A New Family of 3-Error Correcting Codes with Bch Like Domain

Ajay Kumar

Assistant Professor in LLRIET, Moga

Abstract - BCH codes are most studied error correcting codes among the families of coding theory. Bracken and Helleseth (2009) discovered some new zero set leading to triple-error-correcting codes. Kasami and Bracken find these triples for the binary triple error correcting Code .Furthermore Kumar and Vinocha (2013) found some other roots of a family of error correcting BCH type codes In this work, we study on a new family of triple error correcting codes similar to BCH Code and proposed some new roots of error correcting code having roots $\{1, 4^m+1, 4^{2m}+1\}$ ***and*** $\{1, 4^m+1, 4^{3m}+1\}$ ***where gcd (m, n) =1.***

Keywords: least distance, roots, BCH code and cyclic code.

I. INTRODUCTION

The Bose, Chaudhuri and Hocquenghem codes from a large of powerful error- correction cyclic codes.BCH codes is a generalization of the Hamming codes for multiple –error correction. Binary BCH codes were discovered by Hocquenghem (1959) and independently by Bose and Chaudhuri (1960). The cyclic structure of these codes were proved by Peterson (1960).BCHbcodes are an interesting class of linear codes due to their efficient algorithms of encoding and decoding BCH code are best known as a subclass of cyclic codes .BCH code are very important in both theory and practical as they have good error –correcting capability and are generally used in storage device and communication systems .we can represent BCH codes with the help of zeros set .Many authors worked on finding the different zeros set of triple error correcting BCH codes than the existing one. The work of Kasami (1971) was remarkable this field. Bracken and Helleseth (2009) were also given a new technique to find the zero set of the above said codes. In this paper, we proposed a new family of BCH type codes and offer the roots set of the constructed codes. The proposed triple error correcting BCH type Code is a cyclic code with minimum distance seven. We will assume a finite field with 2^n elements and g(X) be the gernator polynomial of the above said codes having θ, θ^4 and θ^5 be its zeros. Let $p_1 = 1$, $p_2 = 4$ and $p_4 = 5$ then the parity check matrix H is

$$\begin{bmatrix} 1 & \tau^{\theta^{p_1}} & \dots & \tau^{\theta^{(2^n-2)p_1}} \\ 1 & \tau^{\theta^{p_2}} & \dots & \tau^{\theta^{(2^n-2)p_2}} \\ 1 & \tau^{\theta^{p_3}} & \dots & \tau^{\theta^{(2^n-2)p_3}} \end{bmatrix}$$

The order of H is given 3n by $2^n - 1$. And code has same parameters as the BCH codes

Argument-1: An equation of the form $x^{4^k+1} + bx^{4^k} + cx = d$ defined on GF (2^n) has no more than five solutions in x when gcd (k, n) =1 for all b, c and d in GF (2^n). [A.W. Bluher, 2004].

For calculating minimum distance a famous result in coding theory is that if there are no sets of d – 1 column in parity check matrix then the code has minimum distance at least d. We will prove our results by contradicting the fact that H has six linear non independent columns. Which result the minimum distance of the code are seven.

II. LIST OF ROOTS OF 3-ERROR CORRECTING CODES

Roots	Situation	References
$\{1, 2^m+1, 2^{2m}+1\}$ $\{1, 2^m+1, 2^{3m}+1\}$	gcd(m,n)=1 ,n is odd	Bracken and Helleseth 2009
$\{1, 2^{2m}+1, 2^{4m}+1\}$ $\{1, 2^{2m}+1, 2^{6m}+1\}$	gcd(2m,n)=1 ,n is odd	Kumar and Vinocha2013
$\{1, 2^{3m}+1, 2^{6m}+1\}$ $\{1, 2^{3m}+1, 2^{9m}+1\}$	gcd(3m,n)=1 ,n is odd	Kumar 2016
$\{1, 4^m+1, 4^{2m}+1\}$	gcd(m,n)=1 ,n is odd	Theorem-3.1
$\{1, 4^m+1, 4^{4m}+1\}$	gcd(m ,n)=1, n is odd	Theorem-3.2

III. NEW FAMILY OF TRIPLE ERROR CORRECTING CODES

In this subsection we are given a new family of BCH like codes and proposed the roots of the proposed codes. Theorem 3.1 and 3.2 are supporting our argument

Theorem 3.1The set $\{1, 4^m+1, 4^{2m}+1\}$ *are the* roots of a new type of triple –error-correcting codes similar to BCH code provided gcd (m, n) =1for all x∈GF (2^n).

