Ascending chains of monoid and encoding

Antonio Aparecido de Andrade and Tariq Shah

***Abstract*— Let B be any fixed finite commutative ring with identity and $k \geq 0$ is an integer. For any prime p there are the ascending chains $B[X;\mathbb{Z}_0] \subset B[X;\frac{1}{p}\mathbb{Z}_0] \subset B[X;\frac{1}{2p}\mathbb{Z}_0] \subset \cdots \subset B[X;\frac{1}{kp}\mathbb{Z}_0] \subset \cdots$ of commutative monoid rings, where $\mathbb{Z}_0 \subset \frac{1}{p}\mathbb{Z}_0 \subset \frac{1}{2p}\mathbb{Z}_0 \subset \cdots \subset \frac{1}{kp}\mathbb{Z}_0 \subset \cdots$ are the ascending chains of cyclic monoids. We established the construction technique of cyclic codes through the monoid ring $B[X;\frac{1}{kp}\mathbb{Z}_0]$ instead of a polynomial ring. Moreover we independently considered BCH, alternant, Goppa, Srivastava codes through a monoid ring $B[X;\frac{1}{kp}\mathbb{Z}_0]$, where we improved several results of [1] in more broader sense.**

***Keywords*— Monoid ring, cyclic code, BCH code, alternant code, Goppa code, Srivastava code.**

I. Introduction

The finite commutative rings are of most interest in commutative algebra due to their applications. An ideal in a commutative ring plays an essential role for its application and it is often important to know when an ideal in a ring is singly generated or principal. A useful class of rings in this perspective is the polynomial rings in one indeterminate with coefficients from a finite field, that is, Euclidean domains and hence a principal ideal domains. The coding for error control has vital role in high speed digital computers and in the design of modern communication systems. Most of the classical error-correcting codes are ideals in finite commutative rings, especially in factor rings of Euclidean domains of polynomials and group rings, that is cyclic codes are principal ideals in the quotient ring $\mathbb{F}_q[X]/(X^n-1)$, where $\mathbb{F}_q$ is finite Galois field and (X^n-1) is non prime ideal generated by the polynomial X^n-1 in $\mathbb{F}_q[X]$.

Cazaran and Kelarev [2] have given necessary and sufficient conditions for an ideal to be the principal; further they described all finite factor rings $\mathbb{Z}_m[X_1,\cdots,X_n]/I$, where I is an ideal generated by an univariate polynomial, which are commutative principal ideal rings. But in [3], Cazaran and Kelarev characterize the certain finite commutative rings as a principal ideal rings. Though, the extension of a BCH code C embedded in a semigroup ring $\mathbb{F}[S]$, where S is a finite semigroup, was considered in 2006 by Cazaran et al. [4], where an algorithm was given for computing the weights of extensions for these codes embedded in semigroup rings as ideals. Kelarev [5] provides the information relating various ring constructions and about polynomial codes, where in Sections 9.1 and 9.2 which are very closely related to semigroup rings, devoted for error-correcting codes in ring constructions. Section 9.1 is dealing error-correcting cyclic codes of length n which are ideals in group ring $\mathbb{F}[G]$ with $\mathbb{F}$ a field and G a finite torsion group of order n. Another work concerning extensions of BCH codes in various ring constructions has been given by Kelarev in [6] and [7], where the results can also be considered as the special cases of particular type of semigroup rings.

A. A. Andrade and R. Palazzo Jr. [1] discussed the cyclic, BCH, alternant, Goppa and Srivastava codes through the polynomial ring $B[X;\mathbb{Z}_0]$, where B is any finite commutative ring with identity. In this study, we introduce the construction techniques of these codes through monoid ring $B[X;\frac{1}{kp}\mathbb{Z}_0]$, where p is any prime integer and $k \geq 1$, instead of a polynomial ring $B[X;\mathbb{Z}_0]$ as considered in [1]. In fact corresponding to the family $\mathbb{Z}_0 \subset \frac{1}{p}\mathbb{Z}_0 \subset \cdots \subset \frac{1}{(k-1)p}\mathbb{Z}_0 \subset \frac{1}{kp}\mathbb{Z}_0 \subset \cdots$, where p is any prime integer and $k \geq 1$, of ascending chains of cyclic monoids there is a family of ascending chains $B[X;\mathbb{Z}_0] \subset B[X;\frac{1}{p}\mathbb{Z}_0] \subset \cdots \subset B[X;\frac{1}{(k-1)p}\mathbb{Z}_0] \subset B[X;\frac{1}{kp}\mathbb{Z}_0] \subset \cdots$ of commutative monoid rings.

The procedure used in this study for constructing linear codes through the monoid ring $B[X;\frac{1}{kp}\mathbb{Z}_0]$ is simple like polynomial's set up and technique adopted here is quite different to the embedding of linear polynomial codes in a semigroup ring or in a group algebra, which has been considered by many authors.

II. Preliminaries

Let $(B,+,\cdot)$ be an associative (commutative) ring and $(S,*)$ is a semigroup. The set SB of all finitely nonzero functions a from S into B forms a ring with respect to binary operations addition and multiplication defined as $(a+b)(s) = a(s) + b(s)$ and $(ab)(s) = \sum_{t*u=s} a(t)b(u)$, whereas the symbol $\sum_{t*u=s}$ shows the sum, taken over all pairs (t,u) of elements of S with $t*u=s$ and it is understood that if s is not expressible in the form $t*u$ for any $t,\ u \in S$, then $(ab)(s)=0$. The set SB is known as semigroup ring of S over B. If S is a monoid, then SB is called monoid ring. The semigroup ring SB is represented as $B[S]$ whenever S is a multiplicative semigroup and its elements are written either as $\sum_{s\in S} a(s)s$ or as $\sum_{i=1}^{n} a(s_i)s_i$. The SB has representation $B[X;S]$ whenever S is an additive semigroup. Since there is an isomorphism between additive semigroup S and multiplicative semigroup $\{X^s : s \in S\}$, it follows that a nonzero element f of $B[X;S]$ is uniquely represented in the canonical form $\sum_{i=1}^{n} a(s_i)X^{s_i} = \sum_{i=1}^{n} a_i X^{s_i}$, where $a_i \neq 0$ and $s_i \neq s_j$ for $i \neq j$ [8].

