COMPUTATIONAL & APPLIED MATHEMATICS

Volume 30, N. 2, pp. 349–366, 2011

ISSN 0101-8205
www.scielo.br/cam

Encoding through generalized polynomial codes

T. SHAH[1], A. KHAN[1] and A.A. ANDRADE[2]*

[1]Department of Mathematics, Quaid-i-Azam University, Islamabad, Pakistan
[2]Department of Mathematics, Ibilce, Unesp, São José do Rio Preto, SP, Brazil

E-mails: stariqshah@gmail.com / atlasmaths@yahoo.com / andrade@ibilce.unesp.br

Abstract. This paper introduces novel constructions of cyclic codes using semigroup rings instead of polynomial rings. These constructions are applied to define and investigate the BCH, alternant, Goppa, and Srivastava codes. This makes it possible to improve several recent results due to Andrade and Palazzo [1].

Mathematical subject classification: 18B35, 94A15, 20H10.

Key words: semigroup ring, cyclic code, BCH code, alternant code, Goppa code, Srivastava code.

1 Introduction

In ring theory, finite commutative rings are of interest due to many applications. The role of ideals is very essential for these applications and it is often important to know when the ideals in a ring are principal ideals. The very famous class of rings in this regard is the polynomial rings in one indeterminate coefficients from a finite field, in fact it is an Euclidean domain. The coding for error control has a vital role in the design of modern communication systems and high speed digital computers. Most of the classical error-correcting codes are ideals in finite commutative rings, especially in quotient rings of Euclidean domains of polynomials and group rings, i.e., cyclic codes are principal ideals in the quotient ring $\mathbb{F}_q[X]/(X^n - 1)$.

#CAM-187/10. Received: 09/II/10. Accepted: 01/I/11.
*Acknowledgment to FAPESP by financial support, 2007/56052-8.

On the above ideas, Cazaran and Kelarev [2] established necessary and sufficient conditions for an ideal to have a single generator and described all finite quotient rings $\mathbb{Z}_m[X_1, \cdots, X_n]/I$, where I is an ideal generated by univariate polynomials which are commutative principal ideal rings. In another paper, Cazaran and Kelarev [3] obtained conditions for the certain rings to be finite commutative principal ideal rings. However, the extension of a BCH code C embedded in a semigroup ring $F[S]$, where S is a finite semigroup, was considered in 2006 by Cazaran et. all [4], where an algorithm was presented for computing the weights of extensions for these codes embedded in semigroup rings as ideals. A lot of information concerning various ring constructions and about polynomial codes is given by Kelarev [5]. In [5], the whole Sections 9.1 and 9.2 are reserved to error-correcting codes in ring constructions closely related to semigroup rings. Especially, Section 9.1 deals error-correcting cyclic codes of length n which are ideals in group ring $F[G]$, where F is a field and G is a finite torsion group of size n. Another work concerning extensions of BCH codes in various ring constructions has been given by Kelarev ([6, 7]), where the results can also be considered as the special cases of semigroup rings of specific nature.

A.A. Andrade and R. Palazzo Jr. [1] discussed the cyclic, BCH, alternant, Goppa and Srivastava codes over finite rings, which are in fact constructed through a polynomial ring in one indeterminate with a finite coefficient ring. In this paper, we introduce the construction techniques of cyclic codes through a semigroup ring instead of a polynomial ring and then establish the constructions of BCH, alternant, Goppa, Srivastava codes. Here the results of [1] are improved in such a way that instead of cancellative torsion free additive monoid $\mathbb{Z}_0$, the cancellative torsion free additive monoid $\frac{1}{2}\mathbb{Z}_0$ is used which shifts whole construction of a finite quotient ring of a polynomial ring into a finite quotient ring of a semigroup ring of specific type. Furthermore, B is taken as a finite commutative ring with unity in the same spirit of [1]. A cyclic subgroup of group of units of the ring $B[X; \frac{1}{2}\mathbb{Z}_0]/(X^n - 1)$ is fixed analogous to [1]. In this set up the factorization of $X^{2s} - 1$ over the group of units of $B[X; \frac{1}{2}\mathbb{Z}_0]/(X^n - 1)$ is again a difficult task.

The procedure adopted in this work for construction of linear codes through the semigroup ring $B[X; \frac{1}{2}\mathbb{Z}_0]$ is simple as polynomial's set up and our ap-

proach is quite different to the embedding of linear polynomial codes in a semigroup ring or in a group algebra, which has been adopted by several authors.

This paper is organized as follows. In Section 2, the basic results on semigroups and semigroup rings necessary for the construction of the codes are given. In Section 3, the construction of cyclic codes through a semigroup ring is introduced. Section 4, addresses the constructions of BCH and alternant codes through the semigroup rings. In Section 5, a construction of Goppa and Srivastava codes through the semigroup rings is described. Finally, in Section 6, the concluding remarks are presented.

2 Preliminaries

In this section, we review basic facts on commutative semigroup rings from [8]. Assume that $(B, +, \cdot)$ is an associative ring and $(S, *)$ is a semigroup. Let J be the set of all finitely nonzero functions f from S into B. The set J is a ring with respect to binary operations addition and multiplication defined as $(f+g)(s) = f(s) + g(s)$ and $(fg)(s) = \sum_{t*u=s} f(t)g(u)$, where the symbol $\sum_{t*u=s}$ 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 ring J is known as a *semigroup ring* of S over B. If S is a monoid, then J is called a *monoid ring*. This ring J is represented as $B[S]$ whenever S is a multiplicative semigroup and elements of J are written either as $\sum_{s\in S} f(s)s$ or as $\sum_{i=1}^{n} f(s_i)s_i$. The representation of J 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

$$\sum_{i=1}^{n} f(s_i)X^{s_i} = \sum_{i=1}^{n} f_i X^{s_i}, \quad \text{where} \quad f_i \neq 0 \text{ and } s_i \neq s_j \text{ for } i \neq j.$$

The concepts of degree and order are not generally defined in semigroup rings. If the semigroup S is a cancellative torsion free or totally ordered, we can define the degree and the order of an element of the semigroup ring $B[X; S]$

in the following manner; if $\sum_{i=1}^{n} f_i X^{s_i}$ is the canonical form of a nonzero element f of $R[X; S]$, where $s_1 < s_2 < \cdots < s_n$, then s_n is called the *degree of pseudo polynomial* 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

$$\begin{aligned} \deg(fg) &= \deg(f) + \deg(g) \\ \text{ord}(fg) &= \text{ord}(f) + \text{ord}(g). \end{aligned}$$

If the monoid S is $\mathbb{Z}_0$ and B is an associative ring, the semigroup ring J is simply the polynomial ring, that is, $B[X] = B[X; \mathbb{Z}_0] \subset B[X; \frac{1}{2}\mathbb{Z}_0]$. Furthermore in $B[X; \frac{1}{2}\mathbb{Z}_0]$ one may define the degree of a pseudo polynomial because $\frac{1}{2}\mathbb{Z}_0$ is totally ordered.

