Decoding of Quasi-Cyclic Codes up to A New Lower Bound on the Minimum Distance

Alexander Zeh, San Ling

Decoding of Quasi-Cyclic Codes up to A New Lower Bound on the Minimum Distance

Alexander Zeh
Computer Science Department
Technion—Israel Institute of Technology
Haifa, Israel
alex@codingtheory.eu

San Ling
Division of Mathematical Sciences, School of Physical & Mathematical Sciences, Nanyang Technological University
Singapore, Republic of Singapore
lingsan@ntu.edu.sg

***Abstract*—A new lower bound on the minimum Hamming distance of linear quasi-cyclic codes over finite fields is proposed. It is based on spectral analysis and generalizes the Semenov–Trifonov bound in a similar way as the Hartmann–Tzeng bound extends the BCH approach for cyclic codes. Furthermore, a syndrome-based algebraic decoding algorithm is given.**

***Index Terms*—Bound on the minimum distance, efficient decoding, quasi-cyclic code, spectral analysis**

I. Introduction

The class of linear quasi-cyclic codes over finite fields is a generalization of cyclic codes and is known to be asymptotically good (see, e.g., Chen–Peterson–Weldon [1]). Many of the best known linear codes belong to this class (see, e.g., Gulliver–Bhargava [2] and Chen's database [3]). Several good LDPC codes are quasi-cyclic and the connection to convolutional codes was investigated among others in [4]–[6].

The algebraic structure of quasi-cyclic codes was exploited in various ways (see, e.g., Lally–Fitzpatrick [7], Ling–Solé [8]–[10], Barbier *et al.* [11], [12]), but the estimates on the minimum distance are far away from the real minimum distance and thus the guaranteed decoding radius. Recently, Semenov and Trifonov [13] developed a spectral analysis of quasi-cyclic codes based on the work of Lally and Fitzpatrick [7], [14] and formulated a BCH-like lower bound on the minimum distance of quasi-cyclic codes.

We generalize the Semenov–Trifonov [13] bound on the minimum distance of quasi-cyclic codes. Our new approach is similar to the Hartmann–Tzeng (HT, [15], [16]) bound, which generalizes the BCH [17], [18] bound for cyclic codes. Moreover, we prove a quadratic-time syndrome-based algebraic decoding algorithm up to the new bound and show that it is advantageous in the case of burst errors.

This paper is organized as follows. In Section II, we recall the Gröbner basis representation of quasi-cyclic codes of Lally–Fitzpatrick [7], [14] and the definitions of the spectral method of Semenov–Trifonov [13]. The new HT-like bound on the minimum distance is formulated and proven in Section III. Section IV describes a syndrome-based decoding algorithm up to our bound and shows that in the case of burst errors more symbol errors can be corrected. We draw some conclusions in Section V.

A. Zeh has been supported by the German research council (Deutsche Forschungsgemeinschaft, DFG) under grant Ze1016/1-1. S. Ling has been supported by NTU Research Grant M4080456.

II. Preliminaries

A. Reduced Gröbner Basis

Let $\mathbb{F}_q$ denote the finite field of order q and $\mathbb{F}_q[X]$ the polynomial ring over $\mathbb{F}_q$ with indeterminate X. Let z be a positive integer and denote by $[z]$ the set of integers $\{0, 1, \ldots, z-1\}$. A vector of length n is denoted by a lowercase bold letter as $\mathbf{v} = (v_0\, v_1\, \ldots\, v_{n-1})$ and $\mathbf{v} \circ \mathbf{w}$ denotes the scalar product $\sum_{i=0}^{n-1} v_i w_i$ of two vectors $\mathbf{v}, \mathbf{w}$ of length n. An $m \times n$ matrix is denoted by a capital bold letter as $\mathbf{M} = (m_{i,j})_{i\in[m]}^{j\in[n]}$.

A linear $[m \cdot \ell, k, d]_q$ code $\mathcal{C}$ of length $m\ell$, dimension k and minimum Hamming distance d over $\mathbb{F}_q$ is ℓ-quasi-cyclic if every cyclic shift by ℓ of a codeword is again a codeword of $\mathcal{C}$, more explicitly if:

$$(c_{0,0} \ldots c_{\ell-1,0}\ c_{0,1} \ldots c_{\ell-1,1}\ \ldots\ c_{\ell-1,m-1}) \in \mathcal{C} \Rightarrow$$
$$(c_{0,m-1} \ldots c_{\ell-1,m-1}\ c_{0,0} \ldots c_{\ell-1,0}\ \ldots c_{\ell-1,m-2}) \in \mathcal{C}.$$

We can represent a codeword of an $[m \cdot \ell, k, d]_q$ ℓ-quasi-cyclic code as $\mathbf{c}(X) = (c_0(X)\ c_1(X)\ \ldots\ c_{\ell-1}(X)) \in \mathbb{F}_q[X]^\ell$, where

$$c_i(X) \stackrel{\text{def}}{=} \sum_{j=0}^{m-1} c_{i,j} X^j, \quad \forall i \in [\ell].$$

Then, the defining property of $\mathcal{C}$ is that each component $c_i(X)$ of $\mathbf{c}(X)$ is closed under multiplication by X and reduction modulo $X^m - 1$. Lally and Fitzpatrick [7], [14] showed that this enables us to see a quasi-cyclic code as an $\mathbb{F}_q[X]/\langle X^m - 1\rangle$-submodule of the algebra $(\mathbb{F}_q[X]/\langle X^m - 1\rangle)^\ell$ and they proved that every quasi-cyclic code has a generating set in the form of a reduced Gröbner basis with respect to the position-over-term order in $\mathbb{F}_q[X]^\ell$. This basis can be represented in the form of an upper-triangular $\ell \times \ell$ matrix with entries in $\mathbb{F}_q[X]$ as follows:

$$\widetilde{\mathbf{G}}(X) = \begin{pmatrix} g_{0,0}(X) & g_{0,1}(X) & \cdots & g_{0,\ell-1}(X) \\ & g_{1,1}(X) & \cdots & g_{1,\ell-1}(X) \\ & \mathbf{0} & \ddots & \vdots \\ & & & g_{\ell-1,\ell-1}(X) \end{pmatrix}, \quad (1)$$

where the following conditions must be fulfilled:

