COMPUTATIONAL & APPLIED MATHEMATICS
Volume 24, N. 2, pp. 231–244, 2005
Copyright © 2005 SBMAC
ISSN 0101-8205
www.scielo.br/cam

Goppa and Srivastava codes over finite rings

ANTONIO APARECIDO DE ANDRADE[1]
and REGINALDO PALAZZO JR.[2*]

[1]Department of Mathematics, Ibilce, Unesp, 15054-000 São José do Rio Preto, SP, Brazil
[2]Department of Telematics, Feec, Unicamp, 13083-852 Campinas, SP, Brazil

E-mails: andrade@ibilce.unesp.br / palazzo@dt.fee.unicamp.br

Abstract. Goppa and Srivastava codes over arbitrary local finite commutative rings with identity are constructed in terms of parity-cleck matrices. An efficient decoding procedure, based on the modified Berlekamp-Massey algorithm, is proposed for Goppa codes.

Mathematical subject classification: 11T71, 94B05, 94B40.

Key words: Goppa code, Srivastava code.

1 Introduction

Goppa codes form a subclass of alternant codes and they are described in terms of a polynomial called Goppa polynomial. The most famous subclasses of alternant codes are BCH codes and Goppa codes, the former for their simple and easily instrumented decoding algorithm, and the latter for meeting the Gilbert-Varshamov bound. However, most of the work regarding construction and decoding of Goppa codes has been done considering codes over finite fields. On the other hand, linear codes over rings have recently generated a great deal of interest.

Linear codes over local finite commutative rings with identity have been discussed in papers by Andrade [1], [2], [3] where it was extended the notion of Hamming, Reed-Solomon, BCH and alternant codes over these rings.

In this paper we describe a construction technique of Goppa and Srivastava codes over local finite commutative rings. The core of the construction technique

#609/04. Received: 3/VI/04. Accepted: 11/V/05.

mimics that of Goppa codes over a finite field, and is addressed, in this paper, from the point of view of specifying a cyclic subgroup of the group of units of an extension ring of finite rings. The decoding algorithm for Goppa codes consists of four major steps: (1) calculation of the syndromes, (2) calculation of the elementary symmetric functions by modified Berlekamp-Massey algorithm, (3) calculation of the error-location numbers, and (4) calculation of the error magnitudes.

This paper is organized as follows. In Section 2, we describe a construction of Goppa codes over local finite commutative rings and an efficient decoding procedure. In Section 3, we describe a construction of Srivastava codes over local finite commutative rings. Finally, in Section 5, the concluding remarks are drawn.

2 Goppa Codes

In this section we describe a construction technique of Goppa codes over arbitrary local finite commutative rings in terms of parity-check matrices, which is very similar to the one proposed by Goppa [4] over finite fields. First, we review basic facts from the Galois theory of local finite commutative rings.

Throughout this paper $\mathcal{A}$ 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 will be 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 $f(x)$ is also irreducible in $\mathcal{A}[x]$ [5, Theorem XIII.7]. Let $\mathcal{R}$ be the ring $\mathcal{A}[x]/\langle f(x)\rangle$. Then $\mathcal{R}$ is a local finite commutative ring with identity and it 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 unique maximal ideal of $\mathcal{R}$, and $\mathbb{K}_1^*$ is the multiplicative group of $\mathbb{K}_1$, whose order is $p^{mh} - 1$.

Let $\mathcal{R}^*$ denote 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 subgroup 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 [5, Theorem XVIII.2]. This cyclic group has order $s = p^{mh} - 1$.

The Goppa codes are specified in terms of a polynomial $g(z)$ called 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 $d \geq deg(g(z)) + 1$.

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 $\eta = (\alpha_1, \alpha_2, \cdots, \alpha_n)$ be a vector consisting of distinct elements of $\mathcal{G}_s$ such that $g(\alpha_i)$ are units from $\mathcal{R}$ for $i = 1, 2, \cdots, n$.

Definition 2.1. *A shortened Goppa code $C(\eta, \omega, g)$ of length $n \leq s$ over $\mathcal{A}$ has parity-check matrix*

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

where $\omega = (g(\alpha_1^{-1}), g(\alpha_2^{-1}), \cdots, g(\alpha_n^{-1}))$. The polynomial $g(z)$ is called Goppa polynomial.

