# A New Bound on the Minimum Distance of Cyclic Codes Using Small-Minimum-Distance Cyclic Codes

Alexander Zeh, Sergey Bezzateev

# A New Bound on the Minimum Distance of Cyclic Codes Using Small-Minimum-Distance Cyclic Codes

Alexander Zeh and Sergey Bezzateev*

August 29, 2012

**Abstract**

A new bound on the minimum distance of $q$-ary cyclic codes is proposed. It is based on the description by another cyclic code with small minimum distance. The connection to the BCH bound and the Hartmann–Tzeng (HT) bound is formulated explicitly. We show that for many cases our approach improves the HT bound. Furthermore, we refine our bound for several families of cyclic codes.

We define syndromes and formulate a Key Equation that allows an efficient decoding up to our bound with the Extended Euclidean Algorithm. It turns out that lowest-code-rate cyclic codes with small minimum distances are useful for our approach. Therefore, we give a sufficient condition for binary cyclic codes of arbitrary length to have minimum distance two or three and lowest code-rate.

**Keywords: BCH Bound - Bound on the Minimum Distance - Cyclic Code - Decoding - Hartmann–Tzeng Bound**

**Mathematics Subject Classification: 94A24 - 94A55 - 94B15 - 94B35**

## 1 Introduction

In this paper, we introduce a technique that uses an $(n_\ell, k_\ell)$ $q_\ell$-ary cyclic code $\mathcal{L}$ with minimum distance $d_\ell$ to bound the minimum distance $d$ of another $(n, k)$ $q$-ary cyclic code $\mathcal{C}$. The descriptive cyclic code $\mathcal{L}$ is called non-zero-locator code. It turns out that the non-zero-locator code gives a good lower bound $d^*$ on the minimum distance $d$ of the described cyclic code $\mathcal{C}$ if the code-rate $k_\ell/n_\ell$ of $\mathcal{L}$ is low and its minimum distance $d_\ell$ is relatively small.

*Alexander Zeh is with the Institute of Communications Engineering, University of Ulm, Ulm, Germany and INRIA Saclay–Île-de-France, École Polytechnique ParisTech, Palaiseau Cedex, France. Sergey Bezzateev is with the Saint Petersburg State University of Airspace Instrumentation, St. Petersburg, Russia, Email: alexander.zeh@uni-ulm.de, bsv@aanet.ru. The material in this contribution was presented in part to the IEEE International Symposium on Information Theory (ISIT 2012) in Boston, USA [18].

The algebraic relation between the cyclic non-zero-locator code $\mathcal{L}$ and the cyclic code $\mathcal{C}$ provides the formulation of syndromes and a Key Equation that allows an efficient decoding up to $\lfloor (d^* - 1)/2 \rfloor$ errors with the Extended Euclidean Algorithm (EEA).

We give an explicit relation of $d^*$ to the BCH bound [1,10] and its generalization: the Hartmann–Tzeng (HT) bound [7–9]. In many cases our bound is better than the HT bound, although our approach is not a generalization of the HT bound as the Roos bound [14, 15] and the bound of van Lint and Wilson [11] are.

In our previous work [17] we associated rational functions with a subset of the defining set of a given cyclic code $\mathcal{C}$. This can be seen as a special case of the presented approach. The main advantage of this contribution is that we can express the bound on the minimum distance of a given cyclic code $\mathcal{C}$ in terms of properties of the associated cyclic non-zero-locator code $\mathcal{L}$.

This paper is organized as follows. In Section 2, we give necessary preliminaries of cyclic codes, the HT bound and recall the definition of cyclic Reed–Solomon (RS) codes, which we use later as non-zero-locator code. The concept of the non-zero-locator code is introduced in Section 3 and the main theorem on the minimum distance is proven. The connection to the Hartmann–Tzeng bound is given in Section 4. Furthermore, several families of cyclic codes are identified. We give sufficient conditions for binary cyclic codes with minimum distance two and three and lowest code-rate in Section 5. A generalized syndrome definition, Key Equation and Forney's formula are given in Section 6. Section 7 concludes this contribution.

# 2 Preliminaries

Let $q$ be a power of a prime and let $\mathbb{F}_q$ denote the finite field of order $q$ and $\mathbb{F}_q[x]$ the set of all univariate polynomials with coefficients in $\mathbb{F}_q$ and indeterminate $x$. A $q$-ary cyclic code over $\mathbb{F}_q$ of length $n$, dimension $k$ and minimum distance $d$ is denoted by $\mathcal{C}(q; n, k, d) \subset \mathbb{F}_q^n$ and it is an ideal in the ring $\mathbb{F}_q[x]/(x^n - 1)$ generated by $g(x)$. A codeword $\mathbf{c} = (c_0\ c_1\ \ldots\ c_{n-1}) \in \mathcal{C}$ is associated with a polynomial $c(x) = \sum_{i=0}^{n-1} c_i x^i \in \mathbb{F}_q[x]$, where $g(x)$ divides $c(x)$. We assume that $x^n - 1$ has $n$ different roots. Let $\mathbb{F}_{q^s}$ be an extension field of $\mathbb{F}_q$ and let $\alpha \in \mathbb{F}_{q^s}$ be a primitive $n$th root of unity. The cyclotomic coset $M_r^{(n)}$ modulo $n$ over $\mathbb{F}_q$ is denoted by:

$$M_r^{(n)} = \{rq^j \bmod n \,|\, j = 0, 1, \ldots, n_r - 1\},$$

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

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

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

$$D_{\mathcal{C}} = \{0 \le i \le n - 1 \,|\, g(\alpha^i) = 0\} = M_{r_1}^{(n)} \cup M_{r_2}^{(n)} \cup \cdots \cup M_{r_m}^{(n)}.$$

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

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

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

**Theorem 1** (Hartmann–Tzeng (HT) Bound, [8]). *Let a $q$-ary cyclic code $\mathcal{C}(q;n,k,d)$ with 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*

$$\{b_1 + i_1 m_1 + i_2 m_2 \mid 0 \le i_1 \le d_0 - 2,\ 0 \le i_2 \le \nu\} \subseteq D_{\mathcal{C}}.$$

*Then $d \ge d_0 + \nu$.*

Note that for $\nu = 0$ the HT bound becomes the BCH bound [1, 10]. Further generalizations were proposed by Roos [14, 15] and van Lint and Wilson [11]. Decoding up to the HT bound and to some particular cases of the Roos bound was formulated by Feng and Tzeng [5, Section VI].

We consider cyclic Reed–Solomon (RS) codes [13] 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 $\alpha$ denote an element of multiplicative order $n$ in $\mathbb{F}_q$. Let $\delta$ 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 $n|(q-1)$ and dimension $k$, denoted by $\mathcal{RS}(q;n,k;\delta)$, is defined by:*

$$\mathcal{RS}(q;n,k;\delta) = \{m(x)g_\delta(x) : \deg m(x) < k\}. \tag{1}$$

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

# 3 The Non-Zero-Locator Code

We relate another cyclic code — the so-called non-zero-locator code $\mathcal{L}$ — to a given cyclic code $\mathcal{C}$. In the following, we connect a infinite sequence of an evaluated polynomial $c(x) \in \mathcal{C}$ to a sum of fractions. This allows to draw the relation to our previous approach [17]. Furthermore, we can use familiar properties of cyclic codes rather than abstract properties of rational functions. The obtained bound can be expressed in terms of parameters of the associated non-zero-locator code $\mathcal{L}$.

