**British Journal of Applied Science & Technology**
**4(6): 929-944, 2014**

**SCIENCEDOMAIN** *international*
www.sciencedomain.org

# Construction Techniques of Generator Polynomials of BCH Codes

**T. Shah[1], A. Qamar[1] and A. A. Andrade[2*]**

[1] *Department of Mathematics, Quaid-i-Azam University, Islamabad, Pakistan*
[2] *Department of Mathematics, São Paulo State University at São José do Rio Preto, São Paulo, Brazil*

***Original Research Article***

*Received: 22 July 2013*
*Accepted: 21 November 2013*
*Published: 27 December 2013*

## Abstract

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 (each $\mathcal{A}_i$ is constructed by the direct product of suitable Galois rings with multiplicative group $\mathcal{A}_i^*$ of units) and $\mathcal{K}_0 \subset \mathcal{K}_1 \subset \cdots \subset \mathcal{K}_{t-1} \subset \mathcal{K}_t$ be the corresponding chain of unitary commutative rings (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), where $t$ is a non negative integer. In this work presents three different types of constructions of generator polynomials of sequences of BCH codes having entries from $\mathcal{A}_i^*$ and $\mathcal{K}_i^*$ for each $i$, where $0 \leq i \leq t$.

*Keywords: Units of a ring, BCH code, Galois rings*

2010 Mathematics Subject Classification: 11T71, 94A15, 14G50

# 1 Introduction

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 preserve the concept of linear independence among its elements is similar to a vector space over a field. Though it is the constraint that an $r \times r$ submatrix of $r \times n$ generator matrix $M$ over $\mathcal{A}$ is non-singular, or equivalently, has determinant unit in $\mathcal{A}$. The existence of non-singular matrices having not obligatory the 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 carry 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 [1] of a matrix $M$, that is the largest integer $r$ such that $r \times r$ submatrix of $M$ has determinant unit in $\mathcal{A}$.

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

Linear codes over finite rings have been discussed in a series of papers initiated by Blake [2], [3], and Spiegel [4], [5]. However a remarkable development, nonetheless, began by Forney et al. [6]. The structure of, the multiplicative group of unit elements of certain local finite commutative rings have recently raised a great interest for its wonderful application in algebraic coding theory. Using multiplicative group of unit elements of a Galois ring extension of $\mathbb{Z}_{p^m}$, Shankar [7] has constructed BCH codes over $\mathbb{Z}_{p^m}$. However, Andrade and Palazzo [8] have further extend these construction of BCH codes over finite commutative rings with identity. Both construction techniques of [7] and [8] 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 study is to get the factorization of $x^s - 1$ over the group of units of the appropriate extension ring of the given local ring.

There exist corresponding Galois ring extensions $\mathcal{R}_i = GR(p^m, h_i)$, where $0 \le i \le t$, $h = b^t$, $b$ is prime, $t$ is a positive integer and $h_i = b^i$ (respectively, there residue fields $\mathbb{K}_i$, where $0 \le i \le t$ and $h_i = b^i$) of unitary local ring $(\mathcal{R}, \mathcal{M})$ with $p^m$ elements (respectively, $p$ elements and residue field $\mathcal{R}/\mathcal{M}$). For each $i$, for $0 \le i \le t$, 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 to $p$ (an extension in [7, Theorem 2]). Furthermore, if $\overline{\beta^i}$ generates a cyclic subgroup of order $n_i$ in $\mathbb{K}_i^*$. Then $\beta^i$ 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 $i$ [7, Lemma 1]. Then by extending the given algorithm [7] for constructing a BCH codes with symbols from the local ring $\mathcal{A}$ for each member in chains of Galois rings and residue fields, respectively. Consequently there are two situations: $s_i = b^i$ for $i = 2$ or $s_i = b^i$ for $i \ge 2$. By these motivations in this paper for any $t \in \mathbb{Z}^+$, we 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 $0 \le i \le t$, it follows that $\mathcal{A}_i$ is direct product of Galois rings, i.e.,

$$\begin{array}{ccccccccc}
\mathcal{A}_0 & = & \mathcal{R}_{0,1} & \times & \mathcal{R}_{0,2} & \times & \cdots & \times & \mathcal{R}_{0,r} \\
\cap & & \cap & & \cap & & & & \cap \\
\mathcal{A}_1 & = & \mathcal{R}_{1,1} & \times & \mathcal{R}_{1,2} & \times & \cdots & \times & \mathcal{R}_{1,r} \\
\cap & & \cap & & \cap & & & & \cap \\
\vdots & & \vdots & & \vdots & & \ddots & & \vdots \\
\cap & & \cap & & \cap & & & & \cap \\
\mathcal{A}_t & = & \mathcal{R}_{t,1} & \times & \mathcal{R}_{t,2} & \times & \cdots & \times & \mathcal{R}_{t,r}
\end{array}$$

Whereas $\mathcal{R}_{0,j} \subset \mathcal{R}_{1,j} \subset \cdots \subset \mathcal{R}_{t-1,j} \subset \mathcal{R}_{t,j}$, for each $1 \le j \le r$, is the chain of Galois rings. In construction I we have different $\mathcal{R}_{i,j}$ with same characteristic $p$. In constructions II and III we take different $\mathcal{R}_{i,j}$ with different characteristic $p_j$, where $1 \le j \le r$.

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

$$\begin{array}{ccccccccc}
\mathcal{K}_0 & = & \mathbb{K}_{0,1} & \times & \mathbb{K}_{0,2} & \times & \cdots & \times & \mathbb{K}_{0,r} \\
\cap & & \cap & & \cap & & & & \cap \\
\mathcal{K}_1 & = & \mathbb{K}_{1,1} & \times & \mathbb{K}_{1,2} & \times & \cdots & \times & \mathbb{K}_{1,r} \\
\cap & & \cap & & \cap & & & & \cap \\
\vdots & & \vdots & & \vdots & & \ddots & & \vdots \\
\cap & & \cap & & \cap & & & & \cap \\
\mathcal{K}_t & = & \mathbb{K}_{t,1} & \times & \mathbb{K}_{t,2} & \times & \cdots & \times & \mathbb{K}_{t,r}.
\end{array}$$

Whereas $\mathbb{K}_{0,j} \subset \mathbb{K}_{1,j} \subset \cdots \subset \mathbb{K}_{t-1,j} \subset \mathbb{K}_{t,j}$, for each $1 \le j \le r$, is the chain of corresponding residue fields. In construction I we have $\mathbb{K}_{i,j} = \mathbb{K}_{i,j+1}$ and different in remaining types. It follows that $\mathcal{A}_i^*$ and $\mathcal{K}_i^*$, for each $i$, where $0 \le i \le t$, are multiplicative groups of units of $\mathcal{A}_i$ and $\mathcal{K}_i$, respectively.

# 2 Construction I

For each $j$ such that $1 \leq j \leq r$, let $p$ be any prime and $m_j$ be a positive integer. Then ring $A_j = \mathbb{Z}_{p^{m_j}}$ is the unitary finite local commutative ring with maximal ideal $M_j$ and residue field $K = \frac{A_j}{M_j} = \mathbb{Z}_p$. The natural projection $\pi_j : A_j[x] \to K[x]$ is defined by $\pi_j(\sum_{k=0}^{n} a_k x^k) = \sum_{k=0}^{n} \overline{a_k} x^k$, where $\overline{a_k} = a_k + M_j$ for $k = 0, \cdots, n$. Thus, the natural ring morphism $A_j \to K$ is simply the restrictions of $\pi_j$ to the constant polynomial. Now, if $f_j(x) \in A_j[x]$ is a collection of basic irreducible polynomials with degree $h = b^t$, where each $b$ is a prime and $t$ is a positive integer, then $\mathcal{R}_j = \frac{A_j[x]}{(f_j(x))} = GR(p^{m_j}, h)$ is the Galois ring extension of $A_j$ and

$$\mathbb{K} = \frac{\mathcal{R}_j}{\mathcal{M}_j} = \frac{A_j[x]/(f_j(x))}{(M_j, f_j(x))/(f_j(x))} = \frac{A_j[x]}{(M_j, f_j(x))} = \frac{(A_j/M_j)[x]}{(\pi_j(f_j(x)))} = \frac{\mathbb{K}[x]}{(\pi_j(f_j(x)))} = GF(p^h)$$

is the residue field of $\mathcal{R}_j$, where $\mathcal{M}_j = (M_j, f_j(x))/(f_j(x))$ is the corresponding maximal ideal of $\mathcal{R}_j$.

Since $1, b, b^2, \cdots, b^{t-1}, b^t$ are the only divisors of $h$, and take $h_0 = 1, h_1 = b, h_2 = b^2, \cdots, h_t = b^t = h$, therefore by [1, Lemma XVI.7] there exist basic irreducible polynomials $f_{1,j}(x), f_{2,j}(x), \cdots, f_{t,j}(x) \in A_j[x]$ with degrees $h_1, h_2, \cdots, h_t$, respectively, such that we can constitute the Galois subrings $\mathcal{R}_{i,j} = \frac{\mathbb{Z}_{p^{m_j}}[x]}{(f_{i,j}(x))} = GR(p^{m_j}, h_i)$ of $\mathcal{R}_j$ with the maximal ideal $\mathcal{M}_{i,j} = (M_j, f_{i,j}(x))/(f_{i,j}(x))$, for each $i, j$, where $0 \leq i \leq t$ and $1 \leq j \leq r$. Thus the residue field of each $\mathcal{R}_{i,j}$ becomes

$$\mathbb{K}_i = \frac{\mathcal{R}_{i,j}}{\mathcal{M}_{i,j}} = \frac{A_j[X]/(f_{i,j}(x))}{(M_j, f_{i,j}(x))/(f_{i,j}(x))} = \frac{A_j[x]}{(M_j, f_{i,j}(x))} = \frac{(A_j/M_j)[x]}{(\pi_j(f_{i,j}(x)))} = \frac{\mathbb{K}[x]}{(\overline{f}_{i,j}(x))} = GF(p^{h_i}).$$

As each $h_i$ divides $h_{i+1}$ for all $0 \leq i \leq t$, so by [1, Lemma XVI.7] it follows that

$$A_j = \mathcal{R}_{0,j} \subset \mathcal{R}_{1,j} \subset \mathcal{R}_{2,j} \subset \cdots \subset \mathcal{R}_{t-1,j} \subset \mathcal{R}_{t,j} = \mathcal{R}_j$$

is the chain 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 $\mathcal{A}_i$=$\mathcal{R}_{i,1} \times \mathcal{R}_{i,2} \times \mathcal{R}_{i,3} \times \cdots \times \mathcal{R}_{i,r}$, for each $i$ such that $0 \leq i \leq t$, then we get a chain of 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 an other 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 each $i$ such that $0 \leq i \leq t$.

Let $\mathcal{A}_i^*, \mathcal{R}_{i,j}^*$ and $\mathbb{K}_i^*$ be the multiplicative groups of units of $\mathcal{A}_i, \mathcal{R}_{i,j}$ and $\mathbb{K}_i$ respectively, for each $i, j$, where $0 \leq i \leq t$ and $1 \leq j \leq r$. Now, the next theorem extended [1, Theorem XVIII.1], which has a fundamental role in the decomposition of the polynomial $x^{s_i} - 1$ into linear factors over the ring $\mathcal{A}_i^*$. This theorem asserts that for each element $\alpha_i \in \mathcal{A}_i^*$ there exist unique elements $\beta_{i,j} \in \mathcal{R}_{i,j}^*$, for each $i, j$, where $0 \leq i \leq t$ and $1 \leq j \leq r$, such that $\alpha_i = (\beta_{i,1}, \beta_{i,2}, \cdots, \beta_{i,r})$.

**Theorem 2.1.** *Let $\mathcal{A}_i = \mathcal{R}_{i,1} \times \mathcal{R}_{i,2} \times \mathcal{R}_{i,3} \times \cdots \times \mathcal{R}_{i,r}$ for each $i$ such that $0 \leq i \leq t$, where each $\mathcal{R}_{i,j}$ is a local commutative ring. Then $\mathcal{A}_i^* = \mathcal{R}_{i,1}^* \times \mathcal{R}_{i,2}^* \times \mathcal{R}_{i,3}^* \times \cdots \times \mathcal{R}_{i,r}^*$, for each $i, j$, where $0 \leq i \leq t$ and $1 \leq j \leq r$.*

Note that $\overline{\beta}_{i,1} = \overline{\beta}_{i,2} = \overline{\beta}_{i,3} = \cdots = \overline{\beta}_{i,r} = \overline{\beta}_i$, and therefore $\overline{\alpha}_i = (\overline{\beta}_i, \overline{\beta}_i, \overline{\beta}_i, \cdots, \overline{\beta}_i)$. Following theorem indicates the condition under which $x^{s_i} - 1$ can be factored over $\mathcal{A}_i^*$, for each $i$, such that $0 \leq i \leq t$.