1) $g_{i,j}(X) = 0, \quad \forall 0 \le j < i < \ell,$
2) $\deg g_{j,i}(X) < \deg g_{i,i}(X), \quad \forall j < i, i \in [\ell],$
3) $g_{i,i}(X) | (X^m - 1), \quad \forall i \in [\ell],$
4) if $g_{i,i}(X) = X^m - 1$ then $g_{i,j}(X) = 0, \quad \forall j = i+1, \ldots, \ell-1.$

A codeword of $\mathcal{C}$ can be represented as $\mathbf{c}(X) = \mathbf{a}(X)\widetilde{\mathbf{G}}(X)$ and it follows that $k = m\ell - \sum_{i=0}^{\ell-1} \deg g_{i,i}(X)$.

For $\ell = 1$, the generator matrix $\widetilde{\mathbf{G}}(X)$ becomes the well-known generator polynomial of a cyclic code of degree $m-k$. We restrict ourselves throughout this paper to the single-root case, i.e., $\gcd(m, \text{char}(\mathbb{F}_q)) = 1$.

B. Spectral Analysis of Quasi-Cyclic Codes

Let $\widetilde{\mathbf{G}}(X)$ be the upper-triangular generator matrix of a given $[m \cdot \ell, k, d]_q$ ℓ-quasi-cyclic code $\mathcal{C}$ in reduced Gröbner basis form as in (1). Let $\alpha \in \mathbb{F}_{q^r}$ be an m-th root of unity. An eigenvalue $\lambda_i = \alpha^{j_i}$ of $\mathcal{C}$ is defined to be a root of $\det(\widetilde{\mathbf{G}}(X))$, i.e., a root of $\prod_{i=0}^{\ell-1} g_{i,i}(X)$. The *algebraic* multiplicity of λ_i is the largest integer u_i such that $(X - \lambda_i)^{u_i} \mid \det(\widetilde{\mathbf{G}}(X))$. Semenov and Trifonov [13] defined the *geometric* multiplicity of an eigenvalue λ_i as the dimension of the right kernel of the matrix $\widetilde{\mathbf{G}}(\lambda_i)$, i.e., the dimension of the solution space of the homogeneous linear system of equations:

$$\widetilde{\mathbf{G}}(\lambda_i)\mathbf{v} = \mathbf{0}. \tag{2}$$

The solution space of (2) is called the right kernel eigenspace and it is denoted by $\mathcal{V}_i$. Furthermore, it was shown that, for a matrix $\widetilde{\mathbf{G}}(X) \in \mathbb{F}_q[X]^{\ell \times \ell}$ in the reduced Gröbner basis representation, the algebraic multiplicity u_i of an eigenvalue λ_i equals the geometric multiplicity (see [13, Lemma 1]). Moreover, they gave in [13] an explicit construction of the parity-check matrix of an $[m \cdot \ell, k, d]_q$ ℓ-quasi-cyclic code $\mathcal{C}$ and proved a BCH-like [17], [18] lower bound on d using the parity-check matrix and the so-called eigencode. We generalize their approach, but do not explicitly need the parity-check matrix for the proof though the eigencode is still needed.

Definition 1 (Eigencode)**.** *Let $\mathcal{V} \subseteq \mathbb{F}_{q^r}^{\ell}$ be an eigenspace. Define the $[n^{ec} = \ell, k^{ec}, d^{ec}]_q$ eigencode corresponding to $\mathcal{V}$ by*

$$\mathbb{C}(\mathcal{V}) \stackrel{\text{def}}{=} \left\{ (c_0 \ldots c_{\ell-1}) \in \mathbb{F}_q^{\ell} \mid \forall \mathbf{v} \in \mathcal{V} : \sum_{i=0}^{\ell-1} v_i c_i = 0 \right\}. \tag{3}$$

If there exists $\mathbf{v} = (v_0 \ v_1 \ \ldots \ v_{\ell-1}) \in \mathcal{V}$ such that the elements $v_0, v_1, \ldots, v_{\ell-1}$ are linearly independent over $\mathbb{F}_q$, then $\mathbb{C}(\mathcal{V}) = \{(0 \ 0 \ \ldots \ 0)\}$ and d^{ec} is infinity. To describe quasi-cyclic codes explicitly, we need to recall the following facts about cyclic codes. A q-cyclotomic coset M_i is defined as:

$$M_i \stackrel{\text{def}}{=} \left\{ iq^j \mod m \,|\, j \in [a] \right\}, \tag{4}$$

where a is the smallest positive integer such that $iq^a \equiv i \bmod m$. The minimal polynomial in $\mathbb{F}_q[X]$ of the element $\alpha^i \in \mathbb{F}_{q^r}$ is given by $m_i(X) = \prod_{j \in M_i} (X - \alpha^j)$.

III. Improved Lower Bound

In this section, we generalize the lower bound on the minimum distance of quasi-cyclic codes given in [13, Thm. 2] in a similar way as the Hartmann–Tzeng bound [15], [16] generalizes the BCH bound [17], [18] for cyclic codes.

