Mathematical Sciences
a SpringerOpen Journal

ORIGINAL RESEARCH Open Access

Construction and decoding of BCH codes over chain of commutative rings

Tariq Shah[1], Attiq Qamar[1] and Antonio Aparecido de Andrade[2*]

Abstract

In this paper, we present a new construction and decoding of BCH codes over certain rings. Thus, for a nonnegative integer t, let $\mathcal{A}_0 \subset \mathcal{A}_1 \subset \cdots \subset \mathcal{A}_{t-1} \subset \mathcal{A}_t$ be a chain of unitary commutative rings, where each $\mathcal{A}_i$ is constructed by the direct product of appropriate Galois rings, and its projection to the fields is $\mathcal{K}_0 \subset \mathcal{K}_1 \subset \cdots \subset \mathcal{K}_{t-1} \subset \mathcal{K}_t$ (another chain of unitary commutative rings), where each $\mathcal{K}_i$ is made by the direct product of corresponding residue fields of given Galois rings. Also, $\mathcal{A}_i^*$ and $\mathcal{K}_i^*$ are the groups of units of $\mathcal{A}_i$ and $\mathcal{K}_i$, respectively. This correspondence presents a construction technique of generator polynomials of the sequence of Bose, Chaudhuri, and Hocquenghem (BCH) codes possessing entries from $\mathcal{A}_i^*$ and $\mathcal{K}_i^*$ for each i, where $0 \leq i \leq t$. By the construction of BCH codes, we are confined to get the best code rate and error correction capability; however, the proposed contribution offers a choice to opt a worthy BCH code concerning code rate and error correction capability. In the second phase, we extend the modified Berlekamp-Massey algorithm for the above chains of unitary commutative local rings in such a way that the error will be corrected of the sequences of codewords from the sequences of BCH codes at once. This process is not much different than the original one, but it deals a sequence of codewords from the sequence of codes over the chain of Galois rings.

Keywords: Units of a Galois ring, BCH code, McCoy rank, Direct product of Galois rings

MSC: 11T71; 94A15; 14G50

Introduction

Linear codes over finite rings have been hashed out in a series of papers introduced by Blake [1,2], Spiegel [3,4], and Forney [5]. Recently, a keen interest about the structure of the multiplicative group of units of certain finite local commutative rings has been developed in coding theory owing to its wondrous application, especially in the construction of Bose, Chaudhuri, and Hocquenghem (BCH) codes. Using the multiplicative group of unit elements of a Galois ring extension of $\mathbb{Z}_{p^m}$, Shankar [6] has constructed BCH codes over $\mathbb{Z}_{p^m}$. However, Andrade and Palazzo [7] have further extended this construction of BCH codes over finite commutative rings with identity. Both construction techniques of [6] and [7] have been addressed from the approach of specifying a cyclic subgroup of the group of units of an extension ring of finite commutative rings. The complexity of this study is to get the factorization of $x^n - 1$ over the group of units of the appropriate extension ring of the given local ring and then construct the generator polynomial for BCH codes.

Let $\mathcal{A}$ be a finite commutative ring with identity. The ring $\mathcal{A}^n$, with $n \in \mathbb{Z}^+$, being a free $\mathcal{A}$-module that preserves the concept of linear independence among its elements, is similar to a vector space over a field. Though it has the constraint that an $r \times r$ submatrix of $r \times n$ generator matrix M over $\mathcal{A}$ is non-singular or, equivalently, has a determinant unit in $\mathcal{A}$, the existence of non-singular matrices having no obligatory unit elements is, in fact, the primary obstacle in working over a local ring instead of a field. The notion of elementary row operations in a matrix, and its consequences, also carries over $\mathcal{A}$ with the understanding that only multiplication of a row by a unit element in $\mathcal{A}$ is allowed, which is in contrast to the multiplication by any nonzero element in the case of a field. The structure of the multiplicative group of units of $\mathcal{A}$ is the main motivation to calculate the McCoy rank [8] of a

*Correspondence: andrade@ibilce.unesp.br
[2]Department of Mathematics, São Paulo State University, São José do Rio Preto, São Paulo, 15054-000, Brazil
Full list of author information is available at the end of the article

matrix M, that is, the largest integer r such that the $r \times r$ submatrix of M has a determinant unit in $\mathcal{A}$.

Andrade and Palazzo [9] describe a construction technique of a matrix

$$M = \begin{bmatrix} \alpha_1 & \alpha_2 & \cdots & \alpha_n \\ \alpha_1^2 & \alpha_2^2 & \cdots & \alpha_n^2 \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^k & \alpha_2^k & \cdots & \alpha_n^k \end{bmatrix}$$

based on the vector $\eta = (\alpha_1, \alpha_2, \cdots, \alpha_n)$, where α_i, for $1 \leq i \leq n$, are distinct units in the unitary local ring $\mathcal{A}$ such that $1 - \alpha_j$, for $1 \leq j \leq l$, are units. By this, one can obtain the McCoy rank of the matrix M, whereas the findings of these types of units are linked with the multiplicative group $\mathcal{A}^*$ of units of the ring $\mathcal{A}$.

For $h = b^t$, where b is a prime and t is a positive integer, there exist corresponding Galois ring extensions $\mathcal{R}_i = GR(p^m, h_i)$, where $0 \leq i \leq t$ and $h_i = b^i$ (respectively, their residue fields $\mathbb{K}_i$, where $0 \leq i \leq t$ and $h_i = b^i$) of unitary local ring $(\mathcal{R}, \mathcal{M})$ with p^m elements (respectively, p elements of residue field $\mathcal{R}/\mathcal{M}$). For each i, where $0 \leq i \leq t$, it follows that $\mathcal{R}_i^*$ has one and only one cyclic subgroup G_{n_i} of order n_i (divides $p^{h_i} - 1$) relatively prime to p (it extends Theorem 2 of [6]). Furthermore, if $\overline{\beta}_i$ generates a cyclic subgroup of order n_i in $\mathbb{K}_i^*$, then β^i generates a cyclic subgroup of order $n_i d_i$ in $\mathcal{R}_i^*$, where d_i is an integer greater than or equal to 1, and $(\beta^i)^{d_i}$ generates the cyclic subgroup G_{n_i} in $\mathcal{R}_i^*$ for each i (an extension of Lemma 1 of [6]). Consequently, by extending the given algorithm of [6] for constructing a BCH type of codes with symbols from the local ring $\mathcal{A}$ for each member in chains of Galois rings and residue fields, respectively, there are two situations: $h_i = b^i$ for $i = 2$ or $h_i = b^i$ for $i \geq 2$. By these motivations, in this paper, for any $t \in \mathbb{Z}^+$, let $\mathcal{A}_0 \subset \mathcal{A}_1 \subset \cdots \subset \mathcal{A}_{t-1} \subset \mathcal{A}_t$ be a chain of unitary commutative rings, whereas for each i such that $0 \leq i \leq t$, it follows that $\mathcal{A}_i$ is a direct product of Galois rings, i.e.,

$$\begin{array}{ccccccc} \mathcal{A}_0 & = & \mathcal{R}_0 & \times & \mathcal{R}_0 & \times \cdots \times & \mathcal{R}_0 \\ \cap & & \cap & & & & \\ \mathcal{A}_1 & = & \mathcal{R}_1 & \times & \mathcal{R}_1 & \times \cdots \times & \mathcal{R}_1 \\ \cap & & \cap & & & & \\ \vdots & & \vdots & & & & \\ \cap & & \cap & & & & \\ \mathcal{A}_t & = & \mathcal{R}_t & \times & \mathcal{R}_t & \times \cdots \times & \mathcal{R}_t, \end{array}$$

whereas $\mathcal{R}_0 \subset \mathcal{R}_1 \subset \cdots \subset \mathcal{R}_{t-1} \subset \mathcal{R}_t$ is the chain of Galois rings. Corresponding to the chain $\mathcal{A}_0 \subset \mathcal{A}_1 \subset \cdots \subset \mathcal{A}_{t-1} \subset \mathcal{A}_t$, there is the chain of rings $\mathcal{K}_0 \subset \mathcal{K}_1 \subset \cdots \subset \mathcal{K}_{t-1} \subset \mathcal{K}_t$ constituted through the direct product of their residue fields, i.e.,

$$\begin{array}{ccccccc} \mathcal{K}_0 & = & \mathbb{K}_0 & \times & \mathbb{K}_0 & \times \cdots \times & \mathbb{K}_0 \\ \cap & & \cap & & & & \\ \mathcal{K}_1 & = & \mathbb{K}_1 & \times & \mathbb{K}_1 & \times \cdots \times & \mathbb{K}_1 \\ \cap & & \cap & & & & \\ \vdots & & \vdots & & & & \\ \cap & & \cap & & & & \\ \mathcal{K}_t & = & \mathbb{K}_t & \times & \mathbb{K}_t & \times \cdots \times & \mathbb{K}_t, \end{array}$$

whereas $\mathbb{K}_0 \subset \mathbb{K}_1 \subset \cdots \subset \mathbb{K}_{t-1} \subset \mathbb{K}_t$ is the chain of corresponding residue fields. Also, $\mathcal{A}_i^*$ and $\mathcal{K}_i^*$ for each i, where $0 \leq i \leq t$, are multiplicative groups of units of $\mathcal{A}_i$ and $\mathcal{K}_i$, respectively.

In this work, we present a construction technique of generator polynomials of BCH codes having entries from $\mathcal{A}_i^*$ and $\mathcal{K}_i^*$ for each i, where $0 \leq i \leq t$. Thus, this paper is organized as follows: the 'Preliminaries' section 2 contains a brief introduction of the basics of polynomial rings and some results from [7]. In the 'Sequences of BCH codes' section, we describe the construction technique of the sequence of BCH codes over the chain of commutative rings constructed by the direct product of appropriate chains of Galois rings. In the 'Decoding procedure of BCH codes' section, we present the decoding procedure for the constructed BCH codes. The 'Conclusions' section concludes the whole discussion.

Methods

Preliminaries

Assume that (A, M) is a finite unitary local commutative ring with residue field $\mathbb{K} = \frac{A}{M} \cong GF(p^m)$, where p is a prime integer and m is a positive integer. The natural projection $\pi : A[x] \to \mathbb{K}[x]$ is defined by $\pi(\sum_{i=0}^{n} a_i x^i) = \sum_{i=0}^{n} \overline{a_i} x^i$, where $\overline{a_i} = a_i + M$ for $i = 0, \cdots, n$. Thus, the natural ring morphism $A \to \mathbb{K}$ is simply the restriction of π to the constant polynomials. In the following, we recall some definitions and results from [8] for the sake of quick reference.

Definition 1. *Let $a(x)$ be a polynomial in $A[x]$. We say that*

1. *$a(x)$ is a unit if there exists a polynomial $b(x) \in A[x]$ such that $a(x)b(x) = 1$.*
2. *$a(x) \neq 0$ is a zero divisor if there exists a polynomial $b(x) \in A[x] \setminus \{0\}$ such that $a(x)b(x) = 0$.*
3. *$a(x)$ is regular if $a(x)$ is not a zero divisor.*
4. *$a(x)$ is irreducible if $a(x)$ is not a unit, and if $a(x) = a_1(x)a_2(x)$, then either $a_1(x)$ is a unit or $a_2(x)$ is a unit.*

Theorem 2. (Theorem XIII.2 of [8]) *Let (A,M) be a local ring and $a(x) = \sum_{i=0}^{n} a_i x^i \in A[x]$. The following assertions are equivalent:*

1. *$a(x)$ is regular.*
2. *$\langle a_1, a_2, \cdots, a_n \rangle = A$.*
3. *a_i is a unit for some i, for $0 \le i \le n$.*
4. *$\pi(a(x)) \neq 0$.*

Theorem 3. (Theorem XV.1 of [8]) *Let (A,M) be a local ring and $a(x)$ be a regular polynomial in $A[x]$ such that $\pi(a(x))$ has a simple (i.e., non-multiple) zero $\bar{\alpha}$ in $\mathbb{K}$. Then, $a(x)$ has one and only one zero α with $\pi(\alpha) = \bar{\alpha}$.*

Theorem 4. (Theorem XIII.7 of [8]) *Let (A,M) be a local ring and $a(x)$ be a regular polynomial in $A[x]$ such that $\pi(a(x))$ is irreducible in $\mathbb{K}[x]$. Then, $a(x)$ is irreducible in $A[x]$.*

Let A_j be a finite local ring with characteristic p_j, for each j such that $1 \le j \le s$. Let $\mathbb{K}_j$ be the residue fields of local rings $R_j = A_j[x]/\langle f_j(x)\rangle$, where $f_j(x)$ is a basic irreducible polynomial over A_j of degree h, for each j such that $1 \le j \le s$.

