Describing A Cyclic Code by Another Cyclic Code

Alexander Zeh, Sergey Bezzateev

Describing A Cyclic Code by Another Cyclic Code

Alexander Zeh
Institute of Communications Engineering
University of Ulm, Ulm, Germany and
Research Center INRIA Saclay/École Polytechnique, Paris, France
alexander.zeh@uni-ulm.de

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

***Abstract*—A new approach to bound the minimum distance of q-ary cyclic codes is presented. The connection to the BCH and the Hartmann–Tzeng bound is formulated and it is shown that for several cases an improvement is achieved.**

We associate a second cyclic code to the original one and bound its minimum distance in terms of parameters of the associated code.

***Index Terms*—BCH Bound, Cyclic Code, Hartmann–Tzeng Bound**

I. Introduction

Cyclic codes play an important role in coding theory and many communication systems. Their cyclic structure allows among other things efficient decoding methods. For many cyclic codes, the minimum distance is not known, and hence we will investigate the minimum Hamming distance of q-ary cyclic codes in this contribution.

The Bose–Ray-Chaudhuri–Hocquenghem (BCH, [1], [2]) bound uses *the longest* consecutive sequence in the defining set of the code to bound the minimum distance. Its generalization, the Hartmann–Tzeng (HT, [3], [4]) bound, is based on *several* consecutive sets of zeros. Further generalizations are the contributions of Roos [5], [6], van Lint and Wilson [7], Duursma and Kötter [8] and Duursma and Pellikaan [9]. Other approaches include the Boston bounds [10] and the bound by Betti and Sala [11].

Our approach uses a second cyclic code — the *non-zero-locator code* — to describe the defining set of the cyclic code which allows to bound its minimum distance. It turns out that a good bound on the minimum distance is achieved, if the non-zero-locator code has low rate and a small distance.

This contribution is a generalization of our previous work [12], [13], where we used the power series expansion of a fraction of two co-prime polynomials and associated it with the code. The advantage of this extension is that we can directly use well-known properties of cyclic codes to describe another cyclic code rather than abstract properties of power series expansions. Further, this contribution is a generalization of [12], [13] since the non-zero-locator code can be seen as a sum of several power series expansions.

Our contribution is structured as follows. We introduce necessary preliminaries of q-ary cyclic codes in Section II and recall the HT bound. Section III gives the definition of the non-zero-locator code and proves the main theorem on the minimum distance. Single parity check and cyclic Reed–Solomon codes are used as non-zero-locator codes and the connection to the HT bound is shown in Section IV. Section V concludes this contribution.

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

II. Preliminaries

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 indeterminate x. A q-ary cyclic code $\mathcal{C}$ over $\mathbb{F}_q$ of length n, dimension k and minimum distance d is denoted by $\mathcal{C}(q;n,k,d)$. A codeword $c(x)=\sum_{i=0}^{n-1} c_i x^i$ of $\mathcal{C}(q;n,k,d)$ is a multiple of its generator polynomial $g(x)\in\mathbb{F}_q[x]$ with roots in $\mathbb{F}_{q^s}$, where $n \mid (q^s-1)$. Let $\alpha\in\mathbb{F}_{q^s}$ be a primitive nth root of unity. 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 $\mathcal{C}(q;n,k,d)$ is the set containing the indices of the zeros of the generator polynomial $g(x)$ and can be partitioned into m cyclotomic cosets:

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

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

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

Let us recall a well-known bound on the minimum distance of cyclic codes.

Theorem 1 (Hartmann–Tzeng (HT) Bound, [3]) *Let a q-ary cyclic code $\mathcal{C}(q;n,k,d)$ with the defining set $D_{\mathcal{C}}$ be given. Suppose there exist the integers b_1, m_1 and m_2 with $\gcd(n,m_1)=1$ and $\gcd(n,m_2)=1$ such that*

$$\{b_1+i_1m_1+i_2m_2 \mid 0\le i_1\le d_0-2,\ 0\le i_2\le \nu\}\subseteq D_{\mathcal{C}}.$$

Then, $d \geq d_0 + \nu$.

