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

Alexander Zeh, Antonia Wachter 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, 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 only 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] further generalizes this idea by exploiting several sets of nonconsecutive elements in the defining set. Further bounds are the Boston bounds [10] the bound by Betti–Sala [11].

Although this 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 [12]. 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 based on the representation of the code by rational functions. This approach originates from decoding Goppa [13]–[16] codes. We fit the roots of the $q$-ary cyclic code to non-zeros 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 [17]. 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 the Boston bounds. We give tables for $q = 2, 3, 5, 7$ and a length up to 62, where we count the number of codes for which our bound is better than the BCH bound.

As a second part, we give a general 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 formula [13] for the error evaluation. The time complexity of the whole decoding is quadratic with the length of the cyclic code.

This contribution is structured as follows. Section II gives some basic definitions, recalls 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 cyclic codes can be described by rational functions and prove our new lower bound on the minimum distance. Section IV provides several identified classes and we refine the lower bound of these codes. Tables compare our new lower bound 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. 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 and let $F = \text{GF}(q)$ denote a finite field of order $q$. A $q$-ary cyclic code of length $n$, dimension $k$ and minimum distance $d$ is denoted by $C(q^n; n, k, d)$. A codeword of $C(q^n; n, k, d)$ is a multiple of its generator polynomial $g(x)$ with roots in $\text{GF}(q^s)$, where $n | (q^s - 1)$. Let $\alpha$ be a $n$th root of unity of $\text{GF}(q^n)$. A cyclotomic coset $M_r$ is given by:

$$M_r = \{rq^j \mid j = 0, 1, \ldots, n_r - 1\},$$

where $n_r$ is the smallest integer such that $rq^{n_r} \equiv r \mod n$.

It is well-known that the minimal polynomial of the element...
\( \alpha^r \) is given by:
\[
M_r(x) = \prod_{i \in M_r} (x - \alpha^i).
\] (2)

The defining set \( D_C \) of a \( q \)-ary cyclic code \( C(q^n; n, k, d) \) is the set of zeros of the generator polynomial \( g(x) \) and can be partitioned into \( w \) cyclotomic cosets:
\[
D_C = \{ 0 \leq i \leq n - 1 \mid g(\alpha^i) = 0 \}
\]
\[
= M_{r_1} \cup M_{r_2} \cup \cdots \cup M_{r_w}.
\] (3)

Hence, the generator polynomial \( g(x) \) of degree \( n - k \) of \( C(q^n; n, k, d) \) is
\[
g(x) = \sum_{i=1}^{w} M_{r_i}(x).
\] (4)

The following lemma states the cardinality of all cyclotomic cosets \( M_r \), if \( r \) is co-prime to the length \( n \).

**Lemma 1 (Cardinality)** Let \( \ell \) be the smallest integer such that the length \( n \) divides \( (q^\ell - 1) \), then the cardinality of the cyclotomic coset \( M_r \) is \( |M_r| = \ell \) 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
\[
r \cdot q^j \equiv 0 \mod n \iff r \cdot (q^\ell - 1) \equiv 0 \mod n.
\]

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

Let us state some preliminaries on rational functions.

**Definition 1 (Period of a Power Series)** Let \( a(x) = \sum_{j=0}^{\infty} a_j x^j \) be given. The period \( p(a(x)) \) of the infinite sequence \( a(x) \) is the smallest \( p \), such that
\[
a(x) = \sum_{j=0}^{p-1} a_j x^j \equiv 0 \mod x^p + 1.
\]

**Lemma 2 (Length of the Period)** Let \( \alpha \) be an element of multiplicative order \( n \) in \( GF(q^n) \), where \( n \mid (q^r - 1) \). Let \( h(x), f(x) \in GF(q)[x] \) with \( \deg \gcd(h(x), f(x)) = 0 \) be given. The formal power series is \( h(x)/f(x) = \sum_{j=0}^{\infty} a_j x^j \) over \( GF(q) \) with period \( p(h(x)/f(x)) = p \). If the period \( p \) and \( n \) are co-prime then
\[
\deg \gcd(f(xa^i), f(xa^j)) = 0, \forall i \neq j.
\]

**Proof:** From Definition 1 we have
\[
h(x)(-x^p + 1) = f(x)(a_0 + a_1 x + \ldots + a_p - 1 x^{p-1}),
\] (5)

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 \( f(xa^i) \) and \( f(xa^j) \), for any \( i \neq j, i, j = 0, \ldots, n - 1 \):
\[
x^p \alpha^p - 1 \equiv 0 \mod f(xa^i) \quad \text{and} \quad x^p \alpha^p - 1 \equiv 0 \mod f(xa^j).
\] (6)

Assume there is some element \( \beta \in GF(q^{nx}) \setminus \{0\}, u = \deg f(x) \), such that
\[
f(\beta \alpha^i) = f(\beta \alpha^j) = 0,
\]
i.e., \( \gcd(f(xa^i), f(xa^j)) = 0 \mod (x - \beta) \).

**Equation (4)** 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 we obtain \( \alpha^{ip} = \alpha^{jp} \), 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 recall shortly well-known bounds on the minimum distance of cyclic codes.

**Theorem 1 (Hartmann–Tzeng (HT) Bound, [5])** Let \( C(q^n; n, k, d) \) be a \( q \)-ary cyclic code with the defining set \( D_C \). Let
\[
\{ b + i_1 c_1 + i_2 c_2 \mid 0 \leq i_1 \leq \mu - 2, 0 \leq i_2 \leq \nu \} \subseteq D_C, \quad (7)
\]
where \( \gcd(c_1, c_2) = 1 \) and \( \gcd(n, c_2) = 1 \). Then \( d \geq \mu + \nu \).