The order and degree of an element of a semigroup ring are not generally defined but if S is a totally ordered semigroup,

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¸ Departament 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.

the degree and the order of an element of $B[X;S]$ is defined in the following manner: if $a=\sum_{i=1}^{n} a_i X^{s_i}$ is the canonical form of the nonzero element $a \in B[X;S]$, where $s_1 < s_2 < \cdots < s_n$, then s_n is the degree of a and written as $deg(a)=s_n$ and similarly the order of a is written as $ord(a)=s_1$. Now, if R is an integral domain, then for $f,g \in B[X;S]$, it follows that $deg(ab)=deg(a)+deg(b)$ and $ord(ab)=ord(a)+ord(b)$.

If S is $\mathbb{Z}_0$, the additive monoid of non negative integers and B is an associative commutative ring, the semigroup ring is simply the polynomial ring $B[X]$. It can be observed that $B[X]=B[X;\mathbb{Z}_0] \subset B[X;\frac{1}{kp}\mathbb{Z}_0]$. Furthermore, as $\frac{1}{kp}\mathbb{Z}_0$ is an ordered monoid, it follows that we can define the degree of elements in $B[X;\frac{1}{kp}\mathbb{Z}_0]$.

In this study initially we replaced the construction technique of cyclic codes by a monoid ring $B[X;\frac{1}{kp}\mathbb{Z}_0]$, where p is any prime integer and $k \geq 0$, instead of a polynomial ring. After it we independently considered BCH, alternant, Goppa, Srivastava codes and by this new way of construction with utilizing the same lines as adopted in [1], where almost all the results stand as a particular case of findings of this paper. That is, in this work we take B as a finite commutative ring with unity and in the same spirit of [1], we fixed a cyclic subgroup of group of units of the factor ring $B[X;\frac{1}{kp}\mathbb{Z}_0]/((X^{\frac{1}{kp}})^{kpn}-1)$. The factorization of $X^{kpn}-1$ over the group of units of $B[X;\frac{1}{kp}\mathbb{Z}_0]/((X^{\frac{1}{kp}})^{kpn}-1)$ is again the central issue as [1]. Under consideration processes of constructing linear codes through the monoid ring $B[X;\frac{1}{kp}\mathbb{Z}_0]$ is very similar to linear codes over a finite ring.

III. Ascending chains and cyclic codes

If the ideal $I =< a >$ is principal ideal of a unitary commutative ring R, then in any factor ring $\overline{R}$ of R, the corresponding ideal $\overline{I} =< \overline{a} >$, where $\overline{a}$ is the residue class of a [9]. Hence, every factor ring of a principal ideal ring (PIR) is a PIR as well. Consequently the ring $\frac{\mathbb{F}_q[X;\mathbb{Z}_0]}{(X^n-1)}$, where q is a power of a prime, is a PIR as $\mathbb{F}_q[X;\mathbb{Z}_0]$ is an Euclidean domain [10, Theorem 8.4]. Similarly, $\Re=\frac{\mathbb{Z}_q[X;\mathbb{Z}_0]}{(X^n-1)}$ is a PIR [1].

Let B be a commutative ring with identity. For any prime integer p and $k \geq 0$, we get the following family of strict ascending chains of commutative monoid rings.

$$B[X;\mathbb{Z}_0] \subset B[X;\frac{1}{p}\mathbb{Z}_0] \subset B[X;\frac{1}{2p}\mathbb{Z}_0] \subset B[X;\frac{1}{3p}\mathbb{Z}_0] \subset \cdots$$

However, as a consequence we obtain the corresponding canonical epimorphism

$$\begin{array}{ccccccc} B[X;\mathbb{Z}_0] & \subset & B[X;\frac{1}{p}\mathbb{Z}_0] & \subset & B[X;\frac{1}{2p}\mathbb{Z}_0] & \subset & \cdots \\ \downarrow & & \downarrow & & \downarrow & & \\ \frac{B[X;\mathbb{Z}_0]}{(X^n-1)} & & \frac{B[X;\frac{1}{p}\mathbb{Z}_0]}{((X^{\frac{1}{p}})^{pn}-1)} & & \frac{B[X;\frac{1}{2p}\mathbb{Z}_0]}{((X^{\frac{1}{2p}})^{2pn}-1)} & & \end{array}$$

$$\begin{array}{ccccc} \cdots & \subset & B[X;\frac{1}{kp}\mathbb{Z}_0] & \subset & \cdots \\ & & \downarrow & & \\ & & \frac{B[X;\frac{1}{kp}\mathbb{Z}_0]}{((X^{\frac{1}{kp}})^{kpn}-1)} & & \cdots \end{array}$$

By the same argument of [1], it follows that the factor ring of Euclidean monoid domain $\frac{\mathbb{F}_q[X;\frac{1}{kp}\mathbb{Z}_0]}{((X^{\frac{1}{kp}})^{kpn}-1)}$, where q is a power of a prime and p is any fixed prime integer and $k \geq 0$, is a PIR and $\frac{\mathbb{Z}_q[X;\frac{1}{kp}\mathbb{Z}_0]}{((X^{\frac{1}{kp}})^{kpn}-1)}$ is a PIR. The homomorphic image of a PIR is again a PIR by [11, Proposition (38.4)]. By the same spirit of [1], if B is a commutative ring with identity, then $\Re=\frac{B[X;\frac{1}{kp}\mathbb{Z}_0]}{((X^{\frac{1}{kp}})^{kpn}-1)}$, where p is any prime integer and $k \geq 0$, is a finite ring by [8, Theorem 7.2].

