Thirteenth International Workshop on Algebraic and Combinatorial Coding Theory
June 15-21, 2012, Pomorie, Bulgaria *pp. 352–357*

A new error and erasure decoding approach for cyclic codes [1]

Alexander Zeh alexander.zeh@uni-ulm.de
Institute of Communications Engineering, University of Ulm, Ulm, Germany and
INRIA Saclay–Île-de-France, Ecole Polytechnique ParisTech, Palaiseau Cedex, France
Sergey Bezzateev bsv@aanet.ru
Saint Petersburg State University of Airspace Instrumentation, St. Petersburg, Russia

Abstract. A cyclic code is associated with another cyclic code to bound its minimum distance. The algebraic relation between these two codes allows the formulation of syndromes and a key equation. In this contribution, we outline the decoding approach for the case of errors and erasures and show how the Extended Euclidean Algorithm can be used for decoding.

1 Introduction

The BCH bound [1, 3] is based on the longest sequence of consecutive indexes in the defining set of a cyclic code. Many other lower bounds (Hartmann–Tzeng, Roos, AB bound) on the minimum distance of cyclic codes are generalizations of the BCH bound and consider multiple sets of (non-)consecutive roots.

Our approach is based on the association of a second cyclic code with the original one and we search the longest sequence where each element is the product of at least one root of the two codes. This approach is a generalization of our previous work [6, 7], which uses rational functions. Furthermore, it allows to 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 code.

In the next section, we give some necessary preliminaries before we describe in Section 3 our approach — called non-zero-locator code — and recall the lower bound on the minimum distance of the original code. Section 4 describes the decoding approach in case of errors and erasures by means of an explicit syndrome formula, a key equation and the necessary modification of the Extended Euclidean Algorithm (EEA).

[1]This work has been supported by the German Research Council "Deutsche Forschungsgemeinschaft" (DFG) under grant BO 867/22-1.

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 in Hamming metric is denoted by $\mathcal{C}(q; n, k, d)$. A codeword $(c_0\ c_1\ \ldots\ c_{n-1})$ of $\mathcal{C}(q; n, k, d)$ is denoted by $c(x) = \sum_{i=0}^{n-1} c_i x^i \in \mathbb{F}_q[x]$ in polynomial form. The generator polynomial of $\mathcal{C}$ has roots in an extension field $\mathbb{F}_{q^s}$, where $n|(q^s - 1)$. Let $\alpha \in \mathbb{F}_{q^s}$ be a primitive nth root of unity.

3 Non-zero-locator code

We relate another cyclic code — the so-called non-zero-locator code $\mathcal{L}$ — to a given cyclic code $\mathcal{C}$. The obtained bound d^* on the minimum distance d of $\mathcal{C}$ can be expressed in terms of parameters of the associated non-zero-locator code $\mathcal{L}$.

Let us establish a connection between the codewords $c(x)$ of a given cyclic code $\mathcal{C}$ and a 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 $\mathcal{Y}$ denote the set of indexes of non-zero coefficients of $c(x) = \sum_{i\in\mathcal{Y}} c_i x^i$. Let $\alpha \in \mathbb{F}_{q^s}$ be an element of order n. Then we have the following relation for all $c(x) \in \mathcal{C}(q; n, k, d)$:

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

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

Definition 1 (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 nth roots of unity. Let $\gcd(n, n_\ell) = 1$ and let $\mathbb{F}_{q_\ell} = \mathbb{F}_{q^t}$ be an extension field of $\mathbb{F}_q$. Let $\mathbb{F}_{q_\ell^{s_\ell}}$ contain the n_ℓth 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_ℓ.*

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 $\forall\, c(x) \in \mathcal{C}$:

$$\sum_{j=0}^{\infty} c(\alpha^{j+e})a(\beta^j)x^j \equiv 0 \bmod x^{\mu-1}, \tag{2}$$

holds.

Let r denote the least common multiple of s and $t \cdot s_\ell$ and let γ 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_ℓ.

Before we prove the main theorem on the minimum distance d of the given cyclic code $\mathcal{C}$, we describe Definition 1. 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 $j = 0, \ldots, \mu-2$.

Theorem 1 (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 μ be given as in Definition 1. Then the minimum distance d of $\mathcal{C}(q; n, k, d)$ satisfies the following inequality:*

$$d \geq d^* \stackrel{\text{def}}{=} \left\lceil \frac{\mu}{d_\ell} \right\rceil, \tag{3}$$

Proof. See [7]. □

4 Error/erasure decoding approach

Let the set $\mathcal{E} = \{i_0, i_1, \ldots, i_{\varepsilon-1}\}$ with cardinality $|\mathcal{E}| = \varepsilon$ be the set of erroneous positions. The corresponding error polynomial is denoted by $e(x) = \sum_{i\in\mathcal{E}} e_i x^i$. Let "?" mark an erasure and let the set $\mathcal{D} = \{j_0, j_1, \ldots, j_{\delta-1}\}$ with cardinality $|\mathcal{D}| = \delta$ be the set of erased positions. Let the received polynomial $\widetilde{r}(x) = \sum_{i=0}^{n-1} \widetilde{r}_i x^i$ with $\widetilde{r}_i \in \mathbb{F}_q \cup \{?\}$.