Note that for \( c_2 = 0 \) the HT bound becomes the BCH bound [4, 5]. A further generalization was proposed by Roos [8, 9].

**C. BCH Bound as Rational Function**

Let \( c(x) = \sum_{i=0}^{n-1} c_i x^i \) be a codeword of a cyclic code \( C(q^n; n, k, d \geq \mu) \). W.l.o.g., we assume that \( c(\alpha^i) = 0 \forall i = 0, \ldots, \mu - 2 \). Let the formal power series \( a(\alpha^i x) \):
\[
a(\alpha^i x) = \frac{1}{1 - \alpha x} = \sum_{j=0}^{\infty} (\alpha x)^j
\]
be given. We associate the power series \( a(\alpha^i x) \) with the codeword \( c(x) \) in the following way:
\[
\sum_{j=0}^{\infty} c(\alpha^i x) x^j = \sum_{i=0}^{n-1} c_i + \sum_{i=0}^{n-1} c_i \alpha^i x + \sum_{i=0}^{n-1} c_i (\alpha x)^2 + \ldots \equiv 0 \mod x^{\mu - 1}.
\] (9)

and with [8] we obtain:
\[
\sum_{i=0}^{n-1} c_i \frac{1}{1 - \alpha x} \equiv 0 \mod x^{\mu - 1}.
\] (10)

Let \( W \) be the set of nonzero positions \( c_i \) of a codeword \( (c_0 c_1 \ldots c_{n-1}) \) with minimal weight \( d_{\min} \). With \( gcd(1 - \alpha^i x, 1 - \alpha x) = 1 \forall i \neq j \), we can write [10]:
\[
\sum_{i \in W} c_i \left( \frac{1}{j_{\neq i}} \right) \equiv 0 \mod x^{\mu - 1},
\] (11)

where the degree of the numerator is smaller than or equal to \( d_{\min} - 1 \) and to \( d_{\min} - 1 \) has to be greater than or equal to \( \mu - 1 \) to obtain zero on the RHS of (11). Then, the minimum distance \( d \) of the cyclic code \( C \) is \( d \geq d_{\min} \geq \mu \). Note that in the
case of \( c(\alpha^i) = 0 \) \( \forall i = b + c_1, b + 2c_1, \ldots, b + (\mu - 2)c_1 \) and \( \gcd(n, c_1) = 1 \). (10) becomes:
\[
\sum_{i=0}^{n-1} c_i \frac{\alpha^{bi}}{1-\alpha^{ci}x} \equiv 0 \mod x^{\mu-1}.
\]
Let \( r(x) = c(x) + c(x) \) be the received word and let the set \( \mathcal{E} \subseteq \{0, \ldots, n - 1\} \) denote the error positions. The syndrome polynomial \( S(x) \) for \( q \)-ary cyclic codes is:
\[
S(x) = \sum_{i=0}^{n-1} r_i \frac{\alpha^{bi}}{1-\alpha^{ci}x} \mod x^{\mu-1}
\]
\[
\equiv \sum_{i \in \mathcal{E}} \frac{e_i \alpha^{bi}}{1-\alpha^{ci}x} \mod x^{\mu-1}
\]
\[
= \frac{\sum_{i \in \mathcal{E}} (e_i \cdot \alpha^{bi}) \prod_{j \in \mathcal{E}} (1-\alpha^{j}x)}{\prod_{i \in \mathcal{E}} (1-\alpha^{ci}x)} \mod x^{\mu-1},
\]
where the numerator is called the error-evaluator polynomial and the denominator is the error-locator polynomial.

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 [13, 14] and generalized Goppa codes [15, 16]. We do not present the theory of Goppa codes here, since the properties of rational functions introduced in Section II are sufficient.

Let a rational function define a power series \( a(b, \alpha^i x) \):
\[
a(b, \alpha^i x) = \frac{\alpha^{bi}h(\alpha^i x)}{f(\alpha^i x)} = \sum_{j=0}^{\infty} a_j \alpha^{bi}(\alpha^i)^j
\]
\[
= \alpha^{bi}a_0 + a_1 \alpha^{bi} \alpha^{j} x + a_2 \alpha^{bi} (\alpha^i x)^2 + \ldots,
\]
where \( h(x), f(x) \in GF(q)[x] \), \( \deg \gcd(h(x), f(x)) = 0 \) and \( u \equiv \deg f(\alpha^i x) > v \equiv \deg h(\alpha^i x). \)

Similar to the case of the BCH bound, we associate the codeword \( c(x) \) with the power series of the rational function \( h(\alpha^i x)/f(\alpha^i x) \):
\[
\sum_{j=0}^{\infty} a_j c(\alpha^{j+b})x^j = \sum_{j=0}^{n-1} \sum_{i=0}^{\infty} a_j c(\alpha^{i+j+b})x^j
\]
\[
= \sum_{i=0}^{n-1} c_i \left( \sum_{j=0}^{\infty} a_j \alpha^i (\alpha^{j+b})x^j \right)
\]
\[
= \sum_{i=0}^{n-1} \frac{\alpha^{bi}h(\alpha^i x)}{f(\alpha^i x)} \equiv 0 \mod x^{\mu-1},
\]
such that \( \mu \) is maximized.

