TEMA Tend. Mat. Apl. Comput., **12**, No. 2 (2011), 79-89.
doi: 10.5540/tema.2011.012.02.0079
© *Uma Publicação da Sociedade Brasileira de Matemática Aplicada e Computacional.*

A Note on Linear Codes over Semigroup Rings[1]

A.A. de ANDRADE[2], Department of Mathematics, IBILCE, UNESP - Univ Estadual Paulista, 15054-000, São José do Rio Preto, SP, Brasil.

T. SHAH, A. KHAN[3], Department of Mathematics, Quaid-i-Azam University, Islamabad, Pakistan.

Abstract. In this paper, we introduced new construction techniques of BCH, alternant, Goppa, Srivastava codes through the semigroup ring $B[X; \frac{1}{3}\mathbb{Z}_0]$ instead of the polynomial ring $B[X; \mathbb{Z}_0]$, where B is a finite commutative ring with identity, and for these constructions we improve the several results of [1]. After this, we present a decoding principle for BCH, alternant and Goppa codes which is based on modified Berlekamp-Massey algorithm. This algorithm corrects all errors up to the Hamming weight $t \leq r/2$, i.e., whose minimum Hamming distance is $r + 1$.

Key-words. Semigroup ring, BCH code, alternant code, Goppa code, Srivastava code.

1. Introduction

Having the construction of codes over rings as the main motivation for the linear codes, and in particular of BCH, alternant, Goppa and Srivastava codes, in this paper we address the constructions these codes over semigroup rings. In [1] Andrade and Palazzo discussed the BCH, alternant, Goppa and Srivastava codes through the polynomial ring $B[X; \mathbb{Z}_0]$, where B is finite commutative ring with identity and $\mathbb{Z}_0 = \mathbb{Z}^+ \cup \{0\}$. In [2] T. Shah et. al. considered linear codes over the semigroup ring $B[X; \frac{1}{2}\mathbb{Z}_0]/(X^n - 1)$. In this paper, we introduce construction techniques of these codes through the semigroup ring $B[X; \frac{1}{3}\mathbb{Z}_0]$ instead of the polynomial ring $B[X; \mathbb{Z}_0]$, where we improve the results of [1].

In this work we take B as a finite commutative ring with unity and in the same spirit of [1], we fix a cyclic subgroup of group of units of the ring $B[X; \frac{1}{3}\mathbb{Z}_0]/(X^n - 1)$. The factorization of $X^s - 1$ over the group of units of $B[X; \frac{1}{3}\mathbb{Z}_0]/(X^n - 1)$ is the main problem. These processes of constructing linear codes through the semigroup ring $B[X; \frac{1}{3}\mathbb{Z}_0]$ are very similar to linear codes over finite rings and this work needs Galois extension rings, because some of the properties of Galois extension fields do not hold here.

This paper is organized as follows. In Section 2, we give some basic results on semigroups and semigroup rings necessary for the construction of the codes.

[1] The authors are very grateful to FAPESP for the financial support, 2007/56052-8.

[2] andrade@ibilce.unesp.br

[3] stariqshah@gmail.com, atlasmaths@yahoo.com

Recebido em 26 Abril 2010; Aceito em 28 Abril 2011.

In Section 3, we address the constructions of BCH and alternant codes through a semigroup ring instead of a polynomial ring. In Section 4, we describe a construction of Goppa and Srivastava codes through a semigroup ring. In Section 5, we present a decoding principle for BCH, alternant and Goppa codes constructed through a semigroup ring, which is based on modified Berlekamp-Massey algorithm [3]. This algorithm corrects all errors up to the Hamming weight $t \leq r/2$, i.e., whose minimum Hamming distance is $r+1$.

2. Basic Results

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 the binary operations of 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 set J is known as the *semigroup ring* of S over B. If S is a monoid, then J is called a monoid ring. The ring J is represented as $B[S]$ whenever S is a multiplicative semigroup and the 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 $\sum_{i=1}^{n} f(s_i)X^{s_i} = \sum_{i=1}^{n} f_i X^{s_i}$, where $f_i \neq 0$ and $s_i \neq s_j$ for $i \neq j$.

The concepts of degree and order are not generally defined in semigroup rings. But if we consider S to be a totally ordered semigroup, we can define the degree and order of an element of semigroup ring $B[X; S]$ in the following manner; if $f = \sum_{i=1}^{n} f_i X^{s_i}$ is the canonical form of the nonzero element $f \in B[X; S]$, 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 $\operatorname{ord}(f) = s_1$. Now, if B is an integral domain, then $\deg(fg)$ =$\deg(f)$+$\deg(g)$ and $\operatorname{ord}(fg)$ =$\operatorname{ord}(f)$+$\operatorname{ord}(g)$, for $f, g \in B[X; S]$.