Definition 2.2. *Let $C(\eta, \omega, g)$ be a Goppa code.*

- *If $g(z)$ is irreducible then $C(\eta, \omega, g)$ is called an irreducible Goppa code.*
- *If, for all $\mathbf{c} = (c_1, c_2, \cdots, c_n) \in C(\eta, \omega, g)$, it is true that $\mathbf{c}^{'} = (c_n, c_{n-1}, \cdots, c_1) \in C(\eta, \omega, g)$, then $C(\eta, \omega, g)$ is called a reversible Goppa code.*
- *If $g(\mathrm{z}) = (\mathrm{z} - \alpha)^r$ then $C(\eta, \omega, g)$ is called a commutative Goppa code.*
- *If $g(z)$ has no multiple zeros then $C(\eta, \omega, g)$ is called a separable Goppa code.*

Remark 2.1. Let $C(\eta, \omega, g)$ be a Goppa code.

1. We have $C(\eta, \omega, g)$ is a linear code.

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

3. For a Goppa code with 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

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

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

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 Goppa codes with Goppa polynomial $g_l(z) = (z - \beta_l)^{r_l}$, 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. Alternant codes are a special case of Goppa codes [3, Definition 2.1].

It is possible to obtain an estimate of the minimum Hamming distance d of $C(\eta, \omega, g)$ directly from the Goppa polynomial $g(z)$. The next theorem provides such an estimate.

Theorem 2.1. *The code $C(\eta, \omega, g)$ has minimum Hamming distance $d \geq r+1$.*

Proof. We have $C(\eta, \omega, g)$ is an alternant code $C(n, \eta, \omega)$ with $\eta = (\alpha_1, \alpha_2, \cdots, \alpha_n)$ and $\omega = (g(\alpha_1)^{-1}, g(\alpha_2)^{-1}, \cdots, g(\alpha_n)^{-1})$ [3, Definition 2.1]. By [3, Theorem 2.1] it follows $C(\eta, \omega, g)$ has minimum distance $d \geq r + 1$.

Example 2.1. Let $\mathcal{A} = \mathbb{Z}_2[i]$ and $\mathcal{R} = \frac{\mathcal{A}[x]}{\langle f(x) \rangle}$, where $f(x) = x^3 + x + 1$ is irreducible over $\mathcal{A}$ and $i^2 = -1$. 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 $\eta = (\alpha, \alpha^4, 1, \alpha^2)$, $g(z) = z^3 + z^2 + 1$ and $\omega = (g(\alpha)^{-1}, g(\alpha^4)^{-1}, g(1)^{-1}, g(\alpha^2)^{-1}) = (\alpha^3, \alpha^5, 1, \alpha^6)$. Since $deg(g(z)) = 3$, it follows that

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

is the parity-check matrix of a Goppa code $C(\eta, \omega, g)$ over $\mathcal{A}$ with length 4 and minimum Hamming distance at least 4.

Example 2.2. Let $\mathcal{A} = \mathbb{Z}_2[i]$ and $\mathcal{R} = \frac{\mathcal{A}[x]}{\langle f(x) \rangle}$, 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 $g(z) = z^4 + z^3 + 1$, $\eta = (1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6, \alpha^8, \alpha^9, \alpha^{10}, \alpha^{12})$ and $\omega = (1, \alpha^6, \alpha^{12}, \alpha^{13}, \alpha^9, \alpha^{10}, \alpha^{11}, \alpha^3, \alpha^{14}, \alpha^5, \alpha^7)$. Since $\deg(g(z)) = 4$, it follows that

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

is the parity-check matrix of a Goppa code $C(\eta, \omega, g)$ over $\mathbb{Z}_2[i]$ with length 11 and minimum Hamming distance at least 5.

2.1 Decoding procedure

In this subsection we present a decoding algorithm for Goppa codes $C(\eta, \omega, g)$. This algorithm is based on the modified Berlekamp-Massey algorithm [6] which corrects all errors up to the Hamming weight $t \leq r/2$, i.e., whose minimum Hamming distance is $r + 1$.

We first establish some notation. Let $\mathcal{R}$ be a local finite commutative ring with identity as defined in Section 2 and α be a primitive element of the cyclic group $\mathcal{G}_s$, where $s = p^{mh} - 1$. 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 $\mathbf{e} = (e_1, e_2, \cdots, e_n) = \mathbf{b} - \mathbf{c}$.

