ELSEVIER Linear Algebra and its Applications 286 (1999) 69–85

LINEAR ALGEBRA AND ITS APPLICATIONS

# Construction and decoding of BCH Codes over finite commutative rings [1]

Antonio Aparecido de Andrade [a,*], Reginaldo Palazzo Jr. [b]

[a] *Department of Mathematics, Ibilce-Unesp, P.O. Box 136, 15054-000, São José do Rio Preto, SP, Brazil*

[b] *Department of Telematics, Feec-Unicamp, P.O. Box 6101, 13081-970, Campinas, SP, Brazil*

Received 25 November 1997; accepted 22 July 1998

Submitted by R.A. Brualdi

**Abstract**

BCH codes over arbitrary finite commutative rings with identity are derived in terms of their locator vector. The derivation is based on the factorization of $x^s - 1$ over the unit ring of an appropriate extension of the finite ring. We present an efficient decoding procedure, based on the modified Berlekamp–Massey algorithm, for these codes. The code construction and the decoding procedures are very similar to the BCH codes over finite integer rings. 

*AMS classification:* 94B05; 94B35

*Keywords:* BCH codes; Galois extension; Syndrome calculation; Modified Berlekamp–Massey algorithm; Error-location numbers; Forney's method

## 1. Introduction

Linear codes over rings have recently raised a great interest for their new role in algebraic coding theory and for their successful application in combined

* Corresponding author. E-mail: andrade@mat.itbilce.unesp.br.

[1] This work has been supported by Fundação de Amparo à Pesquisa do Estado de São Paulo, FAPESP, under Grant No. 95/4720-8, and by Conselho Nacional de Desenvolvimento Científico e Tecnológico, CNPq, under Grant No. 301416/85-0.


PII: S0024-3795(98)10163-5

coding and modulation. A paper by Hammons et al. [1], has shown that certain binary nonlinear codes can be viewed, through a Gray mapping, as linear codes over the ring $\mathbb{Z}_4$. Gerônimo et al. [2] have further shown the existence of a class of linear codes over the ring $\mathbb{Z}_4 \times \mathbb{Z}_2^{k-2}$, $k > 2$, from which new binary nonlinear codes may be constructed. Note that this class of linear codes belongs to the class of concatenated codes.

Early work by Shankar [3] extended the notion of BCH codes over $GF(p)$ to classes of codes over finite rings $\mathbb{Z}_m$, with $m$ a positive integer. Recently Interlando, et al. [4] have proposed a decoding procedure based on the modified Berlekamp–Massey algorithm for these codes, defined over integer residue rings $\mathbb{Z}_q$, where $q$ is a power of a prime $p$. Since the Berlekamp–Massey algorithm takes a sequence of elements from a field and finds the shortest linear recurrence (or linear feedback shift register) that can generate this sequence, Sloane and Reeds [5] extended the algorithm to the case when the elements of the sequence are integers modulo $m$, where $m$ is an arbitrary integer with known prime decomposition.

Having the ring $\mathbb{Z}_4 \times \mathbb{Z}_2^{k-2}$ as the main motivation for the construction of linear codes, and in particular of cyclic codes, we present a construction technique of BCH codes over finite commutative rings with identity and a decoding algorithm for these codes. The construction technique is addressed, in this paper, from the point of view of specifying a cyclic subgroup of the group of units of an extension ring of finite rings. The core of the problem is the factorization of $x^s - 1$ over the group of units of the appropriate extension ring. The decoding algorithm consists of four major steps: (1) calculation of the syndromes, (2) calculation of the elementary symmetric functions by a modified Berlekamp–Massey algorithm, (3) calculation of the error-location numbers, and (4) calculation of the error magnitudes.

This paper is organized as follows. Sections 2 and 3 describe the construction of BCH codes over local finite rings and over arbitrary finite rings, respectively. In Section 4, the decoding procedure for BCH codes defined over local finite rings, which is akin to the decoding procedure for BCH codes defined over an integer residue ring $\mathbb{Z}_q$, is presented. We close this section by presenting some examples of the proposed decoding algorithm. Finally, in Section 5 the concluding remarks are drawn.

## 2. BCH Codes over local finite rings

In this section we describe a construction technique of BCH codes over local finite rings which is very similar to the one proposed by Shankar over $\mathbb{Z}_q$, [3]. This construction requires working on Galois extension rings, where some properties of the Galois extension fields are lost. First, we review the key properties of Galois extension rings, which serve to characterize BCH codes.

Throughout this section $A$ denotes a local finite commutative ring with identity, with maximal ideal $\mathcal{M}$ and residue field $\mathbb{K} = A/\mathcal{M} = GF(p^m)$, for some prime $p$, $m$ a positive integer, and $A[x]$ denotes the ring of polynomials in the variable $x$ over $A$. The natural projection $A[x] \to \mathbb{K}[x]$ is denoted by $\mu$, where $\mu(a(x)) = \bar{a}(x)$. Thus, the natural ring morphism $A \to \mathbb{K}$ is simply the restriction of $\mu$ to the constant polynomials. We employ the usual terminology for polynomials, i.e., monic, degree, etc. (see page 252 of [6]).

**Definition 2.1.** Let $f(x)$ be a polynomial in $A[x]$. We say that
- $f(x)$ is a *unit* if there is a polynomial $g(x) \in A[x]$, $g(x) \neq 0$, with $f(x)g(x) = 1$.
- $f(x) \neq 0$ is a *zero divisor* if there is a polynomial $g(x) \in A[x]$, $g(x) \neq 0$, with $f(x)g(x) = 0$.
- $f(x)$ is *regular* if $f(x)$ is not a zero divisor.
- $f(x)$ is *irreducible* if $f(x)$ is not a unit and whenever $f(x) = g(x)h(x)$, then $g(x)$ or $h(x)$ is a unit.

Let $f(x)$ be a monic polynomial of degree $h$ such that $\mu(f(x))$ is irreducible over $\mathbb{K}$ (by Theorem XIII.7 of [6], $f(x)$ is irreducible over $A$). Let $A[x]/\langle f(x)\rangle$ denote the set of residue classes of polynomials in $x$ over $A$ modulo a polynomial $f(x)$. This ring, denoted by $R$, is a commutative local ring with identity, whose maximal ideal is $\overline{\mathcal{M}}_1 = \mathcal{M}_1/\langle f(x)\rangle$, where $\mathcal{M}_1 = \langle \mathcal{M}, f(x)\rangle$ and residue field

$$\mathbb{K}_1 = \frac{R}{\overline{\mathcal{M}}_1} = \frac{A[x]/\langle f(x)\rangle}{\langle \mathcal{M}, f(x)\rangle/\langle f(x)\rangle} = \frac{A[x]}{\langle \mathcal{M}, f(x)\rangle} = \frac{(A/\mathcal{M})[x]}{\langle \mu(f(x))\rangle}$$

whose order is $p^{mh}$. The elements of $R$ which are zero divisors form an additive abelian group and consist of those polynomials of degree $h-1$ (or less) whose coefficients are all zero divisors in $A$. By Theorem XIII.2 of [6], any element in $R$ having at least one coefficient that is a unit in $A$ is a unit in $R$. Now, let $R^*$ be the multiplicative group of units of $R$ and let $\mathbb{K}_1^*$ be the multiplicative group of $\mathbb{K}_1$. It follows that $R^*$ is an abelian group, and therefore it can be expressed as a direct product of cyclic groups [6]. Here, we call attention to the fact that in rings care must be taken regarding zero divisors. That said, we are interested in the cyclic subgroup of $R^*$, denoted by $G_s$, whose elements are the roots of $x^s - 1$ for some positive integer $s$. The Theorem 2.1., which follows directly from [6], Theorem XVIII.2, provides the order of the subgroup of interest.

