On Decoding of BCH Codes

Antonio Aparecido de Andrade
E-mail: andrade@mat.ibilce.unesp.br
Departamento de Matemática - Ibilce - Unesp
Rua Cristovão Colombo, 2265
15054-000, São José do Rio Preto, SP, BRAZIL

Abstract—**This work presents a procedure for decoding BCH codes over finite rings using Fourier transforms in a Galois ring, where the error vector is determined as the inverse Fourier transform of the syndrome vector** $S = (S_0, S_1, \cdots, S_{n-1})$.

Keywords—**Fourier transform, Galois ring.**

I. Introduction

There are many methods for decoding a given code. A choice among several different decoding algorithms depends on certain code parameters, such as blocklength and minimum, requiring decoding speed and economy. Construction of procedures for decoding BCH codes has always been one of the objetives in coding research. Interlando, Palazzo and Elia [3] have described an efficient decoding procedure for BCH codes over finite rings $\mathbb{Z}_m$, with m a positive integer, called modified Berlekamp-Massey algorithm. Andrade and Palazzo [2] have proposed a construction technique of BCH codes over finite commutative rings with identity and decoding algorithm for these codes.

Having the decoding of the BCH codes over finite rings as the main motivation, in this work we present an alternative decoding procedure for these codes using the modified Berlekamp-Massey and Fourier transform in a Galois ring. The decoding procedure consists of three major steps: (1) calculation of the syndromes, (2) calculation of the error-locator polynomial, and (3) calculation of the error magnitudes.

This work is organized as follows. In Section 2 we describe Fourier transform in a Galois ring. In Section 3, a decoding procedure for BCH codes defined over local finite rings using Fourier transforms is proposed.

II. Fourier transform

In this section we introduce Fourier transforms over Galois ring which is very similar to the one proposed by Blahut over Galois field [5]. First we collect basic concepts and facts from the Galois theory of commutative rings.

Throughout this work we assume that $\mathcal{A}$ is a finite commutative local ring with identity, with maximal ideal $\mathcal{M}$ and residue field $\mathbb{K} = \frac{\mathcal{A}}{\mathcal{M}} \cong GF(p^m)$, where m is a positive integer and p is a prime. Let $f(x)$ be a monic polynomial of degree h in $\mathcal{A}[x]$, such that $\mu(f(x))$ is irreducible in $\mathbb{K}[x]$, where μ is the natural projection. Then $f(x)$ also is irreducible in $\mathcal{A}[x]$ [4, Theorem XIII.7]. Let $\mathcal{R}$ be the ring $\mathcal{A}[x]/\langle f(x)\rangle$. Then $\mathcal{R}$ is a finite commutative local ring with identity and is called a Galois extension of $\mathcal{A}$ of degree h. Its residue field is $\mathbb{K}_1 = \mathcal{R}/\overline{\mathcal{M}_1} \cong GF(p^{mh})$, where $\overline{\mathcal{M}_1}$ is the maximal ideal of $\mathcal{R}$, and $\mathbb{K}_1^*$ is the multiplicative group of $\mathbb{K}_1$, whose order is $p^{mh} - 1$.

Let $\mathcal{R}^*$ denotes the multiplicative group of units of $\mathcal{R}$. It follows that $\mathcal{R}^*$ is an abelian group, and therefore it can be expressed as a direct product of cyclic groups. We are interested in the maximal cyclic group of $\mathcal{R}^*$, hereafter denoted by $\mathcal{G}_s$, whose elements are the roots of $x^s - 1$ for some positive integer s such that $\gcd(s, p) = 1$. There is only one maximal cyclic subgroup of $\mathcal{R}^*$ having order relatively prime to p [4, Theorem XVIII.2]. This cyclic group has order $s = p^{mh} - 1$.

Definition II.1: Let $\mathbf{v} = (v_0, v_1, \cdots, v_{n-1})$ be a vector over $\mathcal{A}$, where n divides s, and let α be an element of $\mathcal{G}_s$ of order n. The Fourier transform of the vector $\mathbf{v}$ is the vector $\mathbf{V} = (V_0, V_1, \cdots, V_{n-1})$ definded by

$$V_j = \sum_{i=0}^{n-1} \alpha^{i(j+1)} v_i, \quad j = 0, 1, \cdots, n-1. \tag{1}$$

The discrete index i is the *time*, $\mathbf{v}$ is the *time-domain function* or the *signal*, the discrete index j is the *frequency* and $\mathbf{V}$ is the *frequency-domain function* or the *spectrum*.

