# Chain of finite rings and construction of BCH Codes

Antonio Aparecido de Andrade, Tariq Shah and Attiq Qamar

***Abstract*— 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, where 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, 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. This correspondence presents four different type of construction techniques of generator polynomials of sequences of BCH codes having entries from $\mathcal{A}_i^*$ and $\mathcal{K}_i^*$ for each $i$, where $0 \leq i \leq t$. The BCH codes constructed in [1] are limited to given code rate and error correction capability, however, proposed work offers a choice for picking a suitable BCH code concerning code rate and error correction capability.**

***Keywords*— Units of local ring, BCH code, McCoy rank, direct product of local rings.**

## I. INTRODUCTION

Linear codes over finite rings have been discussed in a series of papers initiated by Blake [2], [3], Spiegel [4], [5] and 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 the multiplicative group of unit elements of a Galois ring extension of $\mathbb{Z}_{p^m}$, Shankar [7] has constructed BCH codes over $\mathbb{Z}_{p^m}$. Moreover, Andrade and Palazzo [1] have further extend these constructions of BCH codes over finite commutative rings with identity. Both construction techniques of [1] 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 study is to get the factorization of $x^s - 1$ over the group of units of an appropriate extension ring of the given local ring.

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

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

$$M = \begin{bmatrix} \alpha_1 & \alpha_2 & \cdots & \alpha_n \\ \alpha_1^2 & \alpha_2^2 & \cdots & \alpha_n^2 \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^k & \alpha_2^k & \cdots & \alpha_n^k \end{bmatrix} \quad (1)$$

based on the vector $\eta = (\alpha_1, \alpha_2, \cdots, \alpha_n)$ with $\alpha_i$, 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 is linked with the multiplicative group $\mathcal{A}^*$ of units of the ring $\mathcal{A}$.

For $h = b^t$, where $b$ is 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, there exist 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 and residue field $\mathcal{R}/\mathcal{M}$). For each $i$, for $0 \leq i \leq t$, 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 $p$ (an extension of [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 a cyclic subgroup $G_{n_i}$ in $\mathcal{R}_i^*$ for each $i$ [7, Lemma 1]. So by extending the given algorithm [7] for constructing a BCH-type 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 $i \geq 2$. By these motivations in this paper for any $t \in \mathbb{Z}^+$, if $\mathcal{A}_0 \subset \mathcal{A}_1 \subset \cdots \subset \mathcal{A}_{t-1} \subset \mathcal{A}_t$ is a chain of unitary commutative rings, then for each $i$, such that $0 \leq i \leq t$, it follows that $\mathcal{A}_i$ is a direct product of Galois

Antonio Aparecido de Andrade - Department of Mathematics, São Paulo State University, São José do Rio Preto - SP, Brazil, andrade@ibilce.unesp.br. Tariq Shah and Attiq Qamar - Department of Mathematics, Quaid-i-Azam University, Islamabad, Pakistan, stariqshah@gmail.com, qamar.maths@gmail.com. Acknowledgment to FAPESP by financial support, 2007/56052-8 and 2011/03441-2.

rings, i.e.,

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

Moreover, $\mathcal{R}_{0,j} \subset \mathcal{R}_{1,j} \subset \cdots \subset \mathcal{R}_{t-1,j} \subset \mathcal{R}_{t,j}$, for each $1 \leq j \leq r$, is a chain of Galois rings. In type I, for each $i$, where $0 \leq i \leq t$, it follows that $\mathcal{R}_{i,j} = \mathcal{R}_{i,j+1}$, where $1 \leq j \leq r$, while in type II, we have different $\mathcal{R}_{i,j}$ with same characteristic $p$. In type III and IV, we take different $\mathcal{R}_{i,j}$ with different characteristic $p_j$, where $1 \leq j \leq r$.

Corresponding to 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.,

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

Moreover, $\mathbb{K}_{0,j} \subset \mathbb{K}_{1,j} \subset \cdots \subset \mathbb{K}_{t-1,j} \subset \mathbb{K}_{t,j}$, for each $1 \leq j \leq r$, is a chain of corresponding residue fields. In type I and II, we have $\mathbb{K}_{i,j} = \mathbb{K}_{i,j+1}$ and different in remaining types. Therefore, $\mathcal{A}_i^*$ 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.