**Theorem 2.1.** *There is only one maximal cyclic subgroup of $R^*$ having order relatively prime to $p$. This cyclic subgroup has order $p^{mh} - 1$.*

Denote by $G_s$ the cyclic subgroup of order $s = p^{mh} - 1$ in $R^*$ which has as elements all the roots of $x^s - 1$. Next we report, without proof, two theorems from [7] that will serve as the basis for the construction of $G_s$. These theorems indicate a method for generating this cyclic subgroup.

**Theorem 2.2.** *Suppose that $\alpha$ generates a subgroup of order $s$ (divisor of $p^{mh} - 1$) in $R^*$. Then $x^s - 1$ can be factored as $x^s - 1 = (x - \alpha)(x - \alpha^2)\ldots(x - \alpha^s)$ if and only if $\overline{\alpha}$ has order $s$ in $\mathbb{K}_1^*$.*

Any polynomial $h(x)$ which is a divisor of $x^s - 1$ can be factored uniquely over $\mathbb{K}_1^*$. It follows from Theorem 2.2 that the factorization of $h(x)$ over $G_s$ is also unique. This is stated in the following corollary.

**Corollary 2.1.** *A polynomial $h(x)$, which divides $x^s - 1$ and has coefficients in $A$, can be factored over $G_s$ as $h(x) = (x - \alpha^{e_1})(x - \alpha^{e_2})\ldots(x - \alpha^{e_l})$ if and only if $\overline{h}(x)$ can be factored as $\overline{h}(x) = (x - \overline{\alpha^{e_1}})(x - \overline{\alpha^{e_2}})\ldots(x - \overline{\alpha^{e_l}})$ over the field $\mathbb{K}_1$.*

The next theorem is useful in obtaining the generator of $G_s$. It follows directly from [6], Theorem XVIII.2, that $d$ is a power of $p$.

**Theorem 2.3.** *Suppose $\overline{\alpha}$ generates a cyclic subgroup of order $s$ (divisor of $p^{mh} - 1$) in $\mathbb{K}_1^*$. Then $\alpha$ generates a cyclic subgroup of order $sd$ in $R^*$, where $d$ is an integer greater than or equal to 1 and $\alpha^d$ generates the cyclic subgroup $G_s$ of $R^*$.*

**Definition 2.2.** A shortened *BCH code* $\mathscr{C}(n, \eta)$ of length $n < s$ over $A$ has parity-check matrix

$$H = \begin{bmatrix} \alpha_1 & \alpha_2 & \cdots & \alpha_n \\ \alpha_1^2 & \alpha_2^2 & \cdots & \alpha_n^2 \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{2t} & \alpha_2^{2t} & \cdots & \alpha_n^{2t} \end{bmatrix} \tag{1}$$

for some $t \geqslant 1$, where $\eta = (\alpha_1, \alpha_2, \ldots, \alpha_n)$ is the *locator vector*, consisting of distinct elements of $G_s$. The code $\mathscr{C}(n, \eta)$, with $n = s$, will be called a *BCH code*. In this case, $\eta$ is unique up to permutation of coordinates.

Thus, a codeword $\mathbf{c} = (c_1, c_2, \ldots, c_n) \in A^n$ is in $\mathscr{C}(n, \eta)$ if and only if it satisfies the following parity-check equations over $R$

$$\sum_{i=1}^{n} c_i \alpha_i^l = 0, \quad l = 1, 2, \ldots, 2t. \tag{2}$$

For $l \geqslant 1$, each parity-check equation in Eq. (2) translates into $h$ equations over the ring $A$.

A parity-check matrix $H'$ with elements over $A$ can be obtained by replacing each element of $H$ by the corresponding column vector of length $h$ over $A$. It is possible to obtain an estimate of $d$ (minimum Hamming distance) directly from the parity-check matrix.

**Lemma 2.1** [7]. *Let $\alpha$ be an element of $G_s$ of order $s$. Then the differences $\alpha^{l_1} - \alpha^{l_2}$ are units in $R$ if $0 \leqslant l_1 \neq l_2 \leqslant s-1$.*

**Theorem 2.4.** *The minimum Hamming distance of a BCH code $\mathscr{C}(n, \eta)$ satisfies $d \geqslant 2t+1$.*

**Proof.** Suppose $\mathbf{c}$ is a nonzero codeword in $\mathscr{C}(n, \eta)$ such that $w_H(\mathbf{c}) \leqslant 2t$. Then $\mathbf{c}H^{\mathrm{T}} = 0$. Deleting $n-2t$ columns of the matrix $H$ corresponding to zeros of the codeword, it follows that the new matrix $H'$ is Vandermonde. By Lemma 2.1, it follows that the determinant is a unit in $R$. Thus, the only possibility for $\mathbf{c}$ is the all-zero codeword. □

**Example 2.1.** The ring $\mathscr{A} = \mathbb{Z}_2[i] = \{0, 1, i, 1+i\}$ is a commutative local ring with identity, where the maximal ideal is $\mathscr{M} = \{0, 1+i\}$ and the residue field is $\mathbb{K} = \mathscr{A}/\mathscr{M} = \mathbb{Z}_2$. Let $\mu : \mathscr{A}[x] \to \mathbb{Z}_2[x]$ be the natural projection. The polynomial $f(x) = x^3 + x + 1 \in \mathscr{A}[x]$ is such that $\mu(f(x)) = x^3 + x + 1$ is irreducible over $\mathbb{Z}_2$. By Theorem XIII.7 of [6], $f(x)$ is irreducible over $\mathscr{A}$. Form the ring $R = \mathscr{A}[x]/\langle f(x)\rangle$ and the residue field $\mathbb{K}_1 = \mathbb{K}[x]/\langle\mu(f(x))\rangle$, whose order is $2^3 = 8$. By Theorem 2.1, $R^*$ has only one maximal cyclic subgroup, whose order is $2^3 - 1 = 7$, which we denote by $G_7$. But the element $\alpha$ such that $f(\alpha) = 0$ has order 7 in $R^*$. Hence, the elements of $G_7$ are $1, \alpha, \alpha^2, \ldots, \alpha^6$. Letting $\eta$ be $\eta = (1, \alpha, \ldots, \alpha^6)$, then if $t = 1$ we have a BCH code $\mathscr{C}(7, \eta)$. By Theorem 2.4, this code has minimum Hamming distance at least 3.

### 2.1. BCH Codes as cyclic codes

In this section we show that by choosing a particular ordering $\eta = (\alpha_1, \ldots, \alpha_n)$ the encoding of BCH codes becomes very simple. In addition to that, we refine our estimates of the minimum Hamming distance.

Recalling the definition of BCH code: $\mathbf{c} = (c_1, c_2, \ldots, c_n)$ is a codeword iff $\sum_{i=1}^{n} c_i\alpha_i^l = 0$ for $l = 1, 2, \ldots, 2t$, where $\eta = (\alpha_1, \alpha_2, \ldots, \alpha_n)$ is an arbitrary but fixed ordering of the elements of $G_s$. Although changing from one such ordering to another cannot affect the error correcting capabilities of the code on a memoryless channel, nevertheless there is a "best" ordering for the purpose of implementation. This ordering is to set $\alpha_i = \alpha^{i-1}$, where $\alpha$ is a primitive element of $G_s$. Thus, taking $s = n$ and $\eta = (1, \alpha, \alpha^2, \ldots, \alpha^{n-1})$, where $\alpha$ is a generator of $G_n$, the matrix $H$ in Eq. (1) defines a BCH code that has a generator polynomial. Theorem 2.3 helps to determine the generator of $G_n$, and from Corollary 2.1, it follows that the distinct elements in the sequence

$$\alpha^l, (\alpha^l)^q, (\alpha^l)^{q^2}, \ldots, (\alpha^l)^{q^{h-1}},$$

where $q = p^m$, are all the roots of $M_i(x)$, the minimal polynomial of $\alpha^i$ over $A$, where $\alpha$ is a primitive element in $G_n$. Therefore, $M_i(x)$ can be constructed in a very similar way to $m_i(x)$, the minimal polynomial of $\overline{\alpha^i}$ over $\mathbb{K}$. As a consequence, we have a cyclic code, that is, a code for which every cyclic shift $(c_k, c_{k+1}, \ldots, c_{n-1}, c_0, c_1, \ldots, c_{k-1})$ of a codeword is also a codeword.

