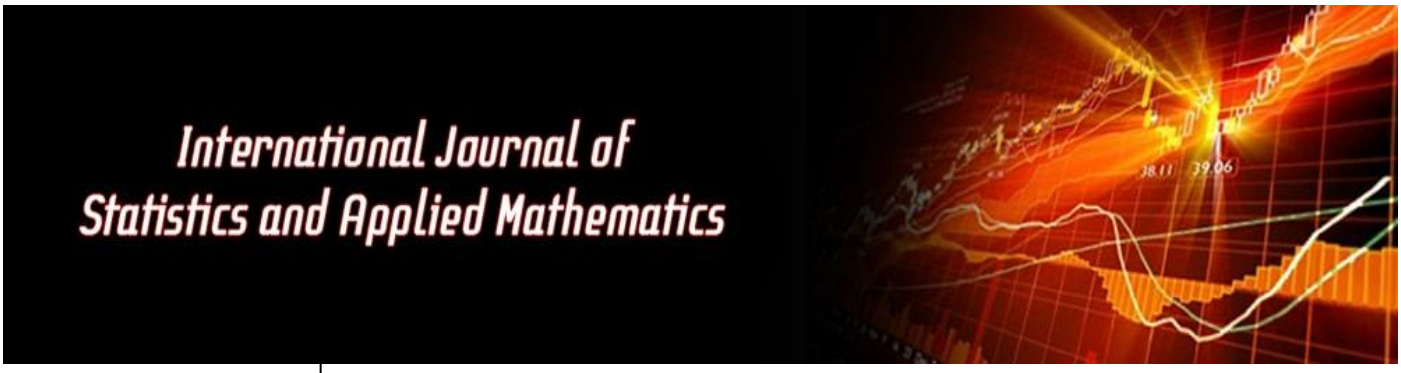
International Journal of Statistics and Applied Mathematics 2017; 2(4): 82-85



ISSN: 2456-1452
Maths 2017; 2(4): 82-85

www.mathsjournal.com
Received: 11-05-2017
Accepted: 12-06-2017

Yecheng Yao
Emory University (USA)

Jiayan Yu
Johns Hopkins University (USA)

Yuejun Sun
University of Pittsburgh (USA)

Weiheng Fu
University of California, Santa Barbara (USA)

Correspondence
Yecheng Yao
Emory University (USA)

Roots of triple error correcting codes with bch resembling domain

Yecheng Yao, Jiayan Yu, Yuejun Sun and Weiheng Fu

Abstract
Cyclic codes are most studied error correcting codes among the families of codes in coding theory. Vinocha and Kumar (2013) discovered some new zero set leading to the triple-error-correcting codes. In the present proposed work, we study on a new zero set of triple error correcting codes like BCH Code and proposed some new roots of error correcting code having roots $\{1, 3^{2a}+1, 3^{4a}+1\}$ and $\{1, 3^{2a}+1, 3^{6a}+1\}$ where gcd (2a, n) =1.

Keywords: Least distance, roots, BCH code and cyclic code

1. Introduction
A significant class of linear code is cyclic codes. Many families of codes including Golay codes, binary Hamming codes and BCH codes are either cyclic or extended cycle codes. BCH codes are a generalization of the Hamming codes for multiple–error correction. The cyclic structure of BCH codes was proved by Peterson (1960). BCH codes is an interesting class of linear codes. BCH codes 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 [7] was remarkable in this field. He suggested some zero set and proved that BCH codes are also represented by these zeros set. In a sequence of papers (2013), (2014) Vinocha and Kumar [11] were given a new technique to find the zero set of the above said codes. In this work, a new zero sets of BCH codes dissimilar from the existed zeros of BCH type codes is proposed. The proposed triple error correcting BCH type Code is a cyclic code with least distance seven. We will assume a Galois field with 2^n elements and g(X) be the gernator polynomial of the above said codes having j, j^3 and j^5 be its zeros. Let s_1= 1, s_2= 4 and s_4= 5 then the parity check matrix H is

$$\begin{bmatrix} 1 & \tau^{\theta^{s_1}} & \dots & \tau^{\theta^{(2^n-2)s_1}} \\ 1 & \tau^{\theta^{s_2}} & \dots & \tau^{\theta^{(2^n-2)s_2}} \\ 1 & \tau^{\theta^{s_3}} & \dots & \tau^{\theta^{(2^n-2)s_3}} \end{bmatrix}$$

