International Journal of Applied Mathematics

Volume 27 No. 1 2014, 65-71
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)
doi: http://dx.doi.org/10.12732/ijam.v27i1.7

GOPPA CODES OVER CERTAIN SEMIGROUPS

Antonio Aparecido de Andrade[1 §], Tariq Shah[2],
Naveed Ahmed Azam[3], Syed Azmat Hussain[4]

[1]Department of Mathematics
São Paulo State University at São José do Rio Preto
São José do Rio Preto - SP, BRAZIL

[2]Department of Mathematics
Quaid-i-Azam University
Islamabad, PAKISTAN

[3]Faculty of Engineering Sciences Ghulam Ishaq Khan
Institute of Engineering Science and Technology
Topi Swabi, PAKISTAN

[4]School of Engineering and Applied Sciences (SEAS)
ISRA University
Islamabad Campus, PAKISTAN

Abstract: A Goppa code is described in terms of a polynomial, known as Goppa polynomial, and in contrast to cyclic codes, where it is difficult to estimate the minimum Hamming distance d from the generator polynomial. Furthermore, a Goppa code has the property that $d \geq deg(h(X)) + 1$, where $h(X)$ is a Goppa polynomial. In this paper, we present a decoding principle for Goppa codes constructed by generalized polynomials, which is based on modified Berlekamp-Massey algorithm.

AMS Subject Classification: 11T71, 20M25, 94B05, 94B40
Key Words: semigroup ring, Goppa code, modified Berlekamp-Massey algorithm

Received: January 13, 2014

[§]Correspondence author

1. Introduction

Let $(S, *)$ be a commutative semigroup and $(R, +, \cdot)$ a commutative associative ring. The set J of all finitely nonzero functions f from S into R is a ring with respect to binary operations addition and multiplication defined as $(f+g)(s) = f(s)+g(s)$ and $(fg)(s) = \sum_{t*u=s} f(t)g(u)$, where the symbol $\sum_{t*u=s}$ indicates that the sum is taken over all pairs (t, u) of elements of S such that $t*u = s$ and if s is not expressible in the form $t*u$ for any $t, u \in S$, then $(fg)(s) = 0$. The set J is known as *semigroup ring* of S over R. If S is a monoid, then J is called monoid ring. This ring J is represented as $B[S]$, where S is a multiplicative semigroup, and the elements of J are written either as $\sum_{s\in S} f(s)s$ or as $\sum_{i=1}^{n} f(s_i)s_i$. The representation of J will be $R[X; S]$ whenever S is an additive semigroup. As there is an isomorphism between additive semigroup S and multiplicative semigroup $\{X^s : s \in S\}$, it follows that a nonzero element f of $R[X; S]$ is uniquely represented in the canonical form $\sum_{i=1}^{n} f(s_i)X^{s_i} = \sum_{i=1}^{n} f_i X^{s_i}$, where $f_i \neq 0$ and $s_i \neq s_j$ for all $i \neq j$. Degree is not generally defined in commutative semigroup rings but if the semigroup S is a totally ordered semigroup, we can define the degree of a generalized polynomial of the semigroup ring $R[X; S]$. If $f = \sum_{i=1}^{n} f_i X^{s_i}$ is the canonical form of the nonzero element $f \in R[X; S]$, where $s_1 < s_2 < \cdots < s_n$, then s_n is called the degree of f and we write $deg(f) = s_n$.

