Spectral Method for Quasi-Cyclic Code Analysis

P. Semenov and P. Trifonov, *Member, IEEE*

***Abstract*—A generalization of the BCH bound to the case of quasi-cyclic codes is proposed. The new approach is based on eigenvalues of matrix polynomials. This results in improved minimum distance estimates compared to the existing bounds.**

***Index Terms*—Quasi-cyclic codes, minimum distance estimation, BCH, eigenvalues, matrix polynomials.**

I. Introduction

DESIGNING reliable data transmission protocols requires employing channel codes with high error correction capability. Furthermore, one should be able to accurately predict the performance of these codes. Since the minimum distance is the main parameter effecting the performance of a code in the high-SNR region, techniques for its estimation are needed.

It was shown in [1, 2, 3] that there exist quasi-cyclic codes (QCC) satisfying the Varshamov-Gilbert bound. Also, many of the existing good LDPC codes are quasi-cyclic ones.

The algebraic structure of QCC was studied in many different ways, but the existing techniques often result in quite poor estimates of the code minimum distance. In this paper we propose a generalization of the well-known spectral method for analysis of cyclic codes, and, in particular, a generalization of the BCH minimum distance bound, to the case of quasi-cycic ones. In many cases the proposed approach results in better estimates of minimum distance compared to the existing ones.

The paper is organized as follows. Section II introduces the necessary background. A novel spectral method for analysis of quasi-cyclic codes is introduced in section III. A comparison of this method with other appropaches is presented in section IV. Finally, some conclusions are drawn.

II. Background

A. Gröbner basis representation of QCC

Definition 1. *A $\mathbb{R}$-module M over ring $\mathbb{R}$ of scalars is an abelian group $(M,+)$ with an operation $\odot : \mathbb{R}\times\mathbb{M}\to\mathbb{M}$ such that for all $r,s\in\mathbb{R}$ and vectors $x,y\in M$ the following satisfy:*

1) $r\odot(x+y)=r\odot x+r\odot y$
2) $(r+s)\odot x=r\odot x+s\odot x$
3) $(r\odot s)\odot x=r\odot(s\odot x)$
4) $1_{\mathbb{R}}\odot x=x$

Manuscript received April 16, 2012. The associate editor coordinating the review of this letter and approving it for publication was A. Burr.

The authors are with the Department of Distributed Computing and Networking, Saint-Petersburg State Polytechnical University, Russian Federation (e-mail: {spk, petert}@dcn.ftk.spbstu.ru).

Digital Object Identifier 10.1109/LCOMM.2012.091712.120834

Any $\mathbb{R}$-module M can be given by its generating set $\langle g_i\in M \mid 0\le i<p\rangle$. So M is just a $\left\{\sum_{j=0}^{p-1} a_i\odot g_i \mid (a_0,a_1,\ldots,a_{p-1})\in\mathbb{R}^p\right\}$. In this paper, $\mathbb{R}$ is the ring of univariate polynomials $\mathbb{F}_q[x]$. M is a set of vectors of such polynomials.

Definition 2. *Linear code over $\mathbb{F}_q[x]$ is $[l,lm]$-quasi-cyclic if it has length lm and every circular shift of any codeword by l positions is also a codeword.*