Given a vector $\eta = (\alpha_1, \alpha_2, \cdots, \alpha_n) = (\alpha^{k_1}, \alpha^{k_2}, \cdots, \alpha^{k_n})$ in $\mathcal{G}_s^n$, we define the *syndrome values* s_l of an error vector $\mathbf{e} = (e_1, e_2, \cdots, e_n)$ as

$$s_l = \sum_{j=1}^{n} e_j g(\alpha_j)^{-1} \alpha_j^l, \quad l \geq 0.$$

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 $\mathbf{s} = (s_0, s_1, \cdots, s_{r-1}) = \mathbf{b}H^t = \mathbf{e}H^t$, then the first r syndrome values s_l can be calculated from the received vector $\mathbf{b}$ as

$$s_l = \sum_{j=1}^{n} e_j g(\alpha_j)^{-1} \alpha_j^l = \sum_{j=1}^{n} b_j g(\alpha_j)^{-1} \alpha_j^l, \quad l = 0, 1, 2, \cdots, r - 1.$$

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

$$\sigma(x) = \prod_{i=1}^{\nu} (x - x_i) = \sum_{i=0}^{\nu} \sigma_i x^{\nu - i},$$

where $\sigma_0 = 1$. Thus, the decoding algorithm being proposed consists of four major steps:

Step 1 – Calculation of the syndrome vector **s** from the received vector.

Step 2 – Calculation of the elementary symmetric functions $\sigma_1, \sigma_2, \cdots, \sigma_\nu$ from **s**, using the modified Berlekamp-Massey algorithm [6].

Step 3 – Calculation of the error-location numbers $x_1, x_2, \cdots, x_\nu$ from σ_1, $\sigma_2, \cdots, \sigma_\nu$, that are roots of $\sigma(x)$.

Step 4 – Calculation of the error magnitudes $y_1, y_2, \cdots, y_\nu$ from x_i and **s**, using Forney's procedure [7].

Now, each step of the decoding algorithm is analyzed. There is no need to comment on Step 1 since the calculation of the vector syndrome is straightforward. The set of possible error-location numbers is a subset of $\{\alpha^0, \alpha^1, \cdots, \alpha^{s-1}\}$. 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 $\mathcal{R}$

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

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 (2). The algorithm is iterative, in the sense that the following $n - l_n$ equations (called *power sums*)

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

are satisfied with l_n as small as possible and $\sigma_0^{(0)} = 1$. The polynomial $\sigma^{(n)}(x) = \sigma_0^{(n)} + \sigma_1^{(n)}x + \cdots + \sigma_{l_n}^{(n)}x^n$ 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 $\mathcal{R}$. The output of the algorithm is a set of values σ_i, $i = 1, 2, \cdots, \nu$, such that Equation (2) holds with minimum ν. Let $\sigma^{(-1)}(x) = 1, l_{-1} = 0, d_{-1} = 1, \sigma^{(0)}(x) = 1, l_0 = 0$ 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 $\sigma^{(n+1)}(x) \leftarrow \sigma^{(n)}(x)$ 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, $\sigma^{(n+1)}(x) \leftarrow \sigma^{(n)}(x) - yx^{n-m}\sigma^{(m)}(x)$ 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 $D^{(n+1)}(x)$ with minimum degree l in the range $\max\{l_n, n + 1 - l_n\} \leq l < l_{n+1}$ such that $\sigma^{(m)}(x)$ defined by $D^{(n+1)}(x) - \sigma^{(n)}(x) = x^{n-m}\sigma^{(m)}(x)$ is a solution for the first m power sums, $d_m = -d_n$, with $\sigma_0^{(m)}$ a zero divisor in $\mathcal{R}$. If such a solution is found, $\sigma^{(n+1)}(x) \leftarrow D^{(n+1)}(x)$ 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 (2). At Step 3, the solution to Equation (2) 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 $x_j = \alpha^{k_i}$, 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:

- compute the roots $z_1, z_2, \cdots, z_\nu$ of $\rho(z)$;

