International Journal of Applied Mathematics
Volume 25 No. 3 2012, 347-356

A NOTE ON UNITS OF FINITE LOCAL RINGS IN AN ASCENDING CHAIN

Antonio Aparecido de Andrade[1] §, Tariq Shah[2]
[1]Department of Mathematics
São Paulo State University at São José do Rio Preto
São José do Rio Preto - SP, BRAZIL
e-mail: andrade@ibilce.unesp.br
[2]Department of Mathematics
Quaid-i-Azam University
Islamabad, PAKISTAN
e-mail: stariqshah@gmail.com

Abstract: In this paper we present matrices over unitary finite commutative local rings connected through an ascending chain of containments, whose elements are units of the corresponding rings in the chain such that the McCoy ranks are the largest ones.

AMS Subject Classification: 11T71, 94A15, 14G50
Key Words: Galois ring, Galois field, BCH code, McCoy rank

1. Introduction

Let $\mathcal{A}$ be a local 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 as in the vector space over a commutative field. Though it is with restriction that an $r \times n$ generator matrix M of the module satisfies the condition that an $r \times r$ submatrix of M is nonsingular, or equivalently, has determinant unit in $\mathcal{A}$. The presence of nonsingular matrices having not necessary the unit elements is, in fact the main hurdle in working over a ring

Received: February 29, 2012

§Correspondence author

instead of a field. The notion of elementary row operations in a matrix, and is consequences, also carry over $\mathcal{A}$ with the understanding that only multiplication of a row by a unit element in $\mathcal{A}$ is permissable, as against 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 [4] of a matrix M, that is the largest integer r such that $r \times r$ submatrix of M has determinant unit in $\mathcal{A}$.

In [2], Andrade and Palazzo describe a construction technique of a matrix

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

based on the vector $\eta = (\alpha_1, \alpha_2, \cdots, \alpha_n)$ with α_i, for $1 \leq i \leq n$, are distinct units in in the 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 $\mathcal{A}$.

In this study we noticed the fact that for a finite local commutative ring $(\mathcal{A}, \mathcal{M})$ there are possibilities that either it has no any proper local subring or it has an ascending chain of local subrings. Since for any prime p and positive integer k, the ring $\mathbb{Z}_{p^k}$ is the particular case of unitary finite local commutative ring $\mathcal{A}$ and of course it does not have any of its proper local subring. Now, if $f(x) \in \mathbb{Z}_{p^k}[x]$ is a basic irreducible polynomial with degree $s = b^t$, where b is a prime and t is a positive integer, then $\frac{\mathbb{Z}_{p^k}[x]}{(f(x))} = GR(p^k, s)$ is the Galois ring extension of $\mathbb{Z}_{p^k}$ and $\frac{\mathbb{Z}_p[x]}{(f(x))} = GF(p, s) = GF(p^s)$ is the corresponding Galois field extension of $\mathbb{Z}_p$. 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 $GR(p^k, s')$ [4, Lemma XVI.7]. For the construction of a chain of Galois rings, [4, Lemma XVI.7] facilitate us as; since $1, b, b^2, \cdots, b^{t-1}, b^t$ are the only divisors of s, therefore let $s_0 = 1, s_1 = b, s_2 = b^2, \cdots, s_t = b^t = s$ and by [4, Lemma XVI.7] there exist (basic) irreducible polynomials $f_0(x), f_1(x), \cdots, f_t(x)$ with degrees $s_0, s_1, \cdots, s_t$, respectively, such that we can constitute the Galois rings $\frac{\mathbb{Z}_{p^k}[x]}{(f_i(x))} = GR(p^k, s_i)$, where $0 \leq i \leq t$. As s_i divides s_{i+1} for all $0 \leq i \leq t$, so by [4, Lemma XVI.7], there is a chain $GR(p^k, s_0) \subset GR(p^k, s_1) \subset GR(p^k, s_2) \subset \cdots \subset GR(p^k, s_t)$ of Galois rings. Again by the same argument $GF(p, s_0) \subset GF(p, s_1) \subset GF(p, s_2) \subset \cdots \subset GF(p, s_t)$ is the respective chain of Galois fields. Other examples of finite local

commutative rings may also be considered in strengthening the argument, for instance the local ring $\mathbb{Z}_2[i]$ consisting on four elements and hence a copy of the local ring $\mathbb{Z}_4$.