A codeword $(c_{0,0},\ldots,c_{l-1,0},c_{0,1},\ldots,c_{l-1,1},\ldots,c_{l-1,m-1})$ of a $[l,lm]$-QCC can be represented as a vector of polynomials $\mathbf{c}(x)=(c_0(x),\ldots,c_{l-1}(x))$, where $c_i(x)=\sum_{j=0}^{m-1}c_{i,j}x^j$. Then the cycic shift of the codeword by l positions is equivalent to elementwise multiplication of the corresponding polynomial vector $\mathbf{c}(x)$ by x modulo x^m-1. This enables one to consider QCC as the $\mathbb{F}_q[x]/\langle x^m-1\rangle$-module of algebra $\left(\mathbb{F}_q[x]/\langle x^m-1\rangle\right)^l$. So, the preimage of QCC is $\mathbb{F}_q[x]$-module of $\left(\mathbb{F}_q[x]\right)^l$ containing submodule $\tilde{K}=\langle(x^m-1)\mathbf{e}_i \mid 0\le i<l\rangle$, where $\mathbf{e}_i$ are unit vectors [4]. Given some basis $G=\{\mathbf{g}_0(x),\ldots,\mathbf{g}_{p-1}(x)\}$ of this module, where $\mathbf{g}_i(x)=(g_{i,0}(x),\ldots,g_{i,l-1}(x))$, one can represent any codeword of the QCC as $\mathbf{c}(x)=\sum_{i=0}^{p-1}a_i(x)\mathbf{g}_i(x)$ modulo x^m-1. It will be convenient to represent the basis as a polynomial matrix $G(x)=\begin{pmatrix} g_{0,0}(x) & \cdots & g_{0,l-1}(x)\\ \vdots & \ddots & \vdots\\ g_{p-1,0}(x) & \cdots & g_{p-1,l-1}(x)\end{pmatrix}$, so that $\mathbf{c}(x)=\mathbf{a}(x)G(x)$. It was shown in [4] that any $\mathbb{F}_q[x]$-module corresponding to a QCC has reduced Gröbner basis with respect to position-over-term ordering [5]. This basis can be represeted as a $l\times l$ polynomial matrix $\tilde{G}(x)$ with the following properties:

1) $\forall i,j: 0\le j<i<l : g_{i,j}(x)=0$;
2) $\forall j<i : \deg g_{j,i}(x)<\deg g_{i,i}(x)$;
3) $\forall i : g_{i,i}(x)\mid(x^m-1)$;
4) if $g_{i,i}(x)=(x^m-1)$, then the i-th row of $\tilde{G}(x)$ is equal to $(x^m-1)\mathbf{e}_i$.

It follows that the dimension of the code is given by $k=lm-\sum_{i=0}^{l-1}\deg g_{i,i}(x)$. It can be also seen that the rank of polynomial matrix $\tilde{G}(x)$ is equal l. By abuse of notation, this Gröbner basis will be referred to as the Gröbner basis of QCC.

B. Eigenvalues of polynomial matrices

Let $A(x)$ be a $l\times l$ polynomial matrix over $\mathbb{F}_q$. If $p(x)=\det A(x)$ is not identically zero, then $A(x)$ is called non-singular. However, substituting x with some roots λ_i of $p(x)$, one obtains singular matrices $A(\lambda_i)$. The roots λ_i of $\det A(x)$ are called eigenvalues of polynomial matrix $A(x)$ [6]. Observe that the eigenvalues may belong to some alebraic extension of the original field $\mathbb{F}_q$. Algebraic multiplicity of eigenvalue λ_i

of polynomial matrix $A(x)$ is the greatest integer u_i such that $(x-\lambda_i)^{u_i} | \det A(x)$.

For any eigenvalue λ_i one can identify right eigenvectors $\mathbf{v}$ as the solutions of the homogeneous system of equations $A(\lambda_i)\mathbf{v} = 0$. The set of all solutions of this system is called the right eigenspace $\mathcal{V}_i$ corresponding to eigenvalue λ_i, and its dimension μ_i is called the geometric multiplicity of eigenvalue λ_i.

It can be shown (see [6]) that for any polynomial matrix $A(x)$ one can construct its Smith normal form $A(x) = U(x)D(x)V(x)$, where $U(x), V(x)$ are square polynomial matrices with $\det U(x), \det V(x) \in \mathbb{F}_q \setminus \{0\}$, $D(x) = \mathrm{diag}(d_0(x), \ldots, d_{w-1}(x), 0, \ldots, 0)$, w is the rank of $A(x)$, and $d_{i-1}(x) \mid d_i(x)$. Hence, the geometric multiplicity of eigenvalue λ is equal to the number of polynomials $d_i(x)$ such that $d_i(\lambda) = 0$. Since for non-singular matrices $\det A(x) = \prod_{i=0}^{l-1} d_i(x)$, one obtains that the geometric multiplicity of any eigenvalue does not exceed its algebraic multiplicity.

