Ascending chain of semigroup rings and encoding

Tariq Shah and Atlas Khan
Department of Mathematics
Quaid-i- Azam University
Islamabad, Pakistan
stariqshah@gmail.com and atlasmaths@yahoo.com

Antonio Aparecido de Andrade
Department of Mathematics
Ibilce - Unesp
São José do Rio Preto - SP, Brazil
andrade@ibilce.unesp.br

***Abstract*— Let B be any finite commutative ring with identity. $\cdots \subset B[X;\frac{1}{a^k}\mathbb{Z}_0]\cdots \subset B[X;\frac{1}{a^2}\mathbb{Z}_0] \subset B[X;\frac{1}{a}\mathbb{Z}_0]$, where $a \in \{2,3,5,7,\cdots\}$, $k \geq 1$, is the descending chain of commutative semigroup rings. All these semigroup rings are containing the polynomial ring $B[X;\mathbb{Z}_0]$. In this paper initially we introduced the construction technique of cyclic codes through a semigroup ring $B[X;\frac{1}{a^k}\mathbb{Z}_0]$ instead of a polynomial ring. After this we separately considered BCH, alternant, Goppa, Srivastava codes and by this new constructions we improve the several results of [1] by adopting the same lines as in [1].**

***Index Terms*— Semigroup ring, BCH code, alternant code, Goppa code, Srivastava code.**

I. Introduction

In [1] A. A. Andrade and R. Palazzo Jr. discussed the cyclic, BCH, alternant, Goppa and Srivastava codes through polynomial ring $B[X;\mathbb{Z}_0]$, where B is any finite commutative ring with identity. In this paper we introduce the construction techniques of these codes through semigroup ring $B[X;\frac{1}{a^k}\mathbb{Z}_0]$, where $a \in \{2,3,5,7,\cdots\}$, $k \geq 1$, instead of a polynomial ring $B[X;\mathbb{Z}_0]$, where we improve the results of [1]. In fact $\cdots \subset B[X;\frac{1}{a^k}\mathbb{Z}_0] \subset B[X;\frac{1}{a^k}\mathbb{Z}_0]$, where $a \in \{2,3,5,7\cdots\}$, $k \geq 1$, the descending chain of commutative semigroup ring in which all these semigroups of the chain are containing the polynomial ring $B[X;\mathbb{Z}_0]$, motivated to address the study of [2], [3], [4], [5] in a unified way and obtain very useful findings by comparaction.

This paper is organized as follows. In Section 2, we give some basic results of semigroups and semigroup rings necessary for the construction of the linear codes. In Section 3, we present the construction of cyclic codes through the semigroup ring $B[X;\frac{1}{a^k}\mathbb{Z}_0]$, where $a \in \{2,3,5,7,\cdots\}$, $k \geq 1$, of generalized nature. In Section 4, we made the constructions of BCH and alternant codes through $B[X;\frac{1}{a^k}\mathbb{Z}_0]$ instead of polynomial ring $B[X;\mathbb{Z}_0]$. In Section 5, we describe a construction of Goppa and Srivastava codes through semigroup ring $B[X;\frac{1}{a^k}\mathbb{Z}_0]$. Finally, in Section 6, the concluding remarks are drawn.

II. Preliminaries

In this section we review basic facts from commutative semigroup rings [6]. Assume that $(S,*)$ is a semigroup and $(B,+,\cdot)$ is an associative (commutative) ring. The set SGR of all finitely nonzero functions f from S into B forms a ring with respect to binary operations addition and multiplication defined as $(f+g)(s) = f(s)+g(s)$ and $(fg)(s) = \sum\limits_{t*u=s} f(t)g(u)$, where the symbol $\sum\limits_{t*u=s}$ indicates that the sum is taken over all pairs (t,u) of elements of S such that $t*u=s$ and it is understood that in the situation where s is not expressible in the form $t*u$ for any t, $u \in S$, then $(fg)(s)=0$. The set SGR is known as *semigroup ring* of S over B. If S is a monoid, then SGR is called monoid ring. This ring SGR is represented as $B[S]$ whenever S is a multiplicative semigroup and elements of SGR are written either as $\sum\limits_{s\in S} f(s)s$ or as $\sum\limits_{i=1}^{n} f(s_i)s_i$. The representation of SGR will be $B[X;S]$ whenever S is an additive semigroup. As there is an isomorphism between additive semigroup S and multiplicative semigroup $\{X^s : s \in S\}$, so a nonzero element f of $B[X;S]$ is uniquely represented in the canonical form $\sum\limits_{i=1}^{n} f(s_i)X^{s_i} = \sum\limits_{i=1}^{n} f_iX^{s_i}$, where $f_i \neq 0$, $s_i \neq s_j$ for $i \neq j$.

The degree and order of an element a semigroup ring $B[X;S]$ are not generally defined but if we consider S to be a totally ordered semigroup, we can define the degree and order of an element of $B[X;S]$ in the following manner; if $f = \sum\limits_{i=1}^{n} f_iX^{s_i}$ is the canonical form of the nonzero element $f \in R[X;S]$, where $s_1 < s_2 < \cdots < s_n$, then s_n is called the degree of f and we write $\deg(f) = s_n$ and similarly the order of f is written as $\text{ord}(f) = s_1$. Now, if R is an integral domain, then for $f,g \in B[X;S]$, we have $\deg(fg)$ =$\deg(f)$+$\deg(g)$ and $\text{ord}(fg)$ =$\text{ord}(f)$+$\text{ord}(g)$.

