On Goppa and Srivastava Codes over Finite Rings

Antonio Aparecido de Andrade and Reginaldo Palazzo Jr.

Abstract— **Goppa and Srivastava have described interesting classes of linear noncyclic error-correcting codes over finite fields. In this work we present a construction technique of Goppa and Srivastava codes over local finite commutative rings with identity in terms of parity-check matrix and an efficient decoding procedure, based on the modified Berlekamp-Massey algorithm, is proposed for the Goppa codes.**

Keywords—**Galois ring, Goppa code, Srivastava code.**

Introduction

In this paper we describe a construction technique of Goppa and Srivastava codes over local finite rings. These constructions require working on Galois extension rings, where some properties of the Galois extension fields are lost. First, we review the key properties of Galois extension rings, which serve to characterize these codes.

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 a positive integer, and $\mathcal{A}[x]$ denotes the ring of polynomials in the variable x over $\mathcal{A}$. The natural projection $\mathcal{A}[x] \rightarrow \mathbb{K}[x]$ 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 $\mathcal{A}[x]$ [1, 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 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 $\mathcal{M}_1 = \langle \mathcal{M}, f(x)\rangle$ and $\overline{\mathcal{M}_1} = \mathcal{M}_1/\langle f(x)\rangle$ 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 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 [1, Theorem XVIII.2]. This cyclic group has order $s = p^{mh}-1$.

This paper is organized as follows. In Section II we review a construction technique of BCH and alternant codes over finite local rings. In Section III, we describe a construction of Goppa codes over finite local rings. In Section IV we describe a construction of Srivastava codes over finite local rings. In Section V an efficient decoding procedure is proposed for Goppa codes.

Supported by FAPESP - 02/07473-7

Department of Mathematics - Ibilce - Unesp, Rua Cristovão Colombo, 2265, 15054-000, São José do Rio Preto, SP, Brazil. E-mail: andrade@mat.ibilce.unesp.br

Department of Telematics - Feec - Unicamp, P.O. Box 6101, 13083-852, Campinas, SP, Brazil. E-mail: palazzo@dt.fee.unicamp.br

I. BCH AND ALTERNANT CODES

In this section we review a construction technique of BCH and alternant codes [2], [3] over local finite rings.

Definition I.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 distincts) of $\mathcal{G}_s$. Then the set of all vectors

$$(w_1 f(\alpha_1), w_2 f(\alpha_2), \cdots, w_n f(\alpha_n)), \tag{1}$$

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

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

Definition I.2: [2, Definition 2.2] A shortened **BCH code** $\mathcal{C}(n,\eta)$ of length $n \leq s$ over $\mathcal{A}$ has parity-check matrix

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

for some $r \geq 1$, where $\eta = (\alpha_1, \alpha_2, \cdots, \alpha_n)$ 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.

Theorem I.1: [2, Theorem 2.4] The minimum Hamming distance of a BCH code $\mathcal{C}(n,\eta)$ satisfies $d \geq r+1$.

Definition I.3: [3, Definition 2.1] A shortened **alternant code** $\mathcal{C}(n,\eta,\mathbf{w})$ of length $n \leq s$ over $\mathcal{A}$ has parity-check matrix

$$H = \begin{bmatrix} w_1 & w_2 & \cdots & w_n \\ w_1\alpha_1 & w_2\alpha_2 & \cdots & w_n\alpha_n \\ w_1\alpha_1^2 & w_2\alpha_2^2 & \cdots & w_n\alpha_n^2 \\ \vdots & \vdots & \ddots & \vdots \\ w_1\alpha_1^{r-1} & w_2\alpha_2^{r-1} & \cdots & w_n\alpha_n^{r-1} \end{bmatrix}, \tag{3}$$

where r is a positive integer and $\eta = (\alpha_1, \alpha_2, \cdots, \alpha_n)$ is the locator 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 of $\mathcal{G}_s$.

Theorem I.2: [3, Theorem 2.1] The code $\mathcal{C}(n,\eta,\mathbf{w})$ has minimum Hamming distance $d \geq r+1$.