Definition 1: A linear code C of length kpn over B is a B-submodule of the B-module of all kpn-tuples of B^{kpn}, and a linear code C over B is cyclic, if whenever $v=(v_0,v_{\frac{1}{kp}},v_{\frac{2}{kp}},\cdots,v_1,\cdots,v_{\frac{kpn-1}{kp}}) \in C$, every cyclic shift $v^{(1)}=(v_{\frac{kpn-1}{kp}},v_0,v_{\frac{1}{kp}},\cdots,v_{\frac{kpn-2}{kp}}) \in C$, with $v_i \in B$ for $0 \leq i \leq \frac{kpn-1}{kp}$.

Let $f(X^{\frac{1}{kp}}) \in B[X;\frac{1}{kp}\mathbb{Z}_0]$ be a monic generalized polynomial of degree n, then $\frac{B[X;\frac{1}{kp}\mathbb{Z}_0]}{(f(X^{\frac{1}{kp}}))}$ is the set of residue classes of generalized polynomials in $B[X;\frac{1}{kp}\mathbb{Z}_0]$ modulo the ideal $(f(X^{\frac{1}{kp}}))$ and a class can be represented as $\overline{a}(X^{\frac{1}{kp}})=\overline{a_0}+\overline{a}_{\frac{1}{kp}}X^{\frac{1}{kp}}+\cdots+\overline{a}_{\frac{kpn-1}{kp}}X^{\frac{kpn-1}{kp}}$. A principal ideal consists of all multiples of a fixed generalized polynomial $g(X^{\frac{1}{kp}})$ by elements of $\frac{B[X;\frac{1}{kp}\mathbb{Z}_0]}{(f(X^{\frac{1}{kp}}))}$, known as generator generalized polynomial of the ideal. Now, we shall prove some results which show a method of obtaining the generator generalized polynomial of a principal ideal. This method shall provide a foundation in constructing a principal ideal in $\frac{B[X;\frac{1}{kp}\mathbb{Z}_0]}{(f(X^{\frac{1}{kp}}))}$. Now, onward $\Re$ shall represent the factor ring $\frac{B[X;\frac{1}{kp}\mathbb{Z}_0]}{(f(X^{\frac{1}{kp}}))}$, whereas $\Re=\frac{B[X]}{(f(X))}$ of [1].

Theorem 1: A subset C of $\Re$ is a cyclic code if and only if C is an ideal of $\Re$.

Proof: Assume C is an ideal in $\Re_{kp}$, and hence a B-module. It is also closed under multiplication by any ring element, in particular under multiplication by $X^{\frac{1}{pk}}$. Hence C is a cyclic code. Conversely, let the subset C is a cyclic code. Then C is closed under addition and multiplication by $X^{\frac{1}{pk}}$. But then it is closed under multiplication by powers of $X^{\frac{1}{kp}}$ and linear combinations of powers of $X^{\frac{1}{pk}}$. This means, C is closed under multiplication by an arbitrary generalized polynomial. Hence, C is an ideal. ■

Lemma 1: Let I be an ideal in the ring $\Re$. If the leading coefficient of some generalized polynomial of lowest degree in I is a unit in B, then there exists a unique monic generalized polynomial of minimal degree in I.

Proof: Let $\overline{f}(X^{\frac{1}{kp}}) \in I$ with lowest degree r in I. If the leading coefficient $\overline{a}_r$ of $\overline{f}(X^{\frac{1}{kp}})$ is a unit in B, it is always possible to get a monic generalized polynomial $\overline{f}_1(X^{\frac{1}{kp}})=\overline{a_r}f(X^{\frac{1}{kp}})$ with the same degree in I. Now, if both $\overline{g}(X^{\frac{1}{kp}})$ and $\overline{f}(X^{\frac{1}{kp}})$ are monic generalized polynomials of minimal degree r in I, then the generalized polynomial $\overline{k}(X^{\frac{1}{kp}})=\overline{f}(X^{\frac{1}{kp}})-\overline{g}(X^{\frac{1}{kp}})$ is in I and has degree fewer than r. Therefore, by the choice of $\overline{f}(X^{\frac{1}{kp}})$ follows that $\overline{k}(X^{\frac{1}{kp}})=0$, and hence $\overline{f}(X^{\frac{1}{kp}})=\overline{g}(X^{\frac{1}{kp}})$. ■

Theorem 2: Let I be an ideal in the ring $\Re$. If the leading coefficient of some generalized polynomial $\overline{g}(X^{\frac{1}{kp}})$ of lowest degree in ideal I is a unit in B, then I is generated by $\overline{g}(X^{\frac{1}{kp}})$.

Proof: Let $\overline{a}(X^{\frac{1}{kp}})$ be a generalized polynomial in I. By Euclidean algorithm there are unique generalized polynomials $\overline{q}(X^{\frac{1}{kp}})$ and $\overline{r}(X^{\frac{1}{kp}})$ with $\overline{a}(X^{\frac{1}{kp}}) = \overline{q}(X^{\frac{1}{kp}})\overline{g}(X^{\frac{1}{kp}}) + \overline{r}(X^{\frac{1}{kp}})$, where $\overline{r}(X^{\frac{1}{kp}}) = 0$ or $\deg(r(X^{\frac{1}{kp}})) < \deg(g(X^{\frac{1}{kp}}))$. So clearly $\overline{r}(X^{\frac{1}{kp}}) \in I$. Hence, by the choice of $\overline{g}(X^{\frac{1}{kp}})$, it follows that $\overline{r}(X^{\frac{1}{kp}}) = 0$ and therefore, $\overline{a}(X^{\frac{1}{kp}}) = \overline{q}(X^{\frac{1}{kp}})\overline{g}(X^{\frac{1}{kp}})$. Thus I is generated by $\overline{g}(X^{\frac{1}{kp}})$. ■

Lemma 2: Let $r(X^{\frac{1}{kp}})$ be a generalized polynomial in $B[X; \frac{1}{kp}\mathbb{Z}_0]$. If $\deg(r(X^{\frac{1}{kp}})) < \deg f(X^{\frac{1}{kp}}))$ and $r(X^{\frac{1}{kp}}) \neq 0$, then $\overline{r}(X^{\frac{1}{kp}})$ is nonzero in $\Re$.