If S is $\mathbb{Z}_0$ and B is an associative ring, the semigroup ring SGR is simply the polynomial ring $B[X]$. Obviously $B[X] = B[X;\mathbb{Z}_0] \subset B[X;\frac{1}{a^k}\mathbb{Z}_0]$. Furthermore as $\frac{1}{a^k}\mathbb{Z}_0$ is an ordered monoid, so we can define the degree of an element (a generalized polynomial) in $B[X;\frac{1}{a^k}\mathbb{Z}_0]$.

In this paper initially we replaced the the construction technique of cyclic codes over a polynomial ring by a semigroup ring $B[X;\frac{1}{a^k}\mathbb{Z}_0]$, where $a \in \{2,3,5,7,\cdots\}$, $k \geq 1$. Further we separately considered BCH, alternant, Goppa, Srivastava codes and by this new way of construction with utilizing the same lines as in [1] we improve the several results of [1]. 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 $B[X;\frac{1}{a^k}\mathbb{Z}_0]/(X^n-1)$. The factorization of $X^{a^k s}-1$ over the group of units of $B[X;\frac{1}{a^k}\mathbb{Z}_0]/(X^n-1)$ is the main problem.

Under consideration processes of constructing linear codes through the semigroup rings $B[X;\frac{1}{a^k}\mathbb{Z}_0]$ are very similar to linear codes over finite rings and this work needs Galois

extension rings, because here some of properties of Galois extension fields are failed.

The coding for error control has vital role in the design of modern communication systems and high speed digital computers. In this study we also mention that the codes through a semigroup ring are more appropriate for computer-to-computer communication.

III. Cyclic codes through the semigroup rings

In [7], if the ideal I for the commutative ring $\Re$ with identity, is generated by the element a of $\Re$, then in any quotient ring $\overline{\Re}$ of $\Re$, the corresponding ideal $\overline{I}$ is generated by the residue class $\overline{a}$ of a. Hence, every quotient ring of a principal ideal ring is a principal ideal ring (PIR) as well.

Consequently the ring $\Re = \frac{\mathbb{F}_q[X;\mathbb{Z}_0]}{(X^n-1)}$, where q is a power of a prime p, is a PIR as $\mathbb{F}_q[X;\mathbb{Z}_0]$ is a Euclidean domain ([8, Theorem 8.4]). Further by the same [1] if q is a power of a prime p, then $\Re = \frac{\mathbb{Z}_q[X;\mathbb{Z}_0]}{(X^n-1)}$ is a PIR.

For a finite commutative ring B with identity and for $a \in \{2,3,5,\cdots\}$, $k \geq 1$, the following

$$\begin{array}{ccccccc} \cdots & \subset & B[X;\frac{1}{a^k}\mathbb{Z}_0] & \cdots & \subset & B[X;\frac{1}{a^2}\mathbb{Z}_0] & \subset & B[X;\frac{1}{a}\mathbb{Z}_0] \\ & & \cup & & & \cup & & \cup \\ \cdots & = & B[X;\mathbb{Z}_0] & \cdots & = & B[X;\mathbb{Z}_0] & = & B[X;\mathbb{Z}_0] \end{array}$$

is strict descending chains of commutative semigroup rings.

By the same argument [1], the quotient ring of Euclidean monoid domain $\Re = \frac{\mathbb{F}_q[X;\frac{1}{a^k}\mathbb{Z}_0]}{(X^n-1)}$, where q is a power of a prime p and $a \in \{2,3,5,\cdots\}$, $k \geq 1$, is a PIR and $\Re = \frac{\mathbb{Z}_q[X;\frac{1}{a^k}\mathbb{Z}_0]}{(X^n-1)}$ is the PIR. The homomorphic image of a PIR is again a PIR [10, Proposition (38.4)].

By [1] if B be a commutative ring with identity, then $\Re = \frac{B[X;\mathbb{Z}_0]}{(X^n-1)}$ is a finite ring. And the linear code C of length n over B is a B-module in the space of all n-tuples of B^n, and a linear code C over B is cyclic, if whenever $v = (v_0, v_1, v_2, \cdots, v_{n-1}) \in C$, every cyclic shift $v^{(1)} = (v_{n-1}, v_0, v_1, \cdots, v_{n-2}) \in C$, with $v_i \in B$, for $0 \leq i \leq n-1$.

Now suppose again that B is a commutative ring with identity, then $\Re = \frac{B[X;\frac{1}{a^k}\mathbb{Z}_0]}{(X^n-1)}$, where $a \in \{2,3,5,7,\cdots\}$, $k \geq 1$, is a finite ring, by [6, Theorem 7.2]. By a linear code C of length $a^k n$ over B we mean a B-module in the space of all $a^k n$-tuples of $B^{a^k n}$, and a linear code C over B is cyclic, if whenever $v = (v_0, v_{\frac{1}{a}}, v_{\frac{2}{a}}, v_1, \cdots, v_{\frac{a^k n-1}{a^k}}) \in C$, every cyclic shift $v^{(1)} = (v_{\frac{a^k n-1}{a^k}}, v_0, v_{\frac{1}{a}}, \cdots, v_{\frac{a^k n-2}{a^k}}) \in C$, with $v_i \in B$, for $0 \leq i \leq \frac{a^k n-1}{a^k}$.

