HAL
archives-ouvertes.fr

Efficient decoding of some classes of binary cyclic codes beyond the Hartmann-Tzeng bound

Alexander Zeh, Antonia Wachter, Sergey Bezzateev

▶ **To cite this version:**

Alexander Zeh, Antonia Wachter, Sergey Bezzateev. Efficient decoding of some classes of binary cyclic codes beyond the Hartmann-Tzeng bound. Bruce Hajek and Simon Litsyn and Boris Ryabko. IEEE International Symposium on Information Theory (ISIT), Jul 2011, St. Petersburg, Russia. IEEE, pp.1017-1021, 2011, <10.1109/ISIT.2011.6033683>. <hal-00647590>

HAL Id: hal-00647590
https://hal.inria.fr/hal-00647590

Submitted on 2 Dec 2011

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Efficient Decoding of Some Classes of Binary Cyclic Codes Beyond the Hartmann–Tzeng Bound

Alexander Zeh and Antonia Wachter
Institute of Telecommunications
and Applied Information Theory
Ulm University, Germany
{alexander.zeh, antonia.wachter}@uni-ulm.de

Sergey Bezzateev
Saint Petersburg State University
of Airspace Instrumentation
St. Petersburg, Russia
bsv@aanet.ru

***Abstract*—A new bound on the distance of binary cyclic codes is proposed. The approach is based on the representation of a subset of the roots of the generator polynomial by a rational function. A new bound on the minimum distance is proven and several classes of binary cyclic codes are identified. For some classes of codes, this bound is better than the known bounds (e.g. BCH or Hartmann–Tzeng bound).**

Furthermore, a quadratic–time decoding algorithm up to this new bound is developed.

***Index Terms*—Binary Cyclic Code, Binary BCH Code, Bound on the Minimum Distance, Efficient Decoding**

I. Introduction

Classical decoding algorithms for binary cyclic codes like the Extended Euclidean Algorithm (EEA, [1]) or the Berlekamp–Massey Algorithm (BMA, [2], [3]) up to the BCH bound [4], [5] use the longest set of consecutive roots of the generator polynomial. Other lower bounds on the minimum distance of cyclic codes are the Hartmann–Tzeng [6]–[8] and the Roos [9], [10] bound, where multiple sets of roots are considered. Feng and Tzeng [11], [12] have shown an extended syndrome matrix for binary cyclic codes up to a length of 63, which allows decoding up to the *actual* distance of the code. However, they fit the available syndromes manually into this structure.

In this contribution, we consider a more general approach. We match a sequence of roots of the generator polynomial of a binary cyclic code to a power series expansion of a rational function. We prove a general new lower bound on the minimum distance for several classes of binary cyclic codes, which are classified by means of their lengths and their defining sets. Furthermore, we propose an efficient decoding algorithm for these classes based on the EEA and a modified Chien search [13].

This contribution is structured as follows. In Section II, we recall some basic definitions for binary cyclic codes. Our new approach is presented in Section III, where the basic principle is explained and the main theorem is proven. Several classes of binary cyclic codes are identified in Section IV. Based on the description of the code by a rational function, a generalized key equation is formulated and a new decoding method is developed in Section V. We carry out a complexity analysis and conclude our work in Section VI.

This work has been supported by DFG, Germany, under grants BO 867/22-1 and BO 867/21-1.

II. Binary Cyclic Codes Revisited

A binary cyclic code of length n, dimension k and distance d is denoted by $\mathcal{C}(2^s; n, k, d)$ and its generator polynomial $g(x)$ has roots in the splitting field $\mathbb{GF}(2^s)$, where $n \mid (2^s-1)$. A cyclotomic coset M_r is given by:

$$M_r = \{r2^j \bmod n \,|\, j = 0, 1, \ldots, n_r - 1\}, \tag{1}$$

where n_r is the smallest integer such that $r2^{n_r} \equiv r \mod n$. Let α be a nth root of unity of $\mathbb{GF}(2^s)$. It is well–known that the minimal polynomial 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 binary cyclic code $\mathcal{C}(2^s; n, k, d)$ is the set of zeros of the generator polynomial $g(x)$ and can be partitioned into w cyclotomic cosets:

$$\begin{aligned} D_\mathcal{C} &= \{0 \le i \le n-1 \,|\, g(\alpha^i) = 0\} \\ &= M_{r_1} \cup M_{r_2} \cup \cdots \cup M_{r_w}. \end{aligned} \tag{3}$$

Hence, the generator polynomial $g(x)$ of degree $n - k$ of $\mathcal{C}(2^s; n, k, d)$ is

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

We give the Hartmann–Tzeng (HT) bound in the following theorem. It was generalized by Roos [9], [10].

