ISSN 2277-3061
Volume 15 Number 5
International Journal of Computers and Technology

EXTENDED SUBCLASS OF CYCLIC SEPARABLE GOPPA CODES

O.P VINOCHA[1] , AJAY KUMAR[2]
[1] I.K GUJRAL PUNJAB TECHNICAL UNIVERSITY, JALANDHAR.
Email: vinochar@yahoo.com
[2] PhD Scholar, I.K GUJRAL PUNJAB TECHNICAL UNIVERSITYJALANDHAR, PUNJAB, INDIA .
E-mail: sharmaajay8426@yahoo.com

ABSTRACT

In 2013 , a new subclass of cyclic Goppa code with Goppa polynomial of degree 2 is presented by Bezzateev and Shekhunova. They proved that this subclass contains all cyclic codes of considered length. In the present work we consider a Goppa polynomial of degree three and proved that the subclass generated by this polynomial represent a cyclic, reversible and separable Goppa code.

Indexing terms

Goppa Codes ; Cyclic Goppa Codes ; Seperable Goppa Codes and Reversible Goppa Codes.

.

INTRODUCTION

The Russian mathematician N.V. Goppa [2] proposed an extended class of BCH code that is known as Goppa code. This class contains BCH codes as a special case and also meets the Gilbert bound for long n. After the existence of these codes, it is possible to design an error processor modeled on Peterson's BCH error processor. The Sugiyama, Hirasawa and Namakwa error processor, derived from Euclid's algorithm was actually designed for these classical Goppa codes, after that Goppa extending his definition by means of algebraic curves over a field. This new geometric class of code contains many explicit codes that exceed the Gilbert bound. These codes have an efficient decoding algorithm and also useful for applications in cryptography.

THE GOOPA CODE:

Let $F \subseteq E$ be the finite field, let g(z) be a polynomial over field E and let P= { $\mu_1 , \mu_2 \dots \dots \mu_n$} be the set of elements with the condition that none of μ_i is root of g(z) . then the Goppa code is defined as the set of codewords $d \in f^n$ such that

$$S(z) = \sum_{j=1}^{n} \frac{d_j}{(z-\mu_j)} \equiv 0 \pmod{g(z)}. \quad [2]$$

Definition 1: A code C is called reversible if for any codeword d= ($d_1 , d_2 \dots\dots d_n$)$\in C$ the code also contains the codeword d^*= ($d_n , d_{n-1} \dots\dots d_1$,) $\in C$ [1].

Definiation2: A Goppa code is called separable if the Goppa polynomial g(x) does not have multiple roots [1].

Bezzateev and Shekhunova [4] presented a subclass of Goppa code and proved that all reversible cyclic codes, defined by a polynomial g(x) = $x^2 + Ax + 1$ with the roots $1 , \alpha^{\pm 1}$ where $\alpha \in GF(2^n)$ are separable Goppa codes. However the subclass of code with g(x) of degree greater than 3 remains an open problem. In this paper, we proposed a subclass of Goppa code by extending the degree of g(x) =$x^3 + Bx^2$+1 with the roots ω , ω^{-1} and ω^{-2} and location set L= {$\mu_1 , \mu_2 \dots \dots \mu_n$}. We prove that this subclass is a cyclic, reversible and separable Goppa code.

2: EXTENDED SUBCLASS OF CYCLIC REVERSIBLE SEPARABLE GOPPA CODES

We consider a location set P and Goppa polynomial G(x) of degree 3. Any codeword (x_1 , x_2…….x_n) of code (P,G) Code satisfies the condition $\sum_{j=0}^{n} x_i = 0$ without having to add additional rows and columns to the parity check matrix.

The (P,G) code is given by the following

G(x) = $x^3 + Bx^2$+1 (2.1)

= $(x-\omega)(x-\omega^{-1})(x-\omega^{-2})$ where B Є GF (q^m) \{0} and location set L= {$\mu_1, \mu_2 \dots\dots \mu_n$} contains in GF($q^{3m}$)\ ($q^{2m}$)\ GF ($q^m$) \{1} ,$\mu_i^2 = \mu_i$,$\mu_n = 1$, $\mu_i^{q^m} = \mu_i^{-1} = \mu_{n-i}$ also G(μ_i) $\neq 0$, $\mu_i \neq \mu_j \; \forall \; i \neq j$.

