Decoding interleaved Reed-Solomon codes beyond their joint error-correcting capability

Alexander Zeh, Antonia Wachter, Martin Bossert

Decoding Cyclic Codes up to a New Bound on the Minimum Distance

Alexander Zeh, Antonia Wachter-Zeh, and Sergey Bezzateev

***Abstract*—A new lower bound on the minimum distance of q-ary cyclic codes is proposed. This bound improves upon the Bose–Chaudhuri–Hocquenghem (BCH) bound and, for some codes, upon the Hartmann–Tzeng (HT) bound. Several Boston bounds are special cases of our bound. For some classes of codes the bound on the minimum distance is refined. Furthermore, a quadratic-time decoding algorithm up to this new bound is developed. The determination of the error locations is based on the Euclidean Algorithm and a modified Chien search. The error evaluation is done by solving a generalization of Forney's formula.**

***Index Terms*—Bose–Chaudhuri–Hocquenghem (BCH) bound, cyclic codes, decoding, Forney's formula, Hartmann–Tzeng (HT) bound, Roos bound.**

I. Introduction

SEVERAL bounds on the minimum distance of cyclic codes are defined by a subset of the defining set of the code. The Bose–Chaudhuri–Hocquenghem (BCH) bound [2], [3] considers *one* set of *consecutive* elements of the defining set. A first extension of this bound was formulated by Hartmann and Tzeng (HT) [4]–[7], where *several* sets of *consecutive* elements are used to increase the lower bound on the minimum distance. The Roos bound [8], [9] generalizes this idea by exploiting *several* sets of *nonconsecutive* elements in the defining set. The contributions of van Lint and Wilson [10], Duursma and Kötter [11] and Duursma and Pellikann [12] are further generalizations. Other approaches include the Boston bounds [13] and the bound by Betti and Sala [14].

Although these improved bounds show that for many codes the actual distance is higher than the BCH bound, there is no general decoding algorithm up to any of these bounds. Hartmann and Tzeng [4], [6] proposed two variants of an iterative decoding algorithm up to the HT bound. However, these algorithms require the calculation of missing syndromes and the solution of non-linear equations. An approach for decoding all binary cyclic codes up to their *actual* minimum distance of length less than 63 was given by Feng and Tzeng [15]. They use a generalized syndrome matrix and fit the known syndrome coefficients manually for each code into the structure of the matrix.

This contribution provides a new lower bound on the minimum distance of q-ary cyclic codes based on a connection of the code with rational functions. This approach originates from decoding Goppa codes [16]–[19]. We match the roots of a q-ary cyclic code to nonzeros of the power series expansion of a rational function. This allows to formulate a new lower bound on the minimum distance of cyclic codes. We identify some classes of cyclic codes and refine the bound on their distance. A wide class of codes, which is covered by our approach, is the class of reversible codes [20]. Our new lower bound is better than the BCH bound and for most codes also better than the HT bound. Moreover, it can be seen as a generalization of some Boston [13] bounds. We give tables for binary and ternary cyclic codes, where we count the number of cyclic codes for which our bound is better than the BCH bound.

As a second part, we give an efficient decoding algorithm up to our new bound. This decoding algorithm is based on a generalized key equation, a modified Chien search and a generalized Forney's formula [21] for the error evaluation. The time complexity of the whole decoding procedure is quadratic with the length of the cyclic code.

This contribution is structured as follows. Section II gives some basic definitions and recapitulates known bounds on the minimum distance of cyclic codes. We show how the BCH bound can be represented by a simple rational function. In Section III, we explain how we associate a rational function to a cyclic code and we prove our new lower bound on the minimum distance. Section IV provides several identified classes and we refine the lower bound of these codes. We compare our new lower bound on the minimum distance with the BCH and the HT bound. In Section V, we show how several Boston bounds are generalized by our principle. The decoding algorithm is given in Section VI. Therefore, a generalized key equation is derived and the decoding radius is proved. Section VII concludes this contribution.

II. Preliminaries

A. Q-Ary Cyclic Codes and Rational Functions

Let q be a power of a prime, let $\mathbb{F}_q$ denote the finite field of order q and let $\mathbb{F}_q[x]$ denote the set of all univariate polynomials with coefficients in $\mathbb{F}_q$ and the indeterminate x. A q-ary cyclic code of length n, dimension k and minimum distance

The material in this contribution was presented in part at the IEEE International Symposium on Information Theory (ISIT 2011) in St. Petersburg, Russia [1]. This work has been supported by DFG, Germany, under grants BO 867/22-1 and BO 867/21-1.

A. Zeh is with the Institute of Communications Engineering, University of Ulm, D-89081 Ulm, Germany and with Research Center INRIA Saclay - Île-de-France, École Polytechnique ParisTech, 91128 Palaiseau Cedex, France (e-mail: alexander.zeh@uni-ulm.de).

A. Wachter-Zeh is with the Institute of Communications Engineering, University of Ulm, D-89081 Ulm, Germany and Institut de Recherche Mathémathique de Rennes (IRMAR), Université de Rennes 1, 35042 Rennes Cedex, France (e-mail: antonia.wachter@uni-ulm.de).

S. Bezzateev is with the Department of Information Systems and Security, Saint Petersburg State University of Airspace Instrumentation, Saint-Petersburg, Russia (e-mail: bsv@aanet.ru).

d is denoted by $\mathcal{C}(\mathbb{F}_q; n, k, d)$. A codeword of $\mathcal{C}(\mathbb{F}_q; n, k, d)$ is a multiple of its generator polynomial $g(x)$ with roots in $\mathbb{F}_{q^s}$, where $n \mid (q^s - 1)$. Let α be an nth root of unity of $\mathbb{F}_{q^s}$. A cyclotomic coset M_r is given by:

$$M_r = \{rq^j \bmod n,\ \forall j = 0, 1, \ldots, n_r - 1\}, \tag{1}$$

where n_r is the smallest integer such that $rq^{n_r} \equiv r \mod n$. It is well-known that the minimal polynomial $M_r(x) \in \mathbb{F}_q[x]$ of the element α^r is given by

$$M_r(x) = \prod_{i \in M_r} (x - \alpha^i). \tag{2}$$

The defining set $D_{\mathcal{C}}$ of a q-ary cyclic code $\mathcal{C}(\mathbb{F}_q; n, k, d)$ is the set containing the indices of the zeros of the generator polynomial $g(x)$ and can be partitioned into w cyclotomic cosets:

$$D_{\mathcal{C}} \stackrel{\text{def}}{=} \{i : g(\alpha^i) = 0\} = M_{r_1} \cup M_{r_2} \cup \cdots \cup M_{r_w}. \tag{3}$$

Hence, the generator polynomial $g(x) \in \mathbb{F}_q[x]$ of degree $n-k$ of $\mathcal{C}(\mathbb{F}_q; n, k, d)$ is

$$g(x) = \prod_{i=1}^{w} M_{r_i}(x). \tag{4}$$

The following lemma states the cardinality of all cyclotomic cosets M_r, if r is co-prime to the length n. We use it later to determine the rate of some classes of cyclic codes.

Lemma 1 (Cardinality): Let s be the smallest integer such that the length n divides $(q^s - 1)$, then the cardinality of the cyclotomic coset M_r is $|M_r| = s$ if $\gcd(n, r) = 1$.

Proof: The cyclotomic coset M_r has cardinality $|M_r| = j$ if and only if j is the smallest integer such that

$$r \cdot q^j \equiv r \mod n \iff r \cdot (q^j - 1) \equiv 0 \mod n.$$

Since $\gcd(n, r) = 1$, this is equivalent to $n \mid (q^j - 1)$. Since s is the smallest integer such that the length n divides $(q^s - 1)$, $j = s$ and hence, $|M_r| = s$. ∎

Let us state some preliminaries on rational functions.

Definition 1 (Period of a Power Series): Let a formal power series $a(x) = \sum_{j=0}^{\infty} a_j x^j$ with $a_j \in \mathbb{F}_q$ be given. The period $p(a(x))$ of the infinite sequence $a(x)$ is the smallest p, such that

$$a(x) = \frac{\sum_{j=0}^{p-1} a_j x^j}{-x^p + 1}$$

holds.

Throughout this paper we use the power series expansion of the fraction of two polynomials $h(x)$ and $f(x)$ in $\mathbb{F}_q[x]$ with

$$v \stackrel{\text{def}}{=} \deg h(x) < u \stackrel{\text{def}}{=} \deg f(x). \tag{5}$$

We require that:

1) $\deg \gcd(h(x), f(x)) = 0$ and
2) $\deg \gcd(f(x\alpha^i), f(x\alpha^j)) = 0, \quad \forall i \neq j, \alpha^i, \alpha^j \in \mathbb{F}_{q^s}$

to prove our main theorem on the minimum distance.

The following lemma establishes a connection between the length n of the code and the period of the power series $h(x)/f(x)$, such that 2) holds.