Fourier transforms of every blocklength do not exist in a Galois ring because elements of every order do not exist. Sometimes we represent a vector $\mathbf{v}$ by a polynomial $\mathbf{v}(x) = v_0 + v_1 x + \cdots + v_{n-1}x^{n-1}$. The polynomial $\mathbf{v}(x)$ can be transformed into a polynomial $\mathbf{V}(x) = V_0 + V_1 x + \cdots + V_{n-1}x^{n-1}$ by means of the Fourier transform. The latter polynomial is called the *spectrum polynomial* or the *associated polynomial* of $\mathbf{v}(x)$.

Lemma II.1: If $\alpha \in \mathcal{G}_s$ is an element of order n, then

$$\sum_{i=0}^{n-1} \alpha^i = \begin{cases} 0 & \text{if} \quad \alpha \neq 1 \\ n & \text{if} \quad \alpha = 1, \end{cases} \tag{2}$$

where n is interpreted as an integer modulo p.

Proof: If $\alpha = 1$ this sum is clearly equal to n. If $\alpha \neq 1$ we have that $\sum_{i=0}^{n-1} \alpha_i = \dfrac{1-\alpha^n}{1-\alpha} = 0$, since $\alpha^n = 1$.

Lemma II.2: Let $\alpha \in \mathcal{G}_s$ be an element of order n. If $\mathbf{v}(x) = v_0 + v_1 x + \cdots + v_{n-1}x^{n-1} \in \mathcal{A}[x]$, then

$$nv_i = \sum_{j=0}^{n-1} \mathbf{v}(\alpha^{j+1})\alpha^{-i(j+1)}, \quad i = 0, 1, \cdots, n-1, \tag{3}$$

where the product $nv_i,\ i = 0, 1, \cdots, n-1$, is interpreted modulo p.

Proof: By Lemma II.1 we have that

$$\sum_{j=0}^{n-1} \mathbf{v}(\alpha^{j+1})\alpha^{-i(j+1)} = \sum_{j=0}^{n-1}\Big(\sum_{k=0}^{n-1} v_k \alpha^{(j+1)k}\Big)\alpha^{-i(j+1)} =$$
$$= \sum_{j=0}^{n-1}\sum_{k=0}^{n-1} v_k \alpha^{(j+1)(k-i)} = \sum_{k=0}^{n-1} v_k \sum_{j=0}^{n-1} \alpha^{(j+1)(k-i)} = nv_i,$$

for all $i = 0, 1, \cdots, n-1$.

Theorem II.1: If $\mathbf{c} = (c_0, c_1, \cdots, c_{n-1}) \in \mathcal{A}^n$ then

1. $nv_i = \alpha^{i(n-1)}\mathbf{V}(\alpha^{-i}),\ i = 0, 1, \cdots, n-1,$
2. $n\mathbf{v} = (\mathbf{V}(1), \alpha^{n-1}\mathbf{V}(\alpha^{-1}), \cdots, \alpha^{(n-1)^2}\mathbf{V}(\alpha^{-(n-1)}),$
3. $n\mathbf{v}(x) = \sum_{i=0}^{n-1} \alpha^{i(n-1)}\mathbf{V}(\alpha^{-i})x^i,$

where $\mathbf{V}(x) = V_0 + V_1 x + \cdots + V_{n-1}x^{n-1}$ and the product $nv_i,\ i = 0, 1, \cdots, n-1$, is interpreted modulo p.