In this study we assume that $(\mathcal{A}_0, \mathcal{M}_0) \subseteq (\mathcal{A}_1, \mathcal{M}_1) \subseteq \cdots \subseteq (\mathcal{A}_{t-1}, \mathcal{M}_{t-1}) \subseteq (\mathcal{A}_t, \mathcal{M}_t) = (\mathcal{A}, \mathcal{M})$, where t is a positive integer, is a chain of local rings with corresponding multiplicative groups $\mathcal{A}_i^*$ of units, where $0 \leq i \leq t$. Now, this study extend the work contained in [2] with a construction technique of a matrix

$$M_i = \begin{bmatrix} \alpha_{i1} & \alpha_{i2} & \cdots & \alpha_{in_i} \\ \alpha_{i1}^2 & \alpha_{i2}^2 & \cdots & \alpha_{in_i}^2 \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_{i1}^{k_i} & \alpha_{i2}^{k_i} & \cdots & \alpha_{in_i}^{k_i} \end{bmatrix} \tag{2}$$

based on the vector $\eta_i = (\alpha_{i1}, \alpha_{i2}, \cdots, \alpha_{in_i})$, with α_{ib}, for $1 \leq b \leq n_i$, are distinct units in the ring $\mathcal{A}_i$ such that $1 - \alpha_{ij}$, for $1 \leq j \leq l_j$, for each i, where $0 \leq i \leq t$, are units. By this, one can obtain the McCoy rank of the matrices M_i, where $0 \leq i \leq t$. However the findings of these type of units is linked with the multiplicative group $\mathcal{A}_i^*$ of units of the ring $\mathcal{A}_i$, where $0 \leq i \leq t$.

2. Preliminaries

We start by giving a brief introduction of essentials of polynomial rings which are necessary for proceeding this study. All rings are supposed to be commutative possessing an identity element 1.

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

In the following we recall some definitions and results from [4] for the sake of quick reference.

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

1. *$a(x)$ is unit if there exists a polynomial $b(x) \in \mathcal{A}[x]$ such that $a(x)b(x) = 1$.*
2. *$a(x) \neq 0$ is zero divisor if there exists a polynomial $b(x) \in \mathcal{A}[x] \backslash \{0\}$ 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. (see [4, Theorem XIII.2]) *Let $(\mathcal{A}, \mathcal{M})$ be a local ring and $a(x) = \sum_{i=0}^{n} a_i x^i \in \mathcal{A}[x]$. The following assertions are equivalent:*

1. *$a(x)$ is regular.*

2. *$< a_1, a_2, \cdots, a_n >= \mathcal{A}$.*

3. *a_i is a unit for some i, for $0 \leq i \leq n$.*

4. *$\pi(a(x)) \neq 0$.*

Theorem 2. (see [4, Theorem XV.1]) *Let $(\mathcal{A}, \mathcal{M})$ be a local ring and $a(x)$ be a regular polynomial in $\mathcal{A}[x]$ such that $\pi(a(x))$ has a simple (i. e., non multiple) zero $\bar{\alpha}$ in $\mathbb{K}$. Then $a(x)$ has one and only one zero α with $\pi(\alpha) = \bar{\alpha}$.*

Theorem 3. (see [4, Theorem XIII.7]) *Let $(\mathcal{A}, \mathcal{M})$ be a local ring and $a(x)$ is regular polynomial in $\mathcal{A}[x]$ such that $\pi(a(x))$ is irreducible in $\mathbb{K}[x]$. Then $a(x)$ is irreducible in $\mathcal{A}[x]$.*