Lemma 2 (Code Length, Period of a Power Series): Let α be an nth root of unity of $\mathbb{F}_{q^s}$, where $n \mid (q^s - 1)$. Let $h(x), f(x) \in \mathbb{F}_q[x]$ with $\deg \gcd(h(x), f(x)) = 0$ and degree as in (5) be given. The formal power series is $h(x)/f(x) \stackrel{\text{def}}{=} \sum_{j=0}^{\infty} a_j x^j$ over $\mathbb{F}_q$ with period $p(h(x)/f(x)) = p$. If the period p and n are co-prime then

$$\deg \gcd(f(x\alpha^i), f(x\alpha^j)) = 0,\ \forall i \neq j.$$

Proof: From Definition 1, we have

$$h(x)(-x^p + 1) = f(x)(a_0 + a_1 x + \ldots + a_{p-1} x^{p-1}),$$

and from $\deg \gcd(f(x), h(x)) = 0$, it follows that $-x^p + 1 \equiv 0 \mod f(x)$. Hence, for two different polynomials $f(x\alpha^i)$ and $f(x\alpha^j)$, for any $i \neq j,\ i, j = 0, \ldots, n-1$:

$$\begin{aligned} x^p \alpha^{ip} - 1 &\equiv 0 \mod f(x\alpha^i) \quad \text{and} \\ x^p \alpha^{jp} - 1 &\equiv 0 \mod f(x\alpha^j). \end{aligned} \tag{6}$$

Assume there is some element $\beta \in \mathbb{F}_{q^{us}} \setminus \{0\}$, such that

$$f(\beta\alpha^i) = f(\beta\alpha^j) = 0,$$

$$\text{i.e., } \gcd(f(x\alpha^i), f(x\alpha^j)) \equiv 0 \mod (x - \beta).$$

Equation (6) gives the following:

$$\beta^p \alpha^{ip} - 1 = 0 \quad \text{and} \quad \beta^p \alpha^{jp} - 1 = 0\,.$$

Therefore, $\beta^p \alpha^{ip} = \beta^p \alpha^{jp}$, and $\alpha^{ip} = \alpha^{jp}$, hence, $\alpha^{(i-j)p} = 1$. For any $i \neq j, i, j = 0, \ldots, n-1$, this can be true only if $\gcd(p, n) > 1$. ∎

B. Known Bounds On the Minimum Distance

Let us shortly recall well-known bounds on the minimum distance of cyclic codes.

Theorem 1 (Hartmann–Tzeng (HT) Bound, [5]): Let $\mathcal{C}(\mathbb{F}_q; n, k, d)$ be a q-ary cyclic code of length n, dimension k, distance d and with defining set $D_{\mathcal{C}}$. Let

$$\{b + i_1 m_1 + i_2 m_2,\ \forall i_1 = 0, \ldots, d_0 - 2, i_2 = 0, \ldots, \nu\} \subseteq D_{\mathcal{C}},$$

where $\gcd(n, m_1) = 1$ and $\gcd(n, m_2) = 1$. Then $d \geq d_{\text{HT}} \stackrel{\text{def}}{=} d_0 + \nu$.

Note that for $\nu = 0$ the HT bound becomes the BCH bound [2], [3] and it is denoted by d_{BCH}. A further generalization was proposed by Roos [8], [9].

C. BCH Bound with Rational Function

Let $c(x) = \sum_{i=0}^{n-1} c_i x^i$ denote the polynomial representation of a codeword $(c_0\ c_1\ \ldots\ c_{n-1})$ of a cyclic code $\mathcal{C}(\mathbb{F}_q; n, k, d \geq d_0)$. We consider the BCH bound in the following and assume that $\nu = 0$ and $m_1 = 1$ and therefore $c(\alpha^i) = 0,\ \forall i = b, \ldots, b + d_0 - 2$, such that d_0 is maximal. Let the formal power series $a(b, \alpha^i x)$

$$a(b, \alpha^i x) \stackrel{\text{def}}{=} \frac{\alpha^{ib}}{1 - \alpha^i x} = \alpha^{ib} \sum_{j=0}^{\infty} (\alpha^i x)^j \tag{7}$$

be given. For any $c(x) \in \mathcal{C}(\mathbb{F}_q; n, k, d)$ we can rewrite the BCH bound as follows:

$$\sum_{j=0}^{\infty} c(\alpha^{j+b})x^j = \sum_{i=0}^{n-1} c_i \alpha^{ib} + \sum_{i=0}^{n-1} c_i \alpha^i \alpha^{ib} x + \ldots \equiv 0 \bmod x^{d_0-1}, \quad (8)$$

and with (7) we can rewrite (8) as:

$$\sum_{i=0}^{n-1} c_i \frac{\alpha^{ib}}{1-\alpha^i x} = \sum_{i=0}^{n-1} c_i \cdot a(b, \alpha^i x) \equiv 0 \bmod x^{d_0-1}. \quad (9)$$

Let $\mathcal{W}$ be the set of nonzero positions of a codeword and let $|\mathcal{W}| = d$. With $\gcd(1-\alpha^i x, 1-\alpha^j x) = 1,\ \forall i \neq j$, we can write (9) as follows:

$$\frac{\sum_{i \in \mathcal{W}} \left(c_i \cdot \alpha^{ib} \cdot \prod_{\substack{j \in \mathcal{W} \\ j \neq i}} (1-\alpha^j x) \right)}{\prod_{i \in \mathcal{W}} (1-\alpha^i x)} \equiv 0 \bmod x^{d_0-1}, \quad (10)$$

where the degree of the numerator is less than or equal to $d-1$ and has to be greater than or equal to $d_0 - 1$ to obtain zero on the RHS of (10). Then, the minimum distance d of a cyclic code $\mathcal{C}$ is $d \geq d_0$.

III. Roots of Cyclic Codes Represented by Rational Functions

Our idea for bounding the distance of q-ary cyclic codes originates from the definition and properties of classical Goppa codes [16], [17] and generalized Goppa codes [18], [19]. We do not present the theory of Goppa codes here, since we use only the properties of rational functions introduced in Section II.

Let b be an integer and let α be an nth root of unity. Let $h(x), f(x) \in \mathbb{F}_q[x]$ with degree v and u and with $\deg \gcd(h(x), f(x)) = 0$ be given. The power series $a(b, \alpha^i x)$ is defined such that:

$$a(b, \alpha^i x) \stackrel{\text{def}}{=} \frac{\alpha^{ib} h(\alpha^i x)}{f(\alpha^i x)} = \sum_{j=0}^{\infty} a_j \alpha^{ib} (\alpha^i x)^j = a_0 \alpha^{ib} + a_1 \alpha^{ib} \alpha^i x + a_2 \alpha^{ib} (\alpha^i x)^2 + \ldots . \quad (11)$$

Similar to the case of the BCH bound, we associate a q-ary cyclic code $\mathcal{C}$ with a power series $a(b, \alpha^i x)$ as follows.

Definition 2 (Connection between Power Series and Code): Let a power series $a(b, \alpha^i x)$ (or respectively two polynomials $h(x), f(x)$ and an integer b) with $\deg \gcd(h(x), f(x)) = 0$ and a q-ary cyclic code $\mathcal{C}(\mathbb{F}_q; n, k, d)$ be given. Furthermore, let $\gcd\left(n, p(h(x)/f(x))\right) = 1$. Let α denote an nth root of unity. Then, there exist a $\mu \geq 0$, such that for all $c(x) \in \mathcal{C}$:

$$\sum_{j=0}^{\infty} a_j c(\alpha^{j+b}) x^j \equiv 0 \bmod x^{\mu-1} \quad (12)$$

holds.

Before we prove the main theorem on the minimum distance of a cyclic code $\mathcal{C}$, let us describe Definition 2. We search the longest "sequence"

$$a_0 c(\alpha^b), a_1 c(\alpha^{b+1}), \ldots, a_{\mu-2} c(\alpha^{b+\mu-2}),$$

that is a zero-sequence, i.e., the product of the coefficient a_j and the evaluated codeword $c(\alpha^{b+j})$ gives zero for all $j = 0, \ldots, \mu-2$. We require a root α^j of the code $\mathcal{C}$, if the coefficient a_{j-b} of the power series $a(b, \alpha^i x)$ is nonzero.

Equation (12) can be rewritten in terms of the polynomials $h(x)$ and $f(x)$ as follows:

$$\sum_{j=0}^{\infty} a_j c(\alpha^{j+b}) x^j = \sum_{j=0}^{\infty} \sum_{i=0}^{n-1} a_j c_i \alpha^{i(j+b)} x^j = \sum_{i=0}^{n-1} c_i \Big(\sum_{j=0}^{\infty} a_j \alpha^{i(j+b)} x^j \Big) = \sum_{i=0}^{n-1} c_i \frac{\alpha^{ib} h(\alpha^i x)}{f(\alpha^i x)} \equiv 0 \bmod x^{\mu-1}. \quad (13)$$

Let $\mathcal{W}$ be the set of nonzero positions of a codeword and let $|\mathcal{W}| = d$. With $\deg \gcd(f(\alpha^i x), f(\alpha^j x)) = 0,\ \forall i \neq j$ (that follows from $\gcd\left(n, p(h(x)/f(x))\right) = 1$ according to Lemma 2), we can write (13) as

$$\frac{\sum_{i \in \mathcal{W}} \left(c_i \cdot \alpha^{ib} \cdot h(\alpha^i x) \cdot \prod_{\substack{j \in \mathcal{W} \\ j \neq i}} f(\alpha^j x) \right)}{\prod_{i \in \mathcal{W}} f(\alpha^i x)} \equiv 0 \bmod x^{\mu-1}, \quad (14)$$

where the degree of the denominator is ud and the numerator has degree smaller than or equal to $(d-1)u + v$. This leads to the following theorem on the minimum distance of $\mathcal{C}$.