The important step in this construction is the factorization of the polynomial $x^n - 1$ over $R^*$. Once the cyclic subgroup $G_n$, of order $n$ such that $n$ divides $p^{mh} - 1$, is known, the construction is reduced to the problem of properly choosing the elements of this group to be the roots of the generator polynomial $g(x)$. Note that this polynomial is a factor of $x^n - 1$.

**Definition 2.3.** Let $\alpha$ be a primitive element of $G_n$. Then, a cyclic BCH code defined over the ring $A$ is a cyclic code of length $n$ generated by a minimal degree polynomial $g(x)$ (over $A$) whose roots are $\alpha^{b+1}, \alpha^{b+2}, \ldots, \alpha^{b+2t}$, for some $b \geqslant 0$, and $t \geqslant 1$, i.e.,

$$g(x) = \mathrm{lcm}\{M_1(x), M_2(x), \ldots, M_{2t}(x)\},$$

where $M_i(x)$, $1 \leqslant i \leqslant 2t$, is the minimal polynomial of $\alpha^{b+i}$ over $A$.

In this case, the locator vector is given by $\eta = (\alpha^0, \alpha^{b+1}, \ldots, \alpha^{(n-1)(b+1)})$ and the parity-check matrix $H$ is given by

$$H = \begin{bmatrix} 1 & \alpha^{b+1} & \alpha^{2(b+1)} & \cdots & \alpha^{(n-1)(b+1)} \\ 1 & \alpha^{b+2} & \alpha^{2(b+2)} & \cdots & \alpha^{(n-1)(b+2)} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ 1 & \alpha^{b+2t} & \alpha^{2(b+2t)} & \cdots & \alpha^{(n-1)(b+2t)} \end{bmatrix}.$$

The lowerbound on the minimum distance, derived in Theorem 2.5, applies to any cyclic code. The BCH codes are a class of cyclic codes whose generator polynomials are chosen such that the minimum distance is guaranteed by this bound.

**Theorem 2.5** (Generalization of [8, Theorem 9.1]). *Let $g(x)$ be the generator polynomial of a cyclic code over $A$, with length $n = s$, and let $\alpha^{e_1}, \alpha^{e_2}, \ldots, \alpha^{e_{n-k}}$ be the roots of $g(x)$ in $G_n$, where $\alpha$ has order $n$. The minimum Hamming distance of the code is greater than the largest number of consecutive integers modulo $n$ in the set $E = \{e_1, e_2, \ldots, e_{n-k}\}$.*

**Proof.** Let $m_0, m_0 + 1, \ldots, m_0 + d_0 - 2$ denote the largest set of consecutive integers modulo $n$ in the set $E$. A cyclic code with roots $\alpha^{e_1}, \alpha^{e_2}, \ldots, \alpha^{e_{n-k}}$ is the null space of the matrix

$$H = \begin{bmatrix} 1 & \alpha^{e_1} & (\alpha^{e_1})^2 & \cdots & (\alpha^{e_1})^{n-1} \\ 1 & \alpha^{e_2} & (\alpha^{e_2})^2 & \cdots & (\alpha^{e_2})^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha^{e_{n-k}} & (\alpha^{e_{n-k}})^2 & \cdots & (\alpha^{e_{n-k}})^{n-1} \end{bmatrix}.$$

Now, if no linear combination of $d_0 - 1$ columns of the matrix

$$H_1 = \begin{bmatrix} 1 & \alpha^{m_0} & (\alpha^{m_0})^2 & \cdots & (\alpha^{m_0})^{n-1} \\ 1 & \alpha^{m_0+1} & (\alpha^{m_0+1})^2 & \cdots & (\alpha^{m_0+1})^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha^{m_0+d_0-2} & (\alpha^{m_0+d_0-2})^2 & \cdots & (\alpha^{m_0+d_0-2})^{n-1} \end{bmatrix}$$

is zero, then clearly no linear combination of $d_0 - 1$ columns of $H$ is zero, and by Corollary 3.1 of [8], it follows that this code has minimum distance $d_0$ or greater. Matrix $H_1$ has the requisite property. This can be seen by examining the determinant of any set of $d_0 - 1$ of its columns

$$H_2 = \begin{bmatrix} (\alpha^{m_0})^{j_1} & (\alpha^{m_0})^{j_2} & \cdots & (\alpha^{m_0})^{j_{d_0-1}} \\ (\alpha^{m_0+1})^{j_1} & (\alpha^{m_0+1})^{j_2} & \cdots & (\alpha^{m_0-1})^{j_{d_0-1}} \\ \vdots & \vdots & \ddots & \vdots \\ (\alpha^{m_0+d_0-2})^{j_1} & (\alpha^{m_0+d_0-2})^{j_2} & \cdots & (\alpha^{m_0+d_0-2})^{j_{d_0-1}} \end{bmatrix}.$$

In what follows, we show that the determinant of the matrix $H_2$ is nonsingular, i.e., it is a unit in $R$. Note that the determinant of the matrix $H_2$ is given by

$$\det(H_2) = \alpha^{m_0(j_1+j_2+\cdots+j_{d_0-1})}\det(H_3) \tag{3}$$

where the matrix $H_3$ is given by

$$H_3 = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ \alpha^{j_1} & \alpha^{j_2} & \cdots & \alpha^{j_{d_0-1}} \\ (\alpha^{j_1})^2 & (\alpha^{j_2})^2 & \cdots & (\alpha^{j_{d_0-1}})^2 \\ \vdots & \vdots & \ddots & \vdots \\ (\alpha^{j_1})^{d_0-2} & (\alpha^{j_2})^{d_0-2} & \cdots & (\alpha^{j_{d_0-1}})^{d_0-2} \end{bmatrix}.$$

The determinant of $H_3$ is Vandermonde and it is given by

$$\det(H_3) = \prod_{j_i > j_k} (\alpha^{j_i} - \alpha^{j_k}). \tag{4}$$

Thus, matrix $H_2$ is nonsingular if and only if Eq. (3) is a unit in $R$ or equivalently if and only if Eq. (4) is a unit in $R$. By Lemma 2.1, it follows that the determinant in Eq. (4) is a unit in $R$. Hence, no combination of $d_0 - 1$ or fewer columns of $H$ is linearly dependent. By Corollary 3.1 of [8], the code, which is the null space of $H$, has minimum Hamming distance at least $d_0$. □

**Example 2.2.** Referring to Example 2.1, if $\alpha$ is a root of $g(x)$, then $g(x) = M_1(x) = (x - \alpha)(x - \alpha^2)(x - \alpha^4)$. Hence, the polynomial $g(x)$ generates a BCH code of length 7 over $\mathbb{Z}_2[i]$ with minimum Hamming distance at least 3.