3. Chain of Finite Local Rings and McCoy Ranks

For a finite local commutative ring $(\mathcal{A}, \mathcal{M})$ there are possibilities that either it is local having no proper local subring or it has an ascending chain of local subrings. In this study we assume $(\mathcal{A}_0, \mathcal{M}_0) \subseteq (\mathcal{A}_1, \mathcal{M}_1) \subseteq \cdots \subseteq (\mathcal{A}_{t-1}, \mathcal{M}_{t-1}) \subseteq (\mathcal{A}_t, \mathcal{M}_t) = (\mathcal{A}, \mathcal{M})$, where t is a positive integer, be the chain of local rings with corresponding multiplicative group of units of $\mathcal{A}_i^*$, where $0 \leq i \leq t$. It follows that $\mathcal{A}_i^*$ is an Abelian group for each i, where $0 \leq i \leq t$, and therefore it can be expressed as a direct product of cyclic groups. We are interested in the maximal cyclic subgroup of $\mathcal{A}_i^*$ for each i, where $0 \leq i \leq t$, hereafter denoted by G_{s_i}, whose elements are the roots of $X^{s_i} - 1$ for some positive integer s_i such that $gcd(p, s_i) = 1$. We also assume that corresponding residue fields are $\mathbb{K}_i = \frac{\mathcal{A}_i}{\mathcal{M}_i} \cong GF(p^{m_i})$, where p is a prime integer, $m_i \in \mathbb{Z}^+$ and $0 \leq i \leq t$.

The following theorem is a direct consequence of [4, Theorem XVIII.2].

Theorem 4. (see [2, Theorem 4]) *There is only one maximal cyclic subgroup of $\mathcal{A}^*$ having order $s = p^m - 1$, which is relatively prime to p.*

The following extends [2, Theorem 4] and it follows by Theorem 4.

Theorem 5. *Let*

$$(\mathcal{A}_0, \mathcal{M}_0) \subseteq (\mathcal{A}_1, \mathcal{M}_1) \subseteq \cdots \subseteq (\mathcal{A}_{t-1}, \mathcal{M}_{t-1}) \subseteq (\mathcal{A}_t, \mathcal{M}_t) = (\mathcal{A}, \mathcal{M}),$$

where t is a positive integer, be a chain of local rings with corresponding multiplicative groups of units $\mathcal{A}_i^*$, where $0 \leq i \leq t$. Then there is only one maximal cyclic subgroup G_{s_i} of $\mathcal{A}_i^*$ with order $s_i = p^{m_i} - 1$, relatively prime to p, for each i, where $0 \leq i \leq t$.

The next two theorems provide a base for the construction of G_s and indicate a method for generating this cyclic subgroup.

Theorem 6. (see [2, Theorem 5]) *Suppose that α generates a cyclic subgroup of order s (divisor of $p^m - 1$) in $\mathcal{A}^*$. Then $x^s - 1$ can be factored as $x^s - 1 = (x - \alpha)(x - \alpha^2) \cdots (x - \alpha^s)$ if and only if with $\bar{\alpha}$ has order s in $\mathbb{K}^*$.*

The following extends [2, Theorem 5].

Theorem 7. *Let*

$$(\mathcal{A}_0, \mathcal{M}_0) \subseteq (\mathcal{A}_1, \mathcal{M}_1) \subseteq \cdots \subseteq (\mathcal{A}_{t-1}, \mathcal{M}_{t-1}) \subseteq (\mathcal{A}_t, \mathcal{M}_t) = (\mathcal{A}, \mathcal{M}),$$

where t is a positive integer, be a chain of local rings with corresponding multiplicative groups of units $\mathcal{A}_i^*$, where $0 \leq i \leq t$. Suppose that α_i generates a cyclic subgroup of order s_i (divisor of $p^{m_i} - 1$) in $\mathcal{A}_i^*$ for each i, where $0 \leq i \leq t$. Then $x^{s_i} - 1$ can be factored as $x^{s_i} - 1 = (x - \alpha_i)(x - \alpha_i^2) \cdots (x - \alpha_i^{s_i})$ if and only if with $\bar{\alpha}_i$ has order s_i, in $\mathbb{K}_i^*$ for each i, where $0 \leq i \leq t$.

