Available online at http://scik.org

J. Math. Comput. Sci. 6 (2016), No. 6, 1169-1176

ISSN: 1927-5307

A CLASS OF NON-BINARY BCH CODE OF BOSE AND MINIMUM DISTANCE

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

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

[2]Department of Mathematics, Tantia College of Engineering, Tantia University, Sri-Ganganagar, India

Abstract. BCH Code is most famous code in the field of coding theory because they have very effective encoding and decoding algorithms. These codes are best considered as cyclic codes. But from the last two decades there is not much progress over the minimum distance of BCH code. To calculate the minimum distance of BCH code is a well-known problem in general. We studied on the dimension of narrow sense Non-binary BCH code $(p,\ u, q^{2l-4}+1)$ and also find out the Bose Distance of non-binary BCH code of design distance $\delta = p^{2l}+1$.

Keywords: coding theory; cyclic codes; BCH code.

2010 AMS Subject Classification: 94A24.

I. Introduction

BCH code has an important place in the field of coding theory. These codes are better considered as a subclass of cyclic codes. Although BCH codes came in to existence in 1959 by Hocquenghem. But progress on minimum distance of said codes are very limited. The dimension of BCH code is found only for the small design distance, but it is a challenging problem to calculate dimension of narrow sense BCH code in general. There exist much type of bounds to find the dimension of BCH code, but these bounds are applicable only for a few cases. Similarly we have a little knowledge about the minimum distance of narrow sense BCH code. P. Charpin [1990] discussed that calculating minimum distance of narrow sense BCH codes is indeed a hard problem. Now from the last two decades a little work on minimum distance and dimension of these codes is done. Ding , Xiaoni and Zhou [] found the dimension , Bose and minimum distance of a narrow sense BCH code with design distance $\delta = p^l + h$, where $l \in [1, u-2]$ and $0 \le h \le \frac{p^l-1}{p^{u-l}} + 1$.

---

*Corresponding author

Received June 22, 2016

We proposed a class of narrow sense BCH code of length n=$p^{2l}-1$ with design distance $\delta = p^{2l}+1$ where$1 \le l \le u-1$. We will find the minimum distance and dimension of these codes and proved that the proposed narrow sense BCH code have Bose distance$\left\lfloor \frac{p^{2u}-1}{p^{2u-2l}-1} \right\rfloor + 1$.

Definition 1.1 A cyclic code of length n over GF(q) is a narrow sense BCH code of designed distance δ with gernator polynomial $g(x) = lcm\{m_1, m_2 \ldots\ldots\ldots m_{\delta-1}\}$, this code has a string of $\delta - 1$ consecutive powers of α as zeros. [3]

Definition 1.2 The maximum design distance of the BCH Code is known as the Bose distance of the BCH code.

Argument1: Let $\delta = p^{2l}$ where $\frac{u}{4} \le l \le u-1$ and $s = u - 2l$ then dimension k of the code $C(p,u,\delta)$ is given by $k = \emptyset(u) - (p-1)^2 \sum_{j=0}^{s-4}(s-j-3)\emptyset(2u-s+j-4)$

Where $\emptyset(u) = p\emptyset(u-2) - (2p-2)\emptyset(2u-s-2)$,$u > 2s$

$\emptyset(j) = 2p^j$ For $0 \le j \le 1$ and $\emptyset(s) = 2p^s - 2$

II Dimension of narrow sense Bose Chaudhuri Hocquenghem code of design distance $\delta = p^{2t}+1$

Theorem 1: Suppose u≥ 4 then the narrow sense BCH Code $C(p, u, p^{2u-4}+1)$ have the following dimension

$$\left(\frac{(p-2)+\sqrt{p^2+4p-12}}{2}\right)^u + \left(\frac{(p-2)-\sqrt{p^2+4p-12}}{2}\right)^u$$

Proof: we know that if the narrow sense BCH has design distance $\delta = p^{2u-4}+1$ then $\bar{\delta} = p^{2u-4}$ will also be the design distance of the code. From argument 1 we conclude that the dimension of the code is $k = \emptyset(u) - (p-1)^2\emptyset(u-6)$

