Construction of BCH codes over certain rings

Antonio Aparecido de Andrade and Tariq Shah

***Abstract*— In this work, we present a construction technique for the generator polynomials of a sequence of BCH codes having symbols from a direct product of residue integer rings $\mathbb{Z}_{p^{m_j}}$, for $1 \leq j \leq t$. We construct a chain of unitary commutative rings $\mathcal{A}_0 \subset \mathcal{A}_1 \subset \cdots \subset \mathcal{A}_{t-1} \subset \mathcal{A}_t$, for a positive integer t, where each $\mathcal{A}_i$ is constructed by a direct product of suitable Galois rings. Corresponding the this chain there is another chain of rings $\mathcal{K}_0 \subset \mathcal{K}_1 \subset \cdots \subset \mathcal{K}_{t-1} \subset \mathcal{K}_t$ constituted through the direct product of their residue fields. Moreover, we obtain the cyclic subgroups $\mathcal{G}_{n_i}$ containing the roots of the polynomials $x^{n_i} - 1$ in the commutative rings $\mathcal{A}_i$, for $0 \leq i \leq t$. The core of the construction of these BCH codes is the factorization of the polynomials $x^{n_i} - 1$ over the cyclic subgroups $\mathcal{G}_{n_i}$, for $i = 1, 2, \cdots, t$.**

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

I. INTRODUCTION

It is well-known that linear algebraic codes having symbols from arbitrary size algebraic structures are constructed in a series of papers initiated by Blake [1], [2], and Spiegel [3], [4]. A great development, nonetheless, began by Shankar [5] who constructed a special class of algebraic codes named as Bose-Chadhuri-Hocquenghem (BCH) codes having symbols from an arbitrary finite integer ring. A further development is made by Palazzo and Interlando [6], they gives a decoding algorithm for the BCH codes having symbols from an arbitrary finite integer rings, consisting on four steps. Furthermore, Andrade and Palazzo [7] extend the study of the construction of BCH codes and constructed BCH codes having symbols from finite unitary commutative rings. Both construction techniques of [5] and [7] have been addressed from the approach of taking a cyclic subgroup of the group of units of an extension ring of a finite commutative local ring. Recently, a remarkable work was presented by the authors in [8] and [9] by constructing a sequence of BCH codes having symbols from the integer rings $\mathbb{Z}_{p^m}$ and $\prod \mathbb{Z}_{p^m}$, respectively, using the chain of maximal cyclic subgroups of the chain of multiplicative groups of units of the chain of Galois rings.

In this correspondence, we establish a construction technique of BCH codes in a sequence having symbols from a direct product of residue integer rings $\mathbb{Z}_{p^{m_j}}$, for $1 \leq j \leq r$. Additionally, we present a decoding procedure for these BCH codes. All the residue fields or Galois fields of residue integer rings $\mathbb{Z}_{p^{m_j}}$ will be same, i.e., $\mathbb{Z}_p$ or the Galois extension of $\mathbb{Z}_p$. The core of the construction of such types of BCH codes is the factorization of the polynomial $x^{n_i} - 1$ over the commutative rings $\mathcal{A}_i$ (the direct product of Galois rings $\mathcal{R}_{i,j}$). This correspondence presents a construction technique of BCH codes corresponding to the chain $\mathcal{A}_0 \subset \mathcal{A}_1 \subset \mathcal{A}_2 \subset \cdots \subset \mathcal{A}_{t-1} \subset \mathcal{A}_t = \mathcal{A}$ of commutative rings and the chain of Galois rings $A_j = \mathcal{R}_{0,j} \subset \mathcal{R}_{1,j} \subset \mathcal{R}_{2,j} \subset \cdots \subset \mathcal{R}_{t-1,j} \subset \mathcal{R}_{t,j} = \mathcal{R}_j$, for $1 \leq j \leq r$.