Corollary 1. (see [2, Corollary 1]) *If $h(x)$ divides $x^s - 1$ and has coefficients in $\mathcal{A}$, then $h(x)$ can be factored over G_s as $h(x) = (x - \alpha^{e_1})(x - \alpha^{e_2}) \cdots (x - \alpha^{e_l})$ if and only if $\bar{h}(x)$ can be factored as $\bar{h}(x) = (x - \bar{\alpha}^{e_1})(x - \bar{\alpha}^{e_2}) \cdots (x - \bar{\alpha}^{e_l})$ over the field $\mathbb{K}$.*

Any polynomial $h_i(x)$ which is a divisor of $x^{s_i} - 1$, where $0 \leq i \leq t$, can be factored uniquely over $\mathbb{K}_i^*$. It follows from above Theorem 7 that the

factorization of $h_i(x)$ over G_{s_i} for each i, where $0 \leq i \leq t$, is also unique. This is stated in the following corollary.

The following extends [2, Corollary 1].

Corollary 2. *Let*

$$(\mathcal{A}_0, \mathcal{M}_0) \subseteq (\mathcal{A}_1, \mathcal{M}_1) \subseteq \cdots \subseteq (\mathcal{A}_{t-1}, \mathcal{M}_{t-1}) \subseteq (\mathcal{A}_t, \mathcal{M}_t) = (\mathcal{A}, \mathcal{M}),$$

where t is a positive integer, be a chain of local rings with corresponding multiplicative groups of units $\mathcal{A}_i^*$, where $0 \leq i \leq t$. Let $h_i(x)$ divides $x^{s_i} - 1$ and has coefficients in $\mathcal{A}_i$ can be factored over G_{s_i} as $h_i(x) = (x - \alpha_i^{e_1})(x - \alpha_i^{e_2}) \cdots (x - \alpha_i^{e_l})$ if and only if $\bar{h}_i(x)$ can be factored as $\bar{h}_i(x) = (x - \bar{\alpha}_i^{e_1})(x - \bar{\alpha}_i^{e_2}) \cdots (x - \bar{\alpha}_i^{e_l})$ over the field $\mathbb{K}_i$ for each i, where $0 \leq i \leq t$.

Theorem 8. (see [2, Theorem 6]) *Suppose $\bar{\alpha}$ generates a cyclic subgroup of order s (divisor of $p^m - 1$) in $\mathbb{K}^*$. Then α generates a cyclic subgroup of order sd in $\mathcal{A}^*$, where $d \in \mathbb{Z}^+$ and α generates the cyclic subgroup G_s of $\mathcal{A}^*$.*

Theorem 9. (see [2, Theorem 7]) *Let α be an element of G_s of order s. Then the differences $\alpha^{l_1} - \alpha^{l_2}$ are units in $\mathcal{A}$ if $0 \leq l_1 \neq l_2 \leq s - 1$.*

The following extend [2, Theorem 6].

Theorem 10. *Let*

$$(\mathcal{A}_0, \mathcal{M}_0) \subseteq (\mathcal{A}_1, \mathcal{M}_1) \subseteq \cdots \subseteq (\mathcal{A}_{t-1}, \mathcal{M}_{t-1}) \subseteq (\mathcal{A}_t, \mathcal{M}_t) = (\mathcal{A}, \mathcal{M}),$$

where t is a positive integer, be a chain of local rings with corresponding multiplicative groups of units $\mathcal{A}_i^*$, where $0 \leq i \leq t$. Suppose $\bar{\alpha}_i$ generates a cyclic subgroup of order s_i (divisor of $p^{m_i} - 1$) in $\mathbb{K}_i^*$. Then α_i generates a cyclic subgroup of order $s_i d_i$ in $\mathcal{A}_i^*$, where $d_i \in \mathbb{Z}^+$ and α_i generates the cyclic subgroup G_{s_i} of $\mathcal{A}_i^*$ for each i, where $0 \leq i \leq t$.

The following generalizes [2, Theorem 7].