Theorem 2 (Minimum Distance): Let a q-ary cyclic code $\mathcal{C}(\mathbb{F}_q; n, k, d)$ be given and let α denote an nth root of unity. Let two co-prime polynomials $h(x)$ and $f(x)$ in $\mathbb{F}_q[x]$ with degrees v and u, respectively and the integers b and μ be given, such that (14) holds. Let $\gcd\left(n, p(h(x)/f(x))\right) = 1$.

Then, the minimum distance d of $\mathcal{C}(\mathbb{F}_q; n, k, d)$ satisfies the following inequality:

$$d \geq d_f \stackrel{\text{def}}{=} \left\lceil \frac{\mu - 1 - v}{u} + 1 \right\rceil. \quad (15)$$

Proof: For a codeword $(c_0\ c_1\ \ldots\ c_{n-1})$ of weight d, the degree of the numerator in (14) is less than or equal to $(d-1)u + v$ and has to be greater than or equal to $\mu - 1$. ■

Example 1 (Binary Cyclic Code): Consider the binary cyclic code $\mathcal{C}(\mathbb{F}_2; 17, 9, 5)$ with defining set $D_{\mathcal{C}} = M_1 = \{1, 2, 4, 8, 16, 15, 13, 9\} \equiv \{1, 2, 4, 8, -1, -2, -4, -8\} \bmod 17$. Let $b = -4, h(x) = x + 1$ and $f(x) = x^2 + x + 1 \in \mathbb{F}_2[x]$ be given. Then, $a(-4, \alpha^i x)$ has according to Definition 1 period of three and we have $(a_0\ a_1\ a_2) = (1\ 0\ 1)$.

The following table illustrates how we match the roots of the generator polynomial to the zeros of the power series expansion $a(-4, \alpha^i x)$. In the first row, the defining set is shown, i.e., $c(\alpha^j) = 0$ for all $j \in D_{\mathcal{C}}$. The □ marks elements that are not necessarily roots of the code. In the second row of the table, the power series expansion $\mathbf{a} = (a_0\ a_1\ a_2\ a_0\ a_1\ \ldots)$ is shown for the considered interval.

$D_{\mathcal{C}}$	-4	□	-2	-1	□	1	2	□	4
a	1	0	1	1	0	1	1	0	1

We have $a_j \cdot c(\alpha^{j-4}) = 0, \forall j = 0, \ldots, 8$, for all $c(x) \in \mathcal{C}(\mathbb{F}_2; 17, 9, 5)$. We obtain a zero-sequence of length $\mu - 1 = 9$ and therefore with Theorem 2, $d_f = 5$. This is the actual distance d of this code.

In next section, we see that $\mathcal{C}(\mathbb{F}_2; 17, 9, 5)$ belongs to the class of reversible codes and we can associate this rational function to the whole class.

Let us illustrate the case where $\deg h(\alpha^i x) > 0$. For $h(\alpha^i x) = h_0 + h_1\alpha^i x + \cdots + h_v(\alpha^i x)^v$ we decompose the power series expansion of (11) into:

$$a(b, \alpha^i x) = \alpha^{ib}\left(\frac{h_0}{f(\alpha^i x)} + \cdots + \frac{h_v(\alpha^i x)^v}{f(\alpha^i x)}\right). \tag{16}$$

Our classification of q-ary cyclic codes based on Theorem 2 works as follows. In the first step, we consider the power series expansion $1/f(x) = (\overline{a}_0 + \overline{a}_1 x + \cdots + \overline{a}_{p-1}x^{p-1})/(-x^p + 1)$ with period $p = p(1/f(\alpha^i x))$. From (16) we can interpret $a(b, \alpha^i x)$ as a linear combination of $v + 1$ shifted series expansion $1/f(\alpha^i x)$:

$$\begin{aligned} & h_0(\overline{a}_0\ \overline{a}_1\ \ldots\ \overline{a}_{p-1}) \\ + & \ h_1(\overline{a}_{p-1}\ \overline{a}_0\ \ldots\ \overline{a}_{p-2}) \\ + & \qquad \vdots \\ + & \ h_v(\overline{a}_{p-v}\ \overline{a}_{p-v+1}\ \ldots\ \overline{a}_{p-1-v}) \\ = & \ (a_0\ a_1\ \ldots\ a_{p-1}). \end{aligned}$$

Then, we can select b such that the characteristic sequence of $a_0c(\alpha^b), a_1c(\alpha^{b+1}), \ldots, a_{\mu-2}c(\alpha^{b+\mu-2})$ becomes zero for the maximal μ of a given code $\mathcal{C}(\mathbb{F}_q; n, k, d)$.

IV. On the Distance of Some Classes of q-ary Cyclic Codes

A. Structure of Classification and Cardinality

Before we describe our classification let us extend Definition 2. We introduce an equivalent parameter to m_1 and m_2 of the HT bound which is denoted by z_1. We search for a given power series $a(b, \alpha^i x)$ and a cyclic code $\mathcal{C}$ the "longest" sequence:

$$a_0c(\alpha^b), a_1c(\alpha^{b+z_1}), \ldots, a_{\mu-2}c(\alpha^{b+(\mu-2)z_1}),$$

that is a zero-sequence of length $\mu - 1$.

We classify q-ary cyclic codes by subsets of their defining set $D_\mathcal{C}$ and their length n. We specify our new lower bound (Theorem 2) on the minimum distance for some classes of codes. Additionally, we compare it to the BCH [2], [3] and the HT [5] bound, which we denote by d_{BCH} and d_{HT}.

We use the following power series expansions $1/f(x)$ over $\mathbb{F}_q$ with period p, where $\mathbf{a} = (a_0\ a_1\ \ldots\ a_{p-1})$ denotes the coefficients.

- $1/(x^2 + x + 1)$ over $\mathbb{F}_q$ with $\mathbf{a} = (1\ \text{-}1\ 0)$ and $p = 3$,
- $1/(x^3 + x^2 + x + 1)$ over $\mathbb{F}_q$ with $\mathbf{a} = (1\ \text{-}1\ 0\ 0)$ and $p = 4$,
- $1/(x^3 + x + 1)$ over $\mathbb{F}_2$ with $\mathbf{a} = (1\ 1\ 1\ 0\ 1\ 0\ 0)$ and $p = 7$,
- $1/(x^4 + x + 1)$ over $\mathbb{F}_2$ with $\mathbf{a} = (1\ 1\ 1\ 1\ 0\ 1\ 0\ 1\ 1\ 0\ 0\ 1\ 0\ 0\ 0)$ and $p = 15$.

We match a power series expansion $a(b, \alpha^i x)$ to the roots of the generator polynomial, such that $a_j \cdot g(\alpha^{b+jz_1}) = a_j \cdot c(\alpha^{b+jz_1}) = 0, \forall j = 0, \ldots, \mu - 2$.

Throughout this section, we assume due to Lemma 2 that $\gcd(n, p) = 1$ and we use Theorem 2 to state the lower bound d_f on the distance of the codes.

In Table I, all cyclic shifts of the power series expansions of $1/(x^2 + x + 1)$ and $1/(x^3 + x^2 + x + 1)$ are shown and the corresponding numerator $h(x)$ is given. First, we apply our approach to the wide class of reversible codes. Afterwards, we show how our principle can equivalently be used for non-reversible codes.

TABLE I
Power series $(a_0\ \ldots\ a_{p-1})$ for the rational functions $1/(x^2 + x + 1)$ and $1/(x^3 + x^2 + x + 1)$ and their corresponding cyclic shift.

$(a_0\ \ldots\ a_{p-1})$	$f(x)$	$h(x)$
(1 -1 0)	$1 + x + x^2$	1
(-1 0 1)	$1 + x + x^2$	$-1 - x$
(0 1 -1)	$1 + x + x^2$	x
(1 -1 0 0)	$1 + x + x^2 + x^3$	1
(0 1 -1 0)	$1 + x + x^2 + x^3$	x
(0 0 1 -1)	$1 + x + x^2 + x^3$	x^2
(-1 0 0 1)	$1 + x + x^2 + x^3$	$-1 - x - x^2$

B. Reversible Codes

In this subsection, we show how our approach can be applied for a large class of cyclic codes — the class of *reversible codes* [20], [22]. A code $\mathcal{C}$ is reversible if for any codeword $\mathbf{c} = (c_0\ c_1\ \ldots\ c_{n-1}) \in \mathcal{C}$ also $\mathbf{c} = (c_{n-1}\ c_{n-2}\ \ldots\ c_0) \in \mathcal{C}$. A cyclic code is reversible if and only if the reciprocal of every zero of the generator polynomial $g(x)$ is also a zero of $g(x)$, i.e.,

$$D_\mathcal{C} = \{i_1, i_2, \ldots, i_\ell, -i_1, -i_2, \ldots, -i_\ell\}. \tag{17}$$

A special class of reversible codes, which we call *symmetric reversible codes* is given based on the following lemma.