For $h = b^t$, where b is prime and t is a positive integer, there exist corresponding Galois rings extensions $\mathcal{R}_{i,j} = GR(p^{m_j}, h_i)$, where $0 \leq i \leq t$, $1 \leq j \leq r$ and $h_i = b^i$ (respectively, there residue field $\mathbb{K}$). For each i, j, where $0 \leq i \leq t$ and $1 \leq j \leq r$, it follows that $\mathcal{R}_{i,j}^*$ has one and only one cyclic subgroup $G_{n_{i,j}}$ of order n_i (divides $p^{h_i} - 1$) relatively prime to p (an extension in [5, Theorem 2]). Furthermore, if β^i generates a cyclic subgroup of order n_i in $\mathbb{K}_i^*$, then $\beta^{i,j}$ generates a cyclic subgroup of order $n_i d_{i,j}$ in $\mathcal{R}_{i,j}^*$, where $d_{i,j}$ are integers greater than or equal to 1, and $(\beta^{i,j})^{d_{i,j}}$ generates the cyclic subgroup $G_{n_{i,j}}$ in $\mathcal{R}_{i,j}^*$. Then by extending the given algorithm presented in [8] for constructing a BCH type codes with symbols from a direct product of $\mathbb{Z}_{p^{m_j}}$, for each member in chains of Galois rings and residue fields, respectively, we obtain BCH type codes having symbols from $\mathbb{Z}_{p^{m_j}}$. Consequently, there are two possibilities: $h_i = b^i$ for $i = 2$ or $h_i = b^i$ for $i \geq 2$. By the above information, let $\mathcal{A}_0 \subset \mathcal{A}_1 \subset \cdots \subset \mathcal{A}_{t-1} \subset \mathcal{A}_t$ be a chain of unitary commutative rings, whereas for each i, such that $0 \leq i \leq t$. Thus, each $\mathcal{A}_i$ is a 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 $1 \leq j \leq r$, is the chain of Galois rings. Corresponding to the chain $\mathcal{A}_0 \subset \mathcal{A}_1 \subset \cdots \subset \mathcal{A}_{t-1} \subset \mathcal{A}_t$, there is another chain of rings $\mathcal{K}_0 \subset \mathcal{K}_1 \subset \cdots \subset \mathcal{K}_{t-1} \subset \mathcal{K}_t$ constituted through the direct product of their residue fields, i.e.,

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

where $\mathbb{K}_0 \subset \mathbb{K}_1 \subset \cdots \subset \mathbb{K}_{t-1} \subset \mathbb{K}_t$ is a chain of corresponding residue fields.

Antonio Aparecido de Andrade, Department of Mathematics, São Paulo State University at São José do Rio Preto - SP, Brazil, E-mail: andrade@ibilce.unesp.br

Tariq Shah¸ Department of Mathematics, Quaid-i-Azam University, Islamabad, Pakistan, E-mail: stariqshah@gmail.com. This work was supported by Fapesp 2013/14783-7 and 2013/04124-6.

This work contains a construction technique of generator polynomials of BCH codes having roots from $\mathcal{A}_i^*$ and $\mathcal{K}_i^*$ for each i, where $0 \leq i \leq t$. Preliminaries II, have a brief introduction of the basics of polynomial rings and some results from [7] for the sake of quick references. Sections III and IV, describe the construction of BCH type codes over rings. Section V, concludes the whole discussion.

II. Preliminaries

Let (R, M) be 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 $\pi : R[x] \to \mathbb{K}[x]$ is defined by $\pi(\sum_{i=0}^{n} a_i x^i) = \sum_{i=0}^{n} \overline{a_i} x^i$, where $\overline{a_i} = a_i + M$ for $i = 0, \cdots, n$. Thus, the natural ring morphism $R \to \mathbb{K}$ is simply the restriction of π to the constant polynomials.

In the following we recall some definitions and results from [10] 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: [10, 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: [10, 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 α with $\pi(\alpha) = \bar{\alpha}$.

