International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

Construction of Upper Bound of Minimum Weight of An Even Formally Self Dual Code Over GF(4)

Dr. Mary Jansi Rani[1], J. Princivishvamalar[2], K. Abinaya Priya[3]

[1] Head and Assistant Professor, Department of Mathematics, Thanthai Hans Roever College, Perambalur

[2, 3] Research Associate, Thanthai Hans Roever College , Perambalur

Abstract: ***In this correspondence, we have constructed an upper bound of minimum weight of an even formally self dual code over GF(4). We have related the properties of self dual codes over GF(4) and discussed to isolate two classes of codes for which the minimum distance d ≤ 2[n/6]. They have established that the minimum weight of an even formally self dual code of length n satisfies d ≤ 2[n / 6]+2 except for the cases n = 12 and n = 14.***

Keywords: Minimum distance, Upper bound, Self dual codes, Formally self dual codes, Weight enumerator, External weight enumerator

1. Introduction

Self dual codes are important for a number of practical and theoretical reason [1,6,7,9,20-26,28,30 ,32]. These codes are of greatest interest when the weight of the code words are divisible by constant. A theorem of Gleasam, Pierce and Turyn [3 ,4 ,36] says that for except for certain trivial codes with minimum distance 2, there are only three cases in which a self dual or formally self dual code over a field GF(q) can have all weights divisible by a constant c > 1 namely ,

a) q = 2 , c = 2 or 4
b) q = 3 , c= 3
c) q = 4 , c =2.

(a) and (b) have been considered in several papers.(c) is discussed exhaustively in P.J.Macwilliams , Am odyzko , NJA Sloane and 1+N Ward [2]. In the present paper we consider to isolate two classes of codes for which the minimum distance d ≤ 2[n/6].

2. Preliminaries

A linear code of length n over GF(4) is a K- dimensional subspace of $\mathbb{F}_4^n$ where $\mathbb{F}_4$ is a field of 4 elements 0 ,1 ,α ,β with $\beta = \alpha^2 = \alpha+1$, $\alpha^3 = \beta^3 = 1$. A linear code c over a $\mathbb{F}_4$ of length n consists of 4^K vectors $\vec{u} = (u_1 ,u_2 ,u_3 , . ..u_n)$, $u_i \in \mathbb{F}_4$ i=1,2……n for $\vec{u} ,\vec{v} \in C$, $\vec{u} + \vec{v} \in C$ and $f\vec{u} \in C$ where $f \in \mathbb{F}_4$. The minimum weight of C is

d= min{ wt ($\vec{u}$) , $\vec{u} \neq \vec{0}$, $\vec{u} \in C$ }

We recall that the weight of $\vec{u}$ written wt ($\vec{u}$) is the number of non zero T $\vec{u} \cdot \vec{v} = \sum_{i=1}^{n} u_i v_i$, the sum evaluated in $\mathbb{F}_4$.

The dual code $C^{\perp}$ of C is given by

$C^{\perp} = \{ \vec{v} \in \mathbb{F}_4^n ,\ \vec{u} . \vec{v} = 0$ for all $\vec{u} \in C\}$

If C is an [n , k , d] code $C^{\perp}$ is an [n , n-k , d^1] code where $d^1 \neq d$ in general.

The conjugate of t $\in \mathbb{F}_4$ is denoted by $\bar{t}$ and $\bar{t} = t^2$, $\vec{\bar{u}} = \{ \bar{u}_1, \bar{u}_2,……. \bar{u}_n \}$.

$\bar{C} = \{ \vec{\bar{u}} ; \vec{u} \in C \}$

The concatenation of two vectors $\vec{u}$ and $\vec{v}$ is the vector

$|\vec{u}|\vec{v}| = (u_1 ,u_2 ,u_3 , ...u_n ,v_1 ,v_2 ,v_3. ... v_n)$.

Let C and D be two linear codes of dimensions k_1 and k_2 respectively over $\mathbb{F}_4$.

The direct sum C ⨁ D of C and D is given by

$C \oplus D = \{ |\vec{u}|\vec{v}| ; \vec{u} \in C , \vec{v} \in D \}$.

If b = C ⨁ D where C ≠ φ , D ≠ φ then b is called a decomposable code Otherwise it is indecomposable.

