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–Trifonov [13]). 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.

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 \( \mathbb{F}_q \). 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 \( v = (v_0 v_1 \ldots v_{n-1}) \) and \( v \circ w \) denotes the scalar product \( \sum_{i=0}^{n-1} v_i w_i \) of two vectors \( v, w \) of length \( n \). An \( m \times n \) matrix is denoted by a capital bold letter as \( M = (m_{ij})_{i \in [m], j \in [n]} \).

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

\[
\begin{align*}
& (c_{0,0} \cdots c_{\ell-1,0} c_{0,1} \cdots c_{\ell-1,1} \cdots c_{\ell-1,m-1}) \in C \Rightarrow \\
& (c_{0,m-1} \cdots c_{\ell-1,m-1} c_{0,0} \cdots c_{\ell-1,0} \cdots c_{\ell-1,m-2}) \in C.
\end{align*}
\]

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

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

Then, the defining property of \( C \) is that each component \( c_i(X) \) of \( c(X) \) 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:

\[
\tilde{G}(X) = \begin{pmatrix} g_{0,0}(X) & g_{0,1}(X) & \cdots & g_{0,\ell-1}(X) \\
g_{1,0}(X) & g_{1,1}(X) & \cdots & g_{1,\ell-1}(X) \\
0 & \ddots & \ddots & \vdots \\
g_{\ell-1,0}(X) & \cdots & g_{\ell-1,\ell-1}(X) \end{pmatrix}, \tag{1}
\]
where the following conditions must be fulfilled:
1) $g_{i,j}(X) = 0$, \forall 0 \leq j < i < \ell,$
2) $\deg g_{i,j}(X) < \deg g_{i,i}(X)$, \forall $j < i, i \in [\ell],$
3) $g_{i,i}(X) | (X^{m} - 1)$, \forall $i \in [\ell],$
4) if $g_{i,i}(X) = X^{m} - 1$ then
$g_{i,j}(X) = 0$, \forall $j = i + 1, \ldots, \ell - 1.$
A codeword of $C$ can be represented as $c(X) = a(X)G(X)$
and it follows that $k = m\ell - \sum_{i=0}^{\ell} \deg g_{i,i}(X).
For $\ell = 1$, the generator matrix $G(X)$ 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., $gcd(m, char(F_q)) = 1.$

B. Spectral Analysis of Quasi-Cyclic Codes

Let $G(X)$ be the upper-triangular generator matrix of a
given $[m \cdot \ell, k, d]_q \ell$-quasi-cyclic code $C$ in reduced Gröbner
basis form as in (1). Let $\alpha \in F_q^*$ be an $m$-th root of unity.
An eigenvalue $\lambda_i = \alpha^{v_i}$ of $C$ is defined to be a root of $det(G(X)),$
i.e., a root of $\prod_{i=1}^{\ell} g_{i,i}(X).$ The algebraic multiplicity of
$\lambda_i$ is the largest integer $u_i$ such that $(X - \lambda_i)^{u_i} | det(G(X)).$
Semenov and Trifonov [13] defined the geometric multiplicity
of an eigenvalue $\lambda_i$ as the dimension of the right kernel of
the matrix $G(\lambda_i),$ i.e., the dimension of the solution space of the
homogeneous linear system of equations:
\[
G(\lambda_i)v = 0. \tag{2}
\]
The solution space of (2) is called the right kernel eigenspace
and is denoted by $\mathcal{V}_i$. Furthermore, it was shown that, for
a matrix $G(X) \in F_q[X]^{\ell \times \ell}$ in the reduced Gröbner basis
representation, the algebraic multiplicity $u_i$ of an eigenvalue
$\lambda_i$ equals the geometric multiplicity (see [13, Lemma 1]).
Moreover, they gave in [13] an explicit construction of the
parity-check matrix of an $[m \cdot \ell, k, d]_q \ell$-quasi-cyclic code $C$
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 $V \subseteq F_q^d$ be an eigenspace.
Define the $[n^{ec} = \ell, k^{ec}, d^{ec}]_q$ eigencode corresponding to $V$
by
\[
\mathcal{C}(V) \defeq \left\{ (c_0, \ldots, c_{\ell-1}) \in F_q^d \mid \forall v \in V : \sum_{i=0}^{\ell-1} v_i c_i = 0 \right\}. \tag{3}
\]
If there exists $v = (v_0, v_1, \ldots, v_{\ell-1}) \in V$ such that the elements
$v_0, v_1, \ldots, v_{\ell-1}$ are linearly independent over $F_q$, then
$\mathcal{C}(V) = \{(0 \ 0 \ \ldots \ 0)\}$ and $d^{ec}$ is infinity. To describe
quasi-cyclic codes explicitly, we need to recall the following facts
about cyclic codes. A $q$-cyclicotomous coset $M_i$ is defined as:
\[
M_i \defeq \left\{ iq^j \mod m \mid j \in [a] \right\}, \tag{4}
\]
where $a$ is the smallest positive integer such that $iq^a \equiv i \mod m$.
The minimal polynomial in $F_{q^r}[X]$ of the element $\alpha^i \in F_{q^r}$
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 $C$ be an $[m \cdot \ell, k, d]_q \ell$-quasi-cyclic code and let $\alpha \in F_q^*$ denote an element of order $m$. Define the set