The Goppa polynomial (1) can be written as

G(x) =$(x-\omega)(x-\omega^{-1})(x-\omega^{-2})$

Such that $\omega + \omega^{-1} + \omega^{-2} = -B$ (2.2)

Given that B Є GF (q^{3m}) it is apparent that $\omega^{q^m}+\omega^{-q^m} + \omega^{-2q^m} = -B$

Then$(\omega^{q^m} - \omega)(\omega^{q^m+1} - 1)(\omega^{q^m+2} - 1) = 0$, therefore

$\omega^{q^m} = \omega$ (2.3)

$\omega^{q^m+1} = 1$ (2.4)

$\omega^{q^m+2} = 1$ (2.5)

Theorem 1: The redundancy of (P,G) Code defined by (2.1) does not exceed 3m+1 and the parity check matrix of this code has a row of 1's .

Proof: we proof our result by using the proposed technique I n [4] .the parity check matrix of the code is

$$H= \begin{bmatrix} \frac{1}{\mu_1^3+B\mu_1^2+1} & \dots & \frac{1}{\mu_{n-1}^3+B\mu_{n-1}^2+1} & \frac{1}{\mu_n^3+B\mu_n^2+1} \\ \frac{\mu_1}{\mu_1^3+B\mu_1^2+1} & \dots & \frac{\mu_{n-1}}{\mu_{n-1}^3+B\mu_{n-1}^2+1} & \frac{\mu_n}{\mu_n^3+B\mu_n^2+1} \\ \frac{\mu_1^2}{\mu_1^3+B\mu_1^2+1} & \dots & \frac{\mu_{n-1}^2}{\mu_{n-1}^3+B\mu_{n-1}^2+1} & \frac{\mu_n^2}{\mu_n^3+B\mu_n^2+1} \end{bmatrix}$$

The linear combination of the first , second and third rows of the matrix gives a row of 1's

$$\left[\frac{\mu_1^3+B\mu_1^2+1}{\mu_1^3+B\mu_1^2+1} \quad \dots\dots \quad \frac{\mu_{n-1}^3+B\mu_{n-1}^2+1}{\mu_{n-1}^3+B\mu_{n-1}^2+1} \quad \frac{\mu_n^3+B\mu_n^2+1}{\mu_n^3+B\mu_n^2+1}\right]$$

=[1 …. 1 1]

Thus we discover that the parity check matrix of the code (1) can be represented by three rows

$$\begin{bmatrix} \frac{1}{\mu_1^3+B\mu_1^2+1} & \cdots & \frac{1}{\mu_{n-1}^3+B\mu_{n-1}^2+1} & \frac{1}{\mu_n^3+B\mu_n^2+1} \\ \frac{\mu_1}{\mu_1^3+B\mu_1^2+1} & \cdots & \frac{\mu_{n-1}}{\mu_{n-1}^3+B\mu_{n-1}^2+1} & \frac{\mu_n}{\mu_n^3+B\mu_n^2+1} \\ 1 & \cdots & 1 & 1 \end{bmatrix}$$

One of which is a row of 1's and therefore the redundancy of the code is 3m+1.

Corollary1: The (P, G,p_1, p_2, p_3) Code , corresponding to the separable code (2.1) has a row of 1's in its parity-check matrix.

Theorem2: The proposed code (2.1) (P, G) code is a reversible code.

Proof: It is sufficient to raise every element of the matrix H to the power of q^m

$$\begin{bmatrix} \frac{1}{\mu_1^3+B\mu_1^2+1} & \cdots & \frac{1}{\mu_{n-1}^3+B\mu_{n-1}^2+1} & \frac{1}{\mu_n^3+B\mu_n^2+1} \\ \frac{\mu_1}{\mu_1^3+B\mu_1^2+1} & \cdots & \frac{\mu_{n-1}}{\mu_{n-1}^3+B\mu_{n-1}^2+1} & \frac{\mu_n}{\mu_n^3+B\mu_n^2+1} \\ 1 & \cdots & 1 & 1 \end{bmatrix}$$