Theorem 3: [10, Theorem XIII.7] Let (R, M) be a local ring and $a(x)$ is a 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: [7, Theorem 3.3] Let $\mathcal{R} = R_1 \times R_2 \times R_3 \times \cdots \times R_r$, 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: [7, 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 α corresponds to $\beta = (\beta_1, \beta_2, \cdots, \beta_r)$, where $j = 1, 2, 3, \cdots, r$.

Theorem 6: [7, Theorem 3.5] For any positive integer l, let $M_l(x)$ be the minimal polynomial of α^l over $\mathcal{R}$, where α 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 $\{(\alpha^l)^m : m = \prod_{j=1}^{r} q_j^{s_j},\ q_j = p_j^{m_j},\ 0 \leq s_j \leq h - 1\}$.

Theorem 7: [7, 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 α 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 commutative rings

For each j such that $1 \leq j \leq r$, let p be any prime and m_j be a positive integer. Then the ring $A_j = \mathbb{Z}_{p^{m_j}}$ is a unitary finite local commutative ring with maximal ideal M_j and residue field $\mathbb{K} = \frac{A_j}{M_j} = \mathbb{Z}_p$. The natural projection $\pi_j : A_j[x] \to \mathbb{K}[x]$ 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 $A_j \to \mathbb{K}$ is simply the restrictions of π_j to the constant polynomials. 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

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

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 $h_0 = 1, h_1 = b, h_2 = b^2, \cdots, h_t = b^t = h$, it follows that, by [10, Lemma XVI.7], that 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 fields of each $\mathcal{R}_{i,j}$ becomes

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

Since each h_i divides h_{i+1} for all $0 \leq i \leq t$, it follows, by [10, Lemma XVI.7], 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 $\mathcal{K}_i = \mathbb{K}_i^r$, 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, we have a problem finding the multiplicative groups $\mathcal{A}_i^*$. With the next theorem we extend [10, 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 8: If $\mathcal{A}_i = \mathcal{R}_{i,1} \times \mathcal{R}_{i,2} \times \mathcal{R}_{i,3} \times \cdots \times \mathcal{R}_{i,r}$, where $0 \leq i \leq t$ and 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 9: 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 $\overline{\beta}_i$ 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: If 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 $0 \leq i \leq t$ and $1 \leq j \leq r$. From the extension of [5, theorem 3], it follows that $\overline{\beta}_i$ has order s_i in $\mathbb{K}_i^*$, for each i such that $0 \leq i \leq t$. Conversely, suppose that $\overline{\beta}_i$ has order s_i in $\mathbb{K}_i^*$, for each i such that $0 \leq i \leq t$. Again, it follows from the extension of [5, 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 $0 \leq i \leq t$ and $1 \leq j \leq r$. Since $\alpha_i = (\beta_{i,1}, \beta_{i,2}, \cdots, \beta_{i,r})$, for each i such that $0 \leq i \leq t$, 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 each i such that $0 \leq i \leq t$. ∎

Let $\mathcal{G}_{n_i}$ be the cyclic subgroup of $\mathcal{A}_i^*$ generated by α_i, for each i such that $0 \leq i \leq t$, i.e., $\mathcal{G}_{n_i}$ contains all the roots of $x^{n_i} - 1$ provided the condition of Theorem 9 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 $\mathcal{A}_i^*$, it necessary to choose certain elements of $\mathcal{G}_{n_i}$, where $n_i = s_i$, as the roots of generator polynomials $g_i(x)$ of the codes. So that, if $\alpha_i^{e_1}, \alpha_i^{e_2}, \alpha_i^{e_3}, \cdots, \alpha_i^{e_{n_i - k_i}}$ are all the roots of $g_i(x)$ in $\mathcal{G}_{n_i}$, we construct $g_i(x)$ as

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

where for each i such that $0 \leq i \leq t$, it follows that $M_i^{e_{l_i}}(x)$ is the minimal polynomials 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 an extension of [5, 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 $0 \leq i \leq t$.