- among the $x_i = \alpha^{k_j}$, $j = 1, 2 \cdots, n$, select those x_i's such that $x_i - z_i$ are zero divisors in $\mathcal{R}$. 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

$$y_j = \frac{\sum_{l=0}^{\nu-1} \sigma_{jl} s_{\nu-1-l}}{E_j \sum_{l=0}^{\nu-1} \sigma_{jl} x_j^{\nu-1-l}}, \tag{3}$$

for $j = 1, 2, \cdots, \nu$, where the coefficients σ_{jl} are recursively defined by

$$\sigma_{j,i} = \sigma_i + x_j \sigma_{j,i-1}, \quad i = 0, 1, \cdots, \nu - 1,$$

starting with $\sigma_0 = \sigma_{j,0} = 1$. The $E_i = g(x_i)^{-1}$, for $i = 1, 2, \cdots, \nu$, are the corresponding location of errors in the vector $\mathbf{w}$. It follows from [9, Theorem 7] that the denominator in Equation (3) is always a unit in $\mathcal{R}$.

Example 2.3. As in Example 2.1, if the received vector is given by $\mathbf{b} = (0, i, 0, 0)$, then the syndrome vector is given by $\mathbf{s} = \mathbf{b}H^t = (i\alpha^5, i\alpha^2, i\alpha^6)$. Applying the modified Berlekamp-Massey algorithm, we obtain the following table

n	$\sigma^{(n)}(z)$	d_n	l_n	$n - l_n$
-1	1	1	0	-1
0	1	$i\alpha^5$	0	0
1	$1 + i\alpha^5 z$	$i\alpha^2 + \alpha^3$	1	0
2	$1 + \alpha^4 z$	0	1	1
3	$1 + \alpha^4 z$	–	1	1

Thus $\sigma^{(3)}(z) = 1 + \alpha^4 z$. The root of $\rho(z) = z + \alpha^4$ (the reciprocal of $\sigma^{(3)}(z)$) is $z_1 = \alpha^4$. Among the elements $1, \alpha, \cdots, \alpha^6$ we have $x_1 = \alpha^4$ is such that $x_1 - z_1 = 0$ is a zero divisor in $\mathcal{R}$. Therefore, x_1 is the correct error-location number, and $k_2 = 4$ indicates that one error has occurred in the second coordinate of the codeword. The correct elementary symmetric function $\sigma_1 = \alpha^4$ is obtained from $x - x_1 = x - \sigma_1 = x - \alpha^4$. Finally, applying Forney's method to **s** and σ_1, gives $y_1 = i$. Therefore, the error pattern is given by $\mathbf{e} = (0, i, 0, 0)$.

Example 2.4. As in Example 2.2, if the received vector is $\mathbf{b} = (0, 0, 1, 0, 0, 0, 0, 0, i, 0, 0)$, then the syndrome vector is given by

$$\mathbf{s} = \mathbf{b}H^t = (\alpha^{12} + i\alpha^{14}, \alpha^{14} + i\alpha^8, \alpha + i\alpha^2, \alpha^3 + i\alpha^{11}).$$

Applying the modified Berlekamp-Massey algorithm, the following table is obtained

n	$\sigma^{(n)}(z)$	d_n	l_n	$n - l_n$
-1	1	1	0	-1
0	1	$\alpha^{12} + i\alpha^{14}$	0	0
1	$1 + (\alpha^{12} + i\alpha^{14})z$	$\alpha^{11} + i\alpha^8$	1	0
2	$1 + (\alpha^{13} + i\alpha^{12})z$	$\alpha^7 + i\alpha^5$	1	1
3	$1 + (\alpha^{10} + i\alpha^{14})z + (\alpha^{12} + i)z^2$	$\alpha^{12} + i\alpha^{12}$	2	1
4	$1 + \alpha^{11}z + \alpha^{11}z^2$	-	2	2