$$\begin{bmatrix} \frac{1}{(\mu_1^3+B\mu_1^2+1)q^m} & \cdots & \frac{1}{(\mu_{n-1}^3+B\mu_{n-1}^2+1)q^m} & \frac{1}{(\mu_n^3+B\mu_n^2+1)q^m} \\ \frac{\mu_1}{(\mu_1^3+B\mu_1^2+1)q^m} & \cdots & \frac{\mu_{n-1}}{(\mu_{n-1}^3+B\mu_{n-1}^2+1)q^m} & \frac{\mu_n}{(\mu_n^3+B\mu_n^2+1)q^m} \\ 1 & \cdots & 1 & 1 \end{bmatrix}$$

$$\begin{bmatrix} \frac{1}{\mu_{n-1}^3+B\mu_{n-1}^2+1} & \cdots & \frac{1}{\mu_1^3+B\mu_1^2+1} & \frac{1}{\mu_n^3+B\mu_n^2+1} \\ \frac{\mu_{n-1}}{\mu_{n-1}^3+B\mu_{n-1}^2+1} & \cdots & \frac{\mu_1}{\mu_1^3+B\mu_1^2+1} & \frac{\mu_n}{\mu_n^3+B\mu_n^2+1} \\ 1 & \cdots & 1 & 1 \end{bmatrix}$$

Hence the code (1) is reversible.

Corollary2: The (P, G,p_1, p_2, p_3) Code corresponding to the separable code (1) is reversible if $p_1 = p_2 = p_3$.

Theorem3: The separable Code (1) with Goppa polynomial G(x) == $(x-\omega)(x-\omega^{-1})(x-\omega^{-2})$is a cyclic, reversible Goppa code.

Proof: The reversibility of the code was proven in theorem 2.

Now for the proof of cyclicity of code (2.1) we will use the approach proposed in [4]

The parity check matrix of the code is

ISSN 2277-3061
Volume 15 Number 5
International Journal of Computers and Technology

$$H=\begin{bmatrix} 1 & \cdots & 1 & 1 \\ \frac{1}{\omega-\mu_1} & \cdots & \frac{1}{\omega-\mu_{n-1}} & \frac{1}{\omega-1} \\ \frac{1}{\omega^{-1}-\mu_1} & \cdots & \frac{1}{\omega^{-1}-\mu_{n-1}} & \frac{1}{\omega^{-1}-1} \\ \frac{1}{\omega^{-2}-\mu_1} & \cdots & \frac{1}{\omega^{-2}-\mu_{n-1}} & \frac{1}{\omega^{-2}-1} \end{bmatrix}$$

$$=\begin{bmatrix} 1 & \cdots & 1 & 1 \\ \frac{\omega^2-1}{\omega-\mu_1}-\omega & \cdots & \frac{\omega^2-1}{\omega-\mu_{n-1}}-\omega & \frac{\omega^2-1}{\omega-1}-\omega \\ \frac{\omega^{-2}-1}{\omega^{-1}-\mu_1}-\omega^{-1} & \cdots & \frac{\omega^2-1}{\omega^{-1}-\mu_{n-1}}-\omega^{-1} & \frac{\omega^2-1}{\omega^{-1}-1}-\omega^{-1} \\ \frac{\omega^{-4}-1}{\omega^{-2}-\mu_1}-\omega^{-2} & \cdots & \frac{\omega^{-4}-1}{\omega^{-2}-\mu_{n-1}}-\omega^{-2} & \frac{\omega^{-4}-1}{\omega^{-2}-1}-\omega^{-2} \end{bmatrix}$$

$$=\begin{bmatrix} 1 & \cdots & 1 & 1 \\ \frac{\omega\mu_1-1}{\omega-\mu_1} & \cdots & \frac{\omega\mu_{n-1}-1}{\omega-\mu_{n-1}} & 1 \\ \frac{\mu_1\omega^{-1}-1}{\omega^{-1}-\mu_1} & \cdots & \frac{\mu_{n-1}\omega^{-1}-1}{\omega^{-1}-\mu_{n-1}} & 1 \\ \frac{\mu_1\omega^{-2}-1}{\omega^{-2}-\mu_1} & \cdots & \frac{\mu_{n-1}\omega^{-2}-1}{\omega^{-2}-\mu_{n-1}} & 1 \end{bmatrix} \quad (3.1)$$