The order of H is given 3n by $2^n - 1$. And code has same parameters as the BCH codes.The basic idea of such error-correcting codes is to add redundant bits in the stream so that the receiving point can still translate the information correctly even if there are mistakes. BCH can be non-binary (such as Reed-Solomon codes used by the Audio CDs and CD-ROMs), and binary. BCH is a generalization from the single error correcting Hamming code. BCH codes are often used over GE (2^8), which means there are 8 different phases carried on the output waves. In this case, a class of codes is three bits, and have 8 possibilities: 000, 001, 010, 100, 011, 101, 110, 111. If we use φ to represent each possibility as φ1, φ2, φ3 … φ8, we can write the information 000110100010 as φ1φ7φ4φ3.

1.1 Literature Survey

Zheng and Mazumder [1] in their research work proposes a One-pass Chase soft-decision decoding algorithm for BCH code based on an efficient polynomial division algorithm and VLSI architecture. The proposed algorithm is more powerful and efficient and has no speed penalty, effectively reducing the overall decoder area relative to traditional hard-decision decoding methods for BCH code.

Pachare *et al*. [2] their proposed work is likely to achieve FIR filters (Finite Impulse Response filter, a type of digital filters) based on a multi-bit error correcting code and can obtain low complexity, reduce delay and achieve efficient protection technique for higher bits data based on VHSIC Hardware Description Language.

Bracken *et al*. [3] in their research work author proposes a triple-error-correcting BCH based on studies as of Kasami and Chang *et al*. The paper also presents a simpler proof of Kasami's triple-error-correcting code, which can lead to new codes of this kind.

Wu *et al*. [5] in their research work proposes the blind recognition of BCH codes based on the property of GFFT of the code polynomial in the faster-than-Nyquist signaling system. Simulation results show the proposed method can maximize the correct recognition probability of the root of the generator polynomial based on the appropriate decision criterion and efficiently recognize BCH codes in the FTN system.

Argument-1: An equation of the form $x^{3^{2k}+1} + bx^{3^{2k}} + cx = d$defined on GF (2^n) has no more than four solutions in x when gcd (k, n) =1 for all b, c and d in GF (2^n) [9].

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.

2. 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 [3]
$\{1, 2^{2m}+1, 2^{4m}+1\}$ $\{1, 2^{2m}+1, 2^{6m}+1\}$	gcd(2m,n)=1,n is odd	Kumar and Vinocha 2013 [10]
$\{1, 3^m+1, 3^{2m}+1\}$ $\{1, 3^m+1, 3^{3m}+1\}$	gcd(m,n)=1,n is odd	Kumar and Vinocha 2014 [12]
$\{1, 3^{2a}+1, 3^{4a}+1\}$	gcd(2a,n)=1,n is odd	Theorem-3.1
$\{1, 3^{2a}+1, 3^{6a}+1\}$	gcd(2a,n)=1, n is odd	Theorem-3.2

3. New zero set of Triple Error Correcting BCH resembling Codes

In this part, we are specified a new zero set of BCH like codes and proposed the roots of the proposed codes. The proof of Theorem 3.1 and 3.2 are given in this section

Theorem 3.1The Triples{1,3^2a+1,3^4a+1}arethezerosetof a new type of 3 –error-correcting codes parallel to BCH code such that gcd (2a, n) =1.