III. Spectral Method

A. Parity check matrix over an extended field

Consider a q-ary $[l, lm]$-QCC $\mathcal{C}$ and its Gröbner basis represented as a $l \times l$ polynomial matrix $\tilde{G}(x)$. For brevity, the eigenvalues of this matrix will be referred to as the eigenvalues of $\mathcal{C}$.

The properties of Gröbner basis outlined in section II-A imply that $\tilde{G}(x)$ is an upper-triangular matrix, i.e. $\det \tilde{G}(x) = \prod_{i=0}^{l-1} g_{i,i}(x)$. Hence, all code eigenvalues are roots of polynomials $g_{i,i}(x)$. Since these polynomials are divisors of $x^m - 1$, all eigenvalues of the code can be represented as $\lambda_i = \alpha^{j_i}$, where $\alpha \in \mathbb{F}_{q^r}$ is a primitive m-th root of unity, and r is the smallest integer such that $m \mid (q^r - 1)$. It can be seen that the concept of quasi-cyclic code eigenvalue is a generalization of the notion of a root of a cyclic code generating polynomial.

Lemma 1. *For any eigenvalue λ_i of $\mathcal{C}$ its algebraic multiplicity u_i is equal to its geometric multiplicity μ_i.*

Proof: Any QCC as a polynomial module contains a submodule $\tilde{K} = \langle (x^m - 1)\mathbf{e}_i \mid 0 \le i < l \rangle$ (see section II-A). Hence, there exists a polynomial matrix $A(x)$ such that

$$A(x)\tilde{G}(x) = (x^m - 1)I, \tag{1}$$

where I is $l \times l$-identity matrix. Consider now the Smith normal form of matrix $\tilde{G}(x) = U(x)D(x)V(x)$. Since the determinant of $\tilde{G}(x)$ is non-zero, there exists inverse of this matrix over the field of rational functions. This enables one to rewrite (1) as

$$\begin{aligned} A(x) &= (x^m - 1)\tilde{G}^{-1}(x) \\ &= (x^m - 1)V^{-1}(x)D^{-1}(x)U^{-1}(x) \\ &= V^{-1}(x)\left((x^m - 1)D^{-1}(x)\right)U^{-1}(x). \end{aligned}$$

This can be further transformed to

$$V(x)A(X)U(x) = \mathrm{diag}\left(\frac{x^m - 1}{d_j(x)}, 0 \le j < l\right).$$

The left-hand side of this expression represents a polynomial matrix. Hence, the elements of the right-hand side matrix must also be polynomials, i.e. $d_j(x) \mid (x^m - 1), 0 \le j < l$. This implies that the algebraic multiplicity u_i of any eigenvalue λ_i is equal to the number of polynomials $d_j(x) : d_j(\lambda_i) = 0$, i.e. its geometric multiplicity. ∎

Let λ_i be an eigenvalue of QCC $\mathcal{C}$ with multiplicity u_i. Consider some basis $\mathbf{v}_{i,j}, 0 \le j < u_i$, of its eigenspace. Let V_i be the $u_i \times l$ matrix obtained by stacking the vectors $\mathbf{v}_{i,j}^T$. Construct a matrix $H_i = (1, \lambda_i, \lambda_i^2, \ldots, \lambda_i^{m-1}) \otimes V_i$, where $\otimes$ denotes the Kronecker product operation. Then the parity check matrix H of code $\mathcal{C}$ can be constructed by stacking the matrices H_i corresponding to all its distinct eigenvalues $\lambda_i, 1 \le i \le t$. The proof for this will be given below in Theorem 1.