Theorem 5. (Theorem 3.3 of [7]) *Let $\mathcal{R} = R_1 \times R_2 \times R_3 \times \cdots \times R_s$, where each R_j is a local finite commutative (Galois) ring. Then, $\mathcal{R}^* = R_1^* \times R_2^* \times R_3^* \times \cdots \times R_s^*$.*

The following theorem indicates the condition under which $x^s - 1$ can be factored over $\mathcal{R}^*$:

Theorem 6. (Theorem 3.4 of [7]) *The polynomials $x^s - 1$ can be factored over the multiplicative group $\mathcal{R}^*$ as $x^s - 1 = (x-\alpha)(x-\alpha^2)\cdots(x-\alpha^s)$ if and only if $\overline{\beta_j}$ has order s in $\mathbb{K}_j^*$, where $gcd(s, p_j) = 1$ and α corresponds to $\beta = (\beta_1, \beta_2, \cdots, \beta_s)$, for $j = 1, 2, 3, \cdots, s$.*

Theorem 7. (Theorem 3.5 of [7]) *For any positive integer l, let $M_l(x)$ be the minimal polynomial of α^l over $\mathcal{R}$, where α generates $\mathcal{G}_n$. Then, $M_l(x) = \prod_{\xi \in B_l}(x-\xi)$, where B_l are all distinct elements of the sequence $\{(\alpha^l)^m : m = \prod_{j=1}^{s} q_j^{s_j},\ q_j = p_j^{m_j},\ 0 \le s_j \le h-1\}$.*

Theorem 8. (Theorem 2.5 of [7]) *Let $g(x)$ be the generator polynomial of BCH code over A with length $n = s$ such that $\alpha^{e_1}, \alpha^{e_2}, \cdots, \alpha^{e_{n-k}}$ are the roots of $g(x)$ in $H_{\alpha,n}$, where α has order n, then the minimum Hamming distance of the code is greater than the largest number of consecutive integers modulo n in $E = \{e_1, e_2, e_3, \cdots, e_{n-k}\}$.*

Sequences of BCH codes

Let (A,M) be a unitary finite local commutative ring with residue field $\mathbb{K} = \frac{A}{M}$ having p^m elements. The natural projection $\pi : A[x] \to K[x]$ is defined by $\pi(\sum_{i=0}^{n} a_i x^i) = \sum_{i=0}^{n} \overline{a_k} x^i$, where $\overline{a_i} = a_i + M$ for $i = 0, 1, \cdots, n$. Thus, the natural ring morphism $A \to \mathbb{K}$ is simply the restriction of π to the constant polynomials. Now, if $f(x) \in A[x]$ is a basic irreducible polynomial with degree $h = b^t$, where b is a prime and t is a positive integer, then $\mathcal{R} = \frac{A[x]}{\langle f(x)\rangle} = GR(p^m, h)$ is the Galois ring extension of A and $\mathbb{K} = \frac{\mathcal{R}}{\mathcal{M}} = \frac{A[x]/\langle f(x)\rangle}{\langle M, f(x)\rangle/\langle f(x)\rangle} = \frac{A[x]}{\langle M, f(x)\rangle} = \frac{(A/M)[x]}{\langle \pi(f(x))\rangle} = GF(p^{mh})$ is the residue field of $\mathcal{R}$, where $\mathcal{M} = \langle M, f(x)\rangle/\langle f(x)\rangle$ is the maximal ideal of $\mathcal{R}$.

For the construction of a chain of Galois rings, the following lemma is of central importance:

Lemma 9. (Lemma VII of [8]) *Every subring of $GR(p^k, h)$ is a Galois ring of the form $GR(p^k, h')$, where h' divides h. Conversely, if h' divides h, then $GR(p^k, h)$ contains a unique copy of $GR(p^k, h')$.*

Since $1, b, b^2, \cdots, b^{t-1}, b^t$ are divisors of h, so take $h_0 = 1, h_1 = b, h_2 = b^2, \cdots, h_t = b^t = h$, and by Lemma 9, it follows that there exist basic irreducible polynomials $f_1(x), f_2(x), \cdots, f_t(x) \in A[x]$ with degrees $h_1, h_2, \cdots, h_t$, respectively, such that we can constitute the Galois subrings $\mathcal{R}_i = \frac{A[x]}{\langle f_i(x)\rangle} = GR(p^m, h_i)$, for each i, where $1 \le i \le t$, of $\mathcal{R}$ with the maximal ideals $\mathcal{M}_i = \langle M, f_i(x)\rangle/\langle f_i(x)\rangle$, for $1 \le i \le t$. Thus, the residue fields of each $\mathcal{R}_i$ becomes

$$\mathbb{K}_i = \frac{\mathcal{R}_i}{\mathcal{M}_i} = \frac{A[x]/\langle f_i(x)\rangle}{\langle M, f_i(x)\rangle/\langle f_i(x)\rangle} = \frac{A[x]}{\langle M, f_i(x)\rangle} = \frac{(A/M)[x]}{\langle \pi(f_i(x))\rangle}$$

$$= \frac{\mathbb{K}[x]}{\langle \bar{f}_i(x)\rangle} = GF(p^{h_i}).$$

As h_i divides h_{i+1} for all $0 \le i \le t$, so by Lemma 9, it follows that there is a chain

$$A = \mathcal{R}_0 \subset \mathcal{R}_1 \subset \mathcal{R}_2 \subset \cdots \subset \mathcal{R}_{t-1} \subset \mathcal{R}_t = \mathcal{R}$$

of Galois rings with corresponding chain of residue fields

$$\mathbb{Z}_p = \mathbb{K}_0 \subset \mathbb{K}_1 \subset \mathbb{K}_2 \subset \cdots \subset \mathbb{K}_{t-1} \subset \mathbb{K}.$$

If $\mathcal{A}_i = \mathcal{R}_i^{r'}$ for $0 \le i \le t$, then we obtain a chain of another unitary commutative rings, i.e.,

$$\mathcal{A}_0 \subset \mathcal{A}_1 \subset \mathcal{A}_2 \subset \cdots \subset \mathcal{A}_{t-1} \subset \mathcal{A}_t = \mathcal{A}$$

with a corresponding chain of rings

$$\mathcal{K}_0 \subseteq \mathcal{K}_1 \subseteq \mathcal{K}_2 \subseteq \cdots \subseteq \mathcal{K}_{t-1} \subseteq \mathcal{K}_t = \mathcal{K},$$

where $\mathcal{K}_i = \mathbb{K}_i^{r'}$ for $0 \le i \le t$.

Let $\mathcal{A}_i^*$ and $\mathbb{K}_i^*$ be the multiplicative group of units of $\mathcal{A}_i$ and $\mathbb{K}_i$, respectively, for $0 \le i \le t$. The next corollary of Theorem XVIII.1 of [8] plays a fundamental role in the decomposition of the polynomial $x^{n_i} - 1$ into linear factors over the rings $\mathcal{A}_i^*$. This theorem asserts that for each element $\alpha_i \in \mathcal{A}_i^*$, there exist unique elements $\beta_i \in \mathcal{R}_i^*$,

for $0 \le i \le t$, such that $\alpha_i = (\beta_i, \beta_i, \cdots, \beta_i)$ are ordered r'-tuples.

Corollary 10. *Let $\mathcal{A}_i = \mathcal{R}_i^{r'}$, for $0 \le i \le t$, where each $\mathcal{R}_i$ is a local finite commutative ring. Then, $\mathcal{A}_i^* = (\mathcal{R}_i^*)^{r'}$.*

The following theorem indicates the condition under which $x^{n_i} - 1$ can be factored over $\mathcal{A}_i^*$, for $0 \le i \le t$:

Theorem 11. *For $0 \le i \le t$, the polynomials $x^{n_i} - 1$ can be factored over the multiplicative groups $\mathcal{A}_i^*$ as $x^{n_i} - 1 = (x-\alpha_i)(x-\alpha_i^2)\cdots(x-\alpha_i^{n_i})$ if and only if $\overline{\beta_i}$ has order $n_i = p^{h_i}-1$ in $\mathbb{K}_i^*$, where $gcd(n_i, p) = 1$ and $\alpha_i = (\beta_i, \beta_i, \cdots, \beta_i)$.*

Proof. Suppose that the polynomials $x^{n_i} - 1$ can be factored over $\mathcal{A}_i^*$ as $x^{n_i} - 1 = (x-\alpha_i)(x-\alpha_i^2)\cdots(x-\alpha_i^{n_i})$. Then, $x^{n_i} - 1$ can be factored over $\mathcal{R}_i^*$ as $x^{n_i} - 1 = (x-\beta_i)(x-\beta_i^2)\cdots(x-\beta_i^{n_i})$, for $0 \le i \le t$. Now, it follows from the extension of Theorem 3 of [6] that $\overline{\beta_i}$ has order n_i in $\mathbb{K}_i^*$, for $0 \le i \le t$. Conversely, suppose that $\overline{\beta_i}$ has order n_i in $\mathbb{K}_i^*$, for $0 \le i \le t$. Again, it follows from the extension of Theorem 3 of [6] that the polynomials $x^{n_i} - 1$ can be factored over $\mathcal{R}_i^*$ as $x^{n_i} - 1 = (x-\beta_i)(x-\beta_i^2)\cdots(x-\beta_i^{n_i})$, for $0 \le i \le t$. Since $\alpha_i = (\beta_i, \beta_i, \cdots, \beta_i)$, for $0 \le i \le t$, it follows that $x^{n_i} - 1 = (x-\alpha_i)(x-\alpha_i^2)\cdots(x-\alpha_i^{n_i})$ over $\mathcal{A}_i^*$, for $0 \le i \le t$. □

Corollary 12. (Theorem 3.4 of [7]) *The polynomials $x^n - 1$ can be factored over the multiplicative group $\mathcal{R}^*$ as $x^n - 1 = (x-\alpha)(x-\alpha^2)\cdots(x-\alpha^n)$ if and only if $\overline{\alpha}$ has order n in $\mathbb{K}^*$, where $gcd(n, p) = 1$.*

Let $\mathcal{G}_{n_i}$ denote the cyclic subgroup of $\mathcal{A}_i^*$ generated by α_i, for each i, where $0 \le i \le t$, i.e., $\mathcal{G}_{n_i}$ contains all the roots of $x^{n_i} - 1$ provided that the conditions of Theorem 11 are met. The BCH codes $\mathcal{C}_i$ over $\mathcal{A}_i^*$ can be obtained as the direct product of BCH codes C_i over $\mathcal{R}_i^*$. To construct the cyclic BCH codes $\mathcal{C}_i$ over $\mathcal{A}_i^*$, we need to choose certain elements of $\mathcal{G}_{n_i}$ as the roots of generator polynomials $g_i(x)$ of the codes, so $\alpha_i^{e_1}, \alpha_i^{e_2}, \alpha_i^{e_3}, \cdots, \alpha_i^{e_{n_i-k_i}}$ are all the roots of $g_i(x)$ in $\mathcal{G}_{n_i}$. We construct $g_i(x)$ as

$$g_i(x) = \mathrm{lcm}\{M_i^{e_1}(x), M_i^{e_2}(x), \cdots, M_i^{e_{n_i-k_i}}(x)\},$$

where $M_i^{e_{l_i}}(x)$ are the minimal polynomials of $\alpha_i^{e_{l_i}}$, for $l_i = 1, 2, \cdots, n_i - k_i$, where each $\alpha_i^{e_{l_i}} = (\beta_i^{e_{l_i}}, \beta_i^{e_{l_i}}, \cdots, \beta_i^{e_{l_i}})$. The following theorem extended Lemma 3 of [6] and provides a method for the construction of $M_i^{e_{l_i}}(x)$, the minimal polynomials of $\alpha_i^{e_{l_i}}$ over the ring $\mathcal{A}_i$.

Theorem 13. *For each i, where $0 \le i \le t$, let $M_i^{e_{l_i}}(x)$ be the minimal polynomials of $\alpha_i^{e_{l_i}}$ over $\mathcal{A}_i$, where $\alpha_i^{e_{l_i}}$ generates $\mathcal{G}_{n_i}$, for $l_i = 1, 2, \cdots, n_i - k_i$. Then, $M_i^{e_{l_i}}(x) = \prod_{\xi_i \in B_i^{l_i}} (x - \xi_i)$, where $B_i^{l_i} = \{(\alpha_i^{e_{l_i}})^{p^{q_i}} : 1 \le l_i \le n_i - k_i,\ 0 \le q_i \le h_i - 1\}$.*

Proof. Let $\overline{M}_i^{e_{l_i}}(x)$ be the projection of $M_i^{e_{l_i}}(x)$ over the fields $\mathbb{K}_i$ and $\overline{M}_{i,j}^{e_{l_i}}(x)$ be the minimal polynomial of $\overline{\alpha}_i^{e_{l_i}}$ over $\mathbb{K}_i^*$, for each i such that $0 \le i \le t$ and $1 \le l_i \le n_i - k_i$. We can verify that each $\overline{M}_i^{e_{l_i}}(x)$ (the projection of $M_i^{e_{l_i}}(x)$) is divisible by $\overline{M}_{i,j}^{e_{l_i}}(x)$ (minimal polynomials of $\overline{\alpha}_i^{e_{l_i}}$), for each i such that $0 \le i \le t$ and $1 \le l_i \le n_i - k_i$. So, among its roots, it has distinct elements of the sequence $\overline{\alpha}_i^{e_{l_i}}, (\overline{\alpha}_i^{e_{l_i}})^p, (\overline{\alpha}_i^{e_{l_i}})^{p^2}, \cdots, (\overline{\alpha}_i^{e_{l_i}})^{p^{h_i-1}}$, for each i such that $0 \le i \le t$ and $1 \le l_i \le n_i - k_i$. Consequently, $M_i^{e_{l_i}}(x)$ has, among its roots, distinct elements of the sequence $\alpha_i^{e_{l_i}}, (\alpha_i^{e_{l_i}})^p, (\alpha_i^{e_{l_i}})^{p^2}, \cdots, (\alpha_i^{e_{l_i}})^{p^{(h_i-1)}}$, for $0 \le i \le t$ and $1 \le l_i \le n_i - k_i$. Thus, any element $\xi_i = (\alpha_i^{e_{l_i}})^{p^{q_i}}$ of the above sequence is a root of $M_i^{e_{l_i}}(x)$, for $0 \le i \le t$, $0 \le q_i \le h_i - 1$ and $1 \le l_i \le n_i - k_i$. Hence, $M_i^{e_{l_i}}(x) = \prod_{\xi_i \in B_i^{l_i}} (x - \xi_i)$. □