\[ D \defeq \{ f, f + z, \ldots, f + (\delta - 2)z, \]
\[ f + 1, f + 1 + z, \ldots, f + 1 + (\delta - 2)z, \]
\[ \ldots, \ldots, \ldots \}
\]
\[ f + \nu, f + \nu + z, \ldots, f + \nu + (\delta - 2)z \}, \]

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

\[ \mathcal{V} \defeq \bigcap_{i \in D} \mathcal{V}_i. \]

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

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

holds for all $c(X) = (c_0(X), c_1(X), \ldots, c_{\ell-1}(X)) \in C$, then,

\[ d \geq d^{ec} \defeq \min(\delta + \nu, d^{ec}). \]

Proof: Let $c_i(X) = \sum_{j=0}^{\ell} c_{i,j} X^j, \forall i \in \ell$, where $c_{i,j} \in F_q$.
We can write the LHS of (5) more explicitly:

\[ \sum_{i=0}^{\ell-1} \left( \sum_{j=0}^{\ell-1} c_{i,j} X^j \right) X^i = 0 \mod X^{\delta-1}, \forall j \in [\nu + 1]. \tag{6}\]

Now, define:

\[ \mathcal{Y} \defeq \{ i_0, i_1, \ldots, i_{\nu+1} \} \defeq \bigcup_{i=0}^{\ell-1} \mathcal{Y}_i \subseteq [m]. \tag{7}\]

We obtain from (6) with (7):

\[ \sum_{i=0}^{\ell-1} \left( \sum_{s \in \mathcal{Y}_i} \sum_{j=0}^{\ell-1} c_{i,s} X^j \right) X^i = 0 \mod X^{\delta-1}, \forall j \in [\nu + 1]. \tag{8}\]

We define $m$ elements in $F_q^*$ as follows:

\[ C_s \defeq \sum_{i=0}^{\ell-1} c_{i,s} X^j, \forall s \in [m]. \tag{9}\]

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

\[ \sum_{s \in \mathcal{Y}_i} \left( \sum_{s \in \mathcal{Y}_i} C_s \alpha^{f+i+j} \right) X^i = 0 \mod X^{\delta-1}, \forall j \in [\nu + 1]. \tag{10}\]
We linearly combine the \( \nu + 1 \) sequences of (10), multiply each of them by an element \( \omega_j \in \mathbb{F}_q \setminus \{0\} \) and obtain:

\[
\sum_{j=0}^{\nu} \omega_j \sum_{i=0}^{\infty} \left( \sum_{s \in \mathcal{Y}} C_i \alpha^{(f+zi+j)s} \right) X^i \equiv 0 \mod X^{d-1}. \tag{11}
\]

Interchanging the sums in (11) leads to:

\[
\sum_{i=0}^{\infty} \left( \sum_{s \in \mathcal{Y}} C_i \alpha^{(f+zi)s} \right) \omega_j X^i \equiv 0 \mod X^{d-1}. \tag{12}
\]

We choose \( \omega_0, \omega_1, \ldots, \omega_\nu \) such that the first \( \nu \) 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:

\[
\begin{pmatrix}
1 & \alpha_{i_0} & \alpha_{i_0}^2 & \cdots & \alpha_{i_0}^\nu \\
1 & \alpha_{i_1} & \alpha_{i_1}^2 & \cdots & \alpha_{i_1}^\nu \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
1 & \alpha_{i_{\nu-1}} & \alpha_{i_{\nu-1}}^2 & \cdots & \alpha_{i_{\nu-1}}^\nu \\
\end{pmatrix}
\begin{pmatrix}
\omega_0 \\
\omega_1 \\
\vdots \\
\omega_\nu \\
\end{pmatrix}
= 
\begin{pmatrix}
0 \\
0 \\
\vdots \\
1 \\
\end{pmatrix}, \tag{13}
\]

with Vandermonde structure and therefore the non-zero solution is unique. Let \( \mathcal{Y} \) be the binomial \([63 \cdot 2, 100, 6]_2\) 2- quasi-cyclic code with \( 2 \times 2 \) generator matrix in reduced Gröbner form as defined in (1):

\[
\tilde{G}(X) = \begin{pmatrix} g_{0,0}(X) & g_{0,1}(X) \\
g_{1,0}(X) & g_{1,1}(X) \end{pmatrix},
\]

where:

\[
g_{0,0}(X) = m_0(X)m_1(X)m_2(X), \quad g_{0,1}(X) = m_0(X)a_0(X), \quad g_{1,1}(X) = g_{0,0}(X)m_5(X), \quad g_{0,1}(X) = X^4 + X^3 + X^2 + X + 1.
\]

