International Journal of Contemporary Mathematical Sciences
Vol. 11, 2016, no. 5, 217 - 226
HIKARI Ltd, www.m-hikari.com
http://dx.doi.org/10.12988/ijcms.2016.615

Study on Coset Distribution of Extended Triple Error Correcting BCH Codes

O.P. Vinocha and Ajay Kumar

Department Mathematics
I.K Gujral Punjab Technical University
Jalandhar (Punjab), India

Abstract

BCH codes are fast decoding code, which makes them a better choice as error-correcting codes. The Triple error correcting BCH code has been the interest of study for a long time. In 2006 Charpin Helleseth and Zinoviev [2] did remarkable work by solving the problem of the coset distribution of the Triple error correcting BCH code of length $n \doteq 2^m - 1$. The objective of this paper is to carefully describes the conditions when syndrome $(S_1 S_3 S_5)$ is increased to $(S_1 S_3 S_5 S_7)$ and find Locator polynomial of extended BCH codes of different weights, which are helpful in finding coset distribution of these codes. Further we will compare the results of T. Kasami [9] and Charpin Helleseth and Zinoviev [2] with our results for m= 8, 9 and 10.

Keywords: Coset distribution; Extended triple error; BCH codes

1 Introduction

The process of determining the weight distribution of a code is very important because it assists in performing error evaluation and analysis. Weight distribution is known for short code and those that are grouped into classes that are understood. For instance, in BCH codes, there is a well-known formula that is used in the calculation of the singular, double and triple error correcting of binary primitive codes. The weight of a binary code is the number of non-zero

words in a code word. A coset on the other hand is the translation of the code by a given vector. The weight of the coset is therefore the least or the minimum weight of all the vectors that make up the coset. The vector within the coset that has the minimum weight is the coset leader and the possible maximum weight forms the covering radius.
The family of triple error correcting BCH codes has been a topic of great interest for several decades. In a series of paper by Horst and Berger and Helleseth [1] the covering radius of these codes is determined to be five. Later the weight distribution of these codes was determined by Kasami [8] for odd m. But the coset distribution of Triple errors correcting BCH codes remained an open problem for several years. This problem was solved by Charpin Helleseth and Zinoviev in 2006. They gave the coset distribution of these triple error correcting BCH codes. In this work we will study if one syndrome is increased in the triple error correcting BCH codes then what will be the Locator polynomials of the given code with different weight, these results will give us direction to find coset distribution of these extended BCH codes also we compare the new results with the previous results given by Charpin, Helleseth and Zinoviev [2]
Coset of a code: A coset of code C is the set of vectors $a + c$ where $a$is an element of galious field with 2^m elements.

Definition 1.1 Coset of a code: A coset of code C is the set of vectors $a + C$for some $a \in GF2^m)$ i.e. $a + C = a + C : a \in GF2^m$

Definition 1.2 Trace of a function: The trace of a function from$GF2^m to GF(2)$ is define as [3] $Tr(x) = \sum_{i=0}^{m-1} x^{2^1}$

Argument 1: The coset distribution of Triple error correcting BCH code of length $n = 2^m - 1$ is given by Van Der Horst and Toby Berger in [1] are

$$K_0 = 1$$
$$K_1 = n$$
$$K_3 = \frac{n(n-1)(n-2)}{6}$$
$$K_4 = \frac{6n^2 + 10n - 3}{6}$$
$$K_5 = \frac{4n(n+2)}{3}$$

Argument 2: The coset distribution of Triple error correcting BCH code of length $N = 2^m$is given by Pascale Charpin, Tor Helleseth and Victor A. Zinoviev [2] are

$$A_0 = 1$$
$$A_1 = N$$
$$A_2 = \frac{N(N-1)}{2}$$

$A_3 = \dfrac{N(N-1)(N-2)}{6}$
$A_4 = \dfrac{(N-1)(6N^2-5N-2)}{6}$
$A_5 = \dfrac{N(N-1)(5N+8)}{6}$
$A_6 = \dfrac{4(N-1)(N+1)}{3}$
The parity check matrix of extended binary triple error correcting BCH code is defined as