If C is an $[n_1 , k_1 , d_1]$ code and D is an $[n_2 , k_2 , d_2]$ code over $\mathbb{F}_4$ then b = C ⨁ D is an $[n_1+n_2 , k_1+k_2 , \min(d_1,d_2)]$code.

Definition 2.1 Let A_i denote the number of code words of weight I in C. The weight enumerate of C is given by

$W_c(x,y) = \sum_{i=0}^{n} A_i x^{n-i} y^i$

Definition 2.2 The complete weight enumerator of C is the polynomial, $CWC_c(x,y,z,t) = \sum_{i,j,k,l} A_{i,j,k,l}\, x^i y^j z^k t^l$

where $A_{i,j,k,l}$ is the number of code words in C containing i 0’s and j 1’s k α ’s and l β ’s it is observed that

$CWC_c (x , y , y , y) = W_c (x , y)$

A linear code C is called even if all the codes have even weight. C is called formally self-dual if C and $C^{\perp}$ have the same weight enumerator

$W_c (x , y)$.

C is said to be weakly self-dual if $C \subset C^{\perp}$, C is called strictly self-dual if $C= C^{\perp}$.

3. Weight Enumerator of an Even Formally Self Dual Code

We can write the enumerator of an even formally self dual code in a particular form. As any positive integer is in one forms 3m , 3m+1 or 3m+2. We take n = 2 (3m+v) where v = 0, 1 or 2 then

$W_c(x,y)=\sum_{i=0}^{m} a_i \eta_2^{n/2-3i}\theta_6^{i}$.........(1) for suitable coefficients a_i which are rational numbers .

In (1) we can choose a_1 , a_2 , …… a_m are chosen that a_1 , a_2 , …… a_{2m} , a_{2m+1} are zero as also a_{2m+3} , a_{2m+5} ,…… a_{3m} and a_{3m+2} are zero if m is odd and 3m+1 , 3m-1 ,……are zero if m is even. So we can rewrite (1) as

$x^n + 0.x^{n-1} y +\ldots\ldots + 0.x^{n-2m-1} y^{2m+1} + A_{m+2} x^{n-2m-2} y^{2m+2} + A_{2m+4} x^{n-2m-4} y^{2m+4} + \ldots\ldots = \eta_n$(say) -----------(2)

The values of a_i (= 0 or otherwise) can be determined uniquely using η_2 and θ_6.

Definition 3.1 Let η_n given in (2) is called the external weight enumerator. If $A^*_{2m+2} \neq 0$ then C has minimum weight $\leq$ 2m+2 . If C has minimum weight = 2m+2 . Then equation (2) we have $W_c (x , y) = \eta_n$

$2m+2 = 2[\frac{n}{6}] +2$

Where $\lfloor x \rfloor$ denotes the greatest integer not greater than x for $x \in \mathbb{R}$.

For n=12, the even formally self dual code denoted by E_{12} has minimum weight 4 = 2[n/6] < 2[n/6] + 2.

Theorem 3.1 For an even formally self dual code [n, n/d, d] if d < 2[n/6] + 2 then d $\leq$ 2[n/6].

Proof If d < 2[n/6] + 2 then

d/2 < [n/6] + 1 (or)

d/2 $\leq$ [n/6] $\Rightarrow$ d $\leq$ 2[n/6].

Remark The upper bound is reached in the case of a [12, 6, 4] code it is known [1]

Fact 1 In (4) A^*_{2m+4} is negative for n $\geq$ 102 , if n = 6m and A^*_{2m+4} is negative for n $\geq$ 122 if n = 6m+1. Further A^*_{2m+4} is negative for n $\geq$ 122 if n = 6m+2. So ,there is no code has weight enumerator η_n for these values of n.

Fact 2 Let b be any constant , suppose that a_i in (1) are chosen that ,

$X^n + A_d x^{n-d} y^d + A_{d+2} x^{n-d-2} y^{d+2} + \ldots\ldots$ Where d $\geq$ 2[n/6] + 2 -2b. Then one of the coefficients A_d , A_{d+2} …….. is negative for all sufficiently large n ,$\eta_{12} = x^{12} + 3y^{12}$

There is no linear code with weight enumerator η_{12} .However if

$W_c (x, y) = \eta_{12} + A_6\theta_6^2$

W_c (x, y) is the weight enumerator of a code of length 12. W = $\eta_{14} + A_4 \eta_2 \theta_6^2$ is the weight enumerator of a code of length 14. A_4 is the number of code words of minimum weight 4.

