JSR Publications

Available Online

J. Sci. Res. **2** (3), 489-493 (2010)

JOURNAL OF SCIENTIFIC RESEARCH

www.banglajol.info/index.php/JSR

Short Communication

New Bounds on the Minimum Average Distance of Binary Codes

M. Basu[1] and S. Bagchi[2]

[1]Department of Mathematics, University of Kalyani, Kalyani, Nadia, W.B., India, Pin-741235

[2]Department of Mathematics, National Institute of Technology, Durgapur, Burdwan, W.B., India Pin-713209

Received 23 June 2009, accepted in revised form 17 August 2010

Abstract

The minimum average Hamming distance of binary codes of length n and cardinality M is denoted by $\beta(n,M)$. All the known lower bounds $\beta(n,M)$ are useful when M is at least of size about $\frac{2^{n-1}}{n}$. In this paper, for large n, we improve upper and lower bounds for $\beta(n,M)$.

Keywords: Binary code; Hamming distance; Minimum average Hamming distance.

DOI: 10.3329/jsr.v2i3.2708 J. Sci. Res. **2** (3), 489-493 (2010)

1. Introduction

In this paper we will consider only binary codes. Let $F_2 = \{0,1\}$ and let F_2^n denote the set of all binary words of length n. For $x, y \in F_2^n$, $d(x,y)$ denotes the Hamming distance between x and y and $wt(x) = d(x,\mathbf{0})$ is the weight of x, where $\mathbf{0}$ denotes all-zero codeword. A binary code C of length n is a non empty subset of F_2^n. An (n, M) code C is a binary code of length n with cardinality M [1].

The average Hamming distance [2] of an (n,M) code C is defined by

$$\bar{d}(C) = \frac{1}{M^2}\sum_{c\in C}\sum_{c'\in C} d(c,c') \tag{1}$$

The minimum average Hamming distance of an (n,M) code is defined by

$$\beta(n,M) = \min\{\bar{d}(C): C \text{ is an } (n,M) \text{ code }\}.$$

An (n,M) code C for which $\bar{d}(C) = \beta(n,M)$ is called extremal code.

[2] *Corresponding author*: satya5050@gmail.com

On the extremal combinatories of Hamming space, Ahlswede and Katona [3] posed the problem to determine the value of $\beta(n, M)$ for $1 \leq M \leq 2^n$. Ahlswede and Althofer [4] observed that this problem also occurs in the construction of good codes for writing efficient memories, introduced by Ahlswede and Zhang [5] as a model for storing and updating information on a rewritable medium with constraints.

2. Preliminaries

The distance distribution of an (n, M) code C is the $(n+1)$-tuple of rational number $\{A_0, A_1, A_2, \dots, A_n\}$, where $A_i = \frac{|\{(c,c') \in C \times C\}: d(c,c')=i|}{M}$, the average numbers of codewords which are at distance i from any given codeword $c \in C$. It is clear that $A_0 = 1$, $\sum_{i=0}^{n} A_i = M$ and $A_i \geq 0$ for $0 \leq i \leq n$.

Let $d(c_i, c_j) = d_{ij}$ *where* $c_i, c_j \in C,\ i,j = 1,2, \dots, n$.

Therefore, $d(c_i, c_j) = d(c_j, c_i) = d_{ij} = d_{ji}$ and $d_{ii} = 0$.

Consequently, the following composition distance table (Table 1) is symmetric and all diagonal elements are zero.

Table 1

distance	C_1	C_2	C_3	…	C_n
C_1	0	d_{12}	d_{13}	…	d_{1n}
C_2	d_{21}	0	d_{23}	…	d_{2n}
C_3	d_{31}	d_{32}	0	…	d_{3n}
.	.	.	.		.
.	.	.	.		.
.	.	.	.		.
C_n	d_{n1}	d_{n2}	d_{n3}	….	0

From Eq. (1), we get

$$\bar{d}(C) = \frac{1}{M^2} \sum_{c \in C} \sum_{c' \in C} d(c, c') = \frac{2}{M^2} . S \tag{2}$$

where S is the sum of upper triangular components of the composition distance table.

In order to develop our main result in the next section we need the following theorems [2,6,7] on bounds.

Theorem 1: $\lim_{n \to \infty} \beta(n, M) = \frac{5}{2}$.

Theorem 2: $\beta(n,M) \geq \begin{cases} \frac{3n}{n+2} - \frac{n}{M}, & if\ n\ is\ even \\ \frac{3(n+1)}{n+3} - \frac{n+1}{M}, & if\ n\ is\ odd. \end{cases}$

3. Main Result

In this section we develop the following result.

Theorem: For any code $C(n,kn)$ satisfy the following inequality

$$\frac{3k-1}{k} \leq \lim_{n\to\infty} \beta(n,kn) \leq \frac{2}{k^2}[2k(k-1)+1],\ k = 3, 4, 5,\ \ldots$$

and $\beta(n,2n) = \frac{5}{2}, for\ n \to \infty$.

