A Class of Triple Error Correcting Bch Likes Codes

O.P.Vinocha, Ajay Kumar

Abstract- In a recent paper, Bracken and Helleseth [2009] showed that one can construct triple-error-correcting codes using zero set consisting different zero set than the BCH codes. In this correspondence we present some new triple error correcting code having zeros $\{1, 2^{2k}+1, 2^{4k}+1\}$ ***and*** $\{1, 2^{2k}+1, 2^{6k}+1\}$ ***where gcd (2k, n) =1 and n be odd.***

Keywords: Triple error, Parity Check matrix & minimum distance.

I. INTRODUCTION

BCH codes [R.Bose and D.Ray-Chaudari, 1960] are of great practical importance for error-correction, particularly if the expected errors are small compared with the length. The BCH code is a subset of cyclic code. The binary primitive triple –error-correcting BCH code with minimum distance d = 7 is a cyclic code. We consider a finite field with 2^n elements. g(x) be the generator polynomial of triple –error-correcting BCH code having $\alpha, \alpha^3 \& \alpha^5$ be its Zeros. The set $\{1, 3, 5\}$ is known as triple. Kasami showed that one can construct similar triple-error-correcting codes using zeros sets of different triples. Later Helleseth and Bracken presented some new triples and in addition they gave some new method for finding these triple. In this paper with the help of some new zeros we construct some triple-error-correcting BCH like codes.

Let H = $\begin{bmatrix} 1 & \alpha^{c_1} & \dots & \alpha^{(2^n-2)c_1} \\ 1 & \alpha^{c_2} & \dots & \alpha^{(2^n-2)c_2} \\ 1 & \alpha^{c_3} & \dots & \alpha^{(2^n-2)c_3} \end{bmatrix}$ be the parity check Matrix of the triple error correcting BCH code where $c_1 = 1, c_2 = 2 \& c_3 = 3$, the order of the matrix is 3n by $2^n - 1$. The code C = $[2^n - 1, 2^n - 3n - 1, d]$ is a code of dimension $2^n - 3n - 1$ and minimum distance d= 7 between any pair of codewords.Generally we are interested in finding triples $\{c_1, c_2, c_3\}$ s.t. H is the parity check matrix of a triple-error-correcting code.

II. PRELIMINARY NOTES

A well known result in coding theory for determining the minimum distance is that if there are no sets of d- 1 linear dependent columns in H then the code C has distance at least d. This fact is easily derived from the fact that C is the null space of H. We will assume in this paper that H has six linearly dependent columns and derive a contradiction, which mean minimum distance is seven.

We know that the codes with zero sets $\{1, 2^k + 1\}$ where gcd (k,n)=1 have minimum distance five. For k=1 this follows since the code is the double –error-correcting BCH codes.

The general result is consequence of the well known result f(x) = $x^{2^k} + 1$ is an APN function when gcd (k , n) =1.

Definition 2.1 An APN function is a function such that f (x+ a) + f(x) =b has at most two solutions x is in GF (2^n) for any a≠ 0 and b in GF(2^n)

Theorem 2.2 The error-correcting code with zero set$\{1, 2^k + 1, 2^{2k} + 1\}$ is triple error correcting provided gcd (k, n) =1.

Proof: proof is given in Carl Bracken and Tor Helleseth [2]

Theorem 2.3 Let n be odd and gcd (k,n) =1 .then the error-correcting codes constructed using zero set $\{1, 2^k + 1,23k+1$ is triple –error-correcting .

Proof: proof is given in Carl Bracken and Tor Helleseth [2]

III. MAIN RESULTS

The zero sets considered by Helleseth and Bracken [1] are $\{1, 2^k + 1, 2^{2k} + 1\}$ and$\{1, 2^k + 1, 2^{3k} + 1\}$ .We consider some new triple $\{1, 2^{2k} + 1, 2^{4k} + 1\}$ and $\{1, 2^{2k} + 1,26k+1$ where gcd (2k, n) =1 and n is odd

Theorem 3.1 The error- correcting code with zero set $\{1, 2^{2k} + 1, 2^{4k} + 1\}$ is a triple –error-correcting provided gcd (2k, n) =1. For odd n.