Theorem 1: A subset C of $\Re = \frac{B[X;\frac{1}{a^k}\mathbb{Z}_0]}{(X^n-1)}$, where $a \in \{2,3,5,7,\cdots\}$, $k \geq 1$, is a cyclic code if and only if C is an ideal of $\Re$.

Proof: Suppose that the subset C is a cyclic code. Then C is closed under addition and under multiplication by $X^{\frac{1}{a^k}}$. But then it is closed under multiplication by powers of $X^{\frac{1}{a^k}}$ and linear combinations of powers of $X^{\frac{1}{a^k}}$. That is, C is closed under multiplication by an arbitrary pseudo polynomial. Hence C is an ideal. Now suppose that the subset C is an ideal in $\Re$. Then C is closed under addition and closed under scalar multiplication. Hence C is a B-module. It is also closed under multiplication by any ring element, in particular under multiplication by $X^{\frac{1}{a^k}}$. Hence C is a cyclic code. ∎

Let $f(X^{\frac{1}{a^k}}) \in B[X;\frac{1}{a^k}\mathbb{Z}_0]$ be a monic pseudo polynomial of degree n, then $\Re = \frac{B[X;\frac{1}{a^k}\mathbb{Z}_0]}{(f(X^{\frac{1}{a^k}}))}$ be the set of residue classes of pseudo polynomials in $B[X;\frac{1}{a^k}\mathbb{Z}_0]$ modulo the ideal $(f(X))$ and a class can be represented as $\overline{a}(X^{\frac{1}{a^k}}) = \overline{a}_0 + \overline{a}_{\frac{1}{a^k}} X^{\frac{1}{a^k}} + \cdots + \overline{a}_{\frac{a^k n-1}{a^k}} X^{\frac{a^k n-1}{a^k}}$. A simple kind of ideal is a principal ideal, which consists of all multiples of a fixed pseudo polynomial $g(X^{\frac{1}{a^k}})$ by elements of $\Re$, called generator pseudo polynomial of the ideal. Now we shall prove some results which show a method of obtaining the generator pseudo polynomial of principal ideal. This method will serve as basis for the construction of a principal ideal in the ring $\Re$.

Lemma 1: Let I be an ideal in the ring $\Re = \frac{B[X;\frac{1}{a^k}\mathbb{Z}_0]}{(X^n-1)}$, where $a \in \{2,3,5,7,\cdots\}$ and $k \geq 1$. If the leading coefficient of some pseudo polynomial of lowest degree in I is a unit in B, then there exists a unique monic pseudo polynomial of minimal degree in I.

Proof: Let $\overline{g}(X^{\frac{1}{a^k}})$ be a pseudo polynomial of lowest degree m in I. If the leading coefficient $\overline{a}_m$ of $\overline{g}(X^{\frac{1}{a^k}})$ is a unit in B, it is always possible to obtain a monic pseudo polynomial $\overline{g}_1(X^{\frac{1}{a^k}}) = \overline{a_m} g(X^{\frac{1}{a^k}})$ with the same degree in I. Now, if $\overline{g}(X^{\frac{1}{a^k}})$ and $\overline{h}(X^{\frac{1}{a^k}})$ are monic pseudo polynomials of minimal degree m in I, then the pseudo polynomial $\overline{k}(X^{\frac{1}{a^k}}) = \overline{g}(X^{\frac{1}{a^k}}) - \overline{h}(X^{\frac{1}{a^k}})$ is a pseudo polynomial in I and has degree fewer than m. Therefore, by the choice of $\overline{g}(X^{\frac{1}{a^k}})$ follows that $\overline{k}(X^{\frac{1}{a^k}}) = 0$, and thus $\overline{g}(X^{\frac{1}{a^k}}) = \overline{h}(X^{\frac{1}{a^k}})$. ∎

Theorem 2: Let I be an ideal in the ring $\Re = \frac{B[X;\frac{1}{a^k}\mathbb{Z}_0]}{(X^n-1)}$, where $a \in \{2,3,5,7,\cdots\}$, and $k \geq 1$. If the leading coefficient of some pseudo polynomial $\overline{g}(X^{\frac{1}{a^k}})$ of lowest degree in I is a unit in B, then I is the principal ideal generated by $\overline{g}(X^{\frac{1}{a^k}})$.