Lemma 2. *The rank of matrix H is equal to $lm - k$, where k is the dimension of $\mathcal{C}$.*

Proof: Lemma 1 implies that the number of rows in H equals $\deg \det \tilde{G}(x) = \sum_{i=0}^{l-1} \deg g_{i,i}(x) = lm - k$ (see Section II-A). It remains to show that they are linearly independent. Assume that there exists a non-zero vector $\mathbf{z} = (z_{0,0}, \ldots, z_{0,u_0-1}, \ldots, z_{t-1,u_{t-1}-1})$ such that $\mathbf{z}H = 0$. The latter equation is equivalent to $\sum_{i=0}^{t-1} \mathbf{z}_i H_i = 0$, where $\mathbf{z}_i = (z_{i,0}, \ldots, z_{i,u_i-1})$ is the subvector corresponding to H_i. It can be seen that $\mathbf{z}_i H_i = (1, \ldots, \lambda_i^{m-1}) \otimes (\mathbf{z}_i V_i)$. Since V_i corresponds to a basis of the eigenspace of λ_i, $\nu_i = (\nu_{i,0}, \ldots, \nu_{i,l-1}) = \mathbf{z}_i V_i$ is a non-zero vector (an eigenvector) if and only if $\mathbf{z}_i \neq 0$. Therefore, one obtains l systems of linear equations

$$(\nu_{0,j}, \ldots, \nu_{t-1,j}) \begin{pmatrix} \lambda_0^0 & \lambda_0^1 & \ldots & \lambda_0^{m-1} \\ \lambda_1^0 & \lambda_1^1 & \ldots & \lambda_1^{m-1} \\ \vdots & \vdots & \ddots & \vdots \\ \lambda_{t-1}^0 & \lambda_{t-1}^1 & \ldots & \lambda_{t-1}^{m-1} \end{pmatrix} = 0, 0 \le j < l.$$

The total number t of distinct eigenvalues cannot exceed m, so the matrix in these systems is a Vandermonde one, i.e. non-singular. Hence, the only solution to these systems corresponds to $\nu_{i,j} = 0, 0 \le i < t, 0 \le j < l$. Hence, $\mathbf{z}_i = 0$ for all i, and the rows of H are linearly independent. ∎

Theorem 1. *The vector $\mathbf{c} \in \mathbb{F}_q^{lm}$ is a codeword of $[l, lm]$-QCC $\mathcal{C}$ iff $H\mathbf{c}^T = 0$, where H is the matrix constructed above.*

Proof: If $\mathbf{c} \in \mathcal{C}$, then the corresponding vector of polynomials satisfies $\mathbf{c}(x) = (c_0(x), \ldots, c_{l-1}(x)) = \mathbf{a}(x)\tilde{G}(x)$, and the statement of the theorem follows by setting $x = \lambda_i$ and multiplying $\mathbf{c}(x)$ by the eigenvectors corresponding to λ_i.

To show the converse, assume that a non-codeword $\widehat{\mathbf{c}}$ satisfies $H\widehat{\mathbf{c}}^T = 0$. $\widehat{\mathbf{c}}$ must be linearly independent from any codeword $\mathbf{c} \in \mathcal{C}$, so the row dimension of H, which is the basis of the nullspace of code generator matrix, must be strictly less than $lm - k$. This contradicts Lemma 2. ∎

B. Minimum Distance of Quasi-Cyclic Codes

The parity check matrix over an extended field $\mathbb{F}_{q^r}$ introduced in Section III provides a natural generalization of the BCH bound to the case of QCC. First, observe that selection of different bases of eigenspaces $\mathcal{V}_i$ results in equivalent check matrices. Furthermore, one can select a subset of parity check equations given by H to analyze code properties and, in

principle, perform decoding. More specifically, one can find an intersection of eigenspaces corresponding to a number of eigenvalues. If this intersection contains some non-zero common eigenvectors with sufficiently good properties, then the minimum distance of the QCC is given by the minimum distance of a cyclic code with a generator polynomial having these eigenvalues as roots.

