International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

A Note on a Subcode of a Linear Q – Ary Code of Length N and an Algorithm for Calculating Minimum Distance

Dr. M. Mary Jansi Rani [1], M.Manikandan[2]

[1, 2]Thanthai Hans Roever College, Perambalur, India

Abstract: ***This Paper Deals with The Calculation Of Minimum Distance Of A Q-Ary Linear Code Of Length N. The Set Of Code Words Having The Left Most Coordinate Position O Forms A Subcode. If C Is An [N, K, D] Code, The Subcode Co So Considered Is Of Dimensions K-1. The Coset Leaders In C/Co Give The Method Calculating Minimum Distance. The Method Does Not Make Use Of The Known Techniques Using A Parity Check Matrix H. In Phillipe Delsarte "Four Fundamental Parameters Of A Code And Their Combinatorial Significance, Information And Control 23, 407 – 438 (1973), The Inner Product Of Two Vectors A And B In*** F_q^n ***Is Considered Using Group Characters Of A Finite Abelian Group (F, +) Of Order Q Over*** Γ***, The Cyclotomic Field Of Complex V[th] Roots Of Unity. The Dual Code Is Defined Via The Inner Product <A, B> Of A, B*** $\in F^N$***, If Reduces To The Classical Concept For Linear Codes Over Finite Fields. However, If A = A0 A1 .... An,*** $B = B_0 B_1 \ldots B_{n-1} \in F_q^n$***. The Inner Product A, B =*** $\sum_{i=0}^{n-1} ai\ bi$ ***Could Be Interpreted Using A Cyclotomic Extension*** $F_q(\xi)$ ***Of*** F_q ***Via Trace Of An Element In*** $F_q(\xi)$***. This Give Get Another Interpretation Of The Inner Product A. B.***

Keywords: Cyclotomic Cosets, Minimum Distance, Co Ordinate Position, Coset Leader, Subcode, Inner Product.

1. Introduction

In [1], Phillipe Delsarte Give An Interesting Account Of The Form Fundamental Parameters Of A Code (Linear Or Not) And Their Combinatorial Significance. While Discussing The Distance Distribution (Which Reduces To Weight Distribution In The Case Of A Linear Code) Of An [N, M] Code $1 \le M \le Q^n$ The Author Introduces An Inner Product Of Vectors In F^n Where F Is A Finite Abelian Group Of Order $Q \ge 2$, Via A Group Character ψ Of F Over $\Gamma\gamma$, The Cyclotomic Field Of Complex V^{th} Roots Of Unity. The Inner Product <A, B> Of N-Tuples $A = (A_0\ A_1 \ldots A_{n-1})$, $B = (B_0\ B_1 \ldots B_{n-1})$ Is Given Interms Of ψ. When The Additive Code C Is A Subgroup Of F^n, The Dual Code C^1 Is Also An Additive Code And Is Defined By,

$$C^1 = \{a \in F^n (a, b) = 1 \quad \text{for all } b \in F^n\}$$

This Duality Is An Involution (In The Sense That $(E^1)' = C$) And C^1 Is Such That C^1 Is Isomorphic To The Quotient Group $\frac{F^n}{C}$. That Is $C^1 \cong \frac{F^n}{C}$ As Mentioned In [1] The Definition Of C^1 Agrees With The Classical Concept Over Finite Fields. Moreover, For Every A, B, C $\in F^N$ One Has (A, B +C) = (A, B) (A, C) More Over, Any Character Of (F^n, T) Can Be Represented In This Manner.

As We Are Handling A Finite Field F_q, It Will Be Nice If We Arrive At An Inner Product Using The Field Structure Of F_q, Instead Of The Character ψ Of A Finite Abelian Group. The Following Approach To An Inner Product Via A Cyclotomic Extension Of A Finite Field Agrees With The Known Definition Of An Inner Product Of Vectors $A = (A_0\ A \ldots A_{n-1})$, $B = (B_0\ B_1 \ldots B_{n-1})$ Belonging To F_q^n .Details Are Given In 1 Preliminary. The Aim Of This Note Is To Propose An Algorithm For The Calculation Of The Minimum Weight Of A Q-Ary Linear Code C Using Partition Of The Set Of Code Words Of C. The Method, Believed To Be New, Does Not Make Use Of The Known Techniques Using A Parity Check Matrix H. A New Interpretation Of The Inner Product Of Vectors A And B In F_q^n Is Also Investigated.