Proof: If $\overline{r}(X^{\frac{1}{kp}}) = \overline{0}$, then there is $q(X^{\frac{1}{kp}}) \neq 0$ in $B[X; \frac{1}{kp}\mathbb{Z}_0]$ such that $r(X^{\frac{1}{kp}}) = f(X^{\frac{1}{kp}})q(X^{\frac{1}{kp}})$. Since $f(X^{\frac{1}{kp}})$ is regular and $r(X^{\frac{1}{kp}}) \neq 0$ it follows that $\deg(r(X^{\frac{1}{kp}})) = \deg(f(X^{\frac{1}{kp}})) + \deg(q(X^{\frac{1}{kp}})) \geq \deg(f(X^{\frac{1}{kp}}))$, which is a contradiction. Hence $\overline{r}(X^{\frac{1}{kp}}) \neq 0$. ■

Lemma 3: Let I be an ideal in the ring $\Re$ and $g(X^{\frac{1}{kp}}) \in B[X; \frac{1}{kp}\mathbb{Z}_0]$ with leading coefficient unit in B such that $\deg(g(X^{\frac{1}{kp}})) < \deg(f(X^{\frac{1}{kp}}))$. If $\overline{g}(X^{\frac{1}{kp}}) \in I$ and has lowest degree in I, then $g(X^{\frac{1}{kp}})$ divides $f(X^{\frac{1}{kp}})$ in $B[X; \frac{1}{kp}\mathbb{Z}_0]$.

Proof: According to Euclidean algorithm for commutative rings there are unique polynomials $\overline{q}(X^{\frac{1}{kp}})$ and $\overline{r}(X^{\frac{1}{kp}})$ such that $\overline{0} = \overline{g}(X^{\frac{1}{kp}})\overline{q}(X^{\frac{1}{kp}}) + \overline{r}(X^{\frac{1}{kp}})$, where $\overline{r}(X^{\frac{1}{kp}}) = \overline{0}$ or $\deg(\overline{r}(X^{\frac{1}{kp}})) < \deg(\overline{g}(X^{\frac{1}{kp}}))$. Thus $\overline{r}(X^{\frac{1}{kp}}) = -\overline{g}(X^{\frac{1}{kp}})\overline{q}(X^{\frac{1}{kp}})$, i.e., $\overline{r}(X^{\frac{1}{kp}})$ is in I. So, it follows by the choice of $\overline{g}(X^{\frac{1}{kp}})$ that $\overline{r}(X^{\frac{1}{kp}}) = \overline{0}$. Also, by Euclidean algorithm for commutative rings, there are unique generalized polynomials $q_1(X^{\frac{1}{kp}})$ and $r_1(X^{\frac{1}{kp}})$ such that $f(X^{\frac{1}{kp}}) = g(X^{\frac{1}{kp}})q_1(X^{\frac{1}{kp}}) + r_1(X^{\frac{1}{kp}})$, where $r_1(X^{\frac{1}{kp}}) = 0$ or $\deg(r_1(X^{\frac{1}{kp}})) < \deg(g(X^{\frac{1}{kp}}))$. So $\overline{0} = \overline{g}(X^{\frac{1}{kp}})\overline{q_1}(X^{\frac{1}{kp}}) + \overline{r_1}(X^{\frac{1}{kp}}) = \overline{g}(X^{\frac{1}{kp}})\overline{q}(X^{\frac{1}{kp}}) + \overline{r}(X^{\frac{1}{kp}})$. Thus $\overline{q_1}(X^{\frac{1}{kp}}) = \overline{q}(X^{\frac{1}{kp}})$ and $\overline{r_1}(X^{\frac{1}{kp}}) = \overline{r}(X^{\frac{1}{kp}}) = \overline{0}$. By Lemma 2 it follows that $r_1(X^{\frac{1}{kp}}) = 0$ and therefore $g(X^{\frac{1}{kp}})$ divides $f(X^{\frac{1}{kp}})$. ■

Theorem 3: Let I be an ideal in the ring $\Re$. If $g(X^{\frac{1}{kp}})$ divides $f(X^{\frac{1}{kp}})$ and $\overline{g}(X^{\frac{1}{kp}}) \in I$, then $\overline{g}(X^{\frac{1}{kp}})$ has lowest degree in $(\overline{g}(X^{\frac{1}{kp}}))$.

Proof: Suppose that there is $\overline{b}(X^{\frac{1}{kp}})$ in $(\overline{g}(X^{\frac{1}{kp}}))$ such that $\deg(\overline{b}(X^{\frac{1}{kp}})) < \deg(\overline{g}(X^{\frac{1}{kp}}))$. Since $\overline{b}(X^{\frac{1}{kp}}) \in (\overline{g}(X^{\frac{1}{kp}}))$, it follows that $\overline{b}(X^{\frac{1}{kp}}) = \overline{g}(X^{\frac{1}{kp}})\overline{h}(X^{\frac{1}{kp}})$ for some $\overline{h}(X^{\frac{1}{kp}}) \in R$. Thus $b(X^{\frac{1}{kp}}) - g(X^{\frac{1}{kp}})h(X^{\frac{1}{kp}}) \in (f(X^{\frac{1}{kp}}))$, i.e., $b(X^{\frac{1}{kp}}) - g(X^{\frac{1}{kp}})h(X^{\frac{1}{kp}}) = f(X^{\frac{1}{kp}})a(X^{\frac{1}{kp}})$ for some $a(X^{\frac{1}{kp}})$ in $B[X; \frac{1}{kp}\mathbb{Z}_0]$. This gives $b(X^{\frac{1}{kp}}) = g(X^{\frac{1}{kp}})h(X^{\frac{1}{kp}}) + f(X^{\frac{1}{kp}})a(X^{\frac{1}{kp}})$. Since $g(X^{\frac{1}{kp}})$ divides $f(X^{\frac{1}{kp}})$, it follows that $g(X^{\frac{1}{kp}})$ divides $g(X^{\frac{1}{kp}})h(X^{\frac{1}{kp}}) + f(X^{\frac{1}{kp}})a(X^{\frac{1}{kp}})$, which implies that $g(X^{\frac{1}{kp}})$ divides $b(X^{\frac{1}{kp}})$, a contradiction. Hence $\overline{g}(X^{\frac{1}{kp}})$ has lowest degree in $(\overline{g}(X^{\frac{1}{kp}}))$. ■