2. Goppa Code

Let (B, N) be a finite local commutative ring with unity and $\mathbb{K}$ the residue field $\frac{B}{N} \cong GF(p^m)$, where p is a prime, m a positive integer. The natural projection $\pi : B[X; \frac{1}{3}\mathbb{Z}_0] \to \mathbb{K}[X; \frac{1}{3}\mathbb{Z}_0]$ is defined by $\pi(a(X^{\frac{1}{3}})) = \overline{a}(X^{\frac{1}{3}})$, i.e., $\pi(\sum_{i=0}^{n} a_i X^{\frac{1}{3}i}) = \sum_{i=0}^{n} \overline{a_i} X^{\frac{1}{3}i}$, where $\overline{a_i} = a_i + N$). Let $f(X^{\frac{1}{3}})$ be a monic pseudo polynomial of degree t in $B[X; \frac{1}{3}\mathbb{Z}_0]$ such that $\pi(f(X^{\frac{1}{3}}))$ is irreducible in $\mathbb{K}[X; \frac{1}{3}\mathbb{Z}_0]$. Since $B[X; \mathbb{Z}_0] \subseteq B[X; \frac{1}{3}\mathbb{Z}_0]$ [1, Theorem 7.2], it follows that $f(X^{\frac{1}{3}})$ is also irreducible in $B[X; \frac{1}{3}\mathbb{Z}_0]$, by [2, Theorem XIII.7]. If $\Re = \frac{B[X; \frac{1}{3}Z_0]}{(f(X^{\frac{1}{3}}))}$, then $\Re$ is a finite commutative local factor semigroup ring with unity and again by [1, Theorem 7.2] accommodate our notions to say that it is a Galois ring extension of B with extension degree t. Its residue field is $\mathbb{K}_1 = \frac{\Re}{N_1} = GF(p^{3mt})$, where N_1 is the maximal ideal of $\Re$, and $\mathbb{K}_1^*$ is the multiplicative group of $\mathbb{K}_1$ whose order is $p^{3mt} - 1$.

Let $\Re^*$ denote the multiplicative group of units of $\Re$ and $\Re^*$ being an Abelian

group can be expressed as a direct product of cyclic groups. Our focus is in the maximal cyclic subgroup of $\Re^*$, hereafter denoted by G_s, whose elements are the roots of $X^s - 1$ for some positive integer s. There is only one maximal cyclic subgroup of $\Re^*$ having order $s = p^{3mt} - 1$. Let $\beta = \alpha^{\frac{1}{3}}$ be a primitive element of the cyclic group G_s, where $s = p^{3mt} - 1$. Let $h(X^{\frac{1}{3}}) = h_0 + h_1 X^{\frac{1}{3}} + h_2(X^{\frac{1}{3}})^2 + \cdots + h_{3r}(X^{\frac{1}{3}})^{3r}$ be a polynomial with coefficients in $\Re$ and $h_{3r} \neq 0$. Let $T = \{\alpha_1, \alpha_2, \cdots, \alpha_n\}$ be a subset of distinct elements of G_s such that $h(\alpha_i)$ are units from $\Re$ for $i = 1, 2, \cdots, n$.

Definition 1. [3, Definition 4] A shortened Goppa code $C(T, h)$ of length $n \leq s$ is a code over B that has parity-check matrix

$$H = \begin{bmatrix} h(\alpha_1)^{-1} & \cdots & h(\alpha_n)^{-1} \\ \alpha_1 h(\alpha_1)^{-1} & \cdots & \alpha_n h(\alpha_n) \\ \vdots & \ddots & \vdots \\ \alpha_1^{3r-1} h(\alpha_1)^{-1} & \cdots & \alpha_n^{3r-1} h(\alpha_n) \end{bmatrix}, \tag{1}$$

where r is a positive integer, $\eta = (\alpha_1, \alpha_2, \cdots, \alpha_n)$ is the locator vector, consisting of distinct elements of G_s and $\omega = (h(\alpha_1)^{-1}, \cdots, h(\alpha_n)^{-1})$ is a vector consisting on elements of G_s.

Theorem 1. (see Theorem 7, [4]) *The Goppa code $C(T, h)$ has minimum Hamming distance $d \geq 3r + 1$.*

3. Decoding Procedure

The decoding algorithm is based on the modified Berlekamp-Massey algorithm [5] which corrects all errors up to the Hamming weight $t \leq \frac{3r}{2}$, i.e., whose minimum Hamming distance is $3r + 1$. The decoding procedure for these codes consists of four major steps: calculation of the syndromes, calculation of the error-locator polynomial, calculation of the error-location numbers, and calculation of the error magnitudes.