Note that for $\nu = 0$ the HT bound becomes the BCH bound [1], [2]. A further generalization was proposed by Roos [5], [6] and van Lint and Wilson [7]. Decoding up to the HT and the Roos bound was formulated by Feng and Tzeng [14, Section VI].

We consider cyclic Reed–Solomon (RS) codes [15] for our approach and therefore recapitulate their definition in the following.

Definition 1 (Cyclic Reed–Solomon Code) *Let n be an integer dividing $q-1$ and let α denote an element of multiplicative order n in $\mathbb{F}_q$. Let δ be an integer. Furthermore, let the generator polynomial $g_\delta(x) \in \mathbb{F}_q[x]$ be defined as:*

$$g_\delta(x) = \prod_{i=\delta}^{\delta+n-k-1} (x - \alpha^i).$$

Then, a cyclic Reed–Solomon code over $\mathbb{F}_q$ of length $n \mid q-1$ and dimension k, denoted by $\mathcal{RS}(q; n, k; \delta)$, is defined by:

$$\mathcal{RS}(q; n, k; \delta) = \{m(x) g_\delta(x) : \deg m(x) < k\}.$$

RS codes are maximum distance separable codes and their minimum distance d is $d = n - k + 1$.

III. The Non-Zero-Locator Code

We extend our earlier approach [12], [13], where we associated a power series expansion of a fraction of two co-prime polynomials with the zeros of a cyclic code. Now, we connect another cyclic code — the so-called non-zero-locator code — to a given cyclic code.

Let us establish a connection between the codewords of a cyclic code and the sum of power series expansions. Let $c(x)$ be a codeword of a given q-ary cyclic code $\mathcal{C}(q; n, k, d)$ and let the set $\mathcal{Y}$ denote the set of indices of nonzero coefficients of $c(x)$

$$c(x) = \sum_{i \in \mathcal{Y}} c_i x^i.$$

Let α be an element of order n. Then, we have the following relation for all $c(x) \in \mathcal{C}(q; n, k, d)$:

$$\sum_{j=0}^{\infty} c(\alpha^j) x^j = \sum_{i \in \mathcal{Y}} \frac{c_i}{1 - x\alpha^i}. \tag{5}$$

Now, we can define the non-zero-locator code.

Definition 2 (Non-Zero-Locator Code) *Let a q-ary cyclic code $\mathcal{C}(q; n, k, d)$ be given. Let α denote an nth root of unity. Let $\gcd(n, n_\ell) = 1$ and let β be an n_ℓth root of unity. Then, $\mathcal{L}(q_\ell; n_\ell, k_\ell, d_\ell)$ is a non-zero-locator code of $\mathcal{C}$ if there exists a $\mu \geq 0$ and an integer e, such that $\forall\, a(x) \in \mathcal{L}$ and $\forall\, c(x) \in \mathcal{C}$:*

$$\sum_{j=0}^{\infty} c(\alpha^{j+e}) a(\beta^j) x^j \equiv 0 \bmod x^{\mu-1},$$

holds.

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

$$c(\alpha^e)a(\beta^0), c(\alpha^{e+1})a(\beta^1), \ldots, c(\alpha^{e+\mu-2})a(\beta^{\mu-2}),$$

that results in a zero-sequence of length $\mu-1$, i.e., the product of the evaluated codeword $a(\beta^j)$ of the non-zero-locator code $\mathcal{L}$ and the evaluated codeword $c(\alpha^{j+e})$ of $\mathcal{C}$ gives zero for all $j = 0, \ldots, \mu-2$.

We require a root β^j of the non-zero-locator code $\mathcal{L}$ at the position j where the cyclic code $\mathcal{C}$ has no zero.