4. Construction of Code

Let C_i be an [n_i, k_i, d_i] q-ary linear code with generator matrix G_i i=1,2.If $n_1 = k_2$, then we can combine these two code to get another new code. We assume that $k_1 > k_2$.

If $n_1 = k_2$ and $n_2 > n_1$, then C_1 is an [n_1 , k_1 , d_1] code and C_2 is an [n_2 , n_1 , d_2] Code. Let as take

$G_1 = [\, I_{k_1} \,|\, A_1 \,]$ and $G_2 = [\, I_{n_1} \,|\, A_2 \,]$ where A_1 is $k_1 \times (n_1 - k_1)$ matrix and A_2 is $n_1 \times (n_2 - n_1)$ matrix. Since $n_2 > n_1$ implies $n_2 - n_1 > 0$.

Let G = G_1G_2, then G = G_1G_2 = $[\, I_{k_1} \,|\, A_1 \,]\ [I_{n_1} | A_2\,]$ = $[I_{k_1} \,|\, A_1 \,|\, GA_2\,]$

Clearly all rows of G are linearly independent and hence G generates an [n_2 , k_1 , d] q- ary linear code. Since G = [$G_1 \,|\, G_1A_2$] and G_1A_2 is an

$k_1 \times (n_2 - n_1)$ matrix, therefore $d_1 \leq d \leq d_1 + n_2 - n_1$.

Theorem 4.1 Let C_i be an [n_i , k_i , d_i] i = 1 , 2 q-ary linear code. If $n_1 = k_2$ and $n_2 > n_1$, then there exits an [n_2 , k_1 , d] q-ary code such that $d_1 \leq d \leq d_1 + n_2 - n_1$.

Let C_1 be an [n , k , d] q-ary linear code with generator matrix G_1 and let G_2 be an [n + 1, n, 2] q-ary linear code with generator matrix G_2. Without loss of generality, we can take G_2 as

$$\left[\begin{array}{c|c} I_n & \begin{matrix}1\\ \vdots \\ 1\end{matrix}\end{array}\right]$$

Then G = G_1G_2 is a $K \times n + 1$ matrix , This implies

$$G=G_1\left[\begin{array}{c|c} I_n & \begin{matrix}1\\ \vdots \\ 1\end{matrix}\end{array}\right] \quad G = \left[\, G_1 I_n \,\middle|\, G_1 \begin{pmatrix}1\\ \vdots \\ 1\end{pmatrix} \right]$$

This implies G generators an [n+1, k, d] code C and the minimum distance d(C) must be greater than or equal to d.

Since $G_1\begin{pmatrix}1\\ \vdots \\ 1\end{pmatrix}$ is $k \times 1$ column matrix , therefore d(C) is either d or d+1.

References

[1] E.R.BerlekampP.J.Macwilliams and NJA Sloane , Gleasar's theorem an self-dual codes IEEE Trans , Information Theory 18[1972]409-414.
[2] E.R.Berelekamp[1968] Algebraic coding theory,Mcgraw-Hill Newyork.
[3] J.H.Canway and V.Pless, on the enumeration of self-dual codes, J.combinatorial theory series A 28 [1980], 26-53 see [12] for errata.
[4] P.J.Macwillioms, A.M.Odlyzko, NJA Sloane and HN Ward – self - dual codes over GF [4] J.combinatorial theoryseriesA 25 [1978] pp 288-318.
[5] C.Huffman,V.Pless, Fundamentals of error correcting codes, Cambridge university press, Indian Edn [2004].
[6] P.J. Macwilliams and NJA Solane, the theory of error - correcting codes, North-Holland Amsterdam, 1977.
[7] F.J.Macwilliams, C.L.Mallows and NJA Solane,generalizations of Gleasors theorem or weight enumerators of self-dual codes, IEEE Trans. Information theory, 18[1972], 794-805.