Let $c(x)$ be a codeword of a given $q$-ary cyclic code $\mathcal{C}(q;n,k,d)$ and let $\mathcal{Y}$ denote the set of indexes of non-zero coefficients of $c(x)$

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

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

$$\begin{aligned}
\sum_{j=0}^{\infty} c(\alpha^j) x^j &= \sum_{j=0}^{\infty} \sum_{i \in \mathcal{Y}} c_i \alpha^{ji} x^j \\
&= \sum_{j=0}^{\infty} \sum_{i \in \mathcal{Y}} c_i (\alpha^i x)^j \\
&= \sum_{i \in \mathcal{Y}} \sum_{j=0}^{\infty} c_i (\alpha^i x)^j \\
&= \sum_{i \in \mathcal{Y}} \frac{c_i}{1 - x\alpha^i}.
\end{aligned} \tag{2}$$

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 $\mathbb{F}_{q^s}$ contain the $n$th roots of unity. Let $\gcd(n,n_\ell)=1$ and let $\mathbb{F}_{q_\ell}=\mathbb{F}_{q^u}$ be an extension field of $\mathbb{F}_q$. Let $\mathbb{F}_{q_\ell^{s_\ell}}$ contain the $n_\ell$th roots of unity. Let $\alpha\in\mathbb{F}_{q^s}$ be an element of order $n$ and let $\beta\in\mathbb{F}_{q_\ell^{s_\ell}}$ be an element of order $n_\ell$.*

*Then $\mathcal{L}(q_\ell;n_\ell,k_\ell,d_\ell)$ is a non-zero-locator code of $\mathcal{C}$ if there exists a $\mu\geq 2$ and an integer $e$, such that $\forall\, a(x)\in\mathcal{L}$ and $\forall\, c(x)\in\mathcal{C}$:*

$$\sum_{j=0}^{\infty} c(\alpha^{j+e})a(\beta^j)x^j \equiv 0 \bmod x^{\mu-1}, \tag{3}$$

*holds.*

**Remark 1.** *Let $r$ denote the least common multiple of $s$ and $u\cdot s_\ell$ and let $\gamma$ be a primitive element in $\mathbb{F}_{q^r}$. Then $\gamma^{(q^r-1)/n}$ and $\gamma^{(q^r-1)/n_\ell}$ are elements of order $n$ and $n_\ell$.*

Before we prove the main theorem on the minimum distance $d$ of the given 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 $j=0,\ldots,\mu-2$. Let us study the following example of a binary cyclic code.

**Example 1** (Binary Code of length $n=21$ [11, 15])**.** *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. Let $\alpha\in\mathbb{F}_{2^6}$ denote an element of order 21.*
*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 indexes where $g(\alpha^i)\neq 0$.*

*We associate a single parity check code of length $n_\ell=5$, dimension $k_\ell=4$ and minimum distance $d_\ell=2$ over $\mathbb{F}_2$ as non-zero-locator code for $\mathcal{C}(2;21,7,8)$ according to Definition 2. Let $\beta\in\mathbb{F}_{2^4}$ be an element of order 5 and let $g(x)=x-1$ be the generator polynomial of $\mathcal{L}$. The defining sets $D_\mathcal{C}$ of $\mathcal{C}(2;21,7,8)$ and $D_\mathcal{L}$ of $\mathcal{L}(2;5,4,2)$ are listed in Table 1. The corresponding product gives the a zero-sequence of length $\mu-1=13$ for $e=0$. A codeword $a(x)\in\mathcal{L}(2;5,4,2)$ "fills" the missing zeros of $\mathcal{C}(2;21,7,8)$ at position 0, 5 and 10 in the interval $[0,12]$.*

Table 1: Defining sets $D_\mathcal{C}$ and $D_\mathcal{L}$ of the binary cyclic code $\mathcal{C}(2;21,7,8)$ of Example 1 and its non-zero-locator code $\mathcal{L}(2;5,4,2)$ in the interval $[0,12]$.

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

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

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

$$\gcd\Big(\prod_{m\in\mathcal{Z}}(1-x\alpha^i\beta^m), \prod_{m\in\mathcal{Z}}(1-x\alpha^j\beta^m)\Big) = 1 \quad \forall i \text{ and } \forall j \neq i,$$

which we use for the degree calculation in the following. For the proof we refer to Lemma 3 in the Appendix.

We rewrite (3) of Definition 2 more explicitly. With $c(x) = \sum_{i\in\mathcal{Y}} c_i x^i$ and $a(x) = \sum_{j\in\mathcal{Z}} a_j x^j$, we obtain:

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

Using (2) for the codeword $a(x)$ of the associated non-zero-locator code leads to:

$$\begin{aligned}\sum_{i\in\mathcal{Y}} c_i\alpha^{ie}\sum_{j=0}^{\infty}\alpha^{ij}a(\beta^j)x^j &= \sum_{i\in\mathcal{Y}} c_i\alpha^{ie}\sum_{j\in\mathcal{Z}}\frac{a_j}{1-x\alpha^i\beta^j} \\ &= \sum_{i\in\mathcal{Y}} c_i\alpha^{ie}\frac{\sum\limits_{j\in\mathcal{Z}}\Big(a_j\prod\limits_{\substack{\ell\in\mathcal{Z}\\ \ell\neq j}}(1-x\alpha^i\beta^\ell)\Big)}{\prod\limits_{j\in\mathcal{Z}}(1-x\alpha^i\beta^j)}. \qquad (4)\end{aligned}$$

Finally using (4) we can rewrite (3) of Definition 2 in the following form:

$$\frac{\sum\limits_{i\in\mathcal{Y}}\Big(c_i\alpha^{ie}\sum\limits_{j\in\mathcal{Z}}\Big(a_j\prod\limits_{\substack{\ell\in\mathcal{Z}\\ \ell\neq j}}(1-x\alpha^i\beta^\ell)\Big)\prod\limits_{\substack{m\in\mathcal{Y}\\ m\neq i}}\prod\limits_{s\in\mathcal{Z}}(1-x\alpha^m\beta^s)\Big)}{\prod\limits_{i\in\mathcal{Y}}\big(\prod\limits_{j\in\mathcal{Z}}(1-x\alpha^i\beta^j)\big)} \equiv 0 \bmod x^{\mu-1}, \qquad (5)$$

where the degree of the denominator is $|\mathcal{Y}|\cdot|\mathcal{Z}|$. The degree of the numerator is smaller than or equal to $(|\mathcal{Y}|-1)\cdot|\mathcal{Z}| + |\mathcal{Z}| - 1 = |\mathcal{Y}|\cdot|\mathcal{Z}| - 1$.

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 $\mathcal{C}(q; n, k, d)$ and its associated non-zero-locator code $\mathcal{L}(q_\ell; n_\ell, k_\ell, d_\ell)$ with $\gcd(n, n_\ell) = 1$ and the integer $\mu$ be given as in Definition 2. Then the minimum distance $d$ of $\mathcal{C}(q; n, k, d)$ satisfies the following inequality:*

$$d \geq d^* \stackrel{\text{def}}{=} \left\lceil \frac{\mu}{d_\ell} \right\rceil. \qquad (6)$$

*Proof.* For a codeword $c(x) \in \mathcal{C}(q; n, k, d)$ of weight $d$ and a codeword $a(x) \in \mathcal{L}(q_\ell; n_\ell, k_\ell, d_\ell)$ of weight $d_\ell$, the degree of the denominator in (5) 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 2** (Binary Code of length $n = 21$)**.** *Let us again consider the binary code $\mathcal{C}(2; 21, 7, 8)$ of Example 1. We have $\mu - 1 = 13$ according to Theorem 2, so $d^* = \lceil 14/2 \rceil = 7$.*

*The HT bound (Theorem 1) gives also $d \geq 6$ (with parameters $b_1 = 1$, $m_1 = 5$, $m_2 = 1$, $d_0 = 5$ and $\nu = 1$). The Roos bound gives $d \geq 8$ [11, Example 1], which is the actual minimum distance of $\mathcal{C}(2; 21, 7, 8)$.*

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

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

of length $\mu - 1$ as in Definition 2, such that $d^*$ of (6) is maximized.

# 4 Comparison to Known Bounds

## 4.1 The Hartmann–Tzeng Bound

We restate the HT bound as given in Theorem 1 to draw a connection to the bound given in Theorem 2. We multiply with the inverse of $m_1$ or $m_2$ modulo $n$, such that:

$$m > \nu + 1 \quad \text{for} \quad \{b_2 + i_1 m + i_2 : 0 \leq i_1 \leq d_0 - 2, 0 \leq i_2 \leq \nu\} \subseteq D_{\mathcal{C}} \tag{7}$$

with $\gcd(n, m) = 1$ for a given code $\mathcal{C}(q; n, k, d)$ holds.

Throughout this section, we refer to this representation of the HT bound. In the following subsection, we consider a single parity check code as non-zero-locator code and draw the connection to a particular case of the HT bound. The general case of (7) is considered in Subsection 4.3, where we use RS codes as non-zero-locator codes.

Some families of cyclic codes are identified in Subsection 4.4.