Theorem 10: For each i such that $0 \leq i \leq t$, if $M_i^{e_{l_i}}(x)$ is the minimal polynomial of $\alpha_i^{e_{l_i}}$ over $\mathcal{A}_i$, where $\alpha_i^{e_{l_i}}$ generates $\mathcal{G}_{n_i}$, for $l_i = 1, 2, \cdots, n_i - k_i$, then $M_i^{e_{l_i}}(x) = \prod_{\xi_i \in B_i^{l_i}} (x - \xi_i)$, where $B_i^{l_i} = \{(\alpha_i^{e_{l_i}})^{m_{i,j}} : m_{i,j} = \prod_{j=1}^{r} p^{q_{i,j}},\ 1 \leq l_i \leq n_i - k_i,\ 0 \leq q_{i,j} \leq h_i - 1\}$.

Proof: Let $\overline{M}_i^{e_{l_i}}(x)$ be the projection of $M_i^{e_{l_i}}(x)$ over the field 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 $0 \leq i \leq t$ and $1 \leq l_i \leq n_i - k_i$. We can verify that each $\overline{M}_i^{e_{l_i}}(x)$ (minimal polynomials of $\overline{\alpha}_i^{e_{l_i}}$) is divisible by $\overline{M}_{i,j}^{e_{l_i}}(x)$ (minimal polynomials of $\overline{\beta}_i^{e_{l_i}}$), for $0 \leq i \leq t$ and $1 \leq l_i \leq n_i - k_i$. Thus it has, among its roots, distinct elements of the sequences $\overline{\alpha}_i^{e_{l_i}}, (\overline{\alpha}_i^{e_{l_i}})^p, (\overline{\alpha}_i^{e_{l_i}})^{p^2}, \cdots, (\overline{\alpha}_i^{e_{l_i}})^{p^{h_i - 1}}$, for $0 \leq i \leq t$ and $1 \leq l_i \leq n_i - k_i$. 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 $0 \leq i \leq t$ and $1 \leq l_i \leq n_i - k_i$. Thus the element $\xi_i = (\alpha_i^{e_{l_i}})^{p^{m_i}}$ is a root of $M_i^{e_{l_i}}(x)$, for each i such that $0 \leq i \leq t$, $0 \leq m_i \leq h_i - 1$ and $1 \leq l_i \leq n_i - k_i$. 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 $0 \leq i \leq t$, it follows that $\overline{M}_i^{e_{l_i}}(x)$ (minimal polynomials 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 theorem extended [7, Theorem 2.5].

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 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 $\mathcal{G}_{n_i}$, where α_i has order n_i. Then 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 $0 \leq i \leq t$.

Proof: For each i, where $0 \leq i \leq t$, 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 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 [11, 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 a unit in each $\mathcal{A}_i$. 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 [11, Corollary 3.1], it follows that each code has minimum distance d_i or greater. ■

We can also use the extension of [5, Theorem 4] for the BCH bound of these codes.

IV. ALGORITHM

An algorithm for construct a BCH type cyclic code 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 given by:

1) Choose irreducible polynomials $f_{i,j}(x)$ 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

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

and its corresponding chain of residue fields is

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

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 $d_{i,j}$. If $\beta_{i_j} = (\eta_{i,j})^{d_{i,j}}$. 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 $\mathcal{G}_{n_i}$. For each i, where $0 \leq i \leq t$, let α_i be an element of $\mathcal{G}_{n_i}$.
4) Let $\alpha_i^{e_1}, \alpha_i^{e_2}, \alpha_i^{e_3}, \cdots, \alpha_i^{e_{n_i-k_i}}$ be the roots of $g_i(x)$. Thus, $M_i^{e_{l_i}}(x)$ 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 least common multiple of the orders of $\alpha_i^{e_1}, \alpha_i^{e_2}, \alpha_i^{e_3}, \cdots, \alpha_i^{e_{n_i-k_i}}$, and the minimum distance of the code is greater than the largest number of consecutive integers modulo n_i in the set $E_i = \{e_1, e_2, e_3, \cdots, e_{n_i-k_i}\}$ for each i, where $0 \leq i \leq t$.