Proof: Let $\overline{a}(X^{\frac{1}{a^k}})$ be a pseudo polynomial in I. By Euclidean algorithm there are unique pseudo polynomials $\overline{q}(X^{\frac{1}{a^k}})$ and $\overline{r}(X^{\frac{1}{a^k}})$ such that $\overline{a}(X^{\frac{1}{a^k}}) = \overline{q}(X^{\frac{1}{a^k}})\overline{g}(X^{\frac{1}{a^k}}) + \overline{r}(X^{\frac{1}{a^k}})$, where $\overline{r}(X^{\frac{1}{a^k}}) = 0$ or $\deg(r(X^{\frac{1}{a^k}})) < \deg(g(X^{\frac{1}{a^k}}))$. By the definition of an ideal, $\overline{r}(X^{\frac{1}{a^k}}) \in I$. Thus by the choice of $\overline{g}(X^{\frac{1}{a^k}})$, we have that $\overline{r}(X^{\frac{1}{a^k}}) = 0$ and therefore, $\overline{a}(X^{\frac{1}{a^k}}) = \overline{q}(X^{\frac{1}{a^k}})\overline{g}(X^{\frac{1}{a^k}})$. Thus every polynomial in I is multiple of $\overline{g}(X^{\frac{1}{a^k}})$, that is, I is generated by $\overline{g}(X^{\frac{1}{a^k}})$ and hence principal. ∎

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

Proof: Suppose that $\overline{r}(X^{\frac{1}{a^k}}) = \overline{0}$. Therefore there is $q(X^{\frac{1}{a^k}}) \neq 0$ in $B[\frac{1}{q^k}\mathbb{Z}_0]$ such that $r(X^{\frac{1}{a^k}}) = f(X^{\frac{1}{a^k}})q(X^{\frac{1}{a^k}})$. Since $f(X^{\frac{1}{a^k}})$ is regular and $r(X^{\frac{1}{a^k}}) \neq 0$ it follows that $\deg(r(X^{\frac{1}{a^k}})) = \deg(f(X^{\frac{1}{a^k}})) + \deg(q(X^{\frac{1}{a^k}})) \geq \deg(f(X^{\frac{1}{a^k}}))$, which is a contradiction since we had already assumed that $\deg(r(X^{\frac{1}{a^k}})) < \deg(f(X^{\frac{1}{a^k}}))$. Hence $\overline{r}(X^{\frac{1}{a^k}}) \neq 0$. ∎

Lemma 3: Let I be an ideal in the ring $\Re = \frac{B[X;\frac{1}{a^k}\mathbb{Z}_0]}{(X^n-1)}$, where $a \in \{2,3,5,7,\cdots\}$, $k \geq 1$ and $g(X^{\frac{1}{a^k}})$ be a pseudo

polynomial in $B[X;\frac{1}{a^k}\mathbb{Z}_0]$ with leading coefficient unit in B such that $\deg(g(X^{\frac{1}{a^k}})) < \deg(f(X^{\frac{1}{a^k}}))$. If $\overline{g}(X^{\frac{1}{a^k}}) \in I$ and has lowest degree in I, then $g(X^{\frac{1}{a^k}})$ divides $f(X^{\frac{1}{a^k}})$.

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

Theorem 3: Let I be an ideal in the ring $\Re = \frac{B[X;\frac{1}{a^k}\mathbb{Z}_0]}{(X^n-1)}$, where $a \in \{2,3,5,7,\cdots\}$ and $k \geq 1$. If $g(X^{\frac{1}{a^k}})$ divides $f(X^{\frac{1}{a^k}})$ and $\overline{g}(X^{\frac{1}{a^k}}) \in I$, then $\overline{g}(X^{\frac{1}{a^k}})$ has lowest degree in $(\overline{g}(X^{\frac{1}{a^k}}))$.

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

IV. BCH AND ALTERNANT CODES THROUGH A SEMIGROUP RING

We construct BCH and alternant codes through a semigroup ring instead of a polynomial ring. First we address the basic properties of Galois extension rings, which are used in the construction of these codes. In this section we assume that (B,N) denotes a finite local commutative ring with unity and residue field $\mathbb{K} = \frac{B}{N} \simeq GF(p^m)$, where p is a prime integer, m a positive integer. The natural projection $\pi : B[X;\frac{1}{a^k}\mathbb{Z}_0] \rightarrow \mathbb{K}[X;\frac{1}{a^k}\mathbb{Z}_0]$ is defined by $\pi(a(X^{\frac{1}{a^k}})) = \overline{a}(X^{\frac{1}{a^k}})$ (i.e. $\pi(\sum_{i=0}^{n} a_i X^{\frac{1}{a^k}i}) = \sum_{i=0}^{n} \overline{a_i} X^{\frac{1}{a^k}i}$, where $\overline{a_i} = a_i + N$). Let $f(X^{\frac{1}{a^k}})$ be a monic pseudo polynomial of degree t in $B[X;\frac{1}{a^k}\mathbb{Z}_0]$ such that $\pi(f(X^{\frac{1}{a^k}}))$ is irreducible in $\mathbb{K}[X;\frac{1}{a^k}\mathbb{Z}_0]$. Since [6, Theorem 7.2] accommodate $B[X;\frac{1}{a^k}\mathbb{Z}_0]$ as $B[\mathbb{Z}_0]$, therefore $f(X^{\frac{1}{a^k}})$ also is irreducible in $B[X;\frac{1}{a^k}\mathbb{Z}_0]$, by [9, Theorem XIII.7]. Take $\Re = \frac{B[X;\frac{1}{a^k}\mathbb{Z}_0]}{(f(X^{\frac{1}{a^k}}))}$. Then $\Re$ is a finite commutative local factor semigroup ring with unity and again [6, Theorem 7.2] accommodate our notions to say that it is a Galois ring extension of B with extension degree t. Its residue field is $\mathbb{K}_1 = \frac{\Re}{\overline{N_1}} \simeq GF(p^{mt})$, where $\overline{N_1}$ is the maximal ideal of $\Re$, and $\mathbb{K}_1^*$ is the multiplicative group of $\mathbb{K}_1$ whose order is $p^{mt}-1$.