## 3. BCH Codes over arbitrary finite rings

Let $A$ be a finite commutative ring with identity. By the Structure Theorem for Finite Commutative Rings, Theorem VI.2 of [6], the ring $A$ decomposes (up to the order of product) uniquely as a direct product (sum) of local rings, i.e., there exists an isomorphism $\phi$ defined by

$$\begin{aligned}\phi &: A \to A_1 \times A_2 \times \cdots \times A_r \\ a &\to \phi(a) = (\phi_1(a), \phi_2(a), \ldots, \phi_r(a)),\end{aligned}$$

where $\phi_i : A \to A_i = A/P_i^m$, $i = 1, 2, \ldots, r$, are the canonical homomorphisms, $P_i$, $i = 1, 2, \ldots, r$ are the maximal ideals of $A$ and $m$ is the smallest positive integer such that $\bigcap_{i=1}^r P_i^m = 0$.

**Theorem 3.1.** *Using the previous notations, the application*

$$\varphi : A[x] \to A_1[x] \times A_2[x] \times \cdots \times A_r[x]$$

*defined by* $\varphi(a(x)) = (\varphi_1(a(x)), \varphi_2(a(x)), \ldots, \varphi_r(a(x)))$, *where* $a(x) = a_0 + a_1x + \cdots + a_nx^n \in A[x]$ *and* $\varphi_i(a(x)) = \phi_i(a_0) + \phi_i(a_1)x + \cdots + \phi_i(a_n)x^n$, $i = 1, 2, \ldots, r$, *is an isomorphism.*

**Proof.** Clearly, $\varphi$ is an injective homomorphism. For the surjective homomorphism, let $g(x)$ be the polynomial $g(x) = (g_1(x), g_2(x), \ldots, g_r(x)) \in A_1[x] \times A_2[x] \times \cdots \times A_r[x]$, where $g_i(x) = a_0^i + a_1^i x + \cdots + a_n^i x^n \in A_i[x]$, $i = 1, 2, \ldots, r$. Since $\phi$ is an isomorphism, there exists $a(x) = a_0 + a_1x + \cdots + a_nx^n \in A[x]$, where $\phi(a_i) = (a_i^1, a_i^2, \ldots, a_i^r)$, $i = 0, 1, 2, \ldots, n$, such that $\varphi(a(x)) = g(x)$. Hence, $\varphi$ is an isomorphism. □

Let us specify a monic polynomial in $A[x]$ in terms of the irreducible polynomials in $A_i[x]$, $i = 1, 2, \ldots, r$. Let $\mathcal{M}_i$ be maximal ideals of the local rings $A_i$ and $\mathbb{K}_i = A_i/\mathcal{M}_i$ be the residue fields, for all $i = 1, 2, \ldots, r$. From Theorem XIII.7 of [6], if $g_i(x)$ in $A_i[x]$ is a monic polynomial such that $\mu(g_i(x))$ is irreducible in $\mathbb{K}_i[x]$, then $g_i(x)$ is irreducible in $A_i[x]$, for all $i = 1, 2, \ldots, r$.

**Theorem 3.2.** *Using the previous notations, if $g_i(x)$ are monic polynomials of degree $h$ such that $\mu(g_i(x))$ are irreducible for all $i = 1, 2, \cdots, r$, then the mapping*

$$\psi : A[x] \to \frac{A_1[x]}{\langle g_1(x)\rangle} \times \frac{A_2[x]}{\langle g_2(x)\rangle} \times \cdots \times \frac{A_r[x]}{\langle g_r(x)\rangle}$$

*defined by*

$$\psi(a(x)) = (\varphi_1(a(x)) + \langle g_1(x)\rangle, \ldots, \varphi_r(a(x)) + \langle g_r(x)\rangle)$$

*is a surjective homomorphism whose kernel is $\langle f(x)\rangle$, where $f(x) = \varphi^{-1}(g(x)) \in A[x]$ is a monic polynomial of degree $h$ over the ring $A$ with the polynomial $g(x) = (g_1(x), g_2(x), \ldots, g_r(x)) \in A_1[x] \times A_2[x] \times \cdots \times A_r[x]$.*

**Proof.** Clearly $\psi$ is a homomorphism. For the surjectiveness, let $h(x)$ be such that

$$h(x) \in \frac{A_1[x]}{\langle g_1(x)\rangle} \times \frac{A_2[x]}{\langle g_2(x)\rangle} \times \cdots \times \frac{A_r[x]}{\langle g_r(x)\rangle}.$$

Thus, we have that $h(x) = (h_1(x) + \langle g_1(x)\rangle, \ldots, h_r(x) + \langle g_r(x)\rangle)$, where $h_i(x) + \langle g_i(x)\rangle \in A_i[x]/\langle g_i(x)\rangle$, $i = 1, 2, \cdots, r$. Since $\varphi$ is surjective, there exists $a(x) \in A[x]$ such that

$$\varphi(a(x)) = (\varphi_1(a(x)), \ldots, \varphi_r(a(x))) = (h_1(x), \ldots, h_r(x)).$$

Therefore, $\psi(a(x)) = h(x)$, i.e., $\psi$ is surjective. It is clear now that $\langle f(x)\rangle \subseteq Ker(\psi)$. Otherwise

$$\varphi(f(x)) = (g_1(x), g_2(x), \ldots, g_r(x)) = (\varphi_1(f(x)), \varphi_2(f(x)), \ldots, \varphi_r(f(x))).$$

Therefore, $\varphi_i(f(x)) = g_i(x)$ for all $i = 1, 2, \ldots, r$. Considering $h(x) \in Ker(\psi)$, i.e.,

$$\psi(h(x)) = (\varphi_1(h(x)) + \langle g_1(x)\rangle, \ldots, \varphi_r(h(x)) + \langle g_r(x)\rangle) = \bar{0},$$

it follows that $\varphi_i(h(x)) = a_i(x)g_i(x)$ with $a_i(x) \in A_i[x]$, $i = 1, \ldots, r$. Considering $a(x) = (a_1(x), \ldots, a_r(x))$, there exists $b(x) \in A[x]$ such that $\varphi(b(x)) = a(x)$, i.e., $\varphi_i(b(x)) = a_i(x)$, $i = 1, 2, \ldots, r$. Therefore, $\varphi_i(h(x)) = \varphi_i(b(x))\varphi_i(f(x)) = \varphi_i(b(x)\,f(x))$, $i = 1, 2, \ldots, r$. Thus, $\varphi(h(x)) = (\varphi_1(h(x)), \varphi_2(h(x)), \ldots, \varphi_r(h(x))) = \varphi(b(x)f(x))$. Since $\varphi$ is injective, $h(x) = b(x)f(x)$, i.e., $h(x) \in \langle f(x)\rangle$. Hence, $Ker(\psi) = \langle f(x)\rangle$. $\square$

**Remark 3.1.** It follows from Theorem 3.4.1 of [9] and Theorem 3.2 that the mapping

$$\psi' : \frac{A[x]}{\langle f(x)\rangle} \to \frac{A_1[x]}{\langle g_1(x)\rangle} \times \frac{A_2[x]}{\langle g_2(x)\rangle} \times \cdots \times \frac{A_r[x]}{\langle g_r(x)\rangle}$$

defined by

$$\psi'(h(x) + \langle f(x)\rangle) = (\varphi_1(h(x)) + \langle g_1(x)\rangle, \ldots, \varphi_r(h(x)) + \langle g_r(x)\rangle),$$

where $h(x) \in A[x]$, is an isomorphism.