$$\begin{pmatrix} 1 & 1 & 1 & 1..... & 1 \\ 0 & 1 & \alpha & \alpha^2..... & \alpha^{n-1} \\ 0 & 1 & \alpha^3 & \alpha^6..... & \alpha^{3(n-1)} \\ 0 & 1 & \alpha^5 & \alpha^{10}..... & \alpha^{5(n-1)} \end{pmatrix}$$

where the order of element α is$n = 2^m - 1$ in $GF(2^{m)}$.The syndrome s of the received vector$r$ is $s = zH^t$ where$z = (z_0, z_1, z_2.z_{n-1})$and H^t denotes the transpose of the matrix H .the locator polynomial z of weight w is defined as $\sigma(z) = Z^w + \sigma_1 Z^{w-1} + ... + \sigma_w$Equivalently, we can find a locator polynomial

$$\sigma(z) = \sum_{i=1}^{w} Z + Z_i$$

whose degree is called the weight of the code such that $S_j = \sum_{i=1}^{w} Z_i^j forj = 1, 3, 5, 7$.
The Newton's identities describe the relationship between the coefficient of locator polynomial and the error location as:
$S_1 + \sigma_1 = 0$
$S_2 + \sigma_1 S_1 + 2\sigma_2 = 0$
$S_3 + \sigma_1 S_2 + \sigma_2 S_1 + 3\sigma_3 = 0$
....
$S_j + \sigma_1 S_{j-1} + \sigma_2 S_{j-2} + ... + j\sigma_{j=0}$ for $j \leqslant w$
We make an assumption that$\sigma_j = 0$ for$j > w$ therefore from the Newton's identities we get
$S_1 = \sigma_1$
$S_3 = S_1^3 + \sigma_2 S_1 + \sigma_3$
$S_5 = S_1^5 + \sigma_2 S_3 + \sigma_3 S_1^2 + \sigma_4 S_1 + \sigma_5$
$S_7 = S_1^7 + \sigma_2 S_5 + \sigma_3 S_1^4 + \sigma_4 S_3 + \sigma_5 S_2 + \sigma_6 S_1 + \sigma_7$

2 Locator Polynomials of Different Weights:

A For the weight w = 1
$\sigma(z) = Z + S_1$

The syndrome $(S_1S_3S_5S_7)$ is calculated by $S_j = Z_I^J$ FOR $J = 1, 3, 5, 7$. Therefore from Newton's identities: $S_1 + \sigma_1 = 0$ this implies $S_1 = \sigma_1$ $S_3 = S_1^3$ $S_5 = S_1^5 and S_7 = S_1^7$ this implies that there are n cosets with syndromes $(S_1, S_1^3, S_1^5, S_1^7)$ where $S_1 \neq 0$ of weight one.

B For the weight w = 2

The coset leader of w =2 has locator polynomial $\sigma(z) = Z^2 + \sigma_1 Z + \sigma_2$.

From the Newton's identities:

$$s_1 = \sigma_1 \tag{1}$$

$$S_3 = S_1^3 + \sigma_2 S_1 \Rightarrow \sigma_2 = \frac{S_3 + S_1^3}{S_1} \tag{2}$$

$$S_5 = S_1^5 + \sigma_2 S_3 \Rightarrow \sigma_2 = \frac{S_5 + S_1^5}{S_3} \tag{3}$$

$$S_7 = S_1^7 + \sigma_2 S_5 \Rightarrow \sigma_2 = \frac{S_7 + S_1^7}{S_5} \tag{4}$$

From (2) and (3) $L = S_3^2 + S_3S_1^3 + S_1S_5 + S_1^6 = 0$. From (3) and (4) $M = S_5^2 + S_5S_1^5 + S_3S_7 + S_1^7S_3 = 0$. From (4) and (2) $N = S_3S_5 + S_5S_1^3 + S_1S_7 + S_1^8 = 0$

Hence we get three locator polynomial for$w = 2$

Case 1 If $\sigma_2 = \dfrac{S_3 + S_1^3}{S_1}$ then locator polynomial is $\sigma(z) = Z_2 + S_1 Z + \dfrac{S_3 + S_1^3}{S_1}$