In addition $B[G]$ is known as group ring whenever G is a group. Particularly $F[G]$ is group algebra, where F is a field. In [5] the Section 9.1 is dealing with error-correcting cyclic codes of length n which are ideals in group ring $F[G]$, where G is taken to be a finite torsion group of size n.

3 Cyclic codes through a semigroup ring

According to [9], if an ideal I of a commutative ring $\Re$ with unity is generated by an 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 (PIR) is a PIR as well. It follows that the ring $\mathbb{Z}_n$ is a PIR for any non prime positive integer n. 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. Also, 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 (see also [1]). By the same argument $\Re = \frac{\mathbb{F}_q[X;\frac{1}{2}\mathbb{Z}_0]}{(X^n-1)}$ and $\Re = \frac{\mathbb{Z}_q[X;\frac{1}{2}\mathbb{Z}_0]}{(X^n-1)}$ are PIRs. Furthermore, the homomorphic image of a PIR is again a PIR [10, Proposition 38.4]. By the same argument as given in [1], if B is a commutative ring with identity, then $\Re = \frac{B[X;\mathbb{Z}_0]}{(X^n-1)}$ is a finite ring.

A *linear code* C of length n over a commutative ring B with identity is a B-submodule in the space of all n-tuples of B^n, and a linear code C over B is a *cyclic code*, if $v = (v_0, v_1, v_2, \cdots, v_{n-1}) \in C$, every cyclic shift $v^{(1)} = (v_{n-1}, v_0, \cdots, v_{n-2}) \in C$, where $v_i \in B$ for $0 \leq i \leq n-1$.

By [8, Theorem 7.2], for a commutative ring B with identity, $\Re = \frac{B[X;\frac{1}{2}Z_0]}{(X^n-1)}$ is a finite ring. A *linear code* C of length $2n$ over B is a B-submodule in the space of all $2n$-tuples of B^{2n} and C is a *cyclic code*, if

$$v = \left(v_0, v_{\frac{1}{2}}, v_1, \cdots, v_{\frac{2n-1}{2}}\right) \in C,$$

every cyclic shift

$$v^{(1)} = \left(v_{\frac{2n-1}{2}}, v_0, v_{\frac{1}{2}}, \cdots, v_{n-1}\right) \in C,$$

where $v_i \in B$ for $i = 0, 1, \cdots, \frac{2n-1}{2}$.

The following theorem generalizes [1, Theorem 2.1].

Theorem 1. *A subset C of $\Re = \frac{B[X;\frac{1}{2}Z_0]}{(X^n-1)}$ 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 multiplication by $X^{\frac{1}{2}}$. But then it is closed under multiplication by powers of $X^{\frac{1}{2}}$ and linear combinations of powers of $X^{\frac{1}{2}}$. 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 scalar multiplication. Hence C is a B-module. It is also closed under multiplication by any ring element, in particular under multiplication by $X^{\frac{1}{2}}$. Hence C is a cyclic code. □

If $f(X^{\frac{1}{2}}) \in B[X; \frac{1}{2}Z_0]$ is a monic pseudo polynomial of degree n, then $\Re = \frac{B[X;\frac{1}{2}Z_0]}{(f(X^{\frac{1}{2}}))}$ is the set of residue classes of pseudo polynomials in $B[X; \frac{1}{2}Z_0]$ modulo the ideal $(f(X^{\frac{1}{2}}))$ and a class can be represented as $\overline{a}(X^{\frac{1}{2}}) = \overline{a}_0 + \overline{a}_{\frac{1}{2}}X^{\frac{1}{2}} + \overline{a}_1 X + \cdots + \overline{a}_{\frac{2n-1}{2}}X^{\frac{2n-1}{2}}$. A principal ideal of $\Re$ consists of all multiples of a fixed pseudo polynomial $g(X^{\frac{1}{2}})$ by elements of $\Re$, where $g(X^{\frac{1}{2}})$ is called a *generator pseudo polynomial* of the ideal. Now we will prove some results which show a method of obtaining the generator pseudo polynomial of a principal ideal. This method will serve as a base for the construction of a principal ideal in the ring $\Re$.

The following lemma generalizes [1, Lemma 2.1].

Lemma 1. *Let I be an ideal in the ring $\Re$. 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 the ideal I.*

Proof. Let $\overline{g}(X^{\frac{1}{2}})$ be a pseudo polynomial of lowest degree m in I. If the leading coefficient $\overline{a}_m$ of $\overline{g}(X^{\frac{1}{2}})$ is a unit in B, it is always possible to obtain a monic pseudo polynomial $\overline{g}_1(X^{\frac{1}{2}}) = \overline{a_m} g(X^{\frac{1}{2}})$ with the same degree in I. Now, if $\overline{g}(X^{\frac{1}{2}})$ and $\overline{h}(X^{\frac{1}{2}})$ are monic pseudo polynomials of minimal degree m in I, then the pseudo polynomial $\overline{k}(X^{\frac{1}{2}}) = \overline{g}(X^{\frac{1}{2}}) - \overline{h}(X^{\frac{1}{2}})$ is a pseudo polynomial in I and has degree fewer than m. Therefore, by the choice of $\overline{g}(X^{\frac{1}{2}})$, it follows that $\overline{k}(X^{\frac{1}{2}}) = 0$, and therefore $\overline{g}(X^{\frac{1}{2}}) = \overline{h}(X^{\frac{1}{2}})$. □

The following theorem generalizes [1, Theorem 2.2].