## II. Basic results

Assume that $(R, M)$ is a finite unitary local commutative ring with residue field $\mathbb{K} = \frac{R}{M} \cong GF(p^m)$, where $p$ is a prime integer, $m$ a positive integer. The natural projection $\pi : R[x] \rightarrow \mathbb{K}[x]$ 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 $R \rightarrow \mathbb{K}$ is simply the restriction of $\pi$ 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 $R[x]$. We say that

1) $a(x)$ is a unit if there exist a polynomial $b(x) \in R[x]$ such that $a(x)b(x) = 1$.
2) $a(x) \neq 0$ is a zero divisor if there exist a polynomial $b(x) \in R[x] \backslash \{0\}$ 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 1:* [8, Theorem XIII.2] Let $(R, M)$ be a local ring and $a(x) = \sum_{i=0}^{n} a_i x^i \in R[x]$. The following assertions are equivalent.

1) $a(x)$ is regular.
2) $< a_1, a_2, \cdots, a_n >= R$.
3) $a_i$ is a unit for some $i$, for $0 \leq i \leq n$.
4) $\pi(a(x)) \neq 0$.

*Theorem 2:* [8, Theorem XV.1] Let $(R, M)$ be a local ring and $a(x)$ be a regular polynomial in $R[x]$ 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 $\alpha$ with $\pi(\alpha) = \bar{\alpha}$.

*Theorem 3:* [8, Theorem XIII.7] Let $(R, M)$ be a local ring and $a(x)$ is regular polynomial in $R[x]$ such that $\pi(a(x))$ is irreducible in $\mathbb{K}[x]$. Then $a(x)$ is irreducible in $R[x]$.

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

*Theorem 4:* [1, Theorem 3.3] If $\mathcal{R} = R_1 \times R_2 \times R_3 \times \cdots \times R_r$, where each $R_j$ is a local finite commutative Galois ring with characteristic $p_j$, then $\mathcal{R}^* = R_1^* \times R_2^* \times R_3^* \times \cdots \times R_r^*$.

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

*Theorem 5:* [1, 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 $j = 1, 2, 3, \cdots, r$.

*Theorem 6:* [1, 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 $B_l$ are all distinct elements of the sequence $\{(\alpha^l)^m : m = \prod_{j=1}^{r} q_j^{s_j},\ q_j = p_j^{m_j},\ 0 \leq s_j \leq h - 1\}$.

*Theorem 7:* [1, Theorem 2.5] If $g(x)$ is a generator polynomial of a 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 $E = \{e_1, e_2, e_3, \cdots, e_{n-k}\}$.

## III. Codes over chain of direct product of finite Galois rings I

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 $\pi : A[x] \rightarrow \mathbb{K}[x]$ 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 $A \rightarrow \mathbb{K}$ is simply the restriction of $\pi$ 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 $\mathcal{R} = \frac{A[x]}{(f(x))} = GR(p^m, h)$ is the Galois ring extension of $A$ and $\mathbb{K} = \frac{\mathcal{R}}{\mathcal{M}} = \frac{A[x]/(f(x))}{(M,f(x))/(f(x))} = \frac{A[x]}{(M,f(x))} = \frac{(A/M)[x]}{(\pi(f(x)))} = GF(p^{mh})$ is residue field of $\mathcal{R}$, where $\mathcal{M} = (M, f(x))/(f(x))$ is the maximal ideal of $\mathcal{R}$.

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

*Lemma 1:* [8, Lemma VII] Every subring of $GR(p^k, s)$ is a Galois ring of the form $GR(p^k, s')$, where $s'$ divides $s$. Conversely, if $s'$ divides $s$, then $GR(p^k, s)$ contains a unique copy of $GR(p^k, s')$.