Theorem 1 (HT Bound, [6]–[8]) *Let $\mathcal{C}(2^s; n, k, d)$ be a binary cyclic code with defining set $D_\mathcal{C}$. Let*

$$\{b + i_1 c_1 + i_2 c_2 \,|\, 0 \le i_1 \le \mu - 2,\ 0 \le i_2 \le \nu\} \subseteq D_\mathcal{C}, \tag{5}$$

where $\gcd(n, c_1) = 1$, $\gcd(n, c_2) = 1$. Then $d \ge \mu + \nu$.

Note that for $c_2 = 0$ the HT bound becomes the BCH bound [4], [5]. Let $c(x)$ be a codeword of the $\mathcal{C}(2^m; n, k, d)$ code with generator polynomial $g(x)$, where $g(\alpha^i) = 0$, $\forall i \in D_\mathcal{C}$. Let the received polynomial be $r(x) = c(x) + e(x)$,

where the set $\mathcal{E} \subseteq \{0, \ldots, n-1\}$, $|\mathcal{E}| = t$ denotes the error positions. The syndrome term can then be calculated by:

$$S_i = e(\alpha^i) = r(\alpha^i), \qquad \forall i \in D_{\mathcal{C}}. \tag{6}$$

For binary extension fields, $S_{2i} = (S_i)^2$. Furthermore, we have $S_{n+i} = S_i$.

III. Description of Binary Cyclic Codes by Rational Functions

Binary cyclic codes can be described by means of rational functions as in [14]. We define a certain fraction $\alpha^{bi} h(\alpha^i x)/f(\alpha^i x)$, where $h(x),\ f(x) \in \mathbb{GF}(2)[x]$ and

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

Furthermore, let $\gcd(h(x), f(x)) = 1$ and $f(x) = 1 + f_1 x + \ldots + f_{u-1} x^{u-1} + f_u x^u$. The fraction $\alpha^{bi} h(\alpha^i x)/f(\alpha^i x)$ can be represented as semi–infinite power series expansion $a(b, \alpha^i x)$:

$$\begin{aligned} a(b, \alpha^i x) = \frac{\alpha^{bi} h(\alpha^i x)}{f(\alpha^i x)} &= \sum_{j=0}^{\infty} a_j \alpha^{bi} (\alpha^i x)^j \\ &= \alpha^{bi} a_0 + a_1 \alpha^{bi} \alpha^{ij} x + a_2 \alpha^{bi} (\alpha^{ij} x)^2 + \ldots. \end{aligned} \tag{7}$$

Let $p(a(b, \alpha^i x)) = p$ denote the period of a semi-infinite sequence. Then, we can rewrite (7) by:

$$a(b, \alpha^i x) = \frac{\alpha^{bi} \sum_{j=0}^{p-1} a_j x^j}{x^p - 1} \tag{8}$$

We associate the codeword $c(x)$ of a binary cyclic code with the power series of the rational function $h(\alpha^i x)/f(\alpha^i x)$:

$$\begin{aligned} \sum_{j=0}^{\infty} a_j c(\alpha^{j+b}) x^j &= \sum_{j=0}^{\infty} \sum_{i=0}^{n-1} a_j c_i \alpha^{i(j+b)} x^j \\ &= \sum_{i=0}^{n-1} c_i \Big(\sum_{j=0}^{\infty} a_j \alpha^{i(j+b)} x^j \Big) \\ &= \sum_{i=0}^{n-1} c_i \frac{\alpha^{ib} h(\alpha^i x)}{f(\alpha^i x)} \\ &\equiv 0 \bmod x^{\mu-1}, \end{aligned} \tag{9}$$

such that μ is maximized.