Theorem 1 (New Lower Bound)**.** *Let $\mathcal{C}$ be an $[m \cdot \ell, k, d]_q$ ℓ-quasi-cyclic code and let $\alpha \in \mathbb{F}_{q^r}$ denote an element of order m. Define the set*

$$\begin{aligned} D \stackrel{\text{def}}{=} \big\{ & f, f+z, \ldots, f+(\delta-2)z, \\ & f+1, f+1+z, \ldots, f+1+(\delta-2)z, \\ & \ddots \quad \ddots \quad \ldots \quad \ddots \\ & f+\nu, f+\nu+z, \ldots, f+\nu+(\delta-2)z \big\}, \end{aligned}$$

for some integers f, $\delta > 2$ and $z > 0$ with $\gcd(m, z) = 1$. Let the eigenvalues $\lambda_i = \alpha^i, \forall i \in D$, their corresponding eigenspaces $\mathcal{V}_i, \forall i \in D$, be given, and let their intersection be $\mathcal{V} \stackrel{\text{def}}{=} \bigcap_{i \in D} \mathcal{V}_i$.

Let d^{ec} denote the distance of the eigencode $\mathbb{C}(\mathcal{V})$ and let $\mathbf{v} = (v_0 \ v_1 \ \ldots \ v_{\ell-1}) \in \mathcal{V}$ be an eigenvector where $v_0, v_1, \ldots, v_{\ell-1}$ are linearly independent over $\mathbb{F}_q$. If

$$\sum_{i=0}^{\infty} \mathbf{c}(\alpha^{f+zi+j}) \circ \mathbf{v} X^i \equiv 0 \mod X^{\delta-1}, \ \forall j \in [\nu+1], \tag{5}$$

holds for all $\mathbf{c}(X) = \big(c_0(X) \ c_1(X) \ \ldots \ c_{\ell-1}(X)\big) \in \mathcal{C}$, then, $d \ge d^* \stackrel{\text{def}}{=} \min(\delta + \nu, d^{ec})$.

Proof: Let $c_i(X) = \sum_{j \in \mathcal{Y}_i} c_{i,j} X^j, \forall i \in [\ell]$, where $c_{i,j} \in \mathbb{F}_q$. We can write the LHS of (5) more explicitly:

$$\sum_{i=0}^{\infty} \left(\sum_{t=0}^{\ell-1} c_t(\alpha^{f+zi+j}) v_t \right) X^i \equiv 0 \bmod X^{\delta-1}, \forall j \in [\nu+1]. \tag{6}$$

Now, define:

$$\mathcal{Y} = \{i_0, i_1, \ldots, i_{y-1}\} \stackrel{\text{def}}{=} \bigcup_{i=0}^{\ell-1} \mathcal{Y}_i \subseteq [m]. \tag{7}$$

We obtain from (6) with (7) :

$$\sum_{i=0}^{\infty} \left(\sum_{s \in \mathcal{Y}} \left(\sum_{t=0}^{\ell-1} c_{t,s} v_t \right) \alpha^{(f+zi+j)s} \right) X^i \equiv 0 \bmod X^{\delta-1}, \ \forall j \in [\nu+1]. \tag{8}$$

We define m elements in $\mathbb{F}_{q^r}$ as follows:

$$C_s \stackrel{\text{def}}{=} \sum_{t=0}^{\ell-1} c_{t,s} v_t, \quad \forall s \in [m]. \tag{9}$$

With (9), we can simplify (8) to

$$\sum_{i=0}^{\infty} \left(\sum_{s \in \mathcal{Y}} C_s \alpha^{(f+zi+j)s} \right) X^i \equiv 0 \bmod X^{\delta-1}, \forall j \in [\nu+1]. \tag{10}$$

We linearly combine the $\nu+1$ sequences of (10), multiply each of them by an element $\omega_j \in \mathbb{F}_{q^r}\backslash\{0\}$ and obtain:

$$\sum_{j=0}^{\nu} \omega_j \sum_{i=0}^{\infty} \left(\sum_{s\in\mathcal{Y}} C_s \alpha^{(f+zi+j)s} \right) X^i \equiv 0 \bmod X^{\delta-1}. \quad (11)$$

Interchanging the sums in (11) leads to:

$$\sum_{i=0}^{\infty} \sum_{s\in\mathcal{Y}} \Big(C_s \alpha^{(f+zi)s} \sum_{j=0}^{\nu} \omega_j \alpha^{js} \Big) X^i \equiv 0 \bmod X^{\delta-1}. \quad (12)$$

We choose $\omega_0, \omega_1, \ldots, \omega_\nu$ such that the first ν terms with coefficients $C_{i_0}, C_{i_1}, \ldots, C_{i_{\nu-1}}$ are annihilated. We obtain the following linear $(\nu+1)\times(\nu+1)$ system of equations:

$$\begin{pmatrix} 1 & \alpha^{i_0} & \alpha^{i_0 2} & \cdots & \alpha^{i_0 \nu} \\ 1 & \alpha^{i_1} & \alpha^{i_1 2} & \cdots & \alpha^{i_1 \nu} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha^{i_\nu} & \alpha^{i_\nu 2} & \cdots & \alpha^{i_\nu \nu} \end{pmatrix} \begin{pmatrix} \omega_0 \\ \omega_1 \\ \vdots \\ \omega_\nu \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix}, \quad (13)$$

with Vandermonde structure and therefore the non-zero solution is unique. Let $\widetilde{\mathcal{Y}} \stackrel{\text{def}}{=} \mathcal{Y} \setminus \{i_0, i_1, \ldots, i_{\nu-1}\}$. Then we can rewrite (12):

$$\sum_{i=0}^{\infty} \sum_{s\in\widetilde{\mathcal{Y}}} \Big(C_s \alpha^{(f+zi)s} \sum_{j=0}^{\nu} \omega_j \alpha^{js} \Big) X^i \equiv 0 \bmod X^{\delta-1}. \quad (14)$$