Lemma 3 (Symmetric Reversible Codes): Let n be the length of a q-ary cyclic code. Any union of cyclotomic cosets is a defining set of a reversible code if and only if $n \mid (q^m + 1)$, for some $m \in \mathbb{N}$.

Proof: Any union of cyclotomic cosets defines a reversible code if and only if any coset is reversible, i.e., if for all r and some integer m:

$$M_r = \{r, r \cdot q, \ldots, r \cdot q^{m-1}, -r, -r \cdot q, \ldots, -r \cdot q^{m-1}\}.$$

Therefore for all r, the following has to hold:

$$r \cdot q^m \equiv -q \mod n \iff r \cdot (q^m + 1) \equiv 0 \mod n.$$

Since $r = 1$ always defines a cyclotomic coset, $(q^m + 1) \equiv 0 \mod n$ has to hold. This is fulfilled if and only if $n \mid (q^m + 1)$ and in this case also $r \cdot (q^m + 1) \equiv 0 \mod n$ holds for any r. ∎

Moreover, the following lemma provides the cardinality of all cyclotomic cosets if $n \mid (q^m + 1)$.

Lemma 4 (Cardinality of Symmetric Reversible Codes): Let m be the smallest integer such that n divides $(q^m + 1)$, then the cardinality of the cyclotomic coset M_r is $|M_r| = 2m$ if $\gcd(n, r) = 1$.

Proof: Since $n \mid (q^m + 1)$, it follows also that $n \mid (q^m + 1)(q^m - 1) = (q^{2m} - 1)$. Since m is the smallest integer such that n divides $(q^m + 1)$, also $s \stackrel{\text{def}}{=} 2m$ is the smallest integer such that $n \mid (q^s - 1)$. With Lemma 1, we obtain $|M_r| = s$ if $\gcd(n, r) = 1$. Therefore, $|M_r| = s = 2m$. ∎

In order to illustrate our bound, we first restrict ourselves to binary codes. To give a new bound on the minimum distance, we first use the rational function $a(x) = h(x)/f(x)$ with $f(x) = x^2 + x + 1$, where $p(a(x)) = 3$. For a binary symmetric reversible code $\mathcal{C}$, we showed that each cyclotomic coset is symmetric. Therefore, if $\{1\} \subseteq D_\mathcal{C}$, we know that $\{-4, -2, -1, 1, 2, 4\}$ is in the defining set. Let us use the (cyclically shifted) power series expansion $\mathbf{a} = (-1\ 0\ 1\ \ldots)$. According to Table I, we have $h(x) = -1 - x$. We match the roots of $\mathcal{C}$ for $b = -4$ and $z_1 = 1$, to a zero-sequence of length $\mu - 1 = 9$. Therefore our bound provides $d \geq d_f = 5$.

Let the defining set $D_\mathcal{C}$ of the binary symmetric reversible code $\mathcal{C}$ additionally include 5. Then we obtain for $b = -6$ and $z_1 = 1$ a sequence of length $\mu - 1 = 13$, which results in $d_f = 7$.

In the same way, if $\{1, 5, 7\} \subseteq D_\mathcal{C}$, we obtain $\mu - 1 = 21$ with $b = -10$ and $z_1 = 1$ and thus, $d_f = 11$. These parameters are shown in Table II and compared with the BCH and HT bounds.

TABLE II
BOUNDS ON THE DISTANCE OF q-ARY CYCLIC CODES OF LENGTH $n \mid (q^s - 1)$ AND $\gcd(n, 3) = 1$, USING $f(x) = x^2 + x + 1$

Binary Symmetric Reversible	$\{1\} \subseteq D_\mathcal{C}$	$\{1, 5\} \subseteq D_\mathcal{C}$	$\{1, 5, 7\} \subseteq D_\mathcal{C}$
	$k \geq n - \ell$	$k \geq n - 2\ell$	$k \geq n - 3\ell$
Binary Reversible	$\{-1, 1\} \subseteq D_\mathcal{C}$	$\{-5, -1, 1, 5\} \subseteq D_\mathcal{C}$	$\{-7, -5, -1, 1, 5, 7\} \subseteq D_\mathcal{C}$
	$k \geq n - 2\ell$	$k \geq n - 4\ell$	$k \geq n - 6\ell$
General q-ary	$\{-4, -2, -1, 1, 2, 4\} \subseteq D_\mathcal{C}$	$\{-5, -4, -2, -1, 1, 2, 4, 5\} \subseteq D_\mathcal{C}$	$\{-10, -7, -5, -4, -2, -1, 1, 2, 4, 5, 7, 10\} \subseteq D_\mathcal{C}$
BCH	$d_{\text{BCH}} = 4$	$d_{\text{BCH}} = 5$	$d_{\text{BCH}} = 8$
	$b = -4$	$b = -5$	$b = -10$
	$m_1 = 3$	$m_1 = 3$	$m_1 = 3$
HT	$d_{\text{HT}} = 5$	$d_{\text{HT}} = 6$	$d_{\text{HT}} = 9$
	$b = -4$	$b = -5$	$b = -10$
	$m_1 = 3$	$m_1 = 3$	$m_1 = 3$
	$m_2 = 2$	$m_2 = 1$	$m_2 = 2$
	$d_0 = 4$, $\nu = 1$	$d_0 = 5$, $\nu = 1$	$d_0 = 8$, $\nu = 1$
Fractions	$d_f = 5$	$d_f = 7$	$d_f = 11$
	$b = -4$	$b = -6$	$b = -10$
	$z_1 = 1$	$z_1 = 1$	$z_1 = 1$
	$\mu = 10$	$\mu = 14$	$\mu = 22$
	$\mathbf{a} = (-1\ 0\ 1)$	$\mathbf{a} = (0\ 1\ -1)$	$\mathbf{a} = (-1\ 0\ 1)$

As mentioned before, reversible codes are defined such that the reciprocal of each root of the generator polynomial is also a root. Therefore, a defining set where $r \subseteq D_\mathcal{C}$, and also $-r \subseteq D_\mathcal{C}$ defines a reversible code if $\gcd(r, n) = 1$ and $\gcd(-r, n) = 1$. The conditions are necessary to guarantee that both cyclotomic cosets have the same cardinality (compare Lemma 1) and hence each reciprocal root is also in the defining set. The second row of Table II shows which subsets have to be in the defining set in order to obtain the same parameters as for binary *symmetric* reversible codes. Note that s is the smallest integer such that the length n divides $q^s - 1$.

This principle can easily be generalized to q-ary codes. The third row of Table II gives these results in general. Note that in Table II, $\gcd(n, p = 3) = 1$ has to hold because of Lemma 2.

Example 2 (Binary Symmetric Reversible Code): The binary cyclic code $\mathcal{C}(\mathbb{F}_2; 17, 9, 5)$ from Example 1 is symmetric reversible since Lemma 3 is fulfilled. If $\{1\} \subseteq D_\mathcal{C}$, then $D_\mathcal{C} = \{1, 2, 4, 8, 16, 15, 13, 9\} \equiv \{1, 2, 4, 8, -1, -2, -4, -8\} \mod 17$ and we obtain $d_f = 5$.

For this class of binary cyclic codes, the bound $d \geq 5$ on the minimum distance can be also obtained by another way (as pointed out by a reviewer). With $b = -4$ and $m_1 = 3$ we know from the BCH bound that the minimum distance is at least four. A binary cyclic code of even weight codewords has the zero in the defining set and we would obtain five consecutive zeros (resulting in a minimum distance of at least six). This implies that a codeword of weight four can not exists and therefore a binary cyclic code $\mathcal{C}$, where $\{-4, -2, -1, 1, 2, 4\} \subseteq D_\mathcal{C}$, has at least minimum distance five.

In Table III, we list some classes of cyclic codes where the denominator $f(x)$ of the rational function $\alpha^{ib} h(\alpha^i x)/f(\alpha^i x)$ has degree three and the period is $p(1/(x^3 + x^2 + x + 1)) = 4$. The power series expansion is $1/(x^3 + x^2 + x + 1) = (1 - x)/(-x^4 + 1)$. Let us consider the second class, where in the case of a binary symmetric reversible code the set $\{3, 5, 11\}$ must be in the defining set of the code. The HT bound gives the same lower bound on the minimum distance as our approach $d_{\text{HT}} = 5$.

Example 3 (Binary Cyclic Code): The binary cyclic code $\mathcal{C}(\mathbb{F}_2; 45, 31, 4)$ with $D_\mathcal{C} = \{-5, -3, 3, 5\} = \{3, 5, 6, 10, 12, 20, 21, 24, 25, 33, 35, 39, 40, 42\}$ is in the class of codes in the first column of Table III. We obtain $d_f = 4$, which is the actual distance of the code.

Note that $3 \mid 45$ and therefore we can not use Table II.

C. Non-Reversible Codes

In this subsection, we show that our principle equivalently can be used for non-reversible codes. We use one $f(x)$ of degree three and one $f(x)$ of degree four. We give some classes of binary cyclic codes in this subsection to show the principle. The power series expansion of the polynomial $f(x) = x^3 + x + 1$ over $\mathbb{F}_2[x]$ has period $p = 7$. To obtain a bound on the minimum distance, we consider the case of

TABLE III
BOUNDS ON THE DISTANCE OF q-ARY CYCLIC CODES OF LENGTH $n|(q^s-1)$ AND $\gcd(n,4)=1$, USING $f(x)=x^3+x^2+x+1$.