If S is $\mathbb{Z}_0$ and B is an associative ring, the semigroup ring J is simply the polynomial ring $B[X]$. Obviously $B[X] = B[X; \mathbb{Z}_0] \subset B[X; \frac{1}{3}\mathbb{Z}_0]$. Furthermore, it is noticed that in $B[X; \frac{1}{3}\mathbb{Z}_0]$ we can define the degree of a pseudo polynomial because $\frac{1}{3}\mathbb{Z}_0$ is an ordered monoid.

3. BCH and Alternant Codes

In this section, we assume that (B, N) is a finite local commutative ring with unity and residue field $\mathbb{K} = \frac{B}{N} \cong GF(p^m)$, where p is a prime and m a positive integer. The natural projection $\pi : B[X; \frac{1}{3}\mathbb{Z}_0] \to \mathbb{K}[X; \frac{1}{3}\mathbb{Z}_0]$ is defined by $\pi(a(X^{\frac{1}{3}})) = \overline{a}(X^{\frac{1}{3}})$, i.e., $\pi(\sum_{i=0}^{n} a_i X^{\frac{1}{3}i}) = \sum_{i=0}^{n} \overline{a_i} X^{\frac{1}{3}i}$, where $\overline{a_i} = a_i + N$, for $i = 0, 1, \cdots, n$. Let $f(X^{\frac{1}{3}})$ be a monic pseudo polynomial of degree t in $B[X; \frac{1}{3}\mathbb{Z}_0]$ such that $\pi(f(X^{\frac{1}{3}}))$ is irreducible in $\mathbb{K}[X; \frac{1}{3}\mathbb{Z}_0]$. By [4, Theorem 7.2] it follows that $B[X; \frac{1}{3}\mathbb{Z}_0]$ can be accommodated as $B[X;\mathbb{Z}_0]$ and following [5, Theorem XIII.7] it follows that $f(X^{\frac{1}{3}})$ is irreducible in $B[X;\frac{1}{3}\mathbb{Z}_0]$. The ring $\Re = \frac{B[X;\frac{1}{3}\mathbb{Z}_0]}{(f(X^{\frac{1}{3}}))}$ is a local finite commutative ring with identity, whose maximal ideal is $N_2 = \frac{N_1}{(f(X^{\frac{1}{3}}))}$, where $N_1 = (N, f(X^{\frac{1}{3}}))$ and the residue field is $\mathbb{K}_1 = \frac{\Re}{N_2} \cong \frac{B[X;\frac{1}{3}\mathbb{Z}_0]}{(N,f(X^{\frac{1}{3}}))} \cong \frac{\mathbb{K}[X;\frac{1}{3}\mathbb{Z}_0]}{(\pi(f(X^{\frac{1}{3}})))} \cong GF(p^{3mt})$, and $\mathbb{K}_1^*$ is the multiplicative group of $\mathbb{K}_1$ whose order is $p^{3mt} - 1$.

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 $s = p^{3mt} - 1$ [5, Theorem XVIII.2].

Definition 3.1. *Let $\eta = (\alpha_1, \cdots, \alpha_n)$ be a vector consisting of distinct elements of G_s, and let $\omega = (\omega_1, \cdots, \omega_n)$ be an arbitrary vector consisting of elements of G_s. The set of all vectors $(\omega_1 f(\alpha_1), \omega_2 f(\alpha_2), \cdots, \omega_n f(\alpha_n))$, where $f(z)$ ranges over all polynomials of degree at most $k - 1$, for $k \in \mathbb{N}$, with coefficients from $\Re$, defines a shortened code C of length $n \leq s$ over $\Re$.*

Definition 3.2. *A shortened BCH code $C(n, \eta)$ of length $n \leq s$ is a code over B that has parity-check matrix*

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

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.

Lemma 3.1. *If $\alpha^{\frac{1}{3}}$ is an element of G_s of order s, then the differences $\alpha^{\frac{1}{3}l_1} - \alpha^{\frac{1}{3}l_2}$ are units in $\Re$ if $0 \leq l_1 \neq l_2 \leq s - 1$.*

Proof. The element $\alpha^{\frac{1}{3}l_1} - \alpha^{\frac{1}{3}l_2}$ can be written as $-\alpha^{\frac{1}{3}l_2}(1 - \alpha^{\frac{1}{3}(l_1 - l_2)})$, where $l_1 > l_2$ and 1 denotes the unity of $\Re$. The factor $-\alpha^{\frac{1}{3}l_2}$ in the product is a unit. The second factor can be written as $1 - \alpha^{\frac{1}{3}j}$ for some integer j in the interval $[1, s-1]$. Now, if the element $1 - \alpha^{\frac{1}{3}j}$, for some $1 \leq j \leq s-1$, were not a unit in $\Re$, then $1 - \alpha^{\frac{1}{3}j} \in N_2$, and consequently, $(\pi(\alpha^{\frac{1}{3}}))^j = \pi(1)$ for $j < s$. Since π is injective when restricted to G_s, it follows that $\pi(\alpha^{\frac{1}{3}})$ has order $j < s$, which is a contradiction. Thus $1 - \alpha^{\frac{1}{3}j} \in \Re$ are units for all $j = 1, 2, \cdots, s - 1$. □

