International Journal of Current Engineering and Technology
E-ISSN 2277 – 4106, P-ISSN 2347 - 5161
©2014 INPRESSCO®, All Rights Reserved
Available at http://inpressco.com/category/ijcet

Research Article

Zero Set of Ternary 3- Error- Correcting BCH Type Codes

O.P Vinocha [1]and Ajay Kumar[2]

[1]Department Mathematics, I.K Gujral Punjab Technical University, Jalandhar, Address FCET, Ferozepur Country India
[2]I.K Gujral Punjab Technical University, Jalandhar, Country India

Accepted 20 February 2014, Available online 25 February 2014, **Vol.4, No.1 (February 2014)**

Abstract

As suggested by Kasami in the 1970s, instead of the BCH Code, different zeros can be used to construct triple-error-correcting codes. Additionally, some new zero sets were discovered by Bracken and Helleseth (2009) resulting in the formulation of triple-error-correcting codes. These triples were found by Kasami and Bracken for the binary triple-error-correcting code. In the present study ,the focus is on the ternary triple-error-correcting BCH type code and a few new triple-error-correcting codes having zeros$\{1\,, 3^m+1, 3^{2m}+1\}$ *and* $\{1\,, 3^m+1, 3^{3m}+1\}$*and where gcd (m, n) =1 has been suggested*

Keywords: *Minimum distance, zeros, BCH code and parity check matrix, cyclic code*

1. Introduction

Owing to their effective encoding and decoding algorithms, cyclic codes are an interesting class of linear codes. The best known subclass of cyclic codes is the BCH code considered to be important in both theory and practical, as it is capable of correcting errors and is used in communication systems and storage devices. A cyclic code with minimum distance seven is the ternary triple-error-correcting BCH Code. With g(X) being the generator polynomial of the aforementioned codes havingθ, $\theta^3$and θ^5 as its zeros, a finite field with 3^n elements is presumed. The set {1, 3, 5} is defined as zero of the code. Rather than the BCH Code, different zeros can be used to construct binary triple-error-correcting codes as demonstrated by Bracken and Helleseth [2009]. The purpose of the present study is to construct some new zero set of triple-error-correcting BCH type code in F3.Let p$_1$= 1, p$_2$= 3 and p$_3$= 5 then the parity check matrix H is

$$\begin{bmatrix} 1 & \varepsilon^{\theta^{p_1}} & \dots & \varepsilon^{\theta^{(3^n-2)p_1}} \\ 1 & \varepsilon^{\theta^{p_2}} & \dots & \varepsilon^{\theta^{(3^n-2)p_2}} \\ 1 & \varepsilon^{\theta^{p_3}} & \dots & \varepsilon^{\theta^{(3^n-2)p_3}} \end{bmatrix}$$

The order of H is given 3n by3^n-1. The code C = $[3^n-1\,, 3^n-3n-1\,,$ d]is a code of dimension 3^n-3n-1 and the minimum distance d= 7 between any pair of codeword.

Argument-1: An equation of the form $x^{3^k+1}+bx^{3^k}+cx=d$ defined on GF (3^n) has a maximum of four solutions in x when gcd (k, n) =1 for all b, c and d in GF (3^n). [A.W. Bluher, 2004].

A notable outcome 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 and this outcome is used for calculating minimum distance. The fact that H has six linear dependent columns is contradicted to prove the results of the present study, where the resulting minimum distance is seven.

2. List of new zeros of 3-Error Correcting codes

Zeros	Conditions	References
$\{1\,, 3^m+1, 3^{2m}+1\}$	gcd(m,n)=1 ,n is odd	Theorem-1
$\{1\,, 3^m+1, 3^{3m}+1\}$	gcd(m ,n)=1, n is odd	Theorem-2

Theorem 3.1 The set $\{1\,, 3^m+1, 3^{2m}+1\}\ are\ the$ zero set of a triple –error-correcting code provided gcd (m, n) =1, with an addition condition that $x+x=0$ for all xGF (3^n).

Proof: The parity check matrix H has less than or equal to six dependent columns then there exist elements p, q, r, s, t, u in GF (3^n) s.t.

$$p+q+r+s+t+u=0$$

$$p^{3^m+1}+\ q^{3^m+1}+r^{3^m+1}+s^{3^m+1}+t^{3^m+1}+u^{3^m+1}=0$$

$$p^{3^{2m}+1}+\ q^{3^{2m}+1}+r^{3^{2m}+1}+s^{3^{2m}+1}+t^{3^{2m}+1}+u^{3^{2m}+1}=0$$

The code with zero set $\{1, 3^m+1\}$ with gcd (m, n) = 1 has minimum distance 5. Thus, from the two equations, it can be understood that the elements p, q, r, s, t, u have to be different.