Remark 14. *Since, for each i such that $0 \le i \le t$, $\overline{M}_i^{e_{l_i}}(x)$ is the projection of $M_i^{e_{l_i}}(x)$ (minimal polynomial of $\alpha_i^{e_{l_i}}$) over the fields $\mathbb{K}_i$, it follows that $\overline{M}_i^{e_{l_i}}(x)$ generates the sequence of codes over the special chain of rings $\mathcal{K}_i = \mathbb{K}_i^{r'}$.*

The lower bound on the minimum distances derived in the following theorem applies to any cyclic code. The BCH codes are a class of cyclic codes whose generator polynomials are chosen so that the minimum distances are guaranteed by this bound. In this sense, the following theorem generalizes Theorem 2.5 of [7]:

Theorem 15. *Let $\mathcal{A}_0 \subset \mathcal{A}_1 \subset \mathcal{A}_2 \subset \cdots \subset \mathcal{A}_{t-1} \subset \mathcal{A}_t$ be the chain. For each i such that $0 \le i \le t$, if $g_i(x)$ is the generator polynomial of BCH code $\mathcal{C}_i$ over $\mathcal{A}_i$ with length n_i such that $\alpha_i^{e_1}, \alpha_i^{e_2}, \cdots, \alpha_i^{e_{n_i-k_i}}$ are the roots of $g_i(x)$ in $\mathcal{G}_{n_i}$, where α_i has order n_i, then the minimum Hamming distance of $\mathcal{C}_i$ is greater than the largest number of consecutive integers modulo n_i in $E_i = \{e_1, e_2, e_3, \cdots, e_{n_i-k_i}\}$.*

Proof. For each i, where $0 \le i \le t$, let $\{k_i, k_i + 1, k_i + 2, \cdots, k_i + d_i - 2\}$ be the largest set of consecutive integers modulo n_i in the set E_i. A sequence of cyclic code with roots $\alpha_i^{e_1}, \alpha_i^{e_2}, \alpha_i^{e_3}, \cdots, \alpha_i^{e_{n_i-k_i}}$ is the null space of the matrix

$$M_i = \begin{bmatrix} 1 & \alpha_i^{e_1} & (\alpha_i^{e_1})^2 & \cdots & (\alpha_i^{e_1})^{n_i-1} \\ 1 & \alpha_i^{e_2} & (\alpha_i^{e_2})^2 & \cdots & (\alpha_i^{e_2})^{n_i-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha_i^{e_{n_i-k_i}} & (\alpha_i^{e_{n_i-k_i}})^2 & \cdots & (\alpha_i^{e_{n_i-k_i}})^{n_i-1} \end{bmatrix}.$$

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

$$M_i^* = \begin{bmatrix} 1 & \alpha_i^{k_i} & (\alpha_i^{k_i})^2 & \cdots & (\alpha_i^{k_i})^{n_i-1} \\ 1 & \alpha_i^{k_i+1} & (\alpha_i^{k_i+1})^2 & \cdots & (\alpha_i^{k_i+1})^{n_i-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha_i^{k_i+d_i-2} & (\alpha_i^{k_i+d_i-2})^2 & \cdots & (\alpha_i^{k_i+d_i-2})^{n_i-1} \end{bmatrix}$$

is zero, then clearly no linear combination of $d_i - 1$ columns of each M_i is zero, and by the extended form of Corollary 3.1 of [10], it follows that each code has a minimum distance d_i or greater. This can be seen by examining the determinants of any $d_i - 1$ columns of the matrices M_i^*. Let M_i^{**} be the matrix where the entries is a collection of any set of $d_i - 1$ columns of matrix M_i^*. Thus,

$$M_i^{**} = \begin{bmatrix} (\alpha_i^{k_i})^{j_1} & (\alpha_i^{k_i})^{j_2} & \cdots & (\alpha_i^{k_i})^{j_{d_i-1}} \\ (\alpha_i^{k_i+1})^{j_1} & (\alpha_i^{k_i+1})^{j_2} & \cdots & (\alpha_i^{k_i+1})^{j_{d_i-1}} \\ \vdots & \vdots & \ddots & \vdots \\ (\alpha_i^{k_i+d_i-2})^{j_1} & (\alpha_i^{k_i+d_i-2})^{j_2} & \cdots & (\alpha_i^{k_i+d_i-2})^{j_{d_i-1}} \end{bmatrix}.$$

Now, we want to show that the determinants of matrices M_i^{**} are non-singular, i.e., it is a unit in each $\mathcal{A}_i$. Note that the determinant of each matrix M_i^{**} is given by

$$det(M_i^{**}) = \alpha_i^{k_i(j_1+j_2+\cdots+j_{d_i-1})} det(M_i^{***}),$$

where the matrix M_i^{***} is given by

$$M_i^{***} = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ \alpha_i^{j_1} & \alpha_i^{j_2} & \cdots & \alpha_i^{j_{d_i-1}} \\ (\alpha_i^{j_1})^2 & (\alpha_i^{j_2})^2 & \cdots & (\alpha_i^{j_{d_i-1}})^2 \\ \vdots & \vdots & \ddots & \vdots \\ (\alpha_i^{j_1})^{d_i-2} & (\alpha_i^{j_2})^{d_i-2} & \cdots & (\alpha_i^{j_{d_i-1}})^{d_i-2} \end{bmatrix}.$$

The determinant of each M_i^{***} is Vandermonde and each having a unit determinant in each ring $\mathcal{A}_i$. Hence, no combination of $d_i - 1$ or fewer columns of each M_i is linearly dependent. So, by Corollary 3.1 of [10], it follows that each code has a minimum distance d_i or greater. □

Corollary 16. (Theorem 2.5 of [7]) *Let $g(x)$ be the generator polynomial of BCH code over A with length n such that $\alpha^{e_1}, \alpha^{e_2}, \cdots, \alpha^{e_{n-k}}$ are the roots of $g(x)$ in $\mathcal{G}_n$, where α has order n. Then, the minimum Hamming distance of the code is greater than the largest number of consecutive integers modulo n in $E = \{e_1, e_2, e_3, \cdots, e_{n-k}\}$.*

We can also use the extension of Theorem 4 of [6] for the BCH bound of these codes.

Algorithm

The algorithm for constructing a BCH type of cyclic codes over the chain of rings $\mathcal{A}_0 \subseteq \mathcal{A}_1 \subseteq \mathcal{A}_2 \subseteq \cdots \subseteq \mathcal{A}_{t-1} \subseteq \mathcal{A}_t = \mathcal{A}$ is then as follows:

1. Choose irreducible polynomials $f_i(x)$ over $\mathbb{Z}_{p^m}$ of degree $h_i = b^i$, for $1 \leq i \leq t$, which are also irreducible over $GF(p)$ and form the chain of Galois rings

$$\mathbb{Z}_{p^m} = GR(p^m, h_0) \subset GR(p^m, h_1) \subset \cdots \subset GR(p^m, h_{t-1}) \subset GR(p^m, h_t) \text{ or}$$

$$A = \mathcal{R}_0 \subseteq \mathcal{R}_1 \subseteq \mathcal{R}_2 \subseteq \cdots \subseteq \mathcal{R}_{t-1} \subseteq \mathcal{R}_t = \mathcal{R}$$

and its corresponding chain of residue fields is

$$\mathbb{Z}_p = GF(p) \subset GF(p^{h_1}) \subset \cdots \subset GF(p^{h_{t-1}}) \subset GF(p^h) \text{ or}$$

$$= \mathbb{K}_0 \subset \mathbb{K}_1 \subset \mathbb{K}_2 \cdots \subset \mathbb{K}_{t-1} \subset \mathbb{K},$$

where each $GF(p^{h_i}) \simeq \frac{\mathbb{K}[x]}{\langle \pi(f_i(x)) \rangle}$, for $1 \leq i \leq t$.

2. Now, put $\mathcal{A}_i = \mathcal{R}_i^{r'}$, for $0 \leq i \leq t$, and get a chain of rings

$$\mathcal{A}_0 \subset \mathcal{A}_1 \subset \mathcal{A}_2 \subset \cdots \subset \mathcal{A}_{t-1} \subset \mathcal{A}_t = \mathcal{A}$$

with another chain of rings

$$\mathcal{K}_0 \subset \mathcal{K}_1 \subset \mathcal{K}_2 \subset \cdots \subset \mathcal{K}_{t-1} \subset \mathcal{K}_t = \mathcal{K},$$

where each $\mathcal{K}_i = \mathbb{K}_i^{r'}$, for $0 \leq i \leq t$.

3. Let $\overline{\eta_i}$ be the primitive element in $\mathbb{K}_i^*$, for $0 \leq i \leq t$. Then, η_i has order $d_i n_i$ in $\mathcal{R}_i^*$ for some integers d_i and put $\beta_i = (\eta_i)^{d_i}$. Thus, $\alpha_i = (\beta_i, \beta_i, \beta_i, \cdots, \beta_i)$ has order n_i in $\mathcal{R}_i^*$ and generates $\mathcal{G}_{n_i}$. Assume that for each i, where $0 \leq i \leq t$, α_i be any element of $\mathcal{G}_{n_i}$.
4. Let $\alpha_i^{e_1}, \alpha_i^{e_2}, \alpha_i^{e_3}, \cdots, \alpha_i^{e_{n_i-k_i}}$ be the roots of $g_i(x)$. Find the minimal polynomials $M_i^{e_{l_i}}(x)$ of $\alpha_i^{e_{l_i}}$, for $l_i = 1, 2, \cdots, n_i - k_i$, where each $\alpha_i^{e_{l_i}} = (\beta_i^{e_{l_i}}, \beta_i^{e_{l_i}}, \beta_i^{e_{l_i}}, \cdots, \beta_i^{e_{l_i}})$. Thus, $g_i(x)$ are given by

$$g_i(x) = lcm\{M_i^{e_1}(x), M_i^{e_2}(x), \cdots, M_i^{e_{n_i-k_i}}(x)\}.$$

The length of each code in the chain is the least common multiple of the orders of $\alpha_i^{e_1}, \alpha_i^{e_2}, \alpha_i^{e_3}, \cdots, \alpha_i^{e_{n_i-k_i}}$, and the minimum distance of the code is greater than the largest number of consecutive integers modulo n_i in the set $E_i = \{e_1, e_2, e_3, \cdots, e_{n_i-k_i}\}$ for each i, where $0 \leq i \leq t$.

Now, we give the following definition of the sequence of the BCH codes over the chain of Galois rings as in [11].

Definition 17. *Let α_i be a primitive element of $\mathcal{G}_{n_i}$. A sequence of BCH-type codes over the chain of Galois rings $\mathcal{A}_i$ is a sequence of cyclic codes of length n_i generated by the polynomials $g_i(x)$ with minimum degree whose distinct roots are $\alpha_i^{b_i+1}, \alpha_i^{b_i+2}, \alpha_i^{b_i+3}, \cdots, \alpha_i^{b_i+2t_i}$, for some $b_i \geq 0$, and $t_i \geq 1$, i.e., $g_i(x) = lcm\{M_i^1(x), M_i^2(x), \cdots, M_i^{2t_i}(x)\}$, where $M_i^{l_i}(x)$, for $1 \leq l_i \leq 2t_i$, are minimal polynomials of $\alpha_i^{b_i+l_i}$.*

From Definition 17, it turns out that $v_i(x) = v_{i,0} + v_{i,1}x + v_{i,2}x^2 + \cdots + v_{i,n_i-1}x^{n_i-1} \in \mathbb{Z}_{p^k}[x]$ is a collection of codewords if and only if $v_i(\alpha_i^{b_i+l_i}) = 0$, for $1 \leq l_i \leq 2t_i$ and $0 \leq i \leq t$. Therefore, a collection of parity-check matrices H_i for the sequence of BCH-type codes having $g_i(x)$ as the generator polynomial is given by

$$H_i = \begin{bmatrix} 1 & \alpha_i^{b_i+1} & \alpha_i^{2(b_i+1)} & \cdots & \alpha_i^{(n_i-1)(b_i+1)} \\ 1 & \alpha_i^{b_i+2} & \alpha_i^{2(b_i+2)} & \cdots & \alpha_i^{(n_i-1)(b_i+2)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha_i^{b_i+2t_i} & \alpha_i^{2(b_i+2t_i)} & \cdots & \alpha_i^{(n_i-1)(b_i+2t_i)} \end{bmatrix}. \quad (1)$$

Thus, $v_i(x)$ is a collection of codewords if and only if $v_i H_i^t = 0$. From the previous discussion, we have the following theorem which is an extension of Theorem 5 of [11]:

Theorem 18. *The minimum Hamming distance of the sequence of BCH codes defined by the matrices in Equation 1 is greater than or equal to $min\{2t_i + 1$, for $0 \leq i \leq t\}$.*

Now, we end this section by the following example:

Example 19. *We initiate by constructing a chain of codes of lengths 1, 3, and 15 over the ring $A = \mathbb{Z}_4$. Since $M = \{0, 2\}$, it follows that $\mathbb{K} = \frac{A}{M} \simeq \mathbb{Z}_2$. The regular polynomial $f(x) = x^4 + x + 1 \in \mathbb{Z}_4[x]$ is such that $\pi(f(x)) = x^4 + x + 1$ is an irreducible polynomial with degree $h = 2^2$ over $\mathbb{Z}_2$. By Theorem 4, it follows that $f(x) = x^4 + x + 1$ is irreducible over A. Let $R = \frac{\mathbb{Z}_4[x]}{\langle f(x)\rangle} = GR(2^2, 4)$ be the Galois ring and $\mathbb{K} = \frac{\mathbb{Z}_2[x]}{\langle \pi(f(x))\rangle} = GF(2^4)$ be the corresponding Galois field. The numbers 1, 2, and 2^2 are the only divisors of 4, and therefore, say, $h_1 = 1$, $h_2 = 2$, and $h_3 = 2^2$. Then, there exist irreducible polynomials $f_1(x) = x^2 - x + 1$ and $f_2(x) = f(x)$ in $\mathbb{Z}_4[x]$ with degrees $h_2 = 2$ and $h_3 = 4$ such that we can constitute the Galois rings $\mathcal{R}_i = \frac{\mathbb{Z}_4[x]}{\langle f_i(x)\rangle} = GR(2^2, h_i)$, where $1 \leq i \leq 2$. So, $A = \mathcal{R}_0 \subset \mathcal{R}_1 \subset \mathcal{R}_2 = \mathcal{R}$. Again, by the same argument, it follows that $\mathbb{K}_i = \frac{\mathbb{Z}_2[x]}{\langle \pi(f_i(x))\rangle} = GF(2^{h_i})$, where $1 \leq i \leq 2$, that is, $\mathbb{K}_0 = \mathbb{Z}_2$, $\mathbb{K}_1 = GF(2^2)$, and $\mathbb{K}_2 = \mathbb{K} = GF(2^4)$, with $\mathbb{K}_0 \subset \mathbb{K}_1 \subset \mathbb{K}$. If $r' = 2$, then $\mathcal{A}_i = \mathcal{R}_i \times \mathcal{R}_i$ such that $\mathcal{A}_0 \subset \mathcal{A}_1 \subset \mathcal{A}_2$. Let $u = \{X\}$ in $\mathcal{R}_i$ such that $\overline{u} = \{x\} \in \mathbb{K}_i$. Then, $\overline{u}$ has order 15 in $\mathbb{K}_2$, and therefore, $\overline{\beta}_2 = \overline{u}$. However, u has order 30 in $\mathcal{R}_2$, so put $\beta_2 = u^2$ and get $\alpha_2 = (\beta_2, \beta_2)$ which generates $\mathcal{G}_{15}$. The elements of $\mathcal{G}_{15}$ are given by*

$$\alpha_2 = (x^2, x^2)$$
$$\alpha_2^2 = (3x + 3, 3x + 3)$$
$$\alpha_2^3 = (3x^3 + 3x^2, 3x^3 + 3x^2)$$
$$\alpha_2^4 = (x^2 + 2x + 1, x^2 + 2x + 1)$$
$$\alpha_2^5 = (2x^3 + x^2 + 3x + 3, 2x^3 + x^2 + 3x + 3)$$
$$\alpha_2^6 = (3x^3 + x^2 + x + 3, 3x^3 + x^2 + x + 3)$$
$$\alpha_2^7 = (x^3 + 3, x^3 + 3)$$
$$\alpha_2^8 = (2x^2 + 3x, 2x^2 + 3x)$$
$$\alpha_2^9 = (3x^3 + 2x + 2, 3x^3 + 2x + 2)$$
$$\alpha_2^{10} = (2x^3 + 3x^2 + x, 2x^3 + 3x^2 + x)$$
$$\alpha_2^{11} = (x^3 + 2x^2 + 3x + 1, x^3 + 2x^2 + 3x + 1)$$
$$\alpha_2^{12} = (3x^3 + x + 2, 3x^3 + x + 2)$$
$$\alpha_2^{13} = (x^3 + 3x^2 + x, x^3 + 3x^2 + x)$$
$$\alpha_2^{14} = (x^3 + 3x^2 + 1, x^3 + 3x^2 + 1)$$
$$\alpha_2^{15} = (1, 1).$$

Also, $\overline{u}$ has order 3 in $\mathbb{K}_1^*$, so $\overline{\beta}_1 = \overline{u}$. However, u has order 6 in $\mathcal{R}_1$, so $\beta_1 = u^2$ and get $\alpha_1 = (\beta_1, \beta_1)$ which generates $\mathcal{G}_3$. The elements of $\mathcal{G}_3$ are given by

$$\alpha_1 = (x + 3, x + 3)$$
$$\alpha_1^2 = (3x, 3x)$$
$$\alpha_1^3 = (1, 1).$$

Put $\beta_0 = 1$ and get $\alpha_0 = (\beta_0, \beta_0)$ which generates $\mathcal{G}_1$. Choose α_2, α_2^3, α_1, and α_0 to be the roots of the generator polynomials $g_i(x)$ of the BCH codes $\mathcal{C}_i$ over the chain $\mathcal{A}_0 \subset \mathcal{A}_1 \subset \mathcal{A}_2$. Thus, $M_0^1(x)$, $M_1^1(x)$, and $M_2^1(x)$ have, as roots, all distinct elements in the sets $B_0^1 = \{\alpha_0\} \subset \mathcal{G}_1$, $B_1^1 = \{\alpha_1, \alpha_1^2\} \subset \mathcal{G}_3$, and $B_2^1 = \{\alpha_2, \alpha_2^2, \alpha_2^4, \alpha_2^8\} \subset \mathcal{G}_{15}$, respectively. So,

$$M_0^1(x) = a_1x + a_3,\ M_1^1(x) = a_1x^2 + a_1x + a_1,\ \text{and}$$
$$M_2^1(x) = a_1x^4 + a_1x^2 + a_3x + a_1,$$

and, similarly,

$$M_2^3(x) = a_1x^4 + a_1x^3 + a_1x^2 + a_1x + a_1.$$

Thus, the generator polynomials are given by

$g_0(x) = a_1x + a_3,\ g_1(x) = a_1x^2 + a_1x + a_1$, *and*

$g_2(x) = a_1x^8 + a_1x^7 + a_2x^6 + a_1x^5 + a_2x^4 + a_1x^3 + a_1x^2 + a_1$,

which generate the cyclic BCH codes $\mathcal{C}_0$, $\mathcal{C}_1$, and $\mathcal{C}_2$ of lengths 1, 3, and 15 over the direct product of $A(r)'$ times with minimum hamming distances at least 2, 4, and 5, respectively. Also,

$$g_0(x) = a_1x + a_1,\ g_1(x) = a_1x^2 + a_1x + a_1, \text{ and}$$

$$g_2(x) = a_1x^8 + a_1x^7 + a_1x^5 + a_1x^3 + a_1x^2 + a_1,$$

generate the cyclic BCH codes $\mathcal{C}'_0$, $\mathcal{C}'_1$, and $\mathcal{C}'_2$ of lengths 1, 3, and 15 over $\mathcal{K}_i$ with minimum hamming distances at least 2, 4, and 5, respectively, for each i such that $0 \le i \le 2$. Note that here $a_1 = (1, 1)$, $a_2 = (2, 2)$, and $a_3 = (3, 3)$. If we take 1, 2, and 3 instead of a_1, a_2, and a_3 in the above polynomial, then we get the generator polynomials of the codes C_i and $\overline{C}_i$ over $\mathcal{R}_i$ and $\mathbb{K}_i$, respectively.

Results and discussion

Decoding procedure of BCH codes

In this section, we turn to the problem of decoding BCH codes of length n_i, contrived to correct up to $r't_i$ errors. In [11], a decoding procedure is proposed based on the modified Berlekamp-Massey algorithm for BCH codes defined over the integer residue ring $\mathbb{Z}_{p^k}$. We have observed that even with almost evident analogous proofs, this decoding procedure is applied to the BCH codes over the chains of arbitrary finite local commutative rings with identity and also to the BCH codes over the direct product of the chain of local commutative rings with identity.

Let $\mathbb{Z}_{p^k} = \mathcal{R}_0 \subset \mathcal{R}_1 \subset \mathcal{R}_2 \subset \cdots \subset \mathcal{R}_{t-1} \subset \mathcal{R}$ be a chain of rings $GR(p^k, h_0) \subset GR(p^k, h_1) \subset GR(p^k, h_2) \subset \cdots \subset GR(p^k, h_t)$ and β_i be a collection of primitive elements of G_{n_i}, for $1 \le i \le t$. Similarly, let $\mathbb{K}_0 \subset \mathbb{K}_1 \subset \mathbb{K}_2 \subset \cdots \subset \mathbb{K}_{t-1} \subset \mathbb{K}$ be the chain of corresponding Galois fields. Since $\mathcal{A}_i = \mathcal{R}_i^{r'}$, for $0 \le i \le t$, it follows that the new chain of rings is given by

$$\mathcal{A}_0 \subset \mathcal{A}_1 \subset \mathcal{A}_2 \subset \cdots \subset \mathcal{A}_{t-1} \subset \mathcal{A}_t = \mathcal{A}$$

with its projection over the chain of fields given by

$$\mathcal{K}_0 \subset \mathcal{K}_1 \subset \mathcal{K}_2 \subset \cdots \subset \mathcal{K}_{t-1} \subset \mathcal{K}_t = \mathcal{K},$$

i.e., each $\mathcal{K}_i = \mathbb{K}_i^{r'}$, for $1 \le i \le t$. Let $c_i = (c_{i,1}, c_{i,2}, c_{i,3}, \cdots, c_{i,n_i})$ be the sequence of transmitted codewords from the sequence of codes $\mathcal{C}_i$. So, each $c_{i,k_i} = (c_{i,k_i}, c_{i,k_i}, c_{i,k_i}, \cdots, c_{i,k_i})$, for $1 \le k_i \le n_i$, is again a sequence of transmitted codewords from the sequence of codes C_i over the chain of Galois rings $\mathcal{R}_0 \subset \mathcal{R}_1 \subset \mathcal{R}_2 \subset \cdots \subset \mathcal{R}_{t-1} \subset \mathcal{R}$. Let $r_i = (r_{i,1}, r_{i,2}, r_{i,3}, \cdots, r_{i,n_i})$ be the sequence of received vectors, where each $r_{i,k_i} = (r_{i,k_{i,1}}, r_{i,k_{i,2}}, r_{i,k_{i,3}}, \cdots, r_{i,k_{i,r'}})$, for $1 \le k_i \le n_i$ and $1 \le i \le t$. Thus, the error vector is given by $e_i = r_i - c_i = (e_{i,1}, e_{i,2}, e_{i,3}, \cdots, e_{i,n_i})$, where $e_{i,k_i} = r_{i,k_i} - c_{i,k_i} = (e_{i,k_{i,1}}, e_{i,k_{i,2}}, e_{i,k_{i,3}}, \cdots, e_{i,k_{i,r'}})$, for $1 \le k_i \le n_i$ and $1 \le i \le t$. The proposed decoding procedure consists of four major steps like in [11], for $1 \le i \le t$:

1. Calculation of sequences of the syndrome $s_i = (s_{i,1}, s_{i,2}, s_{i,3}, \cdots, s_{i,2t_i})$ such that $s_i = r_i H_i^T = (s_{i,1}, s_{i,2}, s_{i,3}, \cdots, s_{i,2t_i})$, where each $s_{i,w_i} = (s_{i,w_{i,1}}, s_{i,w_{i,2}}, s_{i,w_{i,3}}, \cdots, s_{i,w_{i,r'}})$, for $1 \le w_i \le 2t_i$ and $1 \le i \le t$.
2. Calculation of sequences of 'elementary symmetric functions' $\sigma_{i,1}, \sigma_{i,2}, \sigma_{i,3}, \cdots, \sigma_{i,\nu_i}$ from s_i, where each $\sigma_{i,u_i} = (\sigma_{i,u_{i,1}}, \sigma_{i,u_{i,2}}, \sigma_{i,u_{i,3}}, \cdots, \sigma_{i,u_{i,r'}})$, for $1 \le u_i \le \nu_i$ and $1 \le i \le t$.
3. Calculation of the sequences of the error location numbers $X_{i,1}, X_{i,2}, X_{i,3}, \cdots, X_{i,\nu_i}$ from $\sigma_{i,1}, \sigma_{i,2}, \sigma_{i,3}, \cdots, \sigma_{i,\nu_i}$, where each $X_{i,u_i} = (X_{i,u_{i,1}}, X_{i,u_{i,2}}, X_{i,u_{i,3}}, \cdots, X_{i,u_{i,r'}})$, for $1 \le u_i \le \nu_i$ and $1 \le i \le t$.
4. Calculation of the sequences of the error magnitudes $Y_{i,1}, Y_{i,2}, Y_{i,3}, \cdots, Y_{i,\nu_i}$ from $s_{i,j}$, where each $Y_{i,u_i} = (Y_{i,u_{i,1}}, Y_{i,u_{i,2}}, Y_{i,u_{i,3}}, \cdots, Y_{i,u_{i,r'}})$, for $1 \le u_i \le \nu_i$ and $1 \le i \le t$.
5. Without loss of generality, we can assume that the set of consecutive roots of the generator polynomials of the sequence of BCH codes is given by $\alpha_i, \alpha_i^2, \alpha_i^3, \cdots, \alpha_i^{2t_i}$, for $1 \le i \le t$. We can also define the sets of error location numbers, i.e., it consists of the elements $(\beta_i^{\varepsilon_{i,1}}, \beta_i^{\varepsilon_{i,2}}, \cdots, \beta_i^{\varepsilon_{i,r'}})$, where $\varepsilon_{i,j}$ are any positive integers, for $1 \le i \le t$ and $1 \le j \le r'$. Let ν_i be the number of errors introduced by the channel in each code $\mathcal{C}_i$. Thus, the elementary symmetric functions $\sigma_{i,1}, \sigma_{i,2}, \sigma_{i,3}, \cdots, \sigma_{i,\nu_i}$ of the error location numbers $X_{i,1}, X_{i,2}, X_{i,3}, \cdots, X_{i,\nu_i}$ are defined as the coefficients of the polynomials

$$(X - X_{i,1})(X - X_{i,2}) \cdots (X - X_{i,\nu_i}) = X^{\nu_i} + \sigma_{i,1}X^{\nu_i - 1} + \cdots + \sigma_{i,\nu_i - 1}X + \sigma_{i,\nu_i},$$

and also, the relation of syndromes to the error location numbers and to the magnitudes of the errors are given by the equation

$$s_{i,w_i} = \sum_{u_i=1}^{\nu_i} Y_{i,u_i} X_{i,u_i}^{w_i}, \quad \text{for } 1 \le w_i \le 2t_i. \tag{2}$$

In the following, each step of the decoding process is analyzed. Since the syndrome calculation is so simple, there is no need to annotate on step 1.