Let $\beta = \alpha^{\frac{1}{3}}$ be a primitive element of the cyclic group G_s, where $s = p^{3mt} - 1$. 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 $\mathbf{e} = (e_1, e_2, \cdots, e_n) = \mathbf{b} - \mathbf{c}$. Let $\eta = (\alpha_1, \alpha_2, \cdots, \alpha_n) = (\beta^{k_1}, \beta^{k_2}, \cdots, \beta^{k_n})$ be a vector over G_s. Suppose that $\nu \leq t$ is the number of errors which occurred at locations $x_1 =$

$\alpha_{i_1}, x_2 = \alpha_{i_2}, \cdots, x_\nu = \alpha_{i_\nu}$ with values $y_1 = e_{i_1}, y_2 = e_{i_2}, \cdots, y_\nu = e_{i_\nu}$. The *syndrome values* s_l of an error vector $\mathbf{e} = (e_1, e_2, \cdots, e_n)$ is defined as

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

Since $\mathbf{s} = (s_0, s_1, \cdots, s_{3r-1}) = \mathbf{b}H^t = \mathbf{e}H^t$, it follows that the first $3r$ syndrome values s_l can be calculated from the received vector $\mathbf{b}$ as follow

$$s_l = \sum_{j=1}^{n} e_j h(\alpha_j)^{-1} \alpha_j^l = \sum_{j=1}^{n} b_j h(\alpha_j)^{-1} \alpha_j^l, \quad \text{for} \quad l = 0, 1, 2, \cdots, 3r-1.$$

The elementary symmetric functions $\sigma_1, \sigma_2, \cdots, \sigma_\nu$ of the error-location numbers $x_1, \cdots, x_\nu$ 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: calculation of the syndrome vector $\mathbf{s}$ from the received vector; calculation of the elementary symmetric functions $\sigma_1, \sigma_2, \cdots, \sigma_\nu$ from $\mathbf{s}$, using the modified Berlekamp-Massey algorithm [5]; calculation of the error-location numbers $x_1, x_2, \cdots, x_\nu$ from $\sigma_1, \sigma_2, \cdots, \sigma_\nu$, that are roots of $\sigma(X)$; and calculation of the error magnitudes $y_1, y_2, \cdots, y_\nu$ from x_i and $\mathbf{s}$, using Forney's procedure [6].

Since the calculation of the vector syndrome is straightforward, it follows that there is no need to comment on Step 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 $\Re$, i.e.,

$$s_{j+\nu} + s_{j+\nu-1}\sigma_1 + \cdots + s_{j+1}\sigma_{\nu-1} + s_j\sigma_\nu = 0, \quad \text{for} \quad j = 0, 1, 2, \cdots, (3r-1) - \nu, \tag{3.1}$$

where $s_0, s_1, \cdots, s_{3r-1}$ are the components of the syndrome vector. From the modified Berlekamp-Massey algorithm, it follows that the solutions of Equation (3.1). The algorithm is iterative, in the sense that the following $n - l_n$ equations

(called *power sums*)

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

are satisfied with l_n as small as possible and $\sigma_0^{(0)} = 1$. The polynomial $\sigma^{(n)}(X) = \sigma_0^{(n)} + \sigma_1^{(n)}X + \cdots + \sigma_{l_n}^{(n)}X^n$ 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 is formulated as: the inputs to the algorithm are the syndromes $s_0, s_1, \cdots, s_{3r-1}$ which belong to $\Re$. The output of the algorithm is a set of values σ_i, for $i = 1, 2, \cdots, \nu$, such that Equation (3.1) 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 [7]. 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 $\Re$. If such a solution is found, $\sigma^{(n+1)}(X) \leftarrow D^{(n+1)}(X)$ and $l_{n+1} \leftarrow l$.

5. If $n < 3r-1$, 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 $n < 3r-1$ go to 2); else stop.

The coefficients $\sigma_1^{(3r)}, \sigma_2^{(3r)}, \cdots, \sigma_\nu^{(3r)}$ satisfy Equation (3.1).

At Step 3, the set of possible error-location numbers is a subset of G_s and the solution to Equation (3.1) is generally not unique and the reciprocal polynomial $\rho(Z)$ of the polynomial $\sigma^{(3r)}(Z)$ (output by the modified Berlekamp-Massey algorithm), may not be the correct error-locator polynomial $(Z - x_1)(Z - x_2)\cdots(Z - x_\nu)$, where $x_j = \beta^{k_i}$, for $j = 1, 2, \cdots, \nu$ and $i = 1, 2, \cdots, n$, are the correct error-location numbers. Now, compute the roots $z_1, z_2, \cdots, z_\nu$ of $\rho(Z)$, and among the $x_i = \beta^{k_j}$, for $j = 1, 2\cdots, n$, select those x_i's such that $x_i - z_i$ are zero divisors in $\Re$. The selected x_i's will be the correct error-location numbers and each k_j, for $j = 1, 2, \cdots, n$, indicates the position j of the error in the codeword.