Proof: The parity check matrix H has not more than six dependent columns then there exist basics $\mu_1, \mu_2, \mu_3, \nu_1, \nu_2, \nu_3$ in GF (2^n) s.t.

$$\mu_1 + \mu_2 + \mu_3 + \nu_1 + \nu_2 + \nu_3 = 0$$
$$\mu_1^{3^{2a}+1} + \mu_2^{3^{2a}+1} + \mu_3^{3^{2a}+1} + \nu_1^{3^{2a}+1} + \nu_2^{3^{2a}+1} + \nu_3^{3^{2a}+1} = 0$$
$$\mu_1^{3^{4a}+1} + \mu_2^{3^{4a}+1} + \mu_3^{3^{4a}+1} + \nu_1^{3^{4a}+1} + \nu_2^{3^{4a}+1} + \nu_3^{3^{4a}+1} = 0$$

The root set $\{1, 3^{2a}+1\}$ with an additional condition gcd (2a, n) = 1 must have least distance 5. Every element $\mu_1, \mu_2, \mu_3, \nu_1, \nu_2, \nu_3$ has to be dissimilar so from above equation, we get

$$\mu_1 + \mu_2 + \mu_3 = \xi_1$$
$$\mu_1^{3^{2a}+1} + \mu_2^{3^{2a}+1} + \mu_3^{3^{2a}+1} = \xi_2$$
$$\mu_1^{3^{4a}+1} + \mu_2^{3^{4a}+1} + \mu_3^{3^{4a}+1} = \xi_3$$

Now replace with

$$\mu_1 = \mu_1 + \xi_1, \mu_2 = \mu_2 + \xi_1, \mu_3 = \mu_3 + \xi_1$$

$$\mu_1 + \mu_2 + \mu_3 = 0 \quad (3.1)$$

$$\mu_1^{3^{2a}+1} + \mu_2^{3^{2a}+1} + \mu_3^{3^{2a}+1} = \theta \quad (3.2)$$

$$\mu_1^{3^{4a}+1} + \mu_2^{3^{4a}+1} + \mu_3^{3^{4a}+1} = \mu \quad (3.3)$$

Where $\theta = +\ ^{3^{2a}+1}\&\mu = +\ ^{3^{4a}+1}$

From (3.1) substituting $\mu_3 = \mu_1 + \mu_2$

Therefore equations (3.2) & (3.3) becomes

$$\mu_1^{3^{2a}}\mu_2 + \mu_2^{3^{2a}}\mu_1 = \theta$$
$$\mu_1^{3^{4a}}\mu_2 + \mu_2^{3^{4a}}\mu_1 = \mu$$

Substitute $\mu_2 = \mu_1\mu_2$ and we get

$$\mu_1^{3^{2a}+1}(\mu_2 + \mu_2^{3^{2a}}) = \theta \quad (3.4)$$

$$\mu_1^{3^{4a}+1}(\mu_2 + \mu_2^{3^{4a}}) = \mu \quad (3.5)$$

The equations (3.4) can be written as

$$\mu_2 + \mu_2^{3^{2a}} = \theta\mu_1^{-3^{2a}-1}$$

Equation (3.4) implies

$$\mu_2 + \mu_2^{3a} = \theta\mu_1^{-3^{2a}-1} + \theta^{3^a}\mu_1^{-3^{4a}-3^{2a}}$$

Using above equation (3.5) becomes

$$\mu_1^{3^{4a}+1}(\theta\mu_1^{-3^{2a}-1} + \theta^{3^a}\mu_1^{-3^{4a}-3^{2a}}) = \mu$$

Set $z = \mu_1^{3^{2a}-1}$

Therefore, the equation becomes

$$\theta z^{3^{2a}+1} + \mu z + \theta^{3^{2a}} = 0$$

As we know $\theta \neq 0$ this implies by Argument-1 that the above equation has no more than four solutions in z and we get the desired result.

Theorem3.2: The set $\{1, 3^{2a}+1, 3^{6a}+1\} are the$ roots of a new type of triple –error-correcting codes like BCH code provided gcd (2a, 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

$$\mu_1 + \mu_2 + \mu_3 = \xi_1 \quad (3.6)$$

$$\mu_1^{3^{2a}+1} + \mu_2^{3^{2a}+1} + \mu_3^{3^{2a}+1} = \xi_2 \quad (3.7)$$

$$\mu_1^{3^{6a}+1} + \mu_2^{3^{6a}+1} + \mu_3^{3^{6a}+1} = \xi_3 \quad (3.8)$$

Where $\theta = \mu_2 + {\mu_1}^{3^{2a}+1}\&\mu = \mu_3 + {\mu_1}^{3^{6a}+1}$

From (3.6) substituting $\mu_3 = \mu_1 + \mu_2$

Therefore equations (3.7) & (3.8) becomes

$$\mu_1^{3^{2a}}\mu_2 + \mu_2^{3^{2a}}\mu_1 = \theta$$
$$\mu_1^{3^{6a}}\mu_2 + \mu_2^{3^{6a}}\mu_1 = \mu$$

