# Decoding of Repeated-Root Cyclic Codes up to New Bounds on Their Minimum Distance

Alexander Zeh, Markus Ulmschneider

# Decoding of Repeated-Root Cyclic Codes up to New Bounds on Their Minimum Distance

Alexander Zeh
Computer Science Department
Technion, Haifa, Israel
alex@codingtheory.eu

Markus Ulmschneider
Institute of Communications and Navigation
German Aerospace Center (DLR), Germany
markus.ulmschneider@dlr.de

**Abstract**

The well-known approach of Bose, Ray-Chaudhuri and Hocquenghem and its generalization by Hartmann and Tzeng are lower bounds on the minimum distance of simple-root cyclic codes. We generalize these two bounds to the case of repeated-root cyclic codes and present a syndrome-based burst error decoding algorithm with guaranteed decoding radius based on an associated folded cyclic code.

Furthermore, we present a third technique for bounding the minimum Hamming distance based on the embedding of a given repeated-root cyclic code into a repeated-root cyclic product code. A second quadratic-time probabilistic burst error decoding procedure based on the third bound is outlined.

**Index Terms**

Bound on the minimum distance, burst error, efficient decoding, folded code, repeated-root cyclic code, repeated-root cyclic product code

## I. Introduction

The length of a conventional linear cyclic block code $\mathcal{C}$ over a finite field $\mathbb{F}_q$ has to be co-prime to the field characteristic $p$. This guarantees that the generator polynomial of $\mathcal{C}$ has roots of multiplicity at most one and therefore we refer to these codes as simple-root cyclic codes. The approach of Bose and Ray-Chaudhuri and Hocquenghem (BCH, [1], [2]) and of Hartmann and Tzeng (HT, [3], [4]) gives a lower bound on the minimum distance of simple-root cyclic codes. Both approaches are based on consecutive sequences of roots of the generator polynomial. We give—similar to the BCH and the HT bound—two lower bounds on the minimum Hamming distance of a repeated-root cyclic code, i.e., a cyclic code whose length is not relatively co-prime to the characteristic $p$ of the field $\mathbb{F}_q$ and therefore its generator polynomial can have roots with multiplicities greater than one.

Repeated-root cyclic codes were first investigated by Berman [5]. A special class of Maximum Distance Separable (MDS) repeated-root constacyclic codes was treated by Massey *et al.* in [6], [7] and the advantages of a syndrome-based decoding were outlined. An alternative derivation of the minimum Hamming distance of these repeated-single-root MDS codes and their application to secret-key cryptosystems was given by da Rocha in [8]. Castagnoli *et al.* [9]–[11] gave an elaborated description of repeated-root cyclic codes including the explicit construction of the parity-check matrix, which was investigated for the case $q = 2$ slightly earlier by Latypov [12]. Although the asymptotic badness of repeated-root cyclic codes was shown in [9]–[11], several good binary repeated-root cyclic codes were constructed by van Lint in [13] with distances close to the Griesmer bound. Zimmermann [14] reproved some of Castagnoli's result by cyclic group algebra and Nedeloaia gave a squaring construction of all binary repeated-root cyclic codes in [15]. Recent publications of Ling–Niederreiter–Solé [16] and Dinh [17], [18] consider repeated-root quasi-cyclic codes.

Besides the generalization of the BCH and the HT bound to repeated-root cyclic codes, we provide a third lower bound on the minimum Hamming distance. Similar to the approach [19], [20] for simple-root cyclic codes, this bound is based on the embedding of a given repeated-root cyclic code into a repeated-root cyclic product code.

This work has been supported by the German research council (Deutsche Forschungsgemeinschaft, DFG) under grants Bo867/22-1 and Ze1016/1-1 and was initiated when both authors were affiliated with the Institute of Communications Engineering, University of Ulm, Ulm, Germany.

Therefore, we recall the relevant theorems of Burton and Weldon [21] and Lin and Weldon [22] for repeated-root cyclic product codes that are the basis for the proof of our third bound, which generalizes the results of our previous work on simple-root cyclic codes [19], [20]. Moreover, we present two burst error decoding schemes based on the derived bounds.

The paper is structured as follows. In Section II, we give necessary preliminaries for repeated-root cyclic codes and introduce our notation. Section III provides the generalizations of the BCH and the HT bound, which are denoted by $d_{\mathsf{I}}$ and $d_{\mathsf{II}}$ respectively, and in addition a syndrome-based error-correction algorithm with guaranteed decoding radius. The defining set of a repeated-root cyclic product code is given explicitly in Section IV, which is necessary to prove our third bound $d_{\mathsf{III}}$ on the minimum Hamming distance of a repeated-root cyclic code in Section V. Section VI gives a probabilistic burst error decoding approach based on the Generalized Extended Euclidean Algorithm (GEEA, [23]). We conclude this paper in Section VII.

## II. Repeated-Root Cyclic Codes

### A. Notation and Preliminaries

Let $q$ be a power of a prime $p$. $\mathbb{F}_q$ denotes the finite field of order $q$ and characteristic $p$ and $\mathbb{F}_q[X]$ the polynomial ring over $\mathbb{F}_q$ with indeterminate $X$. Let $n$ be a positive integer and denote by $[n)$ the set of integers $\{0, 1, \ldots, n-1\}$. A vector of length $n$ is denoted by a lowercase bold letter as $\mathbf{v} = (v_0\, v_1\, \ldots\, v_{n-1})$. A set is denoted by a capital letter sans serif like $\mathsf{D}$.

A linear $[n, k, d]_q$ code over $\mathbb{F}_q$ of length $n$, dimension $k$ and minimum Hamming distance $d$ is denoted by a calligraphic letter like $\mathcal{C}$.

Let us recapitulate the definition of the Hasse derivative [24] in the following. Let $a(X) = \sum_i a_i X^i$ be a polynomial in $\mathbb{F}_q[X]$, then the $j$-th Hasse derivative is:

$$a^{[j]}(X) \stackrel{\text{def}}{=} \sum_i \binom{i}{j} a_i X^{i-j}. \tag{1}$$

Let $a^{(j)}(X)$ denote the formal $j$-th derivative of $a(X)$. The fact that $a^{(j)}(X) = j!\, a^{[j]}(X)$ explains why the Hasse derivative is considered in fields with a prime characteristic $p$, because then $j! = 0$ and hence also $a^{(j)}(X) = 0$ for all $j \geq p$. We say a univariate polynomial $a(X) \in \mathbb{F}_q[X]$ with $\deg a(X) \geq s$ has a root at $\gamma$ with multiplicity $s$ if:

$$a^{[j]}(\gamma) = 0, \quad \forall j \in [s).$$

### B. Defining Set

A linear $[\overline{n}, \overline{k}, \overline{d}]_q$ simple-root cyclic code $\overline{\mathcal{C}}$ over $\mathbb{F}_q$ with characteristic $p$ is an ideal in the ring $\mathbb{F}_q[X]/(X^{\overline{n}} - 1)$ generated by $\overline{g}(X)$, where $\gcd(\overline{n}, p) = 1$. The generator polynomial $\overline{g}(X) \in \mathbb{F}_q[X]$ has roots with multiplicity at most one in the splitting field $\mathbb{F}_{q^l}$, where $\overline{n} \mid (q^l - 1)$. A cyclotomic coset $M_{i,\overline{n},q}$ is denoted by:

$$M_{i,\overline{n},q} = \big\{\, iq^j \mod \overline{n} \mid j \in [\overline{n}_i) \big\},$$

where $\overline{n}_i$ is the smallest integer such that $iq^{\overline{n}_i} \equiv i \mod \overline{n}$. Let $\gamma$ be an element of order $\overline{n}$ in $\mathbb{F}_{q^l}$. The minimal polynomial of the element $\gamma^i$ is:

$$M_{i,\overline{n},q}(X) = \prod_{j \in M_{i,\overline{n},q}} (X - \gamma^j).$$

Let $\gcd(\overline{n}, p) = 1$ and $n = p^s \overline{n}$. A linear $[n, k, d]_q$ repeated-root cyclic code $\mathcal{C}$ is an ideal in the ring

$$\mathbb{F}_q[X]/(X^n - 1) = \mathbb{F}_q[X]/(X^{\overline{n}} - 1)^{p^s}.$$

The generator polynomial of an $[n, k, d]_q$ repeated-root cyclic code $\mathcal{C}$ is

$$g(X) = \prod_i M_{i,\overline{n},q}(X)^{s_i},$$

where $s_i \leq p^s$. The defining set $\mathsf{D}_\mathcal{C}$ of an $[n = p^s\overline{n}, k, d]_q$ repeated-root cyclic code $\mathcal{C}$ with generator polynomial $g(X)$ is a set of tuples, where the first entry of the tuple is the index of a zero and the second its multiplicity, namely:

$$\mathsf{D}_\mathcal{C} = \left\{ i^{\langle s_i \rangle} \mid 0 \leq i \leq \overline{n} - 1, \quad g^{[j]}(\gamma^i) = 0, \quad \forall j \in [s_i) \right\}, \tag{2}$$