Before we prove the main theorem on the minimum distance of a cyclic code \( C \) we describe relation (13). Let us assume w.l.o.g. that \( b = 0 \) and \( i = 0, 1, \ldots, \mu - 2 \). We search the longest “sequence” \( a_0 c(\alpha^0), a_1 c(\alpha^1), \ldots, a_{\mu-2} c(\alpha^{\mu-2}) \), that results in a zero-sequence of length \( \mu - 1 \), i.e., the product of the coefficient \( a_j \) and the evaluated codeword \( c(\alpha^j) \) gives zero. We require a root \( \alpha^j \) of the code \( C \), if the coefficient \( a_j \) of the power series \( a(x) = h(x)/f(x) \) is non-zero and vice versa. In Section IV we identify several classes of cyclic codes by means of their length and defining set \( D_C \) and map the roots to some power series expansions to obtain a long sequence and therefore a good bound on the distance.

Let \( (c_0, c_1, \ldots, c_{n-1}) \in C(q^s; n, k, d) \) be a codeword of minimal weight \( d_{\text{min}} \) and let \( W \) be the set of nonzero positions \( c_i \). With \( \deg \gcd(f(\alpha^i x), f(\alpha^j x)) = 0 \) \( \forall i \neq j \), we can write (15):
\[
\sum_{i \in W} c_i \cdot (h(\alpha^i x) \cdot \prod_{j \in W} f(\alpha^j x)) \equiv 0 \mod x^{\mu-1}.
\]
The denominator has degree \( ud_{\text{min}} \) and the numerator has degree less than or equal to \((d_{\text{min}}-1)u+v\). This leads directly to the following lemma on the minimum distance.

Theorem 2 (Minimum Distance) Let a \( q \)-ary cyclic code \( C(q^s; n, k, d) \) be given and let \( \alpha \in GF(q^s) \) and \( \alpha^s = 1 \). Let two co-prime polynomials \( h(x) \) and \( f(x) \in GF(q^s)[x] \) with degrees \( v \) and \( u \), respectively and the parameter \( \mu \) be given, such that (17) holds. Then the minimum distance of \( C(q^s; n, k, d) \) satisfies the following inequality:
\[
d \geq df \overset{\text{def}}{=} \left\lfloor \frac{\mu - 1 - v}{u} + 1 \right\rfloor.
\]

Proof: For a codeword \( (c_0, c_1, \ldots, c_{n-1}) \in C(q^s; n, k, d) \) of minimal weight \( d_f \), the degree of the nominator in (16) has degree less than or equal to \((d_f-1)u+v\) and has to be greater than or equal to \( \mu - 1 \).

Similar to the BCH bound, the sequence can have the form \( a_0 c(\alpha^0), a_1 c(\alpha^{b+c_1}), \ldots, a_{u-2} c(\alpha^{b+(\mu-2)c_1}) \). Based on Lemma 2 we require for \( a(b, \alpha^{c_1} x) \) that \( \gcd(n, c_1) = 1 \).

Let us now consider the case where \( \deg h(\alpha^{c_1} x) > 0 \). For \( h(\alpha^{c_1} x) = \sum_{j=0}^v h_j(\alpha^{c_1} x)^j \) we can write the power series expansion of (13) more explicitly:
\[
a(b, \alpha^{c_1} x) = \alpha^{bi} \left( \frac{h_0}{f(\alpha^{c_1} x)} + \frac{h_1 \alpha^{c_1} x}{f(\alpha^{c_1} x)} + \cdots + \frac{h_v(\alpha^{c_1} x)^v}{f(\alpha^{c_1} x)} \right).
\]

Our distance classification works as follows. In the first step, we consider the power series expansion \( 1/f(x) = (\overline{\alpha}_0 + \overline{\alpha}_1 x + \cdots + \overline{\alpha}_{p-1} x^{p-1})/(-x^p + 1) + 1 \) with period \( p = p(1/\alpha^{c_1} x) \).

From (18) we can interpretate \( a(b, \alpha^{c_1} x) \) as linear combination of \( v+1 \) shifted series expansion \( 1/f(\alpha^{c_1} x) \):
\[
h_0(\overline{\alpha}_0, \overline{\alpha}_1, \ldots, \overline{\alpha}_{p-1})
\]
\[
+ h_1(\overline{\alpha}_{p-1}, \overline{\alpha}_0, \ldots, \overline{\alpha}_{p-2})
\]
\[
+ \cdots
\]
\[
+ h_v(\overline{\alpha}_{p-v}, \overline{\alpha}_{p-v+1}, \ldots, \overline{\alpha}_{p-1-v})
\]
\[
(a_0, a_1, \ldots, a_{p-1}).
\]

Then, we choose the parameters \( b \) and \( c_1 \) such that the characteristic sequence of \( a_0 c(\alpha^0), a_1 c(\alpha^{b+c_1}), \ldots, a_{u-2} c(\alpha^{b+(\mu-2)c_1}) \) becomes zero for a codeword \( c(x) \in C(q^s; n, k, d). \)
Example 1 (Binary Cyclic Code) Let us consider the symmetric reversible binary cyclic code $C(2^8; 17, 9, 5)$ with defining set $D_C = \{1, 2, 4, 8, 16, 15, 13, 9\}$ be the set of error positions and let $|E| = t$. Like in (12), we can define the syndrome polynomial $S(x)$:

$$S(x) = \sum_{i=0}^{n-1} r_i \alpha^{i} h(\alpha^{i} x) = \sum_{i \in E} r_i \alpha^{i} h(\alpha^{i} x) \mod x^{\mu-1}. \quad (19)$$

Thus, the explicit form of the syndrome is

$$S(x) = \sum_{j=0}^{\mu-2} a_j r(\alpha^{j+b}) x^j = \sum_{j=0}^{\mu-2} a_j \alpha^{j+b} x^j, \quad (20)$$

which clearly has zero coefficients if $a_j = 0$.

