Bull. Korean Math. Soc. **38** (2001), No. 4, pp. 797–801

A NEW UPPER BOUND FOR SINGLE ERROR-CORRECTING CODES

JUN KYO KIM

ABSTRACT. The purpose of this paper is to give an upper bound for $A[n,4]$, the maximum number of codewords in a binary code of word length n with minimum distance 4 between codewords. We have improved upper bound for $A[12k+11,4]$. In this correspondence we prove $A[23,4] \leq 173716$.

1. Introduction

In this paper we present an upper bound for $A[n,4]$, the maximum number of codewords in a binary code of length n with minimum distance 4 between codewords. An $[n,d]$ code is a code of length n in which any two words have distance at least d. An $[n,d,w]$ code is an $[n,d]$ code in which all words have weight w. An $[n,d]$ code for which the maximum is archived is called optimal. The maximum number of codewords of an $[n,d]$ code is denoted by $A[n,d]$. This function $A[n,d]$ and $A[n,d,w]$, the number of codewords in an optimal $[n,d,w]$ code, has been studied by many authors. Earlier bounds on $A[n,d]$ were given in [7, 11, 2, 1] (also [5, Chapter 9]). Whereas they used the linear programming approach to get upper bound for $A[n,d]$, in a recent paper of [8] they have got improved general upper bound for $A[6k+5,4]$ by combinatorial methods. We obtain the improved upper bound for $A[12k+11,4]$. In the present paper we give upper bounds for $A[n,4]$:

$$(1) \qquad A[n,4] \leq \frac{2^{n-1}A[n,4,3]}{\binom{n}{3} - 4A[n,4,4] + nA[n,4,3]}.$$

Received May 9, 2001.
2000 Mathematics Subject Classification: 94B65, 05B40.
Key words and phrases: bounds on codes, packing.
The author wishes to acknowledge the financial support of the Korea Research Foundation made in the program year of (1999).

In this correspondence we prove $A[23,4] \leq 173716$. For convenience we define some notations and conventions used in this paper. The *weight distribution* of a code is the sequence $(W_i)_{i=0}^n$ where W_i equals the number of codewords of weight i. The distance distribution of C is the sequence $(A_i)_{i=0}^n$ where A_i equals the average number of code words at distance i from a fixed codeword, i.e.,

$$A_i = \frac{1}{|C|} \sum_{x \in C} |\{y \mid y \in C \text{ and } d(x,y) = i\}|.$$

All codes are binary codes of length n with minimum distance 4. Let $n \in \mathbb{N}$, $r \in \{0,1,\cdots,n\}$, and $C \subset \mathbb{F}_{even}^n$ be a code with $A[n,4]$ codewords where $\mathbb{F}_{even}^n = \{x \in \{0,1\}^n \mid d(0,x) \equiv 0 \pmod 2\}$. We first introduce some set.

$$\begin{aligned} B_r(x) &= \{y \in \{0,1\}^n \mid d(x,y) \leq r\}; \\ X &= \mathbb{F}_{odd}^n - \bigcup_{g \in C} B_1(g); \\ S &= \{(x,g) | x \in X, g \in C \text{ and } d(x,g) = 3\}, \end{aligned}$$

where $\mathbb{F}_{odd}^n = \{0,1\}^n - \mathbb{F}_{even}^n$. $B_r(x)$ is called the *sphere with radius r and center x*. For $x \in X$ and $g \in C$, let

$$\begin{aligned} C_x &= \{(x,g) | (x,g) \in S\}; \\ X_g &= \{(x,g) | (x,g) \in S\}. \end{aligned}$$

Hence

$$S = \bigcup_{x \in X} C_x = \bigcup_{g \in C} X_g. \tag{2}$$

2. Upper bounds for $A[n,4]$

Without loss of generality it can be assumed that in an optimal binary code with even minimum distance, only words of even weight occur. The first two theorems are well-known.