Binary Symmetric Reversible	$\{3,5\} \subseteq D_{\mathcal{C}}$	$\{3,5,11\} \subseteq D_{\mathcal{C}}$	$\{3,5,11,13\} \subseteq D_{\mathcal{C}}$
	$k \geq n-2\ell$	$k \geq n-3\ell$	$k \geq n-4\ell$
Binary Reversible	{-5,-3,3,5} $\subseteq D_{\mathcal{C}}$	{-11,-5,-3,3,5,11} $\subseteq D_{\mathcal{C}}$	{-13,-11,-5,-3,3,5,11,13} $\subseteq D_{\mathcal{C}}$
	$k \geq n-4\ell$	$k \geq n-6\ell$	$k \geq n-8\ell$
General q-ary	{-6,-5,-3,3,5,6} $\subseteq D_{\mathcal{C}}$	{-11,-6,-5,-3,3,5,6,11} $\subseteq D_{\mathcal{C}}$	{-13,-11,-6,-5,-3,3,5,6,11,13} $\subseteq D_{\mathcal{C}}$
BCH	$d_{\text{BCH}}=3$	$d_{\text{BCH}}=3$	$d_{\text{BCH}}=4$
	$b=-6$	$b=-6$	$b=-13$
	$m_1=1$	$m_1=1$	$m_1=1$
HT	$d_{\text{HT}}=d_{\text{BCH}}$	$d_{\text{HT}}=5$	$d_{\text{HT}}=6$
	$b=-6$	$b=-11$	$b=-13$
	$m_1=1$	$m_1=8$	$m_1=8$
	$m_2=0$	$m_2=6$	$m_2=2$
	$d_0=3$	$d_0=4$, $\nu=1$	$d_0=5$, $\nu=1$
Fractions	$d_f=4$	$d_f=5$	$d_f=7$
	$b=-9$	$b=-11$	$b=-17$
	$z_1=2$	$z_1=2$	$z_1=2$
	$\mu=11$	$\mu=13$	$\mu=19$
	$\mathbf{a}=$(0 0 1 -1)	$\mathbf{a}=$(0 0 1 -1)	$\mathbf{a}=$(0 0 1 -1)

extended binary cyclic codes, where the 0 is in the defining set $D_{\mathcal{C}}$. Assume that $\{-3,0,1,7\} \subseteq D_{\mathcal{C}}$. The sequence of zeros of the binary code can be matched to the rational function for $b=-4$ and $z_1=1$. The corresponding distance is then $d_f=5$. This and some other combinations of subsets of $D_{\mathcal{C}}$ are shown in Table IV. Another class of binary cyclic codes

TABLE IV
BOUNDS ON THE DISTANCE OF BINARY CYCLIC CODES OF LENGTH $n \mid (2^s-1)$ AND $\gcd(n,7)=1$, USING $f(x)=x^3+x+1$

Binary Codes	$\{-3,0,1,7\} \subseteq D_{\mathcal{C}}$	$\{-3,0,1,7,9\} \subseteq D_{\mathcal{C}}$	$\{-3,0,1,7,9,11\} \subseteq D_{\mathcal{C}}$
	$k \geq n-4\ell$	$k \geq n-5\ell$	$k \geq n-6\ell$
BCH	$d_{\text{BCH}}=4$	$d_{\text{BCH}}=4$	$d_{\text{BCH}}=4$
	$b=-3$	$b=-3$	$b=-3$
	$c_1=5$	$c_1=5$	$c_1=5$
HT	$d_{\text{HT}}=4$	$d_{\text{HT}}=4$	$d_{\text{HT}}=4$
	$b=-3$	$b=-3$	$b=-3$
	$m_1=5$	$m_1=5$	$m_1=5$
	$m_2=0$	$m_2=0$	$m_2=0$
	$d_0=4$, $\nu=0$	$d_0=4$, $\nu=0$	$d_0=4$, $\nu=0$
Fractions	$d_f=5$	$d_f=6$	$d_f=7$
	$b=-4$	$b=-4$	$b=-4$
	$z_1=1$	$z_1=1$	$z_1=1$
	$\mu=14$	$\mu=16$	$\mu=19$
	$\mathbf{a}=$ (1 0 0 1 1 1 0)	$\mathbf{a}=$ (1 0 0 1 1 1 0)	$\mathbf{a}=$ (1 0 0 1 1 1 0)

can be identified using the polynomial $f(x)=x^4+x+1$ with $p(1/f(x))=15$. We use the shifted power series expansion such that $\mathbf{a}=(1\ 0\ 0\ 1\ 0\ 0\ 0\ 1\ 1\ 1\ 1\ 0\ 1\ 0\ 1)$.

As required by Lemma 2, we only consider lengths n, such that $\gcd(n,p=15)=1$. We can match a concatenation of $\mathbf{a}$ to the roots of the generator polynomial for $b=-6$ and $z_1=1$ if $\{1,3,9,-3\} \subseteq D_{\mathcal{C}}$. Our bound on the distance yields $d_f=6$, since $\deg f(x)=4$, whereas the BCH and the HT bound give $d_{\text{BCH}}=d_{\text{HT}}=5$.

Table VI and VII in the appendix show our bound for binary and ternary cyclic codes. We used the power series expansions of $1/(x^2+x+1)$ and $1/(x^3+x^2+x+1)$ to obtain a good refinement of our new bound on the minimum distance. We list the number of codes, for which the BCH bound is not tight ($\#d_{\text{BCH}} < d$), the number of cases, where our bound is better than the BCH bound ($\#d_f > d_{\text{BCH}}$) and count the cases, where our bound is not tight ($\#d_f < d$). All lengths n, for which any union of cyclotomic cosets is a symmetric reversible code, are marked by a star $*$.

V. GENERALIZING BOSTON'S BOUNDS

In [13], Boston gave ten bounds, denoted by d_{B}, on the minimum distance of q-ary cyclic codes, which he proved using algebraic geometry. These bounds are each for a specific subset of the defining set and do not consider whole classes of codes. In this section, we show how our approach generalizes some of these bounds.

Six of Boston's ten bounds are given as follows.

Theorem 3 (Boston Bounds, [13]): The following bounds on the minimum distance of a q-ary cyclic code $\mathcal{C}$ hold:

1) If $3 \nmid n$ and $\{0,1,3,4\} \subseteq D_{\mathcal{C}}$, then $d_{\text{B}}=4$,
2) If $\{0,1,3,5\} \subseteq D_{\mathcal{C}}$, then $d_{\text{B}}=4$,
5) If $3 \nmid n$ and $\{0,1,3,4,6\} \subseteq D_{\mathcal{C}}$, then $d_{\text{B}}=5$,
6) If $4 \nmid n$ and $\{0,1,2,4,5,6,8\} \subseteq D_{\mathcal{C}}$, then $d_{\text{B}}=6$,
7) If $3 \nmid n$ and $\{0,1,3,4,6,7\} \subseteq D_{\mathcal{C}}$, then $d_{\text{B}}=6$,
10) If $3 \nmid n$ and $\{0,1,3,4,6,7,9\} \subseteq D_{\mathcal{C}}$, then $d_{\text{B}}=7$.

We use again two power series expansions $1/f(x)$. The first power series expansion is $1/(x^2+x+1)$ of period $p=3$ with $(a_0\ a_1\ a_2)=(1\ \text{-}1\ 0)$. The second considered power series expansion $1/(x^2+1)$ has period $p=4$ with $(a_0\ a_1\ a_2\ a_3)=(1\ 0\ \text{-}1\ 0)$. Note that the latter is actually a special case of the BCH bound. Table V shows the six Boston bounds. Boston's bounds 1,2,5,6 and 7 are special cases of our bounds. However, for Boston's bound 10, our approach gives a worse bound.

TABLE V
BOSTON'S BOUNDS

No	$\mathcal{I}=$	$f(x)$	$\mathbf{a}$	d_f	Conditions
1	[-1,5]	x^2+x+1	(0 1 -1 ...)	4	$\gcd(n,3)=1$
2	[0,6]	x^2+1	(0 1 0 -1 ...)	4	$\gcd(n,2)=1$
5	[-1,6]	x^2+x+1	(0 1 -1 ...)	5	$\gcd(n,3)=1$
6	[-1,8]	x^2+1	(0 1 0 -1 ...)	6	$\gcd(n,2)=1$
7	[-1,8]	x^2+x+1	(0 1 -1 ...)	6	$\gcd(n,3)=1$
10	[-1,9]	x^2+x+1	(0 1 -1 ...)	6	$\gcd(n,3)=1$

Moreover, Boston raised the following question [13]:

Question 1 (Boston's Question, [13]): Let $3 \nmid n$ and the set $T = \{0, 1, 3, 4, 6, 7, 9, 10, \ldots, r\} \subseteq D_{\mathcal{C}}$. Is the minimum distance d then $d \geq d_{\text{B}} = |T|$?

Counter-examples show that Boston's conjecture is not true (see Example 4), since the actual distance of such codes is not always $d_{\text{B}} = r+1$. However, using the power series expansion of $1/(x^2+x+1)$ with $\mathbf{a} = (0\ 1\ \text{-}1 \ldots)$ we obtain $\mu - 1 = r+2$. The minimum distance of such codes can be bounded by $d_f = \lceil (r+1)/2 + 1 \rceil$ with $u = \deg f(x) = 2$ and $v = h(x) = 1$.