Proof: The parity check matrix H has less than seven non independent columns then there subsist basics p, q, r, s, t, u in GF (2^n) such that

$$\theta_1+\theta_2+\theta_3+\phi_1+\phi_2+\phi_3=0$$

$$\theta_1^{4^m+1}+\theta_2^{4^m+1}+\theta_3^{4^m+1}+\phi_1^{4^m+1}+\phi_2^{4^m+1}+\phi_3^{4^m+1}=0$$

$$\theta_1^{4^m+1}+\theta_2^{4^m+1}+\theta_3^{4^m+1}+\phi_1^{4^m+1}+\phi_2^{4^m+1}+\phi_3^{4^m+1}=0$$

The code with root set $\{1, 4^m+1\}$ with gcd (m, n) = 1 has least distance 5. It follows as of first two equations that every element $\theta_1,\theta_2,\theta_3,\phi_1,\phi_2,\phi_3$ has to be dissimilar

We can write this as

$$\theta_1+\theta_2+\theta_3=\alpha_1$$

$$\theta_1^{4^m+1}+\theta_2^{4^m+1}+\theta_3^{4^m+1}=\alpha_2$$

$$\theta_1^{4^{2m}+1}+\theta_2^{4^{2m}+1}+\theta_3^{4^{2m}+1}=\alpha_3$$

Now Substitute

$$\theta_1=\theta_1+\alpha_1,\theta_2=\theta_2+\alpha_1,\theta_3=\theta_3+\alpha_1$$

$$\theta_1+\theta_2+\theta_3=0 \quad (3.1)$$

$$\theta_1^{4^m+1}+\theta_2^{4^m+1}+\theta_3^{4^m+1}=\omega \quad (3.2)$$

$$\theta_1^{4^{2m}+1}+\theta_2^{4^{2m}+1}+\theta_3^{4^{2m}+1}=\mu \quad (3.3)$$

Where $\omega=\alpha_2+{\alpha_1}^{4^m+1}$&$\mu={\alpha_3}+{\alpha_1}^{4^{2m}+1}$

From (3.1) substituting $\theta_3=\theta_1+\theta_2$

Therefore equations (3.2) & (3.3) becomes

$$\theta_1^{4^m}\theta_2+\theta_2^{4^m}\theta_1=\omega$$

$$\theta_1^{4^{2m}}\theta_2+\theta_2^{4^{2m}}\theta_1=\mu$$

Replace $\theta_2=\theta_1\theta_2$ and we get

$$\theta_1^{4^m+1}(\theta_2+\theta_2^{4^m})=\omega \quad (3.4)$$

$$\theta_1^{4^{2m}+1}(\theta_2+\theta_2^{4^{2m}})=\mu \quad (3.5)$$

The equations (3.4) can be written as

$$\theta_2+\theta_2^{4^m}=\omega\theta_1^{-4^m-1}$$

Equation (3.4) implies

$$\theta_2+\theta_2^{4^{2m}}=\omega\theta_1^{-4^m-1}+\omega^{4^m}\theta_1^{-4^{2m}-4^m}$$

Using above equation (3.5) becomes

$$\theta_1^{4^{2m}+1}(\omega\theta_1^{-4^m-1}+\omega^{4^m}\theta_1^{-4^{2m}-4^m})=\mu$$

Set $\lambda=\theta_1^{4^m-1}$

Therefore the equation becomes

$$\omega\lambda^{4^m+1}+\mu\lambda+\omega^{4^m}=0$$

As we know $\omega\neq 0$ this implies by Argument-1 that the above equation has no more than five solutions in λ and we are done.