Proof: If H has six or less dependent columns then there must exist elements x, y, z, u, v, w in GF(2^n) s.t.

$$x + y + z + u + v + w = 0$$

$$x^{2^{2k}+1} + y^{2^{2k}+1} + z^{2^{2k}+1} + u^{2^{2k}+1} + v^{2^{2k}+1} + w^{2^{2k}+1} = 0$$

$$x^{2^{4k}+1} + y^{2^{4k}+1} + z^{2^{4k}+1} + u^{2^{4k}+1} + v^{2^{4k}+1} + w^{2^{4k}+1} = 0$$

The code with zero set $\{1, 2^{2k} + 1\}$ with gcd (2k, n) = 1 has minimum distance 5. It follows first two equations that all elements x, y ,z , u ,v ,w have to be different

We can write this as $x + y + z = a$

$x^{2^{2k}+1} + y^{2^{2k}+1} + z^{2^{2k}+1}$= b

$x^{2^{4k}+1} + y^{2^{4k}+1} + z^{2^{4k}+1}$= c

Replace x= x+ a , y= y+ a and z= z+ a

$$x + y + z = 0 \quad (1)$$

$$x^{2^{2k}+1} + y^{2^{2k}+1} + z^{2^{2k}+1} = \beta \quad (2)$$

$$x^{2^{4k}+1} + y^{2^{4k}+1} + z^{2^{4k}+1} = \gamma \quad (3)$$

Where β = b + $a^{2^{2k}+1}$ & γ =c+$a^{2^{4k}+1}$

From (1) substituting z = x+ y

Therefore equations (2) & (3) becomes

$x^{2^{2k}}$y + $y^{2^{2k}}x = \beta$

$x^{2^{4k}}$y + $y^{2^{4k}}x = \gamma$

Replace y = x y and we get

$x^{2^{2k}+1}\left(1 + y^{2^{2k}}\right) = \beta$

$x^{2^{4k}+1}\left(1 + y^{2^{4k}}\right) = \gamma$

The above equations can be written as

$$\left(y + y^{2^{2k}}\right) = \beta\, x^{-2^{2k}-1} \quad (4)$$

$$\left(y + y^{2^{4k}}\right) = \gamma\, x^{-2^{4k}-1} \quad (5)$$

Manuscript received August, 2013.

O.P.Vinocha, Principal, Ferozepur college of Engg. and Tech., ferozeshah, Punjab, India

Ajay Kumar, Phd. Scholar, A.P in Dept. of Mathematics, LRRIET, MOGA, Punjab, India

Equation (4) implies

$y + y^{2^{4k}} = \beta^{2^{2k}} x^{-2^{4k}-2^{2k}} + \beta x^{-2^{2k}-1}$

Using above equation (5) becomes

$x^{2^{4k}+1}\left[\beta^{2^{2k}} x^{-2^{4k}-2^{2k}} + \beta x^{-2^{2k}-1}\right] = \gamma$

This become the Linearized equation

$\beta x^{2^{4k}} + \beta^{2^{2k}} x + \gamma x^{2^{2k}} = 0$

As we know $\beta \neq 0$ this implies by Lemma 1 the above equation has no more than four solution in x. and we are done.

Theorem 3.2 Then the code with zero set $\{1, 2^{2k} + 1, 26k+1$ is a triple –error correcting code where n be odd and gcd(2k,n)=1

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

$x^{2^{2k}+1}\left(y + y^{2^{2k}}\right) = \beta$ (1)

$x^{2^{6k}+1}\left(y + y^{2^{6k}}\right) = \gamma$ (2)

Where $\beta = \mathrm{b} + a^{2^{2k}+1}$ & γ =c+$a^{2^{6k}+1}$

From equation (1) implies

$\left(y + y^{2^{2k}}\right) = \beta x^{-2^{2k}-1}$

$\Longrightarrow y + y^{2^{6k}} = \beta^{2^{4k}} x^{-2^{6k}-2^{4k}} + \beta^{2^{2k}} x^{-2^{4k}-2^{2k}} + \beta x^{-2^{2k}-1}$

Therefore equation (2) becomes

$x^{2^{6k}+1}(\beta^{2^{4k}} x^{-2^{6k}-2^{4k}} + \beta^{2^{2k}} x^{-2^{4k}-2^{2k}} + \beta x^{-2^{2k}-1}) = \gamma$