Replace $\mu_2 = \mu_1\mu_2$ and we get

$$\mu_1^{3^{2a}+1}(\mu_2 + \mu_2^{3^{2a}}) = \theta \quad (3.9)$$

$$\mu_1^{3^{6a}+1}(\mu_2 + \mu_2^{3^{6a}}) = \mu \quad (3.10)$$

The equations (3.9) can be written as

$$\mu_2 + \mu_2^{3^{2a}} = \theta\mu_1^{-3^{2a}-1}$$

Equation (3.4) emplies

$$\mu_2 + \mu_2^{3^{6a}} = \theta\mu_1^{-3^{2a}-1} + \theta^{3^{4a}}\mu_1^{-3^{6a}-3^{4a}} + \theta^{3^{2a}}\mu_1^{-3^{4a}-3^{2a}}$$

Using above equation (3.10) becomes

$$\mu_1^{3^{6a}+1}(\theta\mu_1^{-3^{2a}-1} + \theta^{3^{4a}}\mu_1^{-3^{6a}-3^{4a}} + \theta^{3^{2a}}\mu_1^{-3^{4a}-3^{2a}}) = \mu$$

Set $s = \mu_1^{3^{4a}-1}$

Therefore, the equation becomes

$$\theta s^{3^{2a}+1} + \theta^{3^{2a}}s^{3^{2a}} + s\mu + \theta^{3^{4a}} = 0$$

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

Conclusion

In the present work new zeros of triple error correcting BCH type code is discovered. Finding further such type of triples in the family of proposed triple error correcting BCH type codes is an interesting and challenging research problem. In future, we will work on finding the new roots of four or five error correcting codes distinct from the existing one.

References

1. Zheng N, Mazumder P. An Efficient Eligible Error Locator Polynomial Searching Algorithm and Hardware Architecture for One-Pass Chase Decoding of BCH Codes, in IEEE Transactions on Circuits and Systems II: Express Briefs. 2017; 64(5):580-584
2. Pachare, Anand N, Sumit R Vaidya, Sandip B Pawar. Design of BCH Decoder Based On Multi-bit Error Correction Codes Using VHDL. Imperial Journal of Interdisciplinary Research. 2016; 2(7)
3. Bracken, Carl, and Tor Helleseth. Triple-error-correcting BCH-like codes." In Information Theory, 2009. ISIT 2009. IEEE International Symposium on. 2009; 1723-1725. IEEE,
4. Canteaut, Anne, Florent Chabaud. A new algorithm for finding minimum-weight words in a linear code: application to McEliece's cryptosystem and to narrow-sense BCH codes of length 511. IEEE Transactions on Information Theory. 1998; 44(1):367-378.
5. Wu, Gang, Bangning Zhang, Daoxing Guo, Xiaohu Liang. Blind recognition of BCH codes in faster-than-Nyquist signalling system. Electronics Letters. 2016; 52(9):716-718.
6. Bose R, Ray-Chaudari D. On a class of error correcting binary group codes, Information and Control. 1960; (4):68-79,
7. Kasami T. The weight enumerators for several classes of sub codes of the second order binary Reed Muller codes Information and Control 1971; 18:369-394.
8. McWilliams FJ, Sloane NJA. The Theory of Error- Correcting Codes North Holland Amsterdam, 1977.
9. Bluher AW. On$x^{q+1} + ax + b = 0$, "Finite fields and Applications, 2004; 10(4).
10. Vinocha OP, Ajay Kumar. A class of triple error correcting BCH Codes" IJITEE, 2013; 4(4). ISSN: 2278-4075,
11. 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. 2016; 965-968
12. Vinocha OP, Ajay Kumar. Zero Set of Ternary 3-Error-Correcting BCH Type Codes, 2014.