Given an eigenspace $\mathcal{V} \subseteq \mathbb{F}_{q^r}^l$, we define the corresponding eigencode

$$\mathbb{C} = \left\{ c \in \mathbb{F}_q^l \mid \forall v \in \mathcal{V} : \sum_{j=0}^{l-1} v_j c_j = 0 \right\}.$$

If the elements of $v \in \mathcal{V}$ are linearly independent over $\mathbb{F}_q$, then $\mathbb{C} = \{(0, \ldots, 0)\}$ and we assume that its minimum distance is infinite.

Theorem 2. *Let $\alpha \in \mathbb{F}_{q^r}$ be a primitive m-th root of unity, and let for some $b \geq 0$ $\lambda_0 = \alpha^b, \lambda_1 = \alpha^{b+1}, \ldots, \lambda_{\delta-1} = \alpha^{b+\delta-2}$ be eigenvalues of $[l, lm]$-QCC $\mathcal{C}$. Consider the corresponding eigenspaces $\mathcal{V}_i$ and their intersection $\mathcal{V} = \cap_{i=0}^{\delta-1} \mathcal{V}_i$. Let $\mathbb{C}$ be the eigencode given by $\mathcal{V}$ (i.e. the direct sum of eigencodes $\mathbb{C}_i$ corresponding to $\mathcal{V}_i$). Then the minimum distance of $\mathcal{C}$ is given by $d(\mathcal{C}) \geq \min(\delta, d(\mathbb{C}))$.*

Proof: Let V be the matrix corresponding to a basis of $\mathcal{V}$. Then the necessary condition for vector c to be a codeword is given by $\widehat{H} c^T = 0$, where

$$\widehat{H} = \underbrace{\begin{pmatrix} 1 & \alpha^b & \alpha^{2b} & \ldots & \alpha^{b(m-1)} \\ 1 & \alpha^{b+1} & \alpha^{2(b+1)} & \ldots & \alpha^{(b+1)(m-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha^{b+\delta-2} & \alpha^{2(b+\delta-2)} & \ldots & \alpha^{(b+\delta-2)(m-1)} \end{pmatrix}}_{\tilde{H}} \otimes V.$$

Assume that there exists a codeword $c \in \mathcal{C}$ with t non-zero positions, $0 < t < \min(\delta, d(\mathbb{C}))$. Let $\mathbf{c}_i = (c_{0,i}, \ldots, c_{l-1,i}) \in \mathbb{C}$. Since $t < d(\mathbb{C})$, for any non-zero $\mathbf{c}_i$ one obtains $\mathbf{s}_i = V \mathbf{c}_i^T \neq 0$. Hence, $0 < |\{i \mid \mathbf{s}_i \neq 0\}| \leq t < \delta$. The values $\mathbf{s}_i$ must satisfy

$$0 = (\mathbf{s}_0, \ldots, \mathbf{s}_{m-1}) \tilde{H}^T,$$

but this is impossible since $\tilde{H}$ is a parity check matrix of $(m, m - \delta + 1, \delta)$ Reed-Solomon code over $\mathbb{F}_{q^r}$. ∎