In step 2, we want to calculate the elementary symmetric functions. It is equivalent to finding the sequences of solution sets $\sigma_{i,1}, \sigma_{i,2}, \sigma_{i,3}, \cdots, \sigma_{i,\nu_i}$, with minimum possi-

ble v_i, to the following sets of linear recurrent equations over each $\mathcal{R}_i$

$$s_{i,x_i+v_i} + s_{i,x_i+v_i-1}\sigma_{i,1} + \cdots + s_{i,x_i+1}\sigma_{i,v_i-1} + s_{i,x_i}\sigma_{i,v_i} = 0, \quad \text{for } x_i = 1, 2, \cdots, 2t_i - v_i, \tag{3}$$

where the coefficients of σ_{i,u_i}, for $1 \le u_i \le v_i$, are the components of the syndrome vectors. A quick solution to Equation 3 is made available by the following extension of the modified Berlekamp-Massey algorithm that holds for the chain of commutative rings with identity. We concentrate on the fact that in rings, we want to take care about zero divisors, multiple solutions of the systems of linear equations, and also with an inversionless implementation of the extension of the original Berlekamp-Massey algorithm. In [11], it is shown that the solution of each system to Equation 3 is unique if and only if all the error magnitudes are units in $\mathcal{R}_i$. Let the $n_{i,j}$th power sums be defined as

$$\begin{cases} s_{i,j}^{(n_{i,j})}(\sigma_{i,j}^{(0)})^{(n_{i,j})} + s_{i,j}^{(n_{i,j}-1)}(\sigma_{i,j}^{(1)})^{(n_{i,j})} + \cdots + s_{i,j}^{(n_i-l_{n_i})}(\sigma_{i,j}^{(l_{n_{i,j}})})^{(n_{i,j})} = 0 \\ s_{i,j}^{(n_{i,j}-1)}(\sigma_{i,j}^{(0)})^{(n_{i,j})} + s_{i,j}^{(n_{i,j}-2)}(\sigma_{i,j}^{(1)})^{(n_{i,j})} + \cdots + s_{i,j}^{(n_{i,j}-l_{n_{i,j}}-1)}(\sigma_{i,j}^{(l_{n_{i,j}})})^{(n_{i,j})} = 0 \\ \vdots \\ s_{i,j}^{(l_{n_{i,j}}+1)}(\sigma_{i,j}^{(0)})^{(n_{i,j})} + s_{i,j}^{(l_{n_{i,j}})}(\sigma_{i,j}^{(1)})^{(n_{i,j})} + \cdots + s_{i,j}^{(1)}(\sigma_{i,j}^{(l_{n_{i,j}})})^{(n_{i,j})} = 0, \end{cases} \tag{4}$$

where $s_{i,j}^{(1)}, s_{i,j}^{(2)}, s_{i,j}^{(3)}, \cdots, s_{i,j}^{(2t_{i,j})}$ are the sequences of the components of the syndrome vectors and $\sigma_{i,j}^{(1)}, \sigma_{i,j}^{(2)}, \sigma_{i,j}^{(3)}, \cdots, \sigma_{i,j}^{(v_{i,j})}$ are the sequences of elementary symmetric functions. The proposed algorithm is also an iterative method. In this method, at the $n_{i,j}$th step, the decoder seeks to determine the collection of sets of $l_{n_{i,j}}$ values $(\sigma_{i,j}^{(u_{i,j})})^{(n_{i,j})}$ such that the systems of $n_{i,j} - l_{n_{i,j}}$ equations, given in Equation 4, are satisfied with $l_{n_{i,j}}$ as small as possible, for $1 \le i \le t$ and $1 \le j \le r'$, where $(\sigma_{i,j}^{(0)})^{(0)} = 1$, for $1 \le i \le t$ and $1 \le j \le r'$. The polynomials

$$(\sigma_{i,j})^{(n_{i,j})}(X) = (\sigma_{i,j}^{(0)})^{(n_{i,j})} + (\sigma_{i,j}^{(1)})^{(n_{i,j})}X + \cdots + (\sigma_{i,j}^{(l_{n_{i,j}})})^{(n_{i,j})}X^{l_{n_{i,j}}}$$

represent the solutions at the $n_{i,j}$th stage. The $n_{i,j}$th discrepancy will be denoted by $d_{n_{i,j}}$ and defined by

$$d_{n_{i,j}} = s_{i,j}^{(n_{i,j}+1)}(\sigma_{i,j}^{(0)})^{(n_{i,j})} + s_{i,j}^{(n_{i,j})}(\sigma_{i,j}^{(1)})^{(n_{i,j})} + \cdots + s_{i,j}^{(n_{i,j}-l_{n_i}+1)}(\sigma_{i,j}^{(l_{n_{i,j}})})^{(n_{i,j})}.$$

Next, we give two lemmas as extensions of Lemmas 1 and 2 of [11], concerning the determination of $(\sigma_{i,j})^{(n_{i,j}+1)}(X)$ from $(\sigma_{i,j})^{(n_{i,j})}(X)$, that is, we update the solution polynomial $(\sigma_{i,j})^{(n_{i,j})}(X)$ at each $n_{i,j}$th step, although it is not necessary to have the lowest values of $l_{n_{i,j}}$.

The following lemma extended Lemma 1 of [11]:

Lemma 20. *Suppose that $(\sigma_{i,j})^{(n_{i,j})}(X)$, for each i with $1 \le i \le t$ and each j with $1 \le j \le r'$, are solutions to the first $n_{i,j}$ power sums and has next discrepancy $d_{n_{i,j}} \ne 0$. Let*

$$(\sigma_{i,j})^{(m_{i,j})}(X) = 1 + (\sigma_{i,j}^{(1)})^{(m_{i,j})}X + \cdots + (\sigma_{i,j}^{(l_{m_{i,j}})})^{(m_{i,j})}X^{l_{m_{i,j}}}$$

be a polynomial solution to the first $m_{i,j}$ power sums, for each i and j, where $1 \le m_{i,j} < n_{i,j}$, such that the linear equations in $\mathcal{R}_{i,j}$ given by

$$d_{n_{i,j}} - yd_{m_{i,j}} = 0$$

have solutions in y. Then, the polynomials

$$(\sigma_{i,j})^{(n_{i,j}+1)}(X) = (\sigma_{i,j})^{(n_{i,j})}(X) - yX^{n_{i,j}-m_{i,j}}(\sigma_{i,j})^{(m_{i,j})}(X)$$

are solutions to the first $n_{i,j} + 1$ power sums. Moreover, $l_{n_{i,j}+1} = \max\{l_{n_{i,j}}, l_{m_{i,j}} + n_{i,j} - m_{i,j}\}$.

Proof. Since $(\sigma_{i,j})^{(n_{i,j})}(X)$, for each i with $1 \le i \le t$ and each j with $1 \le j \le r'$, are solutions to the first $n_{i,j}$ power sums, it follows that each system of equations in Equation 4 holds, i.e.,

$$\sum_{u_i=0}^{l_{n_i}} s_{i,j_i-u_i}\sigma_{i,u_i}^{(n_i)} = \{d_{n_i}, \text{ if } j_i = n_i + 10 \text{ i } l_{n_i} + 1 \le j_i \le n_i. \tag{5}$$

Similarly, $\sigma_i^{(m_i)}(X)$ is a solution to the first m_i power sums

$$\sum_{u_i=0}^{l_{m_i}} s_{i,j_i-u_i}\sigma_{i,u_i}^{(m_i)} = \{d_{m_i}, \text{ if } j_i = m_i + 10 \text{ if } l_{m_i} + 1 \le j_i \le m_i. \tag{6}$$

If

$$\sigma_i^{(n_i+1)}(X) = \sigma_i^{(n_i)}(X) - yX^{n_i-m_i}\sigma_i^{(m_i)}(X)$$

is a solution to the first $n_i + 1$ power sums, then we must have

$$\sum_{u_i=0}^{l_{n_i+1}} s_{i,j_i-u_i}\sigma_{i,u_i}^{(n_i+1)} = 0, \text{ for } l_{n_i+1} + 1 \le j_i \le n_i + 1. \tag{7}$$

This sum has the form

$$\sum_{u_i=0}^{l_{n_i+1}} s_{i,j_i-u_i}(\sigma_{i,u_i}^{(n_i)} - y\sigma_{i,u_i-(n_i-m_i)}^{(m_i)}). \tag{8}$$

Since $\sigma_{i,u_i}^{(n_i)} = 0$, for $u_i < 0$ and $u_i > l_{n_i}$, and $\sigma_{i,u_i}^{(m_i)} = 0$, for $u_i < 0$ and $u_i > l_{m_i}$, it follows that Equation 8 can be written as

$$\sum_{u_i=0}^{l_{n_i}} s_{i,j_i-u_i}\sigma_{i,u_i}^{(n_i)} - y\sum_{u_i=n_i-m_i}^{l_{m_i}+n_i-m_i} s_{i,j_i-u_i}\sigma_{i,u_i-(n_i-m_i)}^{(m_i)} \tag{9}$$

(or in another way, as $\sum_{u_i=0}^{l_{n_i}} s_{i,j_i-u_i}\,\sigma_{i,u_i}^{(n_i)} - y\sum_{u_i=0}^{l_{m_i}} s_{i,j_i-u_i-(n_i-m_i)}\sigma_{i,u_i}^{(m_i)}$). Note that for $j_i = n_i + 1$, the first sum in Equation 9 has the value d_{n_i} and the second has the value d_{m_i}. Thus, Equation 9 reduces to $d_{n_i} - yd_{m_i} = 0$ and is true. By Equation 5, it follows that the first sum in Equation 9 is zero, provided that $l_{n_i} + 1 \le j_i \le n_i$. By Equation 6, it follows that the second sum in Equation 9 is zero, provided that $l_{m_i} + 1 \le j_i - (n_i - m_i) \le m_i$ or, equivalently, provided that $n_i - m_i + l_{m_i} + 1 \le j_i \le n_i$. Therefore, Equation 9 is satisfied, provided that

$$\max\{l_{n_i}, l_{m_i} + n_i + m_i\} + 1 \le j_i \le n_i + 1.$$

Since $(n_i+1)-\max\{l_{n_i}, l_{m_i}+n_i+m_i\}$ equations in Equation 4 are satisfied by $\sigma_i^{(n_i+1)}(X)$, it follows that their degree is formally given by

$$l_{n_i+1} = \max\{l_{n_i}, l_{m_i} + n_i + m_i\}.$$

Finally, note that the coefficients of the higher powers of the indeterminate X in $\sigma_i^{(n_i+1)}(X)$ may be zero, and therefore, the additional equations in Equation 4 may be further satisfied. □

The following lemma extended Lemma 2 of [11]:

Lemma 21. *For each i, where* $1 \le i \le t$, *let* $\sigma_i^{(n_i)}(X)$, l_{n_i} *and* $d_{n_i} \ne 0$ *be defined as in Lemma 20. Suppose that* $\sigma_i^{(n_i+1)}(X)$ *is any polynomial solution satisfying* $n_i + 1 - l_{n_i+1}$ *power sums. Then,*

$$\sigma_i^{(n_i+1)}(X) = \sigma_i^{(n_i)}(X) - a_i X^{n_i-m_i}\sigma_i^{(m_i)}(X),$$

where each a_i *is a unit in* $\mathcal{R}_i$ *and* $\sigma_{i,0}^{(m_i)}(X) = 1$. *Therefore, each polynomial* $\sigma_i^{(m_i)}(X)$ *is a polynomial solution to the first* $m_i - l_{m_i}$ *equations of Equation 4 and has next discrepancy satisfying* $d_{n_i} + ad_{m_i} = 0$ *and* $l_{m_i} = l_{n_i+1} - (n_i - m_i)$.

