TEMA Tend. Mat. Apl. Comput., **6**, No. 2 (2005), 207-217.
© *Uma Publicação da Sociedade Brasileira de Matemática Aplicada e Computacional.*

Linear Codes over Finite Rings[1]

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

R. PALAZZO Jr.[3], Department of Telematics, FEEC, UNICAMP, 13083-852 Campinas, SP, Brazil.

Abstract. In this paper we present a construction technique of cyclic, BCH, alternat, Goppa and Srivastava codes over a local finite commutative rings with identity.

1. Introduction

Linear codes over finite rings with identity have recently raised a great interest for their new role in algebraic coding theory and for their successful application in combined coding and modulation. Thus, in this paper we address the problems of constructing of new cyclic, BCH, alternant, Goppa and Srivastava codes over local finite commutative rings with identity. These constructions are very similar to the ones over finite fields and these constructions requires working on Galois extension rings, where some properties of the Galois extension fields are lost.

Recent developments have contributed toward achieving the reliability required by todays high-speed digital systems, and the use of coding for error control has become an integral part in the design of modern communication systems and digital computers. Moreover, we mention that the investigation of codes over finite alphabets (for example, finite rings) which are less structured than finite fields may be more appropriate to use for computer-to-computer communication.

This paper is organized as follows. In Section 2, we present a construction technique of cyclic codes over a commutative ring with identity. In Section 3, we present a construction technique of BCH and alternant codes over local finite commutative rings with identity. In Section 4, we describe a construction technique of Goppa and Srivastava codes over local finite commutative rings with identity.

2. Cyclic Codes

Let $\mathcal{A}$ be a commutative ring with identity. The structure of ideals in the ring $\mathcal{R} = \mathcal{A}[x]/\langle x^n - 1\rangle$, have recently raised a great interest for their successful applications

[1] This work has been supported by FAPESP - 02/07473-7.

[2] E-mail: andrade@ibilce.unesp.br

[3] E-mail: palazzo@dt.fee.unicamp.br.

in algebraic coding theory. We recall to the reader that a **linear code** of length n over $\mathcal{A}$ is an $\mathcal{A}$-module in the space of all n-tuples of $\mathcal{A}^n$ and a linear code $\mathcal{C}$ over $\mathcal{A}$ is **cyclic**, if whenever $\mathbf{v} = (v_0, v_1, \ldots, v_{n-1}) \in \mathcal{C}$, every cyclic shift $\mathbf{v}^{(1)} = (v_{n-1}, v_0, \ldots, v_{n-2}) \in \mathcal{C}$, with $v_i \in \mathcal{A}$, $0 \leq i \leq n-1$. A work by Calderbank [6] has shown that the ring $\mathcal{R} = \mathbb{Z}_q[x]/\langle x^n - 1\rangle$, where q is a power of a prime p, is a principal ideal ring and early work by Interlando [9] had given the structure of principal ideals in the ring $\mathcal{R} = \mathbb{Z}_m[x]/\langle x^n - 1\rangle$, where m is a positive integer.

Theorem 2.1 ([1, Theorem 2.1]). *In the ring $\mathcal{R} = \mathcal{A}[x]/\langle x^n - 1\rangle$, a subset $\mathcal{C}$ is a cyclic code if and only if $\mathcal{C}$ is an ideal of $\mathcal{R}$.*

Proof. Suppose that the subset $\mathcal{C}$ is a cyclic code. Then $\mathcal{C}$ is closed under addition and under multiplication by x. But then it is closed under multiplication by powers of x and linear combinations of powers of x. That is, $\mathcal{C}$ is closed under multiplication by an arbitrary polynomial. Hence $\mathcal{C}$ is an ideal. Now suppose that the subset $\mathcal{C}$ is an ideal. Then $\mathcal{C}$ is closed under addition and closed under multiplication by a scalar. Hence $\mathcal{C}$ is an $\mathcal{A}$-module. It is also closed under multiplication by any ring element, in particular under multiplication by x. Hence $\mathcal{C}$ is a cyclic code. □

Let $\mathcal{R} = \mathcal{A}[x]/\langle f(x)\rangle$ be the set of residue classes of polynomials in x over $\mathcal{A}$ modulo a monic polynomial $f(x)$ of degree n over $\mathcal{A}$. This ring is also a commutative ring with identity. It is useful to represent the elements of $\mathcal{R}$ by the polynomials $\overline{a}(x) = \overline{a}_0 + \overline{a}_1 x + \cdots + \overline{a}_{n-1}x^{n-1}$. A particularly simple kind of ideal is a **principal ideal**, which consists of all multiples of a fixed polynomial $g(x)$ by elements of $\mathcal{R}$, called **generator polynomial** of the ideal. Now we will prove some results that will indicate a method of obtain the generator polynomial of a principal ideal. This method will serve as basis for the construction of principal ideals in the ring $\mathcal{R}$. We will also show conditions to decide when a ideal $\mathcal{B}$ is principal.