In the first step of the decoding process, the erasures in $\widetilde{r}(x)$ are substituted by an arbitrary element from $\mathbb{F}_q$. For simplicity, it is common to choose the zero-element. Thus, the corresponding erasure polynomial in $\mathbb{F}_q[x]$ is denoted by $d(x) = \sum_{i\in\mathcal{D}} d_i x^i$, where $\widetilde{r}_i + d_i = c_i + d_i = 0,\ \forall i \in \mathcal{D}$. Let the modified received polynomial $r(x) \in \mathbb{F}_q[x]$ be

$$r(x) = \sum_{i=0}^{n-1} r_i x^i = c(x) + d(x) + e(x). \tag{4}$$

Definition 2 (Syndromes)**.** *Let a q-ary cyclic code $\mathcal{C}(q; n, k, d)$, its associated non-zero-locator code $\mathcal{L}(q_\ell; n_\ell, k_\ell, d_\ell)$ with $\gcd(n, n_\ell) = 1$, the integers μ, e and the modified received polynomial $r(x) \in \mathbb{F}_q[x]$ of (4) be given. Then we define a syndrome polynomial $S(x) \in \mathbb{F}_{q^r}[x]$ as follows:*

$$S(x) \stackrel{\text{def}}{\equiv} \sum_{j=0}^{\infty} r(\alpha^{j+e})a(\beta^j)x^j \mod x^{\mu-1}. \tag{5}$$

Since we know the positions of the erasures, we can compute an erasure-locator polynomial.

Definition 3 (Erasure-Locator Polynomial)**.** *Let the set $\mathcal{D}$ with $|\mathcal{D}| = \delta$ and a codeword $a(x) = \sum_{i\in\mathcal{Z}} a_i x^i \in \mathcal{L}(q_\ell; n_\ell, k_\ell, d_\ell)$ with weight d_ℓ be given. Here $\mathcal{Z}$ denotes the support of $a(x)$. Then we define an erasure-locator polynomial $\Psi(x) \in \mathbb{F}_{q^r}[x]$ as follows:*

$$\Psi(x) \stackrel{\text{def}}{=} \prod_{i\in\mathcal{D}} \Big(\prod_{j\in\mathcal{Z}} \big(1 - x\alpha^i\beta^j\big)\Big). \tag{6}$$

Note that $\Psi(x)$ has degree $\delta \cdot d_\ell$. As in Forney's original approach [2] we define a modified syndrome polynomial $\widetilde{S}(x)$ and point out (in the following lemma), which coefficients of $\widetilde{S}(x)$ depend only on the error $e_{i_0}, e_{i_1}, \ldots, e_{i_{\varepsilon-1}}$.

Lemma 1 (Modified Syndrome Polynomial)**.** *Let the erasure-locator polynomial $\Psi(x)$ of Definition 3 and the syndrome polynomial $S(x)$ of Definition 2 be given. Then the highest $\mu - 1 - \delta \cdot d_\ell$ coefficients of*

$$\widetilde{S}(x) \stackrel{\text{def}}{\equiv} \Psi(x) \cdot S(x) \mod x^{\mu-1} \tag{7}$$

depend only on the error polynomial $e(x)$.

Proof. From (5) we have:

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

and with (1) for $a(x) = \sum_{i\in\mathcal{Z}} a_i x^i$ we can write:

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

and finally, we can write for $S(x)$:

$$S(x) \equiv \frac{\overbrace{\sum_{i\in\mathcal{E}}\Big(e_i\alpha^{ie}\sum_{j\in\mathcal{Z}}\Big(a_j\prod_{\substack{\ell\in\mathcal{Z}\\ \ell\neq j}}(1-x\alpha^i\beta^\ell)\Big)\prod_{\substack{m\in\mathcal{E}\\ m\neq i}}\prod_{s\in\mathcal{Z}}(1-x\alpha^m\beta^s)\Big)}^{\stackrel{\text{def}}{=}\Omega(x)}}{\prod_{i\in\mathcal{E}}\Big(\prod_{j\in\mathcal{Z}}\big(1-x\alpha^i\beta^j\big)\Big)}+$$

$$\frac{\overbrace{\sum_{i\in\mathcal{D}}\Big(d_i\alpha^{ie}\sum_{j\in\mathcal{Z}}\Big(a_j\prod_{\substack{\ell\in\mathcal{Z}\\ \ell\neq j}}(1-x\alpha^i\beta^\ell)\Big)\prod_{\substack{m\in\mathcal{D}\\ m\neq i}}\prod_{s\in\mathcal{Z}}(1-x\alpha^m\beta^s)\Big)}^{\stackrel{\text{def}}{=}A(x)}}{\prod_{i\in\mathcal{D}}\Big(\prod_{j\in\mathcal{Z}}\big(1-x\alpha^i\beta^j\big)\Big)} \mod x^{\mu-1},$$

where $A(x)$ has degree at most $d_\ell\cdot(\delta-1)+d_\ell-1=d_\ell\cdot\delta-1$. □