Let $\Re^*$ denotes the multiplicative group of units of $\Re$. It follows that $\Re^*$ is an abelian group, and therefore it can be expressed as a direct product of cyclic groups. We are interested in the maximal cyclic group of $\Re^*$ hereafter denoted by $G_{a^k s}$, whose elements are the roots of $X^{a^k s}-1$ for some positive integer s. There is only one maximal cyclic subgroup of F having order $a^k s = a^k(p^{mt}-1)$.

Definition 1: A shortened BCH code $C(a^k n,\eta)$ of length $a^k n \leq a^k s$ is a code over B that has parity check matrix

$$H = \begin{bmatrix} \alpha_1 & \alpha_2 & \cdots & \alpha_{a^k n} \\ \alpha_1^2 & \alpha_2^2 & \cdots & \alpha_{a^k n}^2 \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{a^k r} & \alpha_2^{a^k r} & \cdots & \alpha_{a^k n}^{a^k r} \end{bmatrix}$$

for some $r = a^k(n-c) \geq 1$, where $\eta = (\alpha_1,\alpha_2,\cdots,\alpha_{a^k n}) = (\alpha^{k_1},\alpha^{k_2},\cdots,\alpha^{k_{a^k n}})$ is the locator vector, consisting of distinct elements of $G_{a^k s}$. The code $C(a^k n,\eta)$, with $a^k n = a^k s$, will be called a BCH code.

Lemma 4: Let $\alpha^{\frac{1}{a^k}}$ be an element of $G_{a^k s}$ of order $a^k s$. Then the differences $\alpha^{\frac{1}{a^k}l_1} - \alpha^{\frac{1}{a^k}l_2}$ are units in $\Re$ if $0 \leq l_1 \neq l_2 \leq a^k s - 1$.

Proof: As $\alpha^{\frac{1}{a^k}l_1} - \alpha^{\frac{1}{a^k}l_2}$ can be written as $-\alpha^{\frac{1}{a^k}l_2}(1 - \alpha^{\frac{1}{a^k}(l_1-l_2)})$, where $l_1 > l_2$ and 1 denotes the unity of $\Re$. The factor $-\alpha^{\frac{1}{a^k}l_2}$ in the product is a unit. The second factor can be written as $1-\alpha^{\frac{1}{a^k}j}$ for some integer j in the interval $[1, a^k s-1]$. Now if the element $1-\alpha^{\frac{1}{a^k}j}$, for $1 \leq j \leq a^k s-1$, were not a unit in $\Re$, then $1-\alpha^{\frac{1}{a^k}j} \in M_1$, and consequently, $(\pi(\alpha^{\frac{1}{a^k}}))^j = \pi(1)$ for $j < a^k s$, which is a contradiction. Thus $1-\alpha^{\frac{1}{a^k}j} \in \Re$, for $1 \leq j \leq a^k s - 1$. ∎

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

Proof: Suppose c is a nonzero codeword in $C(a^k n,\eta)$ such that $w_H(c) \leq a^k t$. Then $cH^T = 0$. Deleting $a^k n - a^k t$ columns of the matrix H corresponding to zeros of the codeword, it follows that the new matrix H is Vandermonde. By Lemma 4, it follows that the determinant is a unit in $\Re$. Thus the only possibility for c is the all zero codeword. ∎

Definition 2: A shortened alternant code $C(a^k n,\eta,\omega)$ of length $a^k n \leq a^k s$ is a code over B that has parity check matrix

$$H = \begin{bmatrix} \omega_1 & \omega_2 & \cdots & \omega_{a^k n} \\ \omega_1\alpha_1 & \omega_2\alpha_2 & \cdots & \omega_{a^k n}\alpha_{a^k n} \\ \omega_1\alpha_1^2 & \omega_2\alpha_2^2 & \cdots & \omega_{a^k n}\alpha_{a^k n}^2 \\ \vdots & \vdots & \ddots & \vdots \\ \omega_1\alpha_1^{a^k r-1} & \omega_2\alpha_2^{a^k r-1} & \cdots & \omega_{an}\alpha_{a^k n}^{a^k r-1} \end{bmatrix},$$

where r is a positive integer, $\eta = (\alpha_1,\alpha_2,\cdots,\alpha_{a^k n}) = (\alpha^{k_1},\alpha^{k_2},\cdots,\alpha^{k_{a^k n}})$ is the locator vector, consisting of distinct elements of $G_{a^k s}$, and $\omega = (\omega_1,\omega_2,\cdots,\omega_{a^k n})$ is an arbitrary vector consisting of elements of $G_{a^k s}$.