IV. ON THE DISTANCE OF SOME CLASSES OF Q-ARY CODES

A. Structure of Classification and Cardinality

In this section, we classify $q$-ary cyclic codes by subsets of their defining set $D_C$ and their length $n$. We specify our new lower bound of Theorem $[2]$ on the minimum distance of the codes for some classes. 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 over GF$(q)$ with period $p$, where $q = (a_0 a_1 \ldots a_{p-1})$ denotes the coefficients.

- $1/(x^{2} + x + 1)$ over GF$(q)$ with $a = (1\ 1\ 0\ \ldots)$ and $p = 3$;
- $1/(x^{3} + x^{2} + x + 1)$ over GF$(q)$ with $a = (1\ 1\ 0\ \ldots)$ and $p = 4$;
- $1/(x^{3} - x + 1)$ over GF$(2)$ with $a = (1\ 1\ 1\ 0\ 1\ 0\ 0\ \ldots)$ and $p = 7$;
- $1/(x^{4} + x + 1)$ over GF$(2)$ with $a = (1\ 1\ 1\ 0\ 1\ 0\ 1\ 0\ 0\ 0\ 0\ \ldots)$ and $p = 15$.

We match a power series expansion $a(b, \alpha x)$ to the roots of the generator polynomial, such that $a_j \cdot g(a^{j+b+c_1}) = a_j \cdot c(\alpha^{b+j+c_1}) = 0 \forall j = 0, \ldots, \mu - 2$.

Throughout this section, we assume $gcd(n, p) = 1$ and we use Theorem $[2]$ to refine the lower bound $d_f$ on the distance of the codes.

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.

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 $[2, 19]$. A code $C$ is reversible if for any codeword $\mathbf{c} = (c_0 c_1 \ldots c_{n-1}) \in C$ also $\mathbf{c} = (c_{n-1} c_{n-2} \ldots c_0) \in C$ holds. 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.,

$$D_C = \{i_1, i_2, \ldots, i_z, -i_1, -i_2, \ldots, -i_z\}. \quad (21)$$

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. If and only if $n \mid (q^m + 1)$, for some $m \in \mathbb{N}$, then any union of cyclotomic cosets is a defining set of a reversible code.

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 the length $n$ divide $(q^m + 1)$, then the cardinality of the cyclotomic coset $M_r = |M_r| = 2m$ if $gcd(n, r) = 1$.

Proof: Let $\ell$ be the smallest integer such that $n \mid (q^\ell - 1)$. With Lemma $[11]$ we obtain $|M_r| = \ell$ if $gcd(n, r) = 1$. We can factorize $(q^\ell - 1) = (q^{\ell/2} - 1) \cdot (q^{\ell/2} + 1)$. Since $n \nmid (q^{\ell/2} - 1)$ and $n \mid (q^{\ell/2} + 1)$, it follows that $m = \ell/2$. Therefore, $|M_r| = 2m$.

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 $p(a(x)) = 3$.

In the following, we refine our bound for different defining sets. For a binary symmetric reversible code $C$, we showed that each cyclotomic coset is symmetric. Therefore, if $\{1\} \subseteq D_C$, we know that $\{\{4, -2, -1, 0, 1, 2, 4\} \}$ is in the defining set. Let us use the (cyclically shifted) power series expansion $\{1\ 0\ 1\ \ldots\}$. According to Table $[11]$ we have $h(x) = -1 - x$. We match the roots of $C$ for $b = -4$ and $c_1 = 1$, to a zero-sequence of length $\mu - 1 = 9$. Therefore our bound provides $d \geq d_f = 5$.

Let the defining set $D_C$ of the binary symmetric reversible code $C$ additionally include 5. Then we obtain for $b = -6$.
and \( c_1 = 1 \) a sequence of length \( \mu - 1 = 13 \), which results in \( d_f = 7 \).

In the same way, if \( \{1, 5, 7\} \supseteq D_C \), we obtain \( \mu - 1 = 21 \) with \( b = 10 \) and \( c_1 = 1 \) and thus, \( d_f = 11 \). These parameters are shown in Table I and compared with the BCH and HT bounds.

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 \( r \subseteq D_C \), and also \( -r \subseteq D_C \) 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 I 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 \( \ell \) is the smallest integer such that the length \( n \) divides \( q^\ell - 1 \).

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

### Example 2 (Binary Symmetric Reversible Code)

The binary cyclic code \( C[2^3; 17, 9, 5] \) from Example 1 is symmetric reversible since Lemma 2 is fulfilled. If \( \{1\} \subseteq D_C \), then \( D_C = \{1, 2, 4, 8, 16, 15, 13, 9\} \equiv \{1, 2, 4, 8, -1, -2, -4, -8\} \)

mod 17.

The following table illustrates, how we match the roots of the generator polynomial to the zeros of the power series expansion with \( b = -4 \), \( c_1 = 1 \) and \( \mu - 1 = 9 \). In the first row, the defining set is shown, i.e., \( g(\alpha^j) = 0 \) for all \( j \in D_C \). The □ marks elements that are not necessarily roots of the generator polynomial. In the second row of the table, the power series expansion \( a \) is shown for the whole interval.

For all \( j = h, \ldots, b + c_1(\mu - 2) \), we obtain \( a_j \cdot g(\alpha^j) = 0 \).

This is an example for Row 1, Column I of Table I and therefore, \( d_f = 5 \).

In Table II, we list some classes of cyclic codes where the denominator \( f(x) \) of the rational function \( \alpha^h h(\alpha^i x) / f(\alpha^i x) \) has degree three and the period is \( p(1/(x^3 + x^2 + x + 1)) = 4 \). The power series expansion is \( 1/(x^3 + x^2 + x + 1) = (1 – x^2) / (x^3 + x^2 + x + 1) \).