THEOREM 1 (Trivial values). *Let $d, w, n \in \mathbb{N}$ with $w \leq n$. Then*

a) $A[n,d] = A[n+1,d+1]$ *if d is odd,*
b) $A[n,d,w] = \lfloor n/w \rfloor$ *if $d = 2w$,*
c) $A[n,d,w] = 1$ *if $2w < d$,*
d) $A[n,2,w] = \binom{n}{w}$,
e) $A[n,d,w] = A[n,d-1,w]$ *if d is even.*

THEOREM 2 (Johnson [7, p. 98]).

$$A[n,d,w] \le \left\lfloor \frac{n}{w} A[n-1,d,w-1] \right\rfloor, \quad (n \ge w \ge 1), \tag{3}$$

$$A[n,d,w] \le \left\lfloor \frac{n}{n-w} A[n-1,d,w] \right\rfloor, \quad (n > w \ge 0). \tag{4}$$

The *first Johnson bound* $J_1(n,d,w)$ is defined to be the smallest upper bound on $A[n,d,w]$ that is obtained by repeatedly applying (3) and (4) until Theorem 1 can be used. For example

$$J_1[n,4,3] = \begin{cases} \left\lfloor \frac{n}{3} \left\lfloor \frac{n-1}{2} \right\rfloor \right\rfloor & \text{if } n \not\equiv 5 \pmod 6 \\ \left\lfloor \frac{n}{3} \left\lfloor \frac{n-1}{2} \right\rfloor \right\rfloor - 1 & \text{if } n \equiv 5 \pmod 6. \end{cases}$$

Clearly

$$A[n,d,w] \le J_1[n,d,w].$$

THEOREM 3 (Kirkman [9], Schönheim [10]; see also [6, p. 237]).

$$A[n,4,3] = J_1[n,4,3].$$

THEOREM 4 (Brouwer [4]).

a) $A[n,4,4] \le \left\lfloor \frac{n}{4} A[n-1,4,3] \right\rfloor$ *if* $n \equiv 5 \pmod 6$,

b) $A[n,4,4] = \left\lfloor \frac{n}{4} A[n-1,4,3] \right\rfloor$ *if* $n \not\equiv 5 \pmod 6$.

Now suppose that $x \in \{0,1\}^n$ and $g, g' \in C$. Then

$$d(x+g, x+g') = d(g,g') \ge 4.$$

Hence $x + C$ is also code with minimum distance 4. We note that the unions in (2) are actually disjoint unions. Hence each $\{C_x\}$ or $\{X_g\}$ in (2) forms a partition of S ([8]). The next two lemmas lead us directly into the main theorem.

LEMMA 1. *Let* $n \ge 2$. *Then*

$$|S| \le (2^{n-1} - nA[n,4])A[n,4,3]. \tag{5}$$

Proof. Let $x \in X$. From the definition of $A[n,4,3]$ and Theorem 1 e), we obtain

$$\begin{aligned} |C_x| &= |\{g \in C | d(x,g) = 3\}| = |\{g \in C | d(0, g+x) = 3\}| \\ &= |\{g \in x + C | d(0,g) = 3\}| \leq A[n,4,3]. \end{aligned}$$

Since $|X| = (2^{n-1} - nA[n,4])$ and $|S| = \sum_{x \in X} |C_x|$, we have inequality (5). □

LEMMA 2. *Let $n \geq 2$. Then*

$$|S| = A[n,4]\left(\binom{n}{3} - 4 \cdot A_4\right). \tag{6}$$

Proof. Let $g \in C$. From the definition of A_4, we obtain

$$\begin{aligned} |X_g| &= |\{x \in \mathbb{F}^n | d(x,g) = 3\}| \\ &\quad -|\{x \in \mathbb{F}^n | d(x,g) = 3 \text{ and } d(x,C) = 1\}| \\ &= \binom{n}{3} - 4 \cdot |\{g\prime \in C | d(g, g\prime) = 4\}| \\ &= \binom{n}{3} - 4A_4. \end{aligned}$$