With the geometric series we get from (14):

$$\sum_{s\in\widetilde{\mathcal{Y}}} \frac{C_s \alpha^{sf} \Big(\sum\limits_{j=0}^{\nu} \omega_j \alpha^{js} \Big)}{1-\alpha^{zs}X} \equiv 0 \mod X^{\delta-1},$$

and writing each fraction as an equivalent fraction with the least common denominator leads to:

$$\frac{\sum\limits_{s\in\widetilde{\mathcal{Y}}} \Big(C_s \alpha^{sf} \big(\sum\limits_{j=0}^{\nu} \omega_j \alpha^{js} \big) \prod\limits_{\substack{h\in\widetilde{\mathcal{Y}} \\ h\neq s}} (1-\alpha^{zh}X) \Big)}{\prod\limits_{s\in\widetilde{\mathcal{Y}}} (1-\alpha^{zs}X)} \equiv 0 \bmod X^{\delta-1}, \quad (15)$$

where the degree of the numerator is at most $|\widetilde{\mathcal{Y}}|-1 = y-\nu-1$ and has to be at least $\delta-1$.

To bound the distance d we distinguish two cases. For the first case where $d^{ec} > \delta+\nu$, at least $y-\nu$ elements $C_i \in \mathbb{F}_{q^r}$ have to be non-zero such that (15) holds, i.e., at least $y-\nu$ elements $c_{t_0,i_0}, c_{t_1,i_1}, \ldots, c_{t_{y-1-\nu},i_{y-1-\nu}} \in \mathbb{F}_q$ for $t_0, \ldots, t_{y-1-\nu}$ distinct, have to be non-zero and therefore $d-\nu-1 \geq \delta-1 \iff d \geq \delta+\nu$. For the second case where $d^{ec} < \delta+\nu$, at least d^{ec} elements $c_{j,i_0}, c_{j,i_1}, \ldots, c_{j,i_{d^{ec}-1}}$ have to be non-zero (see (9)) such that $C_j = 0$ and if all the other $C_s, s \in \widetilde{\mathcal{Y}}\backslash\{j\}$, are zero, then the LHS of (15) becomes zero. In this case $d \geq d^{ec}$. ∎

For $\nu = 0$, the bound of Theorem 1 becomes the bound of Semenov–Trifonov (see [13, Thm. 2]). We chose to state Thm. 1 in terms of all $\mathbf{c}(X) \in \mathcal{C}$ (see (5)) to easily obtain a syndrome expression (see Section IV). In practice, from the spectral analysis of $\widetilde{\mathbf{G}}(X)$, one can search for eigenvalues of the form α^i, for i in some D of the form in Thm. 1, and determine the corresponding eigencode with its minimum distance. The condition (5) is then automatically satisfied for all codewords $\mathbf{c}(X) \in \mathcal{C}$, with the corresponding f, z and δ.

Example 1 (HT-like Bound for Quasi-Cyclic Code)**.** *Let $\mathcal{C}$ be the binary $[63\cdot 2, 100, 6]_2$ 2-quasi-cyclic code with 2×2 generator matrix in reduced Gröbner form as defined in* (1)*:*

$$\widetilde{\mathbf{G}}(X) = \begin{pmatrix} g_{0,0}(X) & g_{0,1}(X) \\ 0 & g_{1,1}(X) \end{pmatrix},$$

where:

$$g_{0,0}(X) = m_0(X)m_1(X)m_9(X),$$
$$g_{0,1}(X) = g_{0,0}(X)a_{0,1}(X), \quad g_{1,1}(X) = g_{0,0}(X)m_5(X),$$

and $a_{0,1}(X) = X^4+X^3+X^2+X+1$ with $\deg a_{0,1}(X) < \deg m_5(X)$ and $a_{0,1}(X) \nmid (X^{63}-1)$.

Let $\alpha \in \mathbb{F}_{2^6} \cong \mathbb{F}_2[X]/(X^6+X^4+X^3+X+1)$ be an element of order 63. The eigenvalues $\lambda_i = \alpha^i, i \in \{0,1,2,4,8,9,16,18,32,36\} = M_0 \cup M_1 \cup M_9$ are the roots of $g_{0,0}(X)$, $g_{0,1}(X)$, $g_{1,1}(X)$ and have (algebraic and geometric) multiplicity two. Therefore, the corresponding eigenvectors span the full space $\mathbb{F}_{2^6}^2$. The distinct eigenvectors $\mathbf{v}^{(i)}, \forall i \in M_5$, are in $\mathbb{F}_{2^6}^2$ and $v_0^{(i)}, v_1^{(i)} \in \mathbb{F}_{2^6}$, are linearly independent over $\mathbb{F}_2$ for each $i \in M_5$.

With $f=0$, $z=4$, $\delta=4$, $\nu=1$, we obtain two consecutive sequences of eigenvalues $\alpha^0, \alpha^4, \alpha^8$ and $\alpha^1, \alpha^5, \alpha^9$ of length three, where $v_0^{(5)} = 1, v_1^{(5)} = \alpha^4+1$, are linearly independent over $\mathbb{F}_2$ and $\mathbf{v}^{(5)}$ is contained in the intersection of the eigenspaces $\mathcal{V}_i, i \in D \stackrel{\text{def}}{=} \{0,4,8,1,5,9\}$, and therefore $d^{ec} = \infty$ of $\mathbb{C}(\cap_{i\in D}\mathcal{V}_i)$. With Theorem 1, we can bound d to be at least $\delta+\nu = 5$, which is one less than the actual minimum distance for the $[63\cdot 2, 100, 6]_2$ 2-quasi-cyclic code. The bound of Semenov–Trifonov gives $d \geq 4$.

