A New Error and Erasure Decoding Approach for Cyclic Codes

Alexander Zeh[1] and Sergey Bezzateev[2]
[1] Institute of Communications Engineering Ulm University, Germany
Research Center INRIA Saclay - Île-de-France, École Polytechnique ParisTech, France
[2] 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. We outline the decoding approach for the case of errors and erasures and show how the Extended Euclidean Algorithm can be used for decoding.

I. 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.

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:*

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

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

II. ERROR/ERASURE DECODING APPROACH

Let the set $\mathcal{E} = \{i_0, i_1, \dots, i_{\varepsilon-1}\}$ 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 $\mathcal{D} = \{j_0, j_1, \dots, j_{\delta-1}\}$ 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 $r(x) = \sum_{i=0}^{n-1} r_i x^i = c(x) + d(x) + e(x)$.

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 (??) be given. Then we define a syndrome polynomial $S(x) \in \mathbb{F}_{q^r}[x]$ as follows:*

$$S(x) \overset{\text{def}}{\equiv} \sum_{j=0}^{\infty} r(\alpha^{j+e}) a(\beta^j) x^j \mod x^{\mu-1}. \tag{4}$$

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:*

$$\Psi(x) \overset{\text{def}}{=} \prod_{i \in \mathcal{D}} \Big(\prod_{j \in \mathcal{Z}} \big(1 - x\alpha^i \beta^j\big) \Big). \tag{5}$$

Note that $\Psi(x)$ has degree $\delta \cdot d_\ell$. As in Forney's original approach 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 $e_{i_0}, e_{i_1}, \dots, e_{i_{\varepsilon-1}}$.

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*

$$\widetilde{S}(x) \overset{\text{def}}{\equiv} \Psi(x) \cdot S(x) \mod x^{\mu-1} \tag{6}$$

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

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

$$\Lambda(x) \overset{\text{def}}{=} \prod_{i \in \mathcal{E}} \Big(\prod_{j \in \mathcal{Z}} \big(1 - x\alpha^i \beta^j\big) \Big). \tag{7}$$

Let $\widetilde{\Omega}(x) \overset{\text{def}}{=} \Omega(x) \cdot \Psi(x) + A(x) \cdot \Lambda(x)$ and with (6) and (7), we obtain the following *Key Equation*:

$$\widetilde{S}(x) \equiv \frac{\widetilde{\Omega}(x)}{\Lambda(x)} \mod x^{\mu-1}, \text{ with } \begin{array}{ll} \deg \Lambda(x) & = \varepsilon \cdot d_\ell \\ \deg \widetilde{\Omega}(x) & \leq (\varepsilon + \delta) \cdot d_\ell - 1. \end{array} \tag{8}$$

Lemma 2 (Solving the Key Equation). *Assume $\delta < d^* - 1$ erasures occurred. Let $\widetilde{S}(x)$ with $\deg \widetilde{S}(x) \leq \mu - 2$ as in (6) be given. If*

$$\varepsilon = |\mathcal{E}| \leq \left\lfloor \frac{d^* - 1 - \delta}{2} \right\rfloor, \tag{9}$$

then there exists a unique solution of (8) and we can use the EEA 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:

$$\deg r_{i-1}(x) \geq \frac{\mu - 1 + \delta \cdot d_\ell}{2} \quad \textit{and} \quad \deg r_i(x) \leq \frac{\mu - 1 + \delta \cdot d_\ell}{2} - 1. \tag{10}$$

Then the EEA returns the error-locator polynomial $\Lambda(x)$ as in (7) and the error/erasure-evaluation polynomial $\widetilde{\Omega}(x) = \Omega(x) \cdot \Psi(x) + A(x) \cdot \Lambda(x)$ as in (8).