Proof: For the first equality we have that

$$\alpha^{i(n-1)}\mathbf{V}(\alpha^{-i}) = \alpha^{i(n-1)} \sum_{j=0}^{n-1} V_j \alpha^{-ij} =$$
$$= \alpha^{i(n-1)} \sum_{j=0}^{n-1} (\sum_{k=0}^{n-1} \alpha^{k(j+1)} v_k)\alpha^{-ij} =$$
$$= \sum_{j=0}^{n-1}\sum_{k=0}^{n-1} \alpha^{in-i+kj+k-ij} v_k =$$
$$= \sum_{k=0}^{n-1} v_k \sum_{j=0}^{n-1} \alpha^{(j+1)(k-i)} = nv_i.$$

For the second equality we have that

$$(\mathbf{V}(1), \alpha^{n-1}\mathbf{V}(\alpha^{-1}), \cdots, \alpha^{(n-1)^2}\mathbf{V}(\alpha^{-(n-1)})) =$$
$$= (nv_0, nv_1, \cdots, nv_{n-1}) = n\mathbf{v}.$$

For the last equality we have that

$$\sum_{i=0}^{n-1} \alpha^{i(n-1)}\mathbf{V}(\alpha^{-i})x^i =$$
$$= \sum_{i=0}^{n-1} nv_i x^i = n\sum_{i=0}^{n-1} v_i x^i = n\mathbf{v}(x).$$

Corollary II.1: Over $\mathcal{A}$, a vector and its spectrum are related by

$$V_j = \sum_{i=0}^{n-1} \alpha^{i(j+1)} v_i \qquad \text{and} \qquad nv_i = \sum_{j=0}^{n-1} \alpha^{-i(j+1)} V_j,$$

where the product $nv_i, i = 0, 1, \cdots, n-1$, is interpreted modulo p.

Proof: We have that

$$\sum_{j=0}^{n-1} \alpha^{-i(j+1)} V_j = \sum_{j=0}^{n-1} \alpha^{-i(j+1)} \sum_{k=0}^{n-1} v_k \alpha^{k(j+1)} =$$
$$= \sum_{k=0}^{n-1} v_k \sum_{j=0}^{n-1} \alpha^{(j+1)(k-i)} = nv_i.$$

Remark II.1: The coefficients V_j are given by

$$\begin{bmatrix} V_0 \\ V_1 \\ V_2 \\ \vdots \\ V_{n-1} \end{bmatrix} = \begin{bmatrix} 1 & \alpha & \cdots & \alpha^{n-1} \\ 1 & \alpha^2 & \cdots & \alpha^{2(n-1)} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha^{n-1} & \cdots & \alpha^{(n-1)^2} \\ 1 & 1 & \cdots & 1 \end{bmatrix} \begin{bmatrix} v_0 \\ v_1 \\ v_2 \\ \vdots \\ v_{n-1} \end{bmatrix},$$

where the differences $\alpha^j - \alpha^k$ are units for all $0 \le j \ne k \le n-1$ [1, Theorem 7].

Example II.1: Let $\mathcal{A} = \mathbb{Z}_2[i]$ and $\mathcal{R} = \frac{\mathcal{A}[x]}{\langle x^4+x+1\rangle}$, where $f(x) = x^4 + x + 1$ is irreducible over $\mathcal{A}$. Thus $s = 15$ and G_{15} is generated by α, where $\alpha^4 = \alpha + 1$. The element $\beta = \alpha^3$ has order 5. The Fourier transform of the vector $\mathbf{v} = (11101)$ is given by $\mathbf{V} = (\beta^3, \beta, \beta^4, \beta^2, 0)$.

Properties of the spectrum are closely related to the zeros of polynomials, as stated in the following theorem.

Theorem II.2: With the notations above we have that

1. the polynomial $\mathbf{v}(x)$ has a zero at α^{j+1} if and only if the jth frequency component V_j is equal to zero;
2. the polynomial $\mathbf{V}(x)$ has a zero at α^{-i} if and only if the ith time component v_i is equal to zero.

Proof: Part (1) follows from the fact that $\mathbf{v}(\alpha^{j+1}) = \sum_{i=0}^{n-1} v_i \alpha^{i(j+1)} = V_j$, and the proof of part (2) follows from the fact that $\alpha^{i(n-1)}\mathbf{V}(\alpha^{-i}) = nv_i$.

Theorem II.3: (Convolution Theorem) If $e_i = f_i g_i$, for all $i = 0, 1, \cdots, n-1$, then

$$nE_j = \sum_{k=0}^{n-1} F_{(j-k-1)} G_k, \quad j = 0, 1, \cdots, n-1,$$

where $j - k - 1$ is interpreted modulo n and the product nE_j is interpreted modulo p.