**Example 3.1.** Let $A$ be the ring $\mathbb{Z}_5[i] = \{a + bi\colon a, b \in \mathbb{Z}_5\}$. We have that $\mathbb{Z}_5[i]$ is isomorphic to $\mathbb{Z}_5 \times \mathbb{Z}_5$. Now, it can easily be shown that the polynomials $x^2 + 2$ and $x^2 + 3$ are monic and irreducible over the ring $\mathbb{Z}_5$. By Theorem 3.2, the polynomial $x^2 + i$ is monic over the ring $\mathbb{Z}_5[i]$ and $\mathbb{Z}_5[i][x]/\langle x^2 + i\rangle$ is isomorphic to $\mathbb{Z}_5[x]/\langle x^2 + 2\rangle \times \mathbb{Z}_5[x]/\langle x^2 + 3\rangle$.

The next theorem, Theorem XVIII.1 of [6], is fundamental in the decomposition of the polynomial $x^s - 1$ into linear factors over the ring $R^*$. This theorem asserts that for each element $\alpha \in R^*$ there exists a unique element $\beta = (\beta_1, \beta_2, \ldots, \beta_r) \in R_1^* \times R_2^* \times \cdots \times R_r^*$.

**Theorem 3.3.** *Let $R = R_1 \times R_2 \times \cdots \times R_r$, where $R_i$, $i = 1, 2, \ldots, r$, are local commutative rings. Then $R^*$ is the direct product (sum) of groups $R^* = R_1^* \times R_2^* \times \cdots \times R_r^*$.*

Considering $R = A[x]/\langle f(x)\rangle$, $R_i = A_i[x]/\langle g_i(x)\rangle$, $\mathcal{M}_i$ as the maximal ideals of $A_i$, $\mathbb{K}_i = A_i/\mathcal{M}_i = GF(p_i^{m_i})$ as the residue fields of $A_i$ and $\mu_i : A_i[x] \to \mathbb{K}_i[x]$ as the natural projections, for all $i = 1, 2, \ldots, r$, we have that $\overline{\mathcal{M}}_i = \langle \mathcal{M}_i, g_i(x)\rangle/\langle g_i(x)\rangle$ are the maximal ideals of $R_i$ and

$$\overline{\mathbb{K}}_i = \frac{A_i[x]/\langle g_i(x)\rangle}{\langle \mathcal{M}_i, g_i(x)\rangle/\langle g_i(x)\rangle} = \frac{A_i[x]}{\langle \mathcal{M}_i, g_i(x)\rangle} = \frac{(A_i/\mathcal{M}_i)[x]}{\langle \mu_i(g_i(x))\rangle} = GF(p_i^{m_i h}),$$

where $h = \deg(f)$, are the residue fields, for all $i = 1, 2, \cdots, r$. Using the isomorphism $\phi$, we have that the direct product of codes over $A_i$ is isomorphic to a code over $A$ and the minimum distance is $\min_i(d_i)$, where $d_i$ is the minimum distance of the $i$th code over $A_i$, $i = 1, 2, \ldots, r$ [10].

Theorem 3.4 indicates the condition under which $x^s - 1$ can be factored over $R^*$.

**Theorem 3.4** [3]. *The polynomial $x^s - 1$ can be factored over the multiplicative group $R^*$ as $x^s - 1 = (x - \alpha)(x - \alpha^2)\ldots(x - \alpha^s)$ if and only if $\overline{\beta}_i$ has order $s$ in $\overline{\mathbb{K}}_i^*$, where $\gcd(s, p_i) = 1$, $i = 1, 2, \cdots, r$, and $\alpha$ corresponds to $\beta = (\beta_1, \beta_2, \ldots, \beta_r)$, by Theorem 3.3.*

**Proof.** Suppose that the polynomial $x^s - 1$ can be factored over $R^*$ as $x^s - 1 = (x - \alpha)(x - \alpha^2)\ldots(x - \alpha^s)$. Then $x^s - 1$ can be factored over $R_i^*$, $i = 1, 2, \ldots, r$ as $x^s - 1 = (x - \beta_i)(x - \beta_i^2)\ldots(x - \beta_i^s)$. Now, it follows from Theorem 2.2 that $\overline{\beta}_i$ has order $s$ in $\overline{\mathbb{K}}_i^*$, $i = 1, 2, \ldots, r$. Reciprocally, suppose that $\overline{\beta}_i$ has order $s$ in $\overline{\mathbb{K}}_i^*$, $i = 1, 2, \ldots, r$. Thus, from Theorem 2.2, $x^s - 1$

can be factored uniquely over $R_i^*$ as $x^s - 1 = (x - \beta_i)(x - \beta_i^2)\ldots(x - \beta_i^s)$. Taking $\alpha \in R^*$ as the inverse image of the element $\beta = (\beta_1, \beta_2, \ldots, \beta_r) \in R_1^* \times R_2^* \times \cdots \times R_r^*$ (exists by Theorem 3.3), we have that $x^s - 1 = (x - \alpha)(x - \alpha^2)\cdots(x - \alpha^s)$. □

Let $H_{\alpha,s}$ denote the cyclic subgroup of $R^*$ generated by $\alpha$, i.e., $H_{\alpha,s}$ contains all the roots of $x^s - 1$ provided the conditions of Theorem 3.4 are met. A BCH code $\mathscr{C}$ over $A$ can be obtained as the direct product of BCH codes $\mathscr{C}_i$ over $A_i$, $i = 1, 2, \ldots, r$, and the lowerbound on the minimum distance of the code $\mathscr{C}$ is $\min_i(d_i)$, where $d_i$ is the minimum distance of the $i$th code $\mathscr{C}_i$ over $A_i$, $i = 1, 2, \ldots, r$ [10]. To construct a cyclic BCH code over $R^*$, we need to choose certain elements of $H_{\alpha,n}$, $n = s$, as the roots of the generator polynomial $g(x)$ of the code. The BCH bound for this case is established by Theorem 2.5 where the local ring is replaced by an arbitrary finite ring and $G_n$ by $H_{\alpha,n}$. So that, $\alpha^{e_1}, \alpha^{e_2}, \ldots, \alpha^{e_{n-k}}$ are all the roots of $g(x)$ in $H_{\alpha,n}$, we construct $g(x)$ as

$$g(x) = \mathrm{lcm}\{M_{e_1}(x), M_{e_2}(x), \ldots, M_{e_{n-k}}(x)\},$$

where $M_i(x)$ is the minimal polynomial of $\alpha^{e_i}$, $i = 1, 2, \cdots, n - k$. Theorem 3.5 provides us with a method for constructing $M_j(x)$, the minimal polynomial of $\alpha^j$ over $A$. The proof is very similar to the one in [3]. For the sake of completeness we repeat the proof here.

**Theorem 3.5.** *Let $M_j(x)$ be the minimal polynomial of $\alpha^j$ over $A$ where $\alpha$ generates $H_{\alpha,n}$. Then $M_j(x) = \prod_{\lambda \in S_j}(x - \lambda)$, where $S_j$ is all distinct elements of the sequence $\{(\alpha^j)^m\colon m = \prod_{i=1}^r q_i^{s_i},\ \text{for all } 0 \leqslant s_i \leqslant h - 1 \text{ and } q_i = p_i^{m_i},\ i = 1, 2, \ldots, h - 1\}$.*