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

Proof: Suppose c is a nonzero codeword in $C(a^k n, \eta, \omega)$ such that the weight $w_H(c) \leq a^k r$. Then, $cH^T = c(LM)^T = 0$. Setting $b = cM^T$, we obtain $w_H(b) = w_H(c)$ since M is diagonal and invertible. Thus, $bL^T = 0$. Deleting $a^k n - a^k r$ columns of the matrix L that correspond to zeros of the codeword, then the new matrix L is Vandermonde. By Lemma 4, it follows that the determinant is a unit in $\Re$. Thus, the unique possibility for c is the all zero codeword. ∎

V. Goppa and Srivastava Codes through a semigroup ring

In this section we construct a subclass of alternant codes through a semigroup ring instead of a polynomial ring, which is similar to one initiated by Andrade and Palazzo [1] through polynomial rings. Goppa codes are described in terms of Goppa polynomial. In contrast to cyclic codes, where it is difficult to estimate the minimum Hamming distance d from the generator polynomial, Goppa codes have the property that $d \geq deg(h(X)) + 1$.

Let B, $\Re$ and $G_{a^k s}$ as defined in previous section. Let $\alpha^{\frac{1}{a^k}}$ be a primitive element of the cyclic group $G_{a^k s}$, where $a^k s = a^k(p^{mt} - 1)$. Let $h(X) = h_0 + h_1 X + h_2 X^2 + \cdots + h_{a^k r} X^{a^k r}$ be a polynomial with coefficients in $\Re$ and $h_{a^k r} \neq 0$. Let $T = \{\alpha_1, \alpha_2, \cdots, \alpha_{a^k n}\}$ be a subset of distinct elements of $G_{a^k s}$ such that $h(\alpha_i)$ are units from $\Re$, for $i = 1, 2, \cdots, a^k n$.

Definition 3: A shortened Goppa code $C(T, h)$ of length $a^k n \leq a^k s$ is a code over B that has parity-check matrix of the form

$$H = \begin{bmatrix} h(\alpha_1)^{-1} & \cdots & h(\alpha_{a^k n})^{-1} \\ \alpha_1 h(\alpha_1)^{-1} & \cdots & \alpha_{a^k n} h(\alpha_{a^k n}) \\ \vdots & \ddots & \vdots \\ \alpha_1^{a^k r - 1} h(\alpha_1)^{-1} & \cdots & \alpha_{a^k n}^{a^k r - 1} h(\alpha_{a^k n}) \end{bmatrix}, \quad (1)$$

where r is a positive integer, $\eta = (\alpha_1, \alpha_2, \cdots, \alpha_{a^k n}) = (\alpha^{c_1}, \alpha^{c_2}, \cdots, \alpha^{c_{a^k n}})$ is the locator vector, consisting of distinct elements of $G_{a^k s}$, and $\omega = (h(\alpha_1)^{-1}, \cdots, h(\alpha_{a^k n})^{-1})$ is a vector consisting of elements of $G_{a^k s}$.

Definition 4: 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 $c = (c_1, c_2, \cdots, c_{a^k n}) \in C(T, h)$ and $c = (c_{a^k n}, \cdots, c_2, c_1) \in C(T, h)$, then $C(T, h)$ is called a reversible Goppa code.
3) If $h(X) = (X - \alpha)^{a^k r - 1}$, then $C(T, h)$ is called a comulative Goppa code.
4) If $h(X)$ has no multiple zeros, then $C(T, h)$ is called a separable Goppa codes.

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

1) We have that $C(T, h)$ is a linear code.
2) For a code with $h_l(X) = (X - \beta_l)^{a^k r_l}$ being a Goppa polynomial, where $l \in G_{a^k s}$, we have the matrix H_l given by

$$\begin{bmatrix} (\alpha_1 - \beta_l)^{-a^k r_l} & \cdots & (\alpha_{a^k n} - \beta_l)^{-a^k r_l} \\ \alpha_1 (\alpha_1 - \beta_l)^{-a^k r_l} & \cdots & \alpha_{a^k n} (\alpha_{a^k n} - \beta_l)^{-a^k r_l} \\ \vdots & \ddots & \vdots \\ \alpha_1^{a^k r_{l-1}} (\alpha_1 - \beta_l)^{-a^k r_l} & \cdots & \alpha_{a^k n}^{a^k r_{l-1}} (\alpha_{a^k n} - \beta_l)^{-a^k r_l} \end{bmatrix}$$

which is row equivalent to

$$\begin{bmatrix} (\alpha_1 - \beta_l)^{-a^k r_l} & \cdots & (\alpha_{a^k n} - \beta_l)^{-a^k r_l} \\ (\alpha_1 - \beta_l)^{-(a^k r_l - 1)} & \cdots & (\alpha_{a^k n} - \beta_l)^{-(a^k r_l - 1)} \\ \vdots & \ddots & \vdots \\ (\alpha_1 - \beta_l)^{-1} & \cdots & (\alpha_{a^k n} - \beta_l)^{-1} \end{bmatrix}$$

Consequently, if $h(X) = (X - \beta_l)^{a^k r_l} = \prod_{i=1}^{a^k k} h_l(X)$, then the Goppa code is the intersection of the codes with $h_l(X) = (X - \beta_l)^{a^k r_l}$, for $l = 1, 2, \cdots, a^k k$, and its parity check matrix is given by

$$H = \begin{bmatrix} H_1 & H_2 & \cdots & H_{a^k k} \end{bmatrix}^T,$$

where T indicates the transposition.