Lemma 2.1 ([2, Lemma 1]). *Let $\mathcal{B}$ be an ideal in the ring $\mathcal{R}$. If the leading coefficient of some polynomial of lowest degree in $\mathcal{B}$ is a unit in $\mathcal{A}$, then there exists an unique monic polynomial of minimal degree in $\mathcal{B}$.*

Proof. Let $\overline{g}(x)$ be a polynomial of lowest degree m in $\mathcal{B}$. If the leading coefficient $\overline{a}_m$ of $\overline{g}(x)$ is a unit in $\mathcal{A}$, it is always possible to obtain a monic polynomial $\overline{g_1}(x) = \overline{a}_m g(x)$ with the same degree in $\mathcal{B}$. Now, if $\overline{g}(x)$ and $\overline{h}(x)$ are monic polynomials of minimal degree m in $\mathcal{B}$ then the polynomial $\overline{k}(x) = \overline{g}(x) - \overline{h}(x)$ is a polynomial in $\mathcal{B}$ and has degree lower than m. Therefore, by the choice of $\overline{g}(x)$ follow that $\overline{k}(x) = \overline{0}$, and therefore $\overline{g}(x) = \overline{h}(x)$. □

Theorem 2.2 ([2, Theorem 2]). *Let $\mathcal{B}$ be an ideal in the ring $\mathcal{R}$. If the leading coefficient of some polynomial $\overline{g}(x)$ of lowest degree in $\mathcal{B}$ is a unit in $\mathcal{R}$ then $\mathcal{B} = \langle \overline{g}(x)\rangle$, i.e., $\mathcal{B}$ is a principal ideal.*

Proof. Let $\overline{a}(x)$ be a polynomial in $\mathcal{B}$. By euclidean algorithm for commutative rings there are unique polynomials $\overline{q}(x)$ and $\overline{r}(x)$ such that $\overline{a}(x) = \overline{q}(x)\overline{g}(x) + \overline{r}(x)$ where $\overline{r}(x) = \overline{0}$ or $degree(\overline{r}(x)) < degree(\overline{g}(x))$. By the definition of an ideal, $\overline{r}(x) \in \mathcal{B}$. Thus by the choice of $\overline{g}(x)$, we have that $\overline{r}(x) = \overline{0}$ and therefore, $\overline{a}(x) = \overline{q}(x)\overline{g}(x)$. Thus every polynomial in $\mathcal{B}$ is multiple of $\overline{g}(x)$, i.e., $\mathcal{B} = \langle \overline{g}(x)\rangle$. □

Lemma 2.2 ([2, Lemma 2]). *Let $r(x)$ be a polynomial in $\mathcal{A}[x]$. If $r(x) \neq 0$ and $degree(r(x)) < degree(f(x))$, then $\overline{r}(x) \neq \overline{0}$ in $\mathcal{R}$.*

Proof. Suppose that $\overline{r}(x) = \overline{0}$. Therefore there is $q(x) \neq 0$ in $\mathcal{A}[x]$ such that $r(x) = f(x)q(x)$. Since $f(x)$ is regular and $r(x) \neq 0$ it follows that $degree(r(x)) = degree(f(x)) + degree(q(x)) \geq degree(f(x))$, which is a contradiction since we had already assumed that $degree(r(x)) < degree(f(x))$. Therefore $\overline{r}(x) \neq \overline{0}$. □

Theorem 2.3 ([2, Theorem 3]). *Let $\mathcal{B}$ be an ideal in the ring R. Let $g(x)$ be a polynomial in $\mathcal{A}[x]$ such that $degree(g(x)) < degree(f(x))$ and the leading coefficient of $g(x)$ is a unit in $\mathcal{A}$. If $\overline{g}(x) \in \mathcal{B}$ and has lowest degree in $\mathcal{B}$ then $g(x)$ divides $f(x)$.*

Proof. By euclidean algorithm for commutative rings there are unique polynomials $\overline{q}(x)$ and $\overline{r}(x)$ such that $\overline{0} = \overline{g}(x)\overline{q}(x) + \overline{r}(x)$ where $\overline{r}(x) = \overline{0}$ or $degree(\overline{r}(x)) < degree(\overline{g}(x))$. Thus $\overline{r}(x) = -\overline{g}(x)\overline{q}(x)$, i.e., $\overline{r}(x)$ is in $\mathcal{B}$. Therefore by the choice of $\overline{g}(x)$ follows that $\overline{r}(x) = \overline{0}$. Also, by euclidean algorithm for commutative rings, there are unique polynomials $q_1(x)$ and $r_1(x)$ such that $f(x) = g(x)q_1(x) + r_1(x)$ where $r_1(x) = 0$ or $degree(r_1(x)) < degree(g(x))$. Therefore $\overline{0} = \overline{g}(x)\overline{q_1}(x) + \overline{r_1}(x) = \overline{g}(x)\overline{q}(x) + \overline{r}(x)$. Thus $\overline{q_1}(x) = \overline{q}(x)$ and $\overline{r_1}(x) = \overline{r}(x) = \overline{0}$. By Lemma 2.2 it follows that $r_1(x) = 0$ and therefore $g(x)$ divides $f(x)$. □