### Table II

<table>
<thead>
<tr>
<th>Binary</th>
<th>Symmetric</th>
<th>Reversible</th>
</tr>
</thead>
<tbody>
<tr>
<td>( {3, 5} \subseteq D_C )</td>
<td>( {3, 5, 11} \subseteq D_C )</td>
<td>( {3, 5, 11, 13} \subseteq D_C )</td>
</tr>
<tr>
<td>( k \geq n - 2\ell )</td>
<td>( k \geq n - 3\ell )</td>
<td>( k \geq n - 4\ell )</td>
</tr>
</tbody>
</table>

### Table I

<table>
<thead>
<tr>
<th>Binary</th>
<th>Symmetric</th>
<th>Reversible</th>
</tr>
</thead>
<tbody>
<tr>
<td>( {1} \subseteq D_C )</td>
<td>( {1, 5} \subseteq D_C )</td>
<td>( {1, 5, 7} \subseteq D_C )</td>
</tr>
<tr>
<td>( k \geq n - \ell )</td>
<td>( k \geq n - 2\ell )</td>
<td>( k \geq n - 3\ell )</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>General</th>
<th>( {\alpha^i} \subseteq D_C )</th>
<th>( {\alpha^i} \subseteq D_C )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( {\alpha^i} \subseteq D_C )</td>
<td>( {\alpha^i} \subseteq D_C )</td>
<td>( {\alpha^i} \subseteq D_C )</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Fractions</th>
<th>( d_f = 5 )</th>
<th>( d_f = 7 )</th>
<th>( d_f = 4 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( b = -4 )</td>
<td>( b = -6 )</td>
<td>( b = -2 )</td>
<td>( b = -9 )</td>
</tr>
<tr>
<td>( c_1 = 1 )</td>
<td>( c_1 = 1 )</td>
<td>( c_1 = 2 )</td>
<td>( c_1 = 2 )</td>
</tr>
</tbody>
</table>

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 \( GF(2)[x] \) has period \( p = 7 \). To obtain a bound on the minimum distance, we consider the case of

\( x/(x^4 + 1) \). Let us consider the second class, where in the case of a binary symmetric reversible code \( \{3, 5, 11\} \) must be in the defining set of the code. The HT bound give the same lower bound on the minimum distance than our approach \( d_{HT} = 5 \).

In Table III all cyclic shifts of the of the power series expansions of \( 1/(x^2 + x + 1) \) and \( 1/(x^3 + x^2 + x + 1) \) are shown. The corresponding numerators \( h(\alpha^i x) \) are given.
extended binary cyclic codes, where the 0 is in the defining set $D_C$. Assume that $\{\overline{-3, 0, 1, 7}\} \subseteq D_C$. The sequence of zeros of the binary code can be matched to the rational function for $b = -4$ and $c_1 = 2$. The corresponding distance is then $d_f \geq 5$. This and some other combinations of subsets of $D_C$ are shown in Table IV.

### Table III

<table>
<thead>
<tr>
<th>$(a_0 \ldots a_{p-1})$</th>
<th>$f(x)$</th>
<th>$h(x)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$(1 - 1 0)$</td>
<td>$1 + x + x^2$</td>
<td>1</td>
</tr>
<tr>
<td>$(-1 0 1)$</td>
<td>$1 + x + x^2$</td>
<td>$-1 - x$</td>
</tr>
<tr>
<td>$(0 1 - 1)$</td>
<td>$1 + x + x^2$</td>
<td>$x$</td>
</tr>
<tr>
<td>$(1 - 1 0)$</td>
<td>$1 + x + x^2 + x^3$</td>
<td>1</td>
</tr>
<tr>
<td>$(0 1 - 1 0)$</td>
<td>$1 + x + x^2 + x^3$</td>
<td>$x$</td>
</tr>
<tr>
<td>$(0 0 1 - 1)$</td>
<td>$1 + x + x^2 + x^3$</td>
<td>$-1 - x - x^2$</td>
</tr>
</tbody>
</table>

### Table IV

<table>
<thead>
<tr>
<th>Binary Codes</th>
<th>${-3, 0, 1, 7}$</th>
<th>${-3, 0, 1, 7, 9}$</th>
<th>${-3, 0, 1, 7, 9, 11}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\subseteq D_C$</td>
<td>$\subseteq D_C$</td>
<td>$\subseteq D_C$</td>
<td></td>
</tr>
<tr>
<td>$k \geq n - 4$</td>
<td>$k \geq n - 5$</td>
<td>$k \geq n - 6$</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>BCH</th>
<th>$d_{BCH} = 4$</th>
<th>$d_{BCH} = 4$</th>
<th>$d_{BCH} = 5$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$b = -3$</td>
<td>$b = -3$</td>
<td>$b = -3$</td>
<td></td>
</tr>
<tr>
<td>$c_1 = 5$</td>
<td>$c_1 = 5$</td>
<td>$c_1 = 5$</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>HT</th>
<th>$d_{HT} = 4$</th>
<th>$d_{HT} = 4$</th>
<th>$d_{HT} = 5$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$b = -3$</td>
<td>$b = -3$</td>
<td>$b = -3$</td>
<td></td>
</tr>
<tr>
<td>$c_1 = 5, c_2 = 0$</td>
<td>$c_1 = 5, c_2 = 0$</td>
<td>$c_1 = 5, c_2 = 0$</td>
<td></td>
</tr>
<tr>
<td>$\mu = 4, \nu = 0$</td>
<td>$\mu = 4, \nu = 0$</td>
<td>$\mu = 5, \nu = 0$</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Fractions</th>
<th>$d_f = 5$</th>
<th>$d_f = 6$</th>
<th>$d_f = 7$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$b = -4$</td>
<td>$b = -4$</td>
<td>$b = -4$</td>
<td></td>
</tr>
<tr>
<td>$c_1 = 1$</td>
<td>$c_1 = 1$</td>
<td>$c_1 = 1$</td>
<td></td>
</tr>
<tr>
<td>$\mu = 14$</td>
<td>$\mu = 16$</td>
<td>$\mu = 19$</td>
<td></td>
</tr>
<tr>
<td>$a = (1 0 0 1 1 1 0)$</td>
<td>$a = (1 0 0 1 1 1 1 0)$</td>
<td>$a = (1 0 0 1 1 1 0)$</td>
<td></td>
</tr>
</tbody>
</table>