For a given binary cyclic code with generator polynomial $g(x)$, we know that $g(\alpha^i) = 0,\ \forall i \in D_{\mathcal{C}}$ and therefore $c(\alpha^i) = 0$. We associate a rational function $\alpha^{bi} h(\alpha^i x)/f(\alpha^i x)$ with the code such that for each codeword $\mathbf{c} = (c_0\ c_1\ \ldots\ c_{n-1})$ the following holds for some integer μ [14]:

$$\sum_{i=0}^{n-1} c_i \frac{\alpha^{bi} h(\alpha^i x)}{f(\alpha^i x)} \equiv 0 \mod x^{\mu-1}, \tag{10}$$

where $\gcd(f(\alpha^i x), f(\alpha^j x)) = 1$ for all $i \neq j$ and with $c(\alpha^{j+b}) a_{j+b} = 0$ for all $j = 0, \ldots, \mu - 2$. The value of μ should be maximized to increase the lower bound on the distance d_f and therefore the number of errors which can be corrected with our approach (see Section V). Before we state the connection between μ and the minimum distance d of the binary cyclic code, let us give an example.

Example 1 (BCH Code with $n = 2^4 + 1$, $\mathcal{C}(2^8; 17, 9, 5)$) *For $f(x) = 1 + x + x^2$, we have $p(1/f(x)) = 3$ and $(a_0\ a_1\ a_2) = (1\ 1\ 0)$. The defining set $D_{\mathcal{C}}$ of the $\mathcal{C}(2^8; 17, 9, 5)$ code consists of: $D_{\mathcal{C}} = \{1, 2, 4, 8, 16, 15, 13, 9\} \equiv \{1, 2, 4, 8, -1, -2, -4, -8\} \mod 17$. Note that $D_{\mathcal{C}} = M_1$. We associate the elements of the defining set $D_{\mathcal{C}}$ with the sequence of non-zero coefficients of the fraction $h(\alpha^i x)/f(\alpha^i x)$ of length $\mu - 1 = 9$ starting from -4 up to $+4$, where the shift of $(a_0\ a_1\ a_2)$ is done by $h(\alpha^i x)$ (see Table I). In fact we obtain $h(\alpha^i x) = \alpha^{13i} + \alpha^{14i} x$.*

In order to prove our bound and apply our decoding approach (see Section V), $\gcd(f(\alpha^i x), f(\alpha^j x)) = 1$ has to be fulfilled for all $i \neq j$. This gives the following restriction on the period $p(1/f(x))$ of the rational function $1/f(x)$.

Lemma 1 (Period of the Rational Function) *Let $p = p(h(x)/f(x))$ denote the period of the rational function as defined in (7), where $\gcd(h(x), f(x)) = 1$. If and only if $\gcd(p, n) = 1$, where $n | (2^s - 1)$, then $\gcd(f(\alpha^i x), f(\alpha^j x)) = 1,\ \forall i \neq j$.*

Proof: From (8) we have

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

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

$$\begin{aligned} x^p \alpha^{ip} - 1 &\equiv 0 \mod f(\alpha^i x) \quad \text{and} \\ x^p \alpha^{jp} - 1 &\equiv 0 \mod f(\alpha^j x). \end{aligned} \tag{11}$$

Assume there is some element $\beta \in \mathbb{GF}(2^{us}) \setminus \{0\}$, such that

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

Equation (11) gives the following:

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

Therefore, $\alpha^{ip} \beta^p = \alpha^{jp} \beta^p$, and we obtain $\alpha^{ip} = \alpha^{jp}$, hence, $\alpha^{(i-j)p} = 1$. For $i \neq j$, this is true if and only if $p = p(h(x)/f(x))$ divides n. Hence, if and only if $\gcd(p, n) = 1$, $\gcd(f(\alpha^i x), f(\alpha^j x)) = 1,\ \forall i \neq j$. ∎

The minimum distance of a $\mathcal{C}(2^s; n, k, d)$ code that can be described by such a rational function $\alpha^{bi} h(x\alpha^i)/f(x\alpha^i)$ is given by the following lemma.