Furthermore, we introduce the following short-hand notation for a given $z \in \mathbb{Z}$:

$$\mathsf{D}_\mathcal{C}^{[z]} \stackrel{\text{def}}{=} \left\{ (i+z)^{\langle s_i \rangle} \mid i^{\langle s_i \rangle} \in \mathsf{D}_\mathcal{C} \right\}. \tag{3}$$

For two given defining sets $\mathsf{D}_\mathcal{A}$ and $\mathsf{D}_\mathcal{B}$, define

$$\mathsf{D}_\mathcal{A} \stackrel{\max}{\cup} \mathsf{D}_\mathcal{B} \stackrel{\text{def}}{=} \left\{ i^{\langle s_i \rangle} \mid s_i = \max(a_i, b_i), \text{where } i^{\langle a_i \rangle} \in \mathsf{D}_\mathcal{A} \text{ and } i^{\langle b_i \rangle} \in \mathsf{D}_\mathcal{B} \right\}. \tag{4}$$

## III. Two Bounds On the Minimum Hamming Distance of Repeated-Root Cyclic Codes And Burst Error Correction

### A. Lower Bounds on the Minimum Hamming Distance

In the following, we prove two lower bounds on the minimum Hamming distance of repeated-root cyclic codes. They generalize the well-known BCH [1], [2] and HT [3] approach suited for simple-root cyclic codes.

**Theorem 1** (Bound I: BCH-like Bound for a Repeated-Root Cyclic Code)**.** *Let an $[n, k, d]_q$ repeated-root cyclic code $\mathcal{C}$ over $\mathbb{F}_q$ with characteristic $p$ and generator polynomial $g(X)$ with $\deg g(X) \geq p^s - 1$ be given. Let $n = p^s\overline{n}$, where $\gcd(\overline{n}, p) = 1$. Let $\gamma$ be an element of order $\overline{n}$ in an extension field of $\mathbb{F}_q$. Furthermore, let three integers $f$, $m \neq 0$ and $\delta \geq 2$ with $\gcd(\overline{n}, m) = 1$ be given, such that for any codeword $c(X) \in \mathcal{C}$*

$$\sum_{i=0}^{\infty} c^{[p^s-1]}(\gamma^{f+im}) X^i \equiv 0 \mod X^{\delta-1} \tag{5}$$

*holds. Then, the minimum distance of $\mathcal{C}$ is at least $d_I \stackrel{\text{def}}{=} \delta$.*

*Proof:* First, let us prove that the left-hand side of (5) cannot be zero. Assume it is the zero polynomial. Then, all $\gamma^0, \gamma^1, \ldots, \gamma^{\overline{n}-1}$ are roots of the codeword $c(X)$ with multiplicity $p^s$, yielding that $\deg c(X) = p^s\overline{n} = n$, which contradicts the fact that the degree of a codeword $c(X)$ of an $[n, k, d]_q$ code is smaller than $n$. Second, we rewrite the expression left-hand side of (5) more explicitly. Let $\mathsf{Y} = \{i : c_i \neq 0\}$ be the support of a non-zero codeword. We obtain:

$$\begin{aligned} \sum_{i=0}^{\infty} c^{[p^s-1]}(\gamma^{f+im}) X^i &= \sum_{i=0}^{\infty} \sum_{u \in \mathsf{Y}} \tbinom{u}{p^s-1} c_u \left(\gamma^{f+im}\right)^{u-p^s+1} X^i \\ &= \sum_{u \in \mathsf{Y}} \tbinom{u}{p^s-1} c_u \gamma^{(u-p^s+1)f} \sum_{i=0}^{\infty} \left(\gamma^{(u-p^s+1)m} X\right)^i. \end{aligned} \tag{6}$$

With the geometric series, we get from (6):

$$\sum_{u \in \mathsf{Y}} \tbinom{u}{p^s-1} c_u \gamma^{(u-p^s+1)f} \sum_{i=0}^{\infty} \left(\gamma^{(u-p^s+1)m} X\right)^i = \sum_{u \in \mathsf{Y}} \tbinom{u}{p^s-1} c_u \gamma^{(u-p^s+1)f} \frac{1}{1 - \gamma^{(u-p^s+1)m} X}, \tag{7}$$

and with

$$\sum_{i \in \mathsf{Y}} \frac{a_i}{1 - X b_i} = \frac{\sum_{i \in \mathsf{Y}} a_i \frac{D}{1 - X b_i}}{D}, \tag{8}$$

where $D \stackrel{\text{def}}{=} \operatorname{lcm}((1 - X b_i) : i \in \mathsf{Y})$, we obtain from (7):

$$\sum_{u \in \mathsf{Y}} \tbinom{u}{p^s-1} c_u \gamma^{(u-p^s+1)f} \frac{1}{1 - \gamma^{(u-p^s+1)m} X} = \frac{\sum_{u \in \mathsf{Y}} \tbinom{u}{p^s-1} c_u \gamma^{(u-p^s+1)f} \frac{\operatorname{lcm}\left(1 - \gamma^{(j-p^s+1)m} X \,:\, j \in \mathsf{Y}\right)}{1 - \gamma^{(u-p^s+1)m} X}}{\operatorname{lcm}\left(1 - \gamma^{(i-p^s+1)m} X \;:\; i \in \mathsf{Y}\right)} \tag{9}$$

$$\equiv 0 \mod X^{\delta-1}. \tag{10}$$

Obviously, the degree of the numerator of (9) cannot be greater than $|\mathsf{Y}|-1$, and it cannot be smaller than $\delta-1$, since (10) must be fulfilled. Since this is true for all codewords, the minimum distance of $\mathcal{C}$ is not smaller than $|\mathsf{Y}|$. Thus, with $|\mathsf{Y}| \geq \delta$ follows that the true minimum distance of $\mathcal{C}$ is at least $\delta$. ■

Thm. 1 tells us that a repeated-root cyclic code of length $n = p^s\overline{n}$ with generator polynomial $g(X)$ that has $\delta-1$ consecutive zeros of highest multiplicity $p^s$, i.e.,

$$g^{[p^s-1]}(\gamma^f) = g^{[p^s-1]}(\gamma^{f+m}) = \cdots = g^{[p^s-1]}(\gamma^{f+(\delta-2)m}) = 0,$$

has at least minimum distance $\delta$. If $s=0$, the repeated-root cyclic code is a simple-root cyclic code and then Thm. 1 coincides with the BCH bound [1], [2].

**Remark 2** (Parameters)**.** *To obtain the parameters $f, m$ and $\delta$ as in Thm. 1, one needs to check the $(p^s-1)$th Hasse derivative of the given generator polynomial (respectively the defining set) of a given repeated-root cyclic code and find $f$ and $m$ that maximize $\delta$. The advantage of the representation as in* (5) *and in* (11) *is that a syndrome definition can directly be obtained and an algebraic decoding algorithm can be formulated (see Section III-B).*

**Theorem 3** (Bound II: HT-like for a Repeated-Root Cyclic Code)**.** *Let an $[n = p^s\overline{n}, k, d]_q$ repeated-root cyclic code $\mathcal{C}$ over $\mathbb{F}_q$ with characteristic $p$ and generator polynomial $g(X)$ with $\deg g(X) \geq p^s-1$ be given, where $\gcd(\overline{n}, p) = 1$. Let $\gamma$ be an element of order $\overline{n}$ in an extension field of $\mathbb{F}_q$. Furthermore, let four integers $f$, $m \neq 0$, $\delta \geq 2$ and $\nu \geq 0$ with $\gcd(\overline{n}, m) = 1$ be given, such that for any codeword $c(X) \in \mathcal{C}$*

$$\sum_{i=0}^{\infty} c^{[p^s-1]}(\gamma^{f+im+j})X^i \equiv 0 \mod X^{\delta-1}, \quad \forall j \in [\nu+1) \tag{11}$$

*holds. Then, the minimum distance of $\mathcal{C}$ is at least $d_{II} \stackrel{\text{def}}{=} \delta+\nu$.*

*Proof:* Let $c(X) \in \mathcal{C}$ and let $\mathsf{Y} = \{i_0, i_1, \ldots, i_{y-1}\}$ denote the support of $c(X)$, where $y \geq d$ holds for all codewords except the all-zero codeword. We linearly combine the $\nu+1$ sequences from (11). Denote the scalar factors for each power series as in (11) by $\lambda_i \in \mathbb{F}_{q^l}$ for $i \in [\nu+1)$. We obtain:

$$\sum_{i=0}^{\infty}\sum_{j=0}^{\nu} \lambda_j c^{[p^s-1]}(\gamma^{f+im+j})X^i \equiv 0 \mod X^{\delta-1}. \tag{12}$$