This equation has two distinct zeros when $Tr(\dfrac{S_3 + S_1^3}{S_1}) = 0$

Case 2 if $\sigma_2 = \dfrac{S_5 + S_1^5}{S_5}$ then locator polynomial is $\sigma(z) = Z^2 + S_1 Z + \dfrac{S_5 + S_1^5}{S_5}$

Case 3 if $\sigma_2 = \dfrac{S_7 + S_1^7}{S_7}$then locator polynomial is $\sigma(Z) = Z^2 + S_1 Z + \dfrac{S_7 + S_1^7}{S_7}$

This equation has two distinct zeros when $Tr(\dfrac{S_7 + S_1^7}{S_7}) = 0$

C For the weight w=3

The coset leader of $w = 3$ has locator polynomial $\sigma(z) = Z^3 + \sigma_1 Z^2 + \sigma_2 Z + \sigma_3$

From the Newton's identities

$$S_1 = \sigma_1 \tag{5}$$

$$S_3 = S_1^3 + \sigma_2 S_1 + \sigma_3 \tag{6}$$

$$S_5 = S_1^5 + \sigma_2 S_3 + \sigma_3 S_1^2 \tag{7}$$

$$S_7 = S_1^7 + \sigma_2 S_5 + \sigma_3 S_1^4 \tag{8}$$

From (6) and (7)
$\sigma_2 = \dfrac{S_5 + S_3S_1^2}{S_3 + S_1^3}$ Similarly from (7), (8) and (8) and (6) we get the two more values of σ_2 respectively

$\sigma_2 = \dfrac{S_7 + S_5S_1^2}{S_5 + S_1^3}$ and $\sigma_2 = \dfrac{S_7 + S_3S_1^4}{S_5 + S_1^5}$
Case 1 if we take $\sigma_2 = \dfrac{S_5 + S_3S_1^2}{S_3 + S_1^3}$ then from (6) $S_3 = S_1^3 + \sigma_2S_1 + \sigma_3$
$\sigma_3 = S_3 + S_1^3 + \sigma_2S_1$
$\sigma_3 = S_3 + S_1^3 + S_1\dfrac{S_5 + S_3S_1^2}{S_3 + S_1^3}$
$\sigma_3 = \dfrac{S_3^2 + S_1^6 + S_1S_5 + S_3S_1^3}{S_3+_{S_1^3}}$ $\sigma_3 = \dfrac{L}{S_3 + S_1^3}$ where $L = S_3^2 + S_1^6 + S_1S_5 + S_1^3$

Hence the error locator polynomial in this case is $\sigma(z) = Z^3+S_1Z^2+\dfrac{S_5 + S_3S_1^2}{S_3 + S_1^3}Z+$
$+\dfrac{L}{S_3 + S_1^3}$.
Case 2 if we take $\sigma_2 = \dfrac{S_7 + S_5S_1^2}{S_5 + S_1S_3}$ then from (6) we get $3 = \dfrac{M}{S_5 + S_1S_3}$ where $M = S_3S_5 + S_2S_1 + S_3S_1^4 + S_1S_7$. Hence the error locator polynomial in this case is $\sigma(z) = Z^3 + S_1Z^2 + \dfrac{S_7 + S_5S_1^2}{S_5 + S_1S_3}Z + \dfrac{M}{S_5 + S_1S_3}$.
Case 3 if we take$\sigma_2 = \dfrac{S_7 + S_3S_{_1}^{4}}{S_5 + S_1^5}$ then from (6)We get$\sigma_3 = \dfrac{N}{S_5 + S_1^5}$ where $N = S_3S_5 + S_5S_1^3 + S_1S_7 + S_1^8$. Thus the error locator polynomial is
$\sigma(Z) = Z^3 + S_1Z^2 + \dfrac{S_7 + S_3S_{_1}^{4}}{S_5 + S_1^5}Z + \dfrac{N}{S_5 + S_1^5}$.