Example 2.1. *Let $\mathcal{R}$ be a ring given by $\mathcal{R} = \mathbb{Z}_4[x]/\langle f(x)\rangle$, where $f(x) = x^2 - 1$. Let $\mathcal{B} = \{\overline{0}, \overline{1}x + \overline{1}, \overline{2}x + \overline{2}, \overline{3}x + \overline{3}\}$ be an ideal of $\mathcal{R}$. By Theorem 2.2 we have that $\mathcal{B} = \langle \overline{3}x + \overline{3}\rangle$ and by Theorem 2.3 we have that $g(x) = 3x + 3$ divides $f(x)$.*

Theorem 2.4 ([2, Theorem 4]). *Let $\mathcal{B}$ be a ideal in the ring R. If $g(x)$ divides $f(x)$ and $\overline{g}(x) \in \mathcal{B}$ then $\overline{g}(x)$ has lowest degree in $\langle \overline{g}(x)\rangle$.*

Proof. Suppose that there is $\overline{b}(x)$ in $\langle \overline{g}(x)\rangle$ such that $degree(\overline{b}(x)) < degree(\overline{g}(x))$. Since $\overline{b}(x)$ is in $\langle \overline{g}(x)\rangle$, then $\overline{b}(x) = \overline{g}(x)\overline{h}(x)$ for some $\overline{h}(x)$ in $\mathcal{R}$. Thus $b(x) - g(x)h(x)$ is in $< f(x) >$, i.e., $b(x) - g(x)h(x) = f(x)a(x)$ for some $a(x)$ in $\mathcal{A}[x]$. From this, we have that $b(x) = g(x)h(x) + f(x)a(x)$. Since $g(x)$ divides $f(x)$, we have that $g(x)$ divides $g(x)h(x) + f(x)a(x)$, which implies that $g(x)$ divides $b(x)$, a contradiction since we had already assumed that $degree(b(x)) < degree(g(x))$. Therefore $\overline{g}(x)$ has lowest degree in $\langle \overline{g}(x)\rangle$. □

Example 2.2. *Let $\mathcal{R}$ be a ring given by $\mathcal{R} = \mathbb{Z}[x]/\langle x^3+x^2+x+1\rangle$. Let $\mathcal{B}$ be an ideal in $\mathcal{R}$ such that $\overline{g}(x) = \overline{1}x+\overline{1}$ is in $\mathcal{B}$. Since $g(x) = x+1$ divides $f(x) = x^3+x^2+x+1$ we have by Theorem 2.4 that $\overline{g}(x)$ has lowest degree in $\langle \overline{g}(x)\rangle$.*

3. BCH and Alternant Codes

In this section we present a construction technique of BCH and alternant codes over local finite rings. First, we review the key properties of Galois extension rings, which serve to characterize these codes.

Throughout this section we assume that $\mathcal{A}$ denotes a local finite commutative ring with identity, maximal ideal $\mathcal{M}$ and residue field $\mathbb{K} = \frac{\mathcal{A}}{\mathcal{M}} \equiv GF(p^m)$, for some prime p, m a positive integer, and $\mathcal{A}[x]$ denotes the ring of polynomials in the variable x over $\mathcal{A}$. The natural projection $\mathcal{A}[x] \to \mathbb{K}[x]$ is denoted by μ, where $\mu(a(x)) = \overline{a}(x)$. Let $f(x)$ be a monic polynomial of degree h in $\mathcal{A}[x]$ such that $\mu(f(x))$ is irreducible in $\mathbb{K}[x]$. Then $f(x)$ also is irreducible in $\mathcal{A}[x]$ [10, Theorem XIII.7]. Let $\mathcal{R}$ be the ring $\mathcal{A}[x]/\langle f(x)\rangle$. Then $\mathcal{R}$ is a finite commutative local ring with identity and is called a Galois extension of $\mathcal{A}$ of degree h. Its residue field is $\mathbb{K}_1 = \mathcal{R}/\overline{\mathcal{M}_1} \equiv GF(p^{mh})$, where $\overline{\mathcal{M}_1}$ is the maximal ideal of $\mathcal{R}$, and $\mathbb{K}_1^*$ is the multiplicative group of $\mathbb{K}_1$, whose order is $p^{mh} - 1$.

Let $\mathcal{R}^*$ denotes the multiplicative group of units of $\mathcal{R}$. It follows that $\mathcal{R}^*$ 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 $\mathcal{R}^*$, hereafter denoted by $\mathcal{G}_s$, whose elements are the roots of $x^s - 1$ for some positive integer s such that $\gcd(s, p) = 1$. There is only one maximal cyclic subgroup of $\mathcal{R}^*$ having order relatively prime to p [10, Theorem XVIII.2]. This cyclic group has order $s = p^{mh} - 1$.