**Proof.** Let $\overline{M}_j(x)$ be the projection of $M_j(x)$ over the field $\mathbb{K}_i$ and $M_j^{(i)}(x)$ the minimal polynomial of $\overline{\alpha^j}$ over $\overline{\mathbb{K}}_i^*$, for all $i = 1, 2, \ldots, r$. Clearly, $\overline{M}_j(x)$ is divisible by $M_j^{(i)}$, $i = 1, 2, \ldots, r$. Thus, among the roots of $\overline{M}_j(x)$ are the distinct elements of the sequence $\overline{\alpha^j}, \overline{\alpha^{jq_i}}, \overline{\alpha^{jq_i^2}}, \ldots, \overline{\alpha^{jq_i^{h-1}}}$ ($i$th projection). Hence, $M_j(x)$ has, among its roots, distinct elements of the sequence $\alpha^j, \alpha^{jq_i}, \alpha^{jq_i^2}, \ldots, \alpha^{jq_i^{h-1}}$, $i = 1, 2, \ldots, r$. Thus, any element $\gamma$ of the form $\gamma = (\alpha^j)^{q_i^s}$ is a root of $M_j(x)$, $1 \leqslant i \leqslant r$, $0 \leqslant s \leqslant h - 1$. Now, choose any $k$ such that $1 \leqslant k \leqslant r$ and $k \neq i$. Then, we know that $\overline{\gamma}$ in $\overline{\mathbb{K}}_k$, a root of $\overline{M}_j(x)$ in $\overline{\mathbb{K}}_k$, implies that $(\overline{\gamma})^{q_k^l}$ is a root of $\overline{M}_j(x)$ (which has coefficients in $GF(q_k)$), for all $l = 0, 1, \ldots, h - 1$. Hence, $\gamma^{q_k^l} = (\alpha^j)^{q_i^s q_k^l}$ is a root of $M_j(x)$. Proceeding in this manner, we can show that $M_j(x)$ necessarily has as roots all distinct members of $S_j$. However, since $M_j(x)$ is the minimal polynomial of $\alpha^j$ over $A$ and that all distinct elements of $S_j$ exhausts all the roots of $M_j(x)$ it follows that $M_j(x) = \prod_{\lambda \in S_j}(x - \lambda)$. □

**Example 3.2.** Let us construct a BCH code of length 24 with minimum Hamming distance at least 5 over $A = \mathbb{Z}_5[i]$. The element $\alpha = \alpha_1 + 1$

$= \psi^{-1}(\beta_1, \beta_2)$ generates $H_{\alpha,24}$, where $\beta_i = 1 + \gamma_i$ are primitive elements of $R_i$, $i = 1, 2$, respectively. Let $\alpha^4, \alpha^5, \alpha^6, \alpha^7$ be specified as roots of $g(x)$. Then, $M_4(x)$ has as roots all distinct elements in the set $S_4 = \{\alpha^4, \alpha^{20}\}$; $M_5(x)$ has as roots all distinct elements in the set $S_5 = \{\alpha, \alpha^5\}$; $M_6(x)$ has as root the element $\alpha^6$; and $M_7(x)$ has as roots all distinct elements in the set $S_7 = \{\alpha^7, \alpha^{11}\}$. Thus, the polynomial $g(x) = \mathrm{lcm}\{M_4(x), M_5(x), M_6(x), M_7(x)\}$ is given by $g(x) = (x - \alpha)(x - \alpha^4)(x - \alpha^5)(x - \alpha^6)(x - \alpha^7)(x - \alpha^{11})(x - \alpha^{20})$ generates a cyclic BCH code of length 24 over $A$ with minimum distance at least 5.

## 4. Decoding procedure

Interlando et al. [4] proposed a decoding procedure based on the modified Berlekamp–Massey algorithm for BCH codes defined over integer residue rings $\mathbb{Z}_q$, where $q$ is a power of a prime $p$. We remark that with analogous proofs this decoding procedure also applies to the BCH codes over arbitrary local finite commutative ring with identity.

In this section, we present a decoding algorithm for $\mathscr{C}(n, \eta)$, based on the modified Berlekamp–Massey algorithm, that corrects all errors up to Hamming weight $t$, i.e., whose minimum Hamming distance is greater than or equal to $2t + 1$.

We first establish some notation. Let $R$ denote the ring defined in Section 2 and $\alpha$ be a primitive element of $G_s$. Let $\mathbf{c} = (c_1, c_2, \ldots, c_n)$ be the transmitted codeword and $\mathbf{b} = (b_1, b_2, \ldots, b_n)$ be the received vector. The error vector is given by $\mathbf{e} = (e_1, e_2, \ldots, e_n) = \mathbf{b} - \mathbf{c}$. Given a locator vector $\eta = (\alpha_1, \alpha_2, \ldots, \alpha_n) = (\alpha^{k_1}, \alpha^{k_2}, \ldots, \alpha^{k_n})$, over $G_s$, we define the *syndrome values* $s_l$ of an error vector $\mathbf{e} = (e_1, e_2, \ldots, e_n)$ in the standard way

$$s_l = \sum_{j=1}^{n} b_j \alpha_j^l, \quad l \geqslant 0.$$

When $\mathbf{c} \in \mathscr{C}(n, \eta)$ is the transmitted codeword, the first $2t$ syndrome values $s_l$ can be determined from the received vector $\mathbf{b}$, as follows:

$$s_l = \sum_{j=1}^{n} e_j \alpha_j^l = \sum_{j=1}^{n} b_j \alpha_j^l, \quad l = 1, 2, \ldots, 2t.$$

The proposed decoding algorithm consists of four major steps:

*Step* 1: Calculation of the syndrome $\mathbf{s} = (s_1, s_2, \ldots, s_{2t})$ from the received vector;

*Step* 2: Calculation of the elementary symmetric functions $\sigma_1, \sigma_2, \ldots, \sigma_v$ from the syndrome vector $\mathbf{s}$;

*Step* 3: Calculation of the error-location numbers $x_1, x_2, \ldots, x_v$ from $\sigma_1, \ldots, \sigma_v$;

*Step* 4: Calculation of the error magnitudes $y_1, y_2, \ldots, y_v$ from $x_i$ and $\mathbf{s}$.

Now, each step of the decoding procedure is analysed. There is no need to comment on Step 1 since the calculation of syndromes is straightforward.

The set of possible error-location numbers consists of the elements $\alpha^0, \ldots, \alpha^{s-1}$. The elementary symmetric functions $\sigma_1, \sigma_2, \ldots, \sigma_v$ (where $v$ denotes the number of errors introduced by the channel) are defined as the coefficients of the polynomial

$$(x - x_1)(x - x_2) \ldots (x - x_v) = x^v + \sigma_1 x^{v-1} + \cdots + \sigma_{v-1} x + \sigma_v.$$

In Step 2, the calculation of the elementary symmetric functions is equivalent to finding a solution $\sigma_1, \sigma_2, \ldots, \sigma_v$, with minimum possible $v$, to the following set of linear recurrent equations over $R$

$$s_{j+v} + s_{j+v-1}\sigma_1 + \cdots + s_{j+1}\sigma_{v-1} + s_j\sigma_v = 0, \quad j = 1, 2, \ldots, 2t - v, \tag{5}$$

where $s_1, s_2, \ldots, s_{2t}$ are the components of the syndrome vector. A fast solution to the system of linear equations in Eq. (5) is provided by the modified Berlekamp–Massey algorithm, [4], that holds for commutative rings with identity. We call attention to the fact that in rings care must be taken regarding zero divisors, multiple solutions of the system of linear equations, and also with an inversionless implementation of the original Berlekamp–Massey algorithm. The algorithm is iterative, in the sense that the following $n - l_n$ equations (called *power sums*)

$$\begin{cases} s_n\sigma_0^{(n)} + s_{n-1}\sigma_1^{(n)} + \cdots + s_{n-l_n}\sigma_{l_n}^{(n)} = 0 \\ s_{n-1}\sigma_0^{(n)} + s_{n-2}\sigma_1^{(n)} + \cdots + s_{n-l_n-1}\sigma_{l_n}^{(n)} = 0 \\ \quad\vdots \\ s_{l_n+1}\sigma_0^{(n)} + s_{l_n}\sigma_1^{(n)} + \cdots + s_1\sigma_{l_n}^{(n)} = 0 \end{cases}$$

are satisfied with $l_n$ as small as possible and $\sigma^{(0)} = 1$. The polynomial $\sigma^{(n)}(x) = \sigma_0^{(n)} + \sigma_1^{(n)}x + \cdots + \sigma_{l_n}^{(n)}x^{n}$ represents the solution at the $n$th stage. The $n$th *discrepancy* will be denoted by $d_n$ and defined by $d_n = s_{n+1}\sigma_0^{(n)} + s_n\sigma_1^{(n)} + \cdots + s_{n+1-l_n}\sigma_{l_n}^{(n)}$.