**Theorem 2.2.** *For each $i$ such that $0 \leq i \leq t$, the polynomial $x^{s_i} - 1$ can be factored over the multiplicative group $\mathcal{A}_i^*$ as $x^{s_i} - 1 = (x - \alpha_i)(x - \alpha_i^2) \cdots (x - \alpha_i^s)$ if and only if $\bar{\beta}_i$, has order $s_i$ in $\mathbb{K}_i^*$, where $gcd(s_i, p) = 1$ and $\alpha_i = (\beta_{i,1}, \beta_{i,2}, \cdots, \beta_{i,r})$.*

**Proof.** *Suppose that the polynomial $x^{s_i} - 1$ can be factored over $\mathcal{A}_i^*$ as $x^{s_i} - 1 = (x - \alpha_i)(x - \alpha_i^2) \cdots (x - \alpha_i^{s_i})$. Then $x^{s_i} - 1$ can be factored over $\mathcal{R}_{i,j}^*$ as $x^{s_i} - 1 = (x - \beta_{i,j})(x - \beta_{i,j}^2) \cdots (x - \beta_{i,j}^{s_i})$, for each $i$ such that $0 \le i \le t$ and $1 \le j \le r$. Now it follows from the extension of [7, Theorem 3] that $\bar{\beta}_i$ has order $s_i$ in $\mathbb{K}_i^*$, for each $i$ such that $0 \le i \le t$. Conversely, suppose that $\bar{\beta}_i$ has order $s_i$ in $\mathbb{K}_i^*$, for each $i$ such that $0 \le i \le t$. Again it follows from the extension of [7, Theorem 3] that the polynomial $x^{s_i} - 1$ can be factored over $\mathcal{R}_{i,j}^*$as $x^{s_i} - 1 = (x - \beta_{i,j})(x - \beta_{i,j}^2) \cdots (x - \beta_{i,j}^{s_i})$, for $0 \le i \le t$ and $1 \le j \le r$. Since $\alpha_i = (\beta_{i,1}, \beta_{i,2}, \cdots, \beta_{i,r})$, for each $i$ such that $0 \le i \le t$, therefore $x^{s_i} - 1 = (x - \alpha_i)(x - \alpha_i^2) \cdots (x - \alpha_i^{s_i})$ over $\mathcal{A}_i^*$, for each $i$ such that $0 \le i \le t$.*

Let $H_{\alpha_i, s_i}$ denotes the cyclic subgroup of $\mathcal{A}_i^*$ generated by $\alpha_i$, for each $i$ such that $0 \le i \le t$, i.e., $H_{\alpha_i, s_i}$ contains all the roots of $x^{s_i} - 1$ provided the condition of Theorem 2.2 is met. The BCH codes $\mathcal{C}_i$ over $\mathcal{A}_i^*$ can be obtained as the direct product of BCH codes $\mathcal{C}_{i,j}$ over $\mathcal{R}_{i,j}^*$. To construct the cyclic BCH codes over $\mathcal{A}_i^*$, we need to choose certain elements of $H_{\alpha_i, n_i}$, where $n_i = s_i$, as the roots of generator polynomials $g_i(x)$ of the codes. So that, $\alpha_i^{e_1}, \alpha_i^{e_2}, \alpha_i^{e_3}, \cdots, \alpha_i^{e_{n_i - k_i}}$ are all the roots of $g_i(x)$ in $H_{\alpha_i, n_i}$, we construct $g_i(x)$ as

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

where for each $i$ such that $0 \le i \le t$, it follows that $M_i^{e_{l_i}}(x)$ is the minimal polynomial of $\alpha_i^{e_{l_i}}$, for $l = 1, 2, \cdots, n_i - k_i$, whereas each $\alpha_i^{e_{l_i}} = (\beta_{i,1}^{e_{l_i}}, \beta_{i,2}^{e_{l_i}}, \cdots, \beta_{i,r}^{e_{l_i}})$, and $M_i^{e_{l_i}}(x)$. The following theorem is the extension of [7, Lemma 3] and provides us a method for construction of $M_i^{e_{l_i}}(x)$, the minimal polynomial of $\alpha_i^{e_{l_i}}$ over the ring $\mathcal{A}_i$, for $0 \le i \le t$.

**Theorem 2.3.** *For each $i$ such that $0 \le i \le t$, let $M_i^{e_{l_i}}(x)$ be the minimal polynomial of $\alpha_i^{e_{l_i}}$ over $\mathcal{A}_i$, where $\alpha_i^{e_{l_i}}$ generates $H_{\alpha_i, n_i}$, 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 $B_i^{l_i} = \{(\alpha_i^{e_{l_i}})^{m_{i,j}} : m_{i,j} = \prod_{j=1}^{r} p^{q_{i,j}},\ 1 \le l_i \le n_i - k_i,\ 0 \le q_{i,j} \le h_i - 1\}$.*

**Proof.** *Let $\overline{M}_i^{e_{l_i}}(x)$ be the projection of $M_i^{e_{l_i}}(x)$ over the field $\mathbb{K}_i$ and $\overline{M}_i^{e_{l_i}}(x)$ be the minimal polynomial of $\overline{\alpha}_i^{e_{l_i}}$ over $\mathbb{K}_i^*$, for each $i, j$, where $0 \le i \le t$ and $1 \le l_i \le n_i - k_i$. We can verify that each $\overline{M}_i^{e_{l_i}}(x)$ (minimal polynomial of $\overline{\alpha}_i^{e_{l_i}}$) is divisible by $\overline{M}_{i,j}^{e_{l_i}}(x)$ (minimal polynomial of $\overline{\beta}_i^{e_{l_i}}$), for $0 \le i \le t$ and $1 \le l_i \le n_i - k_i$. Thus it has, among its roots, distinct elements of the sequences $\overline{\alpha}_i^{e_{l_i}}, (\overline{\alpha}_i^{e_{li}})^p, (\overline{\alpha}_i^{e_{li}})^{p^2}, \cdots, (\overline{\alpha}_i^{e_{li}})^{p^{h_i - 1}}$, for $0 \le i \le t$ and $1 \le l_i \le n_i - k_i$. Hence $M_i^{e_{l_i}}(x)$ 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 each $i$ such that $0 \le i \le t$ and $1 \le l_i \le n_i - k_i$. Thus the element $\xi_i = (\alpha_i^{e_{l_i}})^{p^{m_i}}$ is the root of $M_i^{e_{l_i}}(x)$, for each $i$ such that $0 \le i \le t$, $0 \le m_i \le h_i - 1$ 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* 2.1. Since, for each $i$ such that $0 \le i \le t$, it follows that $\overline{M}_i^{e_{l_i}}(x)$ (minimal polynomial of $\overline{\alpha}_i^{e_{l_i}}$) is the projection of $M_i^{e_{l_i}}(x)$ (minimal polynomial of $\alpha_i^{e_{l_i}}$) over the rings $\mathcal{K}_i$. So $\overline{M}_i^{e_{l_i}}(x)$ generates the sequence of codes over the special chain of rings $\mathcal{K}_i = K_i^r$.

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 extended [8, Theorem 2.5].

**Theorem 2.4.** *[9, Theorem 11] For each $i$ such that $0 \le i \le t$, let $g_i(x)$ be the generator polynomial of BCH code $\mathcal{C}_i$ over the ring $\mathcal{A}_i$ from the chain $\mathcal{A}_0 \subset \mathcal{A}_1 \subset \mathcal{A}_2 \subset \cdots \subset \mathcal{A}_{t-1} \subset \mathcal{A}_t$, with length $n_i = s_i$, and 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 $g_i(x)$ in $H_{\alpha_i, n_i}$, where $\alpha_i$ has order $n_i$. The minimum Hamming distance of this code is greater than the largest number of consecutive integers modulo $n_i$ in $E_i = \{e_1, e_2, e_3, \cdots, e_{n_i - k_i}\}$, for each $i$ such that $0 \le i \le t$.*

**Corollary 2.5.** *[8, Theorem 2.5] 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 $\alpha$ has order $n$, then minimum Hamming distance of the code is greater than the largest number of consecutive integers modulo $n$ in $E = \{e_1, e_2, e_3, \cdots, e_{n-k}\}$.*

## 2.1 Algorithm

We can also use the extension of [7, Theorem 4] for the BCH bound of these codes. The algorithm for constructing a BCH type cyclic codes over the chain of rings $\mathcal{A}_0 \subset \mathcal{A}_1 \subset \mathcal{A}_2 \subset \cdots \subset \mathcal{A}_{t-1} \subset \mathcal{A}_t = \mathcal{A}$ is then as follows.

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

$$\begin{aligned} \mathbb{Z}_{p^{m_j}} &= GR(p^{m_j}, h_0) \subset GR(p^{m_j}, h_1) \subset \cdots \subset GR(p^{m_j}, h_{t-1}) \subset GR(p^{m_j}, h_t) \text{ or} \\ A_j &= \mathcal{R}_{0,j} \subseteq \mathcal{R}_{1,j} \subseteq \mathcal{R}_{2,j} \subseteq \cdots \subseteq \mathcal{R}_{t-1,j} \subseteq \mathcal{R}_{t,j} = \mathcal{R}_j \end{aligned}$$

   and its corresponding chain of residue fields is

$$\begin{aligned} \mathbb{Z}_p &= GF(p) \subset GF(p^{h_1}) \subset \cdots \subset GF(p^{h_{t-1}}) \subset GF(p^h) \text{ or} \\ &= \mathbb{K}_0 \subset \mathbb{K}_1 \subset \mathbb{K}_2 \cdots \subset \mathbb{K}_{t-1} \subset \mathbb{K}, \end{aligned}$$

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

2. Now put $\mathcal{A}_i = \mathcal{R}_{i,1} \times \mathcal{R}_{i,2} \times \mathcal{R}_{i,3} \times \cdots \times \mathcal{R}_{i,r}$, for $0 \leq i \leq t$, where each $\mathcal{R}_{i,j}$ is a local commutative ring, 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 an other 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 $\overline{\eta}_{i,j} = \overline{\eta}_i$ be the primitive elements in $\mathbb{K}_i^*$, for $0 \leq i \leq t$. Then $\eta_{i,j}$ has order $d_{i,j}.n_i$ in $\mathcal{R}_{i,j}^*$ for some integers $d_{i,j}$, put $\beta_{i,j} = (\eta_{i,j})^{d_{i,j}}$. Then $\alpha_i = (\beta_{1_i}, \beta_{2_i}, \beta_{3_i}, \cdots, \beta_{r_i})$ has order $n_i$ in $\mathcal{R}_{i,j}^*$ and generates $H_{\alpha_i, n_i}$. For each $i$, where $0 \leq i \leq t$, let $\alpha_i$ be any element of $H_{\alpha_i, n_i}$.

4. Let $\alpha_i^{e_1}, \alpha_i^{e_2}, \alpha_i^{e_3}, \cdots, \alpha_i^{e_{n_i - k_i}}$ are chosen to be the roots of $g_i(x)$. Find $M_i^{e_{l_i}}(x)$ are the minimal polynomials of $\alpha_i^{e_{l_i}}$, for $l_i = 1, 2, \cdots, n_i - k_i$, where each $\alpha_i^{e_{l_i}} = (\beta_i^{e_{l_i}}, \beta_i^{e_{l_i}}, \beta_i^{e_{l_i}}, \cdots, \beta_i^{e_{l_i}})$. Then $g_i(x)$ 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 lcm 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 in the set $E_i = \{e_1, e_2, e_3, \cdots, e_{n_i - k_i}\}$ for each $i$, where $0 \leq i \leq t$.