2. Preliminaries

Definition: 1.1 The Trace T $(A_1a_2 \ldots A_n)$ Of $(A_1a_2 \ldots A_n)$ Is Defined To Be

$$T(A_0a_1 \ldots A_{n-1}) = \sum_{i=0}^{n-1} T(ai)$$

$$= N(A_0 + A_1 + A_{n-1})$$

Example: 1

If F4 = {0, 1, α ,β} 1 + 1 = α, 1 + α = β Etc.

T (β 0 α αβ) Where $\beta 0\ \alpha\ \alpha\beta \in F_4^5$ Is Given By

$$T(\beta\ 0\ \alpha\ \alpha\beta) = 5(\beta + \alpha + \alpha + \beta)$$
$$= 5(\alpha + \beta + \alpha + \beta)$$
$$= 5(\alpha + \alpha^2 + \alpha + \alpha^2)$$
$$= 5(1 + \alpha + 1 + \alpha)$$
$$= 5 \times 0 = 0$$

This Makes Eligible For Defining The Inner Product (A, B) Of Vectors A, B $\in F_q^n$ As Follows.

Definition: 1.2 The Inner Product A, B Of A, B $\in F_q^n$ Is Given By

$$(A, B) = \frac{1}{n^2}\sum_{i=0}^{n-1} T(ai)\ T(bi)$$

This Agrees With The Usual Inner Product Consider In The Context Of Q-Ary Linear Codes. For Each $A_i \in F_q$, $T(A_i) = N\ A_i$ (I = 0, 1, 2 .... N). It Is Obvious That This Is Not The Type Of Inner Product Considered Using Group Characters In Phillipe Del Sarte [1].

Let $[T_i]$ Be The Coset Of C Consisting Of All Vectors In F_q^n With Syndrome $\vec{ti}$. Suppose That A Code Word $\vec{y}$ Sent Over A Communication Channel Is Received As Vector. In Nearest Neighbour Decoding, We Find Out The Vector E Of Smallest Weight Such That T – E ∈ C. It Amounts To Finding A Vector E Of Smallest Weight In The Coset Containing R Such That R – E ∈ C Ie The Coset Leader Of Smallest Weight In The Coset Containing R. This Leads To 'Syndrome Decoding' Algorithm.

First Choose A Fixed Parity Check Matrix H.

Step: 1 For Each Syndrome T $\in F_q^{n-12}$ Choosen A Coset Leader E_t Of The Coset [T]. Create A Table Pairing The Syndrome With The Coset Leader.

Step:2 After Receiving A Vector R, Compute Its Syndrome S Using The Parity Check Matrix H.

Step:3 R Is Decoded As The Codeword R – E. For Details See Huffman And Pless [2]. Our Aim Is To Apply A Similar Techniques For Obtaining The Minimum Distanced Of A Q-Ary Code Of Length N .

2. Main Theorem In View Of Sylows First Theorem It Is Possible To Pick An [N, K-1] Q-Ary Sub Code Of A Q-Ary Code Of Length N And Dimension K.

Definition: 2.1 Let C Be A Q-Ary Code Of Length N (N ≥ 2) And Dimension K. A Code Words $C = C_0\ C_1 \ldots\ldots C_{n-1}$ (Where $C_i \in F_q$, I = 0, 1, 2 ... N-1) Is Said To Have The Left Mostcoordinatepositionl$_0$.

For Example: α 01 α β $\in F_4^5$ Has Left-Most Coordinate Position α, (O, 1, α, β) Denoting Elements Of F_4.

Definition: 2.2 Let $A = A_0\ A_1 \ldots A_{n-1}$, $B = B_0\ B_1 \ldots B_{n-1}$ Be Two Code Words In C (Of Dimension K) A And B Are Said To Be Equivalent. Written A ~ B, α If And Only If A And B Agree On The Left-Most Coordinate Position.