The modified Berlekamp–Massey algorithm for commutative rings with identity is formulated as [4]: The inputs to the algorithm are the syndromes $s_1, s_2, \ldots, s_{2t}$ which belong to $R$. The output of the algorithm is a set of values $\sigma_i$, $1 \leqslant i \leqslant v$, such that the Eq. (5) hold with minimum $v$. Let $\sigma^{(-1)}(x) = 1$, $l_{-1} = 0$, $d_{-1} = 1$ and $\sigma^{(0)}(x) = 1$, $l_0 = 0$, $d_0 = s_1$ be the set of initial conditions to start the algorithm as in [8]. Thus, we have the following steps:

1. $n \leftarrow 0$,
2. If $d_n = 0$, then $\sigma^{(n+1)}(x) \leftarrow \sigma^{(n)}(x)$ and $l_{n+1} \leftarrow l_n$ and to go 5;

3. If $d_n \neq 0$, then find an $m \leqslant n-1$ such that $d_n - yd_m = 0$ has a solution in $y$ and $m - l_m$ has the largest value. Then, $\sigma^{(n+1)}(x) \leftarrow \sigma^{(n)}(x) - yx^{n-m}\sigma^{(m)}(x)$ and $l_{n+1} \leftarrow \max\{l_n, l_m + n - m\}$;
4. If $l_{n+1} = \max\{l_n, n+1-l_n\}$ then go to 5, else search for a solution $D^{(n+1)}(x)$ with minimum degree $l$ in the range $\max\{l_n, n+1-l_n\} \leqslant l \langle l_{n+1}$ such that $\sigma^{(m)}(x)$ defined by $D^{(n+1)}(x) - \sigma^{(n)}(x) = x^{n-m}\sigma^{(m)}(x)$ is a solution for the first $m$ power sums, $d_m = -d_n$, with $\sigma_0^{(m)}$ a zero divisor in $R$. If such a solution is found, $\sigma^{(n+1)}(x) \leftarrow D^{(n+1)}(x)$ and $l_{n+1} \leftarrow l$;
5. If $n \langle 2t-1$, then $d_{n+1} \leftarrow s_{n+2} + s_{n+1}\sigma_1^{(n+1)} + \cdots + s_{n+2-l_{n+1}}\sigma_{l_{n+1}}^{(n+1)}$;
6. $n \leftarrow n+1$; if $n < 2t$ go to 2; else stop.

The coefficients $\sigma_1^{(2t)}, \sigma_2^{(2t)}, \ldots, \sigma_v^{(2t)}$ satisfy Eq. (5). The basic difference between the modified Berlekamp–Massey algorithm and the original one lies in the fact that the modified algorithm allows updating a minimal polynomial solution $\sigma^{(n)}(x)$ (at the $n$th step) from a previous solution $\sigma^{(m)}(x)$, whose discrepancy can even be a noninvertible element in the commutative ring under consideration. This process does not necessarily lead to a minimal solution $\sigma^{(n+1)}(x)$ (at the $(n+1)$th stage). So, Step 4, calculated at Step 3, is checked to be a minimal solution. This search consists of finding a polynomial $\sigma^{(m)}(x)$, satisfying certain conditions, and which is a solution for the first $m$ power sums. Since the number of polynomials $\sigma^{(m)}(x)$ to be checked is not too large, Step 4 does not essentially increase the complexity, since the number of polynomials $\sigma^{(m)}(x)$ to be checked is not large.

In Step 3, the calculation of error location numbers over rings requires one more step than over fields, because in $R$ the solution to Eq. (5) is generally not unique and the reciprocal of the polynomial $\sigma^{(2t)}(z)$ (output by the modified Berlekamp–Massey algorithm), namely $\rho(z)$, may not be the right error locator polynomial

$$(z - x_1)(z - x_2)\ldots(z - x_v),$$

where $x_i = \alpha^{k_j}$ ($j$ is an integer in the range $1 \leqslant j \leqslant n$ such that $k_j$ indicates the position of the error in the codeword) are the correct error-location numbers, $v$ is the number of errors, and $\alpha$ is the generator of $G_s$. Thus, the procedure for the calculation of the correct error-location numbers [4] is given by

- Compute the roots of $\rho(z)$ (the reciprocal of $\sigma^{(2t)}(z)$), say, $z_1, z_2, \ldots, z_v$.
- Among the $x_i = \alpha^{k_j}$, $j = 1, 2, \ldots, n$, select those $x_i$'s such that $x_i - z_i$ are zero divisors in $R$. The selected $x_i$'s will be the correct error-location numbers and $k_j$, $j = 1, 2, \ldots, n$, indicates the position of the error in the codeword.

In Step 4, the calculation of the error magnitudes is based on Forney's method [11], where the error magnitudes $y_1, y_2, \ldots, y_v$ are obtained through

$$y_j = \frac{\sum_{l=0}^{v-1} \sigma_{jl} s_{v-l}}{\sum_{l=0}^{v-1} \sigma_{jl} x_j^{v-l}}, \quad j = 1, 2, \ldots, v \tag{6}$$

and the coefficients $\sigma_{jl}$ are recursively defined by

$$\sigma_{j,i} = \sigma_i + x_j\sigma_{j,i-1}, \quad i = 0, 1, \ldots, v-1$$

starting with $\sigma_0 = \sigma_{j,0} = 1$. Here, the critical part is to prove that the denominator in Eq. (6) is always invertible or, in other words, that it is a unit in $R$. From [11] we have that the denominator in Eq. (6) is a product

$$x_j \prod_{i=1, i\neq j}^{v-1} (x_i - x_j),$$

where each factor has the form $\alpha^i - \alpha^j$ with $0 \leqslant i, j \leqslant n-1$ and $i \neq j$. The factors $(x_i - x_j)$ are of the form $(\alpha^{l_1} - \alpha^{l_2})$, and from Lemma 2.1, they are always units in the ring $R$.