The Hasse derivative (as defined in (1)) of (12) leads to:

$$\sum_{i=0}^{\infty}\sum_{j=0}^{\nu} \lambda_j \left( \sum_{u\in\mathsf{Y}} \tbinom{u}{p^s-1} c_u \gamma^{(u-p^s+1)(f+im+j)} \right) X^i \equiv 0 \mod X^{\delta-1}. \tag{13}$$

We re-order (13) according to the coefficients of the codeword and obtain:

$$\begin{aligned}\sum_{i=0}^{\infty}\sum_{u\in\mathsf{Y}}\sum_{j=0}^{\nu} \lambda_j \left( \tbinom{u}{p^s-1} c_u \gamma^{(u-p^s+1)(f+im+j)} \right) X^i &= \sum_{i=0}^{\infty}\sum_{u\in\mathsf{Y}} \left( \tbinom{u}{p^s-1} c_u \gamma^{(u-p^s+1)(f+im)} \sum_{j=0}^{\nu} \alpha^{uj}\lambda_j \right) X^i \\ &\equiv 0 \mod X^{\delta-1}.\end{aligned} \tag{14}$$

We want to annihilate the first $\nu$ terms of $c_{i_0}, c_{i_1}, \ldots, c_{i_{y-1}}$. From (14), the following linear system of equations with $\nu+1$ unknowns is obtained:

$$\begin{pmatrix} 1 & \gamma^{i_0} & \gamma^{i_0 2} & \cdots & \gamma^{i_0\nu} \\ 1 & \gamma^{i_1} & \gamma^{i_1 2} & \cdots & \gamma^{i_1\nu} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \gamma^{i_\nu} & \gamma^{i_\nu 2} & \cdots & \gamma^{i_\nu\nu} \end{pmatrix} \cdot \begin{pmatrix} \lambda_0 \\ \lambda_1 \\ \vdots \\ \lambda_\nu \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix}, \tag{15}$$

and it is guaranteed to find a unique non-zero solution, because the $(\nu+1)\times(\nu+1)$ matrix in (15) is a Vandermonde matrix.

Let $\widetilde{\mathsf{Y}} \stackrel{\text{def}}{=} \mathsf{Y} \setminus \{i_0, i_1, \ldots, i_{\nu-1}\}$. Then, we can rewrite (14):

$$\sum_{i=0}^{\infty} \left( \sum_{u \in \widetilde{\mathsf{Y}}} \tbinom{u}{p^s-1} c_u \gamma^{(u-p^s+1)(f+im)} \sum_{j=0}^{\nu} \gamma^{uj} \lambda_j \right) X^i \equiv 0 \mod X^{\delta-1}.$$

This leads with the geometric series to:

$$\sum_{u \in \widetilde{\mathsf{Y}}} \frac{\tbinom{u}{p^s-1} c_u \gamma^{(u-p^s+1)f} \sum_{j=0}^{\nu} \gamma^{uj} \lambda_j}{1 - \gamma^{(u-p^s+1)m} X} \equiv 0 \mod X^{\delta-1},$$

and can be expressed with one common denominator using (8) as follows:

$$\frac{\sum\limits_{u \in \widetilde{\mathsf{Y}}} \left( \tbinom{u}{p^s-1} c_u \gamma^{(u-p^s+1)f} \sum_{j=0}^{\nu} \gamma^{uj} \lambda_j \frac{\operatorname{lcm}\left(1-\gamma^{(j-p^s+1)m} X \,:\, j \in \mathsf{Y}\right)}{1-\gamma^{(j-p^s+1)m} X} \right)}{\operatorname{lcm}\left(1 - \gamma^{(i-p^s+1)m} X \;:\; i \in \mathsf{Y}\right)} \equiv 0 \mod X^{\delta-1},$$

where the degree of the numerator is smaller than or equal to $y - 1 - \nu$ and has to be at least $\delta - 1$. Therefore for $y \geq d$, we have:

$$\begin{aligned} d - 1 - \nu &\geq \delta - 1, \\ d &\geq d_{\text{II}} \stackrel{\text{def}}{=} \delta + \nu. \end{aligned}$$

■

Note that for $\nu = 0$, Thm. 3 becomes Thm. 1. Thm. 3 tells us that an $[n = p^s \overline{n}, k, d]_q$ repeated-root cyclic code with generator polynomial $g(X)$ that has $\nu+1$ sequences of $\delta - 1$ consecutive zeros of highest multiplicity $p^s$, i.e.,

$$\begin{aligned} g^{[p^s-1]}(\gamma^f) = g^{[p^s-1]}(\gamma^{f+m}) = \cdots = g^{[p^s-1]}(\gamma^{f+(\delta-2)m}) &= 0 \\ g^{[p^s-1]}(\gamma^{f+1}) = g^{[p^s-1]}(\gamma^{f+m+1}) = \cdots = g^{[p^s-1]}(\gamma^{f+(\delta-2)m+1}) &= 0 \\ \vdots \\ g^{[p^s-1]}(\gamma^{f+\nu}) = g^{[p^s-1]}(\gamma^{f+m+\nu}) = \cdots = g^{[p^s-1]}(\gamma^{f+(\delta-2)m+\nu}) &= 0, \end{aligned}$$

has at least minimum distance $\delta + \nu$. If $s = 0$, the repeated-root cyclic code is a simple-root cyclic code and then Thm. 1 coincides with the HT bound [3], [4].

**Remark 4** (Alternative Proof of the Two Bounds)**.** *An $[n = p^s \overline{n}, k, d]_q$ repeated-root cyclic code with considered consecutive set(s) of zeros with multiplicity $p^s$ as in Thm. 1 and Thm. 3 is a sub-code of a cyclic code of length $\overline{n}$ over $\mathbb{F}_{q^{p^s}}$ with the same zeros (see Lemma 7).*

Let us consider an example of a binary repeated-root cyclic code and use Thm. 3 to bound its minimum distance.

**Example 5** (Binary Repeated-Root Cyclic Code)**.** *Let $\mathcal{C}$ be the binary $[34 = 2 \cdot 17, 18, 5]_2$ repeated-root cyclic code with defining set as defined in* (2)*:*

$$\mathsf{D}_{\mathcal{C}} = \left\{ 1^{\langle 2 \rangle}, 2^{\langle 2 \rangle}, 4^{\langle 2 \rangle}, 8^{\langle 2 \rangle}, 9^{\langle 2 \rangle}, 13^{\langle 2 \rangle}, 15^{\langle 2 \rangle}, 16^{\langle 2 \rangle} \right\},$$

*i.e., its generator polynomial is:*

$$g(X) = M_{1,17,2}(X)^2.$$

*Thm. 3 holds for the parameters $f = 1$, $m = 7$, $\delta = 4$ and $\nu = 1$ and therefore the minimum distance of $\mathcal{C}$ is at least 5.*

*B. Syndrome-Based Burst Error Decoding Algorithm up to Bound I and Bound II*

Let $\zeta \in \mathbb{F}_{q^{p^s}}$ be such that $(1 \ \zeta \ \ldots \ \zeta^{p^s-1})$ is an $\mathbb{F}_q$-basis of the extension field $\mathbb{F}_{q^{p^s}}$. We define the following bijective map:

$$\begin{aligned} \phi: \ \mathbb{F}_q^{p^s} &\longrightarrow \mathbb{F}_{q^{p^s}} \\ (a_0 \ a_1 \ \ldots \ a_{p^s-1}) &\longmapsto a_0 + a_1\zeta + \cdots a_{p^s-1}\zeta^{p^s-1}. \end{aligned}$$

**Definition 6** (Folded Code)**.** *Let $\mathcal{C}$ be a linear code over $\mathbb{F}_q$ of length $n = p^s\overline{n}$. The folded code $\mathcal{C}^F$ of length $\overline{n}$ over $\mathbb{F}_{q^{p^s}}$ is defined by:*

$$\mathcal{C}^F \stackrel{\text{def}}{=} \Big\{ \big(\phi(c_0 \ \ldots \ c_{p^s-1}) \ \ldots \ \phi(c_{n-p^s} \ \ldots \ c_{n-1})\big) \ \mid (c_0 \ \ldots \ c_{n-1}) \in \mathcal{C} \Big\}.$$

*Equivalently, we denote the folded polynomial of a given polynomial $c(X) \in \mathbb{F}_q[X]$ by $c^F(X)$.*