Theorem 3.2: The set $\{1, 4^m+1, 4^{3m}+1\}$ *are the* roots of a new type of triple –error-correcting codes similar to BCH code provided gcd (m, n) =1for all x∈GF (2^n) for odd n.

Proof: we use the same concept as we do in theorem 3.1 the systems of equations are

$$\theta_1+\theta_2+\theta_3=0 \quad (3.6)$$

$$\theta_1^{4^m+1}+\theta_2^{4^m+1}+\theta_3^{4^m+1}=\omega \quad (3.7)$$

$$\theta_1^{4^{3m}+1}+\theta_2^{4^{3m}+1}+\theta_3^{4^{3m}+1}=\mu \quad (3.8)$$

Where $\omega=\alpha_2+{\alpha_1}^{4^m+1}$&$\mu={\alpha_3}+{\alpha_1}^{4^{3m}+1}$

From (3.6) substituting $\theta_3=\theta_1+\theta_2$

Therefore equations (3.7) & (3.8) becomes

$$\theta_1^{4^m}\theta_2+\theta_2^{4^m}\theta_1=\omega$$

$$\theta_1^{4^{3m}}\theta_2+\theta_2^{4^{3m}}\theta_1=\mu$$

Replace $\theta_2=\theta_1\theta_2$ and we get

$$\theta_1^{4^m+1}(\theta_2+\theta_2^{4^m})=\omega \quad (3.9)$$

$$\theta_1^{4^{3m}+1}(\theta_2+\theta_2^{4^{3m}})=\mu \quad (3.10)$$

The equations (3.9) can be written as

$$\theta_2+\theta_2^{4^m}=\omega\theta_1^{-4^m-1}$$

Equation (3.4) implies

$$\theta_2+\theta_2^{4^{3m}}=\omega\theta_1^{-4^m-1}+\omega^{4^m}\theta_1^{-4^{2m}-4^m}+\omega^{4^{2m}}\theta_1^{-4^{3m}-4^{2m}}$$

Using above equation (3.10) becomes

$$\theta_1^{4^{3m}+1}(\omega\theta_1^{-4^m-1}+\omega^{4^m}\theta_1^{-4^{2m}-4^m}+\omega^{4^{2m}}\theta_1^{-4^{3m}-4^{2m}})=\mu$$

Set $\rho=\theta_1^{4^{2m}-1}$

Therefore the equation becomes

$$\omega\rho^{4^m+1}+\omega^{4^m}\rho^{4^m}+\rho\mu+\omega^{4^{2m}}=0$$

Hence by argument 1 the above equation has at most five solutions in ρ and we are done.

IV. CONCLUSION

In this work we discover new family of triple error correcting BCH type code with the help of its roots. We used some results from finite field to achieve the desired results. The result is quite affective.

V. FUTURE SCOPES

Finding further such type of triples in family of proposed triple error correcting BCH type codes is an interesting and challenging research problem. We will work on finding the new roots of proposed family of Triple error correcting codes and try to generalize them.

REFERENCES

[1] R.Bose and D.Ray-Chaudari,"On a class of error correcting binary group codes," Information and Control, vol.4, pp-68-79, 1960.

[2] O.P Vinocha and Ajay Kumar "A class of triple error correcting BCH Codes" IJITEE, vol-4, issue-4, ISSN:2278-4075,2013.

[3] Carl Bracken and Tor Helleseth, "Triple error correcting BCH like code," In proceedings of 2009IEEE International conference on symposium o international Theoryvolume4, ISIT'09, pages17241725, Piscataway, NJ, USA, IEEE Press., 2009.

[4] F.J. McWilliams and N.J.A.Sloane, "The Theory of Error-Correcting Codes" North Holland Amsterdam,1977

[5] A.W. Bluher, "On $x^{q+1}+ax+b=0$," Finite fields and Applications, vol.10 (4), 2004

[6] Ajay Kumar, "On Study of Zero set of Triple Error Correcting binary BCH likes Codes", ISBN-978-81-932074-1-3, 3rd International Conference on Recent Innovations in Science Engineering and Management in Sri Venkateswara College of Engineering and Technology, Srikakulam, Andhra Pradesh, pp 965-968,27 Feb. 2016.