Obviously $\frac{\omega\mu_i-1}{\omega-\mu_i} \neq \frac{\omega\mu_j-1}{\omega-\mu_j}$, $\frac{\mu_i\omega^{-1}-1}{\omega^{-1}-\mu_i} \neq \frac{\mu_j\omega^{-1}-1}{\omega^{-1}-\mu_j}$ and $\frac{\mu_i\omega^{-2}-1}{\omega^{-2}-\mu_i} \neq \frac{\mu_j\omega^{-2}-1}{\omega^{-2}-\mu_j}$

Now let us consider three possible cases (3), (4) and (5) for the Goppa polynomial G(x)

Case1: $\omega^{q^m} = \omega$

First for ω

$$\left(\frac{\omega\mu_i-1}{\omega-\mu_i}\right)^{q^m} = \frac{\mu_i^{-1}\omega-1}{\omega-\mu_i^{-1}}$$

$$= \frac{\omega-\mu_i}{\omega\mu_i-1}$$

$$= \left(\frac{\omega\mu_i-1}{\omega-\mu_i}\right)^{-1}$$

This implies $\left(\frac{\omega\mu_i-1}{\omega-\mu_i}\right)^{q^m+1} = 1$ for all i= 1,2…n.

Let we assume that $\frac{\omega\mu_i-1}{\omega-\mu_i} = \rho_i$ it is obvious that the number of different elements ρ_i distinct from the unit is equal to $n-1 = q^m$ and $\rho_i^{q^m+1} = 1$.

Then for ω^{-1}

$$\left(\frac{\mu_i\omega^{-1}-1}{\omega^{-1}-\mu_i}\right)^{q^m} = \frac{\mu_i^{-1}\omega^{-1}-1}{\omega^{-1}-\mu_i^{-1}}$$

$$= \frac{\omega^{-1}-\mu_i}{\mu_i\omega^{-1}-1}$$

$$= \left(\frac{\mu_i\omega^{-1}-1}{\omega^{-1}-\mu_i}\right)^{-1}$$

$\left(\frac{\mu_i\omega^{-1}-1}{\omega^{-1}-\mu_i}\right)^{q^m+1} = 1$ for all i= 1,2…n

And in addition $\frac{\mu_i\omega^{-1}-1}{\omega^{-1}-\mu_i} = \left(\frac{\omega\mu_i-1}{\omega-\mu_i}\right)^{-1} = \rho_i^{-1}$

Finally for ω^{-2}

$\left(\frac{\mu_i\omega^{-2}-1}{\omega^{-2}-\mu_i}\right)^{q^m} = \left(\frac{\omega\mu_i-1}{\omega-\mu_i}\right)^{-2}$

$\left(\frac{\mu_i\omega^{-2}-1}{\omega^{-2}-\mu_i}\right)^{q^m+2}$ =1, for all i= 1,2…n

And in addition $\frac{\mu_i\omega^{-2}-1}{\omega^{-2}-\mu_i} = \left(\frac{\omega\mu_i-1}{\omega-\mu_i}\right)^{-2} = \rho_i^{-2}$

The parity check matrix of the reversible separable Goppa code of the length n= q^m+1 and generator polynomial g(x) with $g(\mu^i) = 0$, I = 0,1 &2 , $\mu \in GF(q^m)$, $\mu^{q^m+1} = 1$ is represented as

$$H=\begin{bmatrix} 1 & \cdots & 1 & 1 \\ \rho_1 & \cdots & \rho_{n-1} & 1 \\ \rho_1^{-1} & \cdots & \rho_{n-1}^{-1} & 1 \\ \rho_1^{-2} & \cdots & \rho_{n-1}^{-2} & 1 \end{bmatrix} \quad (3.2)$$

Case2: $\omega^{q^m+2} = 1$ since the polynomial G(x) should not have roots among the elements of the location set $\mu_i \subset$ GF (q^{3m})\ (q^{2m})\ GF (q^m) ∪{1,2}, $\mu_i^{q^m+2} = 1$

First for ω

$\left(\frac{\omega\mu_i-1}{\omega-\mu_i}\right)^{q^m} = \frac{\mu_i^{-1}\omega^{-2}-1}{\omega^{-2}-\mu_i^{-1}}$

$= \frac{\omega^{-2}-\mu_i}{\mu_i\omega^{-2}-1}$

$= \frac{1-\mu_i\omega^2}{\mu_i-\omega^2}$

Let us we assume that $\frac{1-\mu_i\omega^2}{\mu_i-\omega^2} = \varphi$

Then for ω^{-1}

$\left(\frac{\mu_i\omega^{-1}-1}{\omega^{-1}-\mu_i}\right)^{q^m} = \frac{\mu_i^{-1}\omega^2-1}{\omega^2-\mu_i^{-1}}$