IV. Comparison with Existing Approaches

A. Barbier-Chabot-Quintin bound

A special case of theorem 2 was presented in [7]. Namely, one can consider q-ary $[l, lm]$-QCC $\mathcal{C}$ as the principal ideal in a ring of polynomials with matrix coefficients. Let $G(x) = \sum_{i=0}^{m-1} G_i x^i$ be the matrix polynomial representation of its generating set, where G_i are $l \times l$ matrices. Let X be a $l \times l$ matrix being m-th root of identity matrix such that $G(X^j) = 0$, $0 < j < \delta$. Then the minimum distance of the code is not less than δ. This approach can be used only if $m \mid (q^{le} - 1)$ for some e. In this case one can take X as a companion matrix of an irreducible polynomial $f(x) \in \mathbb{F}_{q^e}[x]$ of degree l, such that $f(\alpha) = 0$. One can always construct the eigendecomposition $X = UDU^{-1}$, where $D = \mathrm{diag}(\lambda_0, \ldots, \lambda_{l-1})$, U is a $l \times l$ matrix with columns being eigenvectors of X, and one of its eigenvalues (assume w.l.o.g. λ_0) is a primitive m-th root of unity. Then one obtains $0 = G(X^j) = \sum_{i=0}^{m-1} A_i (U D^{ij} U^{-1})$. This is equivalent to $\sum_{i=0}^{m-1} A_i U D^{ij} = 0$. In particular, $\sum_{i=0}^{m-1} \lambda_0^{ij} A_i u_0 = 0$, where u_0 is the eigenvector corresponding to eigenvalue $\lambda_0 = \alpha$. This implies that α^j are eigenvalues of the polynomial matrix $G(x)$ with a common eigenvector u_0. Since the eigenvector of a companion matrix corresponding to eigenvalue λ_t is given by $(1, \lambda_t, \ldots, \lambda_t^{l-1})^T$, and $f(x)$ is an irreducible polynomial, one obtains that the elements of u_0 are linearly independent over $\mathbb{F}_{q^e}$. This corresponds to the case considered in theorem 2. However, the technique proposed in this paper neither assumes the existence of root X of $G(x)$ being a companion matrix of some polynomial, nor requires finding m-th root of identity matrix.

B. Lally bound

It was suggested in [8] to decompose q-ary $[l, lm]$-QCC $\mathcal{C}$ into a cyclic code $\mathbb{C}_1$ of length m over $\mathbb{F}_{q^l}$ and a linear code $\mathbb{C}_2$ of length l over $\mathbb{F}_q$. Then the minimum distance of $\mathcal{C}$ is not less than $d_L = d(\mathbb{C}_1) d(\mathbb{C}_2)$. Table I presents a comparison of this bound and the one given by theorem 2 for some codes from database [9]. It can be seen that the proposed method provides substantially improved minimum distance estimates.

TABLE I
QCC MINIMUM DISTANCE BOUNDS

$[n, k, d]$	l	m	δ	d_L
$[63, 13, 24]$	3	21	7	6
$[63, 15, 24]$	3	21	7	4
$[70, 25, 18]$	2	35	7	6
$[78, 36, 16]$	2	39	4	3
$[84, 21, 27]$	4	21	5	1
$[94, 24, 28]$	2	47	11	5
$[105, 35, 25]$	3	35	4	2
$[117, 39, 28]$	3	39	4	1
$[124, 31, 36]$	4	31	6	1
$[138, 35, 38]$	2	69	10	6
$[141, 24, 48]$	3	47	12	5
$[141, 47, 32]$	3	47	4	1
$[146, 45, 36]$	2	73	12	10
$[153, 10, 70]$	3	51	26	18
$[153, 51, 33]$	3	51	4	1
$[156, 13, 68]$	4	39	18	12
$[178, 44, 48]$	2	89	11	7
$[188, 24, 68]$	4	47	14	5
$[195, 13, 88]$	5	88	24	12
$[196, 46, 52]$	4	49	6	3
$[204, 34, 64]$	4	51	12	5
$[204, 49, 51]$	4	51	6	2
$[204, 50, 50]$	4	51	5	3
$[207, 33, 68]$	3	69	12	6
$[210, 58, 50]$	2	105	12	8
$[210, 61, 48]$	2	105	10	10
$[217, 21, 84]$	7	31	14	5
$[219, 19, 88]$	3	73	27	13
$[219, 46, 62]$	3	73	11	5
$[225, 20, 88]$	5	45	15	9
$[234, 12, 112]$	2	117	54	39
$[234, 24, 88]$	2	117	39	39
$[235, 47, 66]$	5	47	6	1
$[252, 11, 120]$	12	21	15	8
$[254, 22, 103]$	2	127	40	29
$[255, 45, 87]$	5	51	13	5