**Lemma 7** (Folding Repeated-Root Cyclic Code)**.** *Let $\mathcal{C}$ be an $[n = p^s\overline{n}, k = p^s\overline{k}, d]_q$ repeated-root cyclic code over $\mathbb{F}_q$ with characteristic $p$ and defining set:*

$$\mathsf{D}_{\mathcal{C}} = \Big\{ i^{\langle p^s \rangle} \mid i \in \mathsf{D}_{\mathcal{C}^F} \Big\},$$

*where $|\mathsf{D}_{\mathcal{C}^F}| = \overline{n} - \overline{k}$. Then the folded code $\mathcal{C}^F$ as in Def. 6 is an $[\overline{n}, \overline{k}, d]_{q^{p^s}}$ simple-root cyclic code with defining set $\mathsf{D}_{\mathcal{C}^F}$.*

*Proof.* Length and dimension of $\mathcal{C}^F$ follow directly from Def. 6. Let us prove the defining set. Every codeword $c(X)$ of the given repeated-root cyclic root $\mathcal{C}$ can be written as

$$c(X) = \sum_{i=0}^{p^s-1} X^i \sum_{j=0}^{\overline{n}-1} c_{i+jp^s} X^{jp^s} = \sum_{i=0}^{p^s-1} X^i \sum_{j=0}^{\overline{k}-1} u_{i,j} X^{jp^s} g(X^{p^s}),$$

where $g(X^{p^s}) = g(X)^{p^s}$ is the generator polynomial of $\mathcal{C}$ with $\overline{n} - \overline{k}$ distinct roots of multiplicity $p^s$. The corresponding codeword of the folded code $\mathcal{C}^F$ over $\mathbb{F}_{q^{p^s}}$ in vector notation is:

$$c^F(X) = \sum_{j=0}^{\overline{n}-1} \begin{pmatrix} c_{0+jp^s} \\ c_{1+jp^s} \\ \vdots \\ c_{p^s-1+jp^s} \end{pmatrix} X^j = \sum_{j=0}^{\overline{k}-1} \begin{pmatrix} u_{0,j} \\ u_{1,j} \\ \vdots \\ u_{p^s-1,j} \end{pmatrix} g(X)$$

and has $\overline{n} - \overline{k}$ distinct roots of multiplicity one. □

Folding as given in Def. 6 is discussed extensively in the literature, especially for Reed–Solomon codes (see e.g. [25]–[27]). The operation is essential to decode a given repeated-root cyclic code. In the following we describe the decoding approach for $p^s$-phased burst errors, i.e., errors measured in $\mathbb{F}_{q^{p^s}}$. The transmitted (or stored) codeword $c(X)$ of a given $[p^s\overline{n}, k, d]_q$ repeated-root cyclic code $\mathcal{C}$ is affected by an error $e(X) \in \mathbb{F}_q[X]$. The received polynomial $r(X) \in \mathbb{F}_q[X]$ is $r(X) = c(X) + e(X)$. We fold the received word $r(X)$ as in Def. 6 and obtain

$$r^F(X) = c^F(X) + e^F(X),$$

where $e^F(X) = \sum_{i \in \mathsf{E}} e_i^F X^i$ and $\mathsf{E}$ is the set of $p^s$-phased burst error with cardinality $|\mathsf{E}| = \varepsilon$. We describe a syndrome-based decoding procedure up to $\varepsilon \leq \lfloor (d_{\text{II}} - 1)/2 \rfloor$ $p^s$-phased burst-errors based on a set of $\nu + 1$ key equations that can be solved by a modified variant of the Extended Euclidean Algorithm (EEA) similar to the procedure to decode simple-root cyclic codes up to the HT bound (see e.g., [23], [28], [29]). Let us first define syndromes in the corresponding extension field.

**Definition 8** (Syndromes)**.** *Let $\mathcal{C}$ be an $[n, k, d]_q$ repeated-root cyclic code over $\mathbb{F}_q$ with characteristic $p$, where $n = p^s\overline{n}$. The integers $f$, $m \neq 0$, $\delta \geq 2$ and $\nu \geq 0$ are given as in Thm. 3. Let $\gamma \in \mathbb{F}_{q^\iota}$ be an element of order*

$\overline{n}$. *We define* $\nu+1$ *syndrome polynomials* $S^{\langle 0\rangle}(X), S^{\langle 1\rangle}(X), \ldots, S^{\langle \nu\rangle}(X) \in \mathbb{F}_{q^{lp^s}}[X]$ *for a received polynomial* $r(X) \in \mathbb{F}_q[X]$*, respectively the folded version* $r^F(X) \in \mathbb{F}_{q^{p^s}}[X]$*, as follows:*

$$S^{\langle t\rangle}(X) \stackrel{\text{def}}{=} \sum_{i=0}^{\delta-2} r^F(\gamma^{f+im+t})X^i, \quad \forall t \in [\nu+1). \tag{16}$$

To obtain an algebraic description in terms of key equations, we define an error-locator polynomial in the following.

**Definition 9** (Error-Locator Polynomial)**.** *Let* $\gamma$ *be an element of order* $\overline{n}$ *in* $\mathbb{F}_{q^l}$ *and let* $m \neq 0$ *as in Thm. 3. The support of the additive error is* $\mathsf{E}$ *with* $|\mathsf{E}| = \varepsilon$*. Define the error-locator polynomial in* $\mathbb{F}_{q^l}[X]$*, as:*

$$\Lambda(X) \stackrel{\text{def}}{=} \prod_{i\in\mathsf{E}} \left(1 - X\gamma^{im}\right), \tag{17}$$

*with degree* $\varepsilon$*.*

We now connect Def. 8 and Def. 9. From the expression of the syndrome polynomials as in (16), we obtain with the folded received polynomial $r^F(X) = c^F(X) + e^F(X)$:

$$\begin{aligned} S^{\langle t\rangle}(X) &= \sum_{i=0}^{\delta-2} r^F(\gamma^{f+im+t})X^i \\ &= \sum_{i=0}^{\delta-2} e^F(\gamma^{f+im+t})X^i \\ &= \sum_{i=0}^{\delta-2} \left( \sum_{j\in\mathsf{E}} \left( \sum_{u=0}^{p^s-1} e_{u+jp^s}\zeta^u \right) \gamma^{(f+im+t)j} \right) X^i, \quad \forall t \in [\nu), \end{aligned} \tag{18}$$

i.e., the syndromes are independent of the folded codeword $c^F(X)$. We use the geometric series and we obtain from (18):

$$\sum_{i=0}^{\infty} \left( \sum_{j\in\mathsf{E}} \left( \sum_{u=0}^{p^s-1} e_{u+jp^s}\zeta^u \right) \gamma^{(f+im+t)j} \right) X^i \equiv \sum_{j\in\mathsf{E}} \left( \sum_{u=0}^{p^s-1} e_{u+jp^s}\zeta^u \right) \frac{\gamma^{(f+t)j}}{1-X\gamma^{jm}} \mod X^{\delta-1}. \tag{19}$$

We need two more steps to obtain a common denominator. From (19), we have:

$$\begin{aligned} S^{\langle t\rangle}(X) &\equiv \sum_{j\in\mathsf{E}} \left( \sum_{u=0}^{p^s-1} e_{u+jp^s}\zeta^u \right) \frac{\gamma^{(f+t)j}}{1-X\gamma^{jm}} \mod X^{\delta-1} \\ &\equiv \frac{\sum_{j\in\mathsf{E}} \left( \sum_{u=0}^{p^s-1} e_{u+jp^s}\zeta^u \right) \gamma^{(f+t)j} \prod_{\substack{i\in\mathsf{E}\\ i\neq j}} (1-X\gamma^{im})}{\prod_{i\in\mathsf{E}}(1-X\gamma^{im})} \mod X^{\delta-1} \\ &\stackrel{\text{def}}{\equiv} \frac{\Omega^{\langle t\rangle}(X)}{\Lambda(X)} \mod X^{\delta-1}, \quad \forall t \in [\nu), \end{aligned} \tag{20}$$

where

$$\Omega^{\langle t\rangle}(X) \stackrel{\text{def}}{=} \sum_{j\in\mathsf{E}} \left( \sum_{u=0}^{p^s-1} e_{u+jp^s}\zeta^u \right) \gamma^{(f+t)j} \prod_{\substack{i\in\mathsf{E}\\ i\neq j}} \left(1-X\gamma^{im}\right), \quad \forall t \in [\nu), \tag{21}$$

are the $\nu+1$ error-evaluator polynomials $\Omega^{\langle 0\rangle}(X), \Omega^{\langle 1\rangle}(X), \ldots, \Omega^{\langle \nu\rangle}(X)$ of degree at most $\varepsilon - 1$.

The $\nu+1$ key equations as in (20) can be collaboratively solved by a so-called multisequence shift-register synthesis (see e.g., [23], [28]). Algorithm 1 is based on the Generalized Extended Euclidean Algorithm (GEEA) that solves the corresponding multisequence problem.