Theorem 3.1. *The minimum Hamming distance of a BCH code $C(n, \eta)$ satisfies $d \geq r + 1$.*

Proof. Assume that c is a nonzero codeword in $C(n, \eta)$ such that $w_H(c) \leq r$. Then $cH^T = 0$. Deleting $n - r$ columns of the matrix H corresponding to zeros of the codeword, it follows that the new matrix H' is Vandermonde's one. By Lemma 3.1, it follows that the determinant is a unit in $\Re$. Thus the only possibility for c is the all zero codeword. □

Example 3.1. *Let* $B = GF(2)[i]$ *and* $\Re = \frac{B[X;\frac{1}{3}\mathbb{Z}_0]}{(f(X^{\frac{1}{3}}))}$, *where* $f(X^{\frac{1}{3}}) = (X^{\frac{1}{3}})^3 + X^{\frac{1}{3}} + 1$ *is irreducible over* B. *If* $\alpha^{\frac{1}{3}}$ *is a root of* $f(X^{\frac{1}{3}})$, *then* $\alpha^{\frac{1}{3}}$ *generates a cyclic group* G_s *of order* $s = 2^3 - 1 = 7$. *Let* $\eta = (1, \alpha, \alpha^{\frac{1}{3}}, \alpha^{\frac{2}{3}}, \alpha^2, \alpha^{\frac{4}{3}})$ *be the locator vector consisting of distinct elements of* G_7. *If* $r = 3$, *then the following matrix*

$$H = \begin{bmatrix} 1 & \alpha & \alpha^{\frac{1}{3}} & \alpha^{\frac{2}{3}} & \alpha^2 & \alpha^{\frac{4}{3}} \\ 1 & \alpha^2 & \alpha^{\frac{2}{3}} & \alpha^{\frac{4}{3}} & \alpha^{\frac{5}{3}} & \alpha^{\frac{1}{3}} \\ 1 & \alpha^{\frac{2}{3}} & \alpha & \alpha^2 & \alpha^{\frac{4}{3}} & \alpha^{\frac{5}{3}} \end{bmatrix}$$

is the parity-check matrix of a BCH code $C(6, \eta)$ *of length* 6 *and, by Theorem 3.1, the minimum Hamming distance at least equal to* 4.

Definition 3.3. *A shortened alternant code* $C(n, \eta, \omega)$ *of length* $n \leq s$ *is a code over* B *that has parity-check matrix*

$$H = \begin{bmatrix} \omega_1 & \cdots & \omega_n \\ \omega_1\alpha_1 & \cdots & \omega_n\alpha_n \\ \omega_1\alpha_1^2 & \cdots & \omega_n\alpha_n^2 \\ \vdots & \ddots & \vdots \\ \omega_1\alpha_1^{r-1} & \cdots & \omega_n\alpha_n^{r-1} \end{bmatrix} = \begin{bmatrix} 1 & \cdots & 1 \\ \alpha_1 & \cdots & \alpha_n \\ \vdots & \ddots & \vdots \\ \alpha_1^{r-1} & \cdots & \alpha_n^{r-1} \end{bmatrix} \begin{bmatrix} w_1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & w_n \end{bmatrix} = LM,$$

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 3.2. *An alternant code* $C(n, \eta, \omega)$ *has minimum Hamming distance* $d \geq r + 1$.

Proof. Assume that c is a nonzero codeword in $C(n, \eta, \omega)$ such that the weight $w_H(c) \leq r$. Then $cH^T = c(LM)^T = 0$. Setting $b = cM^T$ it follows that $w_H(b) = w_H(c)$ since M is diagonal and invertible. Thus $bL^T = 0$. Deleting $n - r$ columns of the matrix L that correspond to zeros of the codeword, it follows that the new matrix L' is Vandermonde's one. By Lemma 3.1, it follows that the determinant is a unit in $\Re$. Thus, the unique possibility for c is the all zero codeword. □