Proof. By hypothesis,

$$\sum_{u_i=0}^{l_{n_i+1}} s_{i,j_i-u_i}\sigma_{i,u_i}^{(n_i+1)} = 0, \text{ for } l_{n_i+1}+1 \le j_i \le n_i+1 \quad (10)$$

and

$$\sum_{u_i=0}^{l_{n_i}} s_{i,j_i-u_i}\sigma_{i,u_i}^{(n_i)} = \{d_{n_i} \ne 0 \text{ if } j_i = n_i+10 \text{ if } l_{n_i}+1 \le j_i \le n_i. \quad (11)$$

Since $\sigma_i^{(n_i)}(X)$ is a minimal solution, for $l_{n_i+1} \ge l_{n_i}$, it follows that subtracting Equation 11 from Equation 10 for $l_{n_i+1} + 1 \le j_i \le n_i + 1$, we get

$$\sum_{u_i=0}^{l_{n_i+1}} s_{i,j_i-u_i}(\sigma_{i,u_i}^{(n_i+1)} - \sigma_{i,u_i}^{(n_i)}) = \{-d_{n_i} \text{ if } j_i = n_i + 10 \text{ if } l_{n_i+1}+1 \le j_i \le n_i. \quad (12)$$

Now, suppose that the first $n_i - m_i$ coefficients of s_{i,j_i-u_i} are zero (note that since $\sigma_{i,0}^{(n_i+1)} = \sigma_{i,0}^{(n_i)} = 1$, it follows that $n_i - m_i > 0$, i.e., $n_i > m_i$). Thus, Equation 12 reduces to

$$\sum_{u_i=n_i-m_i}^{l_{n_i+1}} s_{i,j_i-u_i}(\sigma_{i,u_i}^{(n_i+1)} - \sigma_{i,u_i}^{(n_i)}) = \{-d_{n_i} \text{ if } j_i = n_i + 10 \text{ if } l_{n_i+1}+1 \le j_i \le n_i. \quad (13)$$

Letting $l_{m_i} = l_{n_i+1} - (n_i - m_i)$, Equation 13 can be rewritten as

$$\sum_{u_i=0}^{l_{m_i}} s_{i,j_i-u_i}(\sigma_{i,u_i+n_i-m_i}^{(n_i+1)} - \sigma_{i,u_i+n_i-m_i}^{(n_i)}) = \{-d_{n_i} \text{ if } j_i = m_i + 10 \text{ if } l_{m_i}+1 \le j_i \le m_i. \quad (14)$$

Finally, define the polynomial $\sigma_i^{(m_i)}(X)$ by

$$\sigma_i^{(m_i)} = (\sigma_{i,u_i+n_i-m_i}^{(n_i+1)} - \sigma_{i,u_i+n_i-m_i}^{(n_i)})a^{-1}, \text{ for } 0 \le u_i \le l_{m_i}.$$

Thus,

$$\sum_{u_i=0}^{l_{n_i}} s_{i,j_i-u_i}\sigma_{i,u_i}^{(m_i)} = \{-d_{n_i}a^{-1} = d_{m_i} \text{ if } j_i = m_i + 10 \text{ if } l_{m_i}+1 \le j_i \le m_i. \quad (15)$$

By Equation 15, it follows that each $\sigma_i^{(m_i)}(X)$ is a solution to the first $m_i - l_{m_i}$ equations in Equation 4 and each has next discrepancy d_{m_i} such that $d_{n_i} + ad_{m_i} = 0$. The degree of $\sigma_i^{(m_i)}(X)$ is given formally by $l_{m_i} = l_{n_i+1} - (n_i - m_i)$. Note that the coefficients of the higher powers of the indeterminate X in $\sigma_i^{(m_i)}(X)$ may be zero; thus, some additional equations in Equation 4 may be satisfied, i.e., $\sigma_i^{(m_i)}(X)$ may not be minimal. □

Now, based on these two lemmas, we show that the following theorem is an extension of Theorem 6 of [11]:

Theorem 22. *For each i with $1 \le i \le t$, let $\sigma_i^{(n_i)}(X)$ be a solution polynomial at the n_ith stage and let $\sigma_i^{(m_i)}(X)$ be one of the prior minimal solutions, for $1 \le m_i < n_i$, such that $d_{n_i} - yd_{m_i} = 0$ has solutions in y and $m_i - l_{m_i}$ has the largest value. Further, suppose each $\sigma_i^{(n_i)}(X)$ is updated in the following way:*

1. *If $d_{n_i} = 0$, then*

$$\sigma_i^{(n_i+1)}(X) = \sigma_i^{(n_i)}(X) \text{ and } l_{n_i+1} = l_{n_i}. \tag{16}$$

2. *If $d_{n_i} \neq 0$, then*

$$\sigma_i^{(n_i+1)}(X) = \sigma_i^{(n_i)}(X) - yX^{n_i-m_i}\sigma_i^{(m_i)}(X) \text{ and } l_{n_i+1} = l_{n_i}$$

and

$$l_{n_i+1} = \max\{l_{n_i}, l_{m_i} + n_i - m_i\}. \tag{17}$$

If there is no solution $D^{(n_i+1)}(X)$ with degree less than $\max\{l_{n_i}, l_{m_i} + n_i - m_i\}$ and such that the coefficient of the lowest power of the indeterminate X in $D^{(n_i+1)}(X) - \sigma_i^{(n_i)}(X)$ is a zero divisor in $\mathcal{R}_i$, then each $\sigma_i^{(n_i+1)}(X)$ is a minimal polynomial solution at the $(n_i + 1)$th stage.

Proof. If $d_{n_i} = 0$, then $\sigma_i^{(n_i+1)}(X) = \sigma_i^{(n_i)}(X)$ are minimal solutions since $\sigma_i^{(n_i)}(X)$ are also minimal solutions. Now, consider the case where $d_{n_i} \neq 0$. Since each $\sigma_i^{(m_i)}(X)$ and $\sigma_i^{(n_i)}(X)$ are known, it follows that $\sigma_i^{(n_i+1)}(X)$ also are known by Equation 17. By Lemma 20, it follows that $\sigma_i^{(n_i+1)}(X)$ are polynomial solutions with degree given by

$$l_{n_i+1} = \max\{l_{n_i}, l_{m_i} + n_i - m_i\}.$$

We will now show that these are minimal solutions.

- If $m_i - l_{m_i} \ge n_i - l_{n_i}$, then $l_{n_i+1} = l_{n_i}$ by Lemma 20 and $\sigma_i^{(n_i+1)}(X)$ are minimal solutions at stages $n_i + 1$.
- On the other hand, if $m_i - l_{m_i} < n_i - l_{n_i}$, then

$$l_{n_i+1} = \max\{l_{n_i}, l_{m_i} + n_i - m_i\} = l_{m_i} + n_i - m_i > l_{n_i}.$$

Let us analyze when $\sigma_i^{(n_i+1)}(X)$ are still minimal solutions. Assume that there exist polynomials $D^{(n_i+1)}(X)$ with degree d_i such that $l_{n_i} \le d_i < l_{m_i} + n_i - m_i$ and the coefficients of the lowest power of the indeterminate X in $D^{(n_i+1)}(X) - \sigma_i^{(n_i)}(X)$ are units in $\mathcal{R}_i$. There are two cases to consider:

1. If $d_i = l_{n_i}$, then by Lemma 21, it follows that there are solutions $\sigma_i^{(m_i')}(X)$ with $l_{m_i'} = d_i - (n_i - m_i')$, i.e., with $m_i' - l_{m_i'} = n_i - l_{n_i}$. By hypothesis, it follows that $m_i - l_{m_i} < n_i - l_{n_i}$, and thus, $m_i' - l_{m_i'} > m_i - l_{m_i}$. However, $m_i - l_{m_i}$ was chosen to be the largest of the values $k_i - l_{k_i}$ for the previous solutions, which is a contradiction.
2. If $d_i > l_{n_i}$, then by Lemma 21, it follows that $d_i = l_{m_i'} + n_i - m_i'$. However, since $m_i' - l_{m_i'} \ge m_i - l_{m_i}$, it follows that

$$d_i = n_i - (m_i' - l_{m_i'}) \ge n_i - (m_i - l_{m_i}) = l_{n_i+1} > d_i,$$

i.e., $d_i > d_i$, which is a contradiction.

Thus, if the coefficients of the lower power of X in $D^{(n_i+1)}(X) - \sigma_i^{(n_i)}(X)$ are units in $\mathcal{R}_i$, then $\sigma_i^{(n_i+1)}(X)$ are minimal solutions. □

Note that the solution $\sigma_i^{(n_i+1)}(X)$ provided by Theorem 22 need not be answered because the theorem does not guarantee minimality when in case (2), the coefficients of the lowest power of the indeterminate X in $D^{(n_i+1)}(X) - \sigma_i^{(n_i)}(X)$ are not units in $\mathcal{R}_i$. However, in many cases, it indicates the minimal solutions at the $(n_i + 1)$th stages.

By extension of the lemma [12], we can verify that if $\sigma_i^{(n_i)}(X)$ satisfies $n_i - l_{n_i}$ equations in Equation 4, but not $n_i + 1 - l_{n_i}$ equations, then the solutions $\sigma_i^{(n_i+1)}(X)$ will satisfy $n_i + 1 - l_{n_i+1}$ equations in Equation 4, where

$$l_{n_i+1} \ge \max\{l_{n_i}, n_i + 1 - l_{n_i}\}.$$

Now, by using the arguments of 'section III' of [12], it is straightforward to show that if the linear equation over the chain of the Galois ring $\mathcal{R}_i$, $d_{n_i'} - yd_{m_i'} = 0$, always have solutions in y for $1 \le m_i' < n_i' \le n_i$, then the above inequalities become equalities, i.e.,

$$l_{n_i+1} = \max\{l_{n_i}, n_i + 1 - l_{n_i}\} = \max\{l_{n_i}, n_i - m_i + l_{m_i}\}.$$

In contrast, if there are n_i' such that $d_{n_i'} - yd_{m_i'} = 0$ does not have solutions in y for any m_i', with $1 \le m_i' < n_i' \le n_i$, then the solutions $\sigma_i^{(n_i)}(X)$, for $n_i \ge n_i'$, given by Theorem 22, i.e., by Equations 16 and 17, are not necessarily minimal solutions. In this case, let us suppose that $\sigma_i^{(n_i)}(X)$ are minimal solutions at n_i stages and $\sigma_i^{(n_i+1)}(X)$ are any solution at $(n_i + 1)$ stages (obtained from Equations 16 and 17 of Theorem 22). We analyze it in the following:

1. If $l_{n_i+1} = \max\{l_{n_i}, n_i + 1 - l_{n_i}\}$, then $\sigma_i^{(n_i+1)}(X)$ are already the minimal solutions (at stages $(n_i + 1)$) over the chain of rings $\mathcal{R}_i$, for $1 \le i \le t$.
2. If $l_{n_i+1} > \max\{l_{n_i}, n_i + 1 - l_{n_i}\}$, then it is possible that there are minimal solutions $D^{(n_i+1)}(X)$ with degree l_i, where $\max\{l_{n_i}, n_i + 1 - l_{n_i}\} \le l_i < l_{n_i+1}$. Any collection of polynomials $D^{(n_i+1)}(X)$ with minimum degree l_i (in the range $\max\{l_{n_i}, n_i + 1 - l_{n_i}\} \le l_i < l_{n_i+1}$) will be minimal solutions (at stages $(n_i + 1)$) if and only if the polynomials $\sigma_i^{(m_i)}(X)$ defined by

$$X^{n_i-m_i}\sigma_i^{(m_i)}(X) = D^{(n_i+1)}(X) - \sigma_i^{(n_i)}(X)$$

are solutions for the first m_i power sums, where $d_{m_i} = -d_{n_i}$ and $\sigma_{i,0}^{(m_i)}(X)$ are zero divisors in $\mathcal{R}_i$. Evidence of this emerged in Lemmas 20 and 21 and from Theorem 22.

We can now collect these results and extend the modified Berlekamp-Massey algorithm.