Definition 3.1. *Let $\eta = (\alpha_1, \cdots, \alpha_n)$ be a vector consisting of distinct elements of $\mathcal{G}_s$, and let $\mathbf{w} = (w_1, w_2, \cdots, w_n)$ be an arbitrary vector consisting of elements (not necessarily distinct) of $\mathcal{G}_s$. Then the set of all vectors*

$$(w_1 f(\alpha_1), w_2 f(\alpha_2), \cdots, w_n f(\alpha_n)), \tag{3.1}$$

where $f(z)$ ranges over all polynomials of degree at most $k-1$, $k \in \mathbb{N}$, with coefficients from $\mathcal{R}$, defines a shortened code $\mathcal{C}$ of length $n \leq s$ over $\mathcal{R}$.

Remark 3.1. *Since f has at most $k-1$ zeros, the minimum distance of this code is at least $n - k + 1$.*

Definition 3.2 ([3, Definition 2.2]). *A shortened* **BCH code** *$\mathcal{C}(n, \eta)$ of length $n \leq s$ is a code over $\mathcal{A}$ that has parity check matrix*

$$H = \begin{bmatrix} \alpha_1 & \alpha_2 & \cdots & \alpha_n \\ \alpha_1^2 & \alpha_2^2 & \cdots & \alpha_n^2 \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^r & \alpha_2^r & \cdots & \alpha_n^r \end{bmatrix} \tag{3.2}$$

for some $r \geq 1$, where $\eta = (\alpha_1, \alpha_2, \cdots, \alpha_n) = (\alpha^{k_1}, \alpha^{k_2}, \cdots, \alpha^{k_n})$ is the locator vector, consisting of distinct elements of $\mathcal{G}_s$. The code $\mathcal{C}(n, \eta)$, with $n = s$, will be called a **BCH code**. *In this case, η is unique up to permutation of coordinates.*

Lemma 3.1 ([4, Theorem 7]). *Let α be an element of G_s of order s. Then the differences $\alpha^{l_1} - \alpha^{l_2}$ are units in R if $0 \leq l_1 \neq l_2 \leq s-1$.*

Proof. Note that $\alpha^{l_1} - \alpha^{l_2}$ can be written as $-\alpha^{l_2}(1 - \alpha^{l_1 - l_2})$, where 1 denotes the unity of $\mathcal{R}$. The first term in the product, namely $-\alpha^{l_2}$, is a unit. The second term can be written as $1 - \alpha^j$ for some integer j in the interval $[1, s-1]$. Now, if the element $1 - \alpha^j$, $1 \leq j \leq s-1$, were not a unit in $\mathcal{R}$, then $1 - \alpha^j \in \overline{\mathcal{M}_1}$, and consequently, $(\mu'(\alpha))^j = \mu'(1)$ for $j < s$, which is a contradiction. Thus $1 - \alpha^j \in \mathcal{R}^*$, $1 \leq j \leq s-1$. $\square$

Theorem 3.1 ([3, Theorem 2.4]). *The minimum Hamming distance of a BCH code $\mathcal{C}(n,\eta)$ satisfies $d \geq r+1$.*

Proof. Suppose $\mathbf{c}$ is a nonzero codeword in $\mathcal{C}(n,\eta)$ such that $w_H(\mathbf{c}) \leq 2t$. Then $\mathbf{c}H^T = 0$. Deleting $n-2t$ columns of the matrix H corresponding to zeros of the codeword, it follows that the new matrix H' is Vandermonde. By Lemma 3.1, it follows that the determinant is a unit in $\mathcal{R}$. Thus, the only possibility for $\mathbf{c}$ is the all-zero codeword. □

Example 3.1. *The polynomial $f(x) = x^3 + x + 1$ is irreducible over $GF(2)$ and over $\mathcal{A} = GF(2)[i]$, where $i^2 = -1$. Thus, the ring $\mathcal{R}$ is $\mathcal{R} = \frac{A[x]}{\langle f(x)\rangle}$. We have that if α is a root of $f(x)$, then α generates a cyclic group $\mathcal{G}_s$ of order $s = 2^3 - 1 = 7$. Let $\eta = (\alpha^5, \alpha, 1, \alpha^4, \alpha^2, \alpha^6)$ be the locator vector. If $r = 2$, then the following matrix*

$$H = \begin{bmatrix} \alpha^5 & \alpha & 1 & \alpha^4 & \alpha^2 & \alpha^6 \\ \alpha^3 & \alpha^2 & 1 & \alpha & \alpha^4 & \alpha^5 \end{bmatrix}$$

is the parity-check matrix of a BCH code $\mathcal{C}(6,\eta)$ of length 6 and minimum Hamming distance at least 3.