Example 3.2. *Referring to Example 3.1, if* $\eta = (\alpha^{\frac{1}{3}}, \alpha^2, 1, \alpha^{\frac{2}{3}}, \alpha, \alpha^{\frac{5}{3}})$ *is the locator vector,* $\omega = (\alpha^2, \alpha^{\frac{1}{3}}, \alpha, \alpha^{\frac{5}{3}}, \alpha^{\frac{4}{3}}, 1)$ *and* $r = 3$, *then the following matrix*

$$H = \begin{bmatrix} \alpha^2 & \alpha^{\frac{1}{3}} & \alpha & \alpha^{\frac{5}{3}} & \alpha^{\frac{4}{3}} & 1 \\ 1 & 1 & \alpha & 1 & 1 & \alpha^{\frac{5}{3}} \\ \alpha^{\frac{1}{3}} & \alpha^2 & \alpha & \alpha^{\frac{2}{3}} & \alpha & \alpha \end{bmatrix}$$

is the parity-check matrix of an alternant code $C(6, \eta, \omega)$ *of length* 6 *and, by Theorem 3.2, the minimum Hamming distance at least equal to* 4.

4. Goppa and Srivastava 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 by Andrade and Palazzo [1] through polynomial rings. Goppa codes are described in terms of a Goppa polynomial $h(X)$ and 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 $h(X) = h_0 + h_1X + h_2X^2 + \cdots + h_rX^r$ be a polynomial with coefficients in $\Re$ and $h_r \neq 0$. 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 4.1. *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*

$$H = \begin{bmatrix} h(\alpha_1)^{-1} & \cdots & h(\alpha_n)^{-1} \\ \alpha_1 h(\alpha_1)^{-1} & \cdots & \alpha_n h(\alpha_n) \\ \vdots & \ddots & \vdots \\ \alpha_1^{r-1} h(\alpha_1)^{-1} & \cdots & \alpha_n^{r-1} h(\alpha_n) \end{bmatrix}, \tag{4.1}$$

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 a vector consisting of elements of G_s.

Definition 4.2. *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 $h(X) = (X - \beta)^{r-1}$, 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 code.*

Remark 4.1. *Let $C(T, h)$ be a Goppa code.*

1. *The code $C(T, h)$ is a linear code.*
2. *A Goppa code with Goppa polynomial $h_l(X) = (X - \beta_l)^{r_l}$, where $\beta_l \in G_s$, has parity-check matrix*

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

which is row equivalent to the matrix

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

Consequently, if $h(X) = (X-\beta_l)^{r_l} = \prod_{i=1}^{k} h_l(x)$ *then the Goppa code is the intersection of the codes with* $h_l(X) = (X-\beta_l)^{r_l}$*, for* $l = 1, 2, \cdots, k$*, and its parity check matrix is given by* $H = [\ H_1 \quad H_2 \quad \cdots \quad H_k\ ]^T$*, where* T *indicates the transposition.*

3. *A BCH code is a special case of a Goppa code. To verify this, choose* $h(X) = X^r$ *and* $T = \{\alpha_1, \alpha_2, \cdots, \alpha_n\}$*, where* $\alpha_i \in G_s$*, for all* $i = 1, 2, \cdots, n$*. Then from Equation (4.1) it follows that*

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

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

Theorem 4.1. *A Goppa code* $C(T, h)$ *has minimum Hamming distance* $d \geq r+1$*.*

Proof. A Goppa code $C(T, h)$ is an alternant code $C(n, \eta, \omega)$, where $\eta = (\alpha_1, \alpha_2, \cdots, \alpha_n)$ is the locator vector and $\omega = (h(\alpha_1)^{-1}, h(\alpha_2)^{-1} \cdots, h(\alpha_n)^{-1})$. Therefore, by Theorem 3.2, it follows that $C(T, h)$ has minimum distance $d \geq r+1$. □

Example 4.1. *Referring to Example 3.1, if* $r = 3$, $h(X) = X^3+X^2+X+1$ *and* $T = \{\alpha, \alpha^2, \alpha^{\frac{1}{3}}, \alpha^{\frac{2}{3}}, \alpha^{\frac{4}{3}}, \alpha^{\frac{5}{3}}\}$ *then* $\eta = (\alpha, \alpha^2, \alpha^{\frac{1}{3}}, \alpha^{\frac{2}{3}}, \alpha^{\frac{5}{3}}, \alpha^{\frac{4}{3}})$ *and* $\omega = (\alpha^{\frac{2}{3}}, \alpha^{\frac{1}{3}}, \alpha^{\frac{5}{3}}, \alpha, \alpha^2, \alpha^{\frac{2}{3}})$. *Therefore*

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

is the parity-check matrix of a Goppa code over B *of length* 6 *and, by Theorem 4.1, the minimum Hamming distance is at least equal to* 4*.*

We define Srivastava codes over semigroup ring, which is an interesting subclass of alternant codes which is similar to unpublished work [6], which is proposed by J. N. Srivastava in 1967, as a class of linear codes which are not cyclic having parity-check matrices given by

$$H = (a_{i,j})_{1 \leq i \leq r, 1 \leq j \leq n},$$

where $a_{ij} = \frac{\alpha_j^l}{1-\alpha_i\beta_j}$ for $1 \leq i \leq r, 1 \leq j \leq n$, $\alpha_1, \alpha_2, \cdots, \alpha_r$ are distinct elements from $GF(q^m)$ and $\beta_1, \beta_2, \cdots, \beta_n$ are all the elements of $GF(q^m)$, with $\beta_j \neq \alpha_j^{-1}$ and $\beta_j \neq 0$.