Another class of binary cyclic codes can be identified using the polynomial $f(x) = x^4 + x + 1$ with $p(1/x) = 15$. We use the shifted power series expansion such that $a = (1 0 0 1 0 0 0 1 1 1 1 0 1 0 1)$.

As required by Lemma 2, we only consider lengths $n$, such that $\text{gcd}(n, p = 15) = 1$. We can match a concatenation of $a$ to the roots of the generator polynomial for $b = -6$ and $c_1 = 1$ if $\{1, 3, 9, -3\} \subseteq D_C$. Our new bound on the distance yields $d_f \geq 6$, since $\text{deg} f(x) = 4$, whereas the BCH and the HT bound only give $d_{BCH} \geq 5$ and $d_{HT} \geq 5$.

Tables VII VIII IX in the appendix analyze the bounds for all cyclic codes over $\text{GF}(q)$ for $q = 2, 3, 5, 7$ up to length 62. 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 ($\#d_{BCH} < d$), the number of cases, where our bound is better than the BCH bound ($\#d_f > d_{BCH}$) 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 [10], Boston gave ten bounds 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, [10])** The following bounds on the minimum distance of a $q$-ary cyclic codes $C$ hold:

1. If $3 \nmid n$ and $\{0, 1, 3, 4\} \subseteq D_C$, then $d_B \geq 4$.
2. If $\{0, 1, 3, 5\} \subseteq D_C$, then $d_B \geq 4$.
3. If $3 \nmid n$ and $\{0, 1, 3, 4, 6\} \subseteq D_C$, then $d_B \geq 5$.
4. If $4 \nmid n$ and $\{0, 1, 2, 4, 5, 6, 8\} \subseteq D_C$, then $d_B \geq 6$.
5. If $3 \nmid n$ and $\{0, 1, 1, 3, 4, 6, 7\} \subseteq D_C$, then $d_B \geq 6$.
6. If $3 \nmid n$ and $\{0, 1, 3, 4, 6, 7\} \subseteq D_C$, then $d_B \geq 7$.

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 $(a_0 a_1 a_2) = (1 - 1 0)$. The second considered power series expansion $1/(x + 1)$ has period $p = 4$ with $(a_0 a_1 a_2 a_3) = (1 0 -1 0)$. Note that the latter is actually a special case of the BCH bound. Table V shows the six Boston bounds, which can be generalized by our approach. 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

Generalization of Boston’s Bounds

<table>
<thead>
<tr>
<th>Nr.</th>
<th>$\mathcal{I}$</th>
<th>$f(x)$</th>
<th>$a$</th>
<th>$d_f$</th>
<th>Conditions</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>$[-1,5]$</td>
<td>$x^2 + x + 1$</td>
<td>$(0 1 -1\ldots)$</td>
<td>4</td>
<td>$\text{gcd}(n, 3) = 1$</td>
</tr>
<tr>
<td>2</td>
<td>$[0,6]$</td>
<td>$x^2 + 1$</td>
<td>$(0 1 0 -1\ldots)$</td>
<td>4</td>
<td>$\text{gcd}(n, 2) = 1$</td>
</tr>
<tr>
<td>5</td>
<td>$[-1,6]$</td>
<td>$x^2 + x + 1$</td>
<td>$(0 1 -1\ldots)$</td>
<td>5</td>
<td>$\text{gcd}(n, 3) = 1$</td>
</tr>
<tr>
<td>6</td>
<td>$[-1,8]$</td>
<td>$x^2 + 1$</td>
<td>$(0 1 0 -1\ldots)$</td>
<td>6</td>
<td>$\text{gcd}(n, 2) = 1$</td>
</tr>
<tr>
<td>7</td>
<td>$[-1,8]$</td>
<td>$x^2 + x + 1$</td>
<td>$(0 1 -1\ldots)$</td>
<td>6</td>
<td>$\text{gcd}(n, 3) = 1$</td>
</tr>
<tr>
<td>10</td>
<td>$[-1,9]$</td>
<td>$x^2 + x + 1$</td>
<td>$(0 1 -1\ldots)$</td>
<td>6</td>
<td>$\text{gcd}(n, 3) = 1$</td>
</tr>
</tbody>
</table>

Moreover, Boston raised the following question [10]:

**Question 1 (Boston’s Question, [10])** Let $3 \nmid n$ and the set $\mathcal{T} = \{0, 1, 3, 4, 6, 7, 9, 10, \ldots\} \subseteq D_C$. Is the minimum distance then $d_B \geq |\mathcal{T}|$?

Counter-examples show that Boston’s conjecture is not true (see Example 3), since the actual distance of such codes is not always $d_B \geq r + 1$. However, using the power series expansion of $1/(x^2 + x + 1)$ with $a = (0 1 -1\ldots)$ we obtain $\mu - 1 = r + 2$. The minimum distance of such codes can be
bounded by $d_f \geq \lceil (r + 1)/2 + 1 \rceil$ with $u = \deg f(x) = 2$ and $v = h(x) = 1$.