3) BCH codes are a special case of Goppa codes. For this, choose $h(X) = X^{a^k r}$ and $T = \{\alpha_1, \alpha_2, \cdots, \alpha_{a^k n}\}$, where $\alpha_i \in G_{a^k s}$, for all $i = 1, 2, \cdots, a^k n$. Then from equation (c)

$$H = \begin{bmatrix} \alpha_1^{-a^k r} & \alpha_2^{-a^k r} & \cdots & \alpha_{3n}^{-a^k r} \\ \alpha^{1-a^k r} & \alpha_2^{1-a^k r} & \cdots & \alpha_{a^k n}^{1-a^k r} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{-1} & \alpha_2^{-1} & \cdots & \alpha_{a^k n}^{-1} \end{bmatrix}$$

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

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

Proof: We have that $C(T, h)$ is an alternant code $C(a^k n, \eta, \omega)$ with $\eta = (\alpha_1, \alpha_2, \cdots, \alpha_{a^k n})$ and $\omega = (h(\alpha_1)^{-1}, \cdots, h(\alpha_{a^k n})^{-1})$. Therefore, by Theorem 5, we have that $C(T, h)$ has minimum distance $d \geq a^k r + 1$. ∎

Also we define Srivastava code over semigroup ring, which is the interesting subclass of alternant codes which is similar to unpublished work [11], which is proposed by J. N. Srivastava in 1967, a class of linear codes which are not cyclic that are defined in form the parity-check matrices

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

where $\alpha_1, \alpha_2, \cdots \alpha_r$ are distinct elements from $GF(q^m)$ 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 $l \geq 0$.

Definition 5: A shortened Srivastava code of length $a^k n \leq a^k s$ is a code over B that has parity check matrix

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

where r, l are positive integers and $\alpha_1, \cdots, \alpha_{a^k n}, \beta_1, \beta_2, \cdots, \beta_{a^k r}$ are $a^k n + a^k r$ distinct elements of $G_{a^k s}$.

Theorem 7: The Srivastava code has minimum Hamming distance $d \geq a^k r + 1$.

Proof: We have that the minimum Hamming distance of Srivastava code is at least $a^k r + 1$ if and only if every combination of $a^k r$ or fewer columns of H is linearly independent over $\Re$, or equivalently that the submatrix

$$H_1 = \begin{bmatrix} \frac{\alpha_{i_1}^l}{\alpha_{i_1}-\beta_1} & \frac{\alpha_{i_2}^l}{\alpha_{i_2}-\beta_1} & \cdots & \frac{\alpha_{i_{a^k r}}^l}{\alpha_{i3_r}-\beta_1} \\ \frac{\alpha_{i_1}^l}{\alpha_{i_1}-\beta_2} & \frac{\alpha_2^l}{\alpha_{i_2}-\beta_2} & \cdots & \frac{\alpha_{i_{a^k r}}^l}{\alpha_{i_{a^k r}}-\beta_2} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{\alpha_{i_1}^l}{\alpha_{i_1}-\beta_{a^k r}} & \frac{\alpha_{i_2}^l}{\alpha_{i_2}-\beta_{a^k r}} & \cdots & \frac{\alpha_{i_{a^k r}}^l}{\alpha_{i_{a^k r}}-\beta_{a^k r}} \end{bmatrix}$$

is nonsingular. The determinant of this matrix can be expressed as $det(H_1) = (\alpha_{i_1}, \alpha_{i_2}, \cdots, \alpha_{i_{ar}})^l det(H_2)$. Whereas the matrix H_2 is given by

$$H_2 = \begin{bmatrix} \frac{1}{\alpha_{i_1}-\beta_1} & \frac{1}{\alpha_{i_2}-\beta_1} & \cdots & \frac{1}{\alpha_{i_{a^k r}}-\beta_1} \\ \frac{1}{\alpha_{i_1}-\beta_2} & \frac{1}{\alpha_{i_2}-\beta_2} & \cdots & \frac{1}{\alpha_{i_{a^k r}}-\beta_2} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{1}{\alpha_{i_1}-\beta_{ar}} & \frac{1}{\alpha_{i_2}-\beta_{a^k r}} & \cdots & \frac{1}{\alpha_{i_{a^k r}}-\beta_{a^k r}} \end{bmatrix}.$$

Note that $det(H_2)$ is a Cauchy determinant of order $a^k r$ and therefore we conclude that the determinant of the matrix H_1 is given by

$$det(H_1) = (\alpha_{i_1}, \cdots, \alpha_{i_{a^k r}})^l (-1)^{\binom{a^k r}{2}} \mu,$$

where $\mu = \frac{\phi(\alpha_{i_1}, \cdots, \alpha_{i_{a^k r}}) \phi(\beta_1, \beta_2, \cdots, \beta_{a^k r})}{v(\alpha_{i_1}) v(\alpha_{i_2}) \cdots v(\alpha_{i_{a^k r}})}$, $\phi(\alpha_{i_1}, \cdots, \alpha_{i_{a^k r}}) = (\alpha_{i_j} - \alpha_{i_h})$ and $v(X) = (X - \beta_1)(X - \beta_2) \cdots (X - \beta_{a^k r})$. Then, by Lemma 4, the $det(H_1)$ is a unit in $\Re$ and thus $d \geq a^k r + 1$. ∎