Definition 4.3. *A shortened Srivastava code of length $n \leq s$ is a code over B having parity-check matrix*

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

where r, l are positive integers and $\alpha_1, \cdots, \alpha_n,\ \beta_1, \beta_2, \cdots, \beta_r$ are $n + r$ distinct elements of G_s.

Theorem 4.2. *A Srivastava code has minimum Hamming distance $d \geq r + 1$.*

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

$$H_1 = \begin{bmatrix} \frac{\alpha_{i_1}^l}{\alpha_{i_1}-\beta_1} & \frac{\alpha_{i_2}^l}{\alpha_{i_2}-\beta_1} & \cdots & \frac{\alpha_{i_r}^l}{\alpha_{i3_r}-\beta_1} \\ \frac{\alpha_{i_1}^l}{\alpha_{i_1}-\beta_2} & \frac{\alpha_2^l}{\alpha_{i_2}-\beta_2} & \cdots & \frac{\alpha_{i_r}^l}{\alpha_{i_r}-\beta_2} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{\alpha_{i_1}^l}{\alpha_{i_1}-\beta_r} & \frac{\alpha_{i_2}^l}{\alpha_{i_2}-\beta_r} & \cdots & \frac{\alpha_{i_r}^l}{\alpha_{i_r}-\beta_r} \end{bmatrix}$$

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

$$H_2 = \begin{bmatrix} \frac{1}{\alpha_{i_1}-\beta_1} & \frac{1}{\alpha_{i_2}-\beta_1} & \cdots & \frac{1}{\alpha_{i_{3_r}}-\beta_1} \\ \frac{1}{\alpha_{i_1}-\beta_2} & \frac{1}{\alpha_{i_2}-\beta_2} & \cdots & \frac{1}{\alpha_{i_{3_r}}-\beta_2} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{1}{\alpha_{i_1}-\beta_r} & \frac{1}{\alpha_{i_2}-\beta_r} & \cdots & \frac{1}{\alpha_{i_r}-\beta_r} \end{bmatrix}.$$

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

$$det(H_1) = (\alpha_{i_1}, \cdots, \alpha_{i_r})^l \frac{(-1)^{\binom{r}{2}} \phi(\alpha_{i_1}, \cdots, \alpha_{i3_r})\phi(\beta_1, \beta_2, \cdots, \beta_r)}{v(\alpha_{i_1})v(\alpha_{i_2}) \cdots v(\alpha_{i_r})},$$

where $\phi(\alpha_{i_1}, \cdots, \alpha_{i_r}) = \prod_{i_j < i_h}(\alpha_{i_j} - \alpha_{i_h})$ and $v(x) = (x - \beta_1)(x - \beta_2) \cdots (x - \beta_r)$. Then, by Lemma 3.1, it follows that $det(H_1)$ is a unit in $\Re$ and therefore $d \geq r + 1$. □

Example 4.2. *Referring to Example 3.1, if $n = 4$, $r = 3$, $l = 1$, $\{\alpha_1, \cdots, \alpha_4\} =$*

$\{1, \alpha, \alpha^2, \alpha^{\frac{1}{3}}\}$, $\{\beta_1, \beta_2, \beta_3\} = \{\alpha^{\frac{2}{3}}, \alpha^{\frac{4}{3}}, \alpha^{\frac{5}{3}}\}$ *then the matrix* H *given by*

$$\begin{bmatrix} \frac{1}{1-\alpha^{\frac{2}{3}}} & \frac{\alpha}{\alpha-\alpha^{\frac{2}{3}}} & \frac{\alpha^2}{\alpha^2-\alpha^{\frac{2}{3}}} & \frac{\alpha^{\frac{1}{3}}}{\alpha^{\frac{1}{3}}-\alpha^{\frac{2}{3}}} \\ \frac{1}{1-\alpha^{\frac{4}{3}}} & \frac{\alpha}{\alpha-\alpha^{\frac{4}{3}}} & \frac{\alpha^2}{\alpha^2-\alpha^{\frac{4}{3}}} & \frac{\alpha^{\frac{1}{3}}}{\alpha^{\frac{1}{3}}-\alpha^{\frac{4}{3}}} \\ \frac{1}{1-\alpha^{\frac{5}{3}}} & \frac{\alpha}{\alpha-\alpha^{\frac{5}{3}}} & \frac{\alpha^2}{\alpha^2-\alpha^{\frac{5}{3}}} & \frac{\alpha^{\frac{1}{3}}}{\alpha^{\frac{1}{3}}-\alpha^{\frac{5}{3}}} \end{bmatrix}$$

is the parity-check matrix of a Srivastava code with a minimum distance at least equal to 4.