Example 1: 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 $M_2 = \{0, 2, 4, 6\}$, it follows that $\mathbb{K}_j = \frac{A_j}{M_j} \simeq \mathbb{Z}_2$ for $i = 1, 2$. The regular polynomials $f_1(x) = x^4+x+1 \in \mathbb{Z}_4[x]$ and $f_2(x) = x^4+x+1 \in \mathbb{Z}_8[x]$ are 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 [10, Theorem XIII.7], 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 $h_1 = 1$, $h_2 = 2$ 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 construct 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 $\mathcal{A}_j = \mathcal{R}_{0,j} \subset \mathcal{R}_{1,j} \subset \mathcal{R}_{2,j} = \mathcal{R}_j$, for $j = 1, 2$. Again, by the same argument, it follows that $\mathbb{K}_i = \frac{\mathbb{Z}_2[x]}{(\pi_j(f_{i,j}(x)))} = GF(2, h_i) = GF(2^{h_i})$, where $1 \leq i \leq 2$ and $1 \leq j \leq 2$. That is, $\mathbb{K}_0 = GR(2, 1) = \mathbb{Z}_2$, $\mathbb{K}_1 = GR(2, 2)$, $\mathbb{K}_2 = \mathbb{K} = GR(2, 4)$, with $\mathbb{K}_1 \subset \mathbb{K}_2 \subset \mathbb{K}$. Now, let $\mathcal{A}_i = \mathcal{R}_{i,1} \times \mathcal{R}_{i,2}$ such that $\mathcal{A}_0 \subset \mathcal{A}_1 \subset \mathcal{A}_2$, i.e.,

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

But $\mathcal{K}_i = \mathbb{K}_i \times \mathbb{K}_i$, as discuss in [8],

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

It $u = \{x\}$ in $\mathcal{R}_{i,1}$ is such that $\overline{u} = \{x\}$ in $\mathbb{K}_i$, then $\overline{u}$ has order 15 in $\mathbb{K}_2$, and therefore $\overline{\beta}_2 = \overline{u}$. But u has order 30 in $\mathcal{R}_{2,1}$ and order 60 in $\mathcal{R}_{2,2}$, so put $\beta_{2,1} = (u)^2$ and $\beta_{2,2} = 7u + 7$, and we get $\alpha_2 = (\beta_{2,1}, \beta_{2,2})$ which generate

$\mathcal{G}_{15}$. The elements of $\mathcal{G}_{15}$ are given by

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

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 we get $\alpha_1 = (\beta_{1,1}, \beta_{1,2})$ which generates $\mathcal{G}_3$. The elements of $\mathcal{G}_3$ are given by

$$\begin{aligned}
\alpha_1 &= (u+3, u+7)\\
\alpha_1^2 &= (3u, 7u)\\
\alpha_1^3 &= (1,1).
\end{aligned}$$

Put $\beta_{0,1} = \beta_{0,2} = 1$ and get $\alpha_0 = (\beta_{0,1}, \beta_{0,2})$ which generates $\mathcal{G}_1$. Choose α_i and α_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 elements in the sets $B_0^1 = \{\alpha_0\} \subset \mathcal{G}_1$, $B_1^1 = \{\alpha_1, \alpha_1^2\} \subset \mathcal{G}_3$ and $B_2^1 = \{\alpha_2, \alpha_2^2, \alpha_2^4, \alpha_2^8\} \subset \mathcal{G}_{15}$, respectively. So

$$\begin{aligned}
M_0^1(x) &= (x-\alpha_0) = (x-1)\\
M_1^1(x) &= (x-\alpha_1)(x-\alpha_1^2) = x^2+x+1\\
M_2^1(x) &= (x-\alpha_2)(x-\alpha_2^2)(x-\alpha_2^4)(x-\alpha_2^8)\\
&= x^4 + a_1x^3 + a_2x^2 + a_3x + 1.
\end{aligned}$$

