VOL. 10, NO. 9, MAY 2015 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences

www.arpnjournals.com

ON A POSSIBLE CHARATARIZATION OF A q-ARY LINEAR MDS CODE OF LENGTH n

M. Mary JansiRani[1] and K. Prabhakaran[2]
[1]Department of Mathematics, Thanthai Hans Roever College, India
[2]Thanthai Hans Roever College, India
E-Mail: ersakthi@yahoo.com

ABSTRACT

Let$\mathbb{F}_q$ be a finite field having q – elements (q= p^m, p is a prime, m≥ 1) by a linear [n, k, d] code. We mean a subspace of the vector space if q^n having dimension k and minimum distance d denoting this code by C we analyse certain sub-codes of C. The inequality d$\leq$n-k+1is obtained via a sub-code of dimension (k-1) in which the left- most coordinate position of each of its code words is zero. Under suitable circumstances, it is possible that d$\geq$n-k+1.A q-ary linear code of length n, dimension k and having minimum distance d is said to be a mean distance separable code if d=n-k+1 writing a mean distance separable code as an MDS code, we obtain a possible characterisation of an MDS code. A equivalence relation of the set of code words of a q-ary [n, k, d] code suggests an algorithm for finding the minimum distance of an [n, k, d] code.

Keywords: MDS code, minimum distance, subcode, equivalence relation.

1. INTRODUCTION

If q denotes a finite field having q elements where q= p^m , p is a prime; m$\geq$1. Let d$\geq$1, n$\geq$1 then If q^n is defined by If q^n= {($c_0, c_1, \ldots c_{n-1}$) $c_i \in \mathbb{F}_q$ i= 0, 1, 2,…n-1} If q^n is a vector space of dimension n over $\mathbb{F}_q$.

Definition 1.1 An [n,k]linear code C characteristic of an encoding E: $F_{q^k} \rightarrow F_{q^n}$

Definition 1.2 The weight w ($\vec{c}$) of a code word $\vec{c}$ is given by w($\vec{c}$) = the number of non-zero coordinate positions of $\vec{c} = c_0, c_1, \ldots c_{n-1}$ $c_i \in \mathbb{F}_q$ i= 0, 1, 2,…n-1.

Definition 1.3 Let $\vec{x}$, $\vec{y}$ be vectors in $\mathbb{F}_q$ the Hamming distance d($\vec{x}$, $\vec{y}$) between $\vec{x}$ & $\vec{y}$ is defined as the number of coordinate positions in $\vec{x}$ & $\vec{y}$ which differ.It is known [2] thatd($\vec{x}$, $\vec{y}$) denoting the distance between $\vec{x}$ and $\vec{y}$ gives a function .

Definition 1.4 The minimum distance of a linear code C is the smallest distance between distinct code words of C.

The minimum distance d of a linear code is also the minimum weight of non-zero code words of C. That is d= min {w ($\vec{c}$), $\vec{C} \neq \vec{o}$, $\vec{C} \in$ C}. when q= 3, a linear code over $\mathbb{F}_3$ is called a ternary code.

2. OBSERVATION

A linear [n,k] code C has minimum distance d if and only if its parity check matrix H has a set of d linearly dependent columns but no set of d-1 linearly dependant columns. For any set of k independent columns of a generator matrix G, the corresponding set of coordinates forms an information set for the code C represented by G. The remaining (n-k) coordinates are made a redundancy set in [2].

The generator matrix G of an [n,k] code is a matrix whose rows are linearly independent and span the code. The rows of the parity check matrix H are linearly independent. Hence H is the generator matrix of a different code called the dual of C denoted by $C^{\perp}$. $C^{\perp}$ is an [n,n – k] code.

Definition: 1.5 A linear [n,k] code C is called self-orthogonal if C$\subseteq C^{\perp}$ if C=$C^{\perp}$, C is called a self-dual code.

Definition 1.6 Let C be a linear code of dimension k over F_q . A Subset T of C which also forms a vector space by itself over $\mathbb{F}_q$ is a subspace of C. T is called a sub code of C.

If T is non trivial, 1$\leq$ dim T $\leq$ dim C (or) 1 $\leq$ dim T $\leq$ k.

Definition 1.7 A linear code of length n over $\mathbb{F}_q$ and minimum distance atleast d is called optimal if it has B_q (n, d) code words, where

B_q (n,d) is the largest number of code words in C.

There are other ways of optimizing a linear code C they are

1) To find d_q (n,k) the largest value of d for which there exist a linear [n,k ,d] code over $\mathbb{F}_q$.
2) To find n_q (k,d) the smallest value of n for which there exists a linear [n,k ,d] code over $\mathbb{F}_q$.

The purpose of this note is

- To analysis the native of the minimum distance a of an [n, k, d] code C via certain specific sub code C.

- To obtain certain a possible characterization of a q-arylinear M D S code.