IV. BCH AND ALTERNANT CODES

In this section, we construct BCH and alternant codes through a monoid ring instead of a polynomial ring. First we noticed the fundamental properties of Galois extension rings, which are used in the construction of these codes. Also, we assume that (B, M) is a finite unitary local commutative ring and residue field $\mathbb{K} = \frac{B}{M} \cong GF(q^m)$, where q is a prime integer, m a positive integer. The natural projection $\pi : B[X; \frac{1}{kp}\mathbb{Z}_0] \to \mathbb{K}[X; \frac{1}{kp}\mathbb{Z}_0]$ is defined by $\pi(a(X^{\frac{1}{kp}})) = \overline{a}(X^{\frac{1}{kp}})$, i.e., $\pi(\sum_{i=0}^{kpn} a_i X^{\frac{1}{kp}i}) = \sum_{i=0}^{kpn} \overline{a_i} X^{\frac{1}{kp}i}$, where $\overline{a_i} = a_i + M$ for $i = 0, \cdots, kpn$. Let $f(X^{\frac{1}{kp}})$ be a monic generalized polynomial of degree t in $B[X; \frac{1}{kp}\mathbb{Z}_0]$ such that $\pi(f(X^{\frac{1}{kp}}))$ is irreducible in $\mathbb{K}[X; \frac{1}{kp}\mathbb{Z}_0]$. Since [8, Theorem 7.2] accommodates $B[X; \frac{1}{kp}\mathbb{Z}_0]$ as $B[X]$, it follows that $f(X^{\frac{1}{kp}})$ is also irreducible in $B[X; \frac{1}{kp}\mathbb{Z}_0]$, by [12, Theorem XIII.7]. The ring $\Re$ is a finite commutative local factor ring of a monoid ring whose maximal ideal is $M_2 = \frac{M_1}{(f(X^{\frac{1}{kp}}))}$, where $M_1 = (M, f(X^{\frac{1}{kp}}))$ and the residue field $\mathbb{K}_1 = \frac{\Re}{M_2} \simeq \frac{B[X; \frac{1}{kp}\mathbb{Z}_0]}{(M, f(X^{\frac{1}{kp}}))} \simeq \frac{\mathbb{K}[X; \frac{1}{kp}\mathbb{Z}_0]}{(\pi(f(X^{\frac{1}{kp}})))} \simeq GF(q^{kpmt})$, and $\mathbb{K}_1^*$ is the multiplicative group of $\mathbb{K}_1$ whose order is $s = q^{kpmt} - 1$.

Let $U(\Re)$ denotes the multiplicative group of units of $\Re$. It follows that $U(\Re)$ is an abelian group, and therefore it can be expressed as a direct product of cyclic groups. We are interested in the maximal cyclic subgroup of $U(\Re)$, hereafter denoted by G_s, whose elements are the roots of $X^s - 1$ for some positive integer s such that $gcd(q, s) = 1$. There is only one maximal cyclic subgroup of $U(\Re)$ having order s [12, Theorem XVIII.2].

Before going ahead it must be noticed that the length n of cyclic codes (ideals in $\Re$) under consideration is depends upon $q^{kpmt} - 1$. Though for $\Re$, the length n of cyclic codes (ideals in $\Re$) is depends upon $q^{mt} - 1$, the case of [1, Definition 3.1]. Thus the integer kp have a crucial role in the length of cyclic codes. Furthermore, $\deg(h(X^{\frac{1}{kp}})) \geq \deg(h(X))$ and $\deg(g(X^{\frac{1}{kp}})) \geq \deg(g(X))$, where $k = 0, 1, 2, \cdots$.

It would be worth mentioning that McCoy rank of parity-check matrix over the ring $\Re$ is an integer r [12]. Now onward it is clear that McCoy rank of parity-check matrix over the ring $\Re$ will be kpr.

Definition 2: A shortened BCH code $C(n, \eta)$ over B of length $n \leq s$ has parity-check matrix

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

for some $r \geq 1$, where $\eta = (\alpha_1, \alpha_2, \cdots, \alpha_n)$ is the locator vector, consisting of distinct elements of G_s. The code $C(n, \eta)$, with $n = s$, will be known as a BCH code.

Lemma 4: If α is an element of G_s of order s, then the differences $\alpha^{l_1} - \alpha^{l_2}$ are units in $\Re$ for $0 \leq l_1 \neq l_2 \leq s - 1$.

Proof: The element $\alpha^{l_1} - \alpha^{l_2}$ has the representation $\alpha^{l_1}(1 - \alpha^{l_2 - l_1})$, where 1 is the identity of $\Re$. The factor α^{l_1} in the product is a unit. The second factor can be written as $1 - \alpha^k$ for some integer k in the interval $[1, s - 1]$. Now, if the elements $1 - \alpha^k$, for $1 \leq k \leq s - 1$, were not the units in $\Re$, then $1 - \alpha^k \in M_2$, and consequently $\pi(\alpha)^k = \pi(1)$ for

$k < s$, which a contradiction. Hence $1 - \alpha^k \in \Re$ are units for $1 \leq k \leq s-1$. ■

Theorem 4: The minimum Hamming distance of a BCH code $C(n, \eta)$ satisfies $d \geq kpr + 1$.