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

Proof. Let $\overline{a}(X^{\frac{1}{2}})$ be a pseudo polynomial in I. By Euclidean algorithm there are unique pseudo polynomials $\overline{q}(X^{\frac{1}{2}})$ and $\overline{r}(X^{\frac{1}{2}})$ such that $\overline{a}(X^{\frac{1}{2}}) = \overline{q}(X^{\frac{1}{2}})\overline{g}(X^{\frac{1}{2}}) + \overline{r}(X^{\frac{1}{2}})$, where $\overline{r}(X^{\frac{1}{2}}) = 0$ or $\deg(r(X^{\frac{1}{2}})) < \deg(g(X^{\frac{1}{2}}))$. By the definition of an ideal, $\overline{r}(X^{\frac{1}{2}}) \in I$. Thus, by the choice of $\overline{g}(X^{\frac{1}{2}})$, we have that $\overline{r}(X^{\frac{1}{2}}) = 0$ and therefore, $\overline{a}(X^{\frac{1}{2}}) = \overline{q}(X^{\frac{1}{2}})\overline{g}(X^{\frac{1}{2}})$. Thus every polynomial in I is a multiple of $\overline{g}(X^{\frac{1}{2}})$, that is, I is generated by $\overline{g}(X^{\frac{1}{2}})$ and hence principal. □

The following lemma generalizes [1, Lemma 2.2].

Lemma 2. *Let $r(X^{\frac{1}{2}})$ be a pseudo polynomial in $B[X; \frac{1}{2}Z_0]$. If $r(X^{\frac{1}{2}}) \neq 0$ and $\deg(r(X^{\frac{1}{2}})) < \deg(f(X^{\frac{1}{2}}))$, then $\overline{r}(X^{\frac{1}{2}}) \neq 0$ in $\Re$.*

Proof. Suppose that $\overline{r}(X^{\frac{1}{2}}) = \overline{0}$. Therefore there is $q(X^{\frac{1}{2}}) \neq 0$ in $B[X; \frac{1}{2}\mathbb{Z}_0]$ such that $r(X^{\frac{1}{2}}) = f(X^{\frac{1}{2}})q(X^{\frac{1}{2}})$. Since $f(X^{\frac{1}{2}})$ is regular and $r(X^{\frac{1}{2}}) \neq 0$ it follows that $\deg(r(X^{\frac{1}{2}})) = \deg(f(X^{\frac{1}{2}})) + \deg(q(X^{\frac{1}{2}})) \geq \deg(f(X^{\frac{1}{2}}))$, a contradiction since we had already assumed that $\deg(r(X^{\frac{1}{2}})) < \deg(f(X^{\frac{1}{2}}))$. Hence $\overline{r}(X^{\frac{1}{2}}) \neq 0$. □

The following lemma generalizes [1, Theorem 2.3].

Theorem 3. *Let I be an ideal in the ring $\Re$ and $g(X^{\frac{1}{2}})$ be a pseudo polynomial in $B[X; \frac{1}{2}Z_0]$, where leading coefficient is a unit in B, such that* $\deg(g(X^{\frac{1}{2}})) < \deg(f(X^{\frac{1}{2}}))$. *If $\overline{g}(X^{\frac{1}{2}}) \in I$ and has lowest degree in I, then $g(X^{\frac{1}{2}})$ divides $f(X^{\frac{1}{2}})$.*

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

Example 1. Let $\Re = \frac{\mathbb{Z}_4[X; \frac{1}{2}Z_0]}{(f(X^{\frac{1}{2}}))}$, where $f(X^{\frac{1}{2}}) = (X^{\frac{1}{2}})^4 - 1$. It is easy to verify that

$$I = \left\{0, \overline{1} + \overline{1}X^{\frac{1}{2}} + \overline{1}X + \overline{1}X^{\frac{3}{2}}, \overline{2} + \overline{2}X^{\frac{1}{2}} + \overline{2}X + \overline{2}X^{\frac{3}{2}}, \overline{3} + X^{\frac{1}{2}} + \overline{3}X + \overline{3}X^{\frac{3}{2}}\right\}$$

is an ideal of $\Re$. By Theorem 2, it follows that $I = (\overline{3} + \overline{3}X^{\frac{1}{2}} + \overline{3}X + \overline{3}X^{\frac{3}{2}})$ and by Theorem 3, $g(X^{\frac{1}{2}}) = 3 + 3X^{\frac{1}{2}} + 3X + 3X^{\frac{3}{2}}$ divides $f(X^{\frac{1}{2}})$.

The following theorem generalizes [1, Theorem 2.4].

Theorem 4. *Let I be an ideal in the ring $\Re$. If $g(X^{\frac{1}{2}})$ divides $f(X^{\frac{1}{2}})$ and $\overline{g}(X^{\frac{1}{2}}) \in I$, then $\overline{g}(X^{\frac{1}{2}})$ has lowest degree in the ideal $(\overline{g}(X^{\frac{1}{2}}))$.*