Extension of the modified Berlekamp-Massey algorithm for commutative rings with identity

The collection of syndromes $s_{i,1}, s_{i,2}, s_{i,3}, \cdots, s_{i,2t_i}$ is used as the input for the algorithm. The output of the algorithm will be sets of values $\sigma_{i,1}, \sigma_{i,2}, \sigma_{i,3}, \cdots, \sigma_{i,v_i}$ such that the equations in Equation 3 hold with minimum v_i. We want to have some initial conditions for starting the algorithm as in [10], given by

$$\sigma_i^{(-1)}(X) = 1 \qquad l_{-1_i} = 0 \qquad d_{-1_i} = 1$$
$$\sigma_i^{(0)}(X) = 1 \qquad l_{0_i} = 0 \qquad d_{0_i} = s_{i,1},$$

for each i such that $1 \le i \le t$, where 1 is the unity of $\mathcal{R}_i$ and each $s_{i,1}$ is the first nonzero component of the corresponding syndrome vectors s_i, for each i, for $1 \le i \le t$. Now, we want to do the following steps:

1. Each $n_i \leftarrow 0$.
2. Now, each $d_{n_i} = s_{i,1}$; if any $d_{n_j} = 0$, for some j, $1 \le j \le t$, then for that j,
$$\sigma_j^{(n_j+1)}(X) \leftarrow \sigma_j^{(n_j)}(X) \text{ and } l_{n_j+1} \leftarrow l_{n_j}$$
and go to (5).
3. If any $d_{n_k} \neq 0$, then find an $m_k \le n_k - 1$ such that $d_{n_k} - y d_{m_k} = 0$ has a solution in y and $m_k - l_{m_k}$ has the largest value. Then,
$$\sigma_k^{(n_k+1)}(X) \leftarrow \sigma_k^{(n_k)}(X) - yX^{n_k-m_k}\sigma_k^{(m_k)}(X)$$
and
$$l_{n_k+1} \leftarrow \max\{l_{n_k}, l_{m_k} + n_k - m_k\},$$
where the solution of the equation $d_{n_k} - y d_{m_k} = 0$, can be obtained by any of the algorithms presented in [13].
4. If $l_{n_k+1} = \max\{l_{n_k}, n_k + 1 - l_{n_k}\}$, then go to (5); else, search for solution $D^{(n_k+1)}(X)$ with minimum degree l_k in the range $\max\{l_{n_k}, n_k + 1 - l_{n_k}\} \le l_k < l_{n_k+1}$ such that $\sigma_k^{(m_k)}(X)$ defined by
$$X^{n_k-m_k}\sigma_k^{(m_k)}(X) = D^{(n_k+1)}(X) - \sigma_k^{(n_k)}(X)$$
is a solution for the first m_k power sums, $d_{m_k} = -d_{n_k}$, with $\sigma_{k,0}^{(m_k)}(X)$ as a zero divisor in corresponding $\mathcal{R}_k$. If such a solution is found, then
$$\sigma_k^{(n_k+1)}(X) \leftarrow D^{(n_k+1)}(X) \text{and} l_{n_k+1} \leftarrow l_k.$$
5. If all $n_i < 2t_i - 1$, then
$$d_{n_i+1} \leftarrow s_{i,n_i+2} + s_{i,n_i+1}\sigma_{i,1}^{(n_i+1)} + \cdots + s_{i,n_i+2-l_{n_i+1}}\sigma_{i,l_{n_i+1}}^{(n_i+1)};$$
else, there is no need to find the values of d_{n_i+1}.
6. $n_i \leftarrow n_i + 1$; if $n_i < 2t_i$, then go to (2); else, stop.
7. In this way, we compute $\sigma_i^{(2t_i)}(X)$ in the nth iteration procedure, where $n = \max\{n_i : 1 \le i \le t\}$.

The coefficients $\sigma_{i,1}^{(2t_i)}, \sigma_{i,2}^{(2t_i)}, \sigma_{i,3}^{(2t_i)}, \cdots, \sigma_{i,v_i}^{(2t_i)}$ of $\sigma_i^{(2t_i)}(X)$ satisfy Equation 3, for each i, where $1 \le i \le t$. This concludes step 2. This process contains n iterations, where $n = \max\{n_i : 1 \le i \le t\}$, and in each iteration, it deals t codewords of codes C_i at once, for each i, where $1 \le i \le t$. By this procedure, we compute t elementary symmetric functions in the chain of rings with less computation. This process is not much different than the original one, but it deals a sequence of t codewords from the sequence of codes C_i over the chain of Galois rings $\mathcal{R}_i$, for each i, where $1 \le i \le t$, at a time. Also, this process does not necessarily lead to a minimal solution $\sigma_i^{(n_i+1)}(X)$ (at the $(n_i + 1)$th stages). As in [11], step 4 had to be introduced in the original algorithm so that the new solutions $\sigma_i^{(n_i+1)}(X)$, calculated at step 3, are checked to be minimal solutions. If these are not so, then a search is necessary to be carried out to find minimal solutions, which consists of finding the polynomials $\sigma_i^{(m_i)}(X)$, which are solutions for the first m_i power sums, and satisfying certain conditions. Step 4 does not essentially increase the complexity due to less number of polynomials.

In step 3, the calculation of error location numbers over the chain of rings requires one more step than that over the chain of fields because in $\mathcal{R}_i$, the solutions to Equation 3 are generally not unique and the reciprocals of polynomials $\sigma_i^{(2t_i)}(X)$, namely $\rho_i(X)$, may not be the correct error locator polynomial

$$(X - X_{i,1})(X - X_{i,2}) \cdots (X - X_{i,v_i}), \tag{18}$$

where $X_{i,u_i} = \alpha^{c_{i,u_i}}$ (c_{i,u_i} are integers in the range $0 \le c_{i,u_i} \le n_i - 1$ that indicate the position of the u_ith errors in the sequence of codewords) are the correct error location numbers and v_i are the numbers of errors in the sequence of codewords and are defined earlier.

Now, we describe how to convert the roots of $\rho_i(X)$ into the correct error location numbers. The following proposition extends Proposition 3 of [11]:

Proposition 23. *Suppose that $\rho_i(X)$ has at least v_i distinct roots over $\mathcal{R}_i$, namely $Z_{i,1}, Z_{i,2}, Z_{i,3}, \cdots, Z_{i,v_i}$, that is,*

$$\rho_i(X) = X^{v_i} + \sigma_{i,1} \cdot X^{v_i-1} + \cdots + \sigma_{i,v_i-1} \cdot X + \sigma_{i,v_i} \tag{19}$$
$$= (X - Z_{i,1})(X - Z_{i,2}) \cdots (X - Z_{i,v_i}) \tag{20}$$

(note that at least one sequence of $\rho_i(X)$ produced by the extension of the modified Berlekamp-Massey algorithm will have this property), where σ_{i,u_i} are the elementary symmetric functions found in step 2). Further, suppose that the error magnitudes are $Y_{i,1}, Y_{i,2}, Y_{i,3}, \cdots, Y_{i,\nu_i}$. Then, $Y_{i,u_i}P_{i,u_i} = 0$, where $P_{i,u_i} = \rho_i(X_{i,u_i})$, for $1 \le u_i \le \nu_i$ and $1 \le i \le t$.

Proof. From Equation 19, it follows that

$$Y_{i,u_i}X_{i,u_i}^{j_i}(X^{\nu_i} + \sigma_{i,1}X^{\nu_i-1} + \cdots + \sigma_{i,\nu_i-1}X + \sigma_{i,\nu_i}) \quad (21)$$

$$= Y_{i,u_i}X_{i,u_i}^{j_i}(X - Z_{i,1})(X - Z_{i,2})\cdots(X - Z_{i,\nu_i}), \quad (22)$$

for $1 \le u_i \le \nu_i$, $1 \le j_i \le 2t_i - \nu_i$ and $1 \le i \le t$. Substituting X for X_{i,u_i} in Equation 21 and summing the right-hand side for $1 \le j_i \le 2t_i - \nu_i$, we get

$$s_{j_i+\nu_i} + s_{j_i+\nu_i-1}\sigma_{i,1} + \cdots + s_{j_i+1}\sigma_{i,\nu_i-1} + s_{j_i}\sigma_{i,\nu_i}. \quad (23)$$

Note that Equation 23 vanishes for very j_i such that $1 \le j_i \le 2t_i - \nu_i$ (since the σ_{i,u_i}'s form solutions to the linear system in Equation 3). Consequently,

$$\sum_{u_i=1}^{\nu_i} Y_{i,u_i}X_{i,u_i}^{j_i}(X_{i,u_i}-Z_{i,1})(X_{i,u_i}-Z_{i,2})\cdots(X_{i,u_i}-Z_{i,\nu_i}) = 0, \quad (24)$$

for $1 \le j_i \le 2t_i - \nu_i$ (the left-hand side of Equation 24 is the collection of sums of the right-hand side of Equation 21 for $1 \le u_i \le \nu_i$). In a matrix form, the sets of equations in Equation 24 can be written as

$$\begin{bmatrix} X_{i,1} & X_{i,2} & \cdots & X_{i,\nu_i} \\ X_{i,1}^2 & X_{i,2}^2 & \cdots & X_{i,\nu_i}^2 \\ \vdots & \vdots & \ddots & \vdots \\ X_{i,1}^{2t_i-\nu_i} & X_{i,2}^{2t_i-\nu_i} & \cdots & X_{i,\nu_i}^{2t_i-\nu_i} \end{bmatrix} \begin{bmatrix} Y_{i,1}P_{i,1} \\ Y_{i,2}P_{i,2} \\ \vdots \\ Y_{i,\nu_i}P_{i,\nu_i} \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}, \quad (25)$$

where

$$P_{i,u_i} = \prod_{l_i'=1}^{\nu_i}(X_{i,u_i} - Z_{i,l_i'}), \text{for} 1 \le u_i \le \nu_i \text{and} 0 \le i \le t.$$

Equation 25 can be viewed as homogeneous linear systems over the chain of rings $\mathcal{R}_i$ in the unknowns $Y_{i,1}P_{i,1}, Y_{i,2}P_{i,2}, \cdots, Y_{i,\nu_i}P_{i,\nu_i}$. The values $2t_i - \nu_i$ are always greater than or equal to ν_i (since $\nu_i \le t_i$), and the McCoy rank of the matrices that appears in Equation 25 is ν_i, which is exactly the number of unknowns. By Theorem 5.3 of [14], this implies that the only solutions to Equation 25 are the trivial one, i.e., $Y_{i,u_i}P_{i,u_i} = 0$ for $1 \le u_i \le \nu_i$. □

Thus, from Proposition 23, we concluded that each product P_{i,u_i} is necessarily a zero divisor in $\mathcal{R}_i$. Thus, P_{i,u_i}, where $1 \le u_i \le \nu_i$, has at least l_i'th factors $(X_{i,u_i} - Z_{i,l_i'})$ which are zero divisors in $\mathcal{R}_i$. Moreover, if some $(l_{i,1})$th factors of P_{i,u_i} are zero divisors, say b_{i_1}, and some other $(l_{i,2})$th factors of P_{i,k_i} are also zero divisors, say b_{i_2}, then $l_{i,1} \ne l_{i,2}$ for $u_i \ne k_i$ and $1 \le i \le t$. It can be solved in the following way: Suppose that $l_{i,1} = l_{i,2}$ for $u_i \ne k_i$. Thus, $(X_{i,u_i} - Z_{i,l_{i,1}}) = b_{i_1}$ and $(X_{i,k_i} - Z_{i,l_{i,2}}) = b_{i_2}$. Therefore, $X_{i,u_i} - X_{i,k_i}$ are zero divisors in $\mathcal{R}_i$, which is a contradiction for $u_i \ne k_i$. Hence, there are unique error location numbers X_{i,u_i} in $\mathcal{R}_i$ corresponding to each Z_{i,u_i}, where $1 \le u_i \le \nu_i$, for $0 \le i \le t$.

Based on these given facts, we can obtain the following procedure for the calculation of the correct error location numbers:

1. Compute the roots of each $\rho_i(X)$, say, $Z_{i,1}, Z_{i,2}, Z_{i,3}, \cdots, Z_{i,\nu_i}$.
2. Among $X_{i,0} = \alpha^0, X_{i,1} = \alpha^1, \cdots, X_{i,n_i-1} = \alpha^{n_i-1}$, select those $X_{i,c_{(i,u_i)}}$ such that $(X_{i,c_{(i,u_i)}} - Z_{i,u_i})$ are zero divisors in $\mathcal{R}_i$. The selected elements give the correct error location numbers.

This concludes step 3.

In step 4, the calculation of error magnitudes is based on Forney's method [5], where the error magnitudes $Y_{i,1}, Y_{i,2}, Y_{i,3}, \cdots, Y_{i,\nu_i}$ are given by

$$Y_{i,u_i} = \frac{\sum_{l_i'=1}^{\nu_i-1} \sigma_i^{(u_i,l_i')} s_{\nu_i-l_i'}}{\sum \sigma_i^{(u_i,l_i')} X^{\nu_i-l_i'}} \quad (26)$$

and the coefficients $\sigma_{i,l_i'}$ are defined by

$$\sigma_i^{(u_i,l_i')} = \sigma_{i,u_i} + X_{i,u_i}\sigma_i^{(u_i,l_i'-1)} \text{ for } 0 \le l_i' \le \nu_i - 1.$$

Starting with $\sigma_i^{(u_i,0)} = \sigma_{i,0} = 1$, here, from [11, p. 1018], the denominator of Equation 26 is always a unit in $\mathcal{R}_i$.

Next, we give an example on this four-step decoding procedure.