Proof: Setting the Fourier transform of $e_i = f_i g_i$, for all $i = 0, 1, \cdots, n-1$, we have that

$$\begin{aligned} nE_j &= n\sum_{i=0}^{n-1} \alpha^{i(j+1)} e_i = n\sum_{i=0}^{n-1} \alpha^{i(j+1)} f_i g_i = \\ &= \sum_{i=0}^{n-1} \alpha^{i(j+1)} f_i (n g_i) = \\ &= \sum_{i=0}^{n-1} \alpha^{i(j+1)} f_i (\sum_{k=0}^{n-1} \alpha^{-i(k+1)} G_k) = \\ &= \sum_{k=0}^{n-1} G_k (\sum_{i=0}^{n-1} \alpha^{i(j-k)} f_i = \sum_{k=0}^{n-1} F_{(j-k-1)} G_k. \end{aligned}$$

Theorem II.4: (Translation Property) If $\{v_i\} \leftrightarrow \{V_j\}$ is a Fourier transform pair, then $\{\alpha^i v_i\} \leftrightarrow \{V_{j+1}\}$ is also a Fourier transform pair, where $j + 1$ is interpreted modulo n.

Proof: The proof follows from the fact that $V_{j+1} = \sum_{i=0}^{n-1} \alpha^{i(j+1)} \alpha^i v_i$.

III. Applications

In this section we present a decoding algorithm for BCH codes using the modified Berlekamp-Massey algorithm and the Fourier transform that corrects all errors up to Hamming weight t, i.e., whose minimum Hamming distance is greater than or equal to $2t + 1$. Let $\mathcal{A}$ be the local finite commutative ring and $\mathcal{G}_s = \{1, \alpha, \alpha^2, \cdots, \alpha^s\}$, where $s = p^{mh} - 1$, as defined in Section 2.

Definition III.1: [2, Definition 2.2] A **BCH code** $\mathcal{C}$ of length $n \leq s$ over $\mathcal{A}$ has parity check matriz defined by

$$H = \begin{bmatrix} 1 & \alpha & \alpha^2 & \cdots & \alpha^{n-1} \\ 1 & \alpha^2 & \alpha^4 & \cdots & \alpha^{2(n-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha^{2t} & (\alpha^2)^{2t} & \cdots & (\alpha^{n-1})^{2t} \end{bmatrix}, \quad (4)$$

where $t \geq 1$ and α is an element of order n of $\mathcal{G}_s$.

The minimum Hamming distance of this code is $d \geq 2t+1$ [2, Theorem 2.4] and therefore this code has an error correction capability equals to t.

Let $\mathbf{c} = (c_0, c_1, \cdots, c_{n-1})$ be the transmited codeword and $\mathbf{v} = (v_0, v_1, \cdots, v_{n-1})$ be the received vector. The error vector is given by $\mathbf{e} = (e_0, e_1, \cdots, e_{n-1}) = \mathbf{v} - \mathbf{c}$. The error pattern $\mathbf{e}$ can be described by a list of values and locations of its nonzero components. The location will be given in terms of an *error-location number*. Thus, each nonzero component of $\mathbf{e}$ is described by a pair of elements, y_i (the magnitude of error), and x_i (the error-location number), where y_i is an element of $\mathcal{A}$ and $x_i = \alpha^{i_k}$ is an element of $\mathcal{G}_s$. If at most t errors occur, there are t nonzero components of $\mathbf{e}$, and hence t pairs (x_i, y_i) are required to describe the errors.

Suppose the t errors occur at locations α^{i_k} for $k = 1, 2, \cdots, t$. The error-locator polynomial is

$$\mathbf{\Lambda}(x) = \prod_{k=1}^{t}(1 - x\alpha^{i_k}) = \Lambda_0 + \Lambda_1 x + \cdots + \Lambda_t x^t. \quad (5)$$

Thus the proposed decoding algorithm consists of three major steps:

Step 1 - Calculation of the syndrome vector from the received vector.