Definition 3.3 ([5, Definition 2.1]). *A shortened* **alternant code** $\mathcal{C}(n,\eta,\mathbf{w})$ *of length $n \leq s$ is a code over $\mathcal{A}$ that has parity check matrix*

$$H = \begin{bmatrix} w_1 & w_2 & \cdots & w_n \\ w_1\alpha_1 & w_2\alpha_2 & \cdots & w_n\alpha_n \\ w_1\alpha_1^2 & w_2\alpha_2^2 & \cdots & w_n\alpha_n^2 \\ \vdots & \vdots & \ddots & \vdots \\ w_1\alpha_1^{r-1} & w_2\alpha_2^{r-1} & \cdots & w_n\alpha_n^{r-1} \end{bmatrix}, \tag{3.3}$$

where r is a positive integer, $\eta = (\alpha_1, \alpha_2, \cdots, \alpha_n) = (\alpha^{k_1}, \alpha^{k_2}, \cdots, \alpha^{k_n})$ is the locator vector, consisting of distinct elements of $\mathcal{G}_s$, and $\mathbf{w} = (w_1, w_2, \cdots, w_n)$ is an arbitrary vector consisting of elements of $\mathcal{G}_s$.

It is possible to obtain an estimate of the minimum Hamming distance d directly from the parity-check matrix.

Theorem 3.2 ([5, Theorem 2.1]). *The alternant code $\mathcal{C}(n,\eta,\mathbf{w})$ has minimum Hamming distance $d \geq r+1$.*

Proof. Suppose $\mathbf{c}$ is a nonzero codeword in $\mathcal{C}(n,\eta,\mathbf{w})$ such that $w_H(\mathbf{c}) \leq r$. Then, $\mathbf{c}H^T = \mathbf{c}(XY)^T = 0$. Setting $\mathbf{b} = \mathbf{c}Y^T$, we obtain $w_H(\mathbf{b}) = w_H(\mathbf{c})$ since Y is diagonal and invertible. Thus, $\mathbf{b}X^T = 0$. Deleting $n-r$ columns of the matrix X that correspond to zeros of the codeword, then the new matrix $X^{'}$ is Vandermonde. By Lemma 3.1, it follows that the determinant is an unit in $\mathcal{R}$. Thus, the unique possibility for $\mathbf{c}$ is the all-zero codeword. □

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

$$H = \begin{bmatrix} \alpha^5 & \alpha & 1 & \alpha^4 & \alpha^2 \\ \alpha^6 & \alpha^5 & 1 & 1 & \alpha^4 \end{bmatrix}$$

is the parity-check matrix of an alternant code $\mathcal{C}(5, \eta, \mathbf{w})$ of length 5 and minimum Hamming distance at least 3. Another example of an alternant code is a BCH code.

4. Goppa and Srivastava Codes

In this section, firstly we define an interesting subclass of alternat codes over local finite rings, which is very similar to the one proposed by Goppa [7] over finite fields. Just as cyclic codes are specified in terms of a generator polynomial, so Goppa codes are described in terms of a Goppa polynomial $g(z)$. 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 $d \geq deg(g(z)) + 1$.

Let $\mathcal{A}$, $\mathcal{R}$ and $\mathcal{G}_s$ as defined in Section 3. Let α be a primitive element of the cyclic group $\mathcal{G}_s$, where $s = p^{mh} - 1$. Let $g(z) = g_0 + g_1 z + \cdots + g_r z^r$ be a polynomial with coefficients in $\mathcal{R}$ and $g_r \neq 0$. Let $L = \{\alpha_1, \alpha_2, \cdots, \alpha_n\}$ be a subset of distinct elements of $\mathcal{G}_s$ such that $g(\alpha_i)$ are units from $\mathcal{R}$ for $i = 1, 2, \cdots, n$.

Definition 4.1. *A shortened* **Goppa code** *$\mathcal{C}(L, g)$ of length $n \leq s$ is a code over $\mathcal{A}$ that has parity-check matrix*

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

where r is a positive integer, $\eta = (\alpha_1, \alpha_2, \cdots, \alpha_n) = (\alpha^{k_1}, \alpha^{k_2}, \cdots, \alpha^{k_n})$ is the locator vector, consisting of distinct elements of $\mathcal{G}_s$, and $\mathbf{w} = (g(\alpha_1)^{-1}, \cdots, g(\alpha_n)^{-1})$ is an vector consisting of elements of $\mathcal{G}_s$.

Definition 4.2. *Let $\mathcal{C}(L, g)$ be a Goppa code.*

- *If $g(z)$ is irreducible then $\mathcal{C}(L, g)$ is called an irreducible Goppa code.*
- *If $\mathbf{c} = (c_1, c_2, \cdots, c_n) \in \mathcal{C}(L, g)$ and $\mathbf{c}' = (c_n, c_{n-1}, \cdots, c_1) \in \mathcal{C}(L, g)$ then $\mathcal{C}(L, g)$ is called a reversible Goppa code.*
- *If $g(z) = (z - \alpha)^r$ then $\mathcal{C}(L, g)$ is called a comulative Goppa code.*
- *If $g(z)$ has not multiple zeros then $\mathcal{C}(L, g)$ is called a separable Goppa code.*