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 \( \lambda_i = \alpha^i, i \in \{0, 1, 2, 4, 8, 9, 16, 18, 32, 36\} = M_0 \cup M_1 \cup M_2 \) 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 \( \mathbb{F}_{2^6} \). The distinct eigenvectors \( v^{(i)} \), \( i \in M_5 \), are in \( \mathbb{F}_{2^6} \) and \( v_0 \) and \( v_1 \) 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 \( \alpha_0, \alpha_4, \alpha_8, \alpha_9 \) of length three, where \( v^{(5)} = 1, v^{(5)} = \alpha^4 + 1 \), are linearly independent over \( \mathbb{F}_2 \) and \( v^{(5)} \) is contained in the intersection of the eigenspaces \( V_i, i \in D \triangleq \{0, 4, 8, 1, 5, 9\} \), and therefore \( d_{ec} = \infty \) of \( \mathbb{C}(\cap_{i \in D} V_i) \). 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-CYCLOIC CODES

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

\[
\mathbf{r}(X) = \begin{pmatrix} r_0(X) & \cdots & r_{\ell-1}(X) \end{pmatrix}
= \begin{pmatrix} c_0(X) + \epsilon(X) & \cdots & c_{\ell-1}(X) + \epsilon_{\ell-1}(X) \end{pmatrix},
\]

where

\[
e_i(X) = \sum_{j \in E_i} e_i \cdot X^j, \quad i \in [\ell], \tag{16}
\]

are \( \ell \) error polynomials in \( \mathbb{F}_q[X] \) with \( \epsilon_i \triangleq |E_i| \) and degree less than \( m \). The number of errors in \( \mathbb{F}_q \) is \( \epsilon \triangleq \sum_{i = 0}^{\ell-1} \epsilon_i \).

Define the following set of burst errors:

\[
E \triangleq \bigcup_{i = 0}^{\ell-1} E_i \subseteq [m]. \tag{17}
\]

with cardinality \( \epsilon \triangleq |E| \leq \epsilon \).
In the following, we describe a decoding procedure that is able to decode up to \( \varepsilon \leq \tau \) errors, where:

\[
\tau \leq \frac{d^* - 1}{2}.
\] (18)

Let \( \alpha \in \mathbb{F}_{q^r} \) denote an \( m \)-th root of unity and let the \((\nu + 1)(\delta - 1)\) eigenvalues \( \lambda_i = \alpha^{f+iz+t}, \forall i \in [\delta - 1], j \in [\nu + 1] \), the integer \( f \) and the integer \( z \geq 0 \) with \( \gcd(z, m) = 1 \) be given as stated in Thm. 1. Furthermore, let \( \mathcal{V} = \bigcap_{i \in [\delta - 1], j \in [\nu + 1]} \mathcal{V}_{f+iz+t} \) 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 \( \mathbb{F}_{q^r} \), 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 \( \mathbb{F}_{q^r}[X] \):

\[
S_t(X) \overset{\text{def}}{=} \sum_{i=0}^{\ell - 1} \left( \sum_{j=0}^{\delta - 2} r_j(\alpha^{f+iz+t})v_j \right) X^i \quad \text{mod} \quad X^{\delta - 1},
\]

\[
= \sum_{i=0}^{\delta - 2} \left( \sum_{j=0}^{\ell - 1} r_j(\alpha^{f+iz+t})v_j \right) X^i, \quad \forall t \in [\nu + 1]. \quad (19)
\]

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

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

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

\[
\Lambda(X) = \sum_{i=0}^{\ell - 1} \Lambda_i X^i \overset{\text{def}}{=} \prod_{i \in \mathcal{E}} (1 - X \alpha^{i \varepsilon}). \quad (20)
\]

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):

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

where the degree of each of \( \Omega_0(X), \Omega_1(X), \ldots, \Omega_{\nu}(X) \) is smaller than \( \varepsilon \). 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:

\[
\begin{pmatrix}
S(0) \\
S(1) \\
\vdots \\
S(\nu)
\end{pmatrix}
\begin{pmatrix}
\Lambda_0 \\
\Lambda_{\delta - 1} \\
\vdots \\
\Lambda_1
\end{pmatrix} =
\begin{pmatrix}
T(0) \\
T(1) \\
\vdots \\
T(\nu)
\end{pmatrix},
\]