**Example 2.6.** *We initiate by constructing a chain of codes of lengths* $1$, $3$ *and* $15$, *taking* $A_1 = \mathbb{Z}_4$ *and* $A_2 = \mathbb{Z}_8$. *Since* $M_1 = \{0, 2\}$ *and* $M_2 = \{0, 2, 4, 6\}$, *so* $K_j = \frac{A_j}{M_j} \simeq \mathbb{Z}_2$ *for* $i = 1, 2$. *The regular polynomial* $f_1(x) = x^4 + x + 1 \in \mathbb{Z}_4[x]$ *and* $f_2(x) = x^4 + x + 1 \in \mathbb{Z}_8[x]$ *is such that* $\pi_1(f_1(x)) = x^4 + x + 1$ *and* $\pi_2(f_2(x)) = x^4 + x + 1$ *are irreducible polynomials with degree* $h = 2^2$ *over* $\mathbb{Z}_2$. *By [9, Theorem 3], it follows that* $f_1(x)$ *and* $f_2(x)$ *are irreducible over* $A_1$ *and* $A_2$, *respectively. Let* $\mathcal{R}_1 = \frac{\mathbb{Z}_{2^2}[x]}{(f_1(x))} = GR(2^2, 4)$ *and* $\mathcal{R}_2 = \frac{\mathbb{Z}_{2^3}[x]}{(f_2(x))} = GR(2^3, 4)$ *be the Galois rings and* $\mathbb{K} = \frac{\mathbb{Z}_2[x]}{(\pi_j(f_j(x)))} = GF(2^4)$ *be their corresponding common residue field. Since* $1$, $2$ *and* $2^2$ *are the only divisors of* $4$, *it follows that put* $h_1 = 1$, $h_2 = 2$ *and* $h_3 = 2^2$. *Then there exist irreducible polynomials* $f_{i,1}(x) = x^2 - x + 1$ *and* $f_{i,2}(x) = f_2(x)$ *in* $\mathbb{Z}_4[x]$ *with degrees* $h_2 = 2$ *and* $h_3 = 4$ *such that we can constitute the Galois rings* $\mathcal{R}_{i,1} = \frac{\mathbb{Z}_{2^2}[x]}{(f_{i,1}(x))} = GR(2^2, h_i)$, *and* $\mathcal{R}_{i,2} = \frac{\mathbb{Z}_{2^3}[x]}{(f_{i,2}(x))} = GR(2^3, h_i)$, *where* $1 \leq i \leq 2$. *So* $A_j = \mathcal{R}_{0,j} \subset \mathcal{R}_{1,j} \subset \mathcal{R}_{2,j} = \mathcal{R}_j$, *for* $j = 1, 2$. *Again by the same argument* $\mathbb{K}_i = \frac{\mathbb{Z}_2[x]}{(\pi_j(f_{i,j}(x)))} =$

$GF(2, h_i) = GF(2^{h_i})$, *where* $1 \le i \le 2$ *and* $1 \le j \le 2$. *That is,* $\mathbb{K}_0 = GR(2,1) = Z_2$, $\mathbb{K}_1 = GR(2,2)$, $\mathbb{K}_2 = \mathbb{K} = GR(2,4)$, *with* $\mathbb{K}_1 \subset \mathbb{K}_2 \subset \mathbb{K}$. *Now* $\mathcal{A}_i = \mathcal{R}_{i,1} \times \mathcal{R}_{i,2}$ *such that* $\mathcal{A}_0 \subseteq \mathcal{A}_1 \subseteq \mathcal{A}_2$, *i.e.,*

$$\begin{array}{lcl} \mathcal{A}_0 & = & \mathcal{R}_{0,1} = \mathbb{Z}_4 \quad \times \quad \mathcal{R}_{0,2} = \mathbb{Z}_8 \\ \mathcal{A}_1 & = & \mathcal{R}_{1,1} = \frac{\mathbb{Z}_{2^2}[x]}{(x^2+3x+1)} \quad \times \quad \mathcal{R}_{1,2} = \frac{\mathbb{Z}_{2^3}[x]}{(x^2+7x+2)} \\ \mathcal{A}_2 & = & \mathcal{R}_{2,1} = \frac{\mathbb{Z}_{2^2}[x]}{(x^4+x+1)} \quad \times \quad \mathcal{R}_{2,2} = \frac{\mathbb{Z}_{2^3}[x]}{(x^4+x+1)} \end{array}$$

*and*

$$\begin{array}{lcl} \mathcal{K}_0 & = & \mathbb{K}_0 = \mathbb{Z}_2 \quad \times \quad \mathbb{K}_0 = \mathbb{Z}_2 \\ \mathcal{K}_1 & = & \mathbb{K}_1 = \frac{\mathbb{Z}_2[x]}{(x^2+x+1)} \quad \times \quad \mathbb{K}_{1,2} = \frac{\mathbb{Z}_2[x]}{(x^2+x+2)} \\ \mathcal{K}_2 & = & \mathbb{K}_{2,1} = \frac{\mathbb{Z}_2[x]}{(x^4+x+1)} \quad \times \quad \mathbb{K}_{2,2} = \frac{\mathbb{Z}_2[x]}{(x^4+x+1)}. \end{array}$$

*Let* $u = \{x\}$ *in* $\mathcal{R}_{i,1}$ *such that* $\overline{u} = \{x\}$ *in* $\mathbb{K}_i$. *Then* $\overline{u} + 1$ *has order* $15$ *in* $\mathbb{K}_2$, *so* $\overline{\beta}_2 = \overline{u} + 1$. *But* $u + 1$ *has order* $30$ *in* $\mathcal{R}_{2,1}$ *and* $\mathcal{R}_{2,2}$, *so put* $\beta_{2,1} = \beta_{2,2} = (u+1)^2$ *and get* $\alpha_2 = (\beta_{2,1}, \beta_{2,2})$ *which generate* $H_{\alpha_2,15}$. *Also* $\overline{u}$ *has order* $3$ *in* $\mathbb{K}_1$, *so* $\overline{\beta}_1 = \overline{u}$. *But* $u$ *has order* $6$ *in* $\mathcal{R}_{1,1}$ *and* $\mathcal{R}_{1,2}$, *so* $\beta_{1,1} = \beta_{1,2} = u^2$ *and get* $\alpha_1 = (\beta_{1,1}, \beta_{1,2})$ *which generates* $H_{\alpha_1,3}$. *Put* $\beta_{0,1} = \beta_{0,2} = 1$ *and get* $\alpha_0 = (\beta_{0,1}, \beta_{0,2})$ *which generates* $H_{\alpha_0,1}$. *Choose* $\alpha_i$ *and* $\alpha_i^3$ *to be roots of the generator polynomials* $g_i(x)$ *of the BCH codes* $\mathcal{C}_i$ *over the chain* $\mathcal{A}_0 \subseteq \mathcal{A}_1 \subseteq \mathcal{A}_2$. *Then* $M_0^1(x)$, $M_1^1(x)$ *and* $M_2^1(x)$ *has as roots all distinct element in the sets* $B_0^1 = \{\alpha_0\} \subset H_{\alpha_0,1}$, $B_1^1 = \{\alpha_1, \alpha_1^2\} \subset H_{\alpha_1,3}$ *and* $B_2^1 = \{\alpha_2, \alpha_2^2, \alpha_2^4, \alpha_2^8\} \subset H_{\alpha_2,15}$, *respectively. So*

$$M_0^1(x) = (x - \alpha_0),\ M_1^1(x) = (x - \alpha_1)(x - \alpha_1^2) \text{ and } M_2^1(x) = (x - \alpha_2)(x - \alpha_2^2)(x - \alpha_2^4)(x - \alpha_2^8)$$

*Similarly,*

$$M_0^1(x) = M_0^3(x) = (x - \alpha_0),\ M_1^3(x) = (x - 1) \text{ and } M_2^3(x) = (x - \alpha_2^3)(x - \alpha_2^6)(x - \alpha_2^{12})(x - \alpha_2^9).$$

*Thus the polynomials* $g_i(x) = lcm(M_i^1(x), M_i^3(x))$ *are given by*

$$g_0(x) = (x - 1),\ g_1(x) = (x - 1)(x - \alpha_1)(x - \alpha_1^2),$$

$$g_2(x) = (x - \alpha_2)(x - \alpha_2^2)(x - \alpha_2^3)(x - \alpha_2^4)(x - \alpha_2^6)(x - \alpha_2^8)(x - \alpha_2^9)(x - \alpha_2^{12}),$$

*which generates the cyclic BCH codes* $\mathcal{C}_0$, $\mathcal{C}_1$ *and* $\mathcal{C}_2$ *of length* $1$, $3$ *and* $15$ *with minimum hamming distance at least* $2$, $4$ *and* $5$ *respectively. Also, if we replace* $\alpha_i$ *with* $\overline{\alpha}_i$, *then we get codes over* $\mathcal{K}_i$, *for* $0 \le i \le 2$.

# 3 Construction II

Since for any prime $p_j$ and a positive integers $m$, the collection of rings $A_j = \mathbb{Z}_{p_j^m}$ is the collection of unitary finite local commutative rings with maximal ideals $M_j$ and residue fields $\mathbb{K}_j = \frac{A_j}{M_j}$, for each $j$ such that $1 \le j \le r$. The natural projections $\pi_j : A_j[x] \to \mathbb{K}_j[x]$ is defined by $\pi(\sum_{k=0}^n a_k x^k) = \sum_{k=0}^n \overline{a_k} x^k$, where $\overline{a_k} = a_k + M_j$ for $k = 0, \cdots, n$. Thus, the natural ring morphism $A_j \to \mathbb{K}_j$ is simply the restriction of $\pi_j$ to the constant polynomial. Now, if $f_j(x) \in A_j[x]$ is a basic irreducible polynomial with degree $h = b^t$, where $b$ is a prime and $t$ is a positive integer, then $\mathcal{R}_j = \frac{A_j[x]}{(f_j(x))} = GR(p_j^m, h)$ is the family of the Galois ring extension of $A_j$ and $\mathbb{K}_j = \frac{\mathcal{R}_j}{\mathcal{M}_j} = \frac{A_j[x]/(f_j(x))}{(M_j, f_j(x))/(f_j(x))} = \frac{A_j[x]}{(M_j, f_j(x))} = \frac{(A_j/M_j)[x]}{(\pi_j(f_j(x)))}$ is the collection of residue field of $\mathcal{R}_j$, where $M_j = (M_j, f_j(x))$ is the corresponding collection of the maximal ideals of $\mathcal{R}_j$. For the construction of a chain of Galois rings, [1, Lemma XVI.7] facilitate us.

Since $1, b, b^2, \cdots, b^{t-1}, b^t$ are the only divisors of $h$, and take $h_0 = 1, h_1 = b, h_2 = b^2, \cdots, h_t = b^t = h$, so by [1, Lemma XVI.7] there exist basic irreducible polynomials $f_{1,j}(x), f_{2,j}(x), \cdots, f_{t,j}(x) \in A_j[x]$ with degrees $h_1, h_2, \cdots, h_t$, respectively, such that we can constitute the Galois subrings $\mathcal{R}_{i,j} =$

$\frac{\mathbb{Z}_{p_j^m}[x]}{(f_{i,j}(x))} = GR(p_j^m, h_i)$, of $\mathcal{R}_j$ with the maximal ideals $\mathcal{M}_{i,j} = (M_j, f_{i,j}(x))/(f_{i,j}(x))$, for each $i, j$, where $0 \leq i \leq t$ and $1 \leq j \leq r$. Then the residue field of each $\mathcal{R}_{i,j}$ becomes

$$\mathbb{K}_{i,j} = \frac{\mathcal{R}_{i,j}}{\mathcal{M}_{\mathsf{i,j}}} = \frac{A_j[x]/(f_{i,j}(x))}{(M_j, f_{i,j}(x))/(f_{i,j}(x))} = \frac{A_j[x]}{(M_j, f_{i,j}(x))} = \frac{(A_j/M_j)[x]}{(\pi_j(f_{i,j}(x)))} = \frac{K_j[x]}{(\overline{f}_{i,j}(x))} = GF(p_j^{h_i})$$

As each $h_i$ divides $h_{i+1}$ for each $i$ such that $0 \leq i \leq t$, so by [1, Lemma XVI.7], there are chains

$$A_j = \mathcal{R}_{0,j} \subset \mathcal{R}_{1,j} \subset \mathcal{R}_{2,j} \subset \cdots \subset \mathcal{R}_{t-1,j} \subset \mathcal{R}_{t,j} = \mathcal{R}_j$$

of Galois rings, with corresponding chain of residue fields

$$\mathbb{Z}_{p_j} = \mathbb{K}_{0,j} \subset \mathbb{K}_{1,j} \subset \mathbb{K}_{2,j} \cdots \subset \mathbb{K}_{t-1,j} \subset \mathbb{K}_{t,j} = \mathbb{K}_j$$

Let $\mathcal{A}_i$=$\mathcal{R}_{i,1} \times \mathcal{R}_{i,2} \times \mathcal{R}_{i,3} \times \cdots \times \mathcal{R}_{i,r}$, for $0 \leq i \leq t$. Then we get a chain of 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 an other chain of commutative 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 $\mathcal{K}_i = \mathbb{K}_{i,1} \times \mathbb{K}_{i,2} \times \cdots \times \mathbb{K}_{i,r}$, for each $i$ such that $0 \leq i \leq t$.