**Example 3 (Distance of the $C(3^4; 20, 6, 8)$ code)** Let $D_C = \{0, 1, 2, 3, 4, 6, 7, 8, 9, 10, 12, 14, 16, 18\}$. For Boston’s scheme, we can use $T = \{0, 1, 3, 4, 6, 7, 9, 10, 12\}$ where $|T| = 9$. The actual distance is $d = 8$ and therefore, Boston’s conjecture is not true. The BCH bound yields $d_{BCH} \geq 6$. Our new bound is tight and with $r = 12$, we obtain $d_f \geq [(r + 1)/2 + 1] = 8$.

**VI. Generalized Key Equation and Decoding Algorithm**

Based on the relation between the rational function $h(\alpha^x)/f(\alpha^x)$ and the codewords of a $q$-ary cyclic code $C(q^n; n, k, d)$ as shown in [15] in Section [VI], we introduce a generalized error-locator polynomial $\Lambda(x)$ and error-evaluator polynomial $\Omega(x)$ and set it in relation to the syndrome definition of [19]. Let $E$ denote the set of error positions and let $t = |E|$. We define $\Lambda(x)$ as:

$$\Lambda(x) \equiv \prod_{i \in E} f(\alpha^i). \quad (22)$$

Let

$$\Omega(x) \equiv \sum_{i \in E} \left( e_i \cdot \alpha^i \cdot h(\alpha^i) \cdot \prod_{j \in E, j \neq i} f(\alpha^j) \right), \quad (23)$$

and we obtain with [19] a so-called generalized key equation:

$$\Lambda(x) \cdot S(x) \equiv \Omega(x) \mod x^{\mu - 1}, \quad (24)$$

where $\deg \Omega(x) \leq (t - 1)u + v < \deg \Lambda(x) = tu$, 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 (20). If

$$t = |E| \leq \frac{d_f - 1}{2}, \quad (25)$$

there is a unique solution of the key equation (24) with $\deg \Omega(x) \leq (t - 1)u + v < \deg \Lambda(x) = tu$. We can find this solution by the Extended Euclidean Algorithm with the input polynomials $x^{\mu - 1}$ and $S(x)$.

**Proof:** The key equation (24) can be written as a linear system of equations, with the $t \cdot u + 1$ coefficients of $\Lambda(x)$ as unknowns. If we consider only the equations which do not depend on $\Omega(x)$, we obtain:

$$\begin{pmatrix} S_{tu} & S_{tu-1} & \cdots & S_0 \\ S_{tu+1} & S_{tu} & \cdots & S_1 \\ \vdots \\ S_{\mu-2} & S_{\mu-3} & \cdots & S_{\mu-tu-2} \end{pmatrix} \begin{pmatrix} \Lambda_0 \\ \Lambda_1 \\ \vdots \\ \Lambda_{tu} \end{pmatrix} = \mathbf{0}. \quad (26)$$

There is a unique solution of this linear system of equations if and only if the number of linearly independent equations is greater than or equal to the number of unknowns. One coefficient of $\Lambda(x)$ can be chosen arbitrarily, since a scalar factor does not change the roots. Therefore, we have $\deg \Lambda(x) = tu$ unknowns and $\mu - 1 - \deg \Lambda(x) = \mu - 1 - tu$ equations. For a unique solution, the following has to be fulfilled:

$$tu \leq \mu - 1 - tu \iff \frac{\mu - 1}{2} \leq \frac{(d_f - 1)u + v}{2u} \leq \frac{(d_f - 1)}{2},$$

where we used that $(d_f - 1) \cdot u + v \geq \mu - 1$ from Theorem 2.

As for classical decoding, the system of equations from (20) has a Hankel form and therefore can be solved with the EEA (compare [20]). For this, the EEA has as input polynomials $x^{\mu - 1}$ and $S(x)$ and stop as soon as for the remainder $\deg r_1(x) \leq [(\mu - 1)/2]$ holds. Then, we obtain $\Lambda(x)$ and $\Omega(x)$.

If we have found $\Lambda(x)$, we can determine its factors $f(\alpha^x)$, where $i \in E$. These factors are disjoint since $\deg(\gcd(f(\alpha^x), f(\alpha^x))) = 0$, $\forall i \neq j$ and therefore these factors provide the error positions. We calculate only one root $\beta_i$ of each $f(\alpha^x)$ in a preprocessing step. To find the error positions if $\Lambda(x)$ is given, we do a Chien search with $\beta_0, \beta_1, \ldots, \beta_{\mu - 1}$. This is shown in Algorithm 1 and Theorem 4 proves that each $\beta_i$ uniquely determines $f(\alpha^x)$.

For the non-binary case, we have to calculate the error values at the error positions. This can be done by a generalized Forney formula [18]. In order to obtain this error evaluation formula, we use the explicit expression for $\Omega(x)$ from (23). As mentioned before, the preprocessing step calculates $n$ values $\beta_0, \beta_1, \ldots, \beta_{\mu - 1}$ such that

$$f(\alpha^i \beta_i) = 0, \forall i = 0, \ldots, n - 1, \text{ and } f(\alpha^j \beta_i) \neq 0 \quad \forall j \neq i.$$
Proof: The lemma follows from (27) and the fact that
\[ \Lambda'(x) = \sum_{i \in \mathcal{E}} f'(\alpha^i x) \prod_{j \in \mathcal{E}, j \neq i} f(\alpha^j x) \]
and therefore
\[ \Lambda'(\beta_\ell) = f'(\alpha^\ell \beta_\ell) \prod_{j \in \mathcal{E}, j \neq \ell} f(\alpha^j \beta_\ell). \]

Note that (28) is the classical Forney formula, for \( f(\alpha^i x) = 1 - \alpha^i x \) and \( \alpha^{ib_i} \cdot h(\alpha^i x) = 1 \).