**Algorithm 1:** Decoding a $[p^s\overline{n}, k, d]_q$ repeated-root cyclic code $\mathcal{C}$ up to $\lfloor (d_{\mathsf{ll}} - 1)/2 \rfloor$ $p^s$-phased burst errors.

**Input**: Received word $r(X) \in \mathbb{F}_q[X]$, element $\gamma$ of order $\overline{n}$
Parameters $f$, $m \neq 0$, $\delta \geq 2$ and $\nu \geq 0$ as in Thm. 3
**Output**: Estimated folded codeword $c^F(X)$ or `DecodingFailure`

1 Calculate $S^{\langle 0 \rangle}(X), \ldots, S^{\langle \nu \rangle}(X)$ as in (16) using folded $r^F(X)$ // Syndrome calculation
2 $\Lambda(X), \Omega^{\langle 0 \rangle}(X), \ldots, \Omega^{\langle \nu \rangle}(X) = \texttt{GEEA}\big(X^{\delta-1}, S^{\langle 0 \rangle}(X), \ldots, S^{\langle \nu \rangle}(X)\big)$ // Generalized EEA
3 Find all $i$, where $\Lambda(\gamma_i) = 0 \Rightarrow \mathsf{E} = \{i_0, i_1, \ldots, i_{\varepsilon-1}\}$ // Chien-like search
4 **if** $\varepsilon < \deg \Lambda(X)$ **then**
5 Declare `DecodingFailure`
6 **else**
7 Determine $e^F_{i_0}, e^F_{i_1}, \ldots, e^F_{i_{\varepsilon-1}}$ // Forney error-evaluation
8 $e^F(X) \leftarrow \sum_{\ell \in \mathsf{E}} e^F_\ell X^\ell$
9 $c^F(X) \leftarrow r^F(X) - e^F(X)$

For the $\nu + 2$ input polynomials $X^{\delta-1}$ and $S^{\langle 0 \rangle}(X), S^{\langle 1 \rangle}(X), \ldots, S^{\langle \nu \rangle}(X)$ the GEEA returns the polynomials $\Lambda(X)$, $\Omega^{\langle 0 \rangle}(X)$, $\ldots$, $\Omega^{\langle \nu \rangle}(X)$ in $\mathbb{F}_{q^l}[X]$, such that (20) holds (as in Line 2 of Algorithm 1). One error-evaluator polynomial $\Omega^{\langle i \rangle}(X)$ as given in (21) is sufficient for the error-evaluation in Line 7.

Clearly, for $\nu = 0$ Algorithm 1 decodes up to $\lfloor (d_{\mathsf{l}} - 1)/2 \rfloor$ $p^s$-phased burst errors. Then, the GEEA coincides with the EEA.

## IV. Defining Sets of Repeated-Root Cyclic Product Codes

Our third lower bound on the minimum distance of a given repeated-root cyclic code $\mathcal{A}$ is based on the embedding of $\mathcal{A}$ into a repeated-root cyclic product code $\mathcal{A} \otimes \mathcal{B}$. Therefore, we explicitly give the defining set of a repeated-root cyclic product code and stress important properties.

Let $\mathcal{A}$ be an $[n_a = p^s\overline{n}_a, k_a, d_a]_q$ repeated-root cyclic code, where $\gcd(\overline{n}_a, p) = 1$, and let $\mathcal{B}$ be an $[n_b, k_b, d_b]_q$ simple-root cyclic code. If $\gcd(n_a, n_b) = 1$, then the $[n = p^s\overline{n}_a n_b, k_a k_b, d_a d_b]_q$ product code $\mathcal{C} = \mathcal{A} \otimes \mathcal{B}$ is (repeated-root) cyclic (see e.g., [30, Ch. 18] for linear product codes). Note that the lengths of two repeated-root cyclic codes over the same field cannot be co-prime and therefore a cyclic product code is not possible.

Let us investigate the defining set of a repeated-root cyclic product code in the following theorem, originally stated by Burton and Weldon [21, Corollary IV].

**Theorem 10** (Defining Set and Generator Polynomial of a Cyclic Product Code)**.** *Let $\mathcal{A}$ be an $[n_a = p^s\overline{n}_a, k_a, d_a]_q$ repeated-root cyclic code over $\mathbb{F}_q$ with characteristic $p$, and let $\alpha$ be an element of order $\overline{n}_a$ in $\mathbb{F}_{q^{l_a}}$. Let $\mathcal{B}$ be an $[n_b, k_b, d_b]_q$ simple-root cyclic code and let $\beta$ be an element of order $n_b$ in $\mathbb{F}_{q^{l_b}}$. Let $l = \operatorname{lcm}(l_a, l_b)$. The defining sets of $\mathcal{A}$ and $\mathcal{B}$ are denoted by $\mathsf{D}_\mathcal{A}$ respectively $\mathsf{D}_\mathcal{B}$ and their generator polynomials by $g_a(X)$ respectively $g_b(X)$. Let two integers $a$ and $b$ be given, such that:*

$$an_a + bn_b = 1.$$

*The generator polynomial $g(X)$ of the repeated-root cyclic product code $\mathcal{A} \otimes \mathcal{B}$ is:*

$$g(X) = \gcd\Big(X^{n_a n_b} - 1, g_a(X^{bn_b}) \cdot g_b(X^{an_a})\Big). \tag{22}$$

*Let $\gamma \stackrel{\text{def}}{=} \alpha\beta$ in $\mathbb{F}_{q^l}$ and let:*

$$\overline{\mathsf{D}}_\mathcal{B} = \Big\{ i^{\langle p^s \rangle} \mid i \in \mathsf{D}_\mathcal{B} \Big\}. \tag{23}$$

*Then the defining set of the repeated-root cyclic product code $\mathcal{C} = \mathcal{A} \otimes \mathcal{B}$ is:*

$$\mathsf{D}_\mathcal{C} = \Big\{ \mathsf{D}_\mathcal{A} \cup \mathsf{D}_\mathcal{A}^{[\overline{n}_a]} \cup \mathsf{D}_\mathcal{A}^{[2\overline{n}_a]} \cup \cdots \cup \mathsf{D}_\mathcal{A}^{[(n_b-1)\overline{n}_a]} \Big\} \overset{max}{\cup} \Big\{ \overline{\mathsf{D}}_\mathcal{B} \cup \overline{\mathsf{D}}_\mathcal{B}^{[n_b]} \cup \overline{\mathsf{D}}_\mathcal{B}^{[2n_b]} \cup \cdots \cup \overline{\mathsf{D}}_\mathcal{B}^{[(\overline{n}_a-1)n_b]} \Big\},$$

*where* $\mathsf{D}_{\mathcal{A}}^{[\overline{n}_a]}$ *was defined in* (3) *and the operation in* (4).

For the proof we refer to the proof of [21, Thm. 3 and Corollary IV]. We explicitly give the defining set of the repeated-root cyclic product code $\mathcal{A} \otimes \mathcal{B}$ here and we want to emphasize that the roots of the simple-root cyclic code $\mathcal{B}$ have highest multiplicity $p^s$ in the defining set of $\mathcal{A} \otimes \mathcal{B}$ (see (23)), because

$$g_b(X^{an_a}) = g_b(X^{a\overline{n}_a})^{p^s}.$$

## V. Bound III: Embedding into Repeated-Root Cyclic Product Codes

Similar to Thm. 4 of [31] for a simple-root cyclic code, we embed a given repeated-root cyclic code $\mathcal{A}$ into a repeated-root cyclic product code $\mathcal{A} \otimes \mathcal{B}$ to bound the minimum distance of $\mathcal{A}$.

**Theorem 11** (Bound III: Embedding into a Product Code)**.** *Let* $\mathcal{A}$ *be an* $[n_a = p^s\overline{n}_a, k_a, d_a]_q$ *repeated-root cyclic code over* $\mathbb{F}_q$ *with characteristic* $p$*, where* $\gcd(\overline{n}_a, p) = 1$ *and let* $\mathcal{B}$ *be an* $[n_b, k_b, d_b]_q$ *simple-root cyclic code, respectively, with* $\gcd(n_a, n_b) = 1$*. Let* $\alpha$ *be an element of order* $\overline{n}_a$ *in* $\mathbb{F}_{q^{l_a}}$*,* $\beta$ *of order* $n_b$ *in* $\mathbb{F}_{q^{l_b}}$*, respectively, and let two integers* $f_a$*,* $f_b$ *and two non-zero integers* $m_a \neq 0$*,* $m_b \neq 0$ *with* $\gcd(n_a, m_a) = \gcd(n_b, m_b) = 1$ *be given. Assume that for all codewords* $a(X) \in \mathcal{A}$ *and* $b(X) \in \mathcal{B}$

$$\sum_{i=0}^{\infty} a^{[p^s-1]}(\alpha^{f_a+im_a}) \cdot b(\beta^{f_b+im_b})X^i \equiv 0 \mod X^{\delta-1} \tag{24}$$

*holds for some integer* $\delta \geq 2$*. Then, we obtain:*

$$d_a \geq d_{III} \stackrel{\text{def}}{=} \left\lceil \frac{\delta}{d_b} \right\rceil. \tag{25}$$

*Proof: From Thm. 10 we know that* (24) *corresponds to* $\delta - 1$ *consecutive zeros with highest multiplicity* $p^s$ *of the repeated-root cyclic product code* $\mathcal{A} \otimes \mathcal{B}$*. By Thm. 1, the minimum distance* $d$ *of* $\mathcal{A} \otimes \mathcal{B}$ *is greater than or equal to* $\delta$*. Therefore:*

$$d = d_a d_b \geq \delta \quad \Longleftrightarrow \quad d_a = \left\lceil \frac{\delta}{d_b} \right\rceil.$$

■

Note that the expression of (24) is in $\mathbb{F}_{q^l}[X]$, where $l = \operatorname{lcm}(l_a, l_b)$.