Theorem 11. *Let $(\mathcal{A}_0, \mathcal{M}_0) \subseteq (\mathcal{A}_1, \mathcal{M}_1) \subseteq \cdots \subseteq (\mathcal{A}_{t-1}, \mathcal{M}_{t-1}) \subseteq (\mathcal{A}_t, \mathcal{M}_t) = (\mathcal{A}, \mathcal{M})$, where t is a positive integer, be a chain of local rings with corresponding multiplicative groups of units $\mathcal{A}_i^*$, where $0 \leq i \leq t$. Let α_i be an element of G_{s_i} of order s_i. Then the differences $\alpha_i^{l_{i_1}} - \alpha_i^{l_{i_2}}$ are units in $\mathcal{A}_i$ if $0 \leq l_{i_1} \neq l_{i_2} \leq s_i - 1$ for each i, where $0 \leq i \leq t$.*

By Theorem 11, for each i, where $0 \leq i \leq t$, we obtained that the McCoy rank of the matrix M_i in Equation (2), where $\eta_i = (\alpha_{i1}, \alpha_{i2}, \cdots, \alpha_{in})$ and its power generate the rows of M_i, which is $r_i = \min\{m, n\}$, as any $r_i \times r_i$ submatrix of M_i is Vandermonde.

Example 1. *Let $(\mathcal{A}_0, \mathcal{M}_0) \subseteq (\mathcal{A}_1, \mathcal{M}_1)$ be a chain of local rings with corresponding multiplicative groups of units $\mathcal{A}_i^*$, for $i = 0, 1$, where $A_1 = \mathbb{Z}_{5^2}$ and $A_2 = \mathbb{Z}_{5^3}$. Thus, $\mathcal{A}_0^*$ has only one maximal cyclic subgroup, whose order is 4, which we denote it by G_0, and $\mathcal{A}_1^*$ has only one maximal cyclic subgroup, whose order is 4, which we denote it by G_1. The elements $\alpha = 7 \in A_0$ and $\beta = 57 \in A_1$ have order 4 and generate G_0 and G_1, respectively. Letting $\eta_0 = (\alpha^2, \alpha, \alpha^3)$, $\eta_1 = (\beta, \beta^3, \beta^2)$ and $m = 2$, the matrices*

$$M_0 = \begin{bmatrix} \alpha^2 & \alpha & \alpha^3 \\ 1 & \alpha^2 & \alpha^2 \end{bmatrix} \quad \text{and} \quad M_1 = \begin{bmatrix} \beta & \beta^3 & \beta^2 \\ \beta^2 & \beta^2 & 1 \end{bmatrix}$$

have McCoy ranks equal to 2.

4. Applications

Linear codes over finite rings had been discussed in a series of papers initiated by Blake [8], [9], and Spiegel [5], [6]. The more notable development, nevertheless, began by Forney et al. [7] or Hammons et al. [3], and stated a method for some non linear binary codes with good error correcting capabilities, and can be viewed, through a Gray map, as linear codes over $\mathbb{Z}_4$. However, the structure of the multiplicative group of unit elements of certain local finite rings have recently raised a great interest for their successful application in algebraic coding theory. Shankar [10] has constructed BCH codes over finite rings $\mathbb{Z}_m$, where m is a positive integer. Andrade and Palazzo [1] have further constructed BCH codes over finite commutative rings with identity. Both construction techniques have been addressed from the point of view of specifying a cyclic subgroup of the group of units of an extension ring of finite rings. The core of the problem is the factorization of $x^s - 1$ over the group of units of the appropriate extension ring.

In this section, we present an application involving the multiplicative group $\mathcal{R}_i^*$ in coding theory. With the assumption that $(\mathcal{A}_0, \mathcal{M}_0) \subseteq (\mathcal{A}_1, \mathcal{M}_1) \subseteq \cdots \subseteq (\mathcal{A}_{t-1}, \mathcal{M}_{t-1}) \subseteq (\mathcal{A}_t, \mathcal{M}_t) = (\mathcal{A}, \mathcal{M})$, where t is a positive integer, is a chain of

local rings with corresponding multiplicative groups of units $\mathcal{A}_i^*$, where $0 \leq i \leq t$.