Remark 4.1. *Let $\mathcal{C}(L, g)$ be a Goppa code.*

1. *We have that $\mathcal{C}(L, g)$ is a linear code.*

2. *A parity check matrix with elements form $\mathcal{A}$ is then obtained by replacing each entry of H by the corresponding column vector of length h from $\mathcal{A}$.*

3. *For a code with Goppa polynomial $g_l(z) = (z - \beta_l)^{r_l}$, where $\beta_l \in \mathcal{G}_s$, we have*

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

which is row equivalent to

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

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

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

4. *BCH codes are a special case of Goppa codes. For this, choose $g(z) = z^r$ and $L = \{\alpha_1, \alpha_2, \cdots, \alpha_n\}$, where $\alpha_i \in \mathcal{G}_s$, for all $i = 1, 2, \cdots, n$. Then from Equation (4.1)*

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

which becomes the parity check matrix of a BCH code, Equation (3.2) when α_i^{-1} is replaced by β_i, $i = 1, 2, \cdots, n$.

Theorem 4.1. *The Goppa code $\mathcal{C}(L, g)$ has minimum Hamming distance $d \geq r+1$.*

Proof. We have that $\mathcal{C}(L, g)$ is an alternant code $\mathcal{C}(n, \eta, \mathbf{w})$ with $\eta = (\alpha_1, \alpha_2, \cdots, \alpha_n)$ and $\mathbf{w} = (g(\alpha_1)^{-1}, g(\alpha_2)^{-1}, \cdots, g(\alpha_n)^{-1})$. Therefore by Theorem 3.2 we have that $\mathcal{C}(L, g)$ has minimum distance $d \geq r + 1$. □

Example 4.1. *Let $\mathcal{A} = GF(2)[i]$ and $\mathcal{R} = \frac{\mathcal{A}[x]}{\langle x^4+x+1\rangle}$, where $f(x) = x^4 + x + 1$ is irreducible over $\mathcal{A}$. Thus $s = 15$ and $\mathcal{G}_{15}$ is generated by α, where $\alpha^4 = \alpha + 1$. Let $g(z) = z^4 + z^3 + 1$, $L = \{1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6, \alpha^7, \alpha^8, \alpha^9, \alpha^{10}\}$ and $\mathbf{w} = (1, \alpha^{12}, \alpha^{10}, \alpha^7, \alpha^3, \alpha^{11}, \alpha^6, \alpha^9, \alpha^5, \alpha^{14}, \alpha^{13})$. The matrix*

$$H = \begin{bmatrix} 1 & \alpha^{12} & \alpha^{10} & \alpha^7 & \alpha^3 & \alpha^{11} & \alpha^6 & \alpha^9 & \alpha^5 & \alpha^{14} & \alpha^{13} \\ 1 & \alpha^{14} & 1 & \alpha^4 & \alpha^{11} & \alpha^2 & \alpha^7 & \alpha^{13} & 1 & \alpha^8 & \alpha \\ 1 & \alpha & \alpha^5 & \alpha & \alpha^4 & \alpha^8 & \alpha^8 & \alpha^2 & \alpha^{10} & \alpha^2 & \alpha^4 \\ 1 & \alpha^3 & \alpha^{10} & \alpha^{13} & \alpha^{12} & \alpha^{14} & \alpha^9 & \alpha^6 & \alpha^5 & \alpha^{11} & \alpha^7 \end{bmatrix}$$

is the parity check matrix of a Goppa code over $GF(2)[i]$ of length 11 and minimum Hamming distance at least 5.

Now, we define another interesting subclass of alternant codes over local finite rings which is very similar to the one proposed by J. N. Srivastava in 1967, in unpublished work [8], that are defined by parity check matrices of the form

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

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 $0, \alpha_1^{-1}, \alpha_2^{-1}, \cdots, \alpha_r^{-1}$. The quantity l can be any integer.

Definition 4.3. *A shortened* **Srivastava code** *of length $n \le s$ is a code over $\mathcal{A}$ that has parity check matrix*

$$H = \begin{bmatrix} \frac{\alpha_1^l}{\alpha_1 - \beta_1} & \frac{\alpha_2^l}{\alpha_2 - \beta_1} & \cdots & \frac{\alpha_n^l}{\alpha_n - \beta_1} \\ \frac{\alpha_1^l}{\alpha_1 - \beta_2} & \frac{\alpha_2^l}{\alpha_2 - \beta_2} & \cdots & \frac{\alpha_n^l}{\alpha_n - \beta_2} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{\alpha_1^l}{\alpha_1 - \beta_r} & \frac{\alpha_2^l}{\alpha_2 - \beta_r} & \cdots & \frac{\alpha_n^l}{\alpha_n - \beta_r} \end{bmatrix}, \tag{4.2}$$

where r, l are positive integers and $\alpha_1, \cdots, \alpha_n, \beta_1, \cdots, \beta_r$ are $n + r$ distinct elements of $\mathcal{G}_s$.