Proof: Let c be a nonzero codeword in $C(n, \eta)$ with $w_H(c) \leq kpr$. Then $cH^T = 0$. Deleting $n - kpr$ columns of the matrix H corresponding to zeros of the codeword, it follows that the new matrix is Vandermonde. It follows, by Lemma 4, that the determinant is a unit in $\Re$. Thus, the only possibility for c is the all zero codeword. ■

Definition 3: A shortened alternant code $C(n, \eta, \omega)$ of length $n \leq s$ is a code over B that has parity-check matrix

$$H = \begin{bmatrix} \omega_1 & \omega_2 & \cdots & \omega_n \\ \omega_1\alpha_1 & \omega_2\alpha_2 & \cdots & \omega_n\alpha_n \\ \omega_1\alpha_1^2 & \omega_2\alpha_2^2 & \cdots & \omega_n\alpha_n^2 \\ \vdots & \vdots & \ddots & \vdots \\ \omega_1\alpha_1^{kpr-1} & \omega_2\alpha_2^{kpr-1} & \cdots & \omega_n\alpha_n^{kpr-1} \end{bmatrix}$$
$$= \begin{bmatrix} 1 & \cdots & 1 \\ \alpha_1 & \cdots & \alpha_n \\ \vdots & \ddots & \vdots \\ \alpha_1^{kpr-1} & \cdots & \alpha_n^{kpr-1} \end{bmatrix} \begin{bmatrix} w_1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & w_n \end{bmatrix} = LD, \quad (2)$$

where r is a positive integer, $\eta = (\alpha_1, \alpha_2, \cdots, \alpha_n)$ is the locator vector, consisting of distinct elements of G_s, and $\omega = (\omega_1, \omega_2, \cdots, \omega_n)$ is an arbitrary vector consisting of elements of G_s.

Theorem 5: The alternant code $C(n, \eta, \omega)$ has minimum Hamming distance $d \geq kpr + 1$.

Proof: Suppose c is a nonzero codeword in $C(n, \eta, \omega)$ such that the weight $w_H(c) \leq kpr$. Then $cH^T = c(LD)^T = 0$. Setting $b = cD^T$, it follows that $w_H(b) = w_H(c)$ because D is diagonal and invertible. Thus, $bL^T = 0$. We obtain the new matrix H_1, the Vandermonde by deleting $n - kpr$ columns of the matrix H_1 that correspond to zeros of the codeword. It follows, by Lemma 4, that the determinant is a unit in $\Re$. Thus the only possibility for c is all zero codeword. ■

V. Goppa and Srivastava codes

Let B, $\Re$ and G_s as defined in previous section. Let $\alpha^{\frac{1}{p^k}}$ be a generator element of the cyclic group G_s, where $s = q^{kpmt} - 1$. Let $h(X) = h_0 + h_1X + h_2X^2 + \cdots + h_{pkr}X^{kpr}$ be a polynomial with coefficients in $\Re$ and $h_{kpr} \neq 0$. Let $T = \{\alpha_1, \alpha_2, \cdots, \alpha_n\}$ be a subset of distinct elements of G_s such that $h(\alpha_i)$ are units from $\Re$, for $i = 1, 2, \cdots, n$.

Definition 4: A shortened Goppa code $C(T, h)$ of length $n \leq s$ is a code over B which has parity-check matrix

$$H = \begin{bmatrix} h(\alpha_1)^{-1} & \cdots & h(\alpha_n)^{-1} \\ \alpha_1 h(\alpha_1)^{-1} & \cdots & \alpha_{kpn} h(\alpha_n) \\ \vdots & \ddots & \vdots \\ \alpha_1^{kpr-1} h(\alpha_1)^{-1} & \cdots & \alpha_n^{kpr-1} h(\alpha_n) \end{bmatrix}, \quad (3)$$

where r is a positive integer, $\eta = (\alpha_1, \alpha_2, \cdots, \alpha_n)$ is the locator vector, consisting of distinct elements of G_s, and $\omega = (h(\alpha_1)^{-1}, \cdots, h(\alpha_n)^{-1})$ is a vector consisting of elements of G_s.

Definition 5: Let $C(T, h)$ be a Goppa code.

1) If $h(X)$ is irreducible, then $C(T, h)$ is called an irreducible Goppa code.
2) If $c = (c_1, c_2, \cdots, c_n) \in C(T, h)$ and $c = (c_n, \cdots, c_2, c_1) \in C(T, h)$, then $C(T, h)$ is called a reversible Goppa code.
3) If $h(X) = (X - \alpha)^{kpr-1}$, then $C(T, h)$ is called a cumulative Goppa code.
4) If $h(X)$ has no multiple zeros, then $C(T, h)$ is called a separable Goppa code.

Remark 1: Let $C(T, h)$ be a Goppa code.

1) $C(T, h)$ is a linear code.
2) For a code with Goppa polynomial $h_l(X) = (X - \beta_l)^{kpr_l}$, where $\beta_l \in G_s$, it follows that

$$H_l = \begin{bmatrix} \frac{1}{(\alpha_1-\beta_l)^{kpr_l}} & \frac{1}{(\alpha_2-\beta_l)^{kpr_l}} & \cdots & \frac{1}{(\alpha_n-\beta_l)^{kpr_l}} \\ \frac{\alpha_1}{(\alpha_1-\beta_l)^{kpr_l}} & \frac{\alpha_2}{(\alpha_2-\beta_l)^{kpr_l}} & \cdots & \frac{\alpha_n}{(\alpha_{p^k n}-\beta_l)^{kpr_l}} \\ \vdots & \vdots & \cdots & \vdots \\ \frac{\alpha_1^{kpr_l-1}}{(\alpha_1-\beta_l)^{kpr_l}} & \frac{\alpha_2^{kpr_l-1}}{(\alpha_2-\beta_l)^{kpr_l}} & \cdots & \frac{\alpha_n^{kpr_l-1}}{(\alpha_n-\beta_l)^{kpr_l}} \end{bmatrix}$$

which is row equivalent to

$$\begin{bmatrix} (\alpha_1-\beta_l)^{-kpr_l} & \cdots & (\alpha_n-\beta_l)^{-kpr_l} \\ (\alpha_1-\beta_l)^{-(kpr_l-1)} & \cdots & (\alpha_n-\beta_l)^{-(kpr_l-1)} \\ \vdots & \cdots & \vdots \\ (\alpha_1-\beta_l)^{-1} & \cdots & (\alpha_n-\beta_l)^{-1} \end{bmatrix}.$$