Lemma 2 (Minimum Distance, [14]) *The minimum distance d of a binary cyclic $\mathcal{C}(2^s; n, k, d)$ code defined by* (10) *satisfies the following inequality:*

$$d \geq d_f = \left\lceil \frac{\mu - 1 - v}{u} + 1 \right\rceil. \tag{12}$$

Proof: Let us consider a codeword of minimal weight d_f, then the sum in (10) consists only of d_f fractions. By definition $\gcd(f(\alpha^i x), f(\alpha^j x)) = 1$ for all i, j, hence, the least common denominator is the product of the d_f denominators. Each numerator of the d_f fractions is therefore multiplied by the

other (d_f-1) denominators. Hence, the degree of the resulting numerator is $(d_f-1)\cdot u+v$.

Since the numerator is non-zero, (10) is fulfilled if and only if the degree of the numerator is greater than or equal to $\mu-1$. We obtain $(d_f-1)\cdot u+v \geq \mu-1$ and the statement (12) follows. ∎

IV. Identified Classes of Binary Cyclic Codes

A. Structure of Classification

In this section, we classify binary cyclic codes by subsets of their defining set $D_{\mathcal{C}}$ and their length n. We use three rational functions $1/f(x)$, where the corresponding $f(x) \in \mathbb{GF}(2)[x]$ has degree two, three and four (see the following subsections). In the first row of Tables I,II and V, the necessary roots of the generator polynomial are listed by the corresponding exponent i, such that $g(\alpha^i)=0$. The $\square$ marks elements that are not necessarily roots of the generator polynomial. In the second row of the tables, the sequence $(a_0\ a_1 \dots a_{p-1})$ is arranged consecutively such that it fits to the roots of the generator polynomial.

The interval $\mathcal{I}$ marks start and end of the sequence of roots and non–roots of the binary code that fits to the sequence generated by $\alpha^{bi} f(\alpha^i x)/h(\alpha^i x)$. This characteristic sequence is then used for the decoding procedure in Section V.

Throughout this section, we assume due to Lemma 1 that $\gcd(n, p(1/f(x)))=1$ and we use (12) to give a lower bound d_f on the distance d of the codes. We compare our new bound with the BCH bound [4], [5] and the Hartmann–Tzeng bound [6]–[8], which we denote by d_{BCH} and d_{HT}.

B. Denominator of Degree Two

We consider the rational function $1/f(x)$ with $f(x)=x^2+x+1$, where $(a_0\ a_1\ a_2)=(1\ 1\ 0)$ and $p(1/f(x))=3$. The sequence is shown in Table I.

Let us consider the case of a binary cyclic code with length $n=2^m+\Delta$, where $3 \nmid n$. The cases, where Δ equals 1 or -1 will be analyzed in detail later. The cyclotomic cosets M_1 and M_Δ in ascending order of the exponents are:

$$M_1 = \{1, 2, 4, \dots, 2^m = -\Delta, -2\Delta \dots\} \quad (13)$$

$$M_\Delta = \{\Delta \equiv -2^m, 2\Delta, 4\Delta, \dots, -1, -2, \dots, -2^{m-1}\} \quad (14)$$

If $\{1,-1\} \supseteq D_{\mathcal{C}}$, we always achieve $\mu-1=9$ using $\mathcal{I}=[-4,4]$ from Table I.

Let the defining set $D_{\mathcal{C}}$ of the code with length $n=2^m+\Delta$ additionally include 5 and -5. The sequence in the interval $\mathcal{I}=[-6,6]$ has $\mu-1=13$ with Table I, which results in $d_f=7$.

Let us investigate the case $n=2^m+1$ more in detail. The parameters of this class of binary cyclic codes are summarized in Table III. The cyclotomic coset M_i for $\gcd(i,n)=1$ consists the following elements:

$$M_i = \{i, i2, \dots, i2^m \equiv -i, -i2, \dots, -i2^{m-1}\}.$$

Lemma 3 *If $n=2^m+1$ and $\gcd(n,i)=1$, then the cardinality of the coset M_i is $|M_i|=2m$.*

Proof: Clearly, the following holds:

$$i2^{2m} \equiv i(2^m)^2 \equiv i(-1)^2 \equiv i \mod n.$$

Hence, $|M_i|$ is *at most* $2m$. Now, assume there exists a $j<2m$, such that $i2^j \equiv i \mod n$. For some $\xi \in \mathbb{N}$, this is equivalent to $i(2^j-1)=\xi(2^m+1)$. This is never satisfied for $j<2m$ and $\gcd(2^m+1,i)=1$ and therefore $|M_i|=2m$. ∎

For this special case, where $\Delta=1$, i.e., for the length $n=2^m+1$, we can reduce the necessary elements in the defining sets as shown in Table III.