Proof. Suppose that there is $\overline{b}(X^{\frac{1}{2}})$ in $(\overline{g}(X^{\frac{1}{2}}))$ such that $\deg(\overline{b}(X^{\frac{1}{2}})) < \deg(\overline{g}(X^{\frac{1}{2}}))$. Since $\overline{b}(X^{\frac{1}{2}}) \in (\overline{g}(X^{\frac{1}{2}}))$, it follows that $\overline{b}(X^{\frac{1}{2}}) = \overline{g}(X^{\frac{1}{2}})\overline{h}(X^{\frac{1}{2}})$ for some $\overline{h}(X^{\frac{1}{2}}) \in \Re$. Thus $b(X^{\frac{1}{2}}) - g(X^{\frac{1}{2}})h(X^{\frac{1}{2}}) \in (f(X^{\frac{1}{2}}))$, i.e., $b(X^{\frac{1}{2}}) - g(X^{\frac{1}{2}})h(X^{\frac{1}{2}}) = f(X^{\frac{1}{2}})a(X^{\frac{1}{2}})$ for some $a(X^{\frac{1}{2}})$ in $B[X; \frac{1}{2}\mathbb{Z}_0]$. This gives $b(X^{\frac{1}{2}}) = g(X^{\frac{1}{2}})h(X^{\frac{1}{2}}) + f(X^{\frac{1}{2}})a(X^{\frac{1}{2}})$. Since $g(X^{\frac{1}{2}})$ divides $f(X^{\frac{1}{2}})$, so $g(X^{\frac{1}{2}})$ divides $g(X^{\frac{1}{2}})h(X^{\frac{1}{2}}) + f(X^{\frac{1}{2}})a(X^{\frac{1}{2}})$, which implies that $g(X^{\frac{1}{2}})$ divides $b(X^{\frac{1}{2}})$, a contradiction, since we had already assumed that $\deg(b(X^{\frac{1}{2}})) < \deg(g(X^{\frac{1}{2}}))$. Hence $\overline{g}(X^{\frac{1}{2}})$ has lowest degree in the ideal $(\overline{g}(X^{\frac{1}{2}}))$. □

4 BCH and alternant codes through a semigroup ring

Before the construction of BCH and alternant codes through a semigroup ring instead of a polynomial ring, we discuss the basic properties of Galois extension rings in perspective of quotient ring of semigroup ring of $\frac{1}{2}\mathbb{Z}_0$ over a finite local commutative ring B with unity, which are used in the construction of these codes.

Assume (B, N) is a finite local commutative ring with unity with residue field $\mathbb{K} = \frac{B}{N} \cong GF(p^m)$, where p is a prime and m a positive integer. The natural projection $\pi : B[X; \frac{1}{2}\mathbb{Z}_0] \to \mathbb{K}[X; \frac{1}{2}\mathbb{Z}_0]$ is defined by $\pi(a(X^{\frac{1}{2}})) = \overline{a}(X^{\frac{1}{2}})$, i.e., $\pi(\sum_{i=0}^{2n} a_i X^{\frac{1}{2}i}) = \sum_{i=0}^{2n} \overline{a_i} X^{\frac{1}{2}i}$, where $\overline{a_i} = a_i + N$, for $i = 0, \ldots, 2n$. Let $f(X^{\frac{1}{2}})$ be a monic pseudo polynomial of degree t in $B[X; \frac{1}{2}\mathbb{Z}_0]$ such that $\pi(f(X^{\frac{1}{2}}))$ is irreducible in $\mathbb{K}[X; \frac{1}{2}\mathbb{Z}_0]$. By [8, Theorem 7.2] $B[X; \frac{1}{2}\mathbb{Z}_0]$ can be accommodated as $B[X; \mathbb{Z}_0]$ and following [11, Theorem XIII.7] $f(X^{\frac{1}{2}})$ is irreducible in $B[X; \frac{1}{2}\mathbb{Z}_0]$. The ring $\Re = \frac{B[X; \frac{1}{2}\mathbb{Z}_0]}{(f(X^{\frac{1}{2}}))}$ is a local finite commutative ring with identity, whose maximal ideal is $N_2 = \frac{N_1}{(f(X^{\frac{1}{2}}))}$, where $N_1 = (N, f(X^{\frac{1}{2}}))$ and the residue field $\mathbb{K}_1 = \frac{\Re}{N_2} \simeq \frac{B[X; \frac{1}{2}\mathbb{Z}_0]}{(N, f(X^{\frac{1}{2}}))} \simeq \frac{\mathbb{K}[X; \frac{1}{2}\mathbb{Z}_0]}{(\pi(f(X^{\frac{1}{2}})))} \simeq GF(p^{2mt})$, and $\mathbb{K}_1^*$ is the multiplicative group of $\mathbb{K}_1$ whose order is $p^{2mt} - 1$.

Let the multiplicative group of units of $\Re$ be denoted by $\Re^*$, which 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 $\Re^*$, hereafter denoted by G_s, whose elements are the roots of $X^s - 1$ for some positive integer s such that $gcd(p, s) = 1$. There is only one maximal cyclic subgroup of $\Re^*$ having order $s = p^{2mt} - 1$ [11, Theorem XVIII.2].

4.1 BCH codes

The following definition generalizes [1, Definition 3.1] and accelerate for the construction of a BCH code through a semigroup ring.

Definition 1. *Let $\eta = (\alpha_1, \cdots, \alpha_n)$ be a vector consisting of distinct elements of G_s, and let $\omega = (\omega_1, \omega_2, \cdots, \omega_n)$ be an arbitrary vector consisting of elements (not necessarily distinct) of G_s. Then the set of all vectors*

$$\big(\omega_1 f(\alpha_1), \omega_2 f(\alpha_2), \cdots, \omega_n f(\alpha_n)\big),$$

where $f(Z)$ ranges over all polynomials of degree at most $k-1$, for $k \in N$, with coefficients from $\Re$, defines a shortened code C of length $n \leq s$ over $\Re$.

Remark 1. Since f has at most $k-1$ zeros, it follows that the minimum distance of this code is at least $(n-k)+1$.

The following definition generalizes [1, Definition 3.2].

Definition 2. *A shortened BCH code $C(n,\eta)$ of length $n \leq s$ is a code over B with parity check matrix*

$$H = \begin{bmatrix} \alpha_1 & \alpha_2 & \cdots & \alpha_n \\ \alpha_1^2 & \alpha_2^2 & \cdots & \alpha_n^2 \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{2r} & \alpha_2^{2r} & \cdots & \alpha_n^{2r} \end{bmatrix}$$

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 called a BCH code.

The following lemma generalizes [1, Lemma 3.1].