Hence we have

$$|S| = \sum_{g \in C} |X_g| = \binom{n}{3}|C| - 4|C|A_4.$$

Which is the claimed result. □

Comparison of (5) and (6) leads to

THEOREM 5 (Main theorem).

$$A[n,4] \leq \frac{2^{n-1}A[n,4,3]}{\binom{n}{3} - 4A_4 + nA[n,4,3]}.$$

In [3], it is shown that for $n > 1$

$$A(n,3) \leq \begin{cases} 2^n/(n+1) & \text{if } n \equiv 3 \pmod 4 \\ 2^n/(n+2) & \text{if } n \equiv 2 \pmod 4 \\ 2^n/(n+3) & \text{if } n \equiv 1 \pmod 4 \\ 2^n/(n+4) & \text{if } n \equiv 0 \pmod 4 \end{cases}$$

In paper [8], Kim and Hahn show

$$A(n,3) \le \begin{cases} 2^n/(n+2) & \text{if } n \equiv 0,2 \pmod 6 \\ 2^n/(n+2+2/n) & \text{if } n \equiv 4 \pmod 6 \\ 2^n/n+1 & \text{if } n \equiv 1,3 \pmod 6 \\ 2^n/n+1+8/(n-1) & \text{if } n \equiv 5 \pmod 6. \end{cases}$$

Theorem 5 is sharper than the above results for the case $n \equiv 11 \pmod{12}$

It is known that $A[23,4] \le 173784$ (Best [1]; see also [5, Chapter 9]). Theorem 3, Theorem 4, and the previous theorem yields

THEOREM 6.

$$A[23,4] \le 173716.$$

References

[1] M. R. Best, *Binary Codes with a Minimum Distance of Four*, IEEE Trans. Inform. Theory **IT-26** (1980), 738–742.

[2] M. R. Best, A. E. Brouwer, F. J. MacWilliams, A. M. Odlyzko, and N. J. A. Sloane, *Bounds for Binary Codes of Length Less Than 25*, IEEE Trans. Inform. Theory **IT-24** (1978), 81–93.

[3] M. R. Best and A. E. Brouwer, *The Triply Shortened Binary Hamming Code is Optimal*, Discrete Math. **17** (1977), 235–245.

[4] A. E. Brower, *Optimal Packings of K_4's into a K_n*, J. Comb. Theory **5** (1979), 278–297.

[5] J. H. Conway and N. J. A. Sloane, *Sphere Packings, Lattices and Groups*, New York: Springer-Verlag, 1988.

[6] M. Hall, Jr, *Combinatorial Theory*, Blaisdell: Watham, MA, 1967.

[7] S. M. Johnson, *On Upper Bounds for Unrestricted Binary Error-correcting Codes*, IEEE Trans. Inform. Theory **IT-17** (1971), 203–207.

[8] J. K. Kim and S. G. Hahn *A New Upper Bound for Binary Codes with Minimum Distance Four*, Discrete Math. **187** (1998), 291–295.

[9] T. P. Kirkman, *On a Problem in Combinations*, Cambridge and Dublin Math. J. **2** (1847), 191–204.

[10] J. Schönheim, *On Maximal System of K-tuples*, Studia Sci. Math. Hungar **1** (1966), 363–368.

[11] N. J. A. Sloane, *A Survey of Constructive Coding Theory and a Table of Binary Codes of Highest Known Rate*, Discrete Math. **3** (1972), 265–294.

[12] V. D. Tonchev, *Combinatorial, Configurations, Designs, Codes, Graphs*, Longman, Harlow: New York, 1988.

FACULTY OF LIBERAL ARTS, MIRYANG NATIONAL UNIVERSITY, 1025-1, NAEI-DONG, MIRYANG-SI, GYEONGSANGNAM-DO 627-702, KOREA

E-mail: junkyo@arang.miryang.ac.kr