Example 4 (Distance of the $\mathcal{C}(\mathbb{F}_3; 20, 6, 8)$ code): Let $D_{\mathcal{C}} = \{0, 1, 2, 3, 4, 6, 7, 8, 9, 10, 12, 14, 16, 18\}$. For Boston's scheme, we can use $T = \{0, 1, 3, 4, 6, 7, 9, 10, 12\}$ with $|T| = 9$. The actual distance is $d = 8$ and therefore, Boston's conjecture is not true. The BCH bound yields $d_{\text{BCH}} \geq 6$. Our new bound is tight and with $r = 12$, we obtain $d_f = \lceil (r+1)/2 + 1 \rceil = 8$.

VI. Generalized Key Equation and Decoding Algorithm

In this section, we present an efficient decoding algorithm up our new bound based on a generalized key equation.

Let $(r_0\ r_1\ \ldots\ r_{n-1})$ denote the received word, i.e.,

$$(r_0\ r_1\ \ldots\ r_{n-1}) = (c_0\ c_1\ \ldots\ c_{n-1}) + (e_0\ e_1\ \ldots\ e_{n-1}),$$

and let $r(x) = \sum_{i=0}^{n-1} r_i x^i$ be the received polynomial. Let $\mathcal{E} \subseteq \{0, \ldots, n-1\}$ be the set of error positions and let $|\mathcal{E}| = t$. We define the syndrome polynomial $S(x)$:

$$\begin{aligned} S(x) &\equiv \sum_{i=0}^{n-1} r_i \frac{\alpha^{ib} h(\alpha^i x)}{f(\alpha^i x)} \\ &= \sum_{i \in \mathcal{E}} e_i \frac{\alpha^{ib} h(\alpha^i x)}{f(\alpha^i x)} \mod x^{\mu-1}. \end{aligned} \tag{18}$$

Thus, the explicit form of the syndrome polynomial $S(x)$ is

$$S(x) = \sum_{j=0}^{\mu-2} a_j r(\alpha^{j+b}) x^j = \sum_{j=0}^{\mu-2} a_j e(\alpha^{j+b}) x^j. \tag{19}$$

Based on the relation between the rational function $\alpha^{ib} \cdot h(\alpha^i x)/f(\alpha^i x)$ and all codewords of a q-ary cyclic code $\mathcal{C}(\mathbb{F}_q; n, k, d)$ as defined in Definition 2 in Section III, we introduce a generalized error-locator polynomial $\Lambda(x)$ and error-evaluator polynomial $\Omega(x)$ and relate it to the syndrome definition of (18). Let $\mathcal{E}$ denote the set of error positions and let $t = |\mathcal{E}|$. We define $\Lambda(x)$ as:

$$\Lambda(x) \stackrel{\text{def}}{=} \prod_{i \in \mathcal{E}} f(\alpha^i x). \tag{20}$$

Let

$$\Omega(x) \stackrel{\text{def}}{=} \sum_{i \in \mathcal{E}} \Big(e_i \cdot \alpha^{ib} \cdot h(\alpha^i x) \cdot \prod_{\substack{j \in \mathcal{E} \\ j \neq i}} f(\alpha^j x) \Big), \tag{21}$$

and we obtain with (18) a so-called generalized key equation:

$$\begin{aligned} \Lambda(x) \cdot S(x) &\equiv \Omega(x) \mod x^{\mu-1} \quad \text{with} \\ \deg \Omega(x) &\leq (t-1)u + v \\ &< \deg \Lambda(x) = tu, \end{aligned} \tag{22}$$

since $v < u$.

The main step of our decoding algorithm is to determine $\Lambda(x)$ and $\Omega(x)$ if $S(x)$ is given. The following lemma shows that there is a unique solution for $\Lambda(x)$ if the number of errors is not too big.

Lemma 5 (Solving the Key Equation): Let $S(x)$ with $\deg S(x) = \mu - 2$ be given by (19). If

$$t = |\mathcal{E}| \leq \left\lfloor \frac{d_f - 1}{2} \right\rfloor, \tag{23}$$

there is a unique solution (up to a scalar factor) of the key equation (22) with $\deg \Omega(x) \leq (t-1)u + v < \deg \Lambda(x) = tu$. We can find this solution by the Extended Euclidean Algorithm (EEA) with the input polynomials $x^{\mu-1}$ and $S(x)$.

Proof: We use the properties of the EEA as proven in [23] (see also [22, Theorem 16, p. 367]). It guarantees the uniqueness (up to a scalar factor) of the solution of (22) and provides the stopping criteria of the EEA to obtain $\Lambda(x)$ and $\Omega(x)$.

We require that $\deg \gcd(\Lambda(x), \Omega(x)) = 0$ (which follows from $\deg \gcd(f(x), h(x)) = 0$ and (20) and (21)). Let the polynomials $x^{\mu-1}$ and $S(x)$ be given as input for the EEA and let the EEA stop as soon as the degree of the remainder $\deg r_i(x)$ in the ith step is less than or equal to $\lfloor (\mu-1)/2 \rfloor$. Then, we obtain the unique (except for a scalar factor) solution $\Lambda(x)$ and $\Omega(x)$ of (22), if (23) holds. For the explicit proof we refer to [22, Theorem 16, p. 367]. It shows that there is a unique solution of the generalized key equation (22) and that the EEA finds it if

$$\deg \Lambda(x) = tu \leq \left\lfloor \frac{\mu - 1}{2} \right\rfloor, \tag{24}$$

and therefore

$$t \leq \left\lfloor \frac{\mu - 1}{2u} \right\rfloor = \left\lfloor \frac{(d_f - 1)u + v}{2u} \right\rfloor = \left\lfloor \frac{(d_f - 1)}{2} \right\rfloor, \tag{25}$$

since $v/2u < 1/2$. ∎

Key equation (22) can be written as a linear system of equations, with tu coefficients of a normalized $\Lambda(x)$ as unknowns. If we consider only the equations which do not depend on $\Omega(x)$, we obtain:

$$\begin{pmatrix} S_{tu} & S_{tu-1} & \ldots & S_0 \\ S_{tu+1} & S_{tu} & \ldots & S_1 \\ & & \vdots & \\ S_{\mu-2} & S_{\mu-3} & \ldots & S_{\mu-tu-2} \end{pmatrix} \cdot \begin{pmatrix} 1 \\ \Lambda_1 \\ \vdots \\ \Lambda_{tu} \end{pmatrix} = \mathbf{0}. \tag{26}$$

There is a unique solution if and only if the rank of the syndrome matrix is tu. One coefficient of $\Lambda(x)$ can be chosen arbitrarily (here $\Lambda_0 = 1$), since a scalar factor does not change the roots. From this we obtain the same condition on the decoding radius as in Lemma 5.

If we have found $\Lambda(x)$, we can determine its factors $f(\alpha^i x)$, where $i \in \mathcal{E}$. These factors are disjoint since $\deg(\gcd(f(\alpha^i x), f(\alpha^j x))) = 0$, $\forall i \neq j$ and therefore these factors provide the error positions. We calculate only *one* root β_i of each $f(\alpha^i x)$ in a preprocessing step. To find the error positions if $\Lambda(x)$ is given, we do a Chien search with

$\beta_0, \beta_1, \ldots, \beta_{n-1}$. This is shown in Algorithm 1 and Theorem 4 proves that each β_i uniquely determines $f(\alpha^i x)$.

For the non-binary case, we have to calculate the error values at the error positions. This can be done by a generalized Forney's formula [21]. In order to obtain this error evaluation formula, we use the explicit expression for $\Omega(x)$ from (21). As mentioned before, the preprocessing step calculates n values $\beta_0, \beta_1, \ldots, \beta_{n-1}$ such that

$$f(\alpha^i \beta_i) = 0, \ \forall i = 0, \ldots, n-1, \text{ and } f(\alpha^j \beta_i) \neq 0, \ \forall j \neq i.$$

The evaluation of $\Omega(x)$ at β_ℓ, $\ell \in \mathcal{E}$, yields:

$$\Omega(\beta_\ell) = \sum_{i \in \mathcal{E}} \Big(e_i \cdot \alpha^{ib} \cdot h(\alpha^i \beta_\ell) \cdot \prod_{\substack{j \in \mathcal{E} \\ j \neq i}} f(\alpha^j \beta_\ell) \Big).$$

With $f(\alpha^\ell \beta_\ell) = 0$, the product $\prod_{j \in \mathcal{E}, j \neq i} f(\alpha^j \beta_\ell)$ is zero if $\ell \in \mathcal{E} \backslash \{i\}$ and nonzero only if $\ell = i$. Hence, we obtain

$$\Omega(\beta_\ell) = e_\ell \cdot \alpha^{\ell b} \cdot h(\alpha^\ell \beta_\ell) \cdot \prod_{\substack{j \in \mathcal{E} \\ j \neq \ell}} f(\alpha^j \beta_\ell). \tag{27}$$

This derivation provides the following lemma.