Definition 4.4. *Assume that* $r = kl$ *and let* $\alpha_1, \cdots, \alpha_n$, $\beta_1, \beta_2, \cdots, \beta_k$ *be* $n + k$ *distinct elements of* G_s, $\omega_1, \cdots, \omega_n$ *be elements of* G_s. *A generalized Srivastava code of length* $n \leq s$ *is a code over* B *that has parity check matrix*

$$H = \begin{bmatrix} H_1 & H_2 & \cdots & H_k \end{bmatrix}^T, \tag{4.2}$$

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

Theorem 4.3. *A generalized Srivastava code has minimum Hamming distance* $d \geq kl + 1$.

Proof. The proof of this theorem requires nothing else than on application of Remark 4.1 and Theorem 4.2, since the matrices (4.1) and (4.2) are equivalent, where $g(Z) = (Z - \beta_i)^l$. □

5. Decoding Procedure

The decoding algorithm for BCH, alternant and Goppa codes consists of four major steps: (1) calculation of the syndromes, (2) calculation of the error-locator polynomial, (3) calculation of the error-location numbers, and (4) calculation of the error magnitudes. This algorithm is based on the modified Berlekamp-Massey algorithm [3] which corrects all errors up to the Hamming weight $t \leq r/2$, i.e., whose minimum Hamming distance is $r + 1$. The complexity of the proposed decoding algorithm is essentially the same as that these codes are defined over finite fields.

Let B, $\Re$ and G_s as defined in previous section. Let $\mathbf{c} = (c_1, c_2, \cdots, c_n)$ be a transmitted codeword and $\mathbf{b} = (b_1, b_2, \cdots, b_n)$ be the received vector. Thus the error vector is given by $\mathbf{e} = (e_1, e_2, \cdots, e_n) = \mathbf{b} - \mathbf{c}$. Let $\eta = (\alpha_1, \alpha_2, \cdots, \alpha_n) = (\beta^{k_1}, \beta^{k_2}, \cdots, \beta^{k_n})$ be a vector over $\mathcal{G}_s$, where β is a generator of G_s. Suppose that $\nu \leq t$ is the number of errors which occurred at locations $x_1 = \alpha_{i_1}, x_2 = \alpha_{i_2}, \cdots, x_\nu = \alpha_{i_\nu}$ with values $y_1 = e_{i_1}, y_2 = e_{i_2}, \cdots, y_\nu = e_{i_\nu}$. Since $\mathbf{s} = (s_1, s_2,$

$\cdots, s_r) = \mathbf{b}H^t = \mathbf{e}H^t$, it follows that the first r syndrome values s_l can be calculated from the received vector $\mathbf{b}$. Therefore $s_l = \sum_{j=1}^{n} e_j\alpha_j^l = \sum_{j=1}^{n} b_j\alpha_j^l$, for $l = 1, 2, \cdots, r$, for a BCH code; $s_l = \sum_{j=1}^{n} e_j w_j\alpha_j^l = \sum_{j=1}^{n} b_j w_j\alpha_j^l$, for $l = 0, 1, 2, \cdots, r-1$, for an alternant code; and $s_l = \sum_{j=1}^{n} e_j h(\alpha_j)^{-1}\alpha_j^l = \sum_{j=1}^{n} b_j h(\alpha_j)^{-1}\alpha_j^l$, for $l = 0, 1, 2, \cdots, r-1$, for a Goppa code.

The elementary symmetric functions $\sigma_1, \sigma_2, \cdots, \sigma_\nu$ of the error-location numbers $x_1, x_2, \cdots, x_\nu$ are defined as the coefficients of the polynomial $\sigma(Z) = \prod_{i=1}^{\nu}(Z - x_i) = \sum_{i=0}^{\nu}\sigma_i Z^{\nu-i}$, where $\sigma_0 = 1$. Thus, the decoding algorithm consists of four major steps:
Step 1 Calculation of the syndrome vector $\mathbf{s}$ from the received vector.
Step 2 Calculation of the elementary symmetric functions $\sigma_1, \sigma_2, \cdots, \sigma_\nu$ from $\mathbf{s}$, using the modified Berlekamp-Massey algorithm [3].
Step 3 Calculation of the error-location numbers $x_1, x_2, \cdots, x_\nu$ from $\sigma_1, \sigma_2, \cdots, \sigma_\nu$, that are roots of $\sigma(z)$.
Step 4 Calculation of the error magnitudes $y_1, y_2, \cdots, y_\nu$ from x_i and $\mathbf{s}$, using Forney's procedure [7].