We require $\gcd(n, n_\ell) = 1$ to guarantee that

$$\gcd\Big(\prod_{j \in \mathcal{Y}} (1 - x\alpha^i\beta^j), \prod_{j \in \mathcal{Y}} (1 - x\alpha^m\beta^j)\Big) = 1 \,\forall i \neq m, \tag{6}$$

that we use for the degree calculation in the following. For the proof we refer to [12, Lemma 1]. We rewrite the expression of Definition 2 with (5) more explicitly. Let $\mathcal{Z}$ denote the set of indexes of nonzero coefficients of $a(x) \in \mathcal{L}$.

$$\sum_{j=0}^{\infty} c(\alpha^{j+e}) a(\beta^j) x^j = \sum_{j=0}^{\infty} \sum_{i \in \mathcal{Y}} c_i \alpha^{i(j+e)} a(\beta^j) x^j = \sum_{i \in \mathcal{Y}} c_i \alpha^{ie} \sum_{j=0}^{\infty} \alpha^{ij} a(\beta^j) x^j$$

Using (5) for the two codewords $a(x)$ and $c(x)$ leads to:

$$\sum_{i \in \mathcal{Y}} c_i \alpha^{ie} \sum_{j=0}^{\infty} \alpha^{ij} a(\beta^j) x^j = \sum_{i \in \mathcal{Y}} c_i \alpha^{ie} \sum_{j \in \mathcal{Z}} \frac{a_j}{1 - x\alpha^i\beta^j} = \sum_{i \in \mathcal{Y}} c_i \alpha^{ie} \frac{\sum_{j \in \mathcal{Z}} \Big(a_j \prod_{\substack{\ell \in \mathcal{Z} \\ \ell \neq j}} (1 - x\alpha^i\beta^\ell)\Big)}{\prod_{j \in \mathcal{Z}} (1 - x\alpha^i\beta^j)},$$

and finally we obtain:

$$\frac{\sum_{i \in \mathcal{Y}} \Big(c_i \alpha^{ie} \sum_{j \in \mathcal{Z}} \Big(a_j \prod_{\substack{\ell \in \mathcal{Z} \\ \ell \neq j}} (1 - x\alpha^i\beta^\ell)\Big) \prod_{\substack{m \in \mathcal{Y} \\ m \neq i}} \prod_{o \in \mathcal{Z}} (1 - x\alpha^m\beta^o)\Big)}{\prod_{i \in \mathcal{Y}} \prod_{j \in \mathcal{Z}} (1 - x\alpha^i\beta^j)} \equiv 0 \bmod x^{\mu-1}, \tag{7}$$

where the degree of the denominator is exactly $|\mathcal{Y}| \cdot |\mathcal{Z}|$ due to (6). The degree of the numerator is smaller than or equal to $(|\mathcal{Y}| - 1) \cdot |\mathcal{Z}| + |\mathcal{Z}| - 1$. In the following we assume that the degree of the numerator is $(|\mathcal{Y}|-1)\cdot|\mathcal{Z}|+|\mathcal{Z}|-1 = |\mathcal{Y}|\cdot|\mathcal{Z}|-1$.

This leads to the following theorem on the minimum distance of a cyclic code $\mathcal{C}$.

Theorem 2 (Minimum Distance) *Let a q-ary cyclic code $\mathcal{C}(q; n, k, d)$ with the associated non-zero-locator code $\mathcal{L}(q_\ell; n_\ell, k_\ell, d_\ell)$ and the integers μ and e be given with*