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

Proof. We have that the minimum Hamming distance of this code is at least $r + 1$ if and only if every combination of r or fewer columns of H is linearly independent over $\mathcal{R}$, or equivalently that the submatrix

$$H_1 = \begin{bmatrix} \frac{\alpha_{i_1}^l}{\alpha_{i_1} - \beta_1} & \frac{\alpha_{i_2}^l}{\alpha_{i_2} - \beta_1} & \cdots & \frac{\alpha_{i_r}^l}{\alpha_{i_r} - \beta_1} \\ \frac{\alpha_{i_1}^l}{\alpha_{i_1} - \beta_2} & \frac{\alpha_{i_2}^l}{\alpha_{i_2} - \beta_2} & \cdots & \frac{\alpha_{i_r}^l}{\alpha_{i_r} - \beta_2} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{\alpha_{i_1}^l}{\alpha_{i_1} - \beta_r} & \frac{\alpha_{i_2}^l}{\alpha_{i_2} - \beta_r} & \cdots & \frac{\alpha_{i_r}^l}{\alpha_{i_r} - \beta_r} \end{bmatrix} \tag{4.3}$$

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

$$det(H_1) = (\alpha_{i_1}\alpha_{i_2}\dots\alpha_{i_r})^l det(H_2), \tag{4.4}$$

where the matrix H_2 is given by

$$H_2 = \begin{bmatrix} \frac{1}{\alpha_{i_1}-\beta_1} & \frac{1}{\alpha_{i_2}-\beta_1} & \cdots & \frac{1}{\alpha_{i_r}-\beta_1} \\ \frac{1}{\alpha_{i_1}-\beta_2} & \frac{1}{\alpha_{i_2}-\beta_2} & \cdots & \frac{1}{\alpha_{i_r}-\beta_2} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{1}{\alpha_{i_1}-\beta_r} & \frac{1}{\alpha_{i_2}-\beta_r} & \cdots & \frac{1}{\alpha_{i_r}-\beta_r} \end{bmatrix}. \tag{4.5}$$

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

$$det(H_1) = (\alpha_{i_1}\alpha_{i_2}\dots\alpha_{i_r})^l \frac{(-1)^{\binom{r}{2}} \phi(\alpha_{i_1},\alpha_{i_2},\cdots,\alpha_{i_r})\phi(\beta_1,\beta_2,\cdots,\beta_r)}{\nu(\alpha_{i_1})\nu(\alpha_{i_2})\dots\nu(\alpha_{i_r})}, \tag{4.6}$$

where $\phi(\alpha_{i_1},\alpha_{i_2},\dots,\alpha_{i_r}) = \prod_{i_j<i_h}(\alpha_{i_j}-\alpha_{i_h})$ and $\nu(x) = (x-\beta_1)(x-\beta_2)\cdots(x-\beta_r)$. Then by [4, Theorem 7] we have that $det(H_1)$ is a unit in $\mathcal{R}$ and therefore $d \geq r+1$. □

Definition 4.4. *Suppose $r = kl$ and let $\alpha_1,\cdots,\alpha_n,\beta_1,\cdots,\beta_k$ be $n+k$ distinct elements of $\mathcal{G}_s$, $w_1,\cdots,w_n$ be elements of $\mathcal{G}_s$. A* **generalized Srivastava code** *of length $n \leq s$ is a code over $\mathcal{A}$ that has parity check matrix*

$$H = \begin{bmatrix} H_1 \\ H_2 \\ \vdots \\ H_k \end{bmatrix}, \tag{4.7}$$

where

$$H_j = \begin{bmatrix} \frac{w_1}{\alpha_1-\beta_j} & \frac{w_2}{\alpha_2-\beta_j} & \cdots & \frac{w_n}{\alpha_n-\beta_j} \\ \frac{w_1}{(\alpha_1-\beta_j)^2} & \frac{w_2}{(\alpha_2-\beta_j)^2} & \cdots & \frac{w_n}{(\alpha_n-\beta_j)^2} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{w_1}{(\alpha_1-\beta_j)^l} & \frac{w_2}{(\alpha_2-\beta_j)^l} & \cdots & \frac{w_n}{(\alpha_n-\beta_j)^l} \end{bmatrix}, \tag{4.8}$$

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

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

Proof. The proof of this theorem requires nothing more than the application of the Remark 4.1(3) and of the Theorem 4.2, since the matrices (4.1) and (4.7) are equivalents, where $g(z) = \prod_{i=1}^{k}(z - \beta_i)^l$. □