There is no need to comment on Step 1 since the calculation of the vector syndrome is straightforward. In Step 2, the calculation of the elementary symmetric functions is equivalent to finding a solution $\sigma_1, \sigma_2, \cdots, \sigma_\nu$, with minimum possible ν, to the following set of linear recurrent equations over $\Re$

$$s_{j+\nu} + s_{j+\nu-1}\sigma_1 + \cdots + s_{j+1}\sigma_{\nu-1} + s_j\sigma_\nu = 0, \quad j = 0, 1, 2, \cdots, (r-1) - \nu, \quad (5.1)$$

where $s_0, s_1, \cdots, s_{r-1}$ are the components of the syndrome vector. We make use of the modified Berlekamp-Massey algorithm to find the solutions of Equation (5.1). The algorithm is iterative, in the sense that the following $n - l_n$ equations (called *power sums*)

$$\begin{cases} s_n\sigma_0^{(n)} + s_{n-1}\sigma_1^{(n)} + \cdots + s_{n-l_n}\sigma_{l_n}^{(n)} = 0 \\ s_{n-1}\sigma_0^{(n)} + s_{n-2}\sigma_1^{(n)} + \cdots + s_{n-l_n-1}\sigma_{l_n}^{(n)} = 0 \\ \qquad \vdots \\ s_{l_n+1}\sigma_0^{(n)} + s_{l_n}\sigma_1^{(n)} + \cdots + s_1\sigma_{l_n}^{(n)} = 0 \end{cases}$$

are satisfied with l_n as small as possible and $\sigma_0^{(0)} = 1$. The polynomial $\sigma^{(n)}(Z) = \sigma_0^{(n)} + \sigma_1^{(n)}Z + \cdots + \sigma_{l_n}^{(n)}Z^n$ represents the solution at the n-th stage. The n-th *discrepancy* is denoted by d_n and defined by $d_n = s_n\sigma_0^{(n)} + s_{n-1}\sigma_1^{(n)} + \cdots + s_{n-l_n}\sigma_{l_n}^{(n)}$. The modified Berlekamp-Massey algorithm for commutative rings with identity is formulated as follows. The inputs to the algorithm are the syndromes $s_0, s_1, \cdots, s_{r-1}$ which belong to $\Re$. The output of the algorithm is a set of values σ_i, for $i = 1, 2, \cdots, \nu$, such that Equation (5.1) holds with minimum ν. Let $\sigma^{(-1)}(Z) = 1$, $l_{-1} = 0$, $d_{-1} = 1$, $\sigma^{(0)}(Z) = 1$, $l_0 = 0$ and $d_0 = s_0$ be the a set of initial conditions to start the algorithm as in Peterson [8]. The steps of the algorithm are:
1. $n \leftarrow 0$.

2. If $d_n = 0$, then $\sigma^{(n+1)}(Z) \leftarrow \sigma^{(n)}(Z)$ and $l_{n+1} \leftarrow l_n$ and to go 5).
3. If $d_n \neq 0$, then find $m \leq n-1$ such that $d_n - yd_m = 0$ has a solution y and $m - l_m$ has the largest value. Then, $\sigma^{(n+1)}(Z) \leftarrow \sigma^{(n)}(Z) - yZ^{n-m}\sigma^{(m)}(Z)$ and $l_{n+1} \leftarrow max\{l_n, l_m + n - m\}$.
4. If $l_{n+1} = max\{l_n, n+1-l_n\}$ then go to step 5, else search for a solution $D^{(n+1)}(Z)$ with minimum degree l in the range $max\{l_n, n+1-l_n\} \leq l < l_{n+1}$ such that $\sigma^{(m)}(Z)$ defined by $D^{(n+1)}(Z) - \sigma^{(n)}(Z) = Z^{n-m}\sigma^{(m)}(Z)$ is a solution for the first m power sums, $d_m = -d_n$, with $\sigma_0^{(m)}$ a zero divisor in $\Re$. If such a solution is found, $\sigma^{(n+1)}(Z) \leftarrow D^{(n+1)}(Z)$ and $l_{n+1} \leftarrow l$.
5. If $n < r-1$, then $d_n = s_n + s_{n-1}\sigma_1^{(n)} + \cdots + s_{n-l_n}\sigma_{l_n}^{(n)}$.
6. $n \leftarrow n+1$; if $n < r-1$ go to 2); else stop.