## 4.2 Single Parity Check Code as Non-Zero-Locator Code

Let $\mathcal{P}(n_\ell, n_\ell - 1, 2)$ denote a cyclic single parity check code of length $n_\ell$, dimension $n_\ell - 1$ and minimum distance 2 over an extension field $\mathbb{F}_{q_\ell}$ of $\mathbb{F}_q$. Let $\beta$ be a primitive $n_\ell$th root of unity in an extension field of $\mathbb{F}_{q_\ell}$. The generator polynomial $g(x)$ of $\mathcal{P}(n_\ell, n_\ell - 1, 2)$ is

$$g(x) = x - 1.$$

Furthermore, let a cyclic code $\mathcal{C}$ with defining set $D_{\mathcal{C}}$ be given, such that for the parameters $b_2 = 1$ and $m = \nu + 2$ the normalized HT bound of (7) holds. We illustrate the defining set $D_{\mathcal{P}} = \{0\}$ of $\mathcal{P}$ with length $n_\ell = \nu + 2$ and the defining set $D_{\mathcal{C}}$ in Table 2. The sequence is illustrated in terms

Table 2: Defining sets $D_{\mathcal{C}}$ of a given cyclic code $\mathcal{C}$ and $D_{\mathcal{P}}$ of its associated single parity check code $\mathcal{P}$ of length $n_\ell$ in the interval $[0, m(d_0 - 1)]$.

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $D_{\mathcal{C}}$ | □ | 1 | .. | $m$-1 | □ | $m$+1 | .. | $2m$-1 | □ | .. | $m(d_0$-1)-1 | □ |
| $D_{\mathcal{P}}$ | 0 | □ | .. | □ | 0 | □ | .. | □ | 0 | .. | □ | 0 |

of parameters of the HT bound (7). For this special case, the non-zero-locator code $\mathcal{L}(q_\ell; n_\ell, k_\ell, d_\ell)$ is a $\mathcal{P}(n_\ell, n_\ell - 1, 2)$ code. We have:

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

and we obtain a zero-sequence of length $\mu - 1 = m(d_0 - 1) + 1$. From Theorem 2 we obtain:

$$d^* = \left\lceil \frac{m(d_0 - 1) + 2}{2} \right\rceil = \left\lceil \frac{(\nu + 2)d_0 - \nu}{2} \right\rceil = \left\lceil d_0 + \frac{\nu(d_0 - 1)}{2} \right\rceil, \tag{8}$$

where we used $m = \nu + 2$. In Fig. 1 we illustrate $d^*$ of (8) for different parameters $\nu$ and $d_0$. For $d_0 \geq 4$ (independently from $\nu$) our bound improves the HT bound (see Proposition 1 in the next subsection). Note that for $\nu = 0$ the HT bound and our bound coincide with the BCH bound. Let us study the following example.

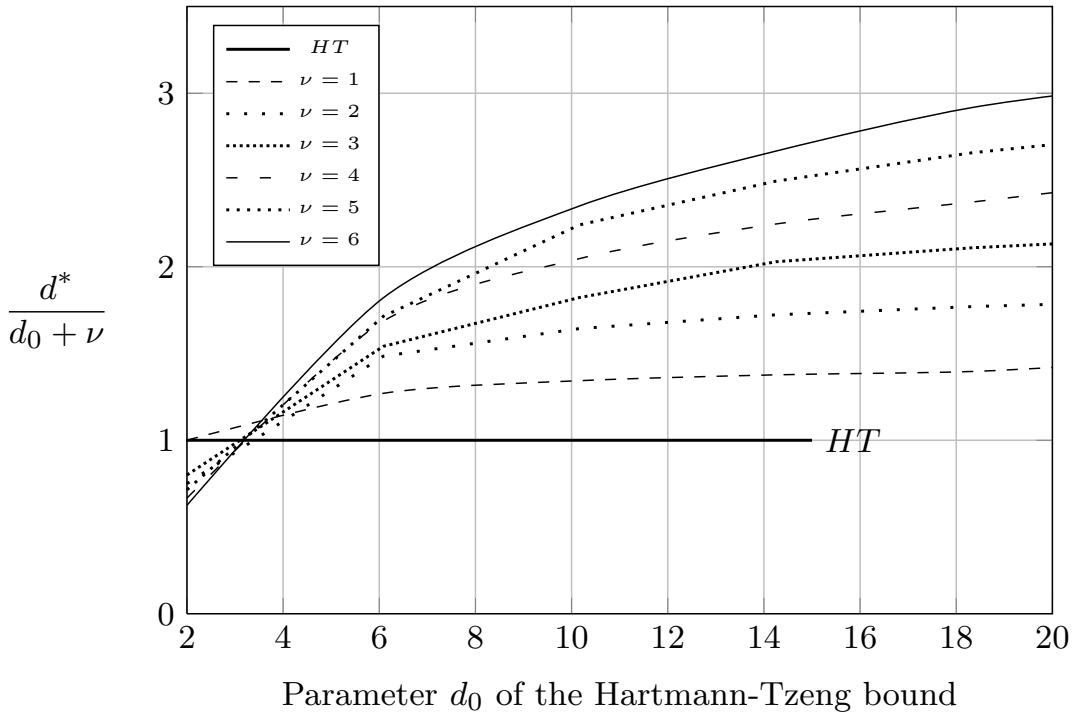


Figure 1: Illustration of the fraction $d^*/(d_0+\nu)$ of our bound $d^*$ of (9) to the Hartmann–Tzeng bound $d_0+\nu$ for $\nu = 1,\ldots,6$ and $d_0 = 2,\ldots,20$. The parameters of the HT bound are $m = \nu+2$ (see Table 2). We used a single parity check code as non-zero-locator code. Our bound $d^*$ is better than the HT bound for $d_0 > 3$.

**Example 3** (Parity Check Code as Non-Zero-Locator Code)**.** *Let us consider the binary reversible [12] cyclic code* $\mathcal{C}(2;65,41,8)$ *with the defining set* $D_{\mathcal{C}} = M_1^{(65)} \cup M_5^{(65)}$*. We know that*

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

*The HT bound gives a lower bound of* $d \geq 6$ *on the minimum distance of* $\mathcal{C}(2;65,41,8)$ *(for* $b_2 = -5$*,* $m = 3$*,* $d_0 = 5$ *and* $\nu = 1$*). We can associate the single parity check code* $\mathcal{P}$ *(3,2,2) over* $\mathbb{F}_{2^2}$ *with generator polynomial* $g(x) = x-1$ *as a non-zero-locator code for* $\mathcal{C}(2;65,41,8)$*. The defining sets* $D_{\mathcal{C}}$ *and* $D_{\mathcal{P}}$ *are shown in Table 3. With (8) we obtain for* $d^*$*:*

Table 3: Subset of the defining sets $D_{\mathcal{C}}$ of the $\mathcal{C}(2;65,41,8)$ code in the interval $[-6,6]$. The set $D_{\mathcal{P}}$ is the defining set of a single parity check code $\mathcal{P}$ of length $n_\ell = 3$ that is the associated non-zero-locator code.

| $D_{\mathcal{C}}$ | □ | -5 | -4 | □ | -2 | -1 | □ | 1 | 2 | □ | 4 | 5 | □ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $D_{\mathcal{P}}$ | 0 | □ | □ | 0 | □ | □ | 0 | □ | □ | 0 | □ | □ | 0 |

$$d^* = \left\lceil d_0 + \frac{\nu(d_0-1)}{2} \right\rceil = \left\lceil 5 + \frac{1(5-1)}{2} \right\rceil = 7.$$

*Furthermore, we can decode up to* $(d^*-1)/2 = 3$ *errors for* $\mathcal{C}(2;65,41,8)$ *(see Section 6).*

## 4.3 Cyclic Reed–Solomon Codes as Non-Zero-Locator Codes

Let a $q$-ary cyclic code $\mathcal{C}$ with defining set $D_{\mathcal{C}}$ be given such that for the parameters $b_2 = 1$ and $m > \nu+2$, the normalized Hartmann–Tzeng bound of (7) with $d_0 > 2$ and $\nu > 0$ holds. Let a

cyclic Reed–Solomon code $\mathcal{RS}(q_\ell; n_\ell, k_\ell; \delta)$ over an extension field $\mathbb{F}_{q_\ell}$ of $\mathbb{F}_q$ with

$$n_\ell = m, \quad k_\ell = \nu + 1, \quad d_\ell = m - \nu, \quad \delta = 0$$

as in Definition 1 be the associated non-zero-locator code.