$\Rightarrow \beta^{2^{4k}} x^{1-2^{4k}} + \beta^{2^{2k}} x^{(2^{4k}-1)(2^{2k}-1)} + \beta x^{2^{2k}(2^{4k}-1)} = \gamma$

Put $r = x^{2^{4k}-1}$ this substitution is 1-1

The Linearized equation is

$\beta r^{2^{2k}+1} + \beta^{2^{2k}} r^{2^{2k}} + \gamma r + \beta^{2^{4k}} = 0$

Hence by Lemma 2 the above equation has at most three solutions in x and we are done.

3.1.0 Special properties

The following result can be found in C. Bracken ,E .Byrne, N.Markin and G.Mc Guire,2007

Lemma 3.1.1 Let s be an integer satisfying gcd (2s, n) =1 and let f(x) = $\sum_{i=0}^{d} r_i x^{2^{si}}$ be a polynomial in GF (2^n) .then f(x) has at most 2^d zeros in GF (2^n).

Lemma 3.1.2: An equation of the form $x^{2^k+1} + bx^{2^k} + cx = d$ defined on GF (2^n). Has no more than three solutions in x when gcd (2k, n) =1 for all b, c and d in GF (2^n). The above lemma is consequence of result in A.W. Bluher, 2004

IV. LABELS OF FIGURES AND TABLES

Triples	Conditions	References
$\{1, 2^{2k}+1, 2^{4k}+1\}$	gcd(2k,n)=1	Theorem-1
$\{1, 2^{2k}+1, 2^{6k}+1\}$	gcd(2k,n)=1	Theorem-2
$\{1, 2^{k}+1, 2^{2k}+1\}$ $\{1, 2^{k}+1, 2^{3k}+1\}$	gcd(k , n) = 1 any n gcd(k , n) = 1 n odd	Bracken and Helleseth, 2009.
$\{1, 2^{t}+1, 2^{t+2}+3\}$	n = 2t + 1 , n odd	A.chang, S.W.Golomb, T.Helleseth andP.V.Kumar 2000.
$\{2^{k}+1, 2^{3k}+1, 2^{5k}+1$	gcd(k , n) = 1 n odd	T. Kasami, 1971.
$\{1, 2^{t}+1, 2^{t-1}+1\}$	n = 2t + 1 , n odd	F.J. McWilliams and N.J.A.Sloane, 1977.

V. CONCLUSIONS

In this work we discussed a class of triple error correcting BCH like codes with the help of zero set is presented. This correspondence also gives some new connections to properties of some special equations of finite fields given in Lemma1 and Lemma 2. Finding further triple with different zero sets is a challenging research problem that may lead to other interesting connection?

REFERENCES

1. R.Bose and D.Ray-Chaudari: "On a class of error correcting binary group codes"Info.and Control, vol.3, pp-68-79-, 1960.
2. Carl Bracken and Tor Helleseth " Triple error correcting BCH like code" In proceedings of 2009IEEE International conference on symposium o international Theory - volume 3,ISIT'09,pages 1723-1725,Piscataway,NJ,USA,2009.IEEE Press.
3. A.chang, S.W.Golomb, T.Helleseth and P.V.Kumar "On a conjectured ideal autocorrelation sequence and a related triple-error correcting cyclic code"IEEE Trans. Inform.Thoery vol.46, pp.680-687, 2000.
4. T. Kasami "The weight enumerators for several classes of sub codes of the second order binary Reed Muller codes "Info.Contr, vol.18, pp.369-394, 1971.
5. F.J. McWilliams and N.J.A.Sloane,"The Theory of Error- Correcting Codes" North Holland Amsterdam, pp288, 1977.
6. A.W. Bluher "On$x^{q+1} + ax + b = 0$" .Finite fields and Applications, vol.10 (3), pp-285-305, 2004.
7. C. Bracken ,E .Byrne, N.Markin and G.Mc Guire " Determining the Non-linearity of a New Family of APN Functions" Proceedings of AAECC-17, Lecture Notes in Computer Science,vol4851,pp-72-79 , 2007.