TABLE III
Cyclic Codes of length $n=2^m+1$ and $\gcd(n,3)=1$, using $f(x)=x^2+x+1$

$\supseteq D_{\mathcal{C}}$	$\mathcal{I}=$	$k\geq$	d_{BCH}	d_{HT}	d_f
$\{1\}$	$[-4,4]$	$n-2m$	4	5	5
$\{1,5\}$	$[-6,6]$	$n-4m$	5	6	7
$\{1,5,7\}$	$[-10,10]$	$n-6m$	8	9	11

We can generalize this lower bound on the minimum distance to the case of a binary cyclic code of length $n=a(2^m+1)$ and $\gcd(n,3)=1$.

Lemma 4 *If $n=a(2^m+1)$ then the cardinality of the coset M_a is $|M_a|=2m$.*

Proof: Similarly as in Lemma 3,

$$i2^{2m} \equiv i(2^m)^2 \equiv i(-1)^2 \equiv i \mod n$$

and assume there exists $j<2m$, such that $a2^j \equiv a \mod n$. Then, for some $\xi \in \mathbb{N}$: $(2^j-1)=\xi(2^m+1)$. This is not satisfied for $j<2m$ and therefore $|M_a|=2m$. ∎

Analogously to $a=1$, new lower bounds on d based on the subsets of $D_{\mathcal{C}}$ can be given.

Example 2 (Cyclic Code $\mathcal{C}(2^8; 85, 69, d_f=7)$) *Let $a=5$ and $m=4$, then $n=5(2^4+1)=85$ and let $\{5,25\} \subseteq D_{\mathcal{C}}$. Then $k=n-|M_5|-|M_{25}|=n-2(2m)=69$.*

In the following, we analyze the case $n=2^m-1$ and $\gcd(n,3)=1$. Let us again distinguish several cases with different subsets of the defining set. An overview of the parameters of the different cases is given in Table IV.

We obtain a lower bound on the dimension of the code by calculating the cardinality of the cosets.

Lemma 5 *If $n=2^m-1$ and $\gcd(n,i)=1$, then the cardinality of the coset M_i is $|M_i|=m$.*

Proof: For this length, $i2^m \equiv i \mod n$, hence, $|M_i| \leq m$. Assume, there exist a $j<m$, such that $i2^j \equiv i \mod n$, i.e., $i(2^j-1)=\xi(2^m-1)$, where $\xi \in \mathbb{N}$. Since $(2^m-1)=(2^{m/2}-1)\cdot(2^{m/2}+1)$, this would be fulfilled for $j=m/2$, but then $i=\xi\cdot(2^{m/2}+1)$ and $\gcd(i,n)\neq 1$. Hence, this is not

TABLE I
NECESSARY ROOTS IN THE DEFINING SET OF A CYCLIC CODE AND POWER SERIES $1/(x^2+x+1)$.

$\subseteq D_{\mathcal{C}}$	$\cdots$	□	-10	□	-8	-7	□	-5	-4	□	-2	-1	□	1	2	□	4	5	□	7	8	□	10	□	$\cdots$
$1/(x^2+x+1)$	$\cdots$	1	-1	0	1	-1	0	1	-1	0	1	-1	0	1	-1	0	1	-1	0	1	-1	0	1	-1	$\cdots$

satisfied for any $j < m$ and $\gcd(i,n) = 1$ and the cardinality of the coset M_i is m. ∎

Hence, $M_i = \{i, i2, \ldots, i2^{m-1}\}$, for all i where $\gcd(n,i) = 1$.

We can rewrite the length by $n = 2^m - 1 = 2^{m-1} + 2^{m-1} - 1 = 2^{m-1} + \Delta$. With (14), we know that $M_{-1} = M_{\Delta} = M_{2^{m-1}-1}$. If we use $\{1,-1\} \supseteq D_{\mathcal{C}}$, we always achieve $\mu - 1 = 9$ using $\mathcal{I} = [-4,4]$ from Table I. This yields $d_f = 5$.