Example I.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 $\eta = (\alpha^5, \alpha, 1, \alpha^4, \alpha^2, \alpha^6, \alpha^3)$ be the locator vector, and set $\mathbf{w} = (\alpha^5, \alpha, 1, \alpha^4, \alpha^2, \alpha^6, \alpha^3)$. If $r = 2$, then the following matrix

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

is the parity-check matrix of an alternant code $\mathcal{C}(7, \eta, \mathbf{w})$.

Example I.2: Another example of an alternant code is a BCH code.

II. Goppa Codes

In this section we define an interesting subclass of alternat codes over local finite rings which is very similar to the one proposed by Goppa [4] 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 constrast to cyclic codes, where it is difficult to estimate the minimum Hamming distance d from the generator polynomial, Goppa codes have the property that $d \geq deg(g(z)) + 1$.

For this, let $\mathcal{A}$, $\mathcal{R}$ and $\mathcal{G}_s$ as in Section I. 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 $L = \{\alpha_1, \alpha_2, \cdots, \alpha_n\} = \{\alpha^{k_1}, \alpha^{k_2}, \cdots, \alpha^{k_n}\}$ 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 II.1: A shortened **Goppa code** $\mathcal{C}(L, g)$ of length $n \leq s$ over $\mathcal{A}$ has parity-check matrix

$$H = \begin{bmatrix} g(\alpha_1)^{-1} & \cdots & g(\alpha_n)^{-1} \\ \alpha_1 g(\alpha_1)^{-1} & \cdots & \alpha_n g(\alpha_n)^{-1} \\ \vdots & \ddots & \vdots \\ \alpha_1^{r-1} g(\alpha_1)^{-1} & \cdots & \alpha_n^{r-1} g(\alpha_n)^{-1} \end{bmatrix}. \quad (4)$$

Definition II.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, for all $\mathbf{c} = (c_1, c_2, \cdots, c_n) \in \mathcal{C}(L, g)$, it is true that $\mathbf{c}' = (c_n, c_{n-1}, \cdots, c_1) \in \mathcal{C}(L, g)$, 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 comutative Goppa code.
- If $g(z)$ has no multiple zeros then $\mathcal{C}(L, g)$ is called a separable Goppa code.

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

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

which is row equivalent to

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

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

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)

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

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

5. Goppa codes are alternant codes, where $\eta = (\alpha_1, \alpha_2, \cdots, \alpha_n)$ and $\mathbf{w} = (g(\alpha_1)^{-1}, g(\alpha_2)^{-1}, \cdots, g(\alpha_n)^{-1})$.

Theorem II.1: The 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 $\mathbf{w} = (g(\alpha_1)^{-1}, \cdots, g(\alpha_n)^{-1})$. Therefore by Theorem I.2 we have that $\mathcal{C}(L, g)$ has minimum distance $d \geq r + 1$.

Example II.1: Referring to Example I.1, letting $L = \{1, \alpha, \alpha^2, \alpha^4\}$, $\eta = (\alpha, \alpha^4, 1, \alpha^2)$, $g(z) = z^3 + z^2 + 1$ and

$\mathbf{w} = (g(\alpha)^{-1}, g(\alpha^4)^{-1}, g(1)^{-1}, g(\alpha^2)^{-1}) = (\alpha^3, \alpha^5, 1, \alpha^6)$, we have a Goppa code over $GF(2)[i]$ with parity-check matrix given by

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

length 4 and minimum Hamming distance at least 4.

Example II.2: 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 $g(z) = z^4 + z^3 + 1$, $L = \{1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6, \alpha^7, \alpha^8, \alpha^9, \}$ and $\mathbf{w} = (1, \alpha^{12}, \alpha^{10}, \alpha^7, \alpha^3, \alpha^{11}, \alpha^6, \alpha^9, \alpha^5, \alpha^{14})$. The matrix given by

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

is the parity-check matrix of a Goppa code over $GF(2)[i]$ of length 10 and minimum Hamming distance at least 5.