IV. Syndrome-Based Decoding of Quasi-Cyclic Codes

In this section, we develop a syndrome-based decoding algorithm, which guarantees to correct up to $\lfloor (d^*-1)/2 \rfloor$ symbol errors in $\mathbb{F}_q$. Let the received word of a given $[m\cdot\ell, k, d]_q$ ℓ-quasi-cyclic code be:

$$\begin{aligned} \mathbf{r}(X) &= \big(r_0(X) & \ldots\ r_{\ell-1}(X) \big) \\ &= \big(c_0(X)+e_0(X) & \ldots\ c_{\ell-1}(X)+e_{\ell-1}(X) \big), \end{aligned}$$

where

$$e_i(X) = \sum_{j\in\mathcal{E}_i} e_{i,j} X^j, \quad i \in [\ell], \quad (16)$$

are ℓ error polynomials in $\mathbb{F}_q[X]$ with $\varepsilon_i \stackrel{\text{def}}{=} |\mathcal{E}_i|$ and degree less than m. The number of errors in $\mathbb{F}_q$ is $\widetilde{\varepsilon} \stackrel{\text{def}}{=} \sum_{i=0}^{\ell-1} \varepsilon_i$. Define the following set of burst errors:

$$\mathcal{E} \stackrel{\text{def}}{=} \bigcup_{i=0}^{\ell-1} \mathcal{E}_i \subseteq [m]. \quad (17)$$

with cardinality $\varepsilon \stackrel{\text{def}}{=} |\mathcal{E}| \leq \widetilde{\varepsilon}$.

In the following, we describe a decoding procedure that is able to decode up to $\varepsilon \leq \tau$ errors, where:

$$\tau \leq \frac{d^* - 1}{2}. \tag{18}$$

Let $\alpha \in \mathbb{F}_{q^r}$ denote an m-th root of unity and let the $(\nu+1)(\delta-1)$ eigenvalues $\lambda_i = \alpha^{f+iz+j}, \forall i \in [\delta - 1], j \in [\nu+1]$, the integer f and the integer $z > 0$ with $\gcd(z, m) = 1$ be given as stated in Thm. 1. Furthermore, let $\mathcal{V} = \bigcap_{i\in[\delta-1], j\in[\nu+1]} \mathcal{V}_{f+iz+j}$ and let one eigenvector $\mathbf{v} = (v_0 \ v_1 \ \ldots \ v_{\ell-1}) \in \mathcal{V}$, where $v_0, v_1, \ldots, v_{\ell-1}$ are linearly independent over $\mathbb{F}_q$, be given. We assume that the minimum distance of the corresponding eigencode $\mathbb{C}(\mathcal{V})$ is greater than $\delta + \nu$. Then, we define the following $\nu + 1$ syndrome polynomials in $\mathbb{F}_{q^r}[X]$:

$$\begin{aligned} S_t(X) &\stackrel{\text{def}}{=} \sum_{i=0}^{\infty} \left(\sum_{j=0}^{\ell-1} r_j(\alpha^{f+iz+t}) v_j \right) X^i \mod X^{\delta-1} \\ &= \sum_{i=0}^{\delta-2} \left(\sum_{j=0}^{\ell-1} r_j(\alpha^{f+iz+t}) v_j \right) X^i, \ \forall t \in [\nu+1]. \end{aligned} \tag{19}$$

From Thm. 1 it follows that the syndrome polynomials as defined in (19) depend only on the error and therefore:

$$S_t(X) = \sum_{i=0}^{\delta-2} \left(\sum_{j=0}^{\ell-1} e_j(\alpha^{f+iz+t}) v_j \right) X^i, \quad \forall t \in [\nu+1].$$

Define an error-locator polynomial in $\mathbb{F}_{q^r}[X]$:

$$\Lambda(X) = \sum_{i=0}^{\varepsilon} \Lambda_i X^i \stackrel{\text{def}}{=} \prod_{i\in\mathcal{E}} (1 - X\alpha^{iz}). \tag{20}$$

Like in the classical case of cyclic codes, we get $\nu + 1$ *Key Equations* with a common error-locator polynomial $\Lambda(X)$ as defined in (20):

$$\Lambda(X) \cdot S_t(X) \equiv \Omega_t(X) \mod X^{\delta-1}, \quad \forall t \in [\nu+1], \tag{21}$$

where the degree of each of $\Omega_0(X), \Omega_1(X), \ldots, \Omega_\nu(X)$ is smaller than ε. Solving these $\nu+1$ Key Equations (21) jointly can be realized by multi-sequence shift-register synthesis and several efficient realizations exist [19]–[21].

Solving (21) jointly is equivalent to solving the following heterogeneous system of equations:

$$\begin{pmatrix} \mathbf{S}^{\langle 0 \rangle} \\ \mathbf{S}^{\langle 1 \rangle} \\ \vdots \\ \mathbf{S}^{\langle \nu \rangle} \end{pmatrix} \begin{pmatrix} \Lambda_\varepsilon \\ \Lambda_{\varepsilon-1} \\ \vdots \\ \Lambda_1 \end{pmatrix} = \begin{pmatrix} \mathbf{T}^{\langle 0 \rangle} \\ \mathbf{T}^{\langle 1 \rangle} \\ \vdots \\ \mathbf{T}^{\langle \nu \rangle} \end{pmatrix}, \tag{22}$$

where each $(\delta - 1 - \varepsilon) \times \varepsilon$ submatrix is a Hankel matrix:

$$\mathbf{S}^{\langle t \rangle} = \left(S_{i+j}^{\langle t \rangle} \right)_{i\in[\delta-1-\varepsilon]}^{j\in[\varepsilon]}, \quad \forall t \in [\nu+1], \tag{23}$$

and each $\mathbf{T}^{\langle t \rangle} = (S_\varepsilon^{\langle t \rangle} \ S_{\varepsilon+1}^{\langle t \rangle} \ \ldots \ S_{\delta-2}^{\langle t \rangle})^T$ with:

$$S_i^{\langle t \rangle} = \sum_{j=0}^{\ell-1} r_j(\alpha^{f+iz+t}) v_j, \quad \forall i \in [\delta-1], t \in [\nu+1].$$