Lemma 3. *Let $\alpha^{\frac{1}{2}}$ be an element of G_s of order s. Then the differences $\alpha^{\frac{1}{2}l_1} - \alpha^{\frac{1}{2}l_2}$ are units in $\Re$ if $0 \leq l_1 \neq l_2 \leq s-1$.*

Proof. The differences $\alpha^{\frac{1}{2}l_1} - \alpha^{\frac{1}{2}l_2}$ can be written as $-\alpha^{\frac{1}{2}l_2}(1 - \alpha^{\frac{1}{2}(l_1-l_2)})$, where $l_1 > l_2$ and 1 denotes the unity of $\Re$. The factor $-\alpha^{\frac{1}{2}l_2}$ in the product is a unit. The second factor can be written as $1 - \alpha^{\frac{1}{2}j}$ for some integer j in the interval $[1, s-1]$. Now if the element $1 - \alpha^{\frac{1}{2}j}$, for $1 \leq j \leq s-1$, is not a unit in $\Re$, then $1 - \alpha^{\frac{1}{2}j} \in N_2$, and consequently, $(\pi(\alpha^{\frac{1}{2}}))^j = \pi(1)$ for $j < s$. Therefore, $\pi(\alpha^{\frac{1}{2}})$ has order $j_0 < s$, which is a contradiction. Thus, the elements $1 - \alpha^{\frac{1}{2}j} \in \Re$ are units for $j = 1, 2, \cdots, s-1$. □

The following theorem generalizes [1, Theorem 3.1].

Theorem 5. *The minimum Hamming distance of a BCH code $C(n,\eta)$ satisfies $d \geq 2r+1$.*

Proof. Assume that c is a nonzero codeword in $C(n, \eta)$ such that $w_H(c) \leq 2t$. Then $cH^T = 0$. Deleting $n - 2t$ columns of the matrix H corresponding to zeros of the codeword, it follows that the new matrix H' is a Vandermonde's one. By Lemma 3, it follows that the determinant of H' is a unit in $\Re$. Thus the only possibility for c is the all zero codeword. □

Example 2. Let $B = GF(2)[i]$ and

$$\Re = \frac{B\left[X; \frac{1}{2}\mathbb{Z}_0\right]}{\left(f(X^{\frac{1}{2}})\right)},$$

where $f(X^{\frac{1}{2}}) = (X^{\frac{1}{2}})^3 + X^{\frac{1}{2}} + 1$ is irreducible over B. If $\alpha^{\frac{1}{2}}$ is a root of $f(X^{\frac{1}{2}})$, then $\alpha^{\frac{1}{2}}$ generates a cyclic group G_s of order $s = 2^3 - 1 = 7$. Let $\eta = (1, \alpha, \alpha^{\frac{3}{2}}, \alpha^2, \alpha^{\frac{5}{2}}, \alpha^3)$ be the locator vector consisting of distinct elements of G_s. If $r = 2$, then the following matrix

$$H = \begin{bmatrix} 1 & \alpha & \alpha^{\frac{3}{2}} & \alpha^2 & \alpha^{\frac{5}{2}} & \alpha^3 \\ 1 & \alpha^2 & \alpha^3 & \alpha^{\frac{1}{2}} & \alpha^{\frac{3}{2}} & \alpha^{\frac{5}{2}} \\ 1 & \alpha^3 & \alpha & \alpha^{\frac{5}{2}} & \alpha^{\frac{1}{2}} & \alpha^2 \\ 1 & \alpha^{\frac{1}{2}} & \alpha^{\frac{5}{2}} & \alpha & \alpha^3 & \alpha^{\frac{5}{2}} \end{bmatrix}$$

is the parity-check matrix of a BCH code $C(6, \eta)$ of length 6 and, by Theorem 5, the minimum Hamming distance is at least equal to 5.

4.2 Alternant codes

The construction of an alternant code through a semigroup ring is initiated in the following definition which is a generalization of [1, Definition 3.3].

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*

$$H = \begin{bmatrix} \omega_1 & \omega_2 & \cdots & \omega_n \\ \omega_1\alpha_1 & \omega_2\alpha_2 & \cdots & \omega_n\alpha_n \\ \omega_1\alpha_1^2 & \omega_2\alpha_2^2 & \cdots & \omega_n\alpha_n^2 \\ \vdots & \vdots & \ddots & \vdots \\ \omega_1\alpha_1^{2r-1} & \omega_2\alpha_2^{2r-1} & \cdots & \omega_n\alpha_n^{2r-1} \end{bmatrix},$$

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

In the Definition 3 we have that

$$H = \begin{bmatrix} 1 & \cdots & 1 \\ \alpha_1 & \cdots & \alpha_n \\ \vdots & \ddots & \vdots \\ \alpha_1^{2r-1} & \cdots & \alpha_n^{2r-1} \end{bmatrix} \begin{bmatrix} w_1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & w_n \end{bmatrix} = LM.$$

The following theorem generalizes [1, Theorem 3.2].

Theorem 6. *The alternant code $C(n, \eta, \omega)$ has minimum Hamming distance $d \geq 2r + 1$.*

Proof. Suppose c is a nonzero codeword in $C(n, \eta, \omega)$ such that the weight $w_H(c) \leq 2r$. Then, $cH^T = c(LM)^T = 0$. Setting $b = cM^T$, we obtain $w_H(b) = w_H(c)$ because M is diagonal and invertible. Thus, $bL^T = 0$. Deleting $n - 2r$ columns of the matrix L that correspond to zeros of the codeword, we have that the new matrix L' is a Vandermonde's one. By Lemma 3, it follows that the determinant of L' is a unit in $\Re$. Thus, the unique possibility for c is the all zero codeword. □

Example 3. Referring to Example 2, if $\eta = (\alpha^2, 1, \alpha, \alpha^{\frac{1}{2}}, \alpha^3, \alpha^{\frac{3}{2}})$ is the locator vector, $\omega = (1, \alpha^{\frac{1}{2}}, \alpha^3, \alpha, \alpha^{\frac{3}{2}}, \alpha^{\frac{5}{2}})$ and $r = 2$, then the following matrix

$$H = \begin{bmatrix} 1 & \alpha^{\frac{1}{2}} & \alpha^3 & \alpha & \alpha^{\frac{3}{2}} & \alpha^{\frac{5}{2}} \\ \alpha^2 & \alpha^{\frac{1}{2}} & \alpha^{\frac{1}{2}} & \alpha^{\frac{3}{2}} & \alpha & \alpha^{\frac{1}{2}} \\ \alpha^{\frac{1}{2}} & \alpha^{\frac{1}{2}} & \alpha^{\frac{3}{2}} & \alpha^2 & \alpha^{\frac{1}{2}} & \alpha^2 \\ \alpha^{\frac{5}{2}} & \alpha^{\frac{1}{2}} & \alpha^{\frac{5}{2}} & \alpha^{\frac{5}{2}} & 1 & 1 \end{bmatrix}$$

is the parity-check matrix of an alternant code $C(6, \eta, \omega)$ of length 6 and, by Theorem 6, the minimum Hamming distance is at least equal to 5.