3. SOME INEQUALITIES INVOLVING d

As mentioned earlier, a linear code C of length n over $\mathbb{F}_q$ is a subspace of dimension k over. As q= p^m (p is a prime, m ≥1) q^n is also a prime power namely p^{mn}. If q^n has q^n elements which are vectors of the form $\vec{a} = (a_0, a_1, \ldots\ldots a_{n-1})$

(F_{q^n},+) is an abelian group of order p^{mn}.

SYLOW'S first theorem [1]

Let G be a group of order $p^s t$ where s≥1 and Gcd (p,t)=1 then G contains a subgroup of order p^j for each j such that 1 ≤ j ≤ s and evens subgroup of G of order p^j (1 ≤ j ≤ mn) is normal in same subgroup of order p^{j+1}.

According (F_{q^n}, +) has subgroups C_j whose orders are q^j (1 ≤ j ≤ k) and $q^j = p^{mj}$ where q= p^m (p is a prime, m ≥ 1).

Definition 2.1 Let C be a q-ary code of length n. The code words $\vec{c}$ of C are n-tuples of the form $\vec{c} = c_0, c_1, \ldots c_{n-1}; c_i \in C_j$ i= 0,1,2,…n-1. $\vec{c}$ -is said to be an (i-0) vector if the coordination at i^{th} place of $\vec{c}$ is o∈ F_q.

Theorem 2.2 Given a q-ary linear [n, k, d] code the sub-code c_0={ $\vec{c} = c_0, c_1, \ldots c_{n-1}; c_i \in \mathrm{F}_q$ i= 0, 1, 2,… n-1} forms as [n,k-1,d] code, whose d^1∈d further, the quotient space C/C_0 is isomorphic to $\mathbb{F}_q$.

Proof: we take the subset T of the coordinates 0,1,2,…n-1to be T ={0} at coordinates position o. then C(T) is the set of code words having 0 at the left most position C(T) is a sub code of C of dimension (k-1).

Next, let T be the set of coordinate positions where a minimum weight code has zeros. There are (n-d) elements in T. The set of code words which are zero in T is a subcode of C. It is denoted by C(T) sub code has (n-d) zeros is specified coordinate positions, C (T) has dimension k-(n-d) or K-n+d. As the dimension of a non-trivial code is k-n+d ≥ 1 or d ≥ n – k+1.

Remark 2.3 we denote by n_q(k, d) the least value of n for which there exists an [n, k, d] code over $\mathbb{F}_q$.

Suppose that [x] denote the smallest integer not smaller that X.

The Griesmer bound for n_q(k, d) says [1] that n_q(k,d) ≥ d+$\frac{d}{q} + \frac{d}{q^2} + \ldots + \frac{d}{q^{k-1}}$ the right side of this equation is denoted by g_q(n,d).The singleton bound states that for any linear [n,k,d]-code over $\mathbb{F}_q$, d ≤ n – k+1 codes with d = n-k+1 is called maximum distance separable codes or MDS codes. If d ≤ n – k+1 => n ≥ d+k-1 in [3] the singleton bound is a weak form of Griesmer bound. As mentioned in [2] as $\frac{d}{q}, \frac{d}{q^2}, \ldots, \frac{d}{q^{k-1}}$ are each for d ≤ k, we get form (2) n_q(k,d) = d+1+…+1(k-1) times = d+k-1. So Griesmer bound is obtained for d ≤ q. It is known that when k = 1, the MDS codes are the [n, 1, n] repetition codes, when q ≤ k when k ≥ q, the only MDS codes are trivial [k, k, 1] codes or [k+1, k, 2] codes. So we consider k>1 and
2 ≤ k ≤ q-1.

Theorem 2.4 Let C be an [n,k,d] code over $\mathbb{F}_q$ then C is an MDS code if and only if C has a sub code C_T of dimension 1 with the following property.

If T is a set of coordinate position say $\{i_1, i_2, \ldots, i_{n-\alpha}\}$ and C_T is a code shortened at it is assumed that 2 ≤ k ≤ q-1.

Proof: As d is the minimum distance of the code there exists a code word having zeros at (n-d) coordinate positions designated by T= {$\mathbb{F}_q$} by defined C(T) is the set of code words of C which are o on T puncturing C(T) on T gives a code of length n-(n-d)=d called the code shortened at T this code is denoted by C_T. If C is an MDS code, d= n-k+1 , C_T is of length d by extending theorem 2.2 if each code word of a code C of length n has n-d zeros at coordinate positions $i_1, i_2, \ldots, i_{n-d}$ dimension of this code is k-(n-d)=k-n+d. when k-n+d=1, k=n-k+1 when C has a sub code of dimension 1 obtained by taking the set of code words of minimum distance d d = n-k+1 or C is an MDS code. Conversely, if C has a sub code C_T containing the code words of C having non distance d and C_T has dimension 1, then k-(n-d)=1 or
d = n-k+1 thus C is an MDS code.