D For the weight w=5

We will discuss the conditions of the cosets of weight 5 for extended error correcting BCH codes .we give a sequence of theorems in which we study the extended error correcting BCH codes of weight 5 with syndrome (S_1, S_3, S_5, S_7) where$S_1 \neq 0$

Theorem 1 The coset S with syndrome(S_1, S_3, S_5, S_7) where $S_1 \neq 0$ such that $L = S_3^2 + S_1^6 + S_1S_5 + S_1^3$, $Tr(\dfrac{S_5 + S_3S_1^3}{a(S_3S_1 + S_1^4)} = 1$ and $Tr(\dfrac{a}{S_1}) = 1$ then S is a coset of weight 5 , where $\sigma_2 = \dfrac{S_5 + S_3S_1^2}{S_3 + S_1^3}$

Proof: Since S is a coset with syndrome $(S_1S_3S_5S_7)$ where $S_1 \neq 0$ there-

fore the weight of coset is at least one. We observe from the trace condition $S_3 \neq S-1^3$ that the coset S has weight at least 2. From trace condition $Tr(\frac{S_5+S_3S_1^3}{a(S_3S_1+S_1^4)})=1$ we observe that the roots of locator polynomial for$w=2$ are not in $GF(2^m)$ this implies $W \neq 2$ further condition $L=0$ inform us that locator polynomial does not have weight $W=3$ that is $W \neq 3$ .Therefore, we make an assumption that the coset S has weight 4 and we will prove by contradiction that S has at least weight5 The coset leader of $W=4$has locator polynomial
$\sigma(z)=Z^4+\sigma_1Z^3+\sigma_2Z^2+\sigma_3Z+\sigma_4$

$$S_1=\sigma_1 \tag{9}$$

$$S_3=S_1^3+\sigma_2S_1+\sigma_3 \tag{10}$$

$$S_5=S_1^5+\sigma_2S_3+\sigma_3S_1^2+\sigma_4S_1 \tag{11}$$

$$S_7=S_1^7+\sigma_2S_5+\sigma_3S_1^4+\sigma_4S_3 \tag{12}$$

From (11) and (12) $\sigma_4=(S_7+S_5S_1^2)+\sigma_2\frac{S_5+S_3S_1^2}{S_3+S_1^3}$

The four distinct zeros of Locator polynomial $\sigma(z)=Z^4+\sigma_1Z^3+\sigma_2Z^2+\sigma_3Z+\sigma_4$ in $G(2^m)$ can be written as $\sigma(z)=[Z^2+aZ+b][Z^2+(a+S1)Z+c]$
Comparing the coefficient we get
$\sigma_1=a+a+S_1$
$\sigma_2=c+a^2+S_1a+b$
$\sigma_3=ab+bS_1+ac$
$\sigma_4=bc$
$b=\frac{\sigma_4}{c}$
After calculating we get
$d=\frac{\sigma_4S_1}{\sigma_3+a(\sigma_2+a^2+S_1a)}$ and $b=\frac{\sigma_3+a(\sigma_2+a^2+S_1a}{S_1}$
We know that the equation Z^2+aZ+b must have two distinct zeros in $GF(2^{m)}$
if $Tr\frac{b}{c^2}=0$
$Tr\frac{b}{c^2}=Tr\frac{\sigma_3+a(\sigma_2+a^2+S_1a}{S_1a^2}$
$=Tr\frac{S_3+S_1^3+S_1(S_5+S_3S_1^2/S_3+S_1^3)+a(S_5+S_3S_1^2/S_3+S_1^3+a^2+aS_1)}{S_1a^2}$
$=Tr\frac{S_3^2+S_1^6+S_1S_5+S_3S_1^3}{S_3+S_1^3)S_1a^2}+Tr\frac{S_5+S_3S_1^3}{a(S_3S_1+S_1^4)}+Tr\frac{a}{S_1}+Tr(1)$
$=Tr\frac{L}{(S_3+S_1^3)S_1a^2}+Tr\frac{S_5+S_3S_1^3}{a(S_3S_1+S_1^4)}+Tr\frac{a}{S_1}+Tr(1)$

$= 0 + Tr\dfrac{S_5 + S_3S_1^3}{a(S_3S_1 + S_1^4)} + Tr\dfrac{a}{S_1} + Tr(1)$
$= 1 + 1 + 1$
$= 1$

Here $Tr\dfrac{b}{a^2} = 1$ this implies contradiction hence we observe that weight of the coset is at least five.