Table 4 shows the defining set $D_\mathcal{C}$ and the defining set $D_{\mathcal{RS}}$ of $\mathcal{RS}(q_\ell; m, \nu + 1; 0)$.

Table 4: Defining sets $D_\mathcal{C}$ for $b_2 = 1$ and $m$ of the HT bound (7) and $D_{\mathcal{RS}}$ of the associated non-zero-locator code in the interval $[-(m-\nu)-1, m(d_0-1)]$.

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

The $n_\ell - (\nu+2) + 1 = m - \nu - 1$ consecutive zeros of the cyclic Reed–Solomon code $\mathcal{RS}(q_\ell; m, \nu + 1; 0)$ fill the missing zeros of the given cyclic code $\mathcal{C}(q; n, k, d)$. The obtained "zero"-sequence has length $\mu - 1 = m(d_0 - 1) + m - \nu - 1$. Therefore, we obtain from (6):

$$d^* = \left\lceil \frac{m(d_0-1) + m - \nu}{m - \nu} \right\rceil = \left\lceil \frac{md_0 - m + m - \nu}{m - \nu} \right\rceil = \left\lceil \frac{md_0 - \nu}{m - \nu} \right\rceil . \tag{9}$$

Note that for $m = \nu + 2$ the Reed–Solomon code is a single parity check code and we obtain the result from (8). Let us precise the cases where our bound $d^*$ is better than the Hartmann–Tzeng

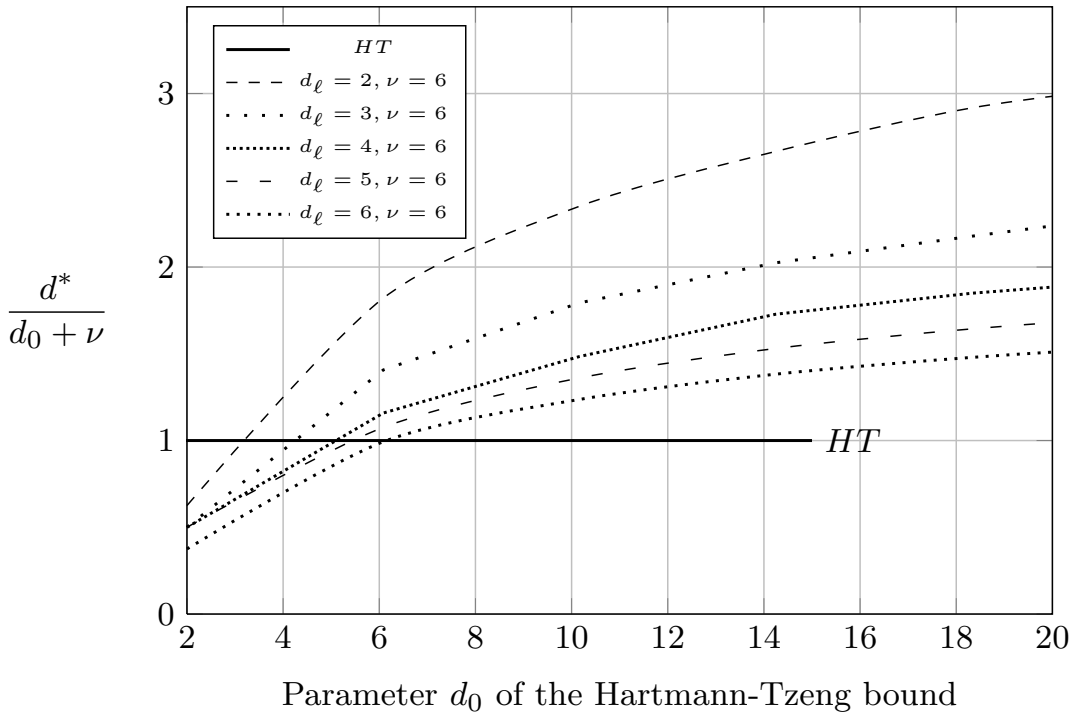


Figure 2: Illustration of the fraction $d^*/(d_0 + \nu)$ of our bound $d^*$ of (9) to the Hartmann–Tzeng bound $d_0 + \nu$ for $\nu = 6$, $d_0 = 2, \ldots, 20$ and $m$. We used an RS code as non-zero-locator code with minimum distance $d_\ell = m - \nu$ (see Table 4).

bound $d_0 + \nu$.

**Proposition 1.** *Let a $q$-ary cyclic code $\mathcal{C}(q; n, k, d)$ with a subset of its defining set $D_\mathcal{C}$ with parameters $b_2$, $m$, $d_0$ and $\nu$ as stated in Theorem 1 be given. Let $\mathcal{L}(q_\ell; m, \nu + 1, m - \nu) =$*

$\mathcal{RS}(q_\ell; m, \nu+1; 0)$ *be the associated non-zero-locator code as in Definition 3 with* $\mu = m(d_0-1)+m-\nu$. *Then for*

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

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

*Proof.* From (9) we have

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

Obviously, for $d^* > d_0 + \nu$, we require that

$$\frac{(d_0-1)\nu}{m-\nu} > \nu \iff d_0 > m - \nu + 1.$$

□

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 minimum distance of the associated RS code $d_\ell = m - \nu$ varies between two and six, are illustrated in Fig. 2.

## 4.4 Some Families of Cyclic Codes and Their Connection to Other Bounds

We identify some families of cyclic codes and refine our bound on the minimum distance of Theorem 2. The classification is done by means of the associated non-zero-locator code. For all codes, we can decode up to $\lfloor (d^*-1)/2 \rfloor$ errors (see Section 6).

### Single Parity Check Code as Non-Zero-Locator Code

Let the defining set $D_\mathcal{C}$ of a given $q$-ary cyclic code $\mathcal{C}(q; n, k, d)$ contain the elements as shown in Table 5. Furthermore, let $\gcd(n, 3) = 1$. We associate a single parity check code $\mathcal{P}(3, 2, 2)$ and

Table 5: Subset of the defining sets $D_\mathcal{C}$ of a given cyclic code $\mathcal{C}$ in the interval $[-10, 10]$. The set $D_\mathcal{L} = \{0\}$ is the defining set of the single parity check code $\mathcal{L}(2; 3, 2, 2)$.

| $D_\mathcal{C}$ | -10 | □ | -8 | -7 | □ | -5 | -4 | □ | -2 | -1 | □ | 1 | 2 | □ | 4 | 5 | □ | 7 | 8 | □ | 10 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $D_\mathcal{L}$ | □ | 0 | □ | □ | 0 | □ | □ | 0 | □ | □ | 0 | □ | □ | 0 | □ | □ | 0 | □ | □ | 0 | □ |

obtain $\mu = 22$ and therefore $d \geq d^* = 11$.

For binary reversible cyclic codes [12,19] we require only $\{1, 5, 7\}$ to be a subset of the defining set since the other elements are then included automatically.

If the binary cyclic code is not reversible, the defining set has to contain $\{-7, -5, -1, 1, 5, 7\}$. This requirement coincides with the 5-error-correcting pair of [4, Proposition 8]. The codes of [4, Proposition 7, Example 21 and 22] require a smaller subset of their defining set $D_\mathcal{C}$. For these codes, we obtain the same bound on the minimum distance of $\mathcal{C}$.

### Binary Hamming Code as Non-Zero-Locator Code

Let the defining set $D_\mathcal{C}$ of a given binary cyclic code $\mathcal{C}(2; n, k, d)$ contain the elements as shown in Table 6. Furthermore, let $\gcd(n, 7) = 1$.

We associate the binary Hamming code $\mathcal{L}(2; 7, 4, 3)$ with defining set $D_\mathcal{L} = \{3, 5, 6\}$. As shown in Table 6, we obtain $\mu = 21$ and therefore $d \geq d^* = 7$.

For binary cyclic codes we require $\{1, 7, 9, 11, 15\}$ to be a subset of the defining set $D_\mathcal{C}$.