Let $\mathcal{A}_i^*$, $\mathcal{K}_i^*$, $\mathcal{R}_{i,j}^*$ and $\mathbb{K}_{i,j}^*$ be the multiplicative groups of units of $\mathcal{A}_i$, $\mathcal{K}_i$, $\mathcal{R}_{i,j}$ and $\mathbb{K}_{i,j}$, respectively, for each $i, j$ where $0 \leq i \leq t$ and $1 \leq j \leq r$. Now the next theorem, extension of [1, Theorem XVIII.1] has a fundamental role in the decomposition of the polynomial $x^{s_i} - 1$ 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 $\beta_{i,j} \in \mathcal{R}_{i,j}^*$, for each $i, j$, where $0 \leq i \leq t$ and $1 \leq j \leq r$, such that $\alpha_i = (\beta_{i,1}, \beta_{i,2}, \cdots, \beta_{i,r})$.

**Theorem 3.1.** *Let $\mathcal{A}_i = \mathcal{R}_{i,1} \times \mathcal{R}_{i,2} \times \mathcal{R}_{i,3} \times \cdots \times \mathcal{R}_{i,r}$, for $0 \leq i \leq t$, where each $\mathcal{R}_{i,j}$ is a local commutative ring. Then for each $i, j$, where $0 \leq i \leq t$ and $1 \leq j \leq r$, it follows that $\mathcal{A}_i^* = \mathcal{R}_{i,1}^* \times \mathcal{R}_{i,2}^* \times \mathcal{R}_{i,3}^* \times \cdots \times \mathcal{R}_{i,r}^*$.*

Note that corresponding $\overline{\alpha}_i = (\overline{\beta}_{i,1}, \overline{\beta}_{i,2}, \cdots, \overline{\beta}_{i,r})$. Following theorem indicates the condition under which $x^{s_i} - 1$ can be factored over $\mathcal{A}_i^*$, for $0 \leq i \leq t$.

**Theorem 3.2.** *For each $i$, where $0 \leq i \leq t$, the polynomial $x^{s_i} - 1$ can be factored over the multiplicative groups $\mathcal{A}_i^*$ as $x^{s_i} - 1 = (x - \alpha_i)(x - \alpha_i^2) \cdots (x - \alpha_i^{s_i})$ if and only if each $\bar{\beta}_{i,j}$, $1 \leq j \leq r$, has order $s_i$ in $\mathbb{K}_{i,j}^*$, where $gcd(s_i, p) = 1$ and $\alpha_i = (\beta_{i,1}, \beta_{i,2}, \cdots, \beta_{i,r})$, for each $i, 0 \leq i \leq t$.*

**Proof.** *For each $i$, where $0 \leq i \leq t$, suppose that the polynomial $x^{s_i} - 1$ can be factored over $\mathcal{A}_i^*$ as $x^{s_i} - 1 = (x - \alpha_i)(x - \alpha_i^2) \cdots (x - \alpha_i^{s_i})$. Then $x^{s_i} - 1$ can be factored over $\mathcal{R}_{i,j}^*$ as $x^{s_i} - 1 = (x - \beta_{i,j})(x - \beta_{i,j}^2) \cdots (x - \beta_{i,j}^{s_i})$ for $0 \leq i \leq t$ and $1 \leq j \leq r$. Now it follows from the extension of [7, Theorem 3] that $\bar{\beta}_{i,j}$ has order $s_i$ in $\mathbb{K}_{i,j}^*$, for $0 \leq i \leq t$ and $1 \leq j \leq r$. Conversely, suppose that $\bar{\beta}_{i,j}$ has order $s_i$ in $\mathbb{K}_{i,j}^*$, for $0 \leq i \leq t$ and $1 \leq j \leq r$. Again it follows from the extension of [7, Theorem 3] that, the polynomial $x^{s_i} - 1$ can be factored over $\mathcal{R}_{i,j}^*$ as $x^{s_i} - 1 = (x - \beta_{i,j})(x - \beta_{i,j}^2) \cdots (x - \beta_{i,j}^{s_i})$, for each $i, j$, where $0 \leq i \leq t$ and $1 \leq j \leq r$. Since $\alpha_i = (\beta_{i,1}, \beta_{i,2}, \cdots, \beta_{i,r})$, for $0 \leq i \leq t$, so $x^{s_i} - 1 = (x - \alpha_i)(x - \alpha_i^2) \cdots (x - \alpha_i^{s_i})$ over $\mathcal{A}_i^*$, for each $i$ such that $0 \leq i \leq t$.*

**Corollary 3.3.** *[8, Theorem 3.4] 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 $\alpha$ corresponds to $\beta = (\beta_1, \beta_2, \cdots, \beta_r)$, where $j = 1, 2, 3, \cdots, r$.*

Let $H_{\alpha_i, s_i}$ denotes the cyclic subgroup of $\mathcal{A}_i^*$ generated by $\alpha_i$, for each $i$ such that $0 \leq i \leq t$, i.e., $H_{\alpha_i, s_i}$ contains all the roots of $x^{s_i} - 1$ provided the condition of above theorem are met. The BCH codes $\mathcal{C}_i$ over $\mathcal{A}_i^*$ can be obtained as the direct product of BCH codes $\mathcal{C}_{i,j}$ over $\mathcal{R}_{i,j}^*$. To construct the cyclic BCH codes over $\mathcal{A}_i^*$, we need to choose certain elements of $H_{\alpha_i,n_i}$ as the roots of generator polynomials $g_i(x)$ of the codes, where $n_i = gcd(p_1^{h_i}, p_2^{h_i}, p_3^{h_i}, \cdots, p_r^{h_i})$. So that, $\alpha_i^{e_1}, \alpha_i^{e_2}, \cdots, \alpha_i^{e_{n_i-k_i}}$ are all the roots of $g_i(x)$ in $H_{\alpha_i,n_i}$, we construct $g_i(x)$ as

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

where $M_i^{e_{l_i}}(x)$ are the minimal polynomials of $\alpha_i^{e_{l_i}}$, for $l = 1, 2, \cdots, n_i - k_i$, where each $\alpha_i^{e_{l_i}} = (\beta_{i,1}^{e_{l_i}}, \beta_{i,2}^{e_{l_i}}, \cdots, \beta_{i,r}^{e_{l_i}})$. The following theorem is the extension of [7, Lemma 3] and provides us a method for construction of $M_i^{e_{l_i}}(x)$, the minimal polynomial of $\alpha_i^{e_{l_i}}$ over the ring $\mathcal{A}_i$.

**Theorem 3.4.** *For each $i$ such that $0 \le i \le t$, let $M_i^{e_{l_i}}(x)$ be the minimal polynomial of $\alpha_i^{e_{l_i}}$ over $\mathcal{A}_i$, where $\alpha_i^{e_{l_i}}$ generates $H_{\alpha_i,n_i}$, for $l_i = 1, 2, \cdots, n_i - k_i$ and $0 \le i \le t$. Then $M_i^{e_{l_i}}(x) = \prod_{\xi_i \in B_i^{l_i}} (x - \xi_i)$, where $B_i^{l_i} = \{(\alpha_i^{e_{l_i}})^{m_{i,j}} : m_{i,j} = \prod_{j=1}^{r} p_i^{q_{i,j}}$, for $1 \le l_i \le n_i - k_i$, $0 \le q_{i,j} \le h_i - 1$ and $0 \le i \le t\}$.*

**Proof.** *Let $\overline{M}_i^{e_{l_i}}(x)$ be the projection of $M_i^{e_{l_i}}(x)$ over the fields $\mathbb{K}_{i,j}$ and $\overline{M}_{i,j}^{e_{l_i}}(x)$ be the minimal polynomial of $\overline{\alpha}_i^{e_{l_i}}$ over $\mathbb{K}_{i,j}^*$, for each $i$ such that $0 \le i \le t$, $1 \le j \le r$ and $1 \le l_i \le n_i - k_i$. We can verify that each $\overline{M}_i^{e_{l_i}}(x)$ is divisible by $\overline{M}_{i,j}^{e_{l_i}}(x)$, for $0 \le i \le t$, $1 \le j \le r$ and $1 \le l_i \le n_i - k_i$. Thus it has, among its roots, distinct elements of the sequences $\overline{\alpha}_i^{e_{l_i}}, (\overline{\alpha}_i^{e_{l_i}})^{p_j}, (\overline{\alpha}_i^{e_{l_i}})^{p_j^2}, \cdots, (\overline{\alpha}_i^{e_{l_i}})^{p_j^{h_i-1}}$, for each $i, j$ such that $0 \le i \le t$, $1 \le j \le r$ and $1 \le l_i \le n_i - k_i$. Hence $M_i^{e_{l_i}}(x)$ has, among its roots, distinct elements of the sequence $\alpha_i^{e_{l_i}}, (\alpha_i^{e_{l_i}})^{p_j}, (\alpha_i^{e_{l_i}})^{p_j^2}, \cdots, (\alpha_i^{e_{l_i}})^{p_j^{h_i-1}}$, for each $i, j$ such that $0 \le i \le t$, $1 \le j \le r$ and $1 \le l_i \le n_i - k_i$. Thus any element $\gamma_i = (\alpha_i^{e_{l_i}})^{p_j^{m_i}}$ of the above sequence is the root of $M_i^{e_{l_i}}(x)$, for each $i, j$ such that $0 \le i \le t$, $1 \le j \le r$, $0 \le m_i \le h_i - 1$ and $1 \le l_i \le n_i - k_i$. Choose any $k$ in the range $1 \le k \le r$ such that $k \ne j$. Then we know that $\gamma_{i,k}$ a root of $\overline{M}_{i,k}^{e_{l_i}}(x)$ implies that $(\gamma_{i,k})^{p_k^{q_i}}$ is a root of $M_i^{e_{l_i}}(x)$ (which has coefficients in $\mathbb{K}_{i,k}$), for $0 \le q_i \le h_i - 1$. Hence $(\gamma_i)^{p_k^{q_i}} = (\alpha_i^{e_{l_i}})^{p_j^{m_i} p_k^{q_i}}$ is a root of $M_i^{e_{l_i}}(x)$. Proceeding in this manner, we can show that $M_i^{e_{l_i}}(x)$ necessarily has as roots all distinct member of $B_i^{l_i}$. But the polynomial $\prod_{\xi_i \in B_i^{l_i}} (x - \xi_i)$ has, by construction, coefficient in the direct product of $A_j$. Hence $M_i^{e_{l_i}}(x) = \prod_{\xi_i \in B_i^{l_i}} (x - \xi_i)$.*

**Corollary 3.5.** *[8, Theorem 3.5] For any positive integer $l$, let $M_l(x)$ be the minimal polynomial of $\alpha^l$ over $\mathcal{R}$, where $\alpha$ generates $H_{\alpha,n}$. Then $M_l(x) = \prod_{\xi \in B_l} (x - \xi)$, where $B_l$ is all distinct elements of the sequence $\{(\alpha^l)^m : m = \prod_{j=1}^{r} q_j^{s_j},\ q_j = p_j^{m_j}$, where $0 \le s_j \le h - 1\}$.*

*Remark* 3.1. Since $\overline{M}_i^{e_{l_i}}(x)$ be the projection of $M_i^{e_{l_i}}(x)$ over the field $\mathbb{K}_{i,j}$, for each $i, j$ such that $0 \le i \le t$ and $1 \le j \le r$. So $\overline{M}_i^{e_{l_i}}(x)$ generates the sequence of codes over the special chain of rings $\mathcal{K}_i = \mathbb{K}_{i,1} \times \mathbb{K}_{i,2} \times \cdots \times \mathbb{K}_{i,r}$, for each $i$ such that $0 \le i \le t$.

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 extended [8, Theorem 2.5].