**Example 4.1.** Let $\mathscr{C}$ be a (15,7) BCH code over $\mathbb{Z}_2[i]$ generated by $g(x) = x^8 + x^4 + x^2 + x + 1$. The ring $R$ is given by $R = \mathbb{Z}_2[i]/\langle x^4 + x + 1\rangle$, where $f(x) = x^4 + x + 1$ is irreducible over $\mathbb{Z}_2$; $G_{15}$ is the cyclic subgroup of $R^*$ which contains all the roots of $x^{15} - 1$; $\alpha$ is a primitive element of $G_{15}$ and $\eta = (1, \alpha, \alpha^2, \ldots, \alpha^{14}) = (\alpha^{k_1}, \alpha^{k_2}, \ldots, \alpha^{k_{15}})$. By inspection, $\alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^6, \alpha^8, \alpha^9$ and $\alpha^{12}$ are roots of $g(x)$. Therefore, $d_{\min}(\mathscr{C}) \geqslant 5$. Hence, this code has an error correction capability equal to $t = 2$. Let $H$ be the parity-check matrix. Assume that the all-zero codeword $\mathbf{c} = (000000000000000)$ is transmitted through the channel and the error pattern is $\mathbf{e} = (0i0000000000010)$. Therefore the received vector is then given by $\mathbf{b} = \mathbf{c} + \mathbf{e}$ and the syndrome vector is given by $\mathbf{s} = \mathbf{b}H^{\mathrm{T}} = (\alpha i + \alpha^{13}, \alpha^2 i + \alpha^{11}, \alpha^3 i + \alpha^9, \alpha^4 i + \alpha^7)$. By the modified Berlekamp–Massey algorithm we obtain that $\sigma^{(4)}(z) = 1 + \alpha^{12}z + \alpha^{14}z^2$. The roots of $\rho(z) = z^2 + \alpha^{12}z + \alpha^{14}$ (the reciprocal of $\sigma^{(4)}(z)$) are $z_1 = \alpha$ and $z_2 = \alpha^{13}$. Among the elements $\alpha^0 = 1, \alpha, \alpha^2, \ldots, \alpha^{14}$, $x_1 = \alpha$ and $x_2 = \alpha^{13}$ are such that $x_1 - z_1 = x_2 - z_2 = 0$ (zero divisors in $R$). Therefore, $x_1$ and $x_2$ are the correct error-location and $k_2 = 1$ and $k_{14} = 13$ indicate that two errors have occured, one in position 2, and the other in position 14, in the codeword. The correct elementary symmetric functions $\sigma_1$ and $\sigma_2$ are obtained from $(x - x_1)(x - x_2) = x^2 + (x_1 + x_2)x + x_1x_2 = x^2 + \sigma_1 x + \sigma_2$. Thus, $\sigma_1 = \alpha^{12}$ and $\sigma_2 = \alpha^{14}$. Finally, Forney's method [11], applied to s, $\sigma_1$ and $\sigma_2$, gives $\sigma_{11} = \sigma_1 + x_1\sigma_{10} = \alpha^{12} + \alpha = \alpha^{13}$ and $\sigma_{21} = \sigma_1 + x_2\sigma_{20} = \alpha^{12} + \alpha^{13} = \alpha$. Thus, by Eq. (6), we obtain that $y_1 = i$ and $y_2 = 1$. Therefore, the error pattern is given by $\mathbf{e} = (0i0000000000010)$.

**Example 4.2.** Referring to Example 3.1, if $\mathscr{C}_1$ is a (4, 1)-code over $\mathbb{Z}_5$ generated by $g_1(x) = 2 + 3x + x^2$ with minimum Hamming distance equal to 3 and if $\mathscr{C}_2$ is a (4, 1)-code over $\mathbb{Z}_5$ generated by $g_2(x) = 1 + x + x^2 + x^3$ with minimum Hamming distance equal to 4, the code $\mathscr{C} \simeq \mathscr{C}_1 \times \mathscr{C}_2$ over $\mathbb{Z}_5$ has minimum Hamming distance equal to 3. Let $\mathbf{c}_1$ be a codeword of $\mathscr{C}_1$ and $\mathbf{c}_2$ be a codeword of $\mathscr{C}_2$. Let $\mathbf{c}_1$ and $\mathbf{c}_2$ be given by $\mathbf{c}_1 = (2, 3, 1, 0)$ and $\mathbf{c}_2 = (1, 1, 1, 1)$. The direct product of $\mathbf{c}_1$ and $\mathbf{c}_2$ leads to $\mathbf{c}_1 \times \mathbf{c}_2 = ((2,1),(3,1),(1,1),(0,1))$. By the isomorphism between $\mathbb{Z}_5[i][x]/\langle x^2+i\rangle$ and the direct product $\mathbb{Z}_5[x]/\langle x^2+2\rangle \times \mathbb{Z}_5[x]/\langle x^2+3\rangle$ the corresponding codeword in $\mathscr{C}$ is $\mathbf{c} = (4+4i, 2+3i, 1, 3+i)$. In a similar way we obtain the remaining codewords of $\mathscr{C}$. The decoding procedure for code $\mathscr{C}$ is as follows. Given the received vector $\mathbf{r} = \mathbf{r}_1 \oplus \mathbf{r}_2$, look up the closest value of each component of $\mathbf{r}$ to the corresponding elements of $\mathbb{Z}_5[i][x]/\langle x^2+i\rangle$. Once they are known, use the isomorphism to find the corresponding 2-tuple associated with each component of $\mathbf{r}$. Now, we know $\mathbf{r}_1$ and $\mathbf{r}_2$. Therefore, decode $\mathbf{r}_1$ by using the modified Berlekamp–Massey algorithm for $\mathscr{C}_1$, obtaining $\mathbf{c}_1'$ and decode $\mathbf{r}_2$ by using the modified Berlekamp–Massey algorithm for $\mathscr{C}_2$, obtaining $\mathbf{c}_2'$. Thus, the transmitted codeword is $\mathbf{c}' = \mathbf{c}_1' \oplus \mathbf{c}_2'$.

## 5. Conclusion

In this paper we presented construction and decoding procedures for BCH codes over finite commutative rings. These procedures followed essentially the same lines as the ones for BCH codes over integer residue rings $\mathbb{Z}_q$, where $q$ is a power of a prime. The construction and the decoding procedures for a BCH code of length $n$ over a finite commutative ring is based on the factorization of $x^s - 1$ over the subgroup of units of an extension ring. Once this is accomplished the procedure is analogous to that for the construction of BCH codes over integer residue rings $\mathbb{Z}_q$. The decoding procedure is based on the modified Berlekamp–Massey algorithm. The complexity of the proposed decoding algorithm is essentially the same as that for BCH codes over integer residue rings, however, with one more search for the correct roots of the error-locator polynomial.

## Acknowledgements

The authors would like to thank the referee for his helpful suggestions and comments which improved the presentation of this paper.

## References

[1] A.R. Hammons, Jr., P.V. Kumar, A.R. Calderbank, N.J.A. Sloane, P. Solé, The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals and related codes, IEEE Trans. Inform. Theory IT-40 (1994) 301–319.

[2] J.R. Gerónimo, R. Palazzo, Jr., S.R. Costa, J.C. Interlando, P. Brumatti, On the existence of $\mathbb{Z}_4 \times \mathbb{Z}_2^{k-2}$-linear codes from the nonexistence of $\mathbb{Z}_2^k$-linear binary codes, $k > 2$, II Pan-American Workshop in Applied Mathematics, Gramado, Brazil, September 7–12, 1997.

[3] P. Shankar, On BCH codes over arbitrary integer rings, IEEE Trans. Inform. Theory IT-25 (1979) 480–483.

[4] J.C. Interlando, R. Palazzo, Jr., M. Elia, On the decoding of Reed-Solomon and BCH codes over integer residue rings, IEEE Trans. Inform. Theory IT-43 (1997) 1013–1021.
[5] J.A. Reeds, N.J.A. Sloane, Shift register synthesis (mod m), SIAM J. Computing 14 (1985) 505–513.
[6] B.R. McDonald, Finite Rings with Identity, Marcel Dekker, New York, 1974.
[7] A.A. Andrade, R. Palazzo Jr., A Note on Units of a Local Finite Rings, submitted for publication.
[8] W.W. Peterson, E.J. Weldon Jr., Error Correcting Codes, 2nd ed., MIT Press, Cambridge, MA, 1972.
[9] I.N. Herstein, Topics in Algebra, Wiley, New York, 1975.
[10] A.A. Andrade, R. Palazzo Jr., Linear Block Codes over Finite Commutative Rings with identity, to appear by Rev. Mat. Estat., São Paulo, Brazil, in portuguese.
[11] G.D. Forney, Jr., On decoding BCH codes, IEEE Trans. Inform. Theory IT-11 (1965) 549–557.