Table 6: Subset of the defining sets $D_{\mathcal{C}}$ of a given cyclic code $\mathcal{C}$ in the interval $[1, 20]$. The set $D_{\mathcal{L}} = \{3, 5, 6\}$ is the defining set of the binary Hamming code $\mathcal{L}(2; 7, 4, 3)$.

| $D_{\mathcal{C}}$ | 1 | 2 | □ | 4 | □ | □ | 7 | 8 | 9 | □ | 11 | □ | □ | 14 | 15 | 16 | □ | 18 | □ | □ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $D_{\mathcal{L}}$ | □ | □ | 3 | □ | 5 | 6 | □ | □ | □ | 3 | □ | 5 | 6 | □ | □ | □ | 3 | □ | 5 | 6 |

### Reed–Solomon Code as Non-Zero-Locator Code

Let the defining set $D_{\mathcal{C}}$ of a given $q$-ary cyclic code $\mathcal{C}(q; n, k, d)$ contain the elements as shown in Table 7. Furthermore, let $\gcd(n, 4) = 1$. We associate an RS code $\mathcal{RS}(q_\ell; 4, 2; \delta = 0)$ over $\mathbb{F}_{q_\ell}$

Table 7: Subset of the defining sets $D_{\mathcal{C}}$ of a given cyclic code $\mathcal{C}$ in the interval $[-17, 17]$ (only odd indexes are illustrated). The set $D_{\mathcal{L}} = \{0, 1\}$ is the defining set of a Reed–Solomon code $\mathcal{RS}(q_\ell; 4, 2; 0)$.

| $D_{\mathcal{C}}$ | □ | □ | -13 | -11 | □ | □ | -5 | -3 | □ | □ | 3 | 5 | □ | □ | 11 | 13 | □ | □ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $D_{\mathcal{RS}}$ | 0 | 1 | □ | □ | 0 | 1 | □ | □ | 0 | 1 | □ | □ | 0 | 1 | □ | □ | 0 | 1 |

which is an extension field of $\mathbb{F}_q$ and consider the sequence

$$c(\alpha^{-17})a(\beta^0), c(\alpha^{-17+2})a(\beta^1), c(\alpha^{-17+4})a(\beta^2), \ldots, c(\alpha^{-17+(\mu-2)\cdot 2})a(\beta^{\mu-2}).$$

We have $\mu = 19$ and with $d_\ell = 3$, we obtain $d \geq d^* = 7$.

For binary reversible cyclic codes, we require $\{3, 5, 11, 13\}$ to be a subset of the defining set $D_{\mathcal{C}}$. Further families can be found in [17] and can be seen as special case of this approach.

As previously seen, we identified cyclic codes by means of their potential non-zero-locator codes. To obtain a huge family of cyclic codes, the cardinality of the required subset of their defining set should be small. This implies a high cardinality of the defining set $|D_{\mathcal{L}}|$ of the associated non-zero-locator code $\mathcal{L}(q_\ell; n_\ell, k_\ell, d_\ell)$. Both leads to a long zero-sequence

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

On the one hand, we need a low code-rate $k_\ell/n_\ell$ which implies a high $|D_{\mathcal{L}}|$. On the other hand, the minimum distance $d_\ell$ of $\mathcal{L}$ should be small to obtain a good bound $d^*$ according to (6).

This motivates the investigation of small-minimum-distance cyclic codes with lowest code-rate. In a first step, we consider binary cyclic codes with minimum distance two and three.

# 5 Binary Cyclic Codes with Minimum Distance Two and Three as Non-Zero-Locator Code

## 5.1 General Idea

As mentioned in Section 3, good candidates for non-zero-locator codes are cyclic codes with small minimum distance and lowest code-rate $k_\ell/n_\ell$. We consider binary cyclic codes with minimum distance two and three and lowest code-rate and show their defining set.

Primitive binary cyclic codes with minimum distance three were investigated by Charpin, Tietäväinen and Zinoviev in [2, 3]. We generalize the results of [2] to binary cyclic codes of arbitrary length and show afterwards the implications, when we want to use them as non-zero-locator codes.

**Lemma 1.** *[2] Let $i, j$ with $0 \leq i < j \leq n-1$ be two arbitrary integers that do not belong to the same cyclotomic coset modulo $n$. Then the binary cyclic code $\mathcal{C}(2; n, k, d)$ with generator polynomial $g(x) = M_i^{(n)}(x) \cdot M_j^{(n)}(x)$ has minimum distance two if and only if* $\gcd(n, i, j) > 1$.

*Proof.* Let $\alpha$ be an $n$th root of unity. A binary cyclic code $\mathcal{C}$ with generator polynomial $g(x) = M_i^{(n)}(x) \cdot M_j^{(n)}(x)$ of length $n$ has minimum distance two if there exist a binomial $c(x) = x^k + x^\ell$ that fulfills

$$c(\alpha^i) = c(\alpha^j) = 0.$$

This holds, if and only if

$$\alpha^{ki} = \alpha^{\ell i} \quad \text{and} \quad \alpha^{kj} = \alpha^{\ell j}$$

or, equivalently,

$$(k-\ell)i \equiv (k-\ell)j \equiv 0 \mod n.$$

Both congruences are valid if and only if $n/\gcd(n, i, j)$ divides $k-\ell$. Therefore, such $k$ and $\ell$ exist if and only if $\gcd(n, i, j) > 1$. □

**Theorem 3** (Binary Cyclic Codes with Minimum Distance Two [2])**.** *Let $i_1, i_2, \ldots, i_s$ with $0 \leq i_1 < \cdots < i_s \leq n-1$ be $s$ arbitrary integers that do not belong to the same cyclotomic coset modulo $n$. Then the binary cyclic code $\mathcal{C}(2; n, k, d)$ with generator polynomial*

$$g(x) = \prod_{j=1}^{s} M_{i_j}^{(n)}(x)$$

*has minimum distance two if and only if* $\gcd(n, i_1, \ldots, i_s) > 1$.

We skip the proof of Theorem 3, because it is straightforward to the proof of Lemma 1.

The following lemma is a generalization of [2, Theorem 1] to binary cyclic codes of arbitrary length.

**Lemma 2** (Binary Cyclic Codes with Minimum Distance Three)**.** *Let $i, j$ with $0 \leq i < j \leq n-1$ be arbitrary integers that do not belong to the same cyclotomic coset modulo $n$. Let $g$ be such that $2^g - 1$ divides $n$. If there exists an integer $r$ with $0 < r < 2^g - 1$, where* $\gcd(r, 2^g - 1) = 1$*, such that both $i$ and $j$ are in $M_r^{(2^g-1)}$, then the binary cyclic code $\mathcal{C}(2; n, k, d)$ with generator polynomial $g(x) = M_i^{(n)}(x) \cdot M_j^{(n)}(x)$ has minimum distance $d \leq 3$. If, moreover,* $\gcd(n, i, j) = 1$*, then $d = 3$.*

*Proof.* Let $\gamma$ be a primitive element of $\mathbb{F}_{2^s}$, let $z = (2^s - 1)/n$ and let $\alpha = \gamma^z$. Let $u = n/(2^g - 1)$, then $\beta = \alpha^u = \gamma^{(2^s-1)/(2^g-1)}$, is a primitive element of $\mathbb{F}_{2^g}$. Let $b$ be an integer in the interval $[1, 2^g - 2]$ such that:

$$1 + \beta + \beta^b = 0.$$

Define

$$c(x) = 1 + x^{u(1/r)} + x^{u(b/r)},$$

where the quotients $1/r$ and $b/r$ are calculated in the ring $\mathbb{Z}_{2^g-1}$ of integers modulo $2^g - 1$. For $i \in M_r^{(2^g-1)}$, two non-negative integers $k$ and $\ell$ exist such that

$$i = \ell(2^g - 1) + 2^k r.$$

Thus,

$$\begin{aligned} c(\alpha^i) &= 1 + \alpha^{ui(1/r)} + \alpha^{ui(b/r)} \\ &= 1 + \beta^{i(1/r)} + \beta^{i(b/r)} \\ &= 1 + \beta^{2^k r(1/r)} + \beta^{2^k r(b/r)} \\ &= 1 + \beta^{2^k} + \beta^{b2^k} \\ &= (1 + \beta + \beta^b)^{2^k} = 0. \end{aligned}$$

□

Note that in [2] the length of the cyclic code was $n = 2^s - 1$ and $u = (2^s - 1)/(2^g - 1)$.

