Available online at http://scik.org

J. Math. Comput. Sci. 6 (2016), No. 6, 1204-1209

ISSN: 1927-5307

GENERALIZATION OF ZERO SET OF NON-BINARY TRIPLE ERROR CORRECTING BCH TYPE CODE

AJAY KUMAR[1,*], RAJESH KUMAR NARULA[1] AND O.P. VINOCHA[2]

[1]Department of Mathematics, PhD Scholar in I.K.G Punjab Technical University, Jalandhar, India

[2]Department of Mathematics, Principal in Tantia college of Engineering, Tantia University, Sri- Ganganagar, India

Abstract. In our previous paper [6] we constructed some zero set $\{1\,,3^m+1, 3^{2m}+1\}$ and $\{1\,,3^m+1, 3^{3m}+1\}$ and proved that these set represented the zeros of triple error correcting code in non binary case. In this work, we proposed the sufficient condition for the existence of zero set $\{1\,,3^l+1, 3^{kl}+1\}$ of Non binary triple –error-correcting code having gcd (l, n) =1.

Keywords: BCH codes; zero set and triple error correcting code.

2010 AMS Subject Classification: 94A24.

1 Introduction

BCH codes are the generalization of the most famous code for single error correcting known as Hamming codes. BCH code are powerful because they have simultaneously reasonably high rates and reasonably good error correcting abilities.BCH codes have a very nice algebraic characterization and they permit efficient shift register encoding. However, their importance is due almost wholly to indeed that these codes have very effective decoding algorithm.

BCH codes can be represented by its zeros. The well-known zero set for the triple error correcting BCH code in binary case is$\{1\,,3\,,5\}$. Kasami [1] gave an idea that Binary BCH like code can be represented by distinct zero set than the existing one. The zero set of binary BCH like code proposed by Kasami is $\{2^l+1\,,2^{3l}+1, 2^{5l}+1\}$.Later Bracken and Helleseth [4] proposed some other zero set $\{1\,,2^k+1, 2^{2k}+1\}$ and $\{1\,,2^k+1, 2^{3k}+1\}$and proved that these zero set also represented BCH like triple error correcting codes. Further added Vinocha and

*Corresponding author

Received August 3, 2016

Kumar [5] gave some other zero set $\{1, 2^{2k}+1, 2^{4k}+1\}$ and $\{1, 2^{2k}+1, 2^{6k}+1\}$ and proved them 3- error correcting BCH type code. The study of different zero set for above said code than the existing one is done in only binary case. Vinocha and Kumar [6] studied on finding the zero set of 3- error correcting BCH type code in non binary cases. They proposed two zero sets namely $\{1, 3^{m}+1, 3^{2m}+1\}$ and $\{1, 3^{m}+1, 3^{3m}+1\}$ and shown that these sets represented triple error correcting BCH type code. In this correspondence we describe the condition for the existence of zero set of 3- error correcting BCH type code in non binary case. The length of the proposed code would be n= 3^m-1 and we would like to add further a condition that the sum of two same elements should be zero in$GF(3^n)$. The parity check matrix H of the above said code is

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

Where $\{p_1, p_2, p_3\}$ are the zero set of the code and each column of the matrix is stand for n bit vector of a field F_3 basis onF_{3^n}.

2 The list of known zeros

Zeros	Conditions	References
$\{1, 2^{k}+1, 2^{2k}+1\}$ $\{1, 2^{k}+1, 2^{3k}+1\}$	gcd(k,n)=1	Bracken and Helleseth[4]
$\{1, 2^{2k}+1, 2^{4k}+1\}$ $\{1, 2^{2k}+1, 2^{6k}+1\}$	gcd(2k,n)=1	Vinocha and Kumar[5]
$\{1, 3^{m}+1, 3^{2m}+1\}$ $\{1, 3^{m}+1, 3^{3m}+1\}$	gcd(m, n)=1	Vinocha and Kumar[6]

Lemma 1: The equation of the form $t^{3^l+1}+at^{3^l}+bt+c=0$ does not have four solutions if $\gcd(l,n)=1$ for all $a, band\ c$ all belongs to F_{3^m} .

3 Sufficient conditions for the zero set of non binary 3- error correcting codes

Theorem 1: The sufficient condition for the code represents by the zero set $\{1, 3^{l}+1, 3^{kl}+1\}$ is a Non binary triple –error-correcting code having gcd (l,n) =1.

Proof: we prove our result by contradicting the fact that the code C has not six linear dependent columns. The parity check matrix H has six or less dependent columns this implies there will be exist elements p, q, r, s, t, u in GF (3^n) s.t.

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

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

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

The minimum distance of code C with zero set $\{1, 3^l + 1\}$ having $gcd\ (l, n)$ = 1 is 5.then we get from the above two equations that all elements p, q, r, s, t, u have to be different

We can write this as $p + q + r = a_1$

$p^{3^l+1} + q^{3^l+1} + r^{3^l+1} = a_2$

$p^{3^{kl}+1} + q^{3^{kl}+1} + r^{3^{kl}+1} = a_3$

Replace p= p+ a_1 , q= q+ a_1 and r= r+ a_1

$p + q + r = 0$ (3.1)

$p^{3^l+1} + q^{3^l+1} + r^{3^l+1} = \omega$ (3.2)

$p^{3^{kl}+1} + q^{3^{kl}+1} + r^{3^{kl}+1} = \mu$ (3.3)

Where $\omega = a_2 + {a_1}^{3^l+1}$&$\mu = a_3 + {a_1}^{3^{kl}+1}$

From (3.1) substituting r = - (p+ q)