Similar to the erasure-locator polynomial, we define an error-locator polynomial as follows:

$$\Lambda(x)\stackrel{\text{def}}{=}\prod_{i\in\mathcal{E}}\Big(\prod_{j\in\mathcal{Z}}\big(1-x\alpha^i\beta^j\big)\Big). \tag{8}$$

Let $\widetilde{\Omega}(x)\stackrel{\text{def}}{=}\Omega(x)\cdot\Psi(x)+A(x)\cdot\Lambda(x)$ and with (7) and (8), we obtain the following *Key Equation*:

$$\widetilde{S}(x)\equiv\frac{\widetilde{\Omega}(x)}{\Lambda(x)} \mod x^{\mu-1}, \text{ with } \begin{array}{ll}\deg\Lambda(x) & =\varepsilon\cdot d_\ell\\ \deg\widetilde{\Omega}(x) & \le(\varepsilon+\delta)\cdot d_\ell-1.\end{array} \tag{9}$$

Note that in the erasure-free case $\Omega(x)$ is the error-evaluator polynomial with $\deg\Omega(x)\le\varepsilon\cdot d_\ell-1$. In the following, we shortly outline how to solve (9) by the EEA described in [5] to decode cyclic codes.

Lemma 2 (Solving the Key Equation)**.** *Assume $\delta<d^*-1$ erasures occurred. Let $\widetilde{S}(x)$ with $\deg\widetilde{S}(x)\le\mu-2$ as in (7) be given. If*

$$\varepsilon=|\mathcal{E}|\le\left\lfloor\frac{d^*-1-\delta}{2}\right\rfloor, \tag{10}$$

then there exists a unique solution of (9) and we can use the EEA [5] with the input polynomials $r_{-1}(x)=x^{\mu-1}$ and $r_0(x)=\widetilde{S}(x)$ to find it. Furthermore, we have the following stopping rule for the EEA: We stop, if the remainder polynomial $r_i(x)$ in the ith step of the EEA fulfills:

$$\deg r_{i-1}(x)\ge\frac{\mu-1+\delta\cdot d_\ell}{2} \quad \textit{and} \quad \deg r_i(x)\le\frac{\mu-1+\delta\cdot d_\ell}{2}-1. \tag{11}$$

Then the EEA returns the error-locator polynomial $\Lambda(x)$ *as in (8) and the error/erasure-evaluation polynomial* $\widetilde{\Omega}(x) = \Omega(x) \cdot \Psi(x) + A(x) \cdot \Lambda(x)$ *as in (9).*

Proof. We refer to the presentation of the EEA as in [4, Ch. 12 §9]. We denote by $r_i(x)$ the remainder and by $u_i(x)$ the connection polynomial of the EEA in the ith step. We proceed the EEA until reaching $r_i(x)$ such that (11) holds.

From the properties of the EEA, we know that $\deg u_i(x) = \deg r_{-1}(x) - \deg r_{i-1}(x)$ and we know that it corresponds to the error-locator polynomial as in (8). Therefore, we obtain:

$$\deg u_i(x) = \varepsilon \cdot d_\ell \leq \left\lfloor \mu - 1 - \frac{\mu - 1 + \delta \cdot d_\ell}{2} \right\rfloor = \left\lfloor \frac{\mu - 1 - \delta \cdot d_\ell}{2} \right\rfloor \Leftrightarrow$$
$$\varepsilon \leq \left\lfloor \frac{d^* - \delta}{2} - \frac{1}{2d_\ell} \right\rfloor = \left\lfloor \frac{d^* - 1 - \delta}{2} \right\rfloor,$$

where we used the fact that $(d^* - \delta)/2$ is a multiple of $1/2$ and therefore $1/(2d_\ell)$ influences the result in the same way as $1/2$ in the last step. □

Furthermore, we know from the EEA that for $\varepsilon \leq \lfloor (d^* - 1 - \delta)/2 \rfloor$ a unique solution $\Lambda(x)$ exists.

References

[1] R. C. Bose and D. K. Ray Chaudhuri. On a Class of Error Correcting Binary Group Codes. *Information and Control*, 3(1):68–79, March 1960.

[2] G. Forney. On Decoding BCH Codes. *Information Theory, IEEE Transactions on*, 11(4):549–557, 1965.

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

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

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

[6] A. Zeh, A. Wachter, and S. Bezzateev. Efficient Decoding of Some Classes of Binary Cyclic Codes beyond the Hartmann–Tzeng Bound. In *Information Theory Proceedings (ISIT), 2011 IEEE International Symposium on*, pages 1017–1021, August 2011.

[7] A. Zeh, A. Wachter-Zeh, and S. Bezzateev. Decoding Cyclic Codes up to a New Bound on the Minimum Distance. *accepted for IEEE Transactions on Information Theory*, May 2012.