Step 2 - Calculation of the error-locator polynomial $\Lambda(x)$ from $\boldsymbol{s}$ using the modified Berlekamp-Massey algorithm [3].

Step 3 - Calculation of the error magnitudes $y_1, y_2, \cdots, y_t$ using an inverse Fourier transform.

The syndromes of this noisy BCH codeword $\mathbf{v}$ are given by

$$S_j = \sum_{k=0}^{n-1} \alpha^{k(j+1)} v_k = \mathbf{v}(\alpha^{j+1}), \qquad j = 0, 1, 2, \cdots, 2t-1. \quad (6)$$

For Equation (6) we have that the syndromes are computed as $2t$ components of a Fourier transform. The received noisy codeword $\mathbf{v} = \mathbf{c} + \mathbf{e}$ has Fourier transform with components $V_j = C_j + E_j$ for $j = 0, 1, 2, \cdots, n-1$ and the syndromes are the $2t$ components of this spectrum from 0 to $2t-1$. But by construction of the BCH code, the parity frequencies for $j = 0, 1, \cdots, 2t-1$ have spectral components equal to zero, i.e., $C_j = 0$, $j = 0, 1, \cdots, 2t-1$, since $\mathbf{c}H^t = \mathbf{0}$. Hence $S_j = V_j = E_j$, for all $j = 0, 1, \cdots, 2t-1$. The block of syndromes gives us a window through which we can look at $2t$ of the n components of the spectrum of the error pattern. But we know from the BCH bound that if the error pattern has weight at most t, then these $2t$ syndromes are enough to uniquely determine the error pattern.

Let the vector $\mathbf{\Lambda} = (\Lambda_0, \Lambda_1, \cdots, \Lambda_{n-1})$. The inverse Fourier transform of the vector $\mathbf{\Lambda}$ is given by $n\lambda_j = \alpha^{j(n-1)}\mathbf{\Lambda}(\alpha^{-j})$ for $j = 0, 1, \cdots, n-1$. Thus $\mathbf{\Lambda}(\alpha^{-j})$ is equal to zero if and only if j is an error location. Thus $\mathbf{\Lambda}(x)$ has been defined so that in the time domain, $n\lambda_j = 0$ whenever $e_j \neq 0$. Therefore $n\lambda_j e_j = 0$ for all j, and thus, by the convolution theorem, the convolution in the frequency domain is zero, i.e.,

$$\sum_{j=0}^{n-1} \Lambda_j E_{k-j-1} = 0, \quad k = 0, 1, \cdots, n-1. \quad (7)$$

Since $\mathbf{\Lambda}(x)$ is a polynomial of degree at most t, we have that $\Lambda_j = 0$ for $j > t$. Then

$$\sum_{j=0}^{t} \Lambda_j E_{k-j-1} = 0, \quad k = 0, 1, \cdots, n-1, \quad (8)$$

and since $\Lambda_0 = 1$ we have

$$E_{k-1} = -\sum_{j=1}^{t} \Lambda_j E_{k-j-1}, \quad (9)$$

for $k = 0, 1, \cdots, n-1$. This is a set of n equations in $n-t$ unknowns (t coefficients of $\mathbf{\Lambda}(x)$ and $n-2t$ components of $\mathbf{E}$) and in $2t$ known values of $\mathbf{E}$ given by the syndromes.

On the other hand, in terms of the pairs (x_i, y_i), we have that

$$S_l = \sum_{i=1}^{t} y_i x_i^l, \; l = 1, 2, \cdots, 2t.$$

Multiply both sides of the Equation (5) by $y_l x_l^{j+t}$ and set $x = x_l^{-1}$. Then the left side is zero, and we have that

$$0 = y_l x_l^{j+t}(1 + \Lambda_1 x_l^{-1} + \Lambda_2 x_l^{-2} + \cdots + \Lambda_{t-1} x_l^{-(t-1)} + \Lambda_t x_l^{-t})$$

or

$$y_l(x_l^{j+t} + \Lambda_1 x_l^{j+t-1} + \cdots + \Lambda_t x_l^j) = 0.$$

Such an equation holds for each l and each j. Sum up these equations from $l = 1$ to $l = t$. This gives, for each j,

$$\sum_{l=1}^{t} y_l(x_l^{j+t} + \Lambda_1 x_l^{j+t-1} + \cdots + \Lambda_t x_l^j) = 0$$

or

$$\sum_{l=1}^{t} y_l x_l^{j+t} + \Lambda_1 \sum_{l=1}^{t} y_l x_l^{j+t-1} + \cdots + \Lambda_t \sum_{l=1}^{t} y_l x_l^j = 0.$$