Similarly,

$$\begin{aligned}
M_2^3(x) &= (x-\alpha_2^3)(x-\alpha_2^6)(x-\alpha_2^{12})(x-\alpha_2^9)\\
&= x^4+x^3+x^2+x+1.
\end{aligned}$$

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

$$\begin{aligned}
g_0(x) &= (x-1)\\
g_1(x) &= x^2+x+1\\
g_2(x) &= (x-\alpha_2)(x-\alpha_2^2)(x-\alpha_2^3)(x-\alpha_2^4)\\
&\quad (x-\alpha_2^6)(x-\alpha_2^8)(x-\alpha_2^9)(x-\alpha_2^{12})\\
&= (x^4+a_1x^3+a_2x^2+a_3x+1)\\
&\quad (x^4+x^3+x^2+x+1)\\
&= x^8 - a_3x^7 + a_3x^6 + a_2x^5 - x^4 + a_2x^3\\
&\quad -a_1x^2 + a_1x + 1,
\end{aligned}$$

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, where 1 represents $(1,1)$ and $a_1 = (0,4)$, $a_2 = (2,6)$ and $a_3 = (3,3)$. Also,

$$\overline{g}_0(x) = x+1,\ \overline{g}_1(x) = x^2+x+1 \text{and}$$

$$\overline{g}_2(x) = x^8+x^7+x^6+x^4+1,$$

generates the cyclic BCH codes $\overline{\mathcal{C}_0}$, $\overline{\mathcal{C}_1}$ and $\overline{\mathcal{C}_2}$ of lengths 1, 3 and 15 over $\mathcal{K}_i$ with minimum hamming distances at least 2, 4 and 5, respectively. Also, if we take $\beta_{i,j}$ and $\overline{\beta}_i$ as a root of generator polynomial, then we get codes over $\mathcal{R}_{i,j}$ and $\mathbb{K}_i$, respectively.

V. Conclusion

Undeterred by [5], we introduce the construction of BCH codes having symbols from the direct product of residue integer rings $\mathbb{Z}_{p^{m_j}}$, for $1 \le j \le r$. For each member in the chain of direct products of Galois rings and residue fields, respectively, we obtain respectively a BCH code over the direct products of local commutative rings $\mathcal{R}_{i,j}$ with different lengths and a BCH code over the direct products of residue fields $\mathbb{K}_{i,j} (= \mathbb{K}_i)$ with proper lengths, i.e.,

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

and

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

where $\overline{\mathcal{C}_{i,j}} = \overline{\mathcal{C}_{i,j+1}}$ for each $0 \le i \le t$ and $0 \le j \le r$. Of course, this technique provides a choice to select a most suitable BCH code $\mathcal{C}_i$ (respectively, BCH code $\overline{\mathcal{C}_i}$), where $0 \le i \le t$, with required error correction capabilities and code rate but with compromising length.

References

[1] I.F. Blake, Codes over certain rings, *Inform. Contr.*, 20, (1972), 396-404.

[2] I.F. Blake, Codes over integer residue rings, *Inform. Contr.*, 29, (1975), 295-300.

[3] E. Spiegel, Codes over $\mathbb{Z}_m$, *Inform. Control*, 35, (1977), 48-51.

[4] E. Spiegel, Codes over $\mathbb{Z}_m$, Reviseted, *Inform. Control*, 37, (1978), 100-104.

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

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

[7] A.A. Andrade and R. Palazzo Jr., Construction and decoding of BCH codes over finite rings, *Linear Algebra Applic.*, 286, (1999), 69-85.

[8] T. Shah, A. Qamar and A.A. Andrade, Constructions and decoding of a sequence of BCH codes, *Mathematical Sciences Research Journal*, 16(9), 2012, 234-250.

[9] T. Shah, A. Qamar and A.A. Andrade, Construction and decoding of BCH codes over chain of commutative rings, *Mathematical Sciences - Springer Open*, 6(51), 2012, 1-14.

[10] B.R. McDonlad, *Finite rings with identity*, Marcel Dekker, New York (1974).

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