**Corollary 1.** *Let $\mathcal{C}$ be a binary cyclic code of length $n$. If there exist no $g$, s.t. $(2^g - 1) \mid n$, then $\mathcal{C}$ cannot have minimum distance three.*

**Theorem 4** (Binary Cyclic Codes with Minimum Distance Three)**.** *Let $i_1, i_2, \ldots, i_s$ with $0 \leq i_1 < \cdots < i_s \leq n - 1$ be $s$ arbitrary integers that do not belong to the same cyclotomic coset modulo $n$. Let $g$ be such that $2^g - 1$ divides $n$. If there exists an integer $r$ with $0 < r < 2^g - 1$, where $\gcd(r, 2^g - 1) = 1$, such that all $s$ integers $i_1, i_2, \ldots, i_s$ are in $M_r^{(2^g-1)}$, then the binary cyclic code $\mathcal{C}(2; n, k, d)$ with generator polynomial*

$$g(x) = \prod_{j=1}^{s} M_{i_j}^{(n)}(x)$$

*has minimum distance $d \leq 3$. If, moreover, $\gcd(n, i_1, \ldots, i_s) = 1$, then $d = 3$.*

We skip the proof of Theorem 4, because it is straightforward to the proof of Lemma 2.

Let us consider a non-primitive binary cyclic code with minimum distance three.

**Example 4** (Non-primitive Binary Cyclic Code with Minimum Distance Three)**.** *Let $n = 119 = (2^3 - 1) \cdot 17$. In this case $g = 3$ (see Theorem 4). Then $\{1, 11, 51\}$ belong to $M_1^{(7)}$ and we have $\gcd(1, 11, 51) = 1$. Therefore the binary cyclic code of length $n = 119$ with generator polynomial*

$$g(x) = M_1^{(119)}(x) \cdot M_{11}^{(119)}(x) \cdot M_{51}^{(119)}(x),$$

*has dimension $k = 68$ and minimum distance $d = 3$.*

## 5.2 Implications for the Non-Zero-Locator Code

We consider lowest-code-rate binary cyclic codes of minimum distance two and three. They are good candidates for non-zero-locator codes.

We first consider lowest-code-rate binary cyclic codes of minimum distance two.

**Proposition 2** (Lowest-Code-Rate Binary Cyclic Codes With Minimum Distance Two)**.** *Let $a > 1$, $g > 1$ and $n$ be three integers, such that $n = ag$. Let $g$ be in the defining set $D_{\mathcal{C}}$. Then the binary cyclic code $\mathcal{C}(2; n, k, 2)$ of length $n$ with defining set:*

$$D_{\mathcal{C}} = \{0, \square, \ldots, \square, g, \square, \ldots, \square, 2g, \square, \ldots, \square, (a-1)g, \square, \ldots, \square\}$$

*is the binary cyclic code of smallest dimension $k = a(g - 1)$, lowest code-rate $R = (g - 1)/g$ and minimum distance two.*

*Proof.* We want to maximize $|D_{\mathcal{C}}|$ while keeping $d$ of $\mathcal{C}$ at two. Therefore, we select for a given $g$ every cyclotomic coset $M_i^{(n)}$ with $\gcd(i,g) > 1$ for all $i = 0,\ldots,n-1$ to be in $D_{\mathcal{C}}$ with aimed minimum distance two. One the one hand, this guarantees the maximization of $|D_{\mathcal{C}}|$ and therefore the minimization of the code-rate. On the other hand, due to the condition $\gcd(i,g) > 1$ (Theorem 3) the minimum distance of $\mathcal{C}$ remains two. □

A direct consequence of Proposition 2 is that we do not need to investigate these binary cyclic codes of minimum distance two any more. We obtain the same result when we select a parity check code $\mathcal{P}(g, g-1, 2)$ as non-zero-locator code.

**Proposition 3** (Lowest-Code-Rate Binary Cyclic Codes With Minimum Distance Three)**.** *Let $a > 1$, $g > 1$ and $n$ be three integers, such that $n = a(2^g-1)$. Let $r$ be an integer with $0 < r < 2^g-1$, where $\gcd(r, 2^g-1) = 1$. Let $r$ be in the defining set $D_{\mathcal{C}}$. Then the binary cyclic code $\mathcal{C}(2; n, k, 3)$ of length $n$ with defining set:*

$$D_{\mathcal{C}} = \{r \cdot i \mod n \mid i = j(2^g-1)+1, j(2^g-1)+2, j(2^g-1)+4, \ldots, j(2^g-1)+2^{g-1} \quad \forall j = 0,\ldots,a-1\} \tag{10}$$

*is the binary cyclic code with the smallest dimension $k = a(2^g-1-g)$, lowest code-rate $R = (2^g-1-g)/(2^g-1)$ and minimum distance three.*

*Proof.* We want to maximize $|D_{\mathcal{C}}|$ while keeping $d$ of $\mathcal{C}$ at three. For a given $r$ and for $(2^g-1)|n$, we select every cyclotomic coset $M_i^{(n)}$ for all $i = 0,\ldots,n-1$ to be in the $D_{\mathcal{C}}$ of $\mathcal{C}$ with aimed minimum distance three, such that $i \in M_r^{(2^g-1)}$. One the one hand, this guarantees the maximization of $|D_{\mathcal{C}}|$ and therefore the minimization of the code-rate. On the other hand, due to the condition that $M_i^{(n)}$ should be selected such that $i \in M_r^{(2^g-1)}$ (Theorem 4) the minimum distance of $\mathcal{C}$ remains three. □

**Remark 2.** *Let $r = 1$ in Proposition 3. Then $M_1^{(2^g-1)} = \{1, 2, 4, \ldots, 2^{g-1}\}$ is the cyclotomic coset of a binary Hamming code of length $2^g-1$. The defining set of the corresponding lowest-code-rate binary cyclic code is a repetition of the defining set of the Hamming code of length $2^g-1$.*

**Example 5** (Non-primitive Binary Cyclic Code with Minimum Distance Three and Lowest Code-Rate)**.** *Let us again consider Example 4 with $n = 119 = (2^3-1)\cdot 17$ and $k = 68$. The binary cyclic code of length $n = 119$ with generator polynomial $g(x) = M_1^{(119)}(x) \cdot M_{11}^{(119)}(x) \cdot M_{51}^{(119)}(x)$ and with minimum distance three has lowest code-rate $R = (2^3-1-3)/(2^3-1) = 68/119$. Its defining set $D_{\mathcal{C}}$ is:*

$$D_{\mathcal{C}} = \{\square, 1, 2, \square, 4, \square, \square, \,|\, \square, 8, 9, \square, 11, \square, \square, \,|\, \square, 15, 16, \square, 18, \square, \square, \,|\, \square, 22, \ldots, 116, \square, \square\}.$$

A consequence of Proposition 3 is that we do not need to investigate any binary cyclic code of minimum distance three any more. We obtain the same result when we take a primitive binary cyclic code with minimum distance three as non-zero-locator code.

# 6 Syndrome-Based Decoding of up to $\lfloor (d^*-1)/2 \rfloor$ Errors

## 6.1 Syndrome Definition

Let a $q$-ary cyclic code $\mathcal{C}(q; n, k, d)$ and its associated $q_\ell$-ary non-zero-locator code $\mathcal{L}(q_\ell; n_\ell, k_\ell, d_\ell)$ with $\gcd(n, n_\ell) = 1$ and the integers $\mu$ and $e$ be given as in Definition 2. Let $\mathbb{F}_{q_\ell} = \mathbb{F}_{q^u}$ be an extension field of $\mathbb{F}_q$. Let $\alpha \in \mathbb{F}_{q^s}$ be a primitive $n$th and let $\beta \in \mathbb{F}_{q_\ell^{s_\ell}}$ be a primitive $n_\ell$th root of

unity. Let $r$ denote the least common multiple of $s$ and $u \cdot s_\ell$. Let $a(x) = \sum_{i\in\mathcal{Z}} a_i x^i$ be a codeword of $\mathcal{L}$ of weight $|\mathcal{Z}| = d_\ell$.

Let the set $\mathcal{E} = \{i_0, i_1, \ldots, i_{t-1}\}$ with cardinality $|\mathcal{E}| = t$ be the set of error positions. The corresponding error polynomial is denoted by $e(x) = \sum_{i\in\mathcal{E}} e_i x^i$. Let the received polynomial be $r(x) = \sum_{i=0}^{n-1} r_i x^i = e(x) + c(x)$.