Therefore equations (3.2) & (3.3) becomes

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

$p^{3^{kl}}q + q^{3^{kl}}p = \mu$

Replace q = pq and we get

$p^{3^l+1}\left(q + q^{3^l}\right) = \omega$ (3.4)

$p^{3^{2m}+1}\left(q + q^{3^{2m}}\right) = \mu$ (3.5)

The equations (3.4) can be written as

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

Similarly we get

$\left(q + q^{3^{2l}}\right) = \omega\, p^{-3^l-1}$

$\left(q^{3^l} + q^{3^{2l}}\right) = \left(\omega\, p^{-3^l-1}\right)^{3^l}$

$\left(q^{3^{2l}} + q^{3^{3l}}\right) = \left(\omega\, p^{-3^l-1}\right)^{3^{2l}}$

………………………………………………

……………………………………………..

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

Adding all we get

$q + q^{3^{kl}} = \sum_{j=0}^{k-1}\left(\omega\, p^{-3^l-1}\right)^{3^{jl}}$

Using above equation (3.5) becomes

$p^{3^{kl}+1}\sum_{j=0}^{k-1}\left(\omega\, p^{-3^l-1}\right)^{3^{jl}} = \mu$ (1)

Our result is based on how many solutions of this equation have. If this equation has no more than 5 solutions then there is no codeword of weight six. This conclude that the minimum distance of the code is seven.

Theorem3.2: For K = 2 the code $\{1\,, 3^l+1, 3^{2l}+1\}$ with $\gcd(l,n)=1$ is a Triple Error correcting non binary BCH type code.

Proof: From the equation (1) we get for k=2

$p^{3^{2l}+1}\sum_{j=0}^{1}\left(\omega\, p^{-3^l-1}\right)^{3^{jl}} = \mu$

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

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

$\omega\, p^{-3^l-1+3^{2l}+1} + \omega^{3^l} p^{-3^{2l}-3^l+3^{2l}+1} = \mu$

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

Since $\gcd(l,n)=1$ this implies gcd $(3^l-1\,,n)=1$ and thus $p \to p^{3^l-1}$ is a one to one correspondence .then we use the transformation $p = p^{3^l-1}$and we get

$\omega\, p^{3^l} + \omega^{3^l} p^{-1} = \mu$

$\omega\, p^{3^l+1} + \omega^{3^l} = \mu p$

$\omega\, p^{3^l+1} - \mu p + \omega^{3^l} = 0$

$$p^{3^l+1} - \frac{\mu}{\omega} p + \omega^{3^{l-1}} = 0 \qquad (2)$$

Lemma 1 informs us that (2) equation have maximum four solutions. This proves the fact that the set $\{1\,, 3^l + 1, 3^{2l} + 1\}$ is a triple error correcting BCH type code.

Theorem3: For K = 3 the code $\{1\,, 3^l + 1, 3^{3l} + 1\}$ with $\gcd(l, n) = 1$ is a Triple Error correcting non binary BCH type code.

Proof: From the equation (1) we get for k=3

$$p^{3^{3l}+1} \sum_{j=0}^{2} \left(\omega\, p^{-3^l-1}\right)^{3^{jl}} = \mu$$

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

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

$$\omega\, p^{-3^l-1+3^{3l}+1} + \omega^{3^l} p^{-3^{2l}-3^l+3^{3l}+1} + \omega^{3^{2l}} p^{-3^{3l}-3^{2l1}+3^{3l}+1} = \mu$$

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

Since $\gcd(l, n) = 1$ this implies gcd $(3^{2l} - 1\,, n) = 1$ and thus $p \to p^{3^{2l}-1}$ is a one to one correspondence .then we use the transformation $p = p^{3^{2l}-1}$and we get

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

$$\omega\, p^{3^l+1} + \omega^{3^l} p^{3^l} + \omega^{3^{2l}} = \mu p$$

$$p^{3^l+1} + \omega^{3^l-1} p^{3^l} - \frac{\mu}{\omega} p + \omega^{3^{2l}-1} = 0$$

Lemma 1 tells that (2) equation has not more than four solutions. This informs us that the set $\{1\,, 3^l + 1, 3^{3l} + 1\}$ is a 3- error correcting BCH type code.

4 Conclusions:

In the present work we proposed the sufficient condition for the existence of distinct zero set of triple error correcting codes in non binary case. This condition is applicable only for k less than or equal to 3. The condition for the existence of zero set off triple error correcting code for k greater than 3 remains here an open problem. We will try to find zero set of triple error correcting codes for above said value in future.

Conflict of Interests

The authors declare that there is no conflict of interests.

REFERENCES

[1] T. Kasami, the weight enumerators for several classes of sub codes of the second order binary Reed Muller codes “Info.Contr, 18(1971), 369-394.

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

[3] A.W. Bluher, On$x^{q+1} + ax + b = 0$, Finite fields and Applications, 10 (3)(2004), 85-305.

[4] Carl Bracken and Tor Helleseth, Triple error correcting BCH like code, In proceedings of 2009IEEE International conference on symposium o international Theory volume3, ISIT’09, pages 1723-1725, Piscataway, NJ, USA, IEEE.

[5] Vinocha and Ajay Kumar, A class of triple error correcting BCH Codes, International Journal of Innovative Technology and Exploring Engineering, 3(2013), issue-3.

[6] Vinocha and Ajay Kumar, Zero Set of Ternary 3- error -correcting BCH type Codes, International Journal of Current Engineering and Technology, 4(2014), issue-1.