At Step 4, the calculation of the error magnitude is based on Forney′s procedure [6]. The error magnitude is given by

$$y_j = \frac{\sum_{l=0}^{\nu-1} \sigma_{jl} s_{\nu-1-l}}{E_j \sum_{l=0}^{\nu-1} \sigma_{jl} x_j^{\nu-1-l}}, \tag{3.2}$$

for $j = 1, 2, \cdots, \nu$, where the coefficients σ_{jl} are recursively defined by $\sigma_{j,i} = \sigma_i + x_j \sigma_{j,i-1}$, for $i = 0, 1, \cdots, \nu - 1$, starting with $\sigma_0 = \sigma_{j,0} = 1$. The $E_j = h(x_i)^{-1}$, for $i = 1, 2, \cdots, \nu$, are the corresponding location of errors in the vector $\mathbf{w}$. It follows from [4] that the denominator in Equation (3.2) is always a unit in $\Re$.

Example 1. Let $B = GF(2)[i]$ and $\Re = \frac{B[X; \frac{1}{3} Z_0]}{(f(X^{\frac{1}{3}}))}$, where $f(X^{\frac{1}{3}}) = (X^{\frac{1}{3}})^9 + (X^{\frac{1}{3}})^3 + 1$ is irreducible over B. If $X^{\frac{1}{3}} = Y$, then $f(Y) = Y^9 + Y^3 + 1$. If $\beta = \alpha^{\frac{1}{3}}$ is a root of $f(Y)$, then $\alpha^{\frac{1}{3}}$ generates a cyclic group G_s of order $s = 2^{3(3)} - 1$. If $h(X^{\frac{1}{3}}) = (X^{\frac{1}{3}})^4 + (X^{\frac{1}{3}})^3 + 1$, $T = \{\alpha, \alpha^5, \alpha^2, 1, \alpha^3, \alpha^{\frac{7}{2}}, \alpha^4, \alpha^6\}$ and $\omega = \{\alpha^2, \alpha^4, \alpha^4, 1, \alpha, \alpha^{\frac{1}{2}}, \alpha^3, \alpha^2\}$, then

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

is the parity check matrix of a Goppa code over B of length 8 and, by Theorem 1, the minimum Hamming distance is at least 5. Now, if the received vector is given by $b = (0, i, 0, 0, 0, 0, 0, 0)$, then the syndrome vector is given by $s = bH^t = (i\alpha^3, i\alpha, i\alpha^6, i\alpha^4)$. Applying the modified Berlekamp-Massey algorithm, it follows that $\sigma^{(4)}(Z) = 1 + \alpha^5 Z$. The root of $\rho(Z) = Z + \alpha^5$ (the reciprocal of $\sigma^{(4)}(Z)$ is $z_1 = \alpha^5$. Among the elements of G_s it follows that $x_1 = \alpha^5$

is such that $x_1 - z_1 = 0$ is a zero divisor in $\Re$. Therefore, x_1 is the correct error-location number, and $k_2 = 5$ indicates that one error has occurred in the second coordinate of the codeword. Finally, applying Forney's method to s and x_1, gives $y_1 = i$. Therefore, the error pattern is given by $e = (0, i, 0, 0, 0, 0, 0, 0)$.

Acknowledgments

We acknowledge the financial support 2013/04124-6 by FAPESP.

References

[1] R. Gilmer, *Commutative Semigroup Rings*, University Chicago Press, Chicago and London (1984).

[2] B.R. McDonald, *Finite Rings with Identity*, Marcel Dekker, New York (1974).

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

[4] A.A. Andrade, R. Palazzo Jr., Linear codes over finite rings, *Tend. Mat. Apl. Comput.*, **6**, No 2 (2005), 207-217.

[5] 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.

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

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