Example 2.5 We consider a code C for which n=4, k=2, d=3 and q=3.
d =n-k+1 = 3 (4-2+1) then [4, 2, 3] over $\mathbb{F}_q$ is given by
0000 11α0 α10α
0111 $\alpha\alpha$10 α0α1

ARPN Journal of Engineering and Applied Sciences

where α^2=1, 0α α α 1α 01101α α+1=0, 1+1=α it is an MDS code, also hence d=q

c_0= {0000, 0111, oα α α } is a sub code of c drawn from the set of code words of weight 3. c_0 is a sub code of C.

4. ANEQUIVALENCE RELATTON

Form sylows theorem it is possible to obtain an [n, k-1] q-ary sub-code of a q-ary code of length n and dimension k.

Definition 3.1 Let C be a q-ary linear code of length n (n ≥ 2) and of dimension k. A code words $\vec{c} = c_0c_1c_2...c_{n-1}, c_i \in \mathrm{F}_q$ is said to have left-most coordinate position $c_0 \in \mathrm{F}_q$.

Definition 3.2 Let $\vec{a} = a_0a_1...a_{n+1}, \vec{b} = b_0b_1...b_{n-1}$ be two code words in C $\vec{a}\,\&\,\vec{b}$ are said to be equivalent if and only if, $\vec{a}$ and $\vec{b}$ agree as equality on the left most coordinate position.

Let C be a q-ary code of length n and of dimension k. the equivalence relation defined on the set-up C as in definition 3.2. Partition C into q-equivalence classes [0], [1], [α]……....[α^{q-2}] Where [α^i], i= (0, 1, 2,…q-2) denotes the equivalence class of code words having the left-most coordinate position [α^i] and [0] denotes the class of code of code words having left most coordinate position 0. Theorem, says that [0] is nothing but the sub code c_0 of C and having dimension k-1.Further, [1], [α]… [α^{q-2}] are co-sets of [0] in C.

Definition 3.3 In a q-ary code of length n, a code word $\vec{c} = c_0c_1c_2...c_{n-1}$ is said to be even like, if $\sum_{i=0}^{n-1} C_i = C_0 + C_1 + ... + C_{n-1}$ =0Otherwise $\vec{C}$ is said to be odd-like.

Even like code words in C form a sub-code ofC over $\mathbb{F}_q$ as also even weight vectors in a binary code.

Example 3.4 C_1= {0000, 0111, 0ααα, 11α0, α10α, 1α01, 101α, αα10, α0α1}

Let E= {0000, 0111, 0ααα} C_1 is a [4, 2, 3] ternery code q=3, $\mathbb{F}_q$ = {0, 1, α} with 1+α = 0, α^2 = 1. E is a sub code of C_1 of dimension l, E consists of evenlike code words of C.

E is a [4, 1, 3] linear code.

$$C/E = \{[E], [E+11\alpha 0], [E+\alpha 10\alpha]\}$$

Let E_1 = [E+11α0] = {[11α0, 1α01, 101α]}

E_2 = [E+α10α] = {α10α, αα10, α0α1}

We get a partition of C into 3 classes and C_1 = $E_1 \cup E_2 \cup E_3$

The partitioning of a code into equivalence classes gives a method of finding the minimum weight of a code C. Since a $\vec{V}\varepsilon C$ for $\vec{V}\varepsilon C$ where a$\mathbb{F}_q$ we note that weight (a$\vec{v}$) = weight of $\vec{v}$. Suppose the class [0] contains code words having minimum weight d_0 we can find the minimum weight of a code word contained in the equivalence class [1], say d_1.But then, d_1 will be the minimum weight of a code word in [α],$\left[\alpha^2\right]$,...,$\left[\alpha^{q-2}\right]$, so we do not have to search for minimum weight code words in all the code-words of C, instead we have only to look for minimum weight That is minimum weight d of a code word=min { d_0, d_1 }. This suggests that we can develop an algorithm for finding minimum weight of a code.

REFERENCES

[1] N. Pendins Topics in algebra vikas pub. House 4th printing 1985 chapter 4, pp.130-143.

[2] C. huffman and Verapless. Fundamental of error – correcting codes Cambridge university press, 2004, chap 1, pp. 2- 47.

[3] R. Hill. optimal linear codes a survey article, 1986.

[4] P.P Greenough and R. Hill optimal linear codes over G F [4], Salfood M 5 4WT England.

[5] J.H. Griesmer .A bound for error -correcting codes I BM J. res develop, vol. 4 pp. 532-542, 1960.

[6] V.N .Logavec an improvement of the Griesmer bound in the case of Small code distance optimization methods and thus Application {Russia}, sibirsk, Energetinstsibirskotdel. akad Nauk SSSR, irkutsk, pp 107,111, 182, 1974.

[7] H.C.A. Vantilborg On the uniqueness of existence of certain codes meeting the various bound, inform centre vol. 44, pp. 16-35, 1980.

[8] F J. Macwlliams and N.J.A sloane the theory of error correcting Codes vol-16 Amsterdam: north Holland SS, 1977.