Thus $\sigma^{(4)}(z) = 1 + \alpha^{11}z + \alpha^{11}z^2$. The roots of $\rho(z) = z^2 + \alpha^{11}z + \alpha^{11}$ (the reciprocal of $\sigma^{(4)}(z)$) are $z_1 = \alpha^2$ and $z_2 = \alpha^9$. Among the elements $1, \alpha, \alpha^2, \cdots, \alpha^{14}$, we have $x_1 = \alpha^2$ and $x_2 = \alpha^9$ are such that $x_1 - z_1 = x_2 - z_2 = 0$ are zero divisors in $\mathcal{R}$. Therefore, x_1 and x_2 are the correct error-location numbers and $k_3 = 2$ and $k_9 = 9$ indicates that two errors have occurred, one in position 3, and the other in position 9, in the codeword. The correct elementary symmetric functions σ_1 and σ_2 are obtained from $(x - x_1)(x - x_2) = x^2 + \sigma_1 x + \sigma_2$. Thus, $\sigma_1 = \sigma_2 = \alpha^{11}$. Finally, Forney's method applied to **s**, σ_1 and σ_2, gives $\sigma_{11} = \sigma_1 + x_1\sigma_{10} = \alpha^{11} + \alpha^2 = \alpha^9$ and $\sigma_{21} = \sigma_1 + x_2\sigma_{20} = \alpha^{11} + \alpha^9 = \alpha^2$. Thus, by Equation (3), we obtain $y_1 = 1$ and $y_2 = i$. Therefore, the error pattern is given by $\mathbf{e} = (0, 0, 1, 0, 0, 0, 0, 0, i, 0, 0)$.

3 Srivastava codes

In this section we define another subclass of alternant codes over local finite commutative rings which is very similar to the one proposed by J. N. Srivastava in 1967, in an unpublished paper [10], called Srivastava codes. These codes over finite fields 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 $0, \alpha_1^{-1}, \alpha_2^{-1}, \cdots, \alpha_r^{-1}$ and $l \ge 0$.

Definition 3.1. *A shortened Srivastava code of length $n \le s$ over $\mathcal{A}$ has parity-check matrix*

$$H = \begin{bmatrix} \frac{\alpha_1^l}{\alpha_1 - \beta_1} & \frac{\alpha_2^l}{\alpha_2 - \beta_1} & \cdots & \frac{\alpha_n^l}{\alpha_n - \beta_1} \\ \frac{\alpha_1^l}{\alpha_1 - \beta_2} & \frac{\alpha_2^l}{\alpha_2 - \beta_2} & \cdots & \frac{\alpha_n^l}{\alpha_n - \beta_2} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{\alpha_1^l}{\alpha_1 - \beta_r} & \frac{\alpha_2^l}{\alpha_2 - \beta_r} & \cdots & \frac{\alpha_n^l}{\alpha_n - \beta_r} \end{bmatrix}, \tag{4}$$

where $\alpha_1, \cdots, \alpha_n, \beta_1, \cdots, \beta_r$ are $n + m$ distinct elements of $\mathcal{G}_s$ and $l \ge 0$.

Theorem 3.1. *The Srivastava code has minimum Hamming distance $d \ge r + 1$.*

Proof. 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

$$H_1 = \begin{bmatrix} \frac{\alpha_{i_1}^l}{\alpha_{i_1} - \beta_1} & \frac{\alpha_{i_2}^l}{\alpha_{i_2} - \beta_1} & \cdots & \frac{\alpha_{i_r}^l}{\alpha_{i_r} - \beta_1} \\ \frac{\alpha_{i_1}^l}{\alpha_{i_1} - \beta_2} & \frac{\alpha_{i_2}^l}{\alpha_{i_2} - \beta_2} & \cdots & \frac{\alpha_{i_r}^l}{\alpha_{i_r} - \beta_2} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{\alpha_{i_1}^l}{\alpha_{i_1} - \beta_r} & \frac{\alpha_{i_2}^l}{\alpha_{i_2} - \beta_r} & \cdots & \frac{\alpha_{i_r}^l}{\alpha_{i_r} - \beta_r} \end{bmatrix} \tag{5}$$

is nonsingular for any subset $\{i_1, \cdots, i_r\}$ of $\{1, 2, \cdots, n\}$. The determinant of this matrix can be expressed as

$$\det(H_1) = (\alpha_{i_1}\alpha_{i_2}\ldots\alpha_{i_r})^l \det(H_2), \tag{6}$$

where the matrix H_2 is given by

$$H_2 = \begin{bmatrix} \frac{1}{\alpha_{i_1}-\beta_1} & \frac{1}{\alpha_{i_2}-\beta_1} & \cdots & \frac{1}{\alpha_{i_r}-\beta_1} \\ \frac{1}{\alpha_{i_1}-\beta_2} & \frac{1}{\alpha_{i_2}-\beta_2} & \cdots & \frac{1}{\alpha_{i_r}-\beta_2} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{1}{\alpha_{i_1}-\beta_r} & \frac{1}{\alpha_{i_2}-\beta_r} & \cdots & \frac{1}{\alpha_{i_r}-\beta_r} \end{bmatrix}. \tag{7}$$