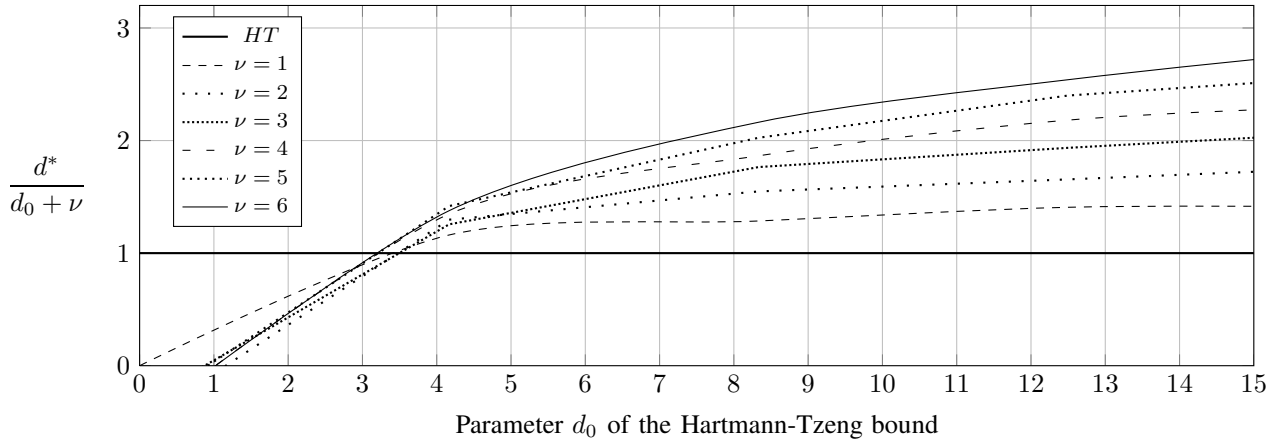

Fig. 1. Illustration of the fraction $d^*/(d_0+\nu)$ of our bound d^* of (11) to the Hartmann–Tzeng bound $d_0+\nu$ for $\nu = 1, \ldots, 6$ and $d_0 = 2, \ldots, 20$. The parameters of the HT bound are $m_1 = \nu + 2$ and $m_2 = 1$ (see Table III). We used a single parity check code as non-zero-locator code. Our bound d^* is for $d_0 > 3$ better than the HT bound.

$\gcd(n, n_\ell) = 1$, *such that (7) holds. Then, the minimum distance* d *of* $\mathcal{C}(q; n, k, d)$ *satisfies the following inequality:*

$$d \geq d^* \stackrel{\text{def}}{=} \left\lceil \frac{\mu}{d_\ell} \right\rceil. \tag{8}$$

Proof: For a codeword $c(x) \in \mathcal{C}(q; n, k, d)$ of weight d and codeword $a(x) \in \mathcal{L}(q_\ell; n_\ell, k_\ell, d_\ell)$ of weight d_ℓ, the degree of the denominator in (2) is $d \cdot d_\ell$. The numerator has degree at most $d \cdot d_\ell - 1$, and has to be greater than or equal to $\mu - 1$. ∎

Example 1 (Binary Code of length $n = 21$ [6], [7]) *Let the binary cyclic code* $\mathcal{C}(2; 21, 7, 8)$ *with generator polynomial* $g(x)$

$$g(x) = M_1^{(21)}(x) \cdot M_3^{(21)}(x) \cdot M_7^{(21)}(x) \cdot M_9^{(21)}(x)$$

be given.

The defining set $D_\mathcal{C} = M_1^{(21)} \cup M_3^{(21)} \cup M_7^{(21)} \cup M_9^{(21)}$ *of* $\mathcal{C}(2; 21, 7, 8)$ *is:*

$$D_\mathcal{C} = \{1, 2, 3, 4, \square, 6, 7, 8, 9, \square, 11, 12, \square, 14, 15, 16, \square, 18\},$$

where the symbol $\square$ *marks the index where* $g(\alpha^i) \neq 0$.