First we establish some notation. If $f_i(x)$ is a monic polynomial of degree h_i in $\mathcal{A}_i[x]$ such that $\pi_i(f_i(x))$ is irreducible in $\mathbb{K}_i[x]$, it follows that $f_i(x)$ is also irreducible in $\mathcal{A}_i[x]$, by [4, Theorem XIII.7]. The ring $\mathcal{R}_i$ is a finite commutative local factor ring of a monoid ring whose maximal ideal is $\mathcal{M}_{i2} = \frac{\mathcal{M}_{i1}}{(f_i(x))}$, where $\mathcal{M}_{i1} = (\mathcal{M}_i, f_i(x))$ and the residue field $\mathbb{K}_{i1} = \frac{\mathcal{R}_i}{\mathcal{M}_{i2}} \simeq \frac{\mathcal{A}_i[x]}{(\mathcal{M}_i, f_i(x))} \simeq \frac{\mathbb{K}_i[x]}{(\pi_i(f_i(x)))} \simeq GF(p^{m_i h_i})$, and $\mathbb{K}_{i1}^*$ is the multiplicative group of $\mathbb{K}_{i1}$ whose order is $s_i = p^{m_i h_i} - 1$ for each i, where $0 \leq i \leq t$.

Now, let $\mathcal{R}_i^*$ denotes the multiplicative group of units of $\mathcal{R}_i$ for each i, where $0 \leq i \leq t$. It follows that $\mathcal{R}_i^*$ is an Abelian group, and therefore it can be expressed as a direct product of cyclic groups for each i, where $0 \leq i \leq t$. We are interested in the maximal cyclic subgroup of $\mathcal{R}_i^*$, hereafter denoted by G_{s_i}, whose elements are the roots of $X^{s_i} - 1$ for some positive integer s_i such that $gcd(p, s_i) = 1$. There is only one maximal cyclic subgroup of $\mathcal{R}_i^*$ having order s_i for each i, where $0 \leq i \leq t$, see [4, Theorem XVIII.2].

Definition 2. *A shortened BCH code $C(n_i, \eta_i)$ over B of length $n_i \leq s_i$ for each i, where $0 \leq i \leq t$, has parity check matrix*

$$H_i = \begin{bmatrix} \alpha_{i1} & \alpha_{i2} & \cdots & \alpha_{in} \\ \alpha_{i1}^2 & \alpha_{i2}^2 & \cdots & \alpha_{in}^2 \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_{i1}^{2a_i} & \alpha_{i2}^{2a_i} & \cdots & \alpha_{in}^{2a_i} \end{bmatrix}$$

for some $a_i \geq 1$, where $\eta_i = (\alpha_{i1}, \alpha_{i2}, \cdots, \alpha_{in})$ is the locator vector, consisting of distinct elements of G_{s_i}. The code $C(n_i, \eta_i)$, with $n_i = s_i$, will be known as a BCH code. In this case η_i is unique up to permutation of coordinates.

Thus a codeword $c_i = (c_{i1}, c_{i2}, \cdots, c_{in_i}) \in \mathcal{A}_i$ is in $C(n_i, \eta_i)$ if and only if it satisfies the following parity-check equations over $\mathcal{R}_i$ for each i, where $0 \leq i \leq t$,

$$\sum_{j=1}^{n_i} c_i \alpha_i^l j = 0, \quad \text{for} \quad l = 1, 2, \cdots, 2a_i. \tag{3}$$

For $l \geq 1$, each parity-check equation in Equation (3) translates into h_i equations over the ring $\mathcal{A}_i$ for each i, where $0 \leq i \leq t$. A parity-check matrix H_i with elements over $\mathcal{A}_i$ can be obtained by replacing each element of H_i by the corresponding column vector of length h_i over $\mathcal{A}_i$. It is possible to obtain

an estimate of d (minimum hamming distance) directly from the parity-check matrix.