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

**Algorithm 1: Decoding \( q \)-ary Cyclic Codes**

**Input:** Received word \( r(x), f(\alpha^x) \), \( \alpha^{ib_i} \cdot h(\alpha^x) \)

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

1. Calculate \( S(x) \) by (20).
2. Solve Key Equation: Obtain \( \Lambda(x), \Omega(x) \) as output of EEA \((x^\mu - 1, S(x))\)
3. Chien–Search: Find all \( i \) for which \( \Lambda(\beta_i) = 0 \), save them as \( \mathcal{E} = \{\alpha_0, \alpha_1, \ldots, \alpha_i\} \)
4. Error Evaluation:
\[ \hat{e}_i = \Omega(\beta_i) / h(\alpha^i \beta_i) \prod_{j \in \mathcal{E}, j \neq \ell} f(\alpha^j \beta_\ell), \]
for all \( \ell \in \mathcal{E} \)
5. \( \hat{e}(x) = \sum_{i \in \mathcal{E}} \hat{e}_i \alpha^i \)
6. \( \hat{c}(x) = r(x) - \hat{e}(x) \)

**Output:** Estimated codeword \( \hat{c}(x) \)

**Theorem 4 (Correctness of Algorithm 4)** 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 4 returns \( \hat{c}(x) = c(x) \) with complexity \( \mathcal{O}(\deg f(x) \cdot n^2) \) operations.

**Proof:** Let \( S(x) \) be defined by (20). 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 4 and also \( \Omega(x) = \Lambda(x) \cdot S(x) \mod x^{\mu - 1} \). To explain the preprocessing and the Chien–search, we note that for each polynomial \( a(x) \) of degree \( u \) defined over GF\( (q^\mu) \) there exists a splitting field, i.e., an extension field GF\( (q^\nu) \) of GF\( (q^\mu) \), in which \( a(x) \) has \( u \) roots. Therefore, each \( f(\alpha^x) \) can be decomposed into \( u = \deg f(\alpha^x) \) linear factors over a field GF\( (q^\mu) \). These factors are disjoint since \( \deg(\gcd(f(\alpha^x), f(\alpha^x))) = 0 \) and hence, one root of \( f(\alpha^x) \) uniquely defines \( f(\alpha^x) \) and \( i \). Hence, \( \Lambda(\beta_i) \) = 0 if and only if \( i \in \mathcal{E} \) 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 4 returns \( \hat{c}(x) = c(x) \).

To prove the complexity, we note that the input polynomials \( S(x) \) and \( x^{\mu - 1} \) of the EEA have degrees \( \mu - 1 \) and \( \mu - 2 \). Therefore, the complexity of the EEA is quadratic in \( \mu \), 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 4 by \( \mathcal{O}((u \cdot n)^2) = \mathcal{O}((\deg f(x) \cdot n)^2) \).

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

**Example 4 (Binary Cyclic Code with \( n = 2^4 + 1 = C(2^8; 17, 9, 5) \)**

We consider again the \( C(2^5; 17, 9, 5) \) code and we have with \( b = -4 \equiv 13 \mod 17 \):

\[
\alpha^{13i} \cdot h(\alpha^{ix}) = \frac{\alpha^{13i} + \alpha^{14i} x}{1 + \alpha^{ix} + \alpha^{ix^2}} = \frac{\alpha^{13i} + \alpha^{15i} x^2 + \alpha^{16i} x^3 + \alpha^{17i} x^4 + \alpha^{18i} x^5 + \alpha^{19i} x^6 + \alpha^{20i} x^7 + \alpha^{21i} x^8 + \alpha^{22i} x^9}{\alpha^{23i} + \alpha^{24i} x^2 + \alpha^{25i} x^3 + \alpha^{26i} x^4 + \alpha^{27i} x^5 + \alpha^{28i} x^6 + \alpha^{29i} x^7 + \alpha^{30i} x^8 + \alpha^{31i} x^9}
\]

and \( d_f = d \).

For the syndrome polynomial, we obtain with \( \mu = 1 = 9 \) and (19), (20) and (29).

\[
S(x) = \sum_{i=0}^{n-1} e_i \cdot (\alpha^{13i} + \alpha^{15i} x^2 + \cdots + \alpha^{4i} x^8)
\]

As in Algorithm 7 we calculate 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 \( \Lambda(x) \):

\[
\begin{pmatrix}
1 \\
S_3 & S_2 & 0 & S_0 \\
S_5 & S_2 & 0 & S_0 \\
S_6 & S_5 & 0 & S_3 \\
S_0 & S_5 & 0 & S_3 \\
\end{pmatrix}
\begin{pmatrix}
A_1 \\
A_2 \\
A_3 \\
A_4 \\
\end{pmatrix}
= 0.
\]

and with both approaches, \( \Lambda(x) \) has the roots \( f(\alpha^i x) = (1 + \alpha^{ix} + \alpha^{ix^2}) \), \( \forall i \in \mathcal{E} \). We know that each \( f(\alpha^i x) = (1 + \alpha^{ix} + \alpha^{ix^2}) \) has two roots in GF\( (2^9) \) which are unique. We have a look-up-table with one root \( \beta_i \) 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 (e.g. BCH, Hartmann–Tzeng and Boston) is shown.

Furthermore, a generalized key equation, relating the syndrome definition and the polynomial for the determination of the error locations is given. This allows the realization of a quadratic-time decoding algorithm and provides an explicit expression for the error evaluation.
VIII. ACKNOWLEDGEMENT

REFERENCES