**Example 12** (Bound by Embedding into a Product Code)**.** *Let* $\mathcal{A}$ *be the* $[34 = 2 \cdot 17, 18, 5]_2$ *repeated-root cyclic code with* $p = 2$*,* $\overline{n}_a = 17$ *and defining set:*

$$\mathsf{D}_{\mathcal{A}} = \left\{1^{\langle 2\rangle}, 2^{\langle 2\rangle}, 4^{\langle 2\rangle}, 8^{\langle 2\rangle}, 9^{\langle 2\rangle}, 13^{\langle 2\rangle}, 15^{\langle 2\rangle}, 16^{\langle 2\rangle}\right\},$$

*of Ex. 5 and let* $\mathcal{B}$ *denote the* $[3, 2, 2]_2$ *simple-root cyclic parity check code with defining set*

$$\mathsf{D}_{\mathcal{B}} = \left\{0^{\langle 1\rangle}\right\}.$$

*Let* $\alpha \in \mathbb{F}_{2^8}$ *and* $\beta \in \mathbb{F}_{2^4}$ *denote elements of order 17 and 3, respectively. Then, for* $f_a = -4$*,* $f_b = -1$ *and* $m_a = m_b = 1$ *Thm. 11 holds for* $\delta = 10$ *and therefore* $d_a \geq 5$*, which is the true minimum distance of* $\mathcal{A}$*.*

*Since* $1 \cdot 34 - 11 \cdot 3 = 1$*, according to Thm. 10, the defining set of the repeated-root cyclic product code* $\mathcal{A} \otimes \mathcal{B}$ *is:*

$$\begin{aligned}
\mathsf{D}_{\mathcal{A}\otimes\mathcal{B}} =& \Big\{ \left\{1^{\langle 2\rangle}, 2^{\langle 2\rangle}, 4^{\langle 2\rangle}, 8^{\langle 2\rangle}, 9^{\langle 2\rangle}, 13^{\langle 2\rangle}, 15^{\langle 2\rangle}, 16^{\langle 2\rangle}\right\} \cup \left\{18^{\langle 2\rangle}, 19^{\langle 2\rangle}, 21^{\langle 2\rangle}, 25^{\langle 2\rangle}, 26^{\langle 2\rangle}, 30^{\langle 2\rangle}, 32^{\langle 2\rangle}, 33^{\langle 2\rangle}\right\} \\
& \cup \left\{35^{\langle 2\rangle}, 36^{\langle 2\rangle}, 38^{\langle 2\rangle}, 42^{\langle 2\rangle}, 43^{\langle 2\rangle}, 47^{\langle 2\rangle}, 49^{\langle 2\rangle}, 50^{\langle 2\rangle}\right\} \Big\} \overset{max}{\cup} \left\{\left\{0^{\langle 2\rangle}\right\} \cup \left\{3^{\langle 2\rangle}\right\} \cup \cdots \cup \left\{48^{\langle 2\rangle}\right\}\right\} \\
=& \Big\{0^{\langle 2\rangle}, 1^{\langle 2\rangle}, 2^{\langle 2\rangle}, 3^{\langle 2\rangle}, 4^{\langle 2\rangle}, 6^{\langle 2\rangle}, 8^{\langle 2\rangle}, 9^{\langle 2\rangle}, 12^{\langle 2\rangle}, 13^{\langle 2\rangle}, 15^{\langle 2\rangle}, 16^{\langle 2\rangle}, 18^{\langle 2\rangle}, 19^{\langle 2\rangle}, 21^{\langle 2\rangle}, 24^{\langle 2\rangle}, 25^{\langle 2\rangle}, 26^{\langle 2\rangle}, 27^{\langle 2\rangle}, \\
& 30^{\langle 2\rangle}, 32^{\langle 2\rangle}, 33^{\langle 2\rangle}, 35^{\langle 2\rangle}, 36^{\langle 2\rangle}, 38^{\langle 2\rangle}, 39^{\langle 2\rangle}, 42^{\langle 2\rangle}, 43^{\langle 2\rangle}, 45^{\langle 2\rangle}, 47^{\langle 2\rangle}, 48^{\langle 2\rangle}, 49^{\langle 2\rangle}, 50^{\langle 2\rangle}\Big\}.
\end{aligned}$$

## VI. Probabilistic Decoding up to Bound III

In contrast to the decoding approach for $p^s$-phased burst errors in Section III-B, we do not use folding (as in Def. 6) in the following. Instead we decode a given $[n_a = p^s\overline{n}_a, k_a, d_a]_q$ repeated-root cyclic code $\mathcal{A}$ (embedded in a repeated-root cyclic product code $\mathcal{A} \otimes \mathcal{B}$ via an associated single-root cyclic code $\mathcal{B}$ as in Thm. 11) as a $p^s$-interleaved code and apply a probabilistic decoder (as e.g. analyzed in [25], [32], [33]). Note that this decoding method also corrects $p^s$-phased burst errors. Let $a(X) \in \mathcal{A}$ and let the received polynomial be $r(X) = a(X)+e(X)$.

Let $p^s$ polynomials $r^{\langle 0\rangle}(X), r^{\langle 1\rangle}(X), \ldots, r^{\langle p^s-1\rangle}(X) \in \mathbb{F}_q[X]$ of degree smaller than $\overline{n}_a$ be given, such that

$$r(X) = \sum_{i=0}^{p^s-1} r^{\langle i\rangle}(X^{p^s})X^i, \tag{26}$$

where $\mathsf{E}_i$ denotes the corresponding error-positions in $r^{\langle i\rangle}(X)$. The set $\mathsf{E} = \cup_{i=0}^{p^s-1}\mathsf{E}_i$ with $\varepsilon = |\mathsf{E}|$ is the set of $p^s$-phased burst-errors.

In the following the set of $p^s$ key equations is derived and the decoding procedure up to $\varepsilon \leq \lfloor \frac{p^s}{p^s-1}(d_{\mathsf{III}} - 1)\rfloor$ $p^s$-phased burst errors is described.

**Definition 13** (Syndromes)**.** *Let $\mathcal{A}$ be an $[n_a = p^s\overline{n}_a, k_a, d_a]_q$ repeated-root cyclic code over $\mathbb{F}_q$ with characteristic $p$, where $\gcd(\overline{n}_a, p) = 1$, and $\mathcal{B}$ an $[n_b, k_b, d_b]_q$ simple-root cyclic code, respectively, with $\gcd(n_a, n_b) = 1$. Let $\alpha$, $\beta$ be elements of order $\overline{n}_a$ in $\mathbb{F}_{q^{l_a}}$ and of order $n_b$ in $\mathbb{F}_{q^{l_b}}$ respectively. The integers $f_a$, $f_b$, $m_a \neq 0$, $m_b \neq 0$ with $\gcd(n_a, m_a) = \gcd(n_b, m_b) = 1$ and $\delta \geq 2$ are given as in Thm. 11. Furthermore, let $b(X) \in \mathcal{B}$ be a codeword of weight $d_b$. We define $p^s$ syndrome polynomials $S^{\langle 0\rangle}(X), S^{\langle 1\rangle}(X), \ldots, S^{\langle p^s-1\rangle}(X) \in \mathbb{F}_{q^l}[X]$, where $l = \mathrm{lcm}(l_a, l_b)$ for the received polynomials $r^{\langle 0\rangle}(X), r^{\langle 1\rangle}(X), \ldots, r^{\langle p^s-1\rangle}(X) \in \mathbb{F}_q[X]$ as in* (26)*:*

$$S^{\langle t\rangle}(X) \stackrel{\text{def}}{=} \sum_{i=0}^{\delta-2} r^{\langle t\rangle}(\alpha^{f_a+im_a}) \cdot b(\beta^{f_b+im_b})X^i, \quad \forall t \in [p^s). \tag{27}$$

To obtain an algebraic description in terms of a key equation, we define an error-locator polynomial in the following.