$= \frac{\omega^2-\mu_i}{\mu_i\omega^2-1}$

$= \frac{\mu_i-\omega^2}{1-\mu_i\omega^2}$

$= \varphi^{-1}$

Finally for ω^{-2}

Proceed like above we get

$$\left(\frac{\mu_i\omega^{-1}-1}{\omega^{-1}-\mu_i}\right)^{q^m} = \left(\frac{1-\mu_i\omega^2}{\mu_i-\omega^2}\right)^{-2} = \varphi^{-2}$$

Therefore the parity check matrix of reversible cyclic code of length n= $q^m - 2$ and generator polynomial g(x) with g $(\mu^i) = 0$, I = 0, ±1 &-2 , $\mu \in GF(q^m)$, $\mu^{q^m-2} = 1$, is represented as

$$H=\begin{bmatrix} 1 & \cdots & 1 & 1 \\ \varphi_1 & \cdots & \varphi_{n-1} & 1 \\ \varphi_1^{-1} & \cdots & \varphi_{n-1}^{-1} & 1 \\ \varphi_1^{-2} & \cdots & \varphi_{n-1}^{-2} & 1 \end{bmatrix} \qquad (3.3)$$

Case3: $\omega^{q^m+1} = 1$ in this case, the code length n= $q^m - 1$, since the polynomial G(x) should not have roots among the elements of the location set $\mu_i \subset$ GF (q^{3m})\ (q^{2m})\ GF (q^m) ∪{1}, $\mu_i^{q^m+1} = 1$

Let us now examine the elements of a parity check matrix of such a code:

$$\left(\frac{\omega\mu_i-1}{\omega-\mu_i}\right)^{q^m} = \frac{\mu_i^{-1}\omega^{-1}-1}{\omega^{-1}-\mu_i^{-1}}$$

$$= \frac{\omega\mu_i-1}{\omega-\mu_i}$$

Let $\frac{\omega\mu_i-1}{\omega-\mu_i} = \delta_i \in GF(q^m)$, for i= 1,2…n

And same as in the previous case for ω^{-1} and ω^{-2}

We get $\frac{\mu_i\omega^{-1}-1}{\omega^{-1}-\mu_i} = \left(\frac{\omega\mu_i-1}{\omega-\mu_i}\right)^{-1}$ and $\frac{\mu_i\omega^{-2}-1}{\omega^{-2}-\mu_i} = \left(\frac{\omega\mu_i-1}{\omega-\mu_i}\right)^{-2}$. The parity check matrix (6) of such a reversible separable (L, G) Code is:

$$H=\begin{bmatrix} 1 & \cdots & 1 & 1 \\ \delta_1 & \cdots & \delta_{n-1} & 1 \\ \delta_1^{-1} & \cdots & \delta_{n-1}^{-1} & 1 \\ \delta_1^{-2} & \cdots & \delta_{n-1}^{-2} & 1 \end{bmatrix} \qquad (3.4)$$

This the required matrix of a reversible cyclic code of length n=$q^m - 1$ and generator polynomial g(x) with $g(\mu^i) = 0$, I = 0,±1 &-2 , $\mu \in GF(q^m)$, $\mu^{q^m-1} = 1$.

Hence we are done.

Theorem4: The Code (P , G, t_1, t_2 , t_3) whose gernator polynomial G(x)= $((x-\omega))^{t_1}(x-\omega^{-1})^{t_2}(x-\omega^{-2})^{t_3}$ and location set P == {μ_1 , μ_2 …… μ_n}, with condition$\mu_i^{q^m} = \mu_i^{-1}$ and none of μ_i is root of G(x) is a cyclic Goppa code.