We define a syndrome polynomial $S(x) \in \mathbb{F}_{q^r}[x]$ as follows:

$$S(x) \stackrel{\text{def}}{=} \sum_{j=0}^{\infty} r(\alpha^{j+e}) a(\beta^j) x^j \mod x^{\mu-1}. \tag{11}$$

Thus, the coefficients $S_j \in \mathbb{F}_{q^r}$ of the above defined syndrome polynomial $S(x) = \sum_{j=0}^{\mu-2} S_j x^j$ are given by

$$S_j = \sum_{i=0}^{n-1} r_i \alpha^{i(j+e)} \cdot \sum_{h=0}^{n_\ell-1} a_h \beta^{hj}, \quad \forall j = 0, \ldots, \mu-2.$$

From Definition 2 we know that the syndrome polynomial $S(x)$ of (11) is independent of the codeword $c(x)$. Now, we can do the same reformulation of the syndrome expression as we did in Section 3 for the codeword $c(x)$ and $a(x)$. We have from (11):

$$\begin{aligned}\sum_{j=0}^{\infty} r(\alpha^{j+e}) a(\beta^j) x^j &\equiv \sum_{j=0}^{\infty} e(\alpha^{j+e}) a(\beta^j) x^j \mod x^{\mu-1} \\ &\equiv \sum_{j=0}^{\infty} \sum_{i\in\mathcal{E}} e_i \alpha^{i(j+e)} a(\beta^j) x^j \mod x^{\mu-1},\end{aligned}$$

and with (2) for $a(x) = \sum_{i\in\mathcal{Z}} a_i x^i$ we can write:

$$\begin{aligned}S(x) &\equiv \sum_{i\in\mathcal{E}} e_i \alpha^{ie} \sum_{j\in\mathcal{Z}} \frac{a_j}{1 - x\alpha^i\beta^j} \mod x^{\mu-1} \\ &\equiv \sum_{i\in\mathcal{E}} e_i \alpha^{ie} \frac{\sum\limits_{j\in\mathcal{Z}} \Big( a_j \prod\limits_{\substack{\ell\in\mathcal{Z}\\ \ell\neq j}} (1 - x\alpha^i\beta^\ell) \Big)}{\prod\limits_{j\in\mathcal{Z}} \big(1 - x\alpha^i\beta^j\big)} \mod x^{\mu-1}.\end{aligned}$$

Finally, we can write for $S(x)$:

$$S(x) \equiv \frac{\sum\limits_{i\in\mathcal{E}} \Big( e_i \alpha^{ie} \sum\limits_{j\in\mathcal{Z}} \Big( a_j \prod\limits_{\substack{\ell\in\mathcal{Z}\\ \ell\neq j}} (1 - x\alpha^i\beta^\ell) \Big) \prod\limits_{\substack{m\in\mathcal{E}\\ m\neq i}} \prod\limits_{s\in\mathcal{Z}} (1 - x\alpha^m\beta^s) \Big)}{\prod\limits_{i\in\mathcal{E}} \Big( \prod\limits_{j\in\mathcal{Z}} \big(1 - x\alpha^i\beta^j\big) \Big)} \mod x^{\mu-1}. \tag{12}$$

We use this explicit syndrome representation in the next section, where we define an error-locator and an error-evaluator polynomial.

## 6.2 Key Equation

To simplify the notation, let the two polynomials $f(x)$ and $h(x) \in \mathbb{F}_{q^r}[x]$ be defined as follows:

$$f(x) \stackrel{\text{def}}{=} \prod_{j\in\mathcal{Z}} \big(1 - x\beta^j\big), \tag{13}$$

$$h(x) \stackrel{\text{def}}{=} \sum_{j\in\mathcal{Z}} \big( a_j \prod_{\substack{\ell\in\mathcal{Z}\\ \ell\neq j}} (1 - x\beta^\ell) \big). \tag{14}$$

Due to $\gcd(n, n_\ell) = 1$ we have $\gcd(f(x\alpha^i), f(x\alpha^j)) = 1, \forall i \neq j$ (for the proof, see Lemma 3 in the Appendix) and therefore each of the $n$ polynomials $f(x\alpha^0)$, $f(x\alpha^1)$, $\ldots$, $f(x\alpha^{n-1})$ can be identified by one root. Let $\kappa \in \mathcal{Z}$. Then, we have $f(\beta^{-\kappa}) = 0$. Furthermore, let $n$ distinct roots $\gamma_0, \gamma_1, \ldots, \gamma_{n-1}$ be defined as:

$$\gamma_i \stackrel{\text{def}}{=} \beta^{-\kappa}\alpha^{-i}, \quad i = 0, \ldots, n-1. \tag{15}$$

Then, each $\gamma_i$ is a root of $f(x\alpha^i)$. Note that each polynomial $f(x\alpha^i)$ has $|\mathcal{Z}| = d_\ell$ roots, but we need only one of them.

Now, we can define an error-locator polynomial $\Lambda(x) \in \mathbb{F}_{q^r}[x]$ as:

$$\Lambda(x) \stackrel{\text{def}}{=} \prod_{i \in \mathcal{E}} f(x\alpha^i). \tag{16}$$

The roots $\gamma_i$ of $\Lambda(x)$ from (15) tell us where the errors are. The corresponding error-evaluator polynomial $\Omega(x) \in \mathbb{F}_{q^r}[x]$ is defined as:

$$\Omega(x) \stackrel{\text{def}}{=} \sum_{i \in \mathcal{E}} \Big( e_i \alpha^{ie} h(x\alpha^i) \prod_{\substack{\ell \in \mathcal{E} \\ \ell \neq i}} f(x\alpha^\ell) \Big). \tag{17}$$

We relate the syndrome definition of (12), the error-locator polynomial $\Lambda(x)$ of (16) and the error-evaluator polynomial $\Omega(x)$ of (17) in form of a *Key Equation*:

$$\begin{gathered} S(x) \equiv \frac{\Omega(x)}{\Lambda(x)} \mod x^{\mu-1}, \text{ with} \\ \deg \Lambda(x) = t \cdot d_\ell, \quad \deg \Omega(x) \leq t \cdot d_\ell - 1 < \deg \Lambda(x). \end{gathered} \tag{18}$$

Solving (18) is similar to the decoding of [16] and we will not go into details. The Extended Euclidean Algorithm (EEA, [16]) with input polynomial $S(x)$ as defined in (11) and the monomial $x^{\mu-1}$ and an adapted stopping rule can be used to solve (18) and we obtain $\Lambda(x)$ and $\Omega(x)$.

## 6.3 Error Evaluation: A Generalized Forney's Formula

To determine the $t$ error values $e_{i_0}, e_{i_1}, \ldots, e_{i_{t-1}}$ from the error-locator polynomial $\Lambda(x)$ and error-locator polynomial $\Omega(x)$, we develop an explicit expression of the error-values (like Forney's formula [6]) in the following.

**Proposition 4.** *(Error Evaluation) Let a $q$-ary cyclic code $\mathcal{C}(q; n, k, d)$ and its associated non-zero-locator code $\mathcal{L}(q_\ell; n_\ell, k_\ell, d_\ell)$ with $\gcd(n, n_\ell) = 1$ and the integers $\mu$ and $e$ be given as in Definition 2. Let $\alpha \in \mathbb{F}_{q^s}$ be a primitive $n$th and let $\beta \in \mathbb{F}_{q^{u \cdot s_\ell}}$ be a primitive $n_\ell$th root of unity. Let $r$ be the least common multiple of $s$ and $u \cdot s_\ell$.*

*Furthermore, let $\gamma_0, \gamma_1, \ldots, \gamma_{n-1}$ be given as in (15) and let two polynomials $\Lambda(x)$ and $\Omega(x) \in \mathbb{F}_{q^r}[x]$ be given as in (16) and (17). Then the error values $e_i$ for all $i \in \mathcal{E}$ are:*

$$\begin{aligned} e_i &= \frac{\Omega(\gamma_i)}{\alpha^{ie} \cdot h(\gamma_i \alpha^i) \cdot \prod\limits_{\substack{\ell \in \mathcal{E} \\ \ell \neq i}} f(\gamma_i \alpha^\ell)} \\ &= \frac{\Omega(\gamma_i) \cdot f'(\gamma_i \alpha^i)}{\Lambda'(\gamma_i) \cdot \alpha^{ie} \cdot h(\gamma_i \alpha^i)}. \end{aligned} \tag{19}$$