5 Goppa and Srivastava codes through a semigroup ring

In this section, we present a construction of Goppa and Srivastava codes through semigroup rings.

5.1 Goppa codes

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 in [1]. A Goppa code is 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_s as defined in previous section. Let $\alpha^{\frac{1}{2}}$ be a generator of the cyclic group G_s, where $s = p^{2mt} - 1$. Let

$$h\left(X^{\frac{1}{2}}\right) = h_0 + h_{\frac{1}{2}}X^{\frac{1}{2}} + \cdots + h_{\frac{2r}{2}}\left(X^{\frac{1}{2}}\right)^{2r}$$

be a polynomial with coefficients in $\Re$, where $h_{\frac{2r}{2}} \neq 0$. Let $T = \{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ be a subset of distinct elements of G_s such that $h(\alpha_i)$ are units from $\Re$, for $i = 1, 2, \cdots, n$.

The following definition generalizes [1, Definition 4.1].

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

$$H = \begin{bmatrix} h(\alpha_1)^{-1} & \cdots & h(\alpha_n)^{-1} \\ \alpha_1 h(\alpha_1)^{-1} & \cdots & \alpha_n h(\alpha_n) \\ \vdots & \ddots & \vdots \\ \alpha_1^{2r-1} h(\alpha_1)^{-1} & \cdots & \alpha_n^{2r-1} h(\alpha_n) \end{bmatrix}, \tag{5.1}$$

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 an vector consisting of elements of* G_s.

The following definition generalizes [1, Definition 4.2].

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

1. *If* $h(X^{\frac{1}{2}})$ *is irreducible, then* $C(T, h)$ *is called an* irreducible Goppa code.

2. *If* $c = (c_1, c_2, \ldots, c_n) \in C(T, h)$ *and* $c = (c_n, \ldots, c_2, c_1) \in C(T, h)$, *then* $C(T, h)$ *is called a* reversible Goppa code.

3. *If* $h(X^{\frac{1}{2}}) = (X^{\frac{1}{2}} - \alpha)^{2r-1}$, *then* $C(T, h)$ *is called a* cumulative Goppa code.

4. *If* $h(X^{\frac{1}{2}})$ *has no multiple zeros, then* $C(T, h)$ *is called a* separable Goppa code.

Remark 2. Let $C(T, h)$ be a Goppa code. Then

1. $C(T, h)$ is a linear code.

2. For a code with Goppa polynomial $h_l(X^{\frac{1}{2}}) = (X^{\frac{1}{2}} - \beta_l)^{2r_l}$, where $\beta_l \in G_s$,

$$H_l = \begin{bmatrix} (\alpha_1 - \beta_l)^{-2r_l} & (\alpha_2 - \beta_l)^{-2r_l} & \cdots & (\alpha_n - \beta_l)^{-2r_l} \\ \alpha_1(\alpha_1 - \beta_l)^{-2r_l} & \alpha_2(\alpha_2 - \beta_l)^{-2r_l} & \cdots & \alpha_n(\alpha_n - \beta_l)^{-2r_l} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{2r_l-1}(\alpha_1 - \beta_l)^{-2r_l} & \alpha_2^{2r_l-1}(\alpha_2 - \beta_l)^{-2r_l} & \cdots & \alpha_n^{2r_l-1}(\alpha_n - \beta_l)^{-2r_l} \end{bmatrix},$$

which is row equivalent to

$$\begin{bmatrix} (\alpha_1 - \beta_l)^{-2r_l} & (\alpha_2 - \beta_l)^{-2r_l} & \cdots & (\alpha_n - \beta_l)^{-2r_l} \\ (\alpha_1 - \beta_l)^{-(2r_l-1)} & (\alpha_2 - \beta_l)^{-(2r_l-1)} & \cdots & (\alpha_n - \beta_l)^{-(2r_l-1)} \\ \vdots & \vdots & \ddots & \vdots \\ (\alpha_1 - \beta_l)^{-1} & (\alpha_2 - \beta_l)^{-1} & \cdots & (\alpha_n - \beta_l)^{-1} \end{bmatrix}.$$

Consequently, if

$$h\left(X^{\frac{1}{2}}\right) = \left(X^{\frac{1}{2}} - \beta_l\right)^{2r_l} = \prod_{i=1}^{2k} h_l\left(X^{\frac{1}{2}}\right)$$

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

$$H = \begin{bmatrix} H_1 \\ H_2 \\ \vdots \\ H_{2k} \end{bmatrix}$$

3. A BCH code is a special case of a Goppa code. To verify this, choose $h(X^{\frac{1}{2}}) = (X^{\frac{1}{2}})^{2r}$ and $T = \{\alpha_1, \alpha_2, \cdots, \alpha_n\}$, where $\alpha_i \in G_s$, for all $i = 1, 2, \cdots, n$. By Equation (5.1) it follows that

$$H = \begin{bmatrix} \alpha_1^{-2r} & \alpha_2^{-2r} & \cdots & \alpha_n^{-2r} \\ \alpha_1^{1-2r} & \alpha_2^{1-2r} & \cdots & \alpha_n^{1-2r} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{-1} & \alpha_2^{-1} & \cdots & \alpha_n^{-1} \end{bmatrix},$$

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

The following theorem generalizes [1, Theorem 4.1].