As a consequence if $h(X) = (X - \beta_l)^{kpr_l} = \prod_{l=1}^{kpr} h_l(X)$, then the Goppa code is the intersection of the codes with $h_l(X) = (X - \beta_l)^{kpr_l}$, for $l = 1, 2, \cdots, kpr$, and hence it has the parity-check matrix

$$H = \begin{bmatrix} H_1 \\ H_2 \\ \vdots \\ H_{kpr} \end{bmatrix}.$$

3) A BCH code is a special case of a Goppa code. For this, choose $h(X) = X^{kpr}$ and $T = \{\alpha_1, \alpha_2, \cdots, \alpha_n\}$, where $\alpha_i \in G_s$, for all $i = 1, 2, \cdots, n$. By Equation (3), it follows that

$$H = \begin{bmatrix} \alpha_1^{-kpr} & \alpha_2^{-kpr} & \cdots & \alpha_n^{-kpr} \\ \alpha^{1-kpr} & \alpha_2^{1-kpr} & \cdots & \alpha_n^{1-kpr} \\ \vdots & \vdots & \cdots & \vdots \\ \alpha_1^{-1} & \alpha_2^{-1} & \cdots & \alpha_n^{-1} \end{bmatrix}$$

and it becomes the parity-check matrix of a BCH code, by Equation (1), when α_i^{-1} is replaced by β_i, for $i = 1, 2, \cdots, n$.

Theorem 6: The Goppa code $C(T, h)$ has minimum Hamming distance $d \geq kpr + 1$.

Proof: Since $C(T, h)$ is an alternant code $C(n, \eta, \omega)$ with $\eta = (\alpha_1, \alpha_2, \cdots, \alpha_n)$ and $\omega = (h(\alpha_1)^{-1}, \cdots, h(\alpha_n)^{-1})$, it follows by Theorem 5 that $C(T, h)$ has minimum distance $d \geq kpr + 1$. ■

This study is dealing with only encoding but one may see [13] and [14] for the Goppa codes obtained through

generalized polynomials of $B[X; \frac{1}{kp}\mathbb{Z}_0]$ whenever $p = 2$ and $k = 1$ for its decoding principle.

Srivastava code is an interesting subclass of the alternant code, which is similar to unpublished work [15], which is proposed by J. N. Srivastava in 1967, a class of linear codes which are not cyclic that are defined in form of the parity-check matrices

$$H = \{\frac{\alpha_j^l}{1-\alpha_i\beta_j}, \quad \text{for} \quad 1 \le i \le r,\ 1 \le j \le n\},$$

where $\alpha_1, \alpha_2, \cdots, \alpha_r$ are distinct elements of $GF(q^m)$ and $\beta_1, \beta_2, \cdots, \beta_n$ are all the elements in $GF(q^m)$, except $0, \alpha_1^{-1}, \alpha_2^{-1}, \cdots, \alpha_r^{-1}$ and $l \ge 0$. In the following, we define the Srivastava code over a monoid ring instead of a polynomial ring, which is in fact generalizes [1, Defination 4.1].

Definition 6: A shortened Srivastava code of length $n \le s$ is a code over B that has parity-check matrix

$$H = \begin{bmatrix} \frac{\alpha_1^l}{\alpha_1-\beta_1} & \frac{\alpha_2^l}{\alpha_2-\beta_1} & \cdots & \frac{\alpha_n^l}{\alpha_n-\beta_1} \\ \frac{\alpha_1^l}{\alpha_1-\beta_2} & \frac{\alpha_2^l}{\alpha_2-\beta_2} & \cdots & \frac{\alpha_n^l}{\alpha_n-\beta_2} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{\alpha_1^l}{\alpha_1-\beta_{kpr}} & \frac{\alpha_2^l}{\alpha_2-\beta_{kpr}} & \cdots & \frac{\alpha_n^n}{\alpha_n-\beta_{kpr}} \end{bmatrix},$$

where l, r are positive integers and $\{\alpha_i\}_{1\le i\le n}, \{\beta_i\}_{1\le i\le kpr}$ are $n + kpr$ distinct elements in G_s.

Theorem 7: A Srivastava code has minimum Hamming distance $d \ge kpr + 1$.

Proof: A Srivastava code has minimum Hamming distance at least $kpr + 1$ if and only if every combination of kpr or fewer columns of H is linearly independent over $\Re$, or equivalently the following submatrix

$$H_1 = \begin{bmatrix} \frac{\alpha_{i_1}^l}{\alpha_{i_1}-\beta_1} & \frac{\alpha_{i_2}^l}{\alpha_{i_2}-\beta_1} & \cdots & \frac{\alpha_{i_{kpr}}^l}{\alpha_{i_{kpr}}-\beta_1} \\ \frac{\alpha_{i_1}^l}{\alpha_{i_1}-\beta_2} & \frac{\alpha_{i_2}^l}{\alpha_{i_2}-\beta_2} & \cdots & \frac{\alpha_{i_{kpr}}^l}{\alpha_{i_{kpr}}-\beta_2} \\ \vdots & \vdots & \cdots & \vdots \\ \frac{\alpha_{i_1}^l}{\alpha_{i_1}-\beta_{kpr}} & \frac{\alpha_{i_2}^l}{\alpha_{i_2}-\beta_{kpr}} & \cdots & \frac{\alpha_{i_{kpr}}^l}{\alpha_{i_{kpr}}-\beta_{kpr}} \end{bmatrix}$$