Theorem 2: The coset S with syndrome $(S_1S_3S_5S_7)$ where $S_1 \neq 0$ such that$M = S_3S_5 + S_3^2S_1 + S_3S_1^4 + S_1S_7 = 0$, $Tr\dfrac{S_7 + S_5S_1^2}{a(S_5 + S_1S_3)} = 1$ and $Tr\dfrac{a}{S_1} =$ 1then S is a coset of weight5 , where $\sigma_2 = \dfrac{S_7 + S_5S_1^2}{S_5 + S_1S_3}$

Proof: The proof is similar as theorem 1.

Theorem 3: The coset S with syndrome $(S_1S_3S_5S_7)$ where $S_1 \neq 0$ such that $N = S_3S_5 + S_5S_1^3 + S_1S_7 + S_1^8 = 0 \quad Tr\dfrac{S_7 + S_3S_1^4}{a(S_5 + S_1^5)} = 1$ and $Tr\dfrac{a}{S_1} = 1$ then S is a coset of weight 5 , where$\sigma_2 = \dfrac{S_7 + S_3S_1^4}{S_5 + S_1^5}$

Proof: The proof is similar as above theorem 1.

3 Comparison of Different Cosets of length $2^m - 1, 2^m$ and $2^m + 1$

The distribution of coset for extended BCH codes of length$N = 2^m + 1$ has minimum distance 9.in this section we determine the coset distribution of the triple error correcting BCH Codes. Denote by B the extended binary BCH code of length $N = 2^m + 1$ whose parity check matrix H is defined as:

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0..... & 0 \\ 0 & 1 & 1 & 1 & 1..... & 1 \\ 0 & 0 & 1 & \alpha & \alpha^2...... & \alpha^{n-1} \\ 0 & 0 & 1 & \alpha^3 & \alpha^6..... & \alpha^{3(n-1)} \\ 0 & 0 & 1 & \alpha^5 & \alpha^{10}..... & \alpha^{5(n-1)} \end{pmatrix}$$

Where has an order of $n = 2^m - 1$ in $GF(2^m)$ and syndrome has 6-tuple $(S_0, S_1, S_3, S_5, S_7)$ Denote by A_i the number of cosets of B of weight i since B is an extended code such that the covering radius of B is 6
$\sum_{i=1}^{7} A_i = 2N^4$ and $\sum_{i=0}^{3} A_2 i - 1$

$$B_0 + B_2 + B_6 + B_8 = N^4 \tag{13}$$

$$B_1 + B_3 + B_5 + B_7 = N^4 \tag{14}$$

We will assume that $B_0 = 1 \quad and \quad B_i = nc_i \qquad for \quad i = 1, 2, 3, 4.$

From (13) we get $B_6 = N^4 - 1 - \dfrac{N(N-1)}{2} - \dfrac{N(N-1)(N-2)(N-3)}{24}$

Therefore $B_6 = \dfrac{5N^4 + 6N^3 - 14N^2 + 3N - 6}{6}$

From (14) $N + \dfrac{N(N-1)(N-2)}{6} + B_5 + B_7 = N^4$

We know that any coset of weight 7 of the code B of length $N = 2^m + 1$ is reduced to a coset of weight 6 of the corresponding code of length $n = 2^m$ therefore $B_7 = \Gamma_6$ i.e. $B_7 = \dfrac{4N(N-2)}{3}$

$B_5 = \dfrac{N(6N^3 - N^2 - 5N + 8)}{6}$

Theorem 4: Let A_i denote the number of cosets with a coset leader of weight i in the extended 3-error correcting binary BCH Code of length $N = 2^m+1$ then coset distribution of B is given where value of m should be equal or greater than 8.