III. SRIVASTAVA CODES

In this section 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 an unpublished work, 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 III.1: A shortened **Srivastava code** of length $n \le s$ over $\mathcal{A}$ has parity-check matrix

$$H = \begin{bmatrix} \frac{\alpha_1^l}{\alpha_1-\beta_1} & \frac{\alpha_2^l}{\alpha_2-\beta_1} & \cdots & \frac{\alpha_n^l}{\alpha_n-\beta_1} \\ \frac{\alpha_1^l}{\alpha_1-\beta_2} & \frac{\alpha_2^l}{\alpha_2-\beta_2} & \cdots & \frac{\alpha_n^l}{\alpha_n-\beta_2} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{\alpha_1^l}{\alpha_1-\beta_r} & \frac{\alpha_2^l}{\alpha_2-\beta_r} & \cdots & \frac{\alpha_n^l}{\alpha_n-\beta_r} \end{bmatrix}, \tag{5}$$

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

Theorem III.1: 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

$$H_1 = \begin{bmatrix} \frac{\alpha_{i_1}^l}{\alpha_{i_1}-\beta_1} & \frac{\alpha_{i_2}^l}{\alpha_{i_2}-\beta_1} & \cdots & \frac{\alpha_{i_r}^l}{\alpha_{i_r}-\beta_1} \\ \frac{\alpha_{i_1}^l}{\alpha_{i_1}-\beta_2} & \frac{\alpha_{i_2}^l}{\alpha_{i_2}-\beta_2} & \cdots & \frac{\alpha_{i_r}^l}{\alpha_{i_r}-\beta_2} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{\alpha_{i_1}^l}{\alpha_{i_1}-\beta_r} & \frac{\alpha_{i_2}^l}{\alpha_{i_2}-\beta_r} & \cdots & \frac{\alpha_{i_r}^l}{\alpha_{i_r}-\beta_r} \end{bmatrix} \tag{6}$$

is nonsingular for any subset $\{i_1, i_2, \cdots, i_r\}$ of $\{1, 2, \cdots, n\}$. The determinant of this matrix can be expressed as

$$det(H_1) = (\alpha_{i_1}\alpha_{i_2}\ldots\alpha_{i_r})^l det(H_2), \tag{7}$$

where the matrix H_2 is given by

$$H_2 = \begin{bmatrix} \frac{1}{\alpha_{i_1}-\beta_1} & \frac{1}{\alpha_{i_2}-\beta_1} & \cdots & \frac{1}{\alpha_{i_r}-\beta_1} \\ \frac{1}{\alpha_{i_1}-\beta_2} & \frac{1}{\alpha_{i_2}-\beta_2} & \cdots & \frac{1}{\alpha_{i_r}-\beta_2} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{1}{\alpha_{i_1}-\beta_r} & \frac{1}{\alpha_{i_2}-\beta_r} & \cdots & \frac{1}{\alpha_{i_r}-\beta_r} \end{bmatrix}. \tag{8}$$

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

$$det(H_1) = (\alpha_{i_1}\alpha_{i_2}\ldots\alpha_{i_r})^l \delta \tag{9}$$

where $\delta = \frac{(-1)^{\binom{r}{2}} \phi(\alpha_{i_1}, \alpha_{i_2}, \cdots, \alpha_{i_r})\phi(\beta_1, \beta_2, \cdots, \beta_r)}{\nu(\alpha_{i_1})\nu(\alpha_{i_2})\ldots\nu(\alpha_{i_r})}$, $\phi(\alpha_{i_1}, \alpha_{i_2}, \ldots, \alpha_{i_r}) = \prod_{i_j < i_h}(\alpha_{i_j} - \alpha_{i_h})$ and $\nu(x) = (x - \beta_1)(x - \beta_2)\cdots(x - \beta_r)$. By [5, Theorem 7] we have that $det(H_1)$ is a unit in $\mathcal{R}$ and therefore $d \ge r + 1$.