Proof: Let C be the (n,kn) code. The code C partitioned by horizontal lines given below:

$$\begin{array}{c}
\underline{0\,0\,0\,0\,0 \cdots 0\,0\,0} \\
1\,0\,0\,0\,0 \cdots 0\,0\,0 \\
0\,1\,0\,0\,0 \cdots 0\,0\,0 \\
\vdots \\
\underline{0\,0\,0\,0\,0 \cdots 0\,0\,1} \\
1\,1\,0\,0\,0 \cdots 0\,0\,0 \\
1\,0\,1\,0\,0 \cdots 0\,0\,0 \\
\vdots \\
\underline{1\,0\,0\,0\,0 \cdots 0\,0\,1} \\
0\,1\,1\,0\,0 \cdots 0\,0\,0 \\
0\,1\,0\,1\,0 \cdots 0\,0\,0 \\
\vdots \\
\underline{0\,1\,0\,0\,0 \cdots 0\,0\,1} \\
0\,0\,1\,1\,0 \cdots 0\,0\,0 \\
0\,0\,1\,0\,1 \cdots 0\,0\,0 \\
\vdots \\
\underline{0\,0\,1\,0\,0 \cdots 0\,0\,1} \\
0\,0\,0\,1\,1 \cdots 0\,0\,0 \\
0\,0\,0\,1\,0 \cdots 0\,0\,0 \\
\vdots \\
\underline{0\,0\,0\,1\,0 \cdots 0\,0\,1} \\
\vdots
\end{array}$$

Except all-zero codeword, the number of codewords between the first two horizontal lines is n, between the next two horizontal lines; the number of code words is n-1 and so on. Proceeding in this way, in order to meet the total number of codewords $kn,$ we need to include the remaining codewords from below the $(k+1)^{\text{th}}$ horizontal line.

First we prove the upper bounds of $\lim_{n\to\infty} \beta(n,\ kn)$.

When $k = 2$, we consider only first three parts of the above codewords.

We can easily prove the following result by using Theorem 2,

$$\beta(n,2n) \le \bar{d}(C) = \frac{5}{2} - \frac{4n-2}{n^2}.$$

Taking limit $n \to \infty$, we have

$$\lim_{n\to\infty} \beta(n, 2n) \le \bar{d}(C) = \frac{5}{2} = \frac{2}{2^2}[2.2(2-1)+1] \tag{3}$$

Again when $k = 3$, we take only first four parts of the above codewords and two codewords from rest. Then by (2), we have

$$\beta(n,3n) \le \bar{d}(C) = \frac{26}{9} - O(\frac{1}{n})$$

Taking limit n$\to \infty$, we have

$$\lim_{n\to\infty} \beta(n,3n) \le \bar{d}(C) = \frac{2}{3^2}.13 = \frac{2}{3^2}[2.3(3-1)+1]$$

Again when $k = 4$, then we take only first five parts of the above codewords and any five codewords from rest. Then by (2), we have

$$\beta(n,4n) \le \bar{d}(C) = \frac{50}{16} - O(\frac{1}{n})$$

Taking limit $n \to \infty$, we have

$$\lim_{n\to\infty} \beta(n,4n) \le \bar{d}(C) = \frac{2}{4^2}.25 = \frac{2}{4^2}[2.4(4-1)+1].$$

In this way, if we increase the value of k, we get a sequential way of the above theorem for right hand side:

$$\lim_{n\to\infty} \beta(n,kn) \le \bar{d}(C) = \frac{2}{k^2}[2k(k-1)+1],\ k = 2, 3, 4, \ldots$$

Now we prove the lower bounds of $\lim_{n\to\infty} \beta(n,kn)$.

From Theorem 2, we have

$$\beta(n,M) \geq \begin{cases} \frac{3n}{n+2} - \frac{n}{M}, & if\ n\ is\ even \\ \frac{3(n+1)}{n+3} - \frac{n+1}{M}, & if\ n\ is\ odd. \end{cases}$$

Taking $M = kn$, we get

$$\beta(n,kn) \geq \begin{cases} \frac{3n}{n+2} - \frac{n}{kn} = \frac{3k-1}{k} - \frac{6}{n+2}, & if\ n\ is\ even \\ \frac{3(n+1)}{n+3} - \frac{n+1}{kn} = \frac{3k-1}{k} - \frac{6kn+n+3}{k(n^2+3n)}, & if\ n\ is\ odd. \end{cases}$$

Taking limit as $n \to \infty$, we have

$$\lim_{n\to\infty} \beta(n,kn) \geq \frac{3k-1}{k} \tag{4}$$

Thus

$$\frac{3k-1}{k} \leq \lim_{n\to\infty} \beta(n,kn) \leq \frac{2}{k^2}[2k(k-1)+1],\ k = 3, 4, \ldots$$

Also, it is clear from (3) and (4),

$$\beta(n,2n) = \frac{5}{2}, for\ n \to \infty.$$

This completes the proof. □

Acknowledgement

The authors are thankful to the reviewers for valuable suggestions which considerably improved the presentation of the paper.

References

1. S. -T. Xia and F. -W. Fu, Discrete Appl. Math. **89**, 269 (1998). doi:10.1016/S0166-218X(98)00081-X
2. B. Mounts, arxiv: 0706.3295v1 [Math.CO] 22 June 2007.
3. R. Ahlswede and G. Katona, Discrete Math. **17**, 1 (1977). doi:10.1016/0012-365X(77)90017-6
4. R. Ahlswede and I. Alth¨ofer, J. Combin. Theory Ser. B **61**, 167 (1994). doi:10.1006/jctb.1994.1042
5. I. Alth¨ofer and T. Sillke, J. Combin. Theory Ser. B **56**, 296 (1992). doi:10.1016/0095-8956(92)90024-R
6. M. R. Best, A. E. Brouwer, F. J. MacWilliams, A. M. Odlyzko, and N. J. A. Sloane, IEEE Trans. on Inform. Theory 24, 81 (Jan. 1978). doi:10.1109/TIT.1978.1055827
7. F. -W. Fu, V. K. Wei and R. W. Yeung, Discrete Appl. Math. **111** (3), 263 (2001). doi:10.1016/S0166-218X(00)00284-5