We associate a single parity check code of length $n_\ell = 5$, $k_\ell = 4$ *distance* $d_\ell = 2$ *as non-zero-locator code for* $\mathcal{C}(2; 21, 7, 8)$ *according to Definition 2. For* $e = 0$ *the subset of the defining set of* $\mathcal{C}(2; 21, 7, 8)$ *and* $\mathcal{L}(2^4; 5, 4, 2)$ *is listed in Table I, where the product gives the a zero-sequence of length* 13*. The codewords* $a(x) \in \mathcal{L}(2^4; 5, 4, 2)$ *"fill" the missing zeros of* $\mathcal{C}(2; 21, 7, 8)$ *at position* 0*,* 5 *and* 10 *in the interval* $[0, 12]$. *We have* $\mu - 1 = 13$ *and therefore* $d^* = \lceil (14)/2 \rceil = 7$. *The HT bound with parameters* $b_1 = 1$, $m_1 = 5$, $d_0 = 3$ *and* $m_2 = 1$, $\nu = 3$ *gives also a lower bound of* 7 *and the Roos bound gives* 8 *[7], which is the minimum distance of* $\mathcal{C}(2; 21, 7, 8)$.

The optimal non-zero-locator code $\mathcal{L}$ for a cyclic code gives a zero sequence

$$c(\alpha^e)a(\beta^0), c(\alpha^{e+1})a(\beta^1), \ldots, c(\alpha^{e+\mu-2})a(\beta^{\mu-2})$$

TABLE I
DEFINING SETS $D_\mathcal{C}$ AND $D_\mathcal{L}$ OF THE BINARY CYCLIC CODE $\mathcal{C}(2; 21, 7, 8)$ AND ITS NON-ZERO-LOCATOR CODE $\mathcal{L}(2^4; 5, 4, 2)$ IN THE INTERVAL $[0, 12]$.

$D_\mathcal{C}$	□	1	2	3	4	□	6	7	8	9	□	11	12
$D_\mathcal{L}$	0	□	□	□	□	0	□	□	□	□	0	□	□

of length $\mu - 1$ as in Definition 2, such that d^* of (8) is maximized.

If we require a small cardinality of the defining set $D_\mathcal{C}$, the cardinality of the defining set $D_\mathcal{L}$ of the non-zero-locator code should be large to obtain a long zero-sequence and therefore $\mathcal{L}$ should have a low rate k_ℓ/n_ℓ. On the other hand, the distance d_ℓ of the non-zero-locator code $\mathcal{L}$ should be small.

IV. Beating the Hartmann–Tzeng Bound Using a Non-Zero-Locator Code

A. Normalization of HT Bound

Let us rewrite the HT bound as given in Theorem 1. We multiply with the inverse of m_2 modulo n. Let $\mathcal{C}(q; n, k, d)$ be a q-ary cyclic code with the defining set $D_\mathcal{C}$. Let

$$\{b_2 + i_1 m + i_2 : 0 \leq i_1 \leq d_0 - 2, 0 \leq i_2 \leq \nu\} \subseteq D_\mathcal{C}, \tag{9}$$

where $\gcd(n, m) = 1$. Then $d \geq d_0 + \nu$.

Note that $m > \nu + 1$. We refer to this representation of the HT bound in this section. In the following, we consider a single parity check code as non-zero-locator code and outline the connection to a particular case of the HT bound. The general case is then considered in Subsection IV-C, where cyclic RS codes are used as non-zero-locator codes.

B. Parity Check Code as Non-Zero-Locator Code

Let a q-ary cyclic code $\mathcal{C}(q; n, k, d)$ with a subset of its defining set with parameters $d_0 > 2$ and $\nu > 0$ be given as stated in (9). Furthermore, let $m = \nu + 2$.

