} & x^{13} \\ x^6 & x^{12} & x^{24} & x^{17} & x^3 \end{bmatrix}^\mathsf{T}$$

and

$$\mathbf{P}^\mathsf{T}(1/x) \cdot \mathbf{P}(x) = \begin{bmatrix} 3 & a & e^* & c & e^* \\ a^* & 3 & b & a^* & d \\ e & b^* & 3 & c & b^* \\ c^* & a & c^* & 3 & d \\ e & d^* & b & d^* & 3 \end{bmatrix},$$

for all $x \in R_{31}$, where

$$a = x + x^5 + x^{25}; b = x^2 + x^{10} + x^{19}; c = x^4 + x^7 + x^{20};$$
$$d = x^8 + x^9 + x^{14}; e = x^{16} + x^{18} + x^{28}.$$

Obviously for $i \in [31]$, each matrix $\mathbf{P}^\mathsf{T}(\rho^{-i}) \cdot \mathbf{P}(\rho^i)$ is Hermitian (in fact nonnegative definite), hence each has 5 real nonnegative eigenvalues, giving a total of $31 \cdot 5 = 155$ nonnegative eigenvalues for $\mathbf{H}^\mathsf{T} \cdot \mathbf{H}$.

We obtain that for each $i \in [31], i \neq 0$, the associated polynomial of $\mathbf{P}^\mathsf{T}(\rho^{-i}) \cdot \mathbf{P}(\rho^i)$ may be written as (using $\rho^{31} = 1$)

$$\begin{aligned} u(\lambda) &= \lambda^2(\lambda^3 - 15\lambda^2 + 62\lambda - 62) \\ &= \lambda^2(\lambda - \lambda_2)(\lambda - \lambda_3)(\lambda - \lambda_4) \end{aligned}$$

where $\lambda_2 = 8.6801$, $\lambda_3 = 4.8459$ and $\lambda_4 = 1.4740$. Also, for $i = 0$ the associated polynomial of $\mathbf{P}^\mathsf{T}(\rho^{-i}) \cdot \mathbf{P}(\rho^i)$ may be written as $u(\lambda) = \lambda^4(\lambda - \lambda_1)$ where $\lambda_1 = 15$. This yields the nonzero eigenvalues of $\mathbf{H}^\mathsf{T} \cdot \mathbf{H}$ as $\{\lambda_1, \lambda_2, \lambda_3, \lambda_4\}$ with multiplicities 1, 30, 30 and 30 respectively. □

IV. Eigenvalues of Nested Circulant Matrices

In this section we define the class of *nested circulant* matrices, and show that they have eigenvalues which are given by evaluating a multivariate associated polynomial at points whose coordinates are particular roots of unity.

Theorem 4 *Let $\mathbf{B} = \mathrm{circ}(\mathbf{b}_0, \mathbf{b}_1, \cdots, \mathbf{b}_{r-1}) \in \mathbb{C}^{rL \times rL}$ be an L-block circulant matrix. Suppose that each subblock $\mathbf{b}_i$, $i \in [r]$, is also circulant, with associated polynomial $p^{(i)}(X) = \sum_{j=0}^{L-1} b_{i,j} X^j$. Define the associated polynomial of $\mathbf{B}$ by*

$$q(X, Y) = \sum_{i=0}^{r-1} \sum_{j=0}^{L-1} b_{i,j} X^i Y^j .$$

Then the set of eigenvalues of $\mathbf{B}$ is given by

$$\{q(x, y) \ : \ x \in R_r, y \in R_L\} .$$

Proof: For each $j \in [L]$ define $u^{(j)}(X) = \sum_{i=0}^{r-1} b_{i,j} X^i$. By Theorem 1, the eigenvalues of $\mathbf{B}$ are equal to those of the matrices given by $\mathbf{W}(x)$ for $x \in R_r$; each of these is circulant with associated polynomial (in Y) given by

$$\sum_{j=0}^{L-1} u^{(j)}(x) Y^j = q(x, Y) \ .$$

Thus the eigenvalues of each $\mathbf{W}(x)$ are equal to $q(x, y)$ for $y \in R_L$, and the result follows.

We next define what is meant by a *nested circulant* matrix.