Theorem 7. *The Goppa code $C(T, h)$ has minimum Hamming distance $d \geq 2r + 1$.*

Proof. The code $C(T, h)$ is an alternant code $C(n, \eta, \omega)$ with $\eta = (\alpha_1, \alpha_2, \ldots, \alpha_n)$ and $\omega = (h(\alpha_1)^{-1}, h(\alpha_2)^{-1}, \ldots, h(\alpha_n)^{-1})$. Therefore, by Theorem 6, $C(T, h)$ has minimum Hamming distance $d \geq 2r + 1$. □

Example 4. Referring to Example 2, if $T = \{1, \alpha, \alpha^{\frac{1}{2}}, \alpha^2, \alpha^{\frac{3}{2}}, \alpha^{\frac{5}{2}}\}$, $h(X^{\frac{1}{2}}) = (X^{\frac{1}{2}})^2 + X^{\frac{1}{2}} + 1$ then $\eta = (1, \alpha, \alpha^{\frac{1}{2}}, \alpha^2, \alpha^{\frac{3}{2}}, \alpha^3)$ and $\omega = (1, \alpha^2, \alpha, \alpha^{\frac{1}{2}}, \alpha, \alpha^{\frac{5}{2}})$. Therefore

$$H = \begin{bmatrix} 1 & \alpha^2 & \alpha & \alpha^{\frac{1}{2}} & \alpha & \alpha^{\frac{5}{2}} \\ 1 & \alpha^3 & \alpha^{\frac{3}{2}} & \alpha^{\frac{5}{2}} & \alpha^{\frac{5}{2}} & \alpha^2 \end{bmatrix}$$

is the parity check matrix of a Goppa code over B of length 6 and, by Theorem 7, the minimum Hamming distance is at least equal to 5.

5.2 Srivastava codes

Srivastava codes form an interesting subclass of alternant codes which is similar to the unpublished work [12], which was proposed by J.N. Srivastava in 1967. A class of linear codes which are not cyclic and defined in the form of parity-check matrices

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

where $\alpha_1, \alpha_2, \ldots, \alpha_r$ are distinct elements from $GF(q^m)$ and $\beta_1, \beta_2, \ldots, \beta_n$ are all the elements in $GF(q^m)$, except $0, \alpha_1^{-1}, \alpha_2^{-1}, \ldots, \alpha_r^{-1}$ and $l \geq 0$.

Now, we can define Srivastava codes over semigroup ring as a generalization of [1, Definition 4.1].

Definition 6. *A* shortened Srivastava code *of length $n \leq s$ is a code over B having parity check matrix*

$$H = \begin{bmatrix} \frac{\alpha_1^l}{\alpha_1-\beta_1} & \frac{\alpha_2^l}{\alpha_2-\beta_1} & \cdots & \frac{\alpha_n^l}{\alpha_n-\beta_1} \\ \frac{\alpha_1^l}{\alpha_1-\beta_2} & \frac{\alpha_2^l}{\alpha_1-\beta_2} & \cdots & \frac{\alpha_n^l}{\alpha_n-\beta_2} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{\alpha_1^l}{\alpha_1-\beta_{2r}} & \frac{\alpha_2^l}{\alpha_1-\beta_{2r}} & \cdots & \frac{\alpha_n^l}{\alpha_n-\beta_{2r}} \end{bmatrix}, \tag{5.2}$$

where r, l are positive integers and $\alpha_1, \ldots, \alpha_n$, $\beta_1, \beta_2, \ldots, \beta_{2r}$ are $n + 2r$ distinct elements of G_s.

The following theorem generalizes [1, Theorem 4.2].

Theorem 8. *The Srivastava code has minimum Hamming distance $d \geq 2r + 1$.*

Proof. The minimum Hamming distance of Srivastava code is at least $2r + 1$ if and only if every combination of $2r$ or fewer columns of H is linearly independent over $\Re$, or equivalently that the submatrix

$$H_1 = \begin{bmatrix} \frac{\alpha_{i_1}^l}{\alpha_{i_1}-\beta_1} & \frac{\alpha_{i_2}^l}{\alpha_{i_2}-\beta_1} & \cdots & \frac{\alpha_{i_r}^l}{\alpha_{i_{2r}}-\beta_1} \\ \frac{\alpha_{i_1}^l}{\alpha_{i_1}-\beta_2} & \frac{\alpha_2^l}{\alpha_{i_2}-\beta_2} & \cdots & \frac{\alpha i_r{}^l}{\alpha_{i_{2r}}-\beta_2} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{\alpha_{i_1}^l}{\alpha_{i_1}-\beta_{2r}} & \frac{\alpha_{i_2}^l}{\alpha_{i_2}-\beta_{2r}} & \cdots & \frac{\alpha_{i_r}^l}{\alpha_{i_{2r}}-\beta_{2r}} \end{bmatrix} \tag{5.3}$$

is nonsingular. The determinant of this submatrix can be expressed as

$$\det(H_1) = \left(\alpha_{i_1}, \alpha_{i_2}, \ldots, \alpha_{i_{2r}}\right)^l \det(H_2),$$

where the matrix H_2 is given by

$$H_2 = \begin{bmatrix} \frac{1}{\alpha_{i_1}-\beta_1} & \frac{1}{\alpha_{i_2}-\beta_1} & \cdots & \frac{1}{\alpha_{i_{2r}}-\beta_1} \\ \frac{1}{\alpha_{i_1}-\beta_2} & \frac{1}{\alpha_{i_2}-\beta_2} & \cdots & \frac{1}{\alpha_{i_{2r}}-\beta_2} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{1}{\alpha_{i_1}-\beta_{2r}} & \frac{1}{\alpha_{i_2}-\beta_{2r}} & \cdots & \frac{1}{\alpha_{i_{2r}}-\beta_{2r}} \end{bmatrix}. \tag{5.4}$$

Note that $\det(H_2)$ is a Cauchy determinant of order $2r$ and therefore we conclude that the determinant of the matrix H_1 is given by

$$\begin{aligned} \det(H_1) \;=\; & (\alpha_{i_1}, \ldots, \alpha_{i_{2r}})^l \frac{(-1)^{\binom{2r}{2}}}{v(\alpha_{i_1})v(\alpha_{i_2})\cdots v(\alpha_{i_{2r}})} \\ & \times \phi\,(\alpha_{i_1}, \ldots, \alpha_{i_{2r}})\,\phi\,(\beta_1, \beta_2, \ldots, \beta_{2r}), \end{aligned}$$

where $\phi(\alpha_{i_1}, \ldots, \alpha_{i_{2r}}) = (\alpha_{i_j} - \alpha_{i_h})$ and $v(X) = (X-\beta_1)(X-\beta_2)\cdots(X-\beta_{2r})$. By Lemma 3 it follows that $\det(H_1)$ is a unit in $\Re$ and therefore $d \geq 2r+1$. □

The following definition generalizes [1, Definition 4.4].