**Theorem 3.6.** *[9, Theorem 11] For each $i$ such that $0 \le i \le t$, let $g_i(x)$ be the generator polynomial of BCH code $\mathcal{C}_i$ over $\mathcal{A}_i$ from the chain $\mathcal{A}_0 \subset \mathcal{A}_1 \subset \mathcal{A}_2 \subset \cdots \subset \mathcal{A}_{t-1} \subset \mathcal{A}_t$, with length $n_i = s_i$, and 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 $g_i(x)$ in $H_{\alpha_i,n_i}$, where $\alpha_i$ has order $n_i$. The minimum Hamming distance of this code is greater than the largest number of consecutive integers modulo $n_i$ in $E_i = \{e_1, e_2, e_3, \cdots, e_{n_i-k_i}\}$, for each $i$ such that $0 \le i \le t$.*

**Corollary 3.7.** *[8, Theorem 2.5] 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 $\alpha$ has order $n$, then minimum Hamming distance of the code is greater than the largest number of consecutive integers modulo $n$ in $E = \{e_1, e_2, e_3, \cdots, e_{n-k}\}$.*

## 3.1 Algorithm

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

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

$$\begin{aligned} \mathbb{Z}_{p_j^m} &= GR(p_j^m, h_0) \subset GR(p_j^m, h_1) \subset \cdots \subset GR(p_j^m, h_{t-1}) \subset GR(p_j^m, h_t) \text{ or} \\ A_j &= \mathcal{R}_{0,j} \subseteq \mathcal{R}_{1,j} \subseteq \mathcal{R}_{2,j} \subseteq \cdots \subseteq \mathcal{R}_{t-1,j} \subseteq \mathcal{R}_{t,j} = \mathcal{R}_j \end{aligned}$$

   and its corresponding chains of residue fields are

$$\begin{aligned} \mathbb{Z}_{p_j} &= GF(p_j) \subset GF(p_j^{h_1}) \subset \cdots \subset GF(p_j^{h_{t-1}}) \subset GF(p_j^{h}) \text{ or} \\ &= \mathbb{K}_{0,j} \subset \mathbb{K}_{1,j} \subset \mathbb{K}_{2,j} \cdots \subset \mathbb{K}_{t-1,j} \subset \mathbb{K}_{t,j} = \mathbb{K}_j, \end{aligned}$$

   where each $GF(p_j^{h_i}) \simeq \frac{\mathbb{K}_j[x]}{(\pi_j(f_{i,j}(x)))}$, for $1 \leq i \leq t$.

2. Now put $\mathcal{A}_i = \mathcal{R}_{i,1} \times \mathcal{R}_{i,2} \times \mathcal{R}_{i,3} \times \cdots \times \mathcal{R}_{i,r}$, for $0 \leq i \leq t$, where each $\mathcal{R}_{i,j}$ is a local commutative ring, 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 an other 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 $\mathcal{K}_i = \mathbb{K}_{i,1} \times \mathbb{K}_{i,2} \times \cdots \times \mathbb{K}_{i,r}$, the direct product of corresponding residue fields $r$ times, for $0 \leq i \leq t$.

3. Let $\overline{\eta}_{i,j}$ be the primitive elements in $\mathbb{K}_{i,j}^*$, for $0 \leq i \leq t$ and $1 \leq j \leq r$ . Then $\eta_{i,j}$ has order $d_{i,j}n_i$ in $\mathcal{R}_{i,j}^*$ for some integers $d_{i,j}$, put $\beta_{i,j} = (\eta_{i,j})^{d_{i,j}}$. Then $\alpha_i = (\beta_{1_i}, \beta_{2_i}, \beta_{3_i}, \cdots, \beta_{r_i})$ has order $n_i$ in $\mathcal{R}_{i,j}^*$ and generates $H_{\alpha_i,n_i}$. Assume for each $i$, where $0 \leq i \leq t$, let $\alpha_i$ be any element of $H_{\alpha_i,n_i}$.

4. Let $\alpha_i^{e_1}, \alpha_i^{e_2}, \alpha_i^{e_3}, \cdots, \alpha_i^{e_{n_i-k_i}}$ are chosen to be the roots of $g_i(x)$. Find $M_i^{e_{l_i}}(x)$ are the minimal polynomials of $\alpha_i^{e_{l_i}}$, for $l_i = 1, 2, \cdots, n_i - k_i$, where each $\alpha_i^{e_{l_i}} = (\beta_i^{e_{l_i}}, \beta_i^{e_{l_i}}, \beta_i^{e_{l_i}}, \cdots, \beta_i^{e_{l_i}})$. Then $g_i(X)$ 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 lcm 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 in the set $E_i = \{e_1, e_2, e_3, \cdots, e_{n_i-k_i}\}$ for each $i$, where $0 \leq i \leq t$.

**Example 3.8.** *We initiate by constructing a chain of codes of lengths* $1, 8$ *and* $16$*, taking* $A_1 = \mathbb{Z}_9$ *and* $A_2 = \mathbb{Z}_{25}$*. Since* $M_1 = \{0, 3, 6\}$ *and* $M_2 = \{0, 5, 10, 15, 20\}$*, it follows that* $K_1 = \frac{A_1}{M_1} \simeq \mathbb{Z}_3$ *and* $K_2 = \frac{A_2}{M_2} \simeq \mathbb{Z}_5$*. The regular polynomials* $f_1(x) = x^4 + x + 8 \in \mathbb{Z}_9[x]$ *and* $f_2(X) = x^4 + x^2 + x + 1 \in \mathbb{Z}_{25}[x]$ *are such that* $\pi_1(f_1(x)) = x^4 + x + 2$ *and* $\pi_2(f_2(x)) = x^4 + x^2 + x + 1$ *are irreducible polynomials with degree* $h = 2^2$ *over* $\mathbb{Z}_3$ *and* $Z_5$*, respectively. By [9, Theorem 3], it follows that* $f_1(x)$ *and* $f_2(x)$ *are irreducible over* $A_1$ *and* $A_2$*. Let* $\mathcal{R}_1 = \frac{\mathbb{Z}_{3^2}[x]}{(f_1(x))} = GR(3^2, 4)$*,* $\mathcal{R}_2 = \frac{\mathbb{Z}_{5^2}[x]}{(f_2(x))} = GR(5^2, 4)$ *be the Galois rings and* $\mathbb{K}_1 = \frac{\mathbb{Z}_3[x]}{(\pi_1(f_1(x)))} = GF(3^4)$*,* $\mathbb{K}_2 = \frac{\mathbb{Z}_5[x]}{(\pi_2(f_2(x)))} = GF(5^4)$ *be their corresponding residue fields. Since* $1$*,* $2$ *and* $2^2$ *are the only divisors of* $4$*, therefore let* $h_1 = 1$*,* $h_2 = 2$*,* $h_3 = 2^2$*. Then there exist irreducible polynomials* $f_{1,1}(x) = x^2 + 1$*,* $f_{2,1}(x) = f_1(x)$ *in* $\mathbb{Z}_9[x]$*, and* $f_{1,2}(x) = x^2 + 2$*,* $f_{2,2}(x) = f_2(x)$ *in* $\mathbb{Z}_{25}[x]$ *with degrees* $h_2 = 2$ *and* $h_3 = 4$ *such that we can constitute the Galois rings*

$\mathcal{R}_{0,1} = A_1$, $\mathcal{R}_{1,1} = \frac{\mathbb{Z}_{3^2}[x]}{(f_{1,1}(x))} = GR(3^2, h_2)$, $\mathcal{R}_{2,1} = \mathcal{R}_1$ *and* $\mathcal{R}_{0,2} = A_2$, $\mathcal{R}_{1,2} = \frac{\mathbb{Z}_{5^2}[x]}{(f_{1,2}(x))} = GR(5^2, h_2)$ *and* $\mathcal{R}_{1,2} = \mathcal{R}_2$. *So*

$$A_j = \mathcal{R}_{0,j} \subset \mathcal{R}_{1,j} \subset \mathcal{R}_{2,j} = \mathcal{R}_j, \ for\ j = 1, 2.$$

*Again by the same argument* $\mathbb{K}_{0,1} = \mathbb{Z}_2$, $\mathbb{K}_{1,1} = \frac{\mathbb{Z}_3[x]}{(\pi_1(f_{1,1}(x)))} = GF(3^2)$, $\mathbb{K}_{2,1} = \mathbb{K}_1$ *and* $\mathbb{K}_{0,2} = \mathbb{Z}_5, \mathbb{K}_{1,2} = \frac{\mathbb{Z}_5[x]}{(\pi_2(f_{1,2}(x)))} = GF(5^2), \mathbb{K}_{2,2} = \mathbb{K}_2$. *So we get chains of fields*

$$A_j = \mathbb{K}_{0,j} \subset \mathbb{K}_{1,j} \subset \mathbb{K}_{2,j} = \mathbb{K}_j, \ for\ j = 1, 2.$$

*Now* $\mathcal{A}_i = \mathcal{R}_{i,1} \times \mathcal{R}_{i,2}$ *such that* $\mathcal{A}_0 \subseteq \mathcal{A}_1 \subseteq \mathcal{A}_2$, *i.e.,*

$$\begin{array}{lllll} \mathcal{A}_0 & = & \mathcal{R}_{0,1} = \mathbb{Z}_9 & \times & \mathcal{R}_{0,2} = \mathbb{Z}_{25} \\ \mathcal{A}_1 & = & \mathcal{R}_{1,1} = \frac{\mathbb{Z}_{3^2}[x]}{(x^2+1)} & \times & \mathcal{R}_{1,2} = \frac{\mathbb{Z}_{5^2}[x]}{(x^2+2)} \\ \mathcal{A}_2 & = & \mathcal{R}_{2,1} = \frac{\mathbb{Z}_{3^2}[x]}{(x^4+x-1)} & \times & \mathcal{R}_{2,2} = \frac{\mathbb{Z}_{5^2}[x]}{(x^4+x^2+x+1)} \end{array}$$

*and*

$$\begin{array}{lllll} \mathcal{K}_0 & = & \mathbb{K}_{0,1} = \mathbb{Z}_3 & \times & \mathbb{K}_{0,2} = \mathbb{Z}_5 \\ \mathcal{K}_1 & = & \mathbb{K}_{1,1} = \frac{\mathbb{Z}_3[x]}{(x^2+1)} & \times & \mathbb{K}_{1,2} = \frac{\mathbb{Z}_5[x]}{(x^2+2)} \\ \mathcal{K}_2 & = & \mathbb{K}_{2,1} = \frac{\mathbb{Z}_3[x]}{(x^4+x-1)} & \times & \mathbb{K}_{2,2} = \frac{\mathbb{Z}_5[x]}{(x^4+x^2+x+1)}. \end{array}$$

*Let* $u = \{x\}$ *in* $\mathcal{R}_{i,j}$ *such that* $\overline{u} = \{x\}$ *in* $\mathbb{K}_{i,j}$. *Then* $\overline{u}+1$ *has order* $8, 24, 80$ *and* $624$ *in* $\mathbb{K}_{1,1}, \mathbb{K}_{1,2}, \mathbb{K}_{2,1}$ *and* $\mathbb{K}_{2,2}$, *respectively. So* $\overline{\beta}_{1,1} = \overline{\beta}_{1,2} = \overline{\beta}_{2,1} = \overline{\beta}_{2,2} = \overline{u}+1$. *But* $u+1$ *has order* $24, 120, 240$ *and* $3120$ *in* $\mathcal{R}_{1,1}, \mathcal{R}_{1,2}, \mathcal{R}_{2,1}$ *and* $\mathcal{R}_{2,2}$, *so put* $\beta_{1,1} = (u+1)^3$, $\beta_{1,2} = \beta_{2,1} = (u+1)^{15}$ *and* $\beta_{2,2} = (u+1)^{195}$ *and get* $\alpha_2 = (\beta_{2,1}, \beta_{2,2})$ *which generates* $H_{\alpha_2,16}$ *and* $\alpha_1 = (\beta_{1,1}, \beta_{1,2})$ *which generates* $H_{\alpha_1,8}$. *Also* $2$ *has order* $4$ *in* $\mathbb{K}_{0,2}$ *and has order* $2$ *in* $\mathbb{K}_{0,1}$, *so* $\overline{\beta}_{0,1} = \overline{\beta}_{0,2} = 2$. *But* $2$ *has order* $20$ *in* $\mathcal{R}_{0,2}$ *and has order* $6$ *in* $\mathcal{R}_{0,1}$, *so* $\beta_{0,1} = 8$ *and* $\beta_{0,2} = 24$ *get* $\alpha_0 = (\beta_{0,1}, \beta_{0,2})$ *which generates* $H_{\alpha_0,2}$. *Choose* $\alpha_i$ *and* $\alpha_i^2$ *to be roots of the generator polynomials* $g_i(x)$ *of the BCH codes* $\mathcal{C}_i$ *over the chain* $\mathcal{A}_0 \subset \mathcal{A}_1 \subset \mathcal{A}_2$. *Then* $M_0^1(x)$, $M_1^1(x)$ *and* $M_2^1(x)$ *has as roots all distinct element in the sets* $B_0^1 = \{\alpha_0\} \subset H_{\alpha_0,2}, B_1^1 = \{\alpha_1, \alpha_1^3, \alpha_1^5, \alpha_1^7\} \subset H_{\alpha_1,8}$ *and* $B_2^1 = \{\alpha_2, \alpha_2^3, \alpha_2^5, \alpha_2^7, \alpha_2^9, \alpha_2^{11}, \alpha_2^{13}, \alpha_2^{15}\} \subset H_{\alpha_2,16}$, *respectively. So*

$$M_0^1(x) = (x - \alpha_0), \ M_1^1(x) = (x - \alpha_1)(x - \alpha_1^3)(x - \alpha_1^5)(x - \alpha_1^7),$$