Definition 5 *Let $m \geq 1$ and let i_t be a positive integer for each $t = 1, 2, \cdots, m$. Also let $\mathbf{B} = \mathrm{circ}(\mathbf{b}_0, \mathbf{b}_1, \cdots, \mathbf{b}_{i_1 - 1})$ be a block-circulant matrix such that for every $t = 1, 2, \cdots, m-1$, $j_t \in [i_t]$*

$$\mathbf{b}_{j_1, j_2, \cdots, j_t} = \mathrm{circ}(\mathbf{b}_{j_1, j_2, \cdots, j_t, 0}, \mathbf{b}_{j_1, j_2, \cdots, j_t, 1}, \cdots, \mathbf{b}_{j_1, j_2, \cdots, j_t, i_{t+1} - 1})$$

is also block-circulant, and that $\mathbf{b}_{j_1, j_2, \cdots, j_m} = b_{j_1, j_2, \cdots, j_m}$ are scalars. Then $\mathbf{B}$ is said to be an m-nested circulant matrix (with dimension $n = \prod_{t=1}^{m} i_t$). The associated polynomial of $\mathbf{B}$ is defined by

$$q(X_1, X_2, \cdots, X_m) = \sum_{j_1=0}^{i_1-1} \sum_{j_2=0}^{i_2-1} \cdots \sum_{j_m=0}^{i_m-1} b_{j_1, j_2, \cdots, j_m} \prod_{t=1}^{m} X_t^{j_t} \quad (10)$$

□

Note that the 1-nested circulants are precisely the circulant matrices, and that the 2-nested circulants are precisely the i_2-block-circulant matrices with circulant subblocks. Also note that the associated polynomial $q(X_1, X_2, \cdots, X_m)$ provides a succinct description of the matrix $\mathbf{B}$.

A straightforward generalization of Theorem 4 is as follows.

Theorem 6 *Let $\mathbf{B}$ be an m-nested circulant matrix with associated polynomial $q(X_1, X_2, \cdots, X_m)$ given by (10) above. Then the set of eigenvalues of $\mathbf{B}$ is given by*

$$\{q(x_1, x_2, \cdots, x_m) \ : \ x_t \in R_{i_t} \quad \forall t = 1, 2, \cdots, m\}$$

Proof: The proof uses induction, and follows the lines of the proof of Theorem 4 in a rather straightforward manner.

Example 7 Here we take an example of an 3-nested circulant (i.e. $m = 3$), where $i_t = 2$ for $t = 1, 2, 3$. The eigenvalues of

$$\mathbf{B} = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$$

are equal to the eigenvalues of

$$\mathbf{B}' = \begin{bmatrix} 0 & 1+x & x & x \\ 1+x & 0 & x & x \\ x & x & 0 & 1+x \\ x & x & 1+x & 0 \end{bmatrix}$$

for $x \in \{-1, 1\}$, which are equal to the eigenvalues of

$$\mathbf{B}'' = \begin{bmatrix} xy & 1+x+xy \\ 1+x+xy & xy \end{bmatrix}$$

for $x \in \{-1, 1\}$ and $y \in \{-1, 1\}$. Finally, these are equal to the set

$$\{q(x, y, z) \ : \ x, y, z \in \{-1, 1\}\}$$

where the associated polynomial of $\mathbf{B}$ is $q(x, y, z) = xy + z(1+x+xy)$. In this example $b_{0,0,0} = 0$, $b_{0,0,1} = 1$, $b_{0,1,0} = 0$, $b_{0,1,1} = 0$, $b_{1,0,0} = 0$, $b_{1,0,1} = 1$, $b_{1,1,0} = 1$, $b_{1,1,1} = 1$; these may be easily obtained by matching the elements of the first column of $\mathbf{B}$ with the binary expansion of the corresponding row position.

This example may be generalized to the case where $n = 2^m$ and the circulant is m-nested; the eigenvalues are real. Note that the choice of the first column in $\mathbf{B}$ determines which terms in $\{1, x, y, z, xy, yz, zx, xyz\}$ are included in the associated polynomial, and hence controls the eigenvalues of $\mathbf{B}$. □

Theorem 8 *If $\mathbf{H}$ is an m-nested circulant matrix, then $\mathbf{B} = \mathbf{H}^\mathsf{T}\mathbf{H}$ is an m-nested circulant matrix.*

Proof: It is straightforward to prove the stronger result that if $\mathbf{A}$ and $\mathbf{B}$ are m-nested circulants with specified nested dimensions, then $\mathbf{A}^\mathsf{T}\mathbf{B}$ is also m-nested circulant, with the same nested dimensions. The proof proceeds by induction on m. The base case $m = 1$ is straightforward. Next, let $\mathbf{A}$ be block-circulant with block entries in the first column equal to some $(m-1)$-nested circulants $\mathbf{A}_i$, and let $\mathbf{B}$ be block-circulant with block entries in the first column equal to some $(m-1)$-nested circulants $\mathbf{B}_j$. The matrix $\mathbf{A}^\mathsf{T}\mathbf{B}$ is then block-circulant, and each block entry is a sum of matrices of the form $\mathbf{A}_i^\mathsf{T}\mathbf{B}_j$. By the principle of induction, each of these matrices is an $(m-1)$-nested circulant, and it is easy to show that a sum of t-nested circulants (of the same nested dimensions) is another t-nested circulant (with these nested dimensions).