C. Tanner bound

A bound on the minimum distance of linear codes with certain symmetry properties, including quasi-cyclic codes, was proposed in [10], which is based on eigenvalues of circulant submatrices of the parity-check matrix. More specifically, if one can construct some vector $\mathbf{v} = (v_0, \ldots, v_{lm-1}) \in \mathbb{F}_{2^t}^{lm}$ with nonzero and distinct components based on eigenvalues and eigenvectors of these matrices, such that its vector powers $(v_0^i, \ldots, v_{lm-1}^i)$ are in the span of parity-check equations for $i \in I \subset \{0, \ldots, 2^t - 2\}$, then the minimum distance of this code is at least that of the cyclic code of length $(2^t - 1)$ with roots α^i, $i \in I$, where α is a primitive element of $\mathbb{F}_{2^t}$. This method essentially requires exhausitive search for all possible values of i which may be too expensive for large finite fields. Furthermore, if no suitable vector $\mathbf{v}$ exists, then one has to revert to linearized polynomial transform, which requires employing even larger finite fields ($\mathbb{F}_{2^m}$ in the notation of this paper). On the contrary, the proposed method obtains the eigenvalues needed by theorem 2 immediately as roots of $\det \tilde{G}(x)$, which can be found using the efficient polynomial factorization algorithms.

V. Conclusions

In this paper a generalization of the BCH bound to the case of quasi-cyclic codes was proposed. It was shown that the novel method provides substantially better minimum distance estimates compared to Lally bound. An important advantage of the proposed approach is that it employs very simple calculations such that finding roots of a scalar polynomial and computing a nullspace basis of a matrix.

VI. Acknowledgements

The authors thank the anonymous reviewers for their comments, which have greatly improved the quality of the paper, and also for pointing [10].

This work was partially supported by the grant MK-1976.2011.9 of the President of Russia.

References

[1] E. Weldon, "Long quasi-cyclic codes are good," *IEEE Trans. Inf. Theory*, vol. 16, no. 1, p. 130, Jan. 1970.

[2] T. Kasami, "A Gilbert-Varhamov bound for quasi-cyclic codes of rate $1/2$," *IEEE Trans. Inf. Theory*, vol. 20, no. 5, p. 674, Sep. 1974.

[3] G. Kabatyansky, "On existence of good cyclic almost linear codes over nonprime fields," *Problems of Inf. Transmission*, no. 3, pp. 175-177, 1977.

[4] K. Lally and P. Fitzpatrick, "Algebraic structure of quasi-cyclic codes," *Discrete Applied Mathematics*, no. 111, pp. 157–175, 2001.

[5] T. Becker and V. Weispfenning, *Gröbner Bases. A Computational Approach to Commutative Algebra*. Springer, 1993.

[6] I. Gohberg, P. Lancaster, and L. Rodman, *Matrix Polynomials*. SIAM, 2009.

[7] M. Barbier, C. Chabot, and G. Quintin, "On quasi-cyclic codes as a generalization of cyclic codes," http://arxiv.org/abs/1108.3754v1.

[8] K. Lally, "Quasicyclic codes of index l over $\mathbb{F}_q$ viewed as $\mathbb{F}_q[x]$-submodules of $\mathbb{F}_{q^t}[x]/\langle x^m - 1\rangle$," in *Proc. 2003 Conference on Applied Algebra and Error-Correcting Codes*, pp. 244–253.

[9] E. Chen, "Tables of known binary quasi-cyclic codes," http://www.tec.hkr.se/∼chen/research/codes/.

[10] R. M. Tanner, "A transform theory for a class of group-invariant codes," *IEEE Trans. Inf. Theory*, vol. 34, pp. 725–775, 1988.