Proof: The Code (P, G, t_1, t_2 , t_3) has the parity check matrix H is expressed as

$$H=\begin{bmatrix} 1 & \cdots & 1 & 1 \\ \frac{1}{\omega-\mu_1} & \cdots & \frac{1}{\omega-\mu_{n-1}} & \frac{1}{\omega-1} \\ \vdots & & \vdots & \vdots \\ \frac{1}{(\omega-\mu_1)^{t_1}} & \vdots & \frac{1}{(\omega-\mu_{n-1})^{t_1}} & \frac{1}{(\omega-1)^{t_1}} \\ \frac{1}{\omega^{-1}-\mu_1} & \ddots & \frac{1}{\omega^{-1}-\mu_{n-1}} & \frac{1}{\omega^{-1}-1} \\ \vdots & \vdots & \vdots & \vdots \\ \frac{1}{(\omega^{-1}-\mu_1)^{t_2}} & \vdots & \frac{1}{(\omega^{-1}-\mu_{n-1})^{t_2}} & \frac{1}{(\omega^{-1}-1)^{t_2}} \\ \frac{1}{\omega^{-2}-\mu_1} & \vdots & \frac{1}{\omega^{-2}-\mu_{n-1}} & \frac{1}{\omega^{-2}-1} \\ \vdots & \vdots & \vdots & \vdots \\ \frac{1}{(\omega^{-2}-\mu_1)^{t_3}} & \vdots & \frac{1}{(\omega^{-2}-\mu_{n-1})^{t_3}} & \frac{1}{(\omega^{-2}-1)^{t_3}} \end{bmatrix}$$

$$=\begin{bmatrix} 1 & \cdots & 1 & 1 \\ \frac{\omega\mu_1-1}{\omega-\mu_1} & \cdots & \frac{\omega\mu_{n-1}-1}{\omega-\mu_{n-1}} & \frac{\omega-1}{\omega-1} \\ \vdots & & \vdots & \vdots \\ \left(\frac{\omega\mu_1-1}{\omega-\mu_1}\right)^{t_1} & \vdots & \left(\frac{\omega\mu_{n-1}-1}{\omega-\mu_{n-1}}\right)^{t_1} & \left(\frac{\omega-1}{\omega-1}\right)^{t_1} \\ \frac{\mu_1\omega^{-1}-1}{\omega^{-1}-\mu_1} & \ddots & \frac{\mu_{n-1}\omega^{-1}-1}{\omega^{-1}-\mu_{n-1}} & \frac{\omega^{-1}-1}{\omega^{-1}-1} \\ \vdots & \vdots & \vdots & \vdots \\ \left(\frac{\mu_1\omega^{-1}-1}{\omega^{-1}-\mu_1}\right)^{t_2} & \vdots & \left(\frac{\mu_{n-1}\omega^{-1}-1}{\omega^{-1}-\mu_{n-1}}\right)^{t_2} & \left(\frac{\omega^{-1}-1}{\omega^{-1}-1}\right)^{t_2} \\ \frac{\mu_1\omega^{-2}-1}{\omega^{-2}-\mu_1} & \vdots & \frac{\mu_{n-1}\omega^{-2}-1}{\omega^{-2}-\mu_{n-1}} & \frac{\omega^{-2}-1}{\omega^{-2}-1} \\ \vdots & \vdots & \vdots & \vdots \\ \left(\frac{\mu_1\omega^{-2}-1}{\omega^{-2}-\mu_1}\right)^{t_3} & \vdots & \frac{\mu_{n-1}\omega^{-2}-1}{\omega^{-2}-\mu_{n-1}}^{t_3} & \left(\frac{\omega^{-2}-1}{\omega^{-2}-1}\right)^{t_3} \end{bmatrix}$$

Taking in to account of theorem 3 , the parity check matrix of the (P , G, t_1, t_2 , t_3) can be represented in three cases as:

(a) For the case $\omega^{q^m} = \omega$

$$\begin{bmatrix} 1 & \cdots & 1 & 1 \\ \rho_1 & \cdots & \rho_{n-1} & 1 \\ \vdots & & \vdots & \vdots \\ {\rho_1}^{t_1} & \vdots & {\rho_1}^{t_2} & 1 \\ {\rho_1}^{-1} & \vdots & {\rho_{n-1}}^{-1} & 1 \\ \vdots & \vdots & \vdots & \vdots \\ {\rho_1}^{-t_2} & \vdots & {\rho_{n-1}}^{-t_2} & 1 \\ {\rho_1}^{-2} & \vdots & {\rho_{n-1}}^{-2} & 1 \\ \vdots & \vdots & \vdots & \vdots \\ {\rho_1}^{-2t_3} & & {\rho_{n-1}}^{-2t_3} & 1 \end{bmatrix}$$