V. Conditions for the Pseudo-Weight Lower Bound to Hold with Equality

It is straightforward to show that a necessary condition for the bound of [13] to hold with equality is that the eigenvalues of $\mathbf{B} = \mathbf{H}^\mathsf{T}\mathbf{H} \in \mathbb{R}^{n \times n}$ are λ_1 with multiplicity 1 and $\lambda_2 < \lambda_1$ with multiplicity $n - 1$.

If $\mathbf{H}$ is circulant with (row) associated polynomial $w(X)$ of degree $k \leq n$, the eigenvalues of $\mathbf{B}$ are precisely $\{|w(x)|^2 \ : \ x \in R_n\}$; therefore the largest eigenvalue of $\mathbf{B}$ is $\lambda_1 = |w(1)|^2 = d^2$ where d is the number of nonzero coefficients in $w(X)$ (noting that $|w(1)|^2 > |w(x)|^2$ for all $x \in R_n^-$). Let $\tilde{w}(X) = X^k w(1/X)$ denote the *reciprocal polynomial* of $w(X)$ which is obtained by reversing the order of coefficients in $w(X)$. Now assume that the bound of [13] holds with equality. Then we must have

$$|w(x)|^2 = w(x) w^*(x) = \lambda_2 \quad \forall \, x \in R_n^-$$

for some positive real number λ_2, i.e.

$$w(x) w(1/x) = \lambda_2 \quad \forall \, x \in R_n^- \ .$$

This is equivalent to

$$w(x)\tilde{w}(x) = \lambda_2 x^k \quad \forall\, x \in R_n^-$$

Thus R_n^- is a subset of the roots of the polynomial $w(X)\tilde{w}(X) - \lambda_2 X^k$, and so

$$w(X)\tilde{w}(X) - \lambda_2 X^k = (1+X+X^2+\cdots+X^{n-1})r(X) \quad (11)$$

where $r(X)$ is a polynomial of degree $2k - n + 1 \geq 0$ with integer coefficients. In the following we give details of this condition for some codes which attain the bound of [13] with equality.

Example 9 The $\mathrm{EG}(2,2)$ code with $q = 2$, $n = 3$, $k = 1$, $d = 2$ has $w(X) = 1 + X$. Here $\lambda_1 = d^2 = 4$ and (11) holds in the form

$$(1 + X)^2 - X = 1 + X + X^2$$

so in this case $\lambda_2 = 1$ and $r(X) = 1$. Here

$$d_{\min} = w_{\mathrm{p}}^{\min}(\mathbf{H}) = n\left(\frac{2d - \lambda_2}{d^2 - \lambda_2}\right) = 3 = q + 1\,.$$

□

Example 10 The $\mathrm{PG}(2,2)$ code with $q = 2$, $n = 7$, $k = 3$, $d = 3$ has $w(X) = 1 + X + X^3$. Here $\lambda_1 = d^2 = 9$ and (11) holds in the form

$$(1 + X + X^3)(1 + X^2 + X^3) - 2X^3 = 1 + X + \cdots + X^6$$

so in this case $\lambda_2 = 2$ and $r(X) = 1$. Here

$$d_{\min} = w_{\mathrm{p}}^{\min}(\mathbf{H}) = n\left(\frac{2d - \lambda_2}{d^2 - \lambda_2}\right) = 4 = q + 2\,.$$

□

Example 11 The $\mathrm{PG}(2,4)$ code with $q = 2$, $n = 21$, $k = 11$, $d = 5$ has $w(X) = 1 + X^2 + X^7 + X^8 + X^{11}$. Here $\lambda_1 = d^2 = 25$ and (11) holds in the form

$$\begin{aligned}(1 + X^2 + X^7 + X^8 + X^{11})(1 + X^3 + X^4 + X^9 + X^{11})\\ -4X^{11} = (1 + X + X^2 + \cdots + X^{20})(1 - X + X^2)\end{aligned}$$

so in this case $\lambda_2 = 4$ and $r(X) = 1 - X + X^2$. Here

$$d_{\min} = w_{\mathrm{p}}^{\min}(\mathbf{H}) = n\left(\frac{2d - \lambda_2}{d^2 - \lambda_2}\right) = 6 = q + 2\,.$$

□

Note that for a general $\mathrm{PG}(2,q)$ code, for the bound to hold with equality we require

$$\begin{aligned} w_{\mathrm{p}}^{\min}(\mathbf{H}) = q + 1 &= n\left(\frac{2d - \lambda_2}{d^2 - \lambda_2}\right) \\ &= (q^2 + q + 1)\left(\frac{2(q+1) - \lambda_2}{(q+1)^2 - \lambda_2}\right)\,. \end{aligned}$$

and therefore we must have $\lambda_2 = q$. Also, for a general $\mathrm{EG}(2,q)$ code, for the bound to hold with equality we require

$$\begin{aligned} w_{\mathrm{p}}^{\min}(\mathbf{H}) = q + 1 &= n\left(\frac{2d - \lambda_2}{d^2 - \lambda_2}\right) \\ &= (q^2 - 1)\left(\frac{2q - \lambda_2}{q^2 - \lambda_2}\right)\,. \end{aligned}$$

and therefore we must have $\lambda_2 = q$ if $q > 2$, whereas for $q = 2$, any λ_2 will achieve the bound.