The elements $1, b, b^2, \cdots, b^{t-1}, b^t$ are divisors of $h$, and so taking $h_0 = 1, h_1 = b, h_2 = b^2, \cdots, h_t = b^t = h$, it follows, by [8, Lemma XVI.7], 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 $\mathcal{R}_i = \frac{A[x]}{(f_i(x))} = GR(p^m, h_i)$, for each $i$, where $1 \le i \le t$, of $\mathcal{R}$ with the maximal ideals $\mathcal{M}_i = (M, f_i(x))/(f_i(x))$, for $1 \le i \le t$. Thus, the residue fields of each $\mathcal{R}_i$ becomes

$$\begin{aligned} \mathbb{K}_i &= \tfrac{\mathcal{R}_i}{\mathcal{M}_i} = \tfrac{A[x]/(f_i(x))}{(M, f_i(x))/(f_i(x))} = \tfrac{A[x]}{(M, f_i(x))} \\ &= \tfrac{(A/M)[x]}{(\pi(f_i(x)))} = \tfrac{K[x]}{(f_i(x))} = GF(p^{h_i}). \end{aligned}$$

As $h_i$ divides $h_{i+1}$ for all $0 \le i \le t$, it follows, by [8, Lemma XVI.7], 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 each $\mathcal{K}_i = \mathbb{K}_i^r$ 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 theorem, extends [8, Theorem XVIII.1] and plays 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 $\beta_i \in \mathcal{R}_i^*$, for $0 \le i \le t$, such that $\alpha_i = (\beta_i, \beta_i, \cdots, \beta_i)$ is an ordered $r$-tuples.

*Theorem 8:* If $\mathcal{A}_i = \mathcal{R}_i^r$, for $0 \le i \le t$, where each $\mathcal{R}_i$ is a local finite commutative ring, then $\mathcal{A}_i^* = (\mathcal{R}_i^*)^r$.

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

*Theorem 9:* For $0 \le i \le t$, the polynomials $x^{s_i} - 1$ 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 $\overline{\beta_i}$ has order $s_i = p^{h_i} - 1$ in $\mathbb{K}_i^*$, where $gcd(s_i, p) = 1$ and $\alpha_i = (\beta_i, \beta_i, \cdots, \beta_i)$.

*Proof.* Suppose that the polynomials $x^{s_i} - 1$ 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 $\mathcal{R}_i^*$ as $x^{s_i} - 1 = (x - \beta_i)(x - \beta_i^2) \cdots (x - \beta_i^{s_i})$, for $0 \le i \le t$. Now, it follows from the extension of [7, Theorem 3] that $\overline{\beta}_i$ has order $s_i$ in $\mathbb{K}_i^*$, for $0 \le i \le t$. Conversely, suppose that $\overline{\beta}_i$ has order $s_i$ in $\mathbb{K}_i^*$, for $0 \le i \le t$. Again, it follows from the extension of [7, Theorem 3] that the polynomials $x^{s_i} - 1$ can be factored over $\mathcal{R}_i^*$ as $x^{s_i} - 1 = (x - \beta_i)(x - \beta_i^2) \cdots (x - \beta_i^{s_i})$, 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 $x^{s_i} - 1 = (x - \alpha_i)(x - \alpha_i^2) \cdots (x - \alpha_i^{s_i})$ over $\mathcal{A}_i^*$, for $0 \le i \le t$.

*Corollary 1:* [1, 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 $i$, 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 Theorem 9 are met. The BCH codes $\mathcal{C}_i$ over $\mathcal{A}_i^*$ can be obtained as the direct product of BCH codes over $\mathcal{R}_i^*$. To construct a 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 $M_i^{e_{l_i}}(x)$ 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 [7, Lemma 3] and provides a method for construction of $M_i^{e_{l_i}}(x)$, the minimal polynomials, of $\alpha_i^{e_{l_i}}$ over the ring $\mathcal{A}_i$.

*Theorem 10:* 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 $H_{\alpha_i, n_i}$, 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 $B_i^{l_i} = \{(\alpha_i^{e_{l_i}})^{p^{q_i}} : 1 \le l_i \le n_i - k_i, \ 0 \le q_i \le h_i - 1\}$.