Theorem 12. (see [2, Theorem 8]) *The minimum Hamming distance d of a BCH code $C(n,\eta)$ is $d \geq 2a+1$, i.e., this code correct up to a errors.*

Theorem 13. *Let $(\mathcal{A}_0,\mathcal{M}_0) \subseteq (\mathcal{A}_1,\mathcal{M}_1) \subseteq \cdots \subseteq (\mathcal{A}_{t-1},\mathcal{M}_{t-1}) \subseteq (\mathcal{A}_t,\mathcal{M}_t) = (\mathcal{A},\mathcal{M})$, where t is a positive integer, be a chain of local rings with corresponding multiplicative groups of units $\mathcal{A}_i^*$, where $0 \leq i \leq t$. The minimum Hamming distance d_i of a BCH code $C(n_i,\eta_i)$ is $d_i \geq 2a_i+1$, i.e., this code correct up to a_i errors for each i, where $0 \leq i \leq t$.*

Proof. Follows by [2, Theorem 8]. □

Example 2. *Let $(\mathcal{A}_0 = \mathbb{Z}_2[i],\mathcal{M}_0) \subseteq (\mathcal{A}_1 = \mathbb{Z}_4[i],\mathcal{M}_1)$ be a chain of local rings with corresponding residue fields $\mathbb{K}_0 = \frac{\mathbb{Z}_2[i]}{\mathcal{M}_0} \simeq \mathbb{Z}_2$ and $\mathbb{K}_1 = \frac{\mathbb{Z}_4[i]}{\mathcal{M}_1} \simeq \mathbb{Z}_2$, respectively. The polynomial $f(x) = x^3+x+1 \in \mathcal{A}_0[x]$ (in $\mathcal{A}_1[x]$) is such that $\mu(f(x))$ is irreducible over $\mathbb{Z}_2$. By Theorem 3, $f(x)$ is irreducible over A_i, for $i = 0,1$. Next, construct the rings $\mathcal{R}_0 = \frac{\mathcal{A}_0[x]}{<f(x)>}$ and $\mathcal{R}_1 = \frac{\mathcal{A}_0[x]}{<f(x)>}$, and its residue fields $\mathbb{K}_{00} = \frac{\mathbb{K}_0[x]}{<\mu(f(x))>}$ and $\mathbb{K}_{11} = \frac{\mathbb{K}_1[x]}{<\mu(f(x))>}$, whose order is $2^3 = 8$. By Theorem 5, $\mathcal{R}_i^*$, for $i = 0,1$ has only maximal cyclic subgroup whose order is $2^3-1 = 7$, denoted by G_{s_i}, for $i = 0,1$. But the elements α and β such that $f(\alpha) = f(\beta) = 0$ have orders 7 in $\mathcal{R}_i^*$, for $i = 0,1$. Letting $\eta_0 = (\alpha,\alpha^3,\alpha^2,\alpha^5)$, $\eta_1 = (\beta^2,\beta,\beta^3,\beta^4)$ and $a_i = 1$, for $i = 0,1$, the matrices M_i, for $i = 0,1$ are given by*

$$M_0 = \begin{bmatrix} \alpha & \alpha^3 & \alpha^2 & \alpha^5 \\ \alpha^2 & \alpha^6 & \alpha^4 & \alpha^3 \end{bmatrix} \quad \text{and} \quad M_1 = \begin{bmatrix} \beta^2 & \beta & \beta^3 & \beta^4 \\ \beta^4 & \beta^2 & \beta^6 & \beta \end{bmatrix}$$

have McCoy ranks equal to 2. Therefore, M_i, for $i = 0,1$, is the parity-check matrix of a shortened BCH code of length 4 over the ring $\mathcal{A}_i$, for $i = 0,1$, such that its minimum Hamming distance is 3. Thus, these codes corrects all errors of Hamming weight 1.

Acknowledgments

Acknowledgments are due to FAPESP by financial support, 2007/56052-8 and 2011/03441-2.

References

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

[2] A.A. Andrade, R. Palazzo Jr., A note on units of finite local rings, *Rev., Mat. Estat., São Paulo*, **18**, No. 2 (2000), 213-222.

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

[4] B.R. McDonlad, *Finite Rings with Identity*, Marcel Dekker, New York (1974).

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

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

[7] G.D. Forney Jr., On decoding BCH codes, *IEEE Trans. Inform. Theory*, **IT-11**, No. 4 (1965), 549-557.

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

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

[10] P. Shankar, On BCH codes over arbitrary integer rings, *IEEE Trans. Inform. Theory*, **IT-25**, No. 4 (1979), 480-483.