Where $\emptyset(u) = p\emptyset(u-2) - (2p-2)\emptyset(u-6)$ (1)

With the initial conditions

$\emptyset(0) = 2$ And $\emptyset(1) = 2p$

There is a well known formula that if $\emptyset(u) = x^u$

Then $x^{s+1} - px^s + p - 1 = 0$

In our case s=2

This implies $x^3 - px^2 + 4p - 8 = 0$ (2)

For calculating dimension of the defined code we have to solve the recurrence relation of (1). We will solve the equation $x^3 - px^2 + 4p - 8 = 0$ in the field of complex numbers that and find the following three roots

$x_1 = 2$

$x_2 = \frac{(p-2)+\sqrt{p^2+4p-12}}{2}$ and

$x_3 = \frac{(p-2)-\sqrt{p^2+4p-12}}{2}$

Let $\emptyset(u) = d + a x_1^u + b x_2^u$ for some constant a, b and d are the elements of complex field

From the initial conditions

$\emptyset(0) = 2$, $\emptyset(1) = 2p$ and $\emptyset(2) = 2p^2 - 2$

We get

$d + a + b = 2$ (3)

$d + a x_1 + b x_2 = 2p$ (4)

$d + a x_1^2 + b x_2^2 = 2p^2 - 2$ (5)

From (3) and (4)

$a(x_1 - 1) + b(x_2 - 1) = 2p - 2$ (6)

And from (4) and (5)

$a(x_1^2 - 1) + b(x_2^2 - 1) = 2p^2 - 2$ (7)

From solving (6) and (7) we get

$a = \frac{(-4p^2+10p+8)-(4p^2-4p-2)\sqrt{p^2+4p-12}}{(p-2)(p^2+4p-12)+(p^2-2p-6)\sqrt{p^2-4p+4}}$

$b = \frac{(4p^2-10p)-(4p-2)\sqrt{p^2-4p+4}}{(p-2)(p^2+4p-12)+(p^2-2p-6)\sqrt{p^2-4p+4}}$

Now from equations (3) (4)and (5) we conclude that d=0

Hence $\emptyset(u) = a x_1^u + b x_2^u$

From (1) we get

$k = \emptyset(u) - (p-1)^2 \emptyset(u-6)$

$= a x_1^u + b x_2^u - (p-1)^2 \emptyset(u-6)$

$a x_1^u + b x_2^u - (p-1)^2 [a x_1^{u-6} + b x_2^{u-6}]$

$= a x_1^{u-6}(x_1^6 - (p-1)^2) + b x_1^{u-6}(x_2^6 - (p-1)^2)$

$= \left(\frac{(p-2)+\sqrt{p^2+4p-12}}{2}\right)^u + \left(\frac{(p-2)-\sqrt{p^2+4p-12}}{2}\right)^u$

Hence we get the desired result.

III Bose and Minimum Distance of narrow sense Bose Chaudhuri Hocquenghem code of Design Distance $\delta = p^{2l} + 1$

Theorem 2: The narrow sense Bose Chaudhuri Hocquenghem code of design distance $\delta = p^{2l} + 1$ has the Bose distance $\delta_B = \left\lfloor \frac{p^{2u}-2}{p^{2(u-l)}-1} \right\rfloor + 1$.

Proof: we study the proof in to two cases

Case1: $\leq \frac{u}{2}$, we define

$\sigma_\delta = \bigcup_{j=1}^{\delta-1} C_i$

Since we have given that $l \leq \frac{u}{2}$

Then $\delta_D = \left\lfloor \frac{p^{2u}-2}{p^{2(u-l)}-1} \right\rfloor + 1$

$= p^{2l} + \left\lfloor \frac{p^{2l}-2}{p^{2(u-l)}-1} \right\rfloor + 1$

$= p^{2l} + 1$

Now we have to prove that $\delta \notin \delta_D$ to get the desired result for any $j \ for \ 0 \leq j \leq u-1$