*and*

$$M_2^1(x) = (x - \alpha_2)(x - \alpha_2^3)(x - \alpha_2^5)(x - \alpha_2^7)(x - \alpha_2^9)(x - \alpha_2^{11})(x - \alpha_2^{13})(x - \alpha_2^{15}).$$

*Similarly,*

$$M_0^2(x) = (x - 1), \ M_1^2(x) = (x - \alpha_1^2)(x - \alpha_1^6) \text{ and } M_2^3(x) = (x - \alpha_2^2)(x - \alpha_2^6)(x - \alpha_2^{10})(x - \alpha_2^{14}).$$

*Thus the polynomials* $g_i(x) = lcm(M_i^1(x), M_i^2(x))$ *are given by*

$$g_0(x) = (x - 1)(x - \alpha_0), \ g_1(x) = (x - \alpha_1)(x - \alpha_1^2)(x - \alpha_1^3)(x - \alpha_1^5)(x - \alpha_1^6)(x - \alpha_1^7), \text{ and}$$

$$g_2(x) = (x-\alpha_2)(x-\alpha_2^2)(x-\alpha_2^3)(x-\alpha_2^5)(x-\alpha_2^6)(x-\alpha_2^7)(x-\alpha_2^9)(x-\alpha_2^{10})(x-\alpha_2^{11})(x-\alpha_2^{13})(x-\alpha_2^{14})(x-\alpha_2^{15})$$

*which generates the cyclic BCH codes* $\mathcal{C}_0$, $\mathcal{C}_1$ *and* $\mathcal{C}_2$ *of length* $2$, $8$ *and* $16$ *with minimum hamming distance at least* $3$, $4$ *and* $4$, *respectively. Similarly we can construct a sequence of cyclic codes over* $\mathcal{K}_i$ *if we replace* $\alpha_i$ *with* $\overline{\alpha}_i$, *for* $0 \leq i \leq 2$.

# 4 Construction III

For any $j$ such that $1 \leq j \leq r$, let $p_j$ be a prime and $m_j$ a positive integer. The ring $A_j = \mathbb{Z}_{p_j^{m_j}}$ is a unitary finite local commutative ring with maximal ideals $M_j$ and residue fields $\mathbb{K}_j = \frac{A_j}{M_j}$. The natural projections $\pi_j : A_j[x] \to \mathbb{K}_j[x]$ is defined by $\pi(\sum_{k=0}^{n} a_k x^k) = \sum_{k=0}^{n} \overline{a_k} x^k$, where $\overline{a_k} = a_k + M_j$ for $k = 0, 1, \cdots, n$. Thus, the natural ring morphism $A_j \to K_j$ is simply the restriction of $\pi_j$ to the constant polynomial. Now, if $f_j(x) \in A_j[x]$ is a basic irreducible polynomial with degree $h = b^t$, where $b$ is a prime and $t$ is a positive integer, then $\mathcal{R}_j = \frac{A_j[x]}{(f_j(x)))} = GR(p_j^{m_j}, h)$ is the collection of the Galois ring extension of $A_j$ and $\mathbb{K}_j = \frac{\mathcal{R}_j}{\mathcal{M}_j} = \frac{A_j[x]/(f_j(x))}{(M_j, f_j(x))/(f_j(x))} = \frac{A_j[x]}{(M_j, f_j(x))} = \frac{(A_j/M_j)[x]}{(\pi_j(f_j(x)))}$ is the residue field of $\mathcal{R}_j$, where $M_j = (M_j, f_j(x))$ is the corresponding maximal ideal of $\mathcal{R}_j$ for each $j$ such that $1 \leq j \leq r$. For the construction of a chain of Galois ring, [1, Lemma XVI.7] facilitate us.

Since $1, b, b^2, \cdots, b^{t-1}, b^t$ are the only divisors of $h$, and take $h_0 = 1, h_1 = b, h_2 = b^2, \cdots, h_t = b^t = h$, so by [1, Lemma XVI.7], there exist basic irreducible polynomials $f_{1,j}(x), f_{2,j}(x), \cdots, f_{t,j}(x) \in A_j[x]$ with degrees $h_1, h_2, \cdots, h_t$, respectively, such that we can constitute the Galois subring $\mathcal{R}_{i,j} = \frac{\mathbb{Z}_{p_j^{m_j}}[x]}{(f_{i,j}(x))} = GR(p_j^{m_j}, h_i)$, of $\mathcal{R}_j$ with the maximal ideal $\mathcal{M}_{i,j} = (M_j, f_{i,j}(x))/(f_{i,j}(x))$, for each $i$ such that $0 \leq i \leq t$ and $1 \leq j \leq r$. Then the residue fields of each $\mathcal{R}_{i,j}$ becomes

$$\mathbb{K}_{i,j} = \frac{\mathcal{R}_{i,j}}{\mathcal{M}_{i,j}} = \frac{A_j[x]/(f_{i,j}(x))}{(M_j, f_{i,j}(x))/(f_{i,j}(x))} = \frac{A_j[x]}{(M_j, f_{i,j}(x))} = \frac{(A_j/M_j)[x]}{(\pi_j(f_{i,j}(x)))} = \frac{K_j[x]}{(\bar{f}_{i,j}(x))} = GF(p_j^{h_i}).$$

As each $h_i$ divides $h_{i+1}$ for all $0 \leq i \leq t$, so by [1, Lemma XVI.7], there is a chain

$$A_j = \mathcal{R}_{0,j} \subset \mathcal{R}_{1,j} \subset \mathcal{R}_{2,j} \subset \cdots \subset \mathcal{R}_{t-1,j} \subset \mathcal{R}_{t,j} = \mathcal{R}_j$$

of Galois rings with corresponding chain of residue fields

$$\mathbb{Z}_{p_j} = \mathbb{K}_{0,j} \subset \mathbb{K}_{1,j} \subset \mathbb{K}_{2,j} \subset \cdots \subset \mathbb{K}_{t-1,j} \subset \mathbb{K}_j.$$

Let $\mathcal{A}_i = \mathcal{R}_{i,1} \times \mathcal{R}_{i,2} \times \mathcal{R}_{i,3} \times \cdots \times \mathcal{R}_{i,r}$, for each $i$ such that $0 \leq i \leq t$. Then we get a chain of 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 an other chain of commutative 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 $\mathcal{K}_i = \mathbb{K}_{1_i} \times \mathbb{K}_{2_i} \times \cdots \times \mathbb{K}_{r_i}$, for each $i$ such that $0 \leq i \leq t$.

Let $\mathcal{A}_i^*$, $\mathcal{K}_i^*$, $\mathcal{R}_{i,j}^*$ and $\mathbb{K}_{i,j}^*$ be the multiplicative groups of units of $\mathcal{A}_i$, $\mathcal{K}_i$, $\mathcal{R}_{i,j}$ and $\mathbb{K}_{i,j}$, for $1 \leq j \leq r$, respectively, for each $i$ such that $0 \leq i \leq t$. Now the next theorem, extension of [1, Theorem XVIII.1], is fundamental in the decomposition of the polynomial $x^{s_i} - 1$ 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 $\beta_{i,j} \in \mathcal{R}_{i,j}^*$, for each $i$, where $0 \leq i \leq t$ and $1 \leq j \leq r$, such that $\alpha_i = (\beta_{i,1}, \beta_{i,2}, \cdots, \beta_{i,r})$.

**Theorem 4.1.** *For each $i$ such that $0 \leq i \leq t$, let $\mathcal{A}_i = \mathcal{R}_{i,1} \times \mathcal{R}_{i,2} \times \mathcal{R}_{i,3} \times \cdots \times \mathcal{R}_{i,r}$, where each $\mathcal{R}_{i,j}$, for $1 \leq j \leq r$, is a local commutative ring. Then $\mathcal{A}_i^* = \mathcal{R}_{i,1}^* \times \mathcal{R}_{i,2}^* \times \mathcal{R}_{i,3}^* \times \cdots \times \mathcal{R}_{i,r}^*$ for each $i$ such that $0 \leq i \leq t$.*

Note that $\overline{\alpha}_i = (\overline{\beta}_{i,1}, \overline{\beta}_{i,2}, \cdots, \overline{\beta}_{i,r})$. Following theorem indicates the condition under which $x^{s_i} - 1$ can be factored over $\mathcal{A}_i^*$, for each $i$ such that $0 \leq i \leq t$.

**Theorem 4.2.** *For each $i$, where $0 \leq i \leq t$, the polynomial $x^{s_i} - 1$ can be factored over the multiplicative group $\mathcal{A}_i^*$ as $x^{s_i} - 1 = (x - \alpha_i)(x - \alpha_i^2) \cdots (x - \alpha_i^s)$ if and only if $\bar{\beta}_{i,j}$, for each $j$ such that $1 \leq j \leq r$, has order $s_i$ in $\mathbb{K}_{i,j}^*$ such that $gcd(s_i, p) = 1$ and $\alpha_i = (\beta_{i,1}, \beta_{i,2}, \cdots, \beta_{i,r})$.*

**Proof.** *Suppose that the polynomial $x^{s_i} - 1$ can be factored over $\mathcal{A}_i^*$ as $x^{s_i} - 1 = (x - \alpha_i)(x - \alpha_i^2) \cdots (x - \alpha_i^{s_i})$, for each $i$ such that $0 \leq i \leq t$. Then $x^{s_i} - 1$ can be factored over $\mathcal{R}_{i,j}^*$ as $x^{s_i} - 1 = (x - \beta_{i,j})(x - \beta_{i,j}^2) \cdots (x - \beta_{i,j}^{s_i})$, for each $1 \leq j \leq r$. Now it follows from the extension of [7, theorem 3] that $\bar{\beta}_{i,j}$ has order $s_i$ in $\mathbb{K}_{i,j}^*$, for each $0 \leq i \leq t$ and for each $1 \leq j \leq r$. Conversely, suppose that $\bar{\beta}_{i,j}$ has order $s_i$ in $\mathbb{K}_{i,j}^*$, for each $i, j$, where $0 \leq i \leq t$ and $1 \leq j \leq r$. Again it* *follows, from the extension of [7, theorem 3], that the polynomial $x^{s_i} - 1$ can be factored over $\mathcal{R}^*_{i,j}$ as $x^{s_i} - 1 = (x - \beta_{i,j})(x - \beta^2_{i,j}) \cdots (x - \beta^{s_i}_{i,j})$, for each $i, j$, where $0 \le i \le t$ and $1 \le j \le r$. Since $\alpha_i = (\beta_{i,1}, \beta_{i,2}, \cdots, \beta_{i,r})$, for $0 \le i \le t$, so $x^{s_i} - 1 = (x - \alpha_i)(x - \alpha_i^2) \cdots (x - \alpha_i^{s_i})$ over $\mathcal{A}^*_i$, for each $i$, where $0 \le i \le t$.*

**Corollary 4.3.** *[8, Theorem 3.4] The polynomial $x^s - 1$ 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 $\alpha$ corresponds to $\beta = (\beta_1, \beta_2, \cdots, \beta_r)$, where $j = 1, 2, 3, \cdots, r$.*

Let $H_{\alpha_i, s_i}$ denotes the cyclic subgroup of $\mathcal{A}^*_i$ generated by $\alpha_i$, for each $i$, where $0 \le i \le t$, i.e., $H_{\alpha_i, s_i}$ contains all the roots of $x^{s_i} - 1$ provided the condition of above theorem are met. The BCH codes $\mathcal{C}_i$ over $\mathcal{A}^*_i$ can be obtained as the direct product of BCH codes $\mathcal{C}_{i,j}$ over $\mathcal{R}^*_{i,j}$. To construct the cyclic BCH codes over $\mathcal{A}^*_i$, we need to choose certain elements of $H_{\alpha_i, n_i}$ as the roots of generator polynomials $g_i(x)$ of the codes, where $n_i = \gcd(p_1^{h_i}, p_2^{h_i}, p_3^{h_i}, \cdots, p_r^{h_i})$. So that, $\alpha_i^{e_1}, \alpha_i^{e_2}, \cdots, \alpha_i^{e_{n_i - k_i}}$ are all the roots of $g_i(x)$ in $H_{\alpha_i, n_i}$, we construct $g_i(x)$ as

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

where $M_i^{e_{l_i}}(x)$ are the minimal polynomials of $\alpha_i^{e_{l_i}}$, for $l = 1, 2, \cdots, n_i - k_i$, where each $\alpha_i^{e_{l_i}} = (\beta^{e_{l_i}}_{i,1}, \beta^{e_{l_i}}_{i,2}, \cdots, \beta^{e_{l_i}}_{i,r})$. The following theorem is the extension of [7, Lemma 3] and provides us a method for construction of $M_i^{e_{l_i}}(x)$, the minimal polynomial of $\alpha_i^{e_{l_i}}$ over the ring $\mathcal{A}_i$.