The individual sums are recognized as syndromes, and thus the equation becomes

$$S_{j+t} + \Lambda_1 S_{j+t-1} + \Lambda_2 S_{j+t-2} + \cdots + \Lambda_t S_j = 0, \quad (10)$$

for $j = 0, 1, \cdots, t-1$. Hence, we have the set of equations

$$\Lambda_1 S_{j+t-1} + \Lambda_2 S_{j+t-2} + \cdots + \Lambda_t S_j = -S_{j+t}, \quad (11)$$

for $j = 0, 1, 2, \cdots, t-1$. This is a set of linear equations relating the syndromes to the coefficients of $\Lambda(x)$. The t equations

$$S_{k-1} = -\sum_{j=1}^{t} \Lambda_j S_{k-j-1}, \quad (12)$$

for $k = t+1, \cdots, 2t$, involve only the known syndromes and the t unknown components of $\mathbf{\Lambda}$. These are always solvable for $\mathbf{\Lambda}$, for example, using the modified Berlekamp-Massey algorithm [3]. The remaning components of $\mathbf{S}$ can then be obtained by recursive extension, that is, using the Equation (12) to find S_{2t+1} from the known components if $\mathbf{S}$ and $\mathbf{\Lambda}$, then find S_{2t+2}, and so on. In this way, we have that S_j is computed for all j, E_j equals S_j, and $C_j = V_j - E_j$. The inverse Fourier transform of the vector $\mathbf{C} = (C_0, C_1, \cdots, C_{n-1})$ completes the decoding.

Example III.1: Let $\mathcal{C}(n, \eta)$ be the BCH code over $\mathbb{Z}_2(i)$ generated by polynomial $g(x) = x^8 + x^4 + x^2 + x + 1$. Let $\mathcal{R} = \frac{\mathbb{Z}_2[i][x]}{\langle x^4+x+1\rangle}$, where $f(x) = x^4+x+1$ is irreducible over $\mathbb{Z}_2$, G_{15} the cyclic subgroup of $\mathcal{R}$ containing the roots of $x^{15}-1$ and α a primitive element of G_{15}. Since $\alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^6, \alpha^8, \alpha^9$ and α^{12} are the roots of $g(x)$ it follows that $d_{min}(\mathcal{C}) \geq 5$ and this can correct up to $t = 2$ errors. Let $\eta = (\alpha_1, \alpha_2, \cdots, \alpha_{15}) = (\alpha^0, \alpha^1, \cdots, \alpha^{14}) = (\alpha^{k_1}, \alpha^{k_2}, \cdots, \alpha^{k_{15}})$ be a locator vector and the parity-check matrix given by

$$H = \begin{bmatrix} 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \cdots & \alpha^{14} \\ 1 & \alpha^2 & \alpha^4 & \alpha^6 & \alpha^8 & \alpha^{10} & \cdots & \alpha^{13} \\ 1 & \alpha^3 & \alpha^6 & \alpha^9 & \alpha^{12} & 1 & \cdots & \alpha^{12} \\ 1 & \alpha^4 & \alpha^8 & \alpha^{12} & \alpha & \alpha^5 & \cdots & \alpha^{11} \end{bmatrix}.$$