Theorem: 1 The Equivalence Class Of Code Words Having O In The Left-Most Coordinate Position Forms A Subcode C_o Of C And C_o Has Dimension K – 1 Over F_q.

Proof When Fq = $\{0,1,\alpha,\alpha^2 \ldots \alpha^{\varepsilon-2}\}$ Where α = Exp $\left(\frac{2\pi i}{q-1}\right)$ The Equivalence Relation Given In Definition 2.2 Partitions C Into Q Classes. In Fact $C \cong F_q^k$, Each Equivalence Class Contains Q^{k-1} Code Words. Since When The Left Most Coordinate Position Is Fixed, We Get Q Classes Due To The Partition. In Partition The Class [0] Has Q^{k-1} Elements Following The Addition Rule F_q, If $\overline{\alpha_0^i}$ = O $A_1\ A_2 \ldots A_{n-1}$ And B_0 = O $B_1\ B_2 \ldots B_{n-1}$, $A_0 + B_0 \in [0]$. Also When A Is In [0], -A Is Also In [0]. 0 = 0 0 0 .... ∈ [0].Therefore

([0], +) Is An Abelian Group Of Order q^{k-1}, For $\alpha^i \in F_q$, $\alpha^i A_0 = \alpha^i$ (0 $A_1\ A_2 \ldots A_{n-1}$)

$= \left(0\ a_1'\ a_2' \ldots a_{n+1}'\right)$ Where $a_j' = \alpha_J\ A_j \in F_q$.

So, [0] Is Closed Under Scalar Multiplication. Thus [0] Is A Subspace Of F_q^n And Its Dimension Is (K-1). For A Basis Of [0] Can Be Put In 1 – 1 Correspondence With The Basis Vectors Of A (K-1)-Dimensional Space. This Complets The Proof Of Theorem 1.

Definition: 2.3 We Define By C(T) The Set Of Codewords Of C For Which The Coordinates Are Zero An T. C(T) Is A Subcode Of C, That Is When

T = {1} In Theorem 1. Puncturing C(T) On T Gives A Code Of Length N – T Called The Code Shortened On T. If Is Denoted By C_T.

Example: 1 A Binary Code Of Length 7 And Having $2^3 = 8$ Code Words Is Given By,

G = 0 0 0 0 0 0 0 01 1 1 0 1 0 0
0 1 1 1 0 1 0 1 0 0 1 1 1 0
0 0 1 1 1 0 1 1 0 1 0 0 1 1
0 1 0 0 1 1 11 1 0 1 0 0 1

When T = {1},

C_1(T) = 0 0 0 0 0 0 0
0 1 1 1 0 1 0
0 1 0 0 1 1 1
0 0 1 1 1 0 1

It Is A Subcode Of C_1, C_1 (T) Has A Basis {0011101, 0100111}

$\frac{C1}{C1(T)} \cong \{0\ 0\ 0\ 0\ 0\ 0\ 0, 1\ 1\ 1\ 0\ 1\ 0\ 0\}$.

C_1 Is A Binary [7, 3. 4] Code Whereas C_1 (T) Is A [7, 2, 4] Subcode Of C_1.

Example: 2 A Ternary [4, 2, 3] Code Is A Linear Code Over $\mathbb{F}_3$ = {0, 1, 2} Where $2^2 \equiv$ (Mod 3). It Is Denoted By C_2 And Its Code Words Are

0 0 0 0 1 0 1 1 2 2 1 0
0 1 1 2 1 1 2 0 2 0 2 2
0 2 2 1 1 2 0 2 2 1 0 1

When T = {1},

$C_2\{T\} = 0\ 0\ 0\ 0, 0\ 1\ 1\ 2, 0\ 2\ 2\ 1$.

C_2(T) Is A Subcode Of C_2 And Having Dimension 1 As

0 1 1 2 + 0 1 1 2 = 0 2 2 1,
0 1 1 2 + 0 2 2 1 = 0 0 0 0.