Define $B_j = \delta p^j \ mod \ n$

When $2l + j < 2u$

We have $B_j = \delta p^j$

$B_j = (p^{2l} + 1)p^j$

$= p^{2l+j} + p^j$

$\geq p^{2l} + 1$

$= \delta$

Similarly when $2l + j \geq 2u$

We get $j \geq 2(u - l) \geq \frac{u}{2}$

This implies $2l + j \leq u + \frac{u}{2}$

$B_j = p^{(2l+j) mod \ 2u} + p^j$

$\geq p^{\frac{u}{2}} + 1$

$\geq \delta$

Hence we conclude that $B_j \notin \delta_D$ for all $j \in [0, m-1]$ then it follows that $\delta_D = \delta_B = \delta$

Case 2: $l > \frac{u}{2}$ as we know $l > 2(u-l)$

Thus there exist two unique integers b, c such that

$l = 2a(u-l) + b$ With $a \geq 1$ and $0 \leq b \leq 2(u-l)$

$\delta_D = \left\lfloor \frac{p^{2u}-2}{p^{2(u-l)}-1} \right\rfloor + 1$

$= p^{2l} + p^b \left(\frac{p^{2(u-l)a}-1}{p^{2(u-l)}-1} \right) + \left\lfloor \frac{p^b-2}{p^{2(u-l)}-1} \right\rfloor + 1$

$$= \begin{Bmatrix} p^{2l} + p^b \left(\frac{p^{2(u-l)a}-1}{p^{2(u-l)}-1} \right) + 1 & if\ 1 \leq b \leq 2(u-l) \\ p^{2l} + \left(\frac{p^{2(u-l)a}-1}{p^{2(u-l)}-1} \right) + 1 & if\ \ b = 0 \end{Bmatrix}$$

We divided case 2 into two sub cases

Sub case 1: when b=0

As $l > \frac{u}{2}$ we have $a \geq 2$ and $l = 2a(u-l)$

Therefore $\delta_D = p^{2a(u-l)} + p^{2(u-l)(a-1)} + \cdots p^{2a(u-l)} + 1$

We will prove in this sub case that $\delta_B = \delta_D$

For this we will prove that every integer j with condition $\delta \leq j \leq \delta_B - 1$ contains in δ_D

$\delta = p^{2l} + 1$

$= p^{2(2u-2l)a} + 1$ and

$\delta p^{2(u-l)} \ mod\ n$

$= (p^{2l} + 1) p^{2(u-l)} \ mod\ n$

$= 1 + p^{2(u-l)}$

$< \delta$

This follows that $\delta \in \delta_D$ and $\delta_{D+1} = \delta_D$ (3)

Now we wish to prove that $\sigma_{p^{2(u-l)a} + p^{2(u-l)(a-1)+1}} = \sigma_\delta$ (4)

Suppose $i = p^{2(u-l)a} + i_0$ for $1 \leq i_0 \leq p^{(2u-2l)(a-1)}$

Then $ip^{2(u-l)} \ mod\ n$

$\left(p^{2(u-l)a} + i_0\right) p^{2(u-l)} \ mod\ n$

$1 + i_0\ p^{2(u-l)}$

$\leq \delta$

The desired result then follows (3)

If a=2 the proof is completed for sub case 1 now if $a \geq 3$

We will prove that $\sigma_{p^{2(u-l)a}+p^{2(u-l)(a-1)}+p^{2(u-l)(a-2)+1}} = \sigma_{\delta}$

Suppose $i = p^{2(u-l)a} + p^{2(u-l)(a-1)} + i_0$ for $1 \leq i_0 \leq p^{(2u-2l)(a-2)}$

Then $ip^{2(u-l)} \ mod \ n$

$\left(p^{2(u-l)a} + p^{2(u-l)(a-1)} + i_0\right)p^{2(u-l)} \ mod \ n$

$1 + p^{2(u-l)a} + i_0 p^{2(u-l)}$

$< p^{2(u-l)a} + p^{2(u-l)(a-1)} + 1$

The desired result then follows (4)

If a=2 the proof is completed now if $a \geq 4$

The process will be same proceed until we will prove that the set $(\delta\ , \delta + 1\ , \delta + 2 \ldots \ldots \delta_{D-1})$

Contains in σ_{δ}

The proof is obvious the p –cyclotomic coset modulo n containing δ_D is given as

$C_{\delta_D} = \left\{p^j \delta_D : \quad 0 \leq j \leq 2(u-l) - 1\right\}$

Clearly δ_D could be the coset leader of C_{δ_D}

Hence $\delta_D = \delta_B$ and we are done.