Since $2^3(2^{m-2} + 2^{m-3} - 1) = 3 \cdot 2^m - 2^3 \equiv 3 - 8 \equiv -5 \mod n$, we know that $M_{-5} = M_{2^{m-2}+2^{m-3}-1}$. Let us use $\{1,5,-1,-5\} \supseteq D_{\mathcal{C}}$ and $\mathcal{I} = [-6,6]$. We obtain $\mu - 1 = 13$ with Table I, which results in $d_f = 7$.

Assume, that $\{1,5,7,-1,-5,-7\} \supseteq D_{\mathcal{C}}$ and $\mathcal{I} = [-10,10]$. Thereby, $-7 \equiv 2^m - 8 \equiv 2^3(2^{m-3} - 1)$, i.e., $M_{-7} = M_{2^{m-3}-1}$. Table I provides a sequence of length $\mu - 1 = 21$ and thus, $d_f = 11$.

TABLE IV
CYCLIC CODES OF LENGTH $n = 2^m - 1$ AND $\gcd(n,3) = 1$, USING $f(x) = x^2 + x + 1$

$\supseteq D_{\mathcal{C}}$	$\mathcal{I} =$	$k \geq$	d_{BCH}	d_{HT}	d_f
$\{1,-1\}$	$[-4,4]$	$n-2m$	4	5	5
$\{1,5,-1,-5\}$	$[-6,6]$	$n-4m$	5	6	7
$\{1,5,7,-1,-5,-7\}$	$[-10,10]$	$n-6m$	8	9	11

C. Denominator of Degree Three

For $f(x) = x^3 + x + 1$, we obtain $p(1/f(x)) = 7$. For $b = 0$ and $h(x) = 1$, we have $(a_0\ a_1 \ldots a_6) = (1\ 1\ 1\ 0\ 1\ 0\ 0)$ and the necessary roots of the generator polynomial of the code are shown in Table II. Let us consider the case of extended cyclic codes, where the 0 is in the defining set $D_{\mathcal{C}}$. Assume that $\{0,1,-3,7\} \supseteq D_{\mathcal{C}}$. In the interval $\mathcal{I} = [-4,8]$, the sequence of zeros can be matched to the rational function. The corresponding distance is then $d_f = 5$. Some other combinations of subsets of the defining set $D_{\mathcal{C}}$ and the corresponding distances are shown in Table VI.

As a special case, we consider $n = 2^m + 3$, where -3 is in cyclotomic coset M_1. We have $d_f = 5$ for $\{0,1,7\} \supseteq D_{\mathcal{C}}$ and $n = 2^m + 3$.

D. Denominator of Degree Four

Let $f(x) = x^4 + x + 1$, then $p(1/f(x)) = 15$. The characteristic sequence $(a_0\ a_1 \ldots a_{14})$ for $b = 0$ and $h(x) = 1$ is illustrated in Table V.

TABLE VI
CYCLIC CODES OF LENGTH n, $\gcd(n,7) = 1$, USING $f(x) = x^3 + x + 1$

$\supseteq D_{\mathcal{C}}$	$\mathcal{I} =$	d_{BCH}	d_{HT}	d_f
$\{0,1,7,-3\}$	$[-4,8]$	4	4	5
$\{0,1,7,9,-3\}$	$[-4,10]$	4	4	6
$\{0,1,7,9,11,-3\}$	$[-4,13]$	4	4	7

Again, we assume a length n, such that $\gcd(n,15) = 1$. In the interval $\mathcal{I} = [-6,16]$ we can match a concatenation of sequences $(a_0\ a_1 \ldots a_{14})$ if $\{1,3,9,-3\} \supseteq D_{\mathcal{C}}$. Since $\deg f(x) = 4$, we obtain $d_f = 6$.

Similarly as before, there are special cases, where we can show that some elements of $D_{\mathcal{C}}$ are in the same coset. These cases are summarized in Table VII.

For $n = 2^m + 1$, we know from the previous classes that $-3 \in M_3$. If the length is $n = 3 \cdot 2^m + 1$, $3 \cdot 2^m \equiv -1 \mod n$ and hence, $-3 \equiv 9 \cdot 2^m \mod n$ and $-3 \in M_9$. For the length $n = 2^m + 3$, $-3 \equiv 2^m \mod m$ and $-3 \in M_1$.