Lemma 6 (Generalized Error Evaluation): Let the integer b, the polynomials $h(\alpha^i x)$, $f(\alpha^i x)$, $\Lambda(x) = \prod_{i \in \mathcal{E}} f(\alpha^i x)$ and $\Omega(x)$ from (21), for all $i = 0, \ldots, n-1$ with $\deg(\gcd(f(\alpha^i x), f(\alpha^j x))) = 0$ be given. Then, the error values e_ℓ for all $\ell \in \mathcal{E}$ are given by

$$\begin{aligned} e_\ell &= \frac{\Omega(\beta_\ell)}{\alpha^{\ell b} \cdot h(\alpha^\ell \beta_\ell) \prod_{\substack{j \in \mathcal{E} \\ j \neq \ell}} f(\alpha^j \beta_\ell)} \\ &= \frac{\Omega(\beta_\ell) \cdot f'(\alpha^\ell \beta_\ell)}{\Lambda'(\beta_\ell) \cdot \alpha^{\ell b} \cdot h(\alpha^\ell \beta_\ell)}, \end{aligned} \tag{28}$$

where $f'(\alpha^i x)$ and $\Lambda'(x)$ denote the derivatives of $f(\alpha^i x)$ and $\Lambda(x)$.

Proof: The lemma follows from (27) and the fact that

$$\Lambda'(x) = \sum_{i \in \mathcal{E}} f'(\alpha^i x) \prod_{\substack{j \in \mathcal{E} \\ j \neq i}} f(\alpha^j x)$$

and therefore

$$\Lambda'(\beta_\ell) = f'(\alpha^\ell \beta_\ell) \prod_{\substack{j \in \mathcal{E} \\ j \neq \ell}} f(\alpha^j \beta_\ell).$$

■

Note that (28) is the classical Forney's formula [21], for $f(\alpha^i x) = 1 - \alpha^i x$ and $\alpha^{ib} \cdot h(\alpha^i x) = 1$.

The decoding approach is summarized in Algorithm 1 and its correctness is proved in Theorem 4.

Algorithm 1: Decoding q-ary Cyclic Codes

Input: Received word $r(x)$, $f(\alpha^i x)$, $\alpha^{ib} \cdot h(\alpha^i x)$

Preprocessing: Calculate one root of each $f(\alpha^i x) \Longrightarrow \beta_0, \beta_1, \ldots, \beta_{n-1}$

1 Calculate $S(x)$ by (19)

2 Solve Key Equation: Obtain $\Lambda(x)$, $\Omega(x)$ as output of $\mathrm{EEA}\,(x^{\mu-1}, S(x))$

3 Chien–Search: Find all i for which $\Lambda(\beta_i) = 0$, save them as $\widehat{\mathcal{E}} = \{i_0, i_1, \ldots, i_t\}$

4 Error Evaluation: $\widehat{e}_\ell = \Omega(\beta_\ell) / \big(h(\alpha^\ell \beta_\ell) \prod_{j \in \mathcal{E}, j \neq \ell} f(\alpha^j \beta_\ell) \big)$, for all $\ell \in \widehat{\mathcal{E}}$

5 $\widehat{e}(x) \leftarrow \sum_{\ell \in \widehat{\mathcal{E}}} \widehat{e}_\ell x^\ell$

6 $\widehat{c}(x) \leftarrow r(x) - \widehat{e}(x)$

Output: Estimated codeword $\widehat{c}(x)$

Theorem 4 (Correctness of Algorithm 1): If the distance $d(r(x), c(x)) \leq \lfloor (d_f - 1)/2 \rfloor$ for some codeword $c(x) \in \mathcal{C}$, then Algorithm 1 returns $\widehat{c}(x) = c(x)$ with complexity $\mathcal{O}((\deg f(x) \cdot n)^2)$ operations.

Proof: Let $S(x)$ be defined by (19). As shown in Lemma 5, we can then solve the key equation uniquely for $\Lambda(x)$ if $t \leq \lfloor (d_f - 1)/2 \rfloor$. Therefore, we obtain $\Lambda(x) = \prod_{i \in \mathcal{E}} f(x, \alpha_i)$ with $\deg \Lambda(x) = tu$ in Step 2 of Algorithm 1 and also $\Omega(x) \equiv \Lambda(x) \cdot S(x) \mod x^{\mu-1}$. To explain the preprocessing and the Chien–search, we note that for each polynomial $a(x)$ of degree u defined over $\mathbb{F}_{q^s}$ there exists a splitting field, i.e., an extension field $\mathbb{F}_{q^{us}}$ of $\mathbb{F}_{q^s}$, in which $a(x)$ has u roots. Therefore, each $f(\alpha^i x)$ can be decomposed into $u = \deg f(\alpha^i x)$ linear factors over a field $\mathbb{F}_{q^{us}}$. These factors are disjoint since $\deg(\gcd(f(\alpha^i x), f(\alpha^j x))) = 0$ and hence, *one* root of $f(\alpha^i x)$ uniquely defines $f(\alpha^i x)$ and i. Hence, $\Lambda(\beta_j) = 0$ if and only if $j \in \mathcal{E}$ and Step 3 correctly identifies the error positions.

Lemma 6 proves the generalized error evaluation and therefore, if $d(r(x), c(x)) \leq \lfloor (d_f - 1)/2 \rfloor$ for some codeword $c(x) \in \mathcal{C}$, Algorithm 1 returns $\widehat{c}(x) = c(x)$.

To prove the complexity, we note that the input polynomials $S(x)$ and $x^{\mu-1}$ of the EEA have degrees at most $\mu - 2$ and $\mu - 1$, respectively. Therefore, the complexity of the EEA is quadratic in μ, i.e., $\mathcal{O}(\mu^2) \approx \mathcal{O}((u \cdot d_f)^2)$. The Chien–search and the generalized error evaluation require the same complexity as for the classical case, which is $\mathcal{O}(n^2)$. Therefore, we can upper bound the complexity of Algorithm 1 by $\mathcal{O}((u \cdot n)^2) = \mathcal{O}((\deg f(x) \cdot n)^2)$. ■

We consider the code from Example 1 to illustrate the decoding algorithm in the following.

Example 5 (Decoding Binary Code): We consider again the $\mathcal{C}(\mathbb{F}_2; 17, 9, 5)$ code and write explicitly the associated power series $a(-4, \alpha^i x)$ in polynomial form:

$$\begin{aligned} a(-4, \alpha^i x) &= \frac{\alpha^{i13} \cdot h(\alpha^i x)}{f(\alpha^i x)} \\ &= \frac{\alpha^{13i} + \alpha^{14i} x}{1 + \alpha^i x + \alpha^{2i} x^2} \\ &= \alpha^{13i} + \alpha^{15i} x^2 + \alpha^{16i} x^3 + \\ &\quad \alpha^i x^5 + \alpha^{2i} x^6 + \alpha^{4i} x^8 \mod x^9. \end{aligned} \tag{29}$$

For the syndrome polynomial, we obtain with $\mu - 1 = 9$ and (18), (19) and (29):

$$\begin{aligned} S(x) &= \sum_{i=0}^{n-1} e_i \cdot (\alpha^{13i} + \alpha^{15i}x^2 + \cdots + \alpha^{4i}x^8) \\ &= \sum_{i \in \mathcal{E}} (\alpha^{13i} + \alpha^{15i}x^2 + \cdots + \alpha^{4i}x^8) \\ &= r(\alpha^{13}) + r(\alpha^{15})x^2 + \cdots + r(\alpha^4)x^8 \\ &= S_0 + S_2x^2 + S_3x^3 + S_5x^5 + S_6x^6 + S_8x^8. \end{aligned}$$

As in Algorithm 1, we calculate $\texttt{EEA}\ (x^9, S(x))$ and stop if the degree of the remainder is smaller than $\lfloor (\mu - 1)/2 \rfloor = 4$. Assume, two errors occurred, then we obtain $\Lambda(x)$ with $\deg \Lambda(x) = tu = 2 \cdot 2 = 4$.

Using the EEA is equivalent to solving the following system of equations for $\Lambda(x)$:

$$\begin{pmatrix} 0 & S_3 & S_2 & 0 & S_0 \\ S_5 & 0 & S_3 & S_2 & 0 \\ S_6 & S_5 & 0 & S_3 & S_2 \\ 0 & S_6 & S_5 & 0 & S_3 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ \Lambda_1 \\ \vdots \\ \Lambda_4 \end{pmatrix} = \mathbf{0}, \qquad (30)$$

and with both approaches, $\Lambda(x)$ has the roots $f(\alpha^i x) = (1 + \alpha^i x + (\alpha^i x)^2)$, $\forall\ i \in \mathcal{E}$. We know that each $f(\alpha^i x) = (1 + \alpha^i x + (\alpha^i x)^2)$ has two roots in $\mathbb{F}_{2^8}$ which are unique. We have a look-up-table with one root β_i of each $f(\alpha_i x)$ and we do the Chien search for $\Lambda(x)$ with $\beta_0, \beta_1, \ldots, \beta_{n-1}$. Since this is a binary code, we do not need an error evaluation and can reconstruct the error.

VII. Conclusion

A new lower bound on the minimum distance of q-ary cyclic codes is proved. For several classes of codes, a more explicit bound on their distance is given. The connection to existing bounds (BCH, HT and Boston) is shown.