The coefficients $\sigma_1^{(r)}, \sigma_2^{(r)}, \cdots, \sigma_\nu^{(r)}$ satisfy Equation (5.1). At Step 3, the solution to Equation (5.1) is generally not unique and the reciprocal polynomial $\rho(Z)$ of the polynomial $\sigma^{(r)}(Z)$ (output by the modified Berlekamp-Massey algorithm), may not be the correct error-locator polynomial $(Z - x_1)(Z - x_2)\cdots(Z - x_\nu)$, where $x_j = \beta^{k_i}$, for $j = 1, 2, \cdots, \nu$ and $i = 1, 2, \cdots, n$, are the correct error-location numbers. Thus, the procedure for the calculation of the correct error-location numbers is the following:
(a) compute the roots $z_1, z_2, \cdots, z_\nu$ of $\rho(Z)$; and
(b) among the $x_i = \beta^{k_j}$, for $j = 1, 2\cdots, n$, select those x_i's such that $x_i - z_i$ are zero divisors in $\Re$. The selected x_i's will be the correct error-location numbers and each k_j, for $j = 1, 2, \cdots, n$, indicates the position j of the error in the codeword.

At Step 4, the calculation of the error magnitude is based on Forney's procedure [7]. The error magnitude is given by

$$y_j = \frac{\sum_{l=0}^{\nu-1} \sigma_{jl} s_{\nu-1-l}}{E_j \sum_{l=0}^{\nu-1} \sigma_{jl} x_j^{\nu-1-l}}, \tag{5.2}$$

for $j = 1, 2, \cdots, \nu$, where the coefficients σ_{jl} are recursively defined by $\sigma_{j,i} = \sigma_i + x_j\sigma_{j,i-1}$, for $i = 0, 1, \cdots, \nu - 1$, starting with $\sigma_0 = \sigma_{j,0} = 1$. The $E_i = 1$ for BCH code, $E_j = w_{i_j}$ for alternant code and $E_j = h(x_i)^{-1}$ for Goppa code, for $i = 1, 2, \cdots, \nu$, are the corresponding location of errors in the vector $\mathbf{w}$. It follows, from Lemma 3.1, that the denominator in Equation (5.2) is always a unit in $\Re$.

Example 5.1. *Referring to Example 3.1, if* $\mathbf{b} = (1, 0, 0, 0, 0, 0)$ *is the received vector, then the syndrome vector is given by* $\mathbf{s} = \mathbf{b}H^t = (1, 1, 1)$. *Applying the modified Berlekamp-Massey algorithm, it follows that* $\sigma^{(6)}(Z) = 1 + Z$. *The root of* $\rho(Z) = Z + 1$ *(the reciprocal of* $\sigma^{(6)}(Z)$*) is* $z_1 = 1$. *Among the elements of* G_s *we have* $x_1 = 1$ *is such that* $x_1 - z_1 = 0$ *is a zero divisor in* $\Re$. *Therefore,* x_1 *is the correct error-location number, and* $k_1 = 1$ *indicates that the error has occurred in the first coordinate of the codeword. Finally, applying Forney's method to* $\mathbf{s}$ *and* x_1, *gives* $y_1 = 1$. *Therefore, the error pattern is given by* $\mathbf{e} = (1, 0, 0, 0, 0, 0)$.

Resumo. Neste trabalho, introduzimos novas técnicas de construções de códigos BCH, alternant, Goppa, Srivastava através do anel semigrupo $B[X; \frac{1}{3}\mathbb{Z}_0]$ em vez do anel de polinômio $B[X; \mathbb{Z}_0]$, onde B é um anel comutativo finito com identidade, e para essas construções melhoramos vários resultados de [1]. Depois disto, apresentamos um principio de decodificação para os códigos BCH, alternant and Goppa baseado no algoritmo de Berlekamp-Massey modificado. Este algoritmo corrige todos os padrões de erros com peso de Hamming $t \leq r/2$, i.e., cuja distância de Hamming mínimua é $r + 1$.

Palavras-chave. Anel semigrupo, código BCH, código alternant, código de Goppa, código Srivastava.

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] T. Shah, A. Khan, A.A. de Andrade, Encoding through generalized polynomial codes, (accepted for publication).

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

[4] R. Gilmer, "Commutative Semigroup Rings", University Chicago Press Chicago and London, 1984.

[5] B.R. McDonlad, "Finite Rings with Identity", Marcel Dekker, New York, 1974.

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

[7] G.D. Forney Jr., On decoding BCH codes, *IEEE Trans. Inform. Theory*, **IT-11** (1965), 549–557.

[8] W.W. Peterson, E.J. Weldon Jr., "Error Correcting Codes", MIT Press, Cambridge, Mass., 1972.