If we consider $n = 2^m - 3$, with $\Delta = -3$ and (13), $-\Delta = 3 \in M_1$. Since $9 \equiv 3 \cdot 2^m \mod n$, $M_9 = M_3 = M_1$.

TABLE VII
CYCLIC CODES OF LENGTH n, $\gcd(n,15) = 1$, USING $f(x) = x^4 + x + 1$

Length	$\supseteq D_{\mathcal{C}}$	$\mathcal{I} =$	d_{BCH}	d_{HT}	d_f
-	$\{1,3,9,-3\}$	$[-6,16]$	5	5	6
$n = 2^m + 1$	$\{1,3,9\}$	$[-6,16]$	5	5	6
$n = 3 \cdot 2^m + 1$	$\{1,3,9\}$	$[-6,16]$	5	5	6
$n = 2^m + 3$	$\{1,3,9\}$	$[-6,16]$	5	5	6
$n = 2^m - 3$	$\{1,-3\}$	$[-6,16]$	5	5	6

V. DECODING ALGORITHM

In this section, we give an efficient decoding algorithm for the classes of Section IV, which corrects up to $(d_f - 1)/2$ errors.

Let $\mathcal{E}$ be the set of error positions. We define a syndrome polynomial $S(x)$:

$$\sum_{i=0}^{n-1} r_i \frac{\alpha^{bi} h(\alpha^i x)}{f(\alpha^i x)} = \sum_{i \in \mathcal{E}} \frac{\alpha^{bi} h(\alpha^i x)}{f(\alpha^i x)} \equiv S(x) \mod x^{\mu-1}. \tag{15}$$

TABLE II
NECESSARY ROOTS IN THE DEFINING SET OF A CYCLIC CODE AND POWER SERIES $1/(x^3+x+1)$.

$\subseteq D_{\mathcal{C}}$	$\cdots$	□	-3	□	□	0	1	2	□	4	□	□	7	8	9	□	11	□	□	□	$\cdots$
$1/(x^3+x+1)$	$\cdots$	0	1	0	0	1	1	1	0	1	0	0	1	1	1	0	1	0	0	1	$\cdots$

TABLE V
NECESSARY ROOTS IN THE DEFINING SET OF A CYCLIC CODE AND POWER SERIES $1/(x^4+x+1)$.

$\subseteq D_{\mathcal{C}}$	$\cdots$	□	-6	□	□	-3	□	□	□	1	2	3	4	□	6	□	8	9	□	□	12	□	□	□	16	□	$\cdots$
$1/(x^4+x+1)$	$\cdots$	1	1	0	0	1	0	0	0	1	1	1	1	0	1	0	1	1	0	0	1	0	0	0	1	1	$\cdots$

With

$$\Lambda(x) \stackrel{\text{def}}{=} \prod_{i\in\mathcal{E}} f(\alpha^i x),$$
$$\Omega(x) \stackrel{\text{def}}{=} \sum_{i\in\mathcal{E}} \Big(\alpha^{ib}\cdot h(\alpha^i x)\cdot \prod_{\substack{j\in\mathcal{E}\\ j\neq i}} f(\alpha^j x)\Big), \tag{16}$$

we can formulate the following key equation:

$$S(x)\cdot\Lambda(x) \equiv \Omega(x) \mod x^{\mu-1}. \tag{17}$$

In order to find $\Lambda(x)$ and $\Omega(x)$, we can solve a linear system of equations or to decrease the complexity, use the EEA or the BMA. Thus, for example calculating $\texttt{EEA}\ (x^{\mu-1}, S(x))$ gives us the polynomial $\Lambda(x)$ (see also [1]). However, $\Lambda(x)$ is *not* the classical error–locator polynomial with α^i as roots, $\forall\ i\in\mathcal{E}$.