Definition III.2: Suppose $r = kl$ and let $\alpha_1, \alpha_2, \cdots, \alpha_n$, $\beta_1, \cdots, \beta_k$ 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 $n \le s$ over $\mathcal{A}$ has parity-check matrix

$$H = \begin{bmatrix} H_1 \\ H_2 \\ \vdots \\ H_k \end{bmatrix}, \tag{10}$$

where

$$H_j = \begin{bmatrix} \frac{w_1}{\alpha_1-\beta_j} & \frac{w_2}{\alpha_2-\beta_j} & \cdots & \frac{w_n}{\alpha_n-\beta_j} \\ \frac{w_1}{(\alpha_1-\beta_j)^2} & \frac{w_2}{(\alpha_2-\beta_j)^2} & \cdots & \frac{w_n}{(\alpha_n-\beta_j)^2} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{w_1}{(\alpha_1-\beta_j)^l} & \frac{w_2}{(\alpha_2-\beta_j)^l} & \cdots & \frac{w_n}{(\alpha_n-\beta_j)^l} \end{bmatrix}, \tag{11}$$

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

Theorem III.2: The generalized Srivastava code has minimum Hamming distance $d \ge kl + 1$.

Proof: The proof of this theorem requires nothing more than the application of the Remark II.1(3) and of the Theorem III.1, since the matrices (4) and (10) are equivalents, where $g(z) = \prod_{i=1}^{k}(z-\beta_i)^l$

Example III.1: Referring to Example II.2, if $n = 5$, $r = 4$, $k = 2$, $l = 2$, $\{\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5\} = \{\alpha^4, \alpha^3, \alpha^5, \alpha, \alpha^7\}$, $\{\beta_1, \beta_2\} = \{\alpha^9, \alpha^6\}$, $\{w_1, w_2, w_3, w_4, w_5\} = \{\alpha, \alpha, \alpha^2, \alpha^4, \alpha^7\}$, then the matrix

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

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

IV. Decoding Procedure

In this section we present a decoding algorithm for Goppa codes $\mathcal{C}$, as defined in Section III. 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 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. Let $\mathbf{b} = (b_1, b_2, \cdots, b_n)$ 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 locator 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

$$s_l = \sum_{j=1}^{n} e_j w_j \alpha_j^l, \quad l \geq 0.$$

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 $y_1 = e_{i_1}, y_2 = e_{i_2}, \cdots, y_\nu = e_{i_\nu}$.

The first r syndrome values s_l can be calculated from the received vector $\mathbf{b}$ as

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

The decoding algorithm being proposed consists of four major steps:

Step 1 - Calculation of the syndrome vector $\mathbf{s} = (s_0, \cdots, s_{r-1})$ from the received vector.

Step 2 - Calculation of the elementary symmetric functions $\sigma_1, \sigma_2, \cdots, \sigma_\nu$ from $\mathbf{s}$.

Step 3 - Calculation of the error-location numbers $x_1, \cdots, x_\nu$ from $\sigma_1, \sigma_2, \cdots, \sigma_\nu$.

Step 4 - Calculation of the error magnitudes $y_1, y_2, \cdots, y_\nu$ from x_i and $\mathbf{s}$.

Now, each step of the decoding algorithm is analysed. There is no need to comment on Step 1 since the calculation of the syndromes is straightforward. The set of error-location numbers is a subset of $\{\alpha^0, \alpha^1, \cdots, \alpha^{s-1}\}$. The elementary symmetric functions $\sigma_1, \sigma_2, \cdots, \sigma_\nu$ (where ν denotes the number of errors introduced by the channel) are defined as the coefficients of the polynomial

$$(x-x_1)(x-x_2)\cdots(x-x_\nu) = x^\nu + \sigma_1 x^{\nu-1} + \cdots + \sigma_{\nu-1}x + \sigma_\nu.$$

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 $\mathcal{R}$

$$s_{j+\nu} + s_{j+\nu-1}\sigma_1 + \cdots + s_{j+1}\sigma_{\nu-1} + s_j\sigma_\nu = 0, \qquad (12)$$

where $j = 0, 1, 2, \cdots, (r-1)-\nu$ and $s_0, s_1, \cdots, s_{r-1}$ are the components of the syndrome vector. We make use of the modified Berlekamp-Massey algorithm to find the solutions of Equation (12). This is possible since the proofs shown in [6] hold for commutative rings with identity as well.