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

$$\det(H_1) = (\alpha_{i_1}\alpha_{i_2}\ldots\alpha_{i_r})^l \; k \; \frac{\phi(\alpha_{i_1}, \alpha_{i_2}, \cdots, \alpha_{i_r})\phi(\beta_1, \beta_2, \cdots, \beta_r)}{\mu(\alpha_{i_1})\mu(\alpha_{i_2})\ldots\mu(\alpha_{i_r})}, \tag{8}$$

where $k = (-1)^m$, $m = \binom{r}{2}$, $\phi(\alpha_{i_1}, \alpha_{i_2}, \ldots, \alpha_{i_r}) = \prod_{i_j < i_h}(\alpha_{i_j} - \alpha_{i_h})$ and $\mu(x) = (x-\beta_1)(x-\beta_2)\cdots(x-\beta_r)$. Then by [9, Theorem 7] we have $\det(H_1)$ is a unit in $\mathcal{R}$ and therefore $d \geq r+1$.

Definition 3.2. *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 $n \leq s$ over $\mathcal{A}$ has parity-check matrix*

$$H = \begin{bmatrix} H_1 \\ H_2 \\ \vdots \\ H_k \end{bmatrix}, \tag{9}$$

where

$$H_j = \begin{bmatrix} \frac{w_1}{\alpha_1-\beta_j} & \frac{w_2}{\alpha_2-\beta_j} & \cdots & \frac{w_n}{\alpha_n-\beta_j} \\ \frac{w_1}{(\alpha_1-\beta_j)^2} & \frac{w_2}{(\alpha_2-\beta_j)^2} & \cdots & \frac{w_n}{(\alpha_n-\beta_j)^2} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{w_1}{(\alpha_1-\beta_j)^l} & \frac{w_2}{(\alpha_2-\beta_j)^l} & \cdots & \frac{w_n}{(\alpha_n-\beta_j)^l} \end{bmatrix}, \qquad (10)$$

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

Theorem 3.2. *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 2.1(3) and of the Theorem 3.1, since the matrices (1) and (9) are equivalent, with $g(z) = \prod_{i=1}^{k}(z - \beta_i)^l$.

Example 3.1. As in Example 2.2, if

$$n = 8,\ r = 6,\ k = 2,\ l = 3,$$
$$\{\alpha_1, \alpha_2, \cdots, \alpha_8\} = \{\alpha^4, \alpha^3, \alpha^5, \alpha, \alpha^7, \alpha^{12}, \alpha^{10}, \alpha^2\},$$
$$\{\beta_1, \beta_2\} = \{\alpha^9, \alpha^6\} \text{ and } \{w_1, \cdots, w_8\} = \{\alpha, \alpha, \alpha^2, \alpha^4, \alpha^7, \alpha^{10}, \alpha^9, \alpha^3\},$$

then the matrix

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

is the parity-check matrix of a generalized Srivastava code over $\mathbb{Z}_2[i]$ of length 8 and minimum distance at least 7.

4 Conclusions

In this paper we presented construction and decoding procedure for Goppa codes over local finite commutative rings with identity. The decoding procedure is based on the modified Berlekamp-Massey algorithm. The complexity of the proposed decoding algorithm is essentially the same as that for Goppa codes over finite fields. Furthermore, we present the construction of Srivastava codes over local finite commutative rings with identity.

5 Acknowledgments

This paper has been supported by Fundação de Amparo à Pesquisa do Estado de São Paulo – FAPESP – 02/07473-7.

REFERENCES

[1] A.A. Andrade and R. Palazzo Jr., Hamming and Reed-Solomon codes over certain rings, *Computational and Applied Mathematics*, **20** (3) (2001), 289–306.

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

[3] A.A. Andrade, J.C. Interlando and R. Palazzo Jr., Alternant and BCH code over certain rings, *Computational and Applied Mathematics*, **22** (2) (2003), 233–247.

[4] V.D. Goppa, A new class of linear error-correcting codes, *Probl. Peredach. Inform.*, **6** (3) (1970), 24–30.

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

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

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

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

[9] A.A. Andrade and R. Palazzo Jr., A note on units of a local finite rings, *Revista de Matemática e Estatística*, **18** (2000), 213–222.

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