Each $f(\alpha^i x)$ can be decomposed into $\deg f(\alpha^i x)$ linear factors over a field $\mathbb{GF}(2^\ell)$, where ℓ is the smallest integer such that $n|(2^\ell-1)$ (in many cases $\ell = s$). The factors of each $f(\alpha^i x)$ are disjoint to the factors of $f(\alpha^j x)$ for all $i\neq j$ since $\gcd(f(\alpha^i x), f(\alpha^j x)) = 1$ for all $i\neq j$. Hence, one root of $f(\alpha^i x)$ uniquely determines α^i. For a certain fraction, we save one root of each $f(\alpha^i x)$, $i = 0,\ldots,n-1$ in a look–up–table. Let us denote these roots by $\beta_0,\beta_1,\ldots,\beta_{n-1}$.

Algorithm 1: Decoding Binary Cyclic Codes

Input: Received Word $r(x)$, $f(x,\alpha_i)$, $h(x,\alpha_i,\delta)$

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

1 Calculate $S(x)$ by (15)
2 Solve Key Equation: Obtain $\Lambda(x)$, $\Omega(x)$ as output of
3 $\texttt{EEA}\,(x^{\mu-1}, S(x))$
4 Chien–Search: Find all i for which $\Lambda(\beta_i) = 0$
5 Save them as $\widehat{\mathcal{E}} = \{i_0, i_1, \ldots, i_t\}$
6 $\widehat{e}(x) \leftarrow \sum_{i\in\widehat{\mathcal{E}}} x^i$
7 $\widehat{c}(x) \leftarrow r(x) - \widehat{e}(x)$

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

As a second step in the decoding process, we have to find α^i for all $i\in\mathcal{E}$ when $\Lambda(x)$ is known. That means we have to find all $f(\alpha^i x)$, which are factors of $\Lambda(x)$. We do a (usual) Chien search [13] for $\Lambda(x)$ with the precomputed $\beta_0,\beta_1,\ldots,\beta_{n-1}$. Since β_i uniquely determines $f(\alpha^i x)$, we obtain all α^i with $i\in\mathcal{E}$. No error evaluation is necessary afterwards since we consider only binary codes.

The decoding idea is summarized in Algorithm 1. The complexity of the decoding algorithm is determined by Steps 2 and 3. The complexity of the EEA is quadratic in μ, i.e., $\mathcal{O}(\mu^2) = \mathcal{O}((\deg f(x)\cdot d_f)^2)$. The Chien–search requires the same complexity as for all classical methods and is $\mathcal{O}(n^2)$. Therefore, we can upper bound the complexity of Algorithm 1 by $\mathcal{O}((\deg f(x)\cdot n)^2)$.

VI. CONCLUSION

We presented a new approach that gives a general bound on the minimum distance of binary cyclic codes. According to this scheme several classes of binary codes were identified and necessary properties were proven. Furthermore, a quadratic–time decoding approach beyond the HT bound was proposed.

After submission to ISIT 2011 we generalized our approach to the q-ary case. A preliminary version can be found on arxiv [15].

REFERENCES

[1] 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.

[2] E. R. Berlekamp, *Algebraic coding theory*. McGraw-Hill, 1968.

[3] J. Massey, "Shift-register synthesis and BCH decoding," *Information Theory, IEEE Transactions on*, vol. 15, no. 1, pp. 122–127, January 2003. [Online]. Available: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=1054260

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

[5] 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

[6] C. Hartmann, "Decoding beyond the BCH bound (Corresp.)," *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

[7] 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

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

[9] 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

[10] ——, "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

[11] G. L. Feng and K. K. Tzeng, "Decoding cyclic and BCH codes up to actual minimum distance using nonrecurrent syndrome dependence relations," *IEEE Transactions on Information Theory*, vol. 37, no. 6, pp. 1716–1723, 1991. [Online]. Available: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=104340

[12] ——, "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

[13] R. T. Chien, "Cyclic decoding procedures for Bose-Chaudhuri-Hocquenghem codes," *IEEE Transactions on Information Theory*, vol. 10, no. 4, pp. 357–363, 1964. [Online]. Available: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=1053699

[14] S. V. Bezzateev and N. A. Shekhunova, "One Generalization of Goppa Codes," pp. 299+, 1997. [Online]. Available: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=613221

[15] A. Zeh, A. Wachter, and S. Bezzateev, "Decoding Cyclic Codes up to a New Bound on the Minimum Distance," May 2011. [Online]. Available: http://arxiv.org/abs/1105.1894