**Theorem 4.4.** *For each $i$ such that $0 \le i \le t$, let $M_i^{e_{l_i}}(x)$ be the minimal polynomial of $\alpha_i^{e_{l_i}}$ over $\mathcal{A}_i$, where $\alpha_i^{e_{l_i}}$ generates $H_{\alpha_i, n_i}$, for $l_i = 1, 2, \cdots, n_i - k_i$ and $0 \le i \le t$. Then $M_i^{e_{l_i}}(x) = \prod_{\xi_i \in B_i^{l_i}} (x - \xi_i)$, where $B_i^{l_i} = \{(\alpha_i^{e_{l_i}})^{m_{i,j}} : m_{i,j} = \prod_{j=1}^r p_i^{q_{i,j}}$, where $1 \le l_i \le n_i - k_i$, $0 \le q_{i,j} \le h_i - 1\}$.*

**Proof.** *Let $\overline{M}_i^{e_{l_i}}(x)$ be the projection of $M_i^{e_{l_i}}(x)$ over the fields $\mathbb{K}_{i,j}$ and $\overline{M}^{e_{l_i}}_{i,j}(x)$ be the minimal polynomial of $\overline{\alpha}_i^{e_{l_i}}$ over $\mathbb{K}^*_{i,j}$, for each $i$, where $0 \le i \le t$, $1 \le j \le r$ and $1 \le l_i \le n_i - k_i$. We can verify that each $\overline{M}_i^{e_{l_i}}(x)$ is divisible by $\overline{M}^{e_{l_i}}_{i,j}(x)$, for $0 \le i \le t$, $1 \le j \le r$ and $1 \le l_i \le n_i - k_i$. Thus it has, among its roots, distinct elements of the sequences $\overline{\alpha}_i^{e_{l_i}}, (\overline{\alpha}_i^{e_{l_i}})^{p_j}, (\overline{\alpha}_i^{e_{l_i}})^{p_j^2}, \cdots, (\overline{\alpha}_i^{e_{l_i}})^{p_j^{h_i - 1}}$, for each $i, j$, where $0 \le i \le t$, $1 \le j \le r$ and $1 \le l_i \le n_i - k_i$. Hence $M_i^{e_{l_i}}(x)$ has, among its roots, distinct elements of the sequence $\alpha_i^{e_{l_i}}, (\alpha_i^{e_{l_i}})^{p_j}, (\alpha_i^{e_{l_i}})^{p_j^2}, \cdots, (\alpha_i^{e_{l_i}})^{p_j^{h_i - 1}}$, for each $i, j$, where $0 \le i \le t$, $1 \le j \le r$ and $1 \le l_i \le n_i - k_i$. Thus any element $\gamma_i = (\alpha_i^{e_{l_i}})^{p_j^{m_i}}$ of the above sequence is the root of $M_i^{e_{l_i}}(x)$, for each $i, j$, where $0 \le i \le t$, $1 \le j \le r$, $0 \le m_i \le h_i - 1$ and $1 \le l_i \le n_i - k_i$. Choose any $k$ in the range $1 \le k \le r$ such that $k \ne j$. Then we know that if $\gamma_{i,k}$ is a root of $\overline{M}^{e_{l_i}}_{i,k}(x)$ implies that $(\gamma_{i,k})^{p_k^{q_i}}$ is a root of $M_i^{e_{l_i}}(x)$ (which has coefficients in $\mathbb{K}_{i,k}$), for $0 \le q_i \le h_i - 1$. Hence $(\gamma_i)^{p_k^{q_i}} = (\alpha_i^{e_{l_i}})^{p_j^{m_i} p_k^{q_i}}$ is a root of $M_i^{e_{l_i}}(x)$. Proceeding in this manner, we can show that $M_i^{e_{l_i}}(x)$ necessarily has as roots all distinct member of $B_i^{l_i}$. But the polynomial $\prod_{\xi_i \in B_i^{l_i}} (x - \xi_i)$ has, by construction, coefficient in the direct product of $A_j$. Hence $M_i^{e_{l_i}}(x) = \prod_{\xi_i \in B_i^{l_i}} (x - \xi_i)$.*

**Corollary 4.5.** *[8, Theorem 3.5] For any positive integer $l$, let $M_l(x)$ be the minimal polynomial of $\alpha^l$ over $\mathcal{R}$, where $\alpha$ generates $H_{\alpha,n}$. Then $M_l(x) = \prod_{\xi \in B_l} (x - \xi)$, where $B_l$ is all distinct elements of the sequence $\{(\alpha^l)^m : m = \prod_{j=1}^r q_j^{s_j},\ q_j = p_j^{m_j},\ 0 \le s_j \le h - 1\}$.*

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 extend [8, Theorem 2.5]

**Theorem 4.6.** *[9, Theorem 11] For each* $i$ *such that* $0 \leq i \leq t$*, let* $g_i(x)$ *be the generator polynomial of BCH code* $\mathcal{C}_i$ *over* $\mathcal{A}_i$ *from the chain* $\mathcal{A}_0 \subset \mathcal{A}_1 \subset \mathcal{A}_2 \subset \cdots \subset \mathcal{A}_{t-1} \subset \mathcal{A}_t$*, with length* $n_i = s_i$*, and 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* $g_i(x)$ *in* $H_{\alpha_i,n_i}$*, where* $\alpha_i$ *has order* $n_i$*. The minimum Hamming distance of this code is greater than the largest number of consecutive integers modulo* $n_i$ *in* $E_i = \{e_1, e_2, e_3, \cdots, e_{n_i-k_i}\}$.

**Corollary 4.7.** *[8, Theorem 2.5] 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* $\alpha$ *has order* $n$*, then minimum Hamming distance of the code is greater than the largest number of consecutive integers modulo* $n$ *in* $E = \{e_1, e_2, e_3, \cdots, e_{n-k}\}$.

## 4.1 Algorithm

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

1. Choose irreducible polynomial $f_{i,j}(x)$ over $\mathbb{Z}_{p_j^{m_j}}$ of degree $h_i = b^i$, for $1 \leq i \leq t$, which are also irreducible over $GF(p)$ and form the chains of Galois rings

$$\begin{aligned} \mathbb{Z}_{p_j^{m_j}} &= GR(p_j^{m_j}, h_0) \subset GR(p_j^{m_j}, h_1) \subset \cdots \subset GR(p_j^{m_j}, h_{t-1}) \subset GR(p_j^{m_j}, h_t) \text{ or} \\ A_j &= \mathcal{R}_{0,j} \subseteq \mathcal{R}_{1,j} \subseteq \mathcal{R}_{2,j} \subseteq \cdots \subseteq \mathcal{R}_{t-1,j} \subseteq \mathcal{R}_{t,j} = \mathcal{R}_j \end{aligned}$$

   and its corresponding chains of residue fields are

$$\begin{aligned} \mathbb{Z}_{p_j} &= GF(p_j) \subset GF(p_j^{h_1}) \subset \cdots \subset GF(p_j^{h_{t-1}}) \subset GF(p_j^{h}) \text{ or} \\ &= \mathbb{K}_{0,j} \subset \mathbb{K}_{1,j} \subset \mathbb{K}_{2,j} \cdots \subset \mathbb{K}_{t-1,j} \subset \mathbb{K}_{t,j} = \mathbb{K}_j, \end{aligned}$$

   where each $GF(p_j^{h_i}) \simeq \frac{K_j[x]}{(\pi_j(f_{i,j}(x)))}$, for $1 \leq i \leq t$.

2. Now put $\mathcal{A}_i = \mathcal{R}_{i,1} \times \mathcal{R}_{i,2} \times \mathcal{R}_{i,3} \times \cdots \times \mathcal{R}_{i,r}$, for $0 \leq i \leq t$, where each $\mathcal{R}_{i,j}$ is local commutative ring, 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 an other 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 $\overline{\eta}_{i,j} = \overline{\eta}_i$ be the primitive elements in $\mathbb{K}_i^*$, for $0 \leq i \leq t$. Then $\eta_{i,j}$ has order $d_{i,j}n_i$ in $\mathcal{R}_{i,j}^*$ for some integers $d_{i,j}$, put $\beta_{i,j} = (\eta_{i,j})^{d_{i,j}}$. Then $\alpha_i = (\beta_{1_i}, \beta_{2_i}, \beta_{3_i}, \cdots, \beta_{r_i})$ has order $n_i$ in $\mathcal{R}_{i,j}^*$ and generates $H_{\alpha_i,n_i}$. Assume for each $i$, where $0 \leq i \leq t$, $\alpha_i$ be any element of $H_{\alpha_i,n_i}$.

4. Let $\alpha_i^{e_1}, \alpha_i^{e_2}, \alpha_i^{e_3}, \cdots, \alpha_i^{e_{n_i-k_i}}$ are chosen to be the roots of $g_i(x)$. Find $M_i^{e_{l_i}}(x)$ are the minimal polynomials of $\alpha_i^{e_{l_i}}$, for $l_i = 1, 2, \cdots, n_i - k_i$, where each $\alpha_i^{e_{l_i}} = (\beta_i^{e_{l_i}}, \beta_i^{e_{l_i}}, \beta_i^{e_{l_i}}, \cdots, \beta_i^{e_{l_i}})$. Then $g_i(x)$ 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 lcm 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 in the set $E_i = \{e_1, e_2, e_3, \cdots, e_{n_i-k_i}\}$ for each $i$, where $0 \leq i \leq t$.