**Definition 14** (Error-Locator Polynomial)**.** *Let $b(X) = \sum_{i\in\mathsf{Y}} b_i X^i$ be a codeword of weight $|\mathsf{Y}| = d_b$ of the associated $[n_b, k_b, d_b]_q$ simple-root cyclic code $\mathcal{B}$. Let $\alpha$ and $\beta$ be elements of order $\overline{n}_a$ in $\mathbb{F}_{q^{l_a}}$ and of order $n_b$ in $\mathbb{F}_{q^{l_b}}$, respectively, and let $m_a \neq 0$ and $m_b \neq 0$ be as in Thm. 11.*

*The support of the additive error is $\mathsf{E}$ with $|\mathsf{E}| = \varepsilon$. Define the error-locator polynomial in $\mathbb{F}_{q^l}[X]$, where $l = \mathrm{lcm}(l_a, l_b)$, as:*

$$\Lambda(X) \stackrel{\text{def}}{=} \prod_{i\in\mathsf{E}} \left( \prod_{j\in\mathsf{Y}} \left(1 - X\alpha^{im_a}\beta^{jm_b}\right) \right), \tag{28}$$

*with degree $\varepsilon \cdot d_b$.*

For some $j \in \mathsf{Y}$, let $\overline{n}_a$ distinct roots of the error-locator polynomial $\Lambda(X)$, as defined in (28), be denoted as:

$$\gamma_i \stackrel{\text{def}}{=} \beta^{-jm_b}\alpha^{-im_a}, \quad \forall i \in [\overline{n}_a). \tag{29}$$

We pre-calculate $\overline{n}_a$ roots as in (29) and identify the error positions of a given error-locator polynomial $\Lambda(X)$ as in Def. 14.

We now connect Def. 13 and Def. 14. From the expression of the syndromes in (27), we obtain:

$$\begin{aligned} S^{\langle t\rangle}(X) &= \sum_{i=0}^{\delta-2} r^{\langle t\rangle}(\alpha^{f_a+im_a}) \cdot b(\beta^{f_b+im_b}) X^i \\ &= \sum_{i=0}^{\delta-2} e^{\langle t\rangle}(\alpha^{f_a+im_a}) \cdot b(\beta^{f_b+im_b}) X^i \\ &= \sum_{i=0}^{\delta-2} \left( \sum_{j\in \mathsf{E}_t} e_j^{\langle t\rangle} \alpha^{(f_a+im_a)j} \cdot \sum_{l\in \mathsf{Y}} b_l \beta^{(f_b+im_b)l} \right) X^i, \quad \forall t \in [p^s). \end{aligned} \tag{30}$$

As in (19), we use the geometric series and we obtain from (30):

$$\sum_{i=0}^{\infty} \left( \sum_{j\in \mathsf{E}_t} e_j^{\langle t\rangle} \alpha^{(f_a+im_a)j} \cdot \sum_{l\in \mathsf{Y}} b_l \beta^{(f_b+im_b)l} \right) X^i \equiv \sum_{j\in \mathsf{E}_t} e_j^{\langle t\rangle} \alpha^{f_a j} \sum_{l\in \mathsf{Y}} \frac{b_l \beta^{f_b l}}{1 - X\alpha^{jm_a}\beta^{lm_b}} \mod X^{\delta-1}. \tag{31}$$

We need two more steps to obtain a common denominator. From (31), we have:

$$\begin{aligned} S^{\langle t\rangle}(X) &\equiv \sum_{j\in \mathsf{E}_t} e_j^{\langle t\rangle} \alpha^{f_a j} \sum_{l\in \mathsf{Y}} \frac{b_l \beta^{f_b l}}{1 - X\alpha^{jm_a}\beta^{lm_b}} \mod X^{\delta-1} \\ &\equiv \sum_{j\in \mathsf{E}_t} e_j^{\langle t\rangle} \alpha^{f_a j} \frac{\sum_{l\in \mathsf{Y}} b_l \beta^{f_b l} \prod_{\substack{i\in \mathsf{Y} \\ i\neq l}} (1 - X\alpha^{jm_a}\beta^{im_b})}{\prod_{i\in \mathsf{Y}} (1 - X\alpha^{jm_a}\beta^{im_b})} \mod X^{\delta-1} \\ &\equiv \frac{\sum_{j\in \mathsf{E}_t} \left( e_j^{\langle t\rangle} \alpha^{f_a j} \sum_{l\in \mathsf{Y}} \left( b_l \beta^{f_b l} \prod_{\substack{i\in \mathsf{Y} \\ i\neq l}} (1 - X\alpha^{jm_a}\beta^{im_b}) \right) \prod_{s\in \mathsf{E}} \prod_{\substack{s\neq j}} \prod_{\iota\in \mathsf{Y}} (1 - X\alpha^{sm_a}\beta^{\iota m_b}) \right)}{\prod_{i\in \mathsf{E}_t} \left( \prod_{j\in \mathsf{Y}} (1 - X\alpha^{im_a}\beta^{jm_b}) \right)} \\ &\stackrel{\text{def}}{\equiv} \frac{\Omega^{\langle t\rangle}(X)}{\Lambda(X)} \mod X^{\delta-1}, \quad \forall t \in [p^s), \end{aligned} \tag{32}$$

where

$$\Omega^{\langle t\rangle}(X) \stackrel{\text{def}}{=} \sum_{j\in \mathsf{E}_t} \left( e_j^{\langle t\rangle} \alpha^{f_a j} \sum_{l\in \mathsf{Y}} \left( b_l \beta^{f_b l} \prod_{\substack{i\in \mathsf{Y} \\ i\neq l}} (1 - X\alpha^{jm_a}\beta^{im_b}) \right) \prod_{s\in \mathsf{E}} \prod_{\substack{s\neq j}} \prod_{\iota\in \mathsf{Y}} (1 - X\alpha^{sm_a}\beta^{\iota m_b}) \right), \quad \forall t \in [p^s) \tag{33}$$

are the $p^s$ error-evaluator polynomials $\Omega^{\langle 0\rangle}(X), \Omega^{\langle 1\rangle}(X), \ldots, \Omega^{\langle p^s-1\rangle}(X)$ of degree at most $\varepsilon d_b - 1$. We skip the explicit error-evaluation and refer to [19, Proposition 4].

Algorithm 2 summarizes the syndrome-based decoding procedure up to $\left\lfloor \frac{p^s}{p^s-1}(d_{\mathsf{III}} - 1) \right\rfloor$ $p^s$-phased burst errors with high probability based on the key equations as in (32) and (33).

**Algorithm 2:** Decoding a $[p^s\overline{n}_a, k_a, d_a]_q$ repeated-root cyclic code $\mathcal{A}$ up to $\left\lfloor \frac{p^s}{p^s-1}(d_{\mathsf{III}}-1) \right\rfloor$ $p^s$-phased burst errors.

**Input**: Received word $r(X)$, codeword $b(X) = \sum_{i\in\mathsf{Y}} b_i X^i \in \mathcal{B}$,
Elements $\alpha$ and $\beta$ of order $n_a$ and $n_b$,
Parameters $f_a$, $f_b$, $m_a \neq 0$, $m_b \neq 0$ and $\delta \geq 2$ as in Thm. 11
**Output**: Estimated codeword $a(X) \in \mathcal{A}$ or `DecodingFailure`

**Preprocess**:
**for** all $i \in [\overline{n}_a)$: calculate $\gamma_i = \beta^{-jm_b}\alpha^{-im_a}$, where $j \in \mathsf{Y}$

1 Calculate $S^{\langle 0\rangle}(X), \ldots, S^{\langle p^s-1\rangle}(X)$ as in (27) using $r^{\langle 0\rangle}(X), \ldots, r^{\langle p^s-1\rangle}(X)$ // Syndrome calculation

2 $\Lambda(X), \Omega^{\langle 0\rangle}(X), \ldots, \Omega^{\langle p^s-1\rangle}(X) = \mathtt{GEEA}\big(X^{\delta-1}, S^{\langle 0\rangle}(X), \ldots, S^{\langle p^s-1\rangle}(X)\big)$ // Generalized EEA

3 Find all $i$, where $\Lambda(\gamma_i) = 0 \Rightarrow \mathsf{E} = \{i_0, i_1, \ldots, i_{\varepsilon-1}\}$ // Chien-like search

4 **if** $\varepsilon|\mathsf{Y}| < \deg\Lambda(X)$ **then**

5 Declare `DecodingFailure`

6 **else**

7 **for** all $i \in [p^s)$: Determine $e^{\langle i\rangle}(X)$ using $\Omega^{\langle i\rangle}(X)$ as in [19, Proposition 4] // Forney-like error-evaluation

8 $e^{\langle i\rangle}(X) \leftarrow \sum_{j\in\mathsf{E}_i} e_j^{\langle i\rangle} X^j$

9 $a(X) \leftarrow \sum_{i=0}^{p^s-1} \left(r^{\langle i\rangle}(X^{p^s}) - e^{\langle i\rangle}(X^{p^s})\right) X^i$

All error-evaluator polynomials $\Omega^{\langle 0\rangle}(X), \Omega^{\langle 1\rangle}(X), \ldots, \Omega^{\langle p^s-1\rangle}(X)$ as defined in (21) are needed for the error-evaluation in Line 7.