$\frac{C_2}{C_2(T)} \cong \{0\ 0\ 0\ 0, 1\ 0\ 1\ 1, 2\ 0\ 2\ 2\}$

Let A_i Denote The Number Of Code Words Having Weight I In C_3. The Weight Enumerator Of C_3 Is The Polynomial

$$W(X, Y) = \sum_{i=0}^{6} Ai\ x^{6-i}\ y^{i} \quad \ldots\ldots(1)$$

Here, $A_0 = 1$, $A_1 = A_2 = 0$, $A_3 = 12$, $A_4 = 18$, $A_5 = 24$ And $A_6 = 9$ Substituting These Values In 1 We Obtain. $W(X, Y) = X^6 + 12x^3 Y^3 + 18 X^2 Y^4 + 24xy^5 + 9y^6$ We Observe That C_3 Is A [6, 3, 3] Quaternary Code.

Theorem: 2 Given A Q-Ary Code Of The Type [N, K, D] There Always Exists A Q-Ary [2n, K, D^1] Code With A Computable Minimum Distance d'.

Proof Let C Be A Q-Ary [N, K, D] Code, Suppose That Co Denotes The Subcode Of C Having Codewords In Which The Left Most Position O. By Theorem 1, Co Is An [N, K-1, D_0] Code Where $D_0 \leq D$. Then The Orthogonal Complement C/ Co Is An [N, 1, d_0'] Code Which Is Isomorphic To F_q. The Minimum Distance d_0' Is Computable. Then $C_0 \oplus C/C_0$ Is A [2n, (K-1)+1, D′] Code. Where

D′ = Min [D_o, d_0'] D′ Is Computable. Therefore Given A Q-Ary [N, K, D] Code, It Is Always Possible To Find A Q-Ary [2n, K, D′] Code With Computable D′.

Example When C Is A [6, 3, 3] Quaternary Code, C_0 Is A [6, 2, 3] Quaternary Code. C/ Co Is A [6, 1, 3] Quaternary Code. So Co $\oplus$ C/C_0 Is A [12, 3, 3] Quaternary Code.

3. An Algorithm To Find Minimum Weight Of An [N, K] Code

Theorem: 3 The Algorithm For Calculating The Minimum Weight D Of A Q-Ary [N, K] Code Of Length N Consists Of The Following Steps.

Step: 1 Determine The Subcode C_0 Of Dimension (K-1) Containing Codewords With Left Most Coordinates Position O, That Is Lies The Codewords In C_0 In A Row.

Step: 2 Determine The Coset Of C_0 By Writing [A] = [C_0 + A] Where A Will Serve As The Element Containing 1's And 0's For The Abelian Group Of Cosets Of C_0 Isomorphic To (F_q, +). List The Elements Of The Coset [A] In A Row.

Step: 3 Determine The Minimum Weight Do Of The Code Words In C_0.

Step: 4 Determine The Min Weight d_0' Of The Code Words In [α].

Step: 5 Determine The Minimum Of The Values D_0, d_0' Found Out In Steps 3 And 4. The Minimum Valued Gives The Minimum Weight D. (Or Minimum Distance D) Of The Code C.

Proof C_0 Is A Subspace Of Dimension K-1 Of The Code C. The Quotient Space C/C_0 Has Dimension And So It Is Isomorphic To F_q. For Non Zero Vector V $\in$ F_q^n If $\alpha \in F_q$ ($\alpha \neq 0$) Wt (αV) = Wt (V) And So We Have Only To Determine The Minimum Weights Code Word In C_0 And [α] . This Completes The Proof Of The Algorithm.

References

[1] Carry Huffman And Veva Pless:Fundamentals Of Errors –Correctingcodes, Cambridge Universitypress(2004)
[2] Chapter. 1 And 7 Sections 1.2, 1.4, 1.5 And Sections 7.1, 7.2, 7.3, 7.5 And 7.6. Pp. 2-18 And 252-272.
[3] T.W. Hungerford: Algebra, Holt, Rinchart And Winston Inc 1974.Chap. V, PP. 230 – 306.
[4] Hill. R (1986) A First Course In Coding Theory Oxford University Press.
[5] F.J.Mawilliams,A.M. Odlyzko, And N.J.A. Sloane : Self-Dual Codes Over GF(4)Journalofcombinatorial Theory, Series A25, 288-318 (1978).
[6] Phillipe Delsarte: Four Foundamental Parameters Of A Code And Their Combinatorial Significance Information & Control 23, 407 – 438 (1973).