Theorem 2 (Decoding up to New Bound)**.** *Let $\mathcal{C}$ be an ℓ-quasi-cyclic code and let the conditions of Thm. 1 hold. Let* (18) *be fulfilled, let the $\nu+1$ syndrome polynomials $S_0(X), S_1(X), \ldots, S_\nu(X)$ be defined as in* (19)*, and let the set of burst errors$\mathcal{E} = \{j_0, j_1, \ldots, j_{\varepsilon-1}\}$ be as defined in* (17)*. Then, the syndrome matrix $\mathbf{S} = (\mathbf{S}^{\langle 0 \rangle} \ \mathbf{S}^{\langle 1 \rangle} \ \ldots \ \mathbf{S}^{\langle \nu \rangle})^T$ with the submatrices from* (23) *has* $\operatorname{rank}(\mathbf{S}) = \varepsilon$.

Proof: Assume w.l.o.g. that $f = 0$. Similar to [20, Section VI], we can decompose the syndrome matrix into three matrices as follows: $\mathbf{S} = (\mathbf{S}^{\langle 0 \rangle} \ \mathbf{S}^{\langle 1 \rangle} \ \cdots \ \mathbf{S}^{\langle \nu \rangle})^T = \mathbf{X} \cdot \mathbf{Y} \cdot \overline{\mathbf{X}} = (\mathbf{X}^{\langle 0 \rangle} \ \mathbf{X}^{\langle 1 \rangle} \ \cdots \ \mathbf{X}^{\langle \nu \rangle})^T \cdot \mathbf{Y} \cdot \overline{\mathbf{X}}$, where $\mathbf{X}$ is a $(\nu+1)(\delta-1-\varepsilon) \times \varepsilon$ matrix over $\mathbb{F}_{q^r}$ and $\mathbf{Y}$ and $\overline{\mathbf{X}}$ are $\varepsilon \times \varepsilon$ matrices over $\mathbb{F}_{q^r}$. Explicitly the decomposition provides the following matrices:

$$\begin{aligned} \mathbf{X}^{\langle t \rangle} &= \left(\alpha^{(t+zi)j} \right)_{i\in[\delta-2-\varepsilon]}^{j\in\mathcal{E}}, \quad t \in [\nu+1], \\ \overline{\mathbf{X}} &= \left(\alpha^{izj} \right)_{i\in\mathcal{E}}^{j\in[\varepsilon]}, \quad \mathbf{Y} = \operatorname{diag}(E_{i_0}, E_{i_1}, \ldots, E_{i_{\varepsilon-1}}), \end{aligned}$$

where $E_i \stackrel{\text{def}}{=} \sum_{t=0}^{\ell-1} e_{i,t} v_t$ for all $i \in \mathcal{E}$.

Since $\mathbf{Y}$ is a diagonal matrix, it is non-singular. From $\gcd(m, z) = 1$, we know that $\overline{\mathbf{X}}$ is a Vandermonde matrix and has full rank. Hence, $\mathbf{Y} \cdot \overline{\mathbf{X}}$ is a non-singular $\varepsilon \times \varepsilon$ matrix and therefore $\operatorname{rank}(\mathbf{S}) = \operatorname{rank}(\mathbf{X})$. In order to analyze the rank of $\mathbf{X}$, we proceed similarly as in [20, Sec. VI]. We use the matrix operation from [22] to rewrite $\mathbf{X} = \mathbf{A} * \mathbf{B}$, where

$$\mathbf{A} = \left(\alpha^{ij} \right)_{i\in[\nu+1]}^{j\in\mathcal{E}} \quad \text{and} \quad \mathbf{B} = \mathbf{X}^{\langle 0 \rangle}.$$

We know from [22] that, if $\operatorname{rank}(\mathbf{A}) + \operatorname{rank}(\mathbf{B}) > \varepsilon$, then $\operatorname{rank}(\mathbf{A} * \mathbf{B}) = \varepsilon$. Since $\gcd(m, z) = 1$, both matrices $\mathbf{A}$ and $\mathbf{B}$ are Vandermonde matrices with $\operatorname{rank}(\mathbf{A}) = \min\{\nu + 1, \varepsilon\}$ and $\operatorname{rank}(\mathbf{B}) = \min\{\delta - 1 - \varepsilon, \varepsilon\}$. Assume w.l.o.g. that $(\delta - 1) > \nu$ (else we can interchange the roles δ and ν in Thm. 1). Therefore, from (18) we obtain $\varepsilon \leq (d^* - 1)/2 = (\delta + \nu - 1)/2 < \delta - 1$. Hence, investigating all four possible cases of $\operatorname{rank}(\mathbf{A}) + \operatorname{rank}(\mathbf{B})$ gives:

$$\begin{aligned} &\nu + 1 + \delta - 1 - \varepsilon \geq 2\varepsilon - \varepsilon + 1 = \varepsilon + 1 > \varepsilon, \\ &\nu + 1 + \varepsilon > \varepsilon, \\ &\varepsilon + \delta - 1 - \varepsilon = \delta - 1 > \varepsilon, \\ &\varepsilon + \varepsilon = 2\varepsilon > \varepsilon, \end{aligned}$$

Thus, $\operatorname{rank}(\mathbf{A}) + \operatorname{rank}(\mathbf{B}) > \varepsilon$. ∎

Algorithm 1 summarizes the whole decoding procedure, where the complexity is dominated by the operation in Line 2. After the syndrome calculation (in Line 1 of Algorithm 1), the $\nu+1$ Key Equations (21) are solved jointly (here in Line 2 with a Generalized Extended Euclidean Algorithm, GEEA [19]). Various other algorithms for solving the Key Equations jointly as in Line 2 with sub-quadratic time complexity exist. Afterwards, the roots of $\Lambda(X)$ as defined in (20) correspond to the positions of the burst errors as defined in (17) (see Line 3).