Definition 7. *Let $\alpha_1, \ldots, \alpha_n, \beta_1, \beta_2, \ldots, \beta_{2r}$ be $n + 2r$ distinct elements of G_s, $\omega_1, \ldots, \omega_n$ be elements of G_s. A* generalized Srivastava code *of length $n \leq s$ is a code over B that has parity check matrix*

$$H = \begin{bmatrix} H_1 \\ H_2 \\ \vdots \\ H_{2r} \end{bmatrix}, \tag{5.5}$$

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 $j = 1, 2, \cdots, 2r$.

The following theorem generalizes [1, Theorem 4.3].

Theorem 9. *The generalized Srivastava code has minimum Hamming distance* $d \geq (2r)l + 1$.

Proof. The proof of this theorem requires nothing else than an application of Remark 2 and Theorem 8, since the matrices given in Equations (5.2) and (5.5) are equivalents, where $h(X^{\frac{1}{2}}) = (X^{\frac{1}{2}} - \beta_i)^l$. □

Example 5. Referring to Example 2, if $l = 2$, $\{\alpha_1, \alpha_2, \cdots, \alpha_5\} = \{1, \alpha^{\frac{5}{2}}, \alpha, \alpha^3, \alpha^2\}$, $\{\beta_1, \beta_2\} = \{\alpha^{\frac{1}{2}}, \alpha^{\frac{3}{2}}\}$, $\{w_1, w_2, \cdots, w_5\} = \{\alpha, 1, \alpha^{\frac{1}{2}}, \alpha^{\frac{5}{2}}, \alpha^2\}$, then the matrix

$$H = \begin{bmatrix} \frac{\alpha}{1-\alpha^{\frac{1}{2}}} & \frac{1}{\alpha^{\frac{5}{2}}-\alpha^{\frac{1}{2}}} & \frac{\alpha^{\frac{1}{2}}}{\alpha-\alpha^{\frac{1}{2}}} & \frac{\alpha^{\frac{5}{2}}}{\alpha^3-\alpha^{\frac{1}{2}}} & \frac{\alpha^2}{\alpha^2-\alpha^{\frac{1}{2}}} \\ \frac{\alpha}{(1-\alpha^{\frac{1}{2}})^2} & \frac{1}{(\alpha^{\frac{5}{2}}-\alpha^{\frac{1}{2}})^2} & \frac{\alpha^{\frac{1}{2}}}{(\alpha-\alpha^{\frac{1}{2}})^2} & \frac{\alpha^{\frac{5}{2}}}{(\alpha^3-\alpha^{\frac{1}{2}})^2} & \frac{\alpha^2}{(\alpha^2-\alpha^{\frac{1}{2}})^2} \\ \frac{\alpha}{1-\alpha^{\frac{3}{2}}} & \frac{1}{\alpha^{\frac{5}{2}}-\alpha^{\frac{3}{2}}} & \frac{\alpha^{\frac{1}{2}}}{\alpha-\alpha^{\frac{3}{2}}} & \frac{\alpha^{\frac{5}{2}}}{\alpha^3-\alpha^{\frac{3}{2}}} & \frac{\alpha^2}{\alpha^2-\alpha^{\frac{3}{2}}} \\ \frac{\alpha}{(1-\alpha^{\frac{3}{2}})^2} & \frac{1}{(\alpha^{\frac{5}{2}}-\alpha^{\frac{3}{2}})^2} & \frac{\alpha^{\frac{1}{2}}}{(\alpha-\alpha^{\frac{3}{2}})^2} & \frac{\alpha^{\frac{5}{2}}}{(\alpha^3-\alpha^{\frac{3}{2}})^2} & \frac{\alpha^2}{(\alpha^2-\alpha^{\frac{3}{2}})^2} \end{bmatrix}$$

is the parity-check matrix of a generalized Srivastava code of length 5 and, by Theorem 9, the minimum Hamming distance is to 5.

6 Conclusion

In [1], there is a treatment of cyclic, BCH, alternant, Goppa and Srivastava codes over a finite ring with length n. Due to the constraints in the method of polynomial rings, used in [1], we proved a more accurate method of getting cyclic, BCH, alternant, Goppa and Srivastava codes over finite rings with length n. In this work, we used the semigroup rings instead of the polynomial rings. Interestingly, we have used the same lines as credited in [1].

Any linear code detects $d - 1$ errors, where d is a minimum distance of a code and correct $\lfloor \frac{d-1}{2} \rfloor$ errors. In the case of [1] for r number of check symbols: $d \geq r + 1$, and $\lfloor \frac{r+1-1}{2} \rfloor = \lfloor \frac{r}{2} \rfloor$ but the method adopted in this paper, $d \geq 2r + 1$. This shows that codes detect at least $2r$ errors and correct $\lfloor \frac{2r+1-1}{2} \rfloor = \lfloor \frac{2r}{2} \rfloor = r$ errors. The linear codes defined in this paper on

polynomial and semigroup rings have the same code rates. However, our novel method provides better error correcting capabilities compared with previous constructions of codes considered in [1].

Acknowledgments. The authors would like to thank the anonymous reviewers for their insightful comments that greatly improved the quality of this work.

REFERENCES

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

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

[3] J. Cazaran and 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 and D. Vertigan, *An algorithm for computing the minimum distances of extensions of BCH codes embedded in semigroup rings*. Semigroup 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, *Multiplicative Ideal Theory*. Marcel Dekker, New York (1972).

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

[12] H.J. Helgert, *Srivastava Codes*. IEEE Trans. Inform. Theory, **IT-18**(2) (1972), 292–297.