Suppose that the received vector is given by $\mathbf{v} = (0i0000000000010) = \mathbf{c} + \mathbf{e}$, where $\mathbf{c}$ is the transmitted vector and $\mathbf{e}$ is the error vector. The sindrome is given by $\mathbf{S} = \mathbf{v}H^T = (S_0, S_1, S_2, S_3)$, where $S_0 = E_0 = \alpha i + \alpha^{13}$, $S_1 = E_1 = \alpha^2 i + \alpha^{11}$, $S_2 = E_2 = \alpha^3 i + \alpha^9$ and $S_3 = E_3 = \alpha^4 i + \alpha^7$. By the modified Berlekamp-Massey algorithm we obtain $\mathbf{\Lambda}(z) = 1 + \alpha^{12} z + \alpha^{14} z^2$. Thus we obtain that $S_4 = E_4 = \alpha^5 i + \alpha^5$, $S_5 = E_5 = \alpha^6 i + \alpha^3$, $S_6 = E_6 = \alpha^7 i + \alpha$, $S_7 = E_7 = \alpha^8 i + \alpha^{14}$, $S_8 = E_8 = \alpha_9 i + \alpha^{12}$, $S_9 = E_9 = \alpha^{10} i + \alpha^{10}$, $S_{10} = E_{10} = \alpha^{11} i + \alpha^8$, $S_{11} = E_{11} = \alpha^{12} i + \alpha^6$, $S_{12} = E_{12} = \alpha^{13} i + \alpha^4$, $S_{13} = E_{13} = \alpha^{14} i + \alpha^2$ and $S_{14} = E_{14} = i + 1$. On the other hand, we have that $V_i = S_i$, $i = 0, 1, \cdots, 14$. Therefore $\mathbf{C} = \mathbf{0}$ and its inverse Fourier transform is given by $\mathbf{c} = \mathbf{0}$. Hence the transmitted vector was the zero vector.

Example III.2: In the Example III.1, letting $\eta = (1, \beta, \cdots, \beta^4)$, where $\beta = \alpha^3$ is a element of order 5, we have that the matrix

$$H = \begin{bmatrix} 1 & \beta & \beta^2 & \beta^3 & \beta^4 \\ 1 & \beta^2 & \beta^4 & \beta & \beta^3 \end{bmatrix}$$

define a BCH code of length 5 and minimum distance at least 3 over $\mathcal{A}$. Suppose that the received vector is given by $\mathbf{v} = (11101) = \mathbf{c} + \mathbf{e}$, where $\mathbf{c}$ is the transmitted vector and $\mathbf{e}$ is the error vector. The syndrome is given by $\mathbf{S} = (S_0, S_1)$, where $S_0 = E_0 = \beta^3$ and $S_1 = E_1 = \beta$. By the modified Berlekamp-Massey algorithm we obtain the following table

n	$\sigma^{(n)}(z)$	d_n	l_n	$n - l_n$
-1	1	1	0	-1
0	1	η^3	0	0
1	$1 + \beta^3 z$	0	1	0
2	$1 + \beta^3 z$	-	1	1

and then $\mathbf{\Lambda}(z) = 1 + \beta^3 z$. Thus we obtain that $S_2 = E_2 = \beta^4$, $S_3 = E_3 = \beta^2$ e $S_4 = E_4 = 1$. Hence $V_0 = \beta^3$, $V_1 = \beta$, $V_2 = \beta^4$, $V_3 = \beta^2$ and $V_4 = 0$. Thus $C_0 = V_0 - E_0 = 0$, $C_1 = V_1 - E_1 = 0$, $C_2 = V_2 - E_2 = 0$, $C_3 = V_3 - E_3 = 0$, $C_4 = V_4 - E_4 = 1$. Therefore $\mathbf{C} = (00001)$ and its inverse Fourier transform is given by $\mathbf{c} = (11111)$. Thus the transmitted vector was the vector $\mathbf{c} = (11111)$.

REFERENCES

[1] Andrade, A.A., Palazzo Jr., R. A note on units of a local finite rings. *Revista de Matemática e Estatística*, vol. 18, pp. 213-222, 2000.

[2] Andrade, A.A., Palazzo Jr., R. Construction and decoding of BCH codes over finite commutative rings. *Linear Algebra Applic.* v.286, pp. 69-85, 1999.

[3] Interlando, J.C., Palazzo Jr., R., Elia, M. *On the decoding of Reed-Solomon and BCH codes over integer residue rings*, IEEE Trans. Inform. Theory, IT-43 (1997), pp. 1013-1021.

[4] McDonald, B.R. *Finite rings with identity*. New York: Marcel Dekker, 1974. 429p.

[5] Blahut, R.E. *Theory and practice of error control codes*. Addison-Wesley Publishing Company, 1984, 500p.