*Proof.* The error-evaluator polynomial $\Omega(x)$ of (17) evaluated at $\gamma_i$ is explicitly

$$\Omega(\gamma_i) = e_i \cdot \alpha^{ie} \cdot h(\gamma_i \alpha^i) \prod_{\substack{\ell \in \mathcal{E} \\ \ell \neq i}} f(\gamma_i \alpha^\ell).$$

The derivative $\Lambda'(x)$ of the error-locator polynomial is

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

Its evaluation at $\gamma_i$ simplifies to

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

□

Note that the classical decoding up to the half the BCH bound of a cyclic code $\mathcal{C}$ corresponds to the case where the associated non-zero-locator code $\mathcal{L}$ is the set of all vectors of length $n_\ell = k_\ell$ over $\mathbb{F}_{q_\ell}$. The zero-sequence of length $\mu - 1$ is the longest set of consecutive zeros of $\mathcal{C}$. Then we can choose $a(x) = 1$ and we obtain the classical syndrome definition, key equation and Forney's formula.

# 7 Conclusion and Outlook

We presented a new technique that uses low-rate cyclic codes with small minimum distances — so-called non-zero-locator codes — to bound the minimum distance of $q$-ary cyclic codes. The algebraic description gives a generalized Key Equation and allows an efficient decoding. We derived some properties of binary cyclic codes of minimum distance two and three and lowest code-rate.

Future work is to find lowest-code-rate small-minimum-distance non-binary cyclic codes and relate them to our method and bound the minimum distance of other cyclic codes. Combined error-erasure decoding with our proposed method seems to be possible.


### Acknowledgments

We thank the anonymous referees for valuable comments that improved the presentation of this paper.

The authors wish to thank Antonia Wachter-Zeh and Daniel Augot for fruitful discussions. This work has been supported by German Research Council "Deutsche Forschungsgemeinschaft" (DFG) under grant BO 867/22-1.


# Appendix

**Lemma 3** (Coprimality of $n$ and $n_\ell$)**.** *Let $[n]$ denote the set of integers $\{0, 1, \ldots, n-1\}$ and let $\mathcal{Z}$ be a subset of $[n_\ell]$. Let $\alpha$ be an element of order $n$ in $\mathbb{F}_{q^s}$ and let $\beta$ denote a primitive element of order $n_\ell$ in $\mathbb{F}_{q_\ell^{s_\ell}}$, where $\mathbb{F}_{q_\ell} = \mathbb{F}_{q^u}$. Let $r$ denote the least common multiple of $s$ and $u \cdot s_\ell$ and*

*let $\gamma$ be a primitive element in $\mathbb{F}_{q^r}$. Let $N = q^r - 1$. Then $\alpha = \gamma^{N/n}$ and $\beta = \gamma^{N/n_\ell}$. We consider univariate polynomials in $\mathbb{F}_{q^r}[x]$. If $\gcd(n, n_\ell) = 1$ then*

$$\gcd\Big(\prod_{m\in\mathcal{Z}}(1 - x\alpha^i\beta^m), \prod_{m\in\mathcal{Z}}(1 - x\alpha^j\beta^m)\Big) = 1 \tag{20}$$

*holds $\forall i, j \in [n]$ with $i \neq j$.*

*Proof.* We show that the contrary does not hold. If (20) does not hold, then there exist a $i$ and $j$ with $i > j$ and $m, m' \in \mathcal{Z}$ with $m \neq m'$ such that

$$\begin{aligned} \alpha^i\beta^m &= \alpha^j\beta^{m'} \\ \alpha^{i-j} &= \beta^{m'-m} \end{aligned} \tag{21}$$

holds. Let us express (21) in terms of $\gamma$. We obtain:

$$\begin{aligned} \gamma^{\frac{N}{n}(i-j)} &= \gamma^{\frac{N}{n_\ell}(m'-m)} \\ \gamma^{\frac{N}{n\cdot n_\ell}\left((i-j)n_\ell-(m'-m)n\right)} &= 1 \\ \Rightarrow (i-j)n_\ell - (m'-m)n &= \lambda\cdot n\cdot n_\ell. \end{aligned}$$

We know that $i - j$ is smaller than $n$ and $m' - m$ is smaller than $n_\ell$. This implies that $\lambda$ is zero. We have:

$$\begin{aligned} (i-j)n_\ell &= (m'-m)n \\ \Rightarrow n_\ell &| (m'-m)n \end{aligned}$$

But $(m' - m) < n_\ell$ and this implies that $\gcd(n, n_\ell) \neq 1$. □

# References


[1] Bose, R.C., Chaudhuri, D.K.R.: On a class of error correcting binary group codes. Information and Control **3**(1), 68–79 (1960) 2, 3

[2] Charpin, P., Tietäväinen, A., Zinoviev, V.: On Binary Cyclic Codes with Minimum Distance $d = 3$. Problems of Information Transmission **33**(4), 287–296 (1997) 10, 11, 12

[3] Charpin, P., Tietäväinen, A., Zinoviev, V.: On the Minimum Distances of Non-Binary Cyclic Codes. Designs, Codes and Cryptography **17**, 81–85 (1999) 10

[4] Duursma, I.M., Koetter, R.: Error-locating pairs for cyclic codes. IEEE Transactions on Information Theory **40**(4), 1108–1121 (2002) 9

[5] Feng, G.L., Tzeng, K.K.: Decoding cyclic and BCH codes up to actual minimum distance using nonrecurrent syndrome dependence relations. IEEE Transactions on Information Theory **37**(6), 1716–1723 (1991) 3

[6] Forney, G.: On decoding BCH codes. IEEE Transactions on Information Theory **11**(4), 549–557 (1965) 15

[7] Hartmann, C.: Decoding beyond the BCH bound. IEEE Transactions on Information Theory **18**(3), 441–444 (1972) 2

[8] Hartmann, C., Tzeng, K.: Generalizations of the BCH bound. Information and Control **20**(5), 489–498 (1972) 2, 3

[9] Hartmann, C., Tzeng, K.: Decoding beyond the BCH bound using multiple sets of syndrome sequences. IEEE Transactions on Information Theory **20**(2) (1974) 2

[10] Hocquenghem, A.: Codes Correcteurs d'Erreurs. Chiffres (Paris) **2**, 147–156 (1959) 2, 3

[11] van Lint, J., Wilson, R.: On the Minimum Distance of Cyclic Codes. IEEE Transactions on Information Theory **32**(1), 23–40 (1986) 2, 3, 4, 5

[12] Massey, J.: Reversible Codes. Information and Control **7**(3), 369–380 (1964) 7, 9

[13] Reed, I.S., Solomon, G.: Polynomial Codes Over Certain Finite Fields. Journal of the Society for Industrial and Applied Mathematics **8**(2), 300–304 (1960) 3

[14] Roos, C.: A generalization of the BCH bound for cyclic codes, including the Hartmann-Tzeng bound. Journal of Combinatorial Theory, Series A **33**(2), 229–232 (1982) 2, 3

[15] Roos, C.: A new lower bound for the minimum distance of a cyclic code. IEEE Transactions on Information Theory **29**(3), 330–332 (1983) 2, 3, 4

[16] Sugiyama, Y., Kasahara, M., Hirasawa, S., Namekawa, T.: A Method for Solving Key Equation for Decoding Goppa Codes. Information and Control **27**(1), 87–99 (1975) 15

[17] Zeh, A., Wachter-Zeh, A., Bezzateev, S.: Decoding Cyclic Codes up to a New Bound on the Minimum Distance. IEEE Transactions on Information Theory **58**(6), 3951–3960 (2012) 2, 3, 10

[18] Zeh, A., Bezzateev, S.: Describing A Cyclic Code by Another Cyclic Code. 2012 IEEE International Symposium on Information Theory Proceedings (ISIT), 2896–2900 (2012) 1

[19] Zetterberg, L.H.: Cyclic codes from irreducible polynomials for correction of multiple errors. IRE Transactions on Information Theory **8**(1), 13–20 (1962) 9