*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 $\overline{M}_i^{e_{l_i}}(x)$ 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 $\overline{M}_i^{e_{l_i}}(x)$ (minimal polynomials of $\overline{\alpha}_i^{e_{l_i}}$) is divisible by $\overline{M}_i^{e_{l_i}}(x)$ (minimal polynomials of $\overline{\beta}_i^{e_{l_i}}$), 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, the polynomial $M_i^{e_{l_i}}(x)$ 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 $0 \le i \le t$, such that $0 \le q_i \le h_i - 1$ 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 1:* For each $i$ such that $0 \le i \le t$, it follows that the minimal polynomial $\overline{M}_i^{e_{l_i}}(x)$ 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 $\mathcal{K}_i = \mathbb{K}_i^r$.

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 [1, Theorem 2.5].

*Theorem 11:* 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 $n_i = s_i$ 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 $H_{\alpha_i, n_i}$, where $\alpha_i$ 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 [10, Corollary 3.1], it follows that each code has minimum distance $d_i$ or greater. This can be seen by examining the determinants of any $d_i - 1$ columns of matrices $M_i^*$. Let following matrix is the 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 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 unit determinant in each $\mathcal{A}_i$. Hence, no combination of $d_i - 1$ or fewer columns of each $M_i$ is linearly dependent. So, by [10, Corollary 3.1], it follows that each code has minimum distance $d_i$ or greater.

*Corollary 2:* [1, Theorem 2.5] If $g(x)$ is a generator polynomial of a 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 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 [7, Theorem 4] for the BCH bound of these codes.

### A. Algorithm

The algorithm for constructing a BCH type 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 $1 \le i \le t$, which are also irreducible over $GF(p)$, and form the chain of Galois rings

$$\begin{aligned} \mathbb{Z}_{p^m} &= GR(p^m, h_0) \subset GR(p^m, h_1) \subset \cdots \\ &\cdots \subset GR(p^m, h_{t-1}) \subset GR(p^m, h_t) \quad \text{or} \\ A &= \mathcal{R}_0 \subseteq \mathcal{R}_1 \subseteq \mathcal{R}_2 \subseteq \cdots \subseteq \mathcal{R}_{t-1} \subseteq \mathcal{R}_t = \mathcal{R} \end{aligned}$$

and its corresponding chain of residue fields is

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

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

2) Now put $\mathcal{A}_i = \mathcal{R}_i^r$, for $0 \le i \le t$ 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 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 $0 \le i \le t$.

3) Let $\overline{\eta}_i$ be the primitive element in $\mathbb{K}_i^*$, for $0 \le i \le t$. Then $\eta_i$ 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 $H_{\alpha_i, n_i}$. Assume for each $i$, where $0 \le i \le t$, $\alpha_i$ be any element of $H_{\alpha_i, n_i}$.

4) If $\alpha_i^{e_1}, \alpha_i^{e_2}, \alpha_i^{e_3}, \cdots, \alpha_i^{e_{n_i-k_i}}$ are chosen to be the roots of $g_i(X)$, then find $M_i^{e_{l_i}}(x)$ the minimal polynomials of $\alpha_i^{e_{l_i}}$, for $l_i = 1, 2, \cdots, n_i - k_i$, where each $\alpha_i^{e_{l_i}} = (\beta_i^{e_{l_i}}, \beta_i^{e_{l_i}}, \beta_i^{e_{l_i}}, \cdots, \beta_i^{e_{l_i}})$. 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 $0 \le i \le t$.