Sub case 2: when $1 \leq b \leq 2(u-l)$

As $l > \frac{u}{2}$ we have $a \geq 2$ and $l = 2a(u-l) + b$

Therefore $\delta_D = p^{2a(u-l)+b} + p^{2(u-l)(a-1)+b} + \cdots p^{2a(u-l)+b} + p^b + 1$

We will prove in this sub case that $\delta_B = \delta_D$

For this we will prove that every integer j with condition $\delta \leq j \leq \delta_B - 1$ contains in δ_D

$\delta = p^{2l} + 1$

$= p^{2(2u-2l)a+2b} + 1$ and

$\delta p^{2(u-l)} \ mod \ n$

$= (p^{2l} + 1)p^{2(u-l)} \ mod \ n$

$= 1 + p^{2(u-l)}$

$< \delta$

This follows that $\delta \in \delta_D$ and $\delta_{D+1} = \delta_D$ (5)

Now we wish to prove that $\sigma_{p^{2(u-l)a+b}+p^{2(u-l)(a-1)+b++1}} = \sigma_{\delta}$ (6)

Suppose $i = p^{2(u-l)a+b} + i_0$ for $1 \leq i_0 \leq p^{(2u-2l)(a-1)+b}$

Then $ip^{2(u-l)}\ mod\ n$

$\left(p^{2(u-l)a+b}+i_0\right)p^{2(u-l)}\ mod\ n$

$1+i_0\ p^{2(u-l)}$

$\leq \delta$

The desired result then follows (5)

If a=2 the proof is completed for sub case 2 now if $a \geq 3$

We will prove that $\sigma_{p^{2(u-l)a+b}+p^{2(u-l)(a-1)+b}+p^{2(u-l)(a-2)+b++1}} = \sigma_\delta$

Suppose $i = p^{2(u-l)a+b} + p^{2(u-l)(a-1)+b} + i_0$ for $1 \leq i_0 \leq p^{(2u-2l)(a-2)+b}$

Then $ip^{2(u-l)}\ mod\ n$

$\left(p^{2(u-l)a+b} + p^{2(u-l)(a-1)+b} + i_0\right)p^{2(u-l)}\ mod\ n$

$1 + p^{2(u-l)a+b} + i_0 p^{2(u-l)}$

$< p^{2(u-l)a+b} + p^{2(u-l)(a-1)+b} + 1$

The desired result then follows (6)

If a=2 the proof is completed now if $a \geq 4$

The process will be same proceed until we will prove that the set $(\delta\ ,\delta+1\ ,\delta+2\ \ldots\ldots\ \delta_{D-1})$

Contains in σ_δ

The proof is obvious the p –cyclotomic coset modulo n containing δ_D is given as

$C_{\delta_D} = \{p^j\delta_D :\quad 0 \leq j \leq 2(u-l)+b-1\}$

Clearly δ_D could be the coset leader of C_{δ_D}

Hence $\delta_D = \delta_B$ and we are done.

IV Conclusions

The main purpose of the work is to calculate dimension and Bose distance of Non binary BCH code with design distance$\delta = p^{2l} + 1$. A new proposed class of Non binary BCH code give arises to some other research problems. We will work in our next paper on the Bose distance of the dual of the proposed BCH code.

Conflict of Interests

The authors declare that there is no conflict of interests.

REFERENCES:

[1] Cun Sheng Ding and Zhengchun Zhou: The BOSE and Minimum distance of class of BCH code, IEEE Trans. vol.61, no 5,2015.

[2] P.Charpin ‘ open problems on cyclic codes’ IEEE Trans. Vol 1, W.C Huffman and VERA press. 1998.

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

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