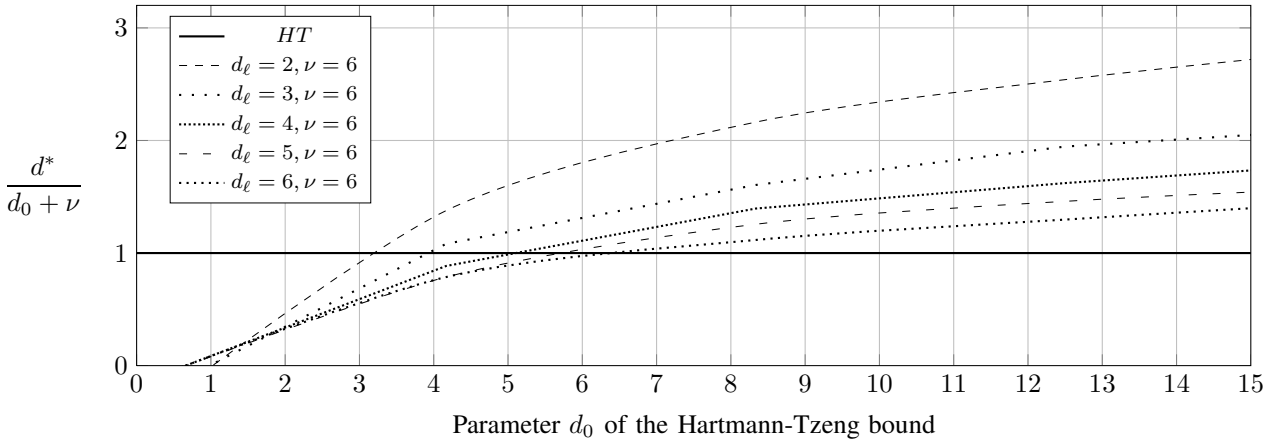

Fig. 2. Illustration of the fraction $d^*/(d_0+\nu)$ of our bound d^* of (11) to the Hartmann–Tzeng bound $d_0+\nu$ for $\nu = 6$, $d_0 = 2, \ldots, 20$, $m_1 = m$ and $m_2 = 1$. We used an RS code as non-zero-locator code with distance $d_\ell = m - \nu$ (see Table II).

We associate a binary single parity check code as non-zero-locator code. Let $\mathcal{L}(2; n_\ell, n_\ell - 1, 2)$ be the cyclic non-zero-locator code with generator polynomial $g(x) = x - 1$. We assume $\gcd(n, n_\ell) = 1$ for the given cyclic code $\mathcal{C}(q; n, k, d)$. We illustrate the set of zeros of the cyclic non-zero-locator code $\mathcal{L}$, i.e., a single parity check code, for the cyclic code $\mathcal{C}(q; n, k, d)$ in Table III. A $\square$ represents the existence of a non-zero of the corresponding code $\mathcal{C}$ or $\mathcal{L}$. The sequence is illustrated in terms of parameters of the HT bound as in (9). The considered code $\mathcal{C}$ has $d_0 - 1$ sets of $\nu + 1$ consecutive zeros, separated by one non-zero. The non-zero-locator code fills exactly this one non-zero.

TABLE III
DEFINING SETS $D_\mathcal{C}$ FOR $b_2 = 0$, $m_1 = m = \nu + 2$, $m_2 = 1$ AND $D_\mathcal{L}$ IN THE INTERVAL $[-1, m(d_0 - 1) - 1]$.

$D_\mathcal{C}$	$\square$	1	..	m-1	$\square$	m+1..		$2m$-1	$\square$	..	$m(d_0$-1)-1	$\square$
$D_\mathcal{L}$	0	$\square$	..	$\square$	0	$\square$	..	$\square$	0	..	$\square$	0

The parameters of the non-zero-locator code $\mathcal{L}(2; n_\ell, k_\ell, d_\ell)$ are:

$$n_\ell = \nu + 2, \quad k_\ell = \nu + 1, \quad d_\ell = 2$$

and we have $\mu - 1 = m \cdot (d_0 - 1) + 1$. From (8) we obtain:

$$\begin{aligned} d^* &= \left\lceil \frac{m(d_0 - 1) + 2}{2} \right\rceil \\ &= \left\lceil \frac{(\nu + 2)d_0 - \nu}{2} \right\rceil . \end{aligned} \tag{10}$$

In Fig. 1 we illustrate d^* of (10) for different parameters ν and d_0 of the HT bound.