*Corresponding author: Ajay Kumar is a PhD Scholar

We can write this as $p + q + r = C_1$

$p^{3^m+1} + q^{3^m+1} + r^{3^m+1} = C_2$

$p^{3^{2m}+1} + q^{3^{2m}+1} + r^{3^{2m}+1} = C_3$

Replacing p= p+ C_1 , q= q+ C_1 and r= r+ C_1

$p + q + r = 0$ (3.1.1)

$p^{3^m+1} + q^{3^m+1} + r^{3^m+1} = \omega$ (3.1.2)

$p^{3^{2m}+1} + q^{3^{2m}+1} + r^{3^{2m}+1} = \mu$ (3.1.3)

Where $\omega = C_2 + {C_1}^{3^m+1}$&$\mu = C_3 + {C_1}^{3^{2m}+1}$

From (3.1.1) substituting r = p+ q

Therefore equations (3.1.2) & (3.1.3) becomes

$p^{3^m}q + q^{3^m}p = \omega$

$p^{3^{2m}}q + q^{3^{2m}}p = \mu$

Replacing q = pq and in order to obtain

$p^{3^m+1}\left(q + q^{3^m}\right) = \omega$(3.1.4)

$p^{3^{2m}+1}\left(q + q^{3^{2m}}\right) = \mu$(3.1.5)

The equations (3.1.4) is

$$\left(q + q^{3^m}\right) = \omega\, p^{-3^m-1}$$

Equation (3.1.4) implies

$$q + q^{3^{2m}} = \omega^{3^m}\, p^{-3^{2m}-3^m} + \omega\, p^{-3^m-1}$$

From equation (3.1.5) the following equation is derived

$$p^{3^{2m}+1}\left[\omega^{3^m}\, p^{-3^{2m}-3^m} + \omega\, p^{-3^m-1}\right] = \mu$$

Put $\lambda = p^{3^m-1}$

Therefore the equation becomes

$$\omega\lambda^{3^m+1} + \mu\lambda + \omega^{3^m} = 0$$

As it is known $\omega \neq 0$ from Argument-1 it can be understood thatλcan have a maximum of four solutions from the above equation

Theorem 3.2: The set $\{1\,, 3^m + 1, 3^{3m} + 1\}\, are\ \ the$ zero set of a triple –error-correcting code such that gcd (m, n) =1, for odd n.

Proof: we use the same concept as we do in theorem 1 the systems of equations are

$p^{3^m+1}\left(q + q^{3^m}\right) = \omega$ (3.2.1)

$p^{3^{3m}+1}\left(q + q^{3^{3m}}\right) = \mu$ (3.2.2)

Where $\omega = C_2 + {C_1}^{3^m+1}$&$\mu = C_3 + {C_1}^{3^{3m}+1}$

From equation (3.2.1) implies

$$\left(q + q^{3^{3m}}\right) = \omega\, p^{-3^{3m}-1}$$

$$\Rightarrow\ q + q^{3^{3m}} = \omega^{3^{2m}}\, p^{-3^{3m}-3^{2m}} + \omega^{3^m}\, p^{-3^{2m}-3^m} + \omega\, p^{-3^m-1}$$

Therefore equation (3.2.2) becomes

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

Put $\Upsilon = p^{3^{2m}-1}$

The equation is

$$\omega\Upsilon^{3^m+1} + \omega^{3^m}\Upsilon^{3^m} - \Upsilon\mu + \omega^{3^{2m}} = 0$$

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

Conclusion

A challenging research problem is to further find such type of triples in ternary case. An attempt in finding zero sets that would be different from the existing ones for this code and working on 4 error-correcting codes would be the focus of future studies.

References

[1] R.Bose and D.Ray-Chaudari (1960), On a class of error correcting binary group codes Info.and Control, vol.3, pp-68-79

[2] O.P Vinocha and Ajay kumar (August -2013), A class of triple error correcting BCH Codes IJITEE, vol-3,issue-3, , ISSN:2278-3075.

[3] Carl Bracken and Tor Helleseth(2009) , Triple error correcting BCH like code, In proceedings of 2009IEEE International conference on symposium o international Theoryvolume3,ISIT'09,pages17231725,Piscataway,NJ,USA,. IEEE Press.

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

[5] A.W. Bluher (2004), On$x^{q+1} + ax + b = 0$, Finite fields and Applications, vol.10 (3), pp-285-305,.*M&T*,3,104-107.