The error values $E_{i_0}, E_{i_0}, \ldots E_{i_{\varepsilon-1}}$ can be obtained from one of the $\nu + 1$ polynomials $\Omega_j(X)$ as given from the Key Equations (21) (see Line 7 in Algorithm 1). In Line 8,

each error value $E_{i_j} \in \mathbb{F}_{q^r}$ is mapped back to the ℓ error symbols $e_{i_j,0}, e_{i_j,1}, \ldots, e_{i_j,\ell-1} \in \mathbb{F}_q$ and the codeword $\mathbf{c}(X) = (c_0(X)\ c_1(X)\ \ldots\ c_{\ell-1}(X))$ can be reconstructed.

Algo 1: DECODING AN $[m\cdot\ell, k, d]_q$ QUASI-CYCLIC CODE

Input: Parameters m, ℓ, k, q, r of the quasi-cyclic code
Received word $\mathbf{r}(X) = (r_0(X)\ \ldots\ r_{\ell-1}(X)) \in \mathbb{F}_q[X]^\ell$
Integers $f, \delta > 2, \nu \geq 0$ and $z > 0$ with $\gcd(z, m) = 1$
Eigenvalues $\lambda_i = \alpha^{f+iz+j},\ \forall i \in [\delta - 1], j \in [\nu + 1]$
Eigenvector $(v_0\ v_1\ \ldots\ v_{\ell-1}) \in \mathbb{F}_{q^r}^\ell$
Output: Estimated codeword
$\mathbf{c}(X) = (c_0(X)\ c_1(X)\ \ldots\ c_{\ell-1}(X))$
or DECODING FAILURE

Calculate $S_0(X), S_1(X), \ldots, S_\nu(X)$ as in (19)
Solving Key Equations jointly
$(\Lambda(X), \Omega_0(X), \Omega_1(X), \ldots, \Omega_\nu(X))$ =
$\mathtt{GEEA}\big(X^{\delta-1}, S_0(X), S_1(X), \ldots, S_\nu(X)\big)$
Find all i: $\Lambda(\alpha^{-iz}) = 0 \Rightarrow \mathcal{E} = \{i_0, i_1, \ldots, i_{\varepsilon-1}\}$
if $\varepsilon < \deg \Lambda(X)$ **then**
    Declare DECODING FAILURE
else
    Determine error values $E_{i_0}, E_{i_1}, \ldots, E_{i_{\varepsilon-1}} \in \mathbb{F}_{q^r}$
    Determine $e_{i_j,0}, e_{i_j,1}, \ldots, e_{i_j,\ell-1} \in \mathbb{F}_q$, s.t.
    $\sum_{t=0}^{\ell-1} e_{i_j,t} v_t = E_{i_j}, \quad \forall i_j \in \mathcal{E}$
    $e_i(X) \leftarrow \sum_{j \in \mathcal{E}_i} e_{j,i} X^j, \quad \forall i \in [\ell]$
    $c_i(X) \leftarrow r_i(X) - e_i(X), \quad \forall i \in [\ell]$

Example 2 (Decoding up to HT-like New Bound)**.** *Suppose the all-zero codeword of the* $[63 \cdot 2, 100, 6]_2$ *2-quasi-cyclic code from Example 1 was transmitted. Let the two received polynomials in* $\mathbb{F}_2[X]$ *be:*

$$r_0(X) = e_0(X) = 1 + X^{32}, \qquad r_1(X) = e_1(X) = X^{32}.$$

We have $\widetilde{\varepsilon} = 3$*, but* $\varepsilon = 2$ *(see* (17)*). The eigenvector* $\mathbf{v}^{(5)} = (1\ \alpha^4\ 1) \in \mathbb{F}_{2^6}^2$ *is contained in the intersection of the eigenspaces* $\cap_{i \in D} \mathcal{V}_i$*, where* $D \stackrel{\text{def}}{=} \{0, 4, 8, 1, 5, 9\}$*, and is used for decoding. The system of two equations as in* (22) *becomes here:*

$$\begin{pmatrix} \alpha^{35} & \alpha^{26} \\ \alpha^{45} & \alpha^{33} \end{pmatrix} \begin{pmatrix} \Lambda_2 \\ \Lambda_1 \end{pmatrix} = \begin{pmatrix} \alpha^7 \\ \alpha^{51} \end{pmatrix},$$

and the corresponding error-locator polynomial is $\sum_{i=0}^{2} \Lambda_i X^i = 1 + \alpha^{49} X + \alpha^2 X^2 = (1 - X)(1 - X\alpha^{128})$*. The error-evaluation gives the two error values in* $\mathbb{F}_{2^6}$*:* $E_0 = 1$ *and* $E_{32} = \alpha^4$*. Therefore we can reconstruct the* $\widetilde{\varepsilon} = 3$ *error values* $e_{0,0} = 1$*,* $e_{32,0} = 1$ *and* $e_{32,1} = 1$ *in* $\mathbb{F}_2$*.*

V. CONCLUSION AND OUTLOOK

We proved a new lower bound on the minimum distance of quasi-cyclic codes based on the spectral analysis introduced by Semenov and Trifonov. Moreover, a syndrome-based decoding algorithm was developed and its correctness proven.

ACKNOWLEDGMENTS

This work was initiated when S. Ling was visiting the CS Department of the Technion. He thanks this institution for its hospitality.