Proof $B_0 = 1$

$B_1 = N$

$B_2 = \dfrac{N(N-1)}{2}$

$B_3 = \dfrac{N(N-1)(N-2)}{6}$

$B_4 = \dfrac{N(N-1)(N-2)(N-3)}{24}$

$B5 = \dfrac{N(6N^3 - N^2 - 5N + 8)}{6}$

$B_6 = \dfrac{5N^4 + 6N^3 - 14N^2 + 3N - 6}{6}$

$B_7 = \dfrac{4N(N-2)}{3}$

In the following tables we compared the number of cosets of BCH codes and extended BCH codes with different length of $2^n - 1, 2^m and 2^m + 1$ .The coset distribution for $n = 2^n - 1, 2^m$are calculated by Charpin Helleseth and Zinoviev [2] in tables for m= 5 ,6, and 7 they conclude that $\Gamma_6 = K_5.$ but these tables are not true for these values .We showed that these tables are true for m= 8,9and 10 and futher we compared the two tables with our results .It is obvious from tables that$K_5 = A_6 = B_7$ for m= 8, 9 and 10.

m	8	9	10
K_0	1	1	1
K_1	255	511	10231
K_2	32385	130305	5227531
K_3	2731135	22108415	177910271
K_4	13926060	111628972	893909676
K_5	87380	349524	1398100

Table 1: Table for cosets of length $2^m - 1$

m	8	9	10
A_0	1	1	1
A_1	256	512	1024
A_2	32640	130816	523776
A_3	2763520	22238720	178433024
A_4	16657195	133737387	6430919682
A_5	14013440	111978496	895307776
A_6	87380	349524	1398100

Table 2: Table for cosets of length 2^m

m	8	9	10
B_0	1	1	1
B_1	257	513	1025
B_2	32896	131328	524800
B_3	2796160	22369536	178956800
B_4	177556160	2852115840	45723462400
B_5	4359586604	69235202988	1103632534700
B_6	21913275642	11677378985	920918515199
B_7	87380	349524	1398100

Table 3: Table for cosets of length $2^m + 1$

4 Conclusion

In this work we discussed the locator polynomials and distribution of the cosets in extended Binary Triple error correcting BCH codes. We also find the coset distribution of BCH codes of length $n = 2^m + 1$ with minimum distance 9 and compared it with previous known results of Charpin, Helleseth and Zinoviev.Comparison of cosets distribution for m= 8, 9 and 10 is shown in Table 1, Table 2 and Table 3 Further study on the locator polynomial of weight 6 and 7 is a challenging research problem that may lead to other interesting connection.

References

[1] Vander Horst and Toby Berger, Complete decoding of triple-error-correcting binary BCH codes, *IEEE Trans. Inform Theory*, **22** (1976), no. 2, 138-147. http://dx.doi.org/10.1109/tit.1976.1055530

[2] Pascale Charpin, Tor Helleseth and Victor A. Zinoviev, The Coset Distribution of Triple-Error-Correcting Binary Primitive BCH Codes, *IEEE Trans. Inform Theory*, **52** (2006), 1727-1732. http://dx.doi.org/10.1109/tit.2006.871605

[3] E.R. Berlekamp, H. Rumsey and G. Solomon, On the solution of algebraic equations over finite fields, *Inform. Contr.*, **10** (1967), 553-564. http://dx.doi.org/10.1016/s0019-9958(67)91016-9

[4] F.J. MacWilliams and N. Sloane, *The Theory of Error Correcting Codes*, North Holland, Amsterdam, Netherland, 1968.

[5] E.R. Berlekamp, *Algebraic Coding Theory*, McGraw-Hill, New York, 1968.

[6] T. Helleseth, All binary 3-error-correcting BCH Codes of length $2^m - i$ have covering radius 5, *IEEE Trans. Inform Theory*, **24** (1978), 257-258. http://dx.doi.org/10.1109/tit.1978.1055847

[7] E.F. Assmus, Jr. and H.F. Mattson, Jr., Some 3-error correcting BCH Codes have covering radius 5, *IEEE Trans. Inform Theory*, **22** (1976), 348-349. http://dx.doi.org/10.1109/tit.1976.1055556

[8] T. Kasami, *Weight Distributions of Bose-Chaudhuri-Hocquenghem Codes, in Combinatorial Mathematics and Its Applications*, R. Boseand T. Dowling, Eds., University of North Carolina Press, Chapel Hill, North Carolina, 1969.

Received: February 11, 2016; Published: April 14, 2016