Example 24. *Let $\mathcal{C}_1$ and $\mathcal{C}_2$ be a collection of $(3,1)$ and $(15,7)$ BCH codes, respectively, over the chain of Galois rings $\mathcal{A}_1 \subset \mathcal{A}_2$, referring to Example 19, with generator polynomials*

$$g_1(x) = x^2+x+1 \quad \textit{and} \quad g_2(x) = x^8+x^7+x^5+x^3+x^2+1.$$

We know that $\alpha_1 = (x+3, x+3)$ and $\alpha_2 = (x^2, x^2)$ be the primitive elements of $\mathcal{G}_3$ and $\mathcal{G}_{15}$, respectively. Both codes $\mathcal{C}_1$ and $\mathcal{C}_2$ have an error-correcting capability equal to $t_1 = 1$ and $t_2 = 2$ errors. So, $\mathcal{C}_1$ and $\mathcal{C}_2$ have an error-correcting

capability equal to $t_1 = 1$ and $t_2 = 2$ errors. Parity-check matrices of $\mathcal{C}_1$ and $\mathcal{C}_2$ are given by

$$H_1 = \begin{bmatrix} 1 & \alpha_1 & \alpha_1^2 \\ 1 & \alpha_1^2 & \alpha_1 \end{bmatrix},$$

$$H_2 = \begin{bmatrix} 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 & \alpha^7 & \alpha^8 & \alpha^9 & \alpha^{10} & \alpha^{11} & \alpha^{12} & \alpha^{13} & \alpha^{14} \\ 1 & \alpha^2 & \alpha^4 & \alpha^6 & \alpha^8 & \alpha^{10} & \alpha^{12} & \alpha^{14} & \alpha & \alpha^3 & \alpha^5 & \alpha^7 & \alpha^9 & \alpha^{11} & \alpha^{13} \\ 1 & \alpha^3 & \alpha^6 & \alpha^9 & \alpha^{12} & 1 & \alpha^3 & \alpha^6 & \alpha^9 & \alpha^{12} & 1 & \alpha^3 & \alpha^6 & \alpha^9 & \alpha^{12} \\ 1 & \alpha^4 & \alpha^8 & \alpha^{12} & \alpha & \alpha^5 & \alpha^9 & \alpha^{13} & \alpha^2 & \alpha^6 & \alpha^{10} & \alpha^{14} & \alpha^3 & \alpha^7 & \alpha^{11} \end{bmatrix}.$$

Assume that the all zero codewords

$c_1 = ((0,0)(0,0)(0,0))$ *and*

$c_2 = ((0,0)(0,0)(0,0)(0,0)(0,0)(0,0)(0,0)(0,0)(0,0)(0,0)$
$\times (0,0)(0,0)(0,0)(0,0)(0,0)$

are transmitted through the channel and the error pattern is

$e_1 = ((0,0)(0,2)(1,0))$ *and*

$e_2 = ((2,0)(0,1)(0,0)(0,0)(0,0)(0,0)(0,0)(0,0)(0,0)(0,0)$
$\times (0,0)(0,0)(0,0)(3,0)(0,2).$

The received vectors are then given by

$r_1 = c_1 + e_1 = ((0,0)(0,2)(1,0))$ *and*

$r_2 = c_2 + e_2 = ((2,0)(0,1)(0,0)(0,0)(0,0)(0,0)(0,0)(0,0)(0,0)$
$\times (0,0)(0,0)(0,0)(0,0)(0,0)(3,0)(0,2).$

Applying the decoding procedure, first, we get syndromes

$s_1 = r_1 H_1^T = (s_{1,1}, s_{1,2})$ *and* $s_2 = r_2 H_2^T = (s_{2,1}\ s_{2,2}\ s_{2,3}\ s_{2,4})$,

where

$s_{1,1} = (s_{1,1_1}, s_{1,1_2}) = (3x, 2x+2), s_{1,2} = (s_{1,2_1}, s_{1,2_2})$
$= (x+3, 2x)$

$s_{2,1} = (s_{2,1_1}, s_{2,1_2}) = (3x^3 + x^2 + 3x + 2, 2x^3 + 3x^2 + 2),$

$s_{2,2} = (s_{2,2_1}, s_{2,2_2}) = (3x^3 + 2x^2 + x + 1, 2x^3 + 2x^2 + x + 3),$

$s_{2,3} = (s_{2,3_1}, s_{2,3_2}) = (x^3 + 2x, x^3 + 3x^2 + 2x)$ and

$s_{2,4} = (s_{2,4_1}, s_{2,4_2}) = (3x^3 + 3, 2x^3 + x^2 + 3).$

The extension of the modified Berlekamp-Massey algorithm is applied to s_1 and s_2, obtaining Table 1, where $s_{1,3} = (x, 2x+2)$, $s_{1,4} = (x+1, 2x)$, and $s_{1,5} = (x, x+1)$, and Table 2, where

$$\sigma_1^{(2)}(X) = 1 + s_{1,5}X$$

and

$$\sigma_2^{(4)}(X) = 1 + s_{2,10}X + s_{2,11}X^2$$

based on a four- and six-iteration process.

The roots of $\rho_1(X) = X + s_{1,5}$ and $\rho_2(X) = X^2 + s_{2,10}X + s_{2,11}$ are $Z_{1,1} = -s_{1,5}$ and $Z_{2,1} = (2x+1, x^2)$, $Z_{2,2} = (x^3 + 3x^2 + x, x^3 + 3x^2 + 1)$. Among the elements of G_3 and G_{15}, it follows that $X_{1,1} = (0, \beta_1)$, $X_{1,2} = (\beta_1^2, 0)$, $X_{2,1} = (1, 0)$, $X_{2,2} = (0, \beta)$, $X_{2,3} = (\beta^{13}, 0)$, and $X_{2,4} = (0, \beta^{14})$ are such that $X_{1,1} - Z_{1,1}$, $X_{1,2} - Z_{1,2}$ are zero divisors in $\mathcal{R}_1 \subset \mathcal{R}_2$ and $X_{2,1} - Z_{2,1}$, $X_{2,2} - Z_{2,2}$ are zero divisors in $\mathcal{R}_1 \subset \mathcal{R}_2$. Therefore, $X_{1,1}$, $X_{1,2}$, $X_{2,1}$, $X_{2,2}$, $X_{2,3}$, and $X_{2,2}$ are the correct error location numbers and indicate that two errors have occurred in c_1, one at position 2 and the other at position 3, while four errors have occurred in c_2, respectively, at positions 1, 2, 14, and 15. The correct elementary symmetric functions $\sigma_{1,1}$, $\sigma_{2,1}$, and $\sigma_{2,2}$ are obtained from

$$(X - X_{1,1}) = X + \sigma_{1,1} \quad \text{and}$$
$$(X - X_{2,1})(X - X_{2,2}) = X^2 + \sigma_{2,1}X + \sigma_{2,2}.$$

Finally, Forney's procedure is applied to s_i, and we get the error magnitudes $Y_{1,1} = 3$, $Y_{1,2} = 6$, $Y_{2,1} = 6$, and $Y_{2,2} = 3$. Therefore, the error pattern is given by

$e_1 = ((0,0)(0,2)(1,0))$ *and*

$e_2 = ((2,0)(0,1)(0,0)(0,0)(0,0)(0,0)(0,0)(0,0)(0,0)(0,0)$
$\times (0,0)(0,0)(0,0)(3,0)(0,2).$

Table 1 Calculation of the polynomial $\sigma_1^{(2)}(X)$

n_1	$\sigma_1^{(n_1)}(X)$	d_{n_1}	l_{n_1}	$n_1 - l_{n_1}$
−1	1	1	0	−1
0	1	$s_{1,1}$	0	0
1	$1 + s_{1,3}X$	$s_{1,4}$	1	0
2	$1 + s_{1,5}X$	−	1	1

Conclusions

For a nonnegative integer t, let $\mathcal{A}_0 \subset \mathcal{A}_1 \subset \cdots \subset \mathcal{A}_{t-1} \subset \mathcal{A}_t$ be a chain of unitary commutative rings, where each $\mathcal{A}_i$ is constructed by the direct product of suitable Galois rings with multiplicative group $\mathcal{A}_i^*$ of units, and let $\mathcal{K}_0 \subset \mathcal{K}_1 \subset \cdots \subset \mathcal{K}_{t-1} \subset \mathcal{K}_t$ be the corresponding chain of unitary commutative rings, where each $\mathcal{K}_i$ is constructed by the direct product of corresponding residue fields of given Galois rings, with multiplicative groups $\mathcal{K}_i^*$ of units. Despite [7], the construction of BCH codes with symbols from the commutative ring $\mathcal{A}_i$, the direct product of local commutative rings $\mathcal{R}_{i,j}$, where $0 \le i \le t$ and $1 \le j \le r'$, has residue fields $\mathbb{K}_{i,j}$, where $0 \le i \le t$ and $1 \le j \le r'$. For each member in the chain of the direct product of Galois rings and residue fields, respectively, we obtain the sequence of BCH codes $\mathcal{C}_0, \mathcal{C}_1, \cdots, \mathcal{C}_{t-1}, \mathcal{C}$ over the direct

Table 2 Calculation of the polynomial $\sigma_2^{(4)}(X)$

n_2	$\sigma_2^{(n_2)}(X)$	d_{n_2}	l_{n_2}	$n_2 - l_{n_2}$
−1	1	1	0	−1
0	1	$s_{2,1}$	0	0
1	$1 + s_{2,3}X$	$s_{2,4}$	1	0
2	$1 + s_{2,5}X$	$s_{2,6}$	1	1
3	$1 + s_{2,7}X + s_{2,8}X^2$	$s_{2,9}$	2	1
4	$1 + s_{2,10}X + s_{2,11}X^2$	−	2	2

product of local commutative rings $\mathcal{R}_{i,j}$ with different lengths and sequences of BCH codes $\mathcal{C}'_0, \mathcal{C}'_1, \cdots, \mathcal{C}'_{t-1}, \mathcal{C}'$ over the direct product of residue fields $\mathbb{K}_{i,j}$ with proper lengths, i.e.,

$$\begin{aligned}
\mathcal{C}_0 &\subset C_{0,0} \times C_{0,1} \times \cdots \times C_{0,r'} \\
\mathcal{C}_1 &\subset C_{1,0} \times C_{1,1} \times \cdots \times C_{1,r'} \\
&\vdots \qquad\qquad \vdots \\
\mathcal{C} &\subset C_{t,0} \times C_{t,1} \times \qquad \times C_{t,r'}
\end{aligned}$$

and

$$\begin{aligned}
\mathcal{C}'_0 &\subset C'_{0,0} \times C'_{0,1} \times \cdots \times C'_{0,r'} \\
\mathcal{C}'_1 &\subset C'_{1,0} \times C'_{1,1} \times \cdots \times C'_{1,r'} \\
&\vdots \qquad\qquad \vdots \\
\mathcal{C}' &\subset C'_{t,0} \times C'_{t,1} \times \qquad \times C'_{t,r'}.
\end{aligned}$$

In fact, this technique provides a choice to select the most suitable BCH code $\mathcal{C}_i$ (respectively, BCH code $\mathcal{C}'_i$), where $0 \leq i \leq t$, with required error-correcting capabilities and code rate but with compromising length. We extend the modified Berlekamp-Massey algorithm for the chain of unitary commutative local rings in such a way that the error will be corrected by a sequence of codewords from the sequence of BCH codes $C_0, C_1, \cdots, C_{t-1}, C$. In this process, step 2 contains n iterations, where $n = \max\{n_i : 0 \leq i \leq t\}$, and in each iteration, it deals t codewords of codes C_i for each i, where $0 \leq i \leq t$ at once. By the algorithm of step 2, we compute t elementary symmetric functions in the chain of rings with less computation. This process is not much different than the original one, but it deals a sequence of t codewords from the sequence of codes C_i over the chain of Galois rings $\mathcal{R}_i$, for each i, where $0 \leq i \leq t$, at once.

Competing interests
The authors declare that they have no competing interests.

Authors' contributions
TS carried out the construction of the BCH codes, participated in the construction, and drafted the manuscript. AQ carried out the decoding procedure, participated in the design of the study, and performed the examples. AAA conceived of the study, participated in its design and coordination, and helped to draft the manuscript. All authors read and approved the final manuscript.

Acknowledgements
The authors would like to thank the anonymous reviewers for their intuitive commentary that significantly improved the worth of this work and the FAPESP for the financial support (2007/56052-8 and 2011/03441-2).

Author details
[1]Department of Mathematics, Quaid-i-Azam University, Islamabad, 45320, Pakistan. [2]Department of Mathematics, São Paulo State University, São José do Rio Preto, São Paulo, 15054-000, Brazil.

Received: 22 May 2012 Accepted: 4 September 2012
Published: 12 October 2012

References

1. Blake, IF: Codes over certain rings. Inform. Contr. **20**, 396–404 (1972)
2. Blake, IF: Codes over integer residue rings. Inform. Contr. **29**, 295-300 (1975)
3. Spiegel, E: Codes over $\mathbb{Z}_m$. Inform. Control. **35**, 48–51 (1977)
4. Spiegel, E: Codes over $\mathbb{Z}_m$, revisited. Inform. Control. **37**, 100–104 (1978)
5. Forney, GDJr: On decoding BCH codes. IEEE Trans. Inform. Theory. **IT-11**, 549–557 (1965)
6. Shankar, P: On BCH codes over arbitrary integer rings. IEEE Trans. Inform. Theory. **IT-25**(4), 480–483 (1979)
7. Andrade, AA, Palazzo, RJr: Construction and decoding of BCH codes over finite rings. Linear Algebra Applic. **286**, 69–85 (1999)
8. McDonlad, BR: Finite Rings with Identity. Marcel Dekker, New York (1974)
9. Andrade, AA, Palazzo, RJr: A note on units of finite local rings. Rev. Mat. Estat., São Paulo. **18**(2), 213–222 (2000)
10. Peterson, WW, Weldon, EJJr: Error Correcting Codes. 2nd ed. MIT, Cambridge (1972)
11. Interlando, JC, Palazzo, RJr, Elia, M: On the decoding of Reed-Solomon and BCH codes over integer residue rings. IEEE Trans. Inform. Theory. **IT-43**, 1013–1021 (1997)
12. Massey, JL: Shift-register synthesis and BCH decoding. IEEE Trans. Inform. Theory. **IT-15**, 122–127 (1969)
13. Elia, M, Interlando, JC, Palazzo, RJr: Computational of units in Galois rings. J. Discrete Mathematica Sci. and Criptography. **3**(1-3), 41–55 (2000)
14. Interlando, IC, Palazzo, RJr: A note on cyclic codes over $\mathbb{Z}_m$. Latin Amer. Appl. Res. 25/S, 83–85 (1995)

doi:10.1186/2251-7456-6-51
Cite this article as: Shah *et al.*: Construction and decoding of BCH codes over chain of commutative rings. *Mathematical Sciences* 2012 **6**:51.