REFERENCES

[1] C. L. Chen, W. W. Peterson, and E. J. Weldon Jr., "Some Results on Quasi-Cyclic Codes", *Inf. Control*, vol. 15, no. 5, pp. 407–423, 1969. DOI: 10.1016/S0019-9958(69)90497-5.

[2] T. Gulliver and V. Bhargava, "Some Best Rate 1/p and Rate (p-1)/p Systematic Quasi-Cyclic Codes", *IEEE Trans. Inform. Theory*, vol. 37, no. 3, pp. 552–555, 1991. DOI: 10.1109/18.79911.

[3] E. Z. Chen, *A Database on Binary Quasi-Cyclic Codes: http://moodle.tec.hkr.se/~chen/research/codes/qc.htm, accessed January 2014*.

[4] G. Solomon and H. C. A. v. Tilborg, "A Connection Between Block and Convolutional Codes", *SIAM J. Appl. Math.*, vol. 37, no. 2, pp. 358–369, 1979. DOI: 10.2307/2100842.

[5] M. Esmaeili, T. A. Gulliver, N. P. Secord, and S. A. Mahmoud, "A Link Between Quasi-Cyclic Codes and Convolutional Codes", *IEEE Trans. Inform. Theory*, vol. 44, no. 1, pp. 431–435, 1998. DOI: 10.1109/18.651076.

[6] K. Lally, "Algebraic Lower Bounds on the Free Distance of Convolutional Codes", *IEEE Trans. Inform. Theory*, vol. 52, no. 5, pp. 2101–2110, 2006. DOI: 10.1109/TIT.2006.872980.

[7] K. Lally and P. Fitzpatrick, "Algebraic Structure of Quasicyclic Codes", *Discrete Appl. Math.*, vol. 111, no. 1-2, pp. 157–175, 2001. DOI: 10.1016/S0166-218X(00)00350-4.

[8] S. Ling and P. Solé, "On the Algebraic Structure of Quasi-Cyclic Codes I: Finite fields", *IEEE Trans. Inform. Theory*, vol. 47, no. 7, pp. 2751–2760, 2001. DOI: 10.1109/18.959257.

[9] S. Ling and P. Solé, "On the Algebraic Structure of Quasi-Cyclic Codes II: Chain Rings", *Des. Codes Cryptogr.*, vol. 30, no. 1, pp. 113–130, 2003. DOI: 10.1023/A:1024715527805.

[10] S. Ling and P. Solé, "On the Algebraic Structure of Quasi-Cyclic Codes III: Generator Theory", *IEEE Trans. Inform. Theory*, vol. 51, no. 7, pp. 2692–2700, 2005. DOI: 10.1109/TIT.2005.850142.

[11] M. Barbier, C. Chabot, and G. Quintin, "On Quasi-Cyclic Codes as a Generalization of Cyclic Codes", *Finite Fields Th. App.*, vol. 18, no. 5, pp. 904–919, 2012. DOI: 10.1016/j.ffa.2012.06.003.

[12] M. Barbier, G. Quintin, and C. Pernet, "On the Decoding of Quasi-BCH Codes", *Intern. Workshop on Coding and Cryptography (WCC)*, Bergen, Norway, 2013.

[13] P. Semenov and P. Trifonov, "Spectral Method for Quasi-Cyclic Code Analysis", *IEEE Comm. Letters*, vol. 16, no. 11, pp. 1840–1843, 2012. DOI: 10.1109/LCOMM.2012.091712.120834.

[14] K. Lally and P. Fitzpatrick, "Construction and Classification of Quasi-cyclic Codes", *Intern. Workshop on Coding and Cryptography (WCC)*, Paris, France, 1999, pp. 11–20.

[15] C. R. P. Hartmann, "Decoding Beyond the BCH Bound", *IEEE Trans. Inform. Theory*, vol. 18, no. 3, pp. 441–444, 1972. DOI: 10.1109/TIT.1972.1054824.

[16] C. R. P. Hartmann and K. K. Tzeng, "Generalizations of the BCH Bound", *Inf. Control*, vol. 20, no. 5, pp. 489–498, 1972. DOI: 10.1016/S0019-9958(72)90887-X.

[17] R. C. Bose and D. K. Ray-Chaudhuri, "On A Class of Error Correcting Binary Group Codes", *Inf. Control*, vol. 3, no. 1, pp. 68–79, 1960. DOI: 10.1016/S0019-9958(60)90287-4.

[18] A. Hocquenghem, "Codes Correcteurs d'Erreurs", *Chiffres (Paris)*, vol. 2, pp. 147–156, 1959.

[19] G.-L. Feng and K. K. Tzeng, "A Generalized Euclidean Algorithm for Multisequence Shift-Register Synthesis", *IEEE Trans. Inform. Theory*, vol. 35, no. 3, pp. 584–594, 1989. DOI: 10.1109/18.30981.

[20] G.-L. Feng and K. Tzeng, "A Generalization of the Berlekamp–Massey Algorithm for Multisequence Shift-Register Synthesis with Applications to Decoding Cyclic Codes", *IEEE Trans. Inform. Theory*, vol. 37, no. 5, pp. 1274–1287, 1991. DOI: 10.1109/18.133246.

[21] A. Zeh and A. Wachter, "Fast Multi-Sequence Shift-Register Synthesis with the Euclidean Algorithm", *Adv. Math. Commun.*, vol. 5, no. 4, pp. 667–680, 2011. DOI: 10.3934/amc.2011.5.667.

[22] J. van Lint and R. Wilson, "On The Minimum Distance of Cyclic Codes", *IEEE Trans. Inform. Theory*, vol. 32, no. 1, pp. 23–40, 1986. DOI: 10.1109/TIT.1986.1057134.