ISSN 2277-3061
Volume 15 Number 5
International Journal of Computers and Technology

$$= \begin{bmatrix} 1 & \cdots & 1 & 1 \\ \rho_1 & \cdots & \rho_{n-1} & 1 \\ \rho_1^2 & \cdots & \rho_{n-1}^2 & 1 \\ \rho_1^t & \cdots & \rho_{n-1}^t & 1 \end{bmatrix} = H_{RC} \qquad (4.1)$$

where $\frac{\omega\mu_i - 1}{\omega - \mu_i} = \rho_i$ and t = max. (t_1 ,t_2 ,t_3) for $i = 1, 2 \ldots \ldots \ldots n.$

the parity check matrix (9) represented the reversible cyclic code of length n= $q^m + 1$ and

Generator polynomial g(x) with g(μ^i) = 0 , I = 0,1 &2 , $\mu \in GF(q^m)$, $\mu^{q^m+1} = 1$

(b) For the case $\omega^{q^m+2} = 1$

$$H \begin{bmatrix} 1 & \cdots & 1 & 1 \\ \varphi_1 & \cdots & \varphi_{n-1} & 1 \\ \vdots & & \vdots & \vdots \\ {\varphi_1}^{t_2} & \vdots & {\varphi_1}^{t_2} & 1 \\ {\varphi_1}^{-1} & \vdots\vdots & {\varphi_{n-1}}^{-1} & 1 \\ \vdots & \vdots & \vdots & \vdots \\ {\varphi_1}^{-t_2} & \vdots & {\varphi_{n-1}}^{-t_2} & 1 \\ {\varphi_1}^{-2} & \vdots & {\varphi_{n-1}}^{-2} & 1 \\ \vdots & \vdots & \vdots & \vdots \\ {\varphi_1}^{-2t_3} & \vdots & {\varphi_{n-1}}^{-2t_3} & 1 \end{bmatrix}$$

Where $\frac{1 - \mu_i\omega^2}{\mu_i - \omega^2} = \varphi$, The parity check matrix of reversible cyclic code of length n= $q^m - 2$ and generator polynomial g(x) with g (μ^i) = 0 , I = 0, ±1 &-2 , $\mu \in GF(q^m)$, $\mu^{q^m-2} = 1$.

(c) For the case $\omega^{q^m+1} = 1$

Similarly the parity check matrix in this case is

$$H \begin{bmatrix} 1 & \cdots & 1 & 1 \\ \delta_1 & \cdots & \delta_{n-1} & 1 \\ \vdots & & \vdots & \vdots \\ {\delta_1}^{t_2} & \vdots & {\delta_1}^{t_2} & 1 \\ {\delta_1}^{-1} & \vdots\vdots & {\delta_{n-1}}^{-1} & 1 \\ \vdots & \vdots & \vdots & \vdots \\ {\delta_1}^{-t_2} & \vdots & {\delta_{n-1}}^{-t_2} & 1 \\ {\delta_1}^{-2} & \vdots & {\delta_{n-1}}^{-2} & 1 \\ \vdots & \vdots & \vdots & \vdots \\ {\delta_1}^{-2t_3} & \vdots & {\delta_{n-1}}^{-2t_3} & 1 \end{bmatrix}$$

where $\frac{\omega\mu_i - 1}{\omega - \mu_i} = \delta_i \in GF(q^m)$, for i= 1,2…n.

Hence we are done.

3. Conclusion:

The present search will give birth to some other interesting subclasses of Goppa codes .In the next paper we will work on Goppa polynomial of degree 4 and also try to find the conditions for the existence of nonreversible cyclic separable Goppa code of degree 3 and more.

4.REFERENCES

I. F.J .McWilliams and N.J.A Sloane, 1977, The Theory of Error Correcting Codes. Amsterdam. The Netherland, North Holland.

II. Oliver Pretzel, 1992, Error –Correcting Codes and Finite Fields. Clarendon Press. Oxford.

III. K.K .Tzeng , K.Zimmermann, 1975 On Extending Goppa Codes to Cyclic Codes, IEEE Trans. Information Theory , Volume -25 , PP-246-250.

IV. Sergey Bezzateev and Natalia Shekhunova 2013, Subclass Of Cyclic Goppa Codes, IEEE Trans. Information Theory.