Example 4.2. *Referring to Example 4.1, if* $n = 7$*,* $r = 6$*,* $k = 2$*,* $l = 3$*,* $\{\alpha_1, \alpha_2, \cdots, \alpha_7\} = \{\alpha^4, \alpha^3, \alpha^5, \alpha, \alpha^7, \alpha^{12}, \alpha^{10}\}$*,* $\{\beta_1, \beta_2\} = \{\alpha^9, \alpha^6\}$*,* $\{w_1, \cdots, w_7\} = \{\alpha, \alpha, \alpha^2, \alpha^4, \alpha^7, \alpha^{10}, \alpha^9\}$*, then the matrix*

$$H = \begin{bmatrix}
\frac{\alpha}{\alpha^4-\alpha^9} & \frac{\alpha}{\alpha^3-\alpha^9} & \frac{\alpha^2}{\alpha^5-\alpha^9} & \frac{\alpha^2}{\alpha-\alpha^9} & \frac{\alpha^5}{\alpha^7-\alpha^9} & \frac{\alpha^{10}}{\alpha^{12}-\alpha^9} & \frac{\alpha^9}{\alpha^{10}-\alpha^9} \\
\frac{\alpha}{(\alpha^4-\alpha^9)^2} & \frac{\alpha}{(\alpha^3-\alpha^9)^2} & \frac{\alpha^2}{(\alpha^5-\alpha^9)^2} & \frac{\alpha^2}{(\alpha-\alpha^9)^2} & \frac{\alpha^5}{(\alpha^7-\alpha^9)^2} & \frac{\alpha^{10}}{(\alpha^{12}-\alpha^9)^2} & \frac{\alpha^9}{(\alpha^{10}-\alpha^9)^2} \\
\frac{\alpha}{(\alpha^4-\alpha^9)^3} & \frac{\alpha}{(\alpha^3-\alpha^9)^3} & \frac{\alpha^2}{(\alpha^5-\alpha^9)^3} & \frac{\alpha^2}{(\alpha-\alpha^9)^3} & \frac{\alpha^5}{(\alpha^7-\alpha^9)^3} & \frac{\alpha^{10}}{(\alpha^{12}-\alpha^9)^3} & \frac{\alpha^9}{(\alpha^{10}-\alpha^9)^3} \\
\frac{\alpha}{\alpha^4-\alpha^6} & \frac{\alpha}{\alpha^3-\alpha^6} & \frac{\alpha^2}{\alpha^5-\alpha^6} & \frac{\alpha^2}{\alpha-\alpha^6} & \frac{\alpha^5}{\alpha^7-\alpha^6} & \frac{\alpha^{10}}{\alpha^{12}-\alpha^6} & \frac{\alpha^9}{\alpha^{10}-\alpha^6} \\
\frac{\alpha}{(\alpha^4-\alpha^6)^2} & \frac{\alpha}{(\alpha^3-\alpha^6)^2} & \frac{\alpha^2}{(\alpha^5-\alpha^6)^2} & \frac{\alpha^2}{(\alpha-\alpha^6)^2} & \frac{\alpha^5}{(\alpha^7-\alpha^6)^2} & \frac{\alpha^{10}}{(\alpha^{12}-\alpha^6)^2} & \frac{\alpha^9}{(\alpha^{10}-\alpha^6)^2} \\
\frac{\alpha}{(\alpha^4-\alpha^6)^3} & \frac{\alpha}{(\alpha^3-\alpha^6)^3} & \frac{\alpha^2}{(\alpha^5-\alpha^6)^3} & \frac{\alpha^2}{(\alpha-\alpha^6)^3} & \frac{\alpha^5}{(\alpha^7-\alpha^6)^3} & \frac{\alpha^{10}}{(\alpha^{12}-\alpha^6)^3} & \frac{\alpha^9}{(\alpha^{10}-\alpha^6)^3}
\end{bmatrix}$$

is the parity-check matrix of a generalized Srivastava code with minimum distance at least 7.

Resumo. Neste trabalho apresentamos uma técnica de construção de códigos cíclicos, BCH, alternantes, Goppa e Srivastava sobre anéis comutativos finitos locais com identidade.

References

[1] A.A. Andrade and R. Palazzo Jr., Códigos de bloco lineares sobre anéis comutativos finitos com identidade, *Rev. Mat. Estat.*, **16** (1998), 161-172.

[2] A.A. Andrade and M.G.C. Andrade, A note on principal ideal rings, *Rev. Mat. Estat.*, **18** (2000), 207-212.

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

[4] A.A. Andrade and R. Palazzo Jr., A note on units of a local finite rings, *Rev. de Mat. Estat.*, **18** (2000), 213-222.

[5] A.A. Andrade, J.C. Interlando and R. Palazzo Jr., Alternant and BCH code over certain rings, *Computational and Applied Mathematics*, **22**, No. 2 (2003), 233-247.

[6] A.R. Calderbank and N.J.A. Sloane, Modular and p-adic cyclic codes, *Des., Codes Cryptogr.*, **6** (1995), 21-35.

[7] V.D. Goppa, A new class of linear error-correcting codes, *Probl. Peredach. Inform.*, **6**, No. 3 (1970), 24-30.

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

[9] J.C. Interlando and R. Palazzo Jr., A note on cyclic codes over $\mathbb{Z}_m$, *Latin Amer. Appl. Res.*, **25/S** (1995), 83-85.

[10] B.R. McDonald, "Finite rings with identity", Marcel Dekker, New York, 1974.