Furthermore, we derived a generalized key equation, which relates the syndrome definition and the polynomial for the determination of the error locations. This allows the realization of a quadratic-time decoding algorithm and provides an explicit expression for the error evaluation.

VIII. Acknowledgment

The authors are grateful to Maximilien Gadouleau for stimulating discussions. We thank the anonymous referees for valuable comments that improved the presentation of this paper.

References

[1] A. Zeh, A. Wachter, and S. Bezzateev, "Efficient decoding of some classes of binary cyclic codes beyond the Hartmann–Tzeng bound," in *Information Theory Proceedings (ISIT), 2011 IEEE International Symposium on*, Aug. 2011, pp. 1017–1021. [Online]. Available: http://dx.doi.org/10.1109/ISIT.2011.6033683

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

[3] R. C. Bose and D. K. R. Chaudhuri, "On a class of error correcting binary group codes," *Information and Control*, vol. 3, no. 1, pp. 68–79, March 1960. [Online]. Available: http://dx.doi.org/10.1016/S0019-9958(60)90287-4

[4] C. Hartmann, "Decoding beyond the BCH bound," *IEEE Transactions on Information Theory*, vol. 18, no. 3, pp. 441–444, May 1972. [Online]. Available: http://dx.doi.org/10.1109/TIT.1972.1054824

[5] C. Hartmann and K. Tzeng, "Generalizations of the BCH bound," *Information and Control*, vol. 20, no. 5, pp. 489–498, June 1972. [Online]. Available: http://dx.doi.org/10.1016/S0019-9958(72)90887-X

[6] ——, "Decoding beyond the BCH bound using multiple sets of syndrome sequences," *Information Theory, IEEE Transactions on*, vol. 20, no. 2, March 1974.

[7] C. Hartmann, K. Tzeng, and R. Chien, "Some results on the minimum distance structure of cyclic codes," *IEEE Transactions on Information Theory*, vol. 18, no. 3, pp. 402–409, May 1972. [Online]. Available: http://dx.doi.org/10.1109/TIT.1972.1054816

[8] C. Roos, "A generalization of the BCH bound for cyclic codes, including the Hartmann-Tzeng bound," *Journal of Combinatorial Theory, Series A*, vol. 33, no. 2, pp. 229–232, September 1982. [Online]. Available: http://dx.doi.org/10.1016/0097-3165(82)90014-0

[9] ——, "A new lower bound for the minimum distance of a cyclic code," *IEEE Transactions on Information Theory*, vol. 29, no. 3, pp. 330–332, May 1983. [Online]. Available: http://dx.doi.org/10.1109/TIT.1983.1056672

[10] J. van Lint and R. Wilson, "On the minimum distance of cyclic codes," *IEEE Transactions on Information Theory*, vol. 32, no. 1, pp. 23–40, January 1986. [Online]. Available: http://dx.doi.org/10.1109/TIT.1986.1057134

[11] I. M. Duursma and R. Koetter, "Error-locating pairs for cyclic codes," *Information Theory, IEEE Transactions on*, vol. 40, no. 4, pp. 1108–1121, August 2002. [Online]. Available: http://dx.doi.org/10.1109/18.335964

[12] I. M. Duursma and R. Pellikaan, "A symmetric Roos bound for linear codes," *J. Comb. Theory Ser. A*, vol. 113, pp. 1677–1688, November 2006.

[13] N. Boston, "Bounding minimum distances of cyclic codes using algebraic geometry," *Electronic Notes in Discrete Mathematics*, vol. 6, pp. 385–394, 2001.

[14] E. Betti and M. Sala, "A New Bound for the Minimum Distance of a Cyclic Code From Its Defining Set," *Information Theory, IEEE Transactions on*, vol. 52, no. 8, pp. 3700–3706, July 2006. [Online]. Available: http://dx.doi.org/10.1109/TIT.2006.876240

[15] G. L. Feng and K. K. Tzeng, "A new procedure for decoding cyclic and BCH codes up to actual minimum distance," *IEEE Transactions on Information Theory*, vol. 40, no. 5, pp. 1364–1374, 1994. [Online]. Available: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=333854

[16] V. D. Goppa, "Rational Representation of Codes and (L,g) Codes," *Probl. Pered. Inform.*, vol. 7, pp. 41–49, September 1971.

[17] ——, "A New Class of Linear Error Correcting Codes," *Probl. Pered. Inform.*, vol. 6, pp. 24–30, September 1970.

[18] S. V. Bezzateev and N. A. Shekhunova, "One Generalization of Goppa Codes," in *Information Theory. 1997. Proceedings., 1997 IEEE International Symposium on*, pp. 299+. [Online]. Available: http://dx.doi.org/10.1109/ISIT.1997.613221

[19] N. A. Shekhunova and E. T. Mironchikov, "Cyclic (L,G) Codes," *Probl. Pered. Inform.*, vol. 17, pp. 3–10, September 1981.

[20] J. Massey, "Reversible Codes," *Information and Control*, vol. 7, no. 3, pp. 369–380, Sep. 1964. [Online]. Available: http://dx.doi.org/10.1016/S0019-9958(64)90438-3

[21] G. Forney, "On decoding BCH codes," *Information Theory, IEEE Transactions on*, vol. 11, no. 4, pp. 549–557, 1965. [Online]. Available: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=1053825

[22] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes (North-Holland Mathematical Library)*. North Holland, June 1988.

[23] Y. Sugiyama, M. Kasahara, S. Hirasawa, and T. Namekawa, "A Method for Solving Key Equation for Decoding Goppa Codes," *Information and Control*, vol. 27, no. 1, pp. 87–99, 1975.

APPENDIX

TABLE VI
BINARY CODES AND BOUNDS WITH $\mathbf{a} = (1\ -1\ 0)$ AND $\mathbf{a} = (1\ -1\ 0\ 0)$

n	# codes	# $d_{\text{BCH}} < d$	# $d_f > d_{\text{BCH}}$	# $d_f < d$
15	32	2	2	0
17*	8	2	2	0
19	4	0	0	0
21	8	2	2	0
23	8	4	0	4
25*	8	0	0	0
27	0	0	0	0
29	4	0	0	0
31	128	34	7	31
33*	0	0	0	0
35	64	24	8	22
37	4	0	0	0
39	0	0	0	0
41*	8	4	4	4
43*	16	6	3	6
45	256	69	22	57
47	8	4	0	4
49	4	0	0	0
51	256	122	4	118
53	4	0	0	0
55	32	16	4	16
57*	32	10	4	10
59	4	0	0	0
61	4	0	0	0
63	8192	4088	509	4088

TABLE VII
TERNARY CYCLIC CODES AND BOUNDS WITH $\mathbf{a} = (1\ -1\ 0)$ AND $\mathbf{a} = (1\ -1\ 0\ 0)$

n	# codes	# $d_{\text{BCH}} < d$	# $d_f > d_{\text{BCH}}$	# $d_f < d$
8	32	2	2	0
11	8	4	2	4
13	32	6	0	0
16	128	16	8	8
20	128	38	6	36
22	64	40	22	40
23	8	4	0	4
26	1024	512	108	490
28	128	18	2	18
32	512	102	46	57
35	32	16	2	16
37	8	4	0	4

Alexander Zeh studied electrical engineering at the University of Applied Science in Stuttgart, with the main topic automation technology. He received his Dipl.-Ing. (BA) degree in 2004. He continued his studies at Universität Stuttgart until 2008, where he received is Dipl.-Ing. in electrical engineering. He participated in the double-diploma program with Télécom ParisTech (former ENST) from 2006 to 2008 and he received also a french diploma. Currently he is a Ph.D. student at the Institute of Communications Engineering, University of Ulm, Germany and at the Computer Science Department (LIX), École Polytechnique ParisTech, Paris, France. His current research interests include coding and information theory, signal processing, telecommunications and the implementation of fast algorithms on FPGAs.

Antonia Wachter-Zeh studied electrical engineering at the University of Applied Science in Ravensburg, with the main topic communication technology. She received her Dipl.-Ing. (BA) degree in 2007. She continued her studies at the University of Ulm until 2009, where she received her M.Sc. in electrical engineering. She is currently working towards the Ph.D. degree at the Institute of Communications Engineering, University of Ulm, Germany and at the Institut de recherche mathématique de Rennes (IRMAR), Université de Rennes 1, Rennes, France. Her major research interests are topics in coding theory.

Sergey V. Bezzateev was born in Leningrad, Soviet Union, on June 10, 1957. He received his diploma in computer science from the Airspace Instrumentation Institute of Leningrad, Soviet Union in 1980. In 1987, he received his Ph.D. degree in information theory from the Airspace Instrumentation Institute of Leningrad. From 1980 to 1993, he was employed by the Airspace Instrumentation Institute. From 1993 to 1995 he worked as researcher at the Nagoya University, Japan, where he co-operated with Prof. Yoshihiro Iwadare. In 1995, he became associate professor at the Department of Information Technologies and Information Security, State University of Airspace Instrumentation (SUAI), Saint Petersburg, Russia. From 2004 till 2007, he was project leader of the Joint Laboratory Samsung-SUAI on Information Security in Wireless Networks. In 2010, he became Professor and the head of Department of Technologies of Information Security in SUAI. His main research interests include coding theory and cryptography.