is nonsingular. However $det(H_1) = (\alpha_{i_1}\alpha_{i_2}\cdots\alpha_{i_{kpr}})^l det(H_2)$, where the matrix H_2 is given by

$$H_2 = \begin{bmatrix} \frac{1}{\alpha_{i_1}-\beta_1} & \frac{1}{\alpha_{i_2}-\beta_1} & \cdots & \frac{1}{\alpha_{i_{kpr}}-\beta_1} \\ \frac{1}{\alpha_{i_1}-\beta_2} & \frac{1}{\alpha_{i_2}-\beta_2} & \cdots & \frac{1}{\alpha_{i_{kpr}}-\beta_2} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{1}{\alpha_{i_1}-\beta_{pr}} & \frac{1}{\alpha_{i_2}-\beta_{kpr}} & \cdots & \frac{1}{\alpha_{i_{kpr}}-\beta_{kpr}} \end{bmatrix}.$$

As $det(H_2)$ is a Cauchy determinant of order kpr, so it can be concluded that $det(H_1) = (\alpha_{i_1}\cdots\alpha_{i_{kpr}})^l\theta$, where $\theta = \frac{(-1)^{\binom{kpr}{2}}\phi(\alpha_{i_1},\cdots,\alpha_{ikpr})\phi(\beta_1,\beta_2,\cdots,\beta_{kpr})}{v(\alpha_{i_1})v(\alpha_{i_2})\cdots v(\alpha_{i_{kpr}})}$, $\phi(\alpha_{i_1}, \cdots, \alpha_{i_{kpr}}) = \prod_{i_j>i_h}(\alpha_{i_j} - \alpha_{i_h})$ and $v(X) = (X-\beta_1)(X-\beta_2)\cdots(X-\beta_{kpr})$. So by Lemma 4 it follows that $det(H_1)$ is a unit in $\Re$ and therefore $d \ge kpr + 1$. ■

Definition 7: Let $r = (kpr)l$ and $\alpha_1, \cdots, \alpha_n$, $\beta_1, \beta_2, \cdots, \beta_{kpr}$ be the $n + kpr$ distinct elements of G_s. Let $\omega_1, \cdots, \omega_n$ be the elements of G_s. A generalized Srivastava code of length $n \le s$ is a code over B that has parity-check matrix given by

$$H = \begin{bmatrix} H_1 \\ H_2 \\ \vdots \\ H_{kpr} \end{bmatrix}, \tag{4}$$

where

$$H_j = \begin{bmatrix} \frac{\omega_1}{\alpha_1-\beta_j} & \frac{\omega_2}{\alpha_2-\beta_j} & \cdots & \frac{\omega_n}{\alpha_n-\beta_j} \\ \frac{\omega_1}{(\alpha_1-\beta_j)^2} & \frac{\omega_2}{(\alpha_2-\beta_j)^2} & \cdots & \frac{\omega_n}{(\alpha_n-\beta_j)^2} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{\omega_1}{(\alpha_1-\beta_j)^l} & \frac{\omega_2}{(\alpha_2-\beta_j)^l} & \cdots & \frac{\omega_n}{(\alpha_n-\beta_j)^l} \end{bmatrix}$$

for $j = 1, 2, \cdots, kpr$.

Theorem 8: A Srivastava code has minimum Hamming distance $d \ge (kpr)l + 1$.

Proof: Follows by Remark 1 and Theorem 7, because the matrices of the Equations (3) and (4) are equivalents, whereas $g(X) = (X - \beta_i)^l$. ■

REFERENCES

[1] A. A. Andrade, R. Palazzo Jr., *Linear codes over finite rings*, Tend. Mat. Apl. Comput., **6**(2), (2005), 207-217.

[2] J. Cazaran, A.V. Kelarev, *Generators and weights of polynomial codes*, Archiv. Math., **69**, (1997), 479-486.

[3] J. Cazaran, A.V. Kelarev, *On finite principal ideal rings*, Acta Math. Univ. Comenianae, **68**(1), (1999), 77-84.

[4] J. Cazaran, A.V. Kelarev, S.J. Quinn, D. Vertigan, *An algorithm for computing the minimum distances of extensions of BCH codes embedded in semigroup rings*, Simgroup Forum, **73**, (2006), 317-329.

[5] A.V. Kelarev, *Ring constructions and applications*, World Scientific, River Edge, New York (2002).

[6] A.V. Kelarev, *An algorithm for BCH codes extended with finite state automata*, Fundamenta Informaticae, **84**(1), (2008), 51-60.

[7] A.V. Kelarev, *Algorithms for computing parameters of graph-based extensions of BCH codes*, Journal of Discrete Algorithms, **5**, (2007), 553-563.

[8] R. Gilmer, *Commutative semigroup rings*, University Chicago Press Chicago and London (1984).

[9] N. Bourbaki, *Anneax principaux*, § 7.1 in Eléments de Mathématiques, Livre II: Algèbre, 2ème ed. Paris, France: Hermann (1964).

[10] R. Gilmer and T. Parker, *Divisibility properties in semigroup rings*, Source: Michigan Math. J., **21**(1), (1974), 65-86.

[11] R. Gilmer, *Multiplicative Ideal Theory*, Marcel Dekker, New York (1972).

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

[13] T. Shah, A. Khan and A. A. Andrade, *Encoding through generalized polynomial codes*, Computational Applied Mathematics, **30**(2), (2011), 349-366.

[14] A. A. Andrade, T. Shah and A. Khan, *Goppa codes through generalized polynomials and its decoding principle*, International Journal of Applied Mathematics, **23**(3), (2010), 515-526.

[15] H. J. Helgret, Srivastava Codes, *IEEE Trans. Inform.* Theory, **18**(2), (1972).