VI. Conclusions and Future Work

A method has been presented for evaluation of the eigenvalue-based lower bound on the AWGNC pseudo-weight based on spectral analysis, for QC and related codes. It was shown that the relevant eigenvalues may be found by computing the eigenvalues of a certain number of small matrices. We also presented a necessary condition for the bound to be attained with equality and gave a few examples of codes for which this happens. Future work involves optimization of QC code designs based on these bounds.

VII. Acknowledgment

The first author was supported by NSF Grant DMS-0708033 and TF-0830608.

References

[1] Z. Li, L. Chen, L. Zheng, 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. 565–578, Jan. 2006.

[2] Y. Dai, Z. Yan and N. Chen, "Optimal overlapped message-passing decoding of quasi-cyclic LDPC codes," *IEEE Transactions on Very Large Scale Integration Systems*, vol. 16, no. 5, pp. 565–578, May 2008.

[3] M. M. Mansour and N. R. Shanbhag, "High-throughput LDPC decoders," *IEEE Transactions on Very Large Scale Integration Systems*, vol. 11, no. 6, pp. 976–996, Dec. 2003.

[4] N. Wiberg, *Codes and Decoding on General Graphs.* Ph.D. Thesis, Linköping University, Sweden, 1996.

[5] R. M. Tanner, "Minimum-distance bounds by graph analysis," *IEEE Trans. on Inform. Theory*, vol. IT–47, no. 2, pp. 808–821, 2001.

[6] P. O. Vontobel and R. Koetter, "Lower bounds on the minimum pseudo-weight of linear codes," in *Proc. IEEE Intern. Symp. on Inform. Theory*, (Chicago, IL, USA), p. 70, June 27–July 2 2004.

[7] P. O. Vontobel and R. Smarandache, "On minimal pseudo-codewords of Tanner graphs from projective planes," in *Proc. 43rd Allerton Conf. on Communications, Control, and Computing*, (Allerton House, Monticello, Illinois, USA), Sep. 28–30 2005. Available online under `http://www.arxiv.org/abs/cs.IT/0510043`.

[8] R. Smarandache and P. O. Vontobel, "Pseudo-codeword analysis of Tanner graphs from projective and Euclidean planes," *IEEE Trans. Inform. Theory*, vol. 53, no. 7, pp. 2376–2393, 2007, available online under http://www.arxiv.org/abs/cs.IT/0602089.

[9] Y. Kou, S. Lin, and M. P. C. Fossorier, "Low-density parity-check codes based on finite geometries: a rediscovery and new results," *IEEE Trans. on Inform. Theory*, vol. IT–47, pp. 2711–2736, Nov. 2001.

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

[11] S. Ling and P. Sole, "On the algebraic structure of quasi-cyclic codes I: finite fields," *IEEE Trans. Inform. Theory*, vol. 47, pp. 2751–2760, 2001.

[12] S. Ling and P. Sole, "On the algebraic structure of quasi-cyclic codes II: Chain rings," *Designs, Codes and Cryptography*, vol. 30, pp. 113–130, 2003.

[13] P. O. Vontobel and R. Koetter, "Lower Bounds on the Minimum Pseudo-Weight of Linear Codes," *Proc. IEEE International Symposium on Information Theory (ISIT)*, June/July 2004, pp. 67, Chicago, USA.

[14] P. O. Vontobel and R. Koetter, "Graph-cover decoding and finite-length analysis of message-passing iterative decoding of LDPC codes," *Submitted to IEEE Trans. Inform. Theory, available online under* `http://www.arxiv.org/abs/cs.IT/0512078`, Dec. 2005.

[15] R. Koetter, W.-C. W. Li, P. O. Vontobel, and J. L. Walker, "Characterizations of pseudo-codewords of (low-density) parity-check codes," *Adv. in Math.*, vol. 213, Aug. 2007.

[16] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*. New York: North-Holland, 1998.

[17] G. J. Tee, "Eigenvectors of block circulant and alternating circulant matrices," *Res. Lett. Inf. Math. Sci.*, vol. 8, 2005.

[18] R. M. Tanner, "A [155,64,20] sparse graph (LDPC) code," presented at the Recent Results Session at the IEEE International Symposium on Information Theory, Sorrento, Italy, June 2000.