Definition 6: Suppose $r = (a^k cl$ and let $\alpha_1, \cdots, \alpha_{a^k n}$, $\beta_1, \beta_2, \cdots, \beta_{a^k c}$ be $a^k n + a^k c$ distinct elements of $G_{a^k s}$, $\omega_1, \cdots, \omega_{a^k n}$ be elements of $G_{a^k s}$. A generalized Srivastava code of length $a^k n \leq a^k s$ is a code over B that has parity check matrix

$$H = \begin{bmatrix} H_1 & H_2 & \cdots & H_{a^k c} \end{bmatrix}^T, \tag{2}$$

where

$$H_j = \begin{bmatrix} \frac{\omega_1}{\alpha_1-\beta_j} & \frac{\omega_2}{\alpha_2-\beta_j} & \cdots & \frac{\omega_{a^k n}}{\alpha_{a^k n}-\beta_j} \\ \frac{\omega_1}{(\alpha_1-\beta_j)^2} & \frac{\omega_2}{(\alpha_2-\beta_j)^2} & \cdots & \frac{\omega_{a^k n}}{(\alpha_{a^k n}-\beta_j)^2} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{\omega_1}{(\alpha_1-\beta_j)^l} & \frac{\omega_2}{(\alpha_2-\beta_j)^l} & \cdots & \frac{\omega_{a^k n}}{(\alpha_{a^k n}-\beta_j)^l} \end{bmatrix}$$

for $j = 1, 2, \cdots, a^k c$.

Theorem 8: The Srivastava code has minimum Hamming distance $d \geq (a^k c)l + 1$.

Proof: The proof requires nothing more than the application of Remark 1 and Theorem 7, since the matrices (1) and (2) are equivalents, where $g(Z) = (Z - \beta_i)^l$. ∎

VI. Conclusion

A linear code detect $d - 1$ errors, where d is a minimum distance of a code and correct $\left\lfloor \frac{d-1}{2} \right\rfloor$ errors. In the usual case of [1] $d \geq r + 1$, where r is the number of check symbols and we have that $\left\lfloor \frac{r+1-1}{2} \right\rfloor = \left\lfloor \frac{r}{2} \right\rfloor$ but method of this work we obtained $d \geq a^k r + 1$, which shows that codes detect and correct at least $a^k r$ errors $\left\lfloor \frac{a^k r+1-1}{2} \right\rfloor = \left\lfloor \frac{a^k r}{2} \right\rfloor$ errors respectively. Thus linear codes obtained through the technique of semigroup rings are better than the linear codes constructed by polynomial rings. The linear codes obtained through both the polynomial rings and the semigroup rings have the same code rate but our way provide the error correcting capability of a code greater than of [1].

Since n and p are relatively prime and therefore by [1] there are binary (if we take $p = 2$) cyclic codes, BCH, alternant, Goppa and Srivastava codes over finite rings with length n. Unfortunately by the way as adopted in the techniques of [1] we can not obtain binary cyclic codes, BCH, alternant, Goppa and Srivastava codes over finite rings with length $a^k n$, where $a \in \{2, 3, 5, 7, \cdots\}$, for $k \geq 1$, as the nature of the construction in [1], $a^k n$ and p are not relatively prime for instance if n is not even and $a \neq 2$. Due to constrains in the method of polynomial rings, used in [1], we provided a more accurate method of getting binary (if we take $p = 2$) cyclic codes, BCH, alternant, Goppa and Srivastava codes over finite rings with length $a^k n$. In this work we used the semigroup ring $B[X; \frac{1}{a^k}\mathbb{Z}_0]$ instead of a polynomial ring $B[X; \mathbb{Z}_0]$, where B is any finite commutative ring with identity. In this work we have used the same lines as credit in [1]. A decoding procedure is an open problem.

References

[1] A. A. de Andrade, R. Palazzo Jr, Linear codes over finite rings,Tema tend. Mat. Apl. Comput., 6, No. **2**(2005), 207 – 217.

[2] Tariq Shah, Atlas Khan and Antonio Aparecido de Andrade, "Encoding through generalized polynomial codes", (Submitted).

[3] Tariq Shah, Atlas Khan and Antonio Aparecido de Andrade, "Encoding through generalized polynomial codes II", (Submitted).

[4] Tariq Shah, Atlas Khan and Antonio Aparecido de Andrade, "Encoding through generalized polynomial codes III", (Submitted).

[5] Tariq Shah, Atlas Khan and Antonio Aparecido de Andrade, "Encoding through generalized polynomial codes IV", (Submitted).

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

[7] N. Bourbaki, "Anneax principaux " § 7.1 in Elements de Mthematiques, Livre, 2eme. Paris, France: Hermann, (1964).

[8] R. Gilmer and T. Parker, Divisibility properties in semigroup rings, (1974), 65 – 86.

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

[10] R. Gilmer, "Multiplicative Ideal Theory", New York (1972).

[11] H. J. Helgret, Srivastava Codes, *IEEE Trans. Inform.* Theory, IT-18, No.2, March 1972.