**Example 4.8.** *We initiate by constructing a chain of codes of lengths $1$, $8$ and $16$, taking $A_1 = \mathbb{Z}_9$ and $A_2 = \mathbb{Z}_5$. Since $M_1 = \{0, 3, 6\}$ and $M_2 = \{0\}$, so $K_1 = \frac{A_1}{M_1} \simeq \mathbb{Z}_3$ and $K_2 = \frac{A_2}{M_2} \simeq \mathbb{Z}_5$. The regular polynomials $f_1(x) = x^4 + x + 8 \in \mathbb{Z}_9[x]$ and $f_2(x) = x^4 + x^2 + x + 1 \in \mathbb{Z}_5[x]$ are such that $\pi_1(f_1(x)) = x^4 + x + 2$ and $\pi_2(f_2(x)) = x^4 + x^2 + x + 1$ are irreducible polynomials with degree $h = 2^2$ over $\mathbb{Z}_3$ and $\mathbb{Z}_5$, respectively. By [9, Theorem 3], it follows that $f_1(x)$ and $f_2(x)$ are irreducible over $A_1$ and $A_2$. Let $\mathcal{R}_1 = \frac{\mathbb{Z}_{3^2}[x]}{(f_1(x))} = GR(3^2, 4)$, $\mathcal{R}_2 = \frac{\mathbb{Z}_5[x]}{(f_2(x))} = GR(5, 4)$ be the Galois rings and $\mathbb{K}_1 = \frac{\mathbb{Z}_3[x]}{(\pi_1(f_1(x)))} = GF(3^4)$, $\mathbb{K}_2 = \frac{\mathbb{Z}_5[x]}{(\pi_2(f_2(x)))} = GF(5^4)$ be their corresponding residue fields. Since $1$, $2$ and $2^2$ are the only divisors of $4$, it follows that $h_1 = 1$, $h_2 = 2$ and $h_3 = 2^2$. Then there exist irreducible polynomials $f_{1,1}(x) = x^2 + 1$, $f_{2,1}(x) = f_1(x)$ in $\mathbb{Z}_9[x]$, and $f_{1,2}(x) = x^2 + 2$, $f_{2,2}(x) = f_2(x)$ in $\mathbb{Z}_5[x]$ with degrees $h_2 = 2$ and $h_3 = 4$ such that we can constitute the Galois rings $\mathcal{R}_{0,1} = A_1$, $\mathcal{R}_{1,1} = \frac{\mathbb{Z}_{3^2}[x]}{(f_{1,1}(x))} = GR(3^2, h_2)$, $\mathcal{R}_{2,1} = \mathcal{R}_1$ and $\mathcal{R}_{0,2} = A_2$, $\mathcal{R}_{1,2} = \frac{\mathbb{Z}_5[x]}{(f_{1,2}(x))} = GR(5, h_2)$ and $\mathcal{R}_{1,2} = \mathcal{R}_2$. So*

$$A_j = \mathcal{R}_{0,j} \subset \mathcal{R}_{1,j} \subset \mathcal{R}_{2,j} = \mathcal{R}_j, \text{ for } j = 1, 2.$$

*Again by the same argument $\mathbb{K}_{0,1} = \mathbb{Z}_3$, $\mathbb{K}_{1,1} = \frac{\mathbb{Z}_3[x]}{(\pi_1(f_{1,1}(x)))} = GF(3^2)$, $\mathbb{K}_{2,1} = \mathbb{K}_1$ and $\mathbb{K}_{0,2} = \mathbb{Z}_5$, $\mathbb{K}_{1,2} = \frac{\mathbb{Z}_5[x]}{(\pi_2(f_{1,2}(x)))} = GF(5^2)$, $\mathbb{K}_{2,2} = \mathbb{K}_2$. So we get chains of fields*

$$A_j = \mathbb{K}_{0,j} \subset \mathbb{K}_{1,j} \subset \mathbb{K}_{2,j} = \mathbb{K}_j, \text{ for } j = 1, 2.$$

*Now $\mathcal{A}_i = \mathcal{R}_{i,1} \times \mathcal{R}_{i,2}$ such that $\mathcal{A}_0 \subseteq \mathcal{A}_1 \subseteq \mathcal{A}_2$, i.e.,*

$$\begin{array}{lllll} \mathcal{A}_0 & = & \mathcal{R}_{0,1} = \mathbb{Z}_9 & \times & \mathcal{R}_{0,2} = \mathbb{Z}_5 \\ \mathcal{A}_1 & = & \mathcal{R}_{1,1} = \frac{\mathbb{Z}_{3^2}[x]}{(x^2+1)} & \times & \mathcal{R}_{1,2} = \frac{\mathbb{Z}_5[x]}{(x^2+2)} \\ \mathcal{A}_2 & = & \mathcal{R}_{2,1} = \frac{\mathbb{Z}_{3^2}[x]}{(x^4+x-1)} & \times & \mathcal{R}_{2,2} = \frac{\mathbb{Z}_5[x]}{(x^4+x^2+x+1)} \end{array}$$

*and*

$$\begin{array}{lllll} \mathcal{K}_0 & = & \mathbb{K}_{0,1} = \mathbb{Z}_3 & \times & \mathbb{K}_{0,2} = \mathbb{Z}_5 \\ \mathcal{K}_1 & = & \mathbb{K}_{1,1} = \frac{\mathbb{Z}_3[x]}{(x^2+1)} & \times & \mathbb{K}_{1,2} = \frac{\mathbb{Z}_5[x]}{(x^2+2)} \\ \mathcal{K}_2 & = & \mathbb{K}_{2,1} = \frac{\mathbb{Z}_3[x]}{(x^4+x-1)} & \times & \mathbb{K}_{2,2} = \frac{\mathbb{Z}_5[x]}{(x^4+x^2+x+1)} \end{array}$$

*Let $u = \{x\}$ in $\mathcal{R}_{i,j}$ such that $\overline{u} = \{X\}$ in $\mathbb{K}_{i,j}$. Then $\overline{u}+1$ has order $8, 24, 80$ and $624$ in $\mathbb{K}_{1,1}, \mathbb{K}_{1,2}, \mathbb{K}_{2,1}$ and $\mathbb{K}_{2,2}$, respectively. So $\overline{\beta}_{1,1} = \overline{\beta}_{1,2} = \overline{\beta}_{2,1} = \overline{\beta}_{2,2} = \overline{u}+1$. But $u+1$ has order $24, 120, 80$ and $624$ in $\mathcal{R}_{1,1}, \mathcal{R}_{1,2}, \mathcal{R}_{2,1}$ and $\mathcal{R}_{2,2}$, so put $\beta_{1,1} = (u+1)^3$, $\beta_{1,2} = (u+1)^{15}$, $\beta_{2,1} = (u+1)^5$ and $\beta_{2,2} = (u+1)^{39}$ and get $\alpha_2 = (\beta_{2,1}, \beta_{2,2})$ which generates $H_{\alpha_2,16}$ and $\alpha_1 = (\beta_{1,1}, \beta_{1,2})$ which generates $H_{\alpha_1,8}$. Also $2$ has order $4$ in $\mathbb{K}_{0,2}$ and has order $2$ in $\mathbb{K}_{0,1}$, so $\overline{\beta}_{0,1} = \overline{\beta}_{0,2} = 2$. But $2$ has order $4$ in $\mathcal{R}_{0,2}$ and has order $6$ in $\mathcal{R}_{0,1}$, so $\beta_{0,1} = 2$ and $\beta_{0,2} = 24$ get $\alpha_0 = (\beta_{0,1}, \beta_{0,2})$ which generates $H_{\alpha_0,2}$. Choose $\alpha_i$ and $\alpha_i^2$ to be roots of the generator polynomials $g_i(X)$ of the BCH codes $\mathcal{C}_i$ over the chain $\mathcal{A}_0 \subset \mathcal{A}_1 \subset \mathcal{A}_2$. Then $M_0^1(x)$, $M_1^1(x)$ and $M_2^1(x)$ has as roots all distinct element in the sets $B_0^1 = \{\alpha_0\} \subset H_{\alpha_0,2}$, $B_1^1 = \{\alpha_1, \alpha_1^3, \alpha_1^5, \alpha_1^7\} \subset H_{\alpha_1,8}$ and $B_2^1 = \{\alpha_2, \alpha_2^3, \alpha_2^5, \alpha_2^7, \alpha_2^9, \alpha_2^{11}, \alpha_2^{13}, \alpha_2^{15}\} \subset H_{\alpha_2,16}$, respectively. So*

$$M_0^1(x) = (x - \alpha_0),\ M_1^1(x) = (x - \alpha_1)(x - \alpha_1^3)(x - \alpha_1^5)(x - \alpha_1^7),$$

*and*

$$M_2^1(x) = (x - \alpha_2)(x - \alpha_2^3)(x - \alpha_2^5)(x - \alpha_2^7)(x - \alpha_2^9)(x - \alpha_2^{11})(x - \alpha_2^{13})(x - \alpha_2^{15})$$

*Similarly,*

$$M_0^2(x) = (x - 1),\ M_1^2(x) = (x - \alpha_1^2)(x - \alpha_1^6),$$
$$M_2^3(x) = (x - \alpha_2^2)(x - \alpha_2^6)(x - \alpha_2^{10})(x - \alpha_2^{14})$$

*Thus the polynomials $g_i(x) = lcm(M_i^1(x), M_i^2(x))$ are given by*

$$g_0(x) = (x - 1)(x - \alpha_0),\ g_1(x) = (x - \alpha_1)(x - \alpha_1^2)(x - \alpha_1^3)(x - \alpha_1^5)(x - \alpha_1^6)(x - \alpha_1^7),$$

$$g_2(x) = (x-\alpha_2)(x-\alpha_2^2)(x-\alpha_2^3)(x-\alpha_2^5)(x-\alpha_2^6)(x-\alpha_2^7)(x-\alpha_2^9)(x-\alpha_2^{10})(x-\alpha_2^{11})(x-\alpha_2^{13})(x-\alpha_2^{14})(x-\alpha_2^{15})$$

*which generates the cyclic BCH codes $\mathcal{C}_0$, $\mathcal{C}_1$ and $\mathcal{C}_2$ of length $2$, $8$ and $16$ with minimum hamming distance $2$, $3$ and $3$, respectively. Similarly, we can construct cyclic codes over $\mathcal{K}_i$ if we replace $\alpha_i$ with $\overline{\alpha}_i$, for $0 \leq i \leq 2$.*

# 5 Conclusion

For a non negative 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 (each $\mathcal{A}_i$ is constructed by the direct product of suitable Galois rings with multiplicative group $\mathcal{A}_i^*$ of units) and $\mathcal{K}_0 \subset \mathcal{K}_1 \subset \cdots \subset \mathcal{K}_{t-1} \subset \mathcal{K}_t$ be the corresponding chain of unitary commutative rings (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 [8], 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 $0 \leq i \leq t$ and $0 \leq j \leq t$ having residue fields $\mathbb{K}_{i,j}$, where $0 \leq i \leq t$. For each member in the chain of 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 product of local commutative rings $\mathcal{R}_{i,j}$ with different lengths and sequence 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.,

$$\begin{array}{ccccccccc}
\mathcal{C}_0 & = & \mathcal{C}_{0,0} & \times & \mathcal{C}_{0,1} & \times & \cdots & \times & \mathcal{C}_{0,r} \\
\mathcal{C}_1 & = & \mathcal{C}_{1,0} & \times & \mathcal{C}_{1,1} & \times & \cdots & \times & \mathcal{C}_{1,r} \\
\vdots & & \vdots & & \vdots & & \ddots & & \vdots \\
\mathcal{C} & = & \mathcal{C}_{t,0} & \times & \mathcal{C}_{t,1} & \times & & \times & \mathcal{C}_{t,r}
\end{array}$$

and

$$\begin{array}{ccccccccc}
\mathcal{C}'_0 & = & \mathcal{C}'_{0,0} & \times & \mathcal{C}'_{0,1} & \times & \cdots & \times & \mathcal{C}'_{0,r} \\
\mathcal{C}'_1 & = & \mathcal{C}'_{1,0} & \times & \mathcal{C}'_{1,1} & \times & \cdots & \times & \mathcal{C}'_{1,r} \\
\vdots & & \vdots & & \vdots & & \ddots & & \vdots \\
\mathcal{C}' & = & \mathcal{C}'_{t,0} & \times & \mathcal{C}'_{t,1} & \times & & \times & \mathcal{C}'_{t,r}.
\end{array}$$

In fact this technique provides a choice to select a most suitable BCH code $\mathcal{C}_i$ (respectively, BCH code $\mathcal{C}'_i$), where $0 \leq i \leq t$, with required error correction capabilities and code rate but with compromising length.

# Acknowledgment

The authors would like to thank the anonymous reviewers for their intuitive commentary that significantly improved the worth of this work and the FAPESP by financial support 2013/04124-6.

# Competing Interests

The authors declare that no competing interests exist.

# References

[1] McDonlad, BR. Finite rings with identity. Marcel Dekker, New York; 1974.

[2] Blake, IF. Codes over certain rings. Information and Control. 1972; 20: 396-404.

[3] Blake, IF. Codes over integer residue rings. Information and Control. 1975; 29: 295-300.

[4] Spiegel, E. Codes over $\mathbb{Z}_m$. Information and Control. 1977: 35: 48-51.

[5] Spiegel, E. Codes over $\mathbb{Z}_m$, revised. Information and Control. 1978; 37: 100-104.

[6] Forney Jr., GD. On decoding BCH codes. IEEE Trans. Inform. Theory. 1965; IT-11(4): 549-557.

[7] Shankar, P. On BCH codes over arbitrary integer rings. IEEE Trans. Inform. Theory. 1979; IT-25(4): 480-483.

[8] Andrade, AA, Palazzo Jr., R. Construction and decoding of BCH codes over finite rings. Linear Algebra and its Applications. 1999; 286: 69-85.

[9] Andrade, AA, Shah, T, Qamar, A. Chain of finite rings and construction of BCH Codes. Proceending of XXX Brazilian Symposium of Telecommunications - SBrT12, 13-16 of September of 2012, Brasília - DF.

---



***Peer-review history:***
*The peer review history for this paper can be accessed here (Please copy paste the total link in your browser address bar)*
*www.sciencedomain.org/review-history.php?iid=366&id=5&aid=*2845