The modified Berlekamp-Massey algorithm for commutative rings with identity is formulated as follows. The inputs to the algorithm are the syndromes $s_0, s_2, \cdots, s_{r-1}$ which belong to R. The output of the algorithm is a set of values $\sigma_i, 1 \leq i \leq \nu$, such that Equation (12) holds with minimum ν. Let $\sigma^{(-1)}(x) = 1, l_{-1} = 0, d_{-1} = 1$ and $\sigma^{(0)}(x) = 1, l_0 = 0, d_0 = s_1$ be the a set of initial conditions to start the algorithm. Thus, we have the following steps:

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 an $m \leq n-1$ such that $d_n - yd_m = 0$ has a solution in 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 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 (12). In Step 3, the solution to Equation (12) is generally not unique and the reciprocal of the polynomial $\sigma^{(r)}(z)$ (output by the modified Berlekamp-Massey algorithm), namely $\rho(z)$, may not be the correct error-locator polynomial

$$(z-x_1)(z-x_2)\cdots(z-x_\nu)$$

where $x_i = \alpha^{k_j}$ are the correct error-location numbers (j is an integer in the range $1 \leq j \leq n$ that indicates the position of the error in the codeword), ν is the number of errors, and α is the generator of $\mathcal{G}_s$. Thus, the procedure for the calculation of the correct error-location numbers is the following

- Compute the roots of $\rho(z)$ (the reciprocal of $\sigma^{(r)}(z)$), say, $z_1, z_2, \cdots, z_\nu$.
- Among the $x_i = \alpha^l, l = 1, 2 \cdots, s$, 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 $x_i = \alpha^{k_j}$, $j = 1, 2, \cdots, n$, indicates the position j of the error in the codeword.

In Step 4, the calculation of the error magnitudes is based on Forney's procedure [7]. The error magnitudes $y_1, y_2, \cdots, y_\nu$ are given by

$$y_j = \frac{\sum_{l=0}^{\nu-1} \sigma_{jl} s_{\nu-1-l}}{E_j \sum_{l=0}^{\nu-1} \sigma_{jl} x_j^{\nu-1-l}}, \quad j = 1, 2, \cdots, \nu \qquad (13)$$

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 $E_j = g(\alpha_{i_j})^{-1}$, $j = 1, 2, \cdots, \nu$, $i = 1, 2, \cdots, n$ are the corresponding location of errors in the vector $\mathbf{w}$. It follows from [5, Theorem 7] that the denominator in Equation (13) is always a unit in $\mathcal{R}$.

Example IV.1: Referring to Example II.1, if the received vector is given by $\mathbf{b} = (0, i, 0, 0)$, we have 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 zero divisor in $\mathcal{R}$. Therefore, x_1 is the correct error-location number, and since $k_2 = 4$ 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 $\mathbf{s}$ and σ_1, gives $y_1 = i$. Therefore, the error pattern is given by $\mathbf{e} = (0, i, 0, 0)$.

Example IV.2: Referring to Example II.2, if the received vector is $\mathbf{b} = (0, i, 0, 0, 0, 0, 0, 0, 0, 1)$, we have 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, we obtain the following table

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 number. We have $k_2 = 2$ and $k_{10} = 9$ indicate that two errors have occurred, one in position 2, and the other in position 10, 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 $\mathbf{s}$, 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 (13), we obtain $y_1 = 1$ and $y_2 = i$. Therefore, the error pattern is given by $\mathbf{e} = (0, 1, 0, 0, 0, 0, 0, 0, 0, i)$.

REFERENCES

[1] McDonald, B.R. *Finite rings with identity*. New York: Marcel Dekker, 1974. 429p.

[2] Andrade, A.A., Palazzo JR., R. Construction and decoding of BCH codes over finite commutative rings. *Linear Algebra Applic.* v.286, pp. 69-85, 1999.

[3] Andrade, A.A., Interlando, J.C., Palazzo Jr., R. Alternant and BCH code over certain rings. *Computational and Applied Mathematics*, to apppear 2003.

[4] Goppa, V.D. A new class of linear error-correcting codes. *Probl. Peredach. Inform.*, Vol. 6, No. 3, pp. 24-30, Sept. 1970.

[5] Andrade, A.A., Palazzo Jr., R. A note on units of a local finite rings. *Revista de Matemática e Estatística*, vol. 18, pp. 213-222, 2000.

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

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