Bound III simplifies to the BCH-like generalization of Bound I (as stated in Thm. 1) if the associated code $\mathcal{B}$ is the trivial $[n_b, n_b, 1]_q$ code and decoding up to $\frac{p^s-1}{p^s}\lfloor (d_{\mathsf{I}}-1)/2 \rfloor$ $p^s$-phased burst errors with high probability is possible. Then the $p^s$ parallel operations (as e.g., the syndrome calculation) are computed over $\mathbb{F}_{q^l}$ instead in $\mathbb{F}_{q^{lp^s}}$.

Note that the $p^s$ cyclic subcodes can be collaboratively list decoded with the approach of Gopalan [34] up to the $q$-ary Johnson radius with relative distance $d_{\mathsf{I}}/n_a$.

## VII. Conclusion

We have proved three lower bounds on the minimum distance of a repeated-root cyclic code, i.e., a cyclic code whose length is not relatively prime to the field characteristic. The two first bounds are generalizations of the BCH and the HT bound to repeated-root cyclic codes. A syndrome-based decoding algorithm with a guaranteed radius was developed. The third bound is similar to a previous published technique for simple-root cyclic codes and is based on the embedding of a given repeated-root cyclic code into a repeated-root cyclic product code. A syndrome-based probabilistic decoding algorithm based on a set of key equations using the third bound was proposed.


## Acknowledgments

The authors are grateful to Antonia Wachter-Zeh, Johan S. R. Nielsen and Ron M. Roth for stimulating discussions.


## References


[1] 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.

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

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

[4] C. R. P. Hartmann and K. K. Tzeng, "Generalizations of the BCH Bound," *Inf. Control*, vol. 20, no. 5, pp. 489–498, 1972.

[5] S. D. Berman, "Semisimple Cyclic and Abelian Codes," *Cybernetics*, vol. 3, no. 3, pp. 17–23, 1967.

[6] J. L. Massey, D. Costello, and J. Justesen, "Polynomial Weights and Code Constructions," *IEEE Trans. Inform. Theory*, vol. 19, no. 1, pp. 101–110, 1973.

[7] J. L. Massey, N. von Seemann, and P. Schöller, "Hasse Derivatives and Repeated-Root Cyclic Codes," in *IEEE International Symposium on Information Theory (ISIT)*, 1986, p. 39.

[8] V. C. da Rocha Jr., "On Repeated-Single-Root Constacyclic Codes," in *Communications and Cryptography*, ser. The Springer International Series in Engineering and Computer Science. Springer US, 1994, no. 276, pp. 93–99.

[9] G. Castagnoli, "On the Minimum Distance of Long Cyclic Codes and Cyclic Redundancy Check Codes," in *PhD Thesis, ETH Zürich*, 1989.

[10] ——, "On the Asymptotic Badness of Cyclic Codes with Block-Lengths Composed from a Fixed Set of Prime Factors," in *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*, vol. 357. Springer Berlin/Heidelberg, 1989, pp. 164–168.

[11] G. Castagnoli, J. L. Massey, P. A. Schöller, and N. von Seemann, "On Repeated-Root Cyclic Codes," *IEEE Trans. Inform. Theory*, vol. 37, no. 2, pp. 337–342, 1991.

[12] R. K. Latypov, "Checking Matrix of a Cyclic Code Generated by Multiple Roots," *Journal of Soviet Mathematics*, vol. 43, no. 3, pp. 2492–2495, 1988.

[13] J. van Lint, "Repeated-Root Cyclic Codes," *IEEE Trans. Inform. Theory*, vol. 37, no. 2, pp. 343–345, 1991.

[14] K.-H. Zimmermann, "On Generalizations of Repeated-Root Cyclic Codes," *IEEE Trans. Inform. Theory*, vol. 42, no. 2, pp. 641–649, 1996.

[15] C.-S. Nedeloaia, "Weight Distributions of Cyclic Self-Dual Codes," *IEEE Trans. Inform. Theory*, vol. 49, no. 6, pp. 1582–1591, 2003.

[16] S. Ling, H. Niederreiter, and P. Solé, "On the Algebraic Structure of Quasi-cyclic Codes IV: Repeated Roots," *Des. Codes Cryptogr.*, vol. 38, no. 3, pp. 337–361, 2006.

[17] H. Q. Dinh, "Repeated-Root Constacyclic Codes of Length $2p^s$," *Finite Fields Th. App.*, vol. 18, no. 1, pp. 133–143, 2012.

[18] ——, "Structure of Repeated-Root Constacyclic Codes of Length $3p^s$ and Their Duals," *Discrete Math.*, vol. 313, no. 9, pp. 983–991, 2013.

S. Ling, H. Niederreiter, and P. Solé, "On the Algebraic Structure of Quasi-cyclic Codes IV: Repeated Roots," *Des. Codes Cryptogr.*, vol. 38, no. 3, pp. 337–361, 2006.

[19] A. Zeh and S. V. Bezzateev, "A New Bound on the Minimum Distance of Cyclic Codes Using Small-Minimum-Distance Cyclic Codes," *Des. Codes Cryptogr.*, vol. 71, no. 2, pp. 229–246, 2014.

[20] A. Zeh, A. Wachter-Zeh, and S. V. Bezzateev, "Decoding Cyclic Codes up to a New Bound on the Minimum Distance," *IEEE Trans. Inform. Theory*, vol. 58, no. 6, pp. 3951–3960, 2012.

[21] H. Burton and E. J. Weldon, "Cyclic Product Codes," *IEEE Trans. Inform. Theory*, vol. 11, no. 3, pp. 433–439, 1965.

[22] S. Lin and E. J. Weldon, "Further Results on Cyclic Product Codes," *IEEE Trans. Inform. Theory*, vol. 16, no. 4, pp. 452–459, 1970.

[23] 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.

[24] H. Hasse, "Theorie der höheren Differentiale in einem algebraischen Funktionenkörper mit vollkommenem Konstantenkörper bei beliebiger Charakteristik," *Journal für die Reine und Angewandte Mathematik*, no. 175, pp. 50–54, 1936.

[25] V. Y. Krachkovsky and Y. X. Lee, "Decoding for Iterative Reed–Solomon Coding Schemes," *IEEE Trans. Magn.*, vol. 33, no. 5, pp. 2740–2742, 1997.

[26] V. R. Sidorenko, G. Schmidt, and M. Bossert, "Decoding Punctured Reed–Solomon Codes up to the Singleton Bound," in *International ITG Conference on Source and Channel Coding (SCC)*, 2008.

[27] V. Guruswami, "Linear-Algebraic List Decoding of Folded Reed–Solomon Codes," in *IEEE Annual Conference on Computational Complexity (CCC)*, 2011, pp. 77–85.

[28] G.-L. Feng and K. 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.

[29] A. Zeh and A. Wachter, "Fast Multi-Sequence Shift-Register Synthesis with the Euclidean Algorithm," *Adv. Math. of Comm.*, vol. 5, no. 4, pp. 667–680, 2011.

[30] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*. North Holland Publishing Co., 1988.

[31] A. Zeh, A. Wachter-Zeh, M. Gadouleau, and S. V. Bezzateev, "Generalizing Bounds on the Minimum Distance of Cyclic Codes Using Cyclic Product Codes," in *IEEE International Symposium on Information Theory (ISIT)*, 2013, pp. 126–130.

[32] V. Y. Krachkovsky, "Decoding of Parallel Reed–Solomon Codes with Applications to Product and Concatenated Codes," in *IEEE International Symposium on Information Theory (ISIT)*, 1998, p. 55.

[33] G. Schmidt, V. R. Sidorenko, and M. Bossert, "Collaborative Decoding of Interleaved Reed–Solomon Codes and Concatenated Code Designs," *IEEE Trans. Inform. Theory*, vol. 55, no. 7, pp. 2991–3012, 2009.

[34] P. Gopalan, V. Guruswami, and P. Raghavendra, "List Decoding Tensor Products and Interleaved Codes," *SIAM J. Comput.*, vol. 40, no. 5, pp. 1432–1462, 2011.