*Example 1:* 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 irreducible polynomial with degree $h = 2^2$ over $\mathbb{Z}_2$. By Theorem 3, it follows that $f(x) = x^4+x+1$ is irreducible over $A$. Let $\mathcal{R} = \frac{\mathbb{Z}_{2^2}[x]}{(f(x))} = GR(2^2, 4)$ be the Galois ring and $\mathbb{K} = \frac{\mathbb{Z}_2[x]}{(\pi(f(x)))} = GF(2^4)$ be the corresponding Galois field. The numbers 1, 2 and $2^2$ are the only divisors of 4 and therefore, say $h_1 = 1$, $h_2 = 2$, $h_3 = 2^2$. Thus there exist irreducible polynomials $f_1(x) = x^2 - x + 1, f_2(x) = f(x)$ in $\mathbb{Z}_4[x]$ with degrees $h_2 = 2$ and $h_3 = 4$ such that we can constitute the Galois rings $\mathcal{R}_i = \frac{\mathbb{Z}_{2^2}[x]}{(f_i(x))} = GR(2^2, h_i)$, where $1 \le i \le 2$. So $A = \mathcal{R}_0 \subset \mathcal{R}_1 \subset \mathcal{R}_2 = \mathcal{R}$. Again by the same argument it follows that $\mathbb{K}_i = \frac{\mathbb{Z}_2[x]}{(\pi(f_i(x)))} = GF(2^{h_i})$, where $1 \le i \le 2$. That is, $\mathbb{K}_0 = \mathbb{Z}_2$, $\mathbb{K}_1 = GF(2^2)$, $\mathbb{K}_2 = \mathbb{K} = GF(2^4)$, with $\mathbb{K}_1 \subset \mathbb{K}_2 \subset \mathbb{K}$. 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 $\overline{u}+1$ has order 15 in $\mathbb{K}_2$, and so $\overline{\beta}_2 = \overline{u}+1$. But $u+1$ has order 30 in $\mathcal{R}_2$, and so put $\beta_2 = (u+1)^2$ and get $\alpha_2 = (\beta_2, \beta_2)$ which generates $H_{\alpha_2,15}$. Also, $\overline{u}$ has order 3 in $\mathbb{K}_1$, and so $\overline{\beta}_1 = \overline{u}$. But $u$ has order 6 in $\mathcal{R}_1$, and so $\beta_1 = u^2$ and get $\alpha_1 = (\beta_1, \beta_1)$ which generates $H_{\alpha_1,3}$. Put $\beta_0 = \beta_0 = 1$ and get $\alpha_0 = (\beta_0, \beta_0)$ 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 $\mathcal{A}_0 \subset \mathcal{A}_1 \subset \mathcal{A}_2$. Then $M_0^1(x)$, $M_1^1(x)$ and $M_2^1(x)$ has as roots all distinct elements 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

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

Similarly,

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

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

$$\begin{aligned}
g_0(x) = \;& (x - 1),\\
g_1(x) = \;& (x - 1)(x - \alpha_1)(x - \alpha_1^2),\\
g_2(x) = \;& (x - \alpha_2)(x - \alpha_2^2)(x - \alpha_2^3)(x - \alpha_2^4)(x - \alpha_2^6)\\
& (x - \alpha_2^8)(x - \alpha_2^9)(x - \alpha_2^{12}),
\end{aligned}$$

which generates the cyclic BCH codes $\mathcal{C}_0$, $\mathcal{C}_1$ and $\mathcal{C}_2$ of lengths $1$, $3$ and $15$ with minimum hamming distances 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 each $i$ such that $0 \leq i \leq 2$. If we take $\beta_i$ and $\overline{\beta}_i$ as a root of generator polynomial, then we get codes over $\mathcal{R}_i$ and $\mathbb{K}_i$, respectively.

## References

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

[2] I.F. Blake, "Codes over certain rings,¨ *Inform. Contr.*, Vol. 20, pp. 396-404, 1972.

[3] I.F. Blake, "Codes over integer residue rings,¨ *Inform. Contr.*, Vol. 29, pp. 295-300, 1975.

[4] E. Spiegel, "Codes over $\mathbb{Z}_m$,¨ *Inform. Control*, Vol. 35, pp. 48-51, 1977.

[5] E. Spiegel, "Codes over $\mathbb{Z}_m$, Reviseted,¨ *Inform. Control*, Vol. 37, pp. 100-104, 1978.

[6] G.D. Forney Jr., "On decoding BCH codes,¨ *IEEE Trans. Inform. Theory*, Vol. IT-11(4), pp. 549-557, 1965.

[7] P. Shankar, "On BCH codes over arbitrary integer rings,¨ *IEEE Trans. Inform. Theory*, Vol. IT-25(4), pp. 480-483, 1979.

[8] B.R. McDonald, *Linear Algebra over commutative rings*, Marcel Dekker, New York, 1984.

[9] A.A. Andrade and R. Palazzo Jr., "A note on units of finite local rings,¨ *Rev. Mat. Estat.*, Sao Pualo, Vol. 18(2), pp. 213-222, 2000.

[10] W.W. Peterson, E.J. Weldon Jr., *Error Correcting Codes*, 2nd ed., MIT Press, Cambridge, MA, 1972.