(22)

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

\[
S(t) = \begin{pmatrix}
S(t) \overset{\text{def}}{=} \sum_{i \in [\delta - 1 - \varepsilon]} S(i)
\end{pmatrix}, \quad \forall t \in [\nu + 1], \quad (23)
\]

and each \(T(t) = \begin{pmatrix} T(t) \overset{\text{def}}{=} \sum_{i \in [\delta - 2]} S(i) \end{pmatrix}^T\) with:

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

**Theorem 2** (Decoding up to New Bound), Let \( C \) be an \( \ell \)-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 \( \mathcal{E} = \{j_0, j_1, \ldots, j_{\ell - 1}\} \) be as defined in (17). Then, the syndrome matrix \( S = (S(0) \ S(1) \ldots S(\nu))^T \) with the submatrices from (23) has rank(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: \( S = (S(0) \ S(1) \ldots S(\nu))^T = X \cdot Y \cdot \Xi \). \( \Xi \) is a Vandermonde matrix with the following matrices:

\[
X(t) = \begin{pmatrix}
(\alpha^{(t+iz)})_{j \in [\delta - \varepsilon - t]} \\
(\alpha^{(t+iz)})_{j \in [\delta - \varepsilon - t]}
\end{pmatrix}, \quad t \in [\nu + 1],
\]

\[
\Xi = \begin{pmatrix}
(\alpha^{(t+iz)})_{j \in [\varepsilon]} \\
(\alpha^{(t+iz)})_{j \in [\varepsilon]}
\end{pmatrix}, \quad Y = \text{diag}(E_{i_0}, E_{i_1}, \ldots, E_{i_{\ell - 1}}),
\]

where \( E_i \overset{\text{def}}{=} \sum_{t=0}^{\ell - 1} c_i t v_t \) for all \( i \in \mathcal{E} \).

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

\[
A = \begin{pmatrix}
(\alpha^{ij})_{j \in [\varepsilon]} \\
(\alpha^{ij})_{j \in [\varepsilon]}
\end{pmatrix}, \quad B = X(0).
\]

We know from [22] that, if \( \text{rank}(A) + \text{rank}(B) > \varepsilon \), then \( \text{rank}(A \ast B) = \varepsilon \). Since \( \text{gcd}(m, z) = 1 \), both matrices \( A \) and \( B \) are Vandermonde matrices with \( \text{rank}(A) = \min\{\nu + 1, \varepsilon\} \) and \( \text{rank}(B) = \min\{\delta - 1 - \varepsilon, \varepsilon\} \). Assume w.l.o.g. that \((\delta - 1) > \nu \) (else we can interchange the roles \( \delta \) and \( \nu \) 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 \( \text{rank}(A) + \text{rank}(B) \) gives:

\[
\begin{align*}
\nu + 1 + \delta - 1 - \varepsilon &\geq 2\varepsilon - \varepsilon + 1 = \varepsilon + 1 > \varepsilon, \\
\nu + 1 + \varepsilon > \varepsilon, \\
\varepsilon + \delta - 1 - \varepsilon = \delta - 1 > \varepsilon, \\
\varepsilon + \varepsilon = 2\varepsilon > \varepsilon.
\end{align*}
\]

Thus, \( \text{rank}(A) + \text{rank}(B) > \varepsilon \). ■

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 \( E_{i_0}, E_{i_1}, \ldots, E_{i_{\ell - 1}} \) 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 $E_{ij} \in \mathbb{F}_q$ is mapped back to the $\ell$ error symbols $e_{i_0, i_1, \ldots, i_{\ell-1}} \in \mathbb{F}_q$ and the codeword $c(X) = (c_0(X), c_1(X), \ldots, c_{\ell-1}(X))$ can be reconstructed.

**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 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: 10.1016/0019-9958(69)90497-5.

[2] T. Galliver and V. Bhargava, “Some Best Rate 1/2 and Rate (p-1)/p Systematic Quasi-Cyclic Codes”, *IEEE Trans. Inform. Theory*, vol. 37, no. 3, pp. 552–555, 1991. DOI: 10.1109/18.29911.

[3] E. Z. Chen, A Database on Binary Quasi-Cyclic Codes: [http://moodle.tei.krt.gr/~chen/research/codes/qc.htm](http://moodle.tei.krt.gr/~chen/research/codes/qc.htm), accessed January 2014.

[4] G. Solomon and H. C. A. van 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. Galliver, 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. Perret, “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)*, Bergen, Norway, 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. 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.