Example 2 (Parity Code as Non-Zero-Locator Code) *Consider a cyclic code $\mathcal{C}(q; n, k, d)$ with the defining set $D_\mathcal{C}$ and let*

$$\{-5, -4, \square, -2, -1, \square, 1, 2, \square, 4, 5, \square\} \subseteq D_\mathcal{C}.$$

Furthermore let $\gcd(n, 3) = 1$. We associate a cyclic single parity check code of length $n_\ell = 3$ with $\mathcal{C}$ and illustrate the corresponding zero-sequence in Table IV. The zero-sequence has length $\mu - 1 = 13$ and we obtain $d^* = \lceil (14)/2 \rceil = 7$. The HT bound gives for $b_2 = -5, m = 3$ and $d_0 = 5$, $\nu = 1$

TABLE IV
DEFINING SETS $D_\mathcal{C}$ FOR $b_2 = -5$, $m_1 = \nu + 2 = 3$, $m_2 = 1$ AND $D_\mathcal{L}$ IN THE INTERVAL $[-6, 6]$.

$D_\mathcal{C}$	$\square$	-5	-4	$\square$	-2	-1	$\square$	1	2	$\square$	4	5	$\square$
$D_\mathcal{L}$	0	$\square$	$\square$	0	$\square$	$\square$	0	$\square$	$\square$	0	$\square$	$\square$	0

a lower bound of $d \geq 6$ on the minimum distance of $\mathcal{C}$.

C. Reed–Solomon Code as Non-Zero-Locator Code

In the previous subsection we associated to q-ary cyclic code $\mathcal{C}$, with a subset of its defining set with parameters $m_1 = m = \nu+2$ and $m_2 = 1$ as stated in Theorem 1, a single parity check code. Now we consider the case were $m > \nu+2$ and associate a RS code to the given q-ary cyclic code.

Let a q-ary cyclic code $\mathcal{C}(q; n, k, d)$ with a subset of its defining set with parameters $d_0 > 2$ and $\nu > 0$ be given as stated in (9). Furthermore, let $m > \nu + 2$.

In Table II, the HT bound (9) with $i_1 = 0, \ldots, d_0 - 2$ and $i_2 = 0, \ldots, \nu$ is illustrated. We choose as non-zero-locator

TABLE II
DEFINING SETS $D_\mathcal{C}$ FOR $b_2 = 1$ AND m OF THE HT BOUND (9) AND $D_{\mathcal{RS}}$ OF THE ASSOCIATED NON-ZERO-LOCATOR CODE IN THE INTERVAL $[-(m - \nu) - 1, m(d_0 - 1)]$.

$D_\mathcal{C}$	$\square$	..	$\square$	1	..	ν+1	$\square$	..	$\square$	m+1	..	$m+\nu$+1	$\square$	..	$\square$	..	$\square$
$D_{\mathcal{RS}}$	0	..	m-ν-2	$\square$	..	$\square$	0	..	m-ν-2	$\square$	..	$\square$	0	..	m-ν-2	..	m-ν-2

code $\mathcal{L}(q_\ell; n_\ell, k_\ell, d_\ell)$ a cyclic RS code with $\delta = 0$ as in Definition 1. The parameters are:

$$n_\ell = m, \quad k_\ell = \nu + 1, \quad d_\ell = m - \nu.$$

The $m - \nu - 1$ consecutive zeros of the non-zero-locator code $\mathcal{L}$, i.e., a cyclic RS code of length m, fill the missing zeros of the given cyclic code $\mathcal{C}(q; n, k, d)$. We obtain for the "zero"-sequence with length $\mu = m(d_0 - 1) + m - \nu - 1$.

Therefore, we obtain from (8):

$$\begin{aligned} d^* &= \left\lceil \frac{m(d_0 - 1) + m - \nu}{m - \nu} \right\rceil \\ &= \left\lceil \frac{md_0 - m + m - \nu}{m - \nu} \right\rceil \\ &= \left\lceil \frac{md_0 - \nu}{m - \nu} \right\rceil. \end{aligned} \quad (11)$$

Note that for $m = \nu + 2$ the non-zero-locator code is a single parity check code and we obtain the result from (10). Fig. 2 shows d^* of (11) normalized to $d_0 + \nu$ for the same parameter $\nu = 6$. We varied the distance d_ℓ of the non-zero-locator code.

