

A Epistle on an Upper Bound for (n,d)

KHARVI SANDEEP¹

^{1,2}Asst Prof, Dept. of mathematics, Sai Vidya Institute of Technology, Karnataka, India.

How to cite this paper: KHARVI SANDEEP¹: A Epistle on an Upper Bound for (n,d), IJIRE-V2I05-10-11

Abstract: In this correspondence, we really want to get an upper bound for the value of (n,d), we have associated with the bounds on the number of code words in linear code C of length n. In particular we have given the exact in equality for (n,d).

Keywords: Minimum distance, upper bound, minimum Hamming distance, lower bound.

Copyright © 2021 by author(s) and 5th Dimension Research Publication
This work is licensed under the Creative Commons Attribution International License (CC BY 4.0).
<http://creativecommons.org/licenses/by/4.0/>

I. INTRODUCTION

Let F_q be a field having q parts, where $q = P^m$ (P a prime and m). A straight code C of perspective k is a subspace of the vector space F_q^n over F_q . C contains n elements which are n -tuples $(f_i, i=1 \text{ to } n)$ and elements. The elements of C are called code words of length n . The distance between two code words is define as follows.

First, the Hamming weight of a vector $\bar{u} = u_1, u_2, \dots, u_n$ is the number of non-zero u_i in \bar{u} written $wt(\bar{u})$. Secondly, the

Hamming distance between two vectors $\bar{u} = u_1, u_2, \dots, u_n$ and

$\bar{v} = v_1, v_2, \dots, v_n$ is the number of places where co-ordinates of \bar{u} and \bar{v} differ and it is denoted by $d(\bar{u}, \bar{v})$.

Evidently, $(F_q^n, +)$ is an abelian group with identity $\bar{0} = 0, 0, 0, \dots, 0$ and $- \bar{v} \in F_q^n$ and $wt(\bar{u} - \bar{v})$ is also well defined.

II. PRELIMINARY RESULTS

Where not given, Proofs or references for the results of this section may be found in section 2 of [7]

The Hamming weight of a vector \bar{u} denoted by $wt(\bar{u})$ is the number of non-zero entries in \bar{u} . For a linear code, the minimum distance is equal to the smallest of the weights of the non-zero code words. If C is an (n, k) code, we let A_i and B_i denoted the number of code words of weight i in C .

2.1 Definition

$$d = \min_{\bar{u} \neq \bar{v}} d(\bar{u}, \bar{v})$$

The minimum distance of the code is the minimum Hamming distance between its code words. That is,

It is known that the minimum distance of a linear code is the minimum weight of any non-zero code word.

2.2 Definition

A linear code of length n , dimension k , and minimum distance d is known as an $[n, k, d]$ code.

Bounds on the number of code words in a linear code C of length n , and minimum distance d having studied by various

Theorem2.3 (The Mac William's Identities)

Let C be an $[n,k]$ code over $GF(q)$. Then the A_i 's and B_i 's satisfy

$$\sum_{j=0}^{n-t} \binom{n-j}{t} A_j - q^{k-t} \sum_{j=0}^t \binom{n-j}{n-t} B_j = 0 \text{ for } t=0, 1, \dots, n$$

Lemma2.4 For an (n,k, d) code over $GF(q)$, $B_i=0$ for each value of i (where $1 \leq i \leq k$) such that there does not exist an $(n-i, k-i+1, d)$ code.

Lemma2.5 Suppose \vec{u} and \vec{v} are linearly independent vectors in $V(n,q)$ then

$$wt(\vec{u}) + wt(\vec{v}) + \sum_{\lambda \in GF(q) \setminus \{0\}} wt(\vec{u} + \lambda \vec{v}) = q(n-z)$$

Where Z denotes the number of co-ordinates places in which both have zero entries.

AN INEQUALITY FOR $B_q(n,d)$

It is known that $B_q(n,d)$ is an non-negative integer power of q . For an $[n,k,d]$ code B_q

$(n,d)=q^k$ If $d > 1$ then $B_q(n,d) \leq B_q(n-1,d-1)$, for $q=2$ $B_2(n,d)=B_2(n-1,d-1)$. Also $B_q(n,n)=q$.

Theorem3.1 For $d \geq 1$, if $n \geq 2d-1$, then $B_q(n,d) \leq q^{d-1}(q-1)^{n-d+1}$(1.1)

Proof In [1] it is shown that $B_q(n,d) \leq q B_q(n-1,d)$

(1.2) Changing d to $d-1$ in (1.2) we obtain

$$B_q(n,d-1) \leq B_q(n-1,d-1) \text{(1.3)}$$

As a code word of length n and minimum distance at least d is contained in a code word of minimum distance at least $d-1$

$$B_q(n,d) \leq B_q(n,d-1) \text{(1.4)}$$

References

- [1] Carry Huffman and Verapless, *Fundamentals of Error Correcting Codes* Cambridge University press, First south Asian Edition (2004)
- [2] L.L. Donhoff and F.E. Hohn, Chapter 2 page 53-57 *Applied Modern Algebra* Macmillan pub to NY (1978)
- [3] P. Delsarte, *Bounds for unrestricted codes by linear programming* Philips Research Report 27 (1972), 272-289.
- [4] P.P. Greenough, *searching for optimal linear codes*, M.Sc Thesis, University of Salford, 1991.
- [5] R. Hill, *Optimal linear codes in proceeding and of second IMA conference on Cryptography and coding* (oxford university press) to appear
- [6] R. Hill and D.E. Newton, *Some optimal ternary linear codes*, *Ars combinatoria* 25A (1988), 61-72
- [7] R. Hill and D.E. Newton, *Optimal ternary linear codes*, to appear in *Design, codes and Cryptography*
- T. Verhoeff, *An updated table of minimum distance bounds for binary linear codes* *IEEE Trans. Info. Theory*, IT-33 (1987) 665-68