Let us precise the cases where our bound d^* is larger than the Hartmann–Tzeng bound $d_0 + \nu$.

Proposition 1 *Let a q-ary cyclic code $\mathcal{C}$ with a subset of its defining set with parameters d_0, ν, $m_1 = m$ and $m_2 = 1$ as stated in Theorem 1 be given. Let $\mathcal{L}(q_\ell; m, \nu + 1, m - \nu)$ be the associated cyclic RS code as in Definition 2. Then, for*

$$d_0 > m - \nu + 1,$$

$d^* > d_0 + \nu$ holds.

Proof: From (11) we have

$$\begin{aligned} d^* &= \left\lceil \frac{md_0 - \nu}{m - \nu} \right\rceil \\ &= \left\lceil \frac{md_0 - d_0\nu + d_0\nu - \nu}{m - \nu} \right\rceil \\ &= \left\lceil d_0 + \frac{(d_0 - 1)\nu}{m - \nu} \right\rceil. \end{aligned}$$

For $d^* > d_0 + \nu$, we need

$$\begin{aligned} \frac{(d_0 - 1)\nu}{m - \nu} &> \nu \\ d_0 &> m - \nu + 1 = d_\ell + 1 \end{aligned} \quad (12)$$

■

For $m - \nu = d_\ell = 2$ the associated RS code is a single parity check code and our bound is better than the HT bound for $d_0 > 3$ (see Fig. 1). Some other cases, where the distance of the associated RS code $m - \nu = d_\ell$ is between two and six, are illustrated in Fig. 2.

V. Conclusion and Outlook

We presented and proved a new bound on the minimum distance of q-ary cyclic codes. The used technique is based on a second cyclic code — the so-called non-zero-locator code. We used non-zero-locator codes that allow us to connect the Hartmann–Tzeng bound directly with our bound. In detail, we used single parity check codes and RS codes and showed for which parameters our bound improves upon the HT bound.

Future work is the decoding up to our bound and the classification of cyclic codes, where the non-zero-locator code gives a good bound on the minimum distance.

Acknowledgement

The authors wish to thank Antonia Wachter-Zeh and Daniel Augot for fruitful discussions.

References

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

[2] 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, Mar. 1960. [Online]. Available: http://dx.doi.org/10.1016/S0019-9958(60)90287-4

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

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

[5] 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, Sep. 1982. [Online]. Available: http://dx.doi.org/10.1016/0097-3165(82)90014-0

[6] ——, "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

[7] 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, Jan. 1986. [Online]. Available: http://dx.doi.org/10.1109/TIT.1986.1057134

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

[9] I. M. Duursma and R. Pellikaan, "A symmetric Roos bound for linear codes," *J. Comb. Theory Ser. A*, vol. 113, pp. 1677–1688, Nov. 2006. [Online]. Available: http://portal.acm.org/citation.cfm?id=1226423

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

[11] 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, Jul. 2006. [Online]. Available: http://dx.doi.org/10.1109/TIT.2006.876240

[12] A. Zeh, A. Wachter, and S. Bezzateev, "Efficient Decoding of Some Classes of Binary Cyclic Codes Beyond the Hartmann-Tzeng Bound," in *2011 IEEE International Symposium on Information Theory Proceedings (ISIT2011)*, St. Petersburg, Russia, Jul. 2011, pp. 1017–1021.

[13] ——, "Decoding Cyclic Codes up to a New Bound on the Minimum Distance," *accepted for IEEE Transactions on Information Theory*, 2012.

[14] 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

[15] I. S. Reed and G. Solomon, "Polynomial Codes Over Certain Finite Fields," *Journal of the Society for Industrial and Applied Mathematics*, vol. 8, no. 2, pp. 300–304, 1960. [Online]. Available: http://dx.doi.org/10.1137/0108018