Improved Upper Bounds on Sizes of Codes

Beniamin Mounits, Tuvi Etzion, *Senior Member, IEEE*, and Simon Litsyn, *Senior Member, IEEE*

***Abstract*—Let $A(n, d)$ denote the maximum possible number of codewords in a binary code of length n and minimum Hamming distance d. For large values of n, the best known upper bound, for fixed d, is the Johnson bound. We give a new upper bound which is at least as good as the Johnson bound for all values of n and d, and for each d there are infinitely many values of n for which the new bound is better than the Johnson bound. For small values of n and d, the best known method to obtain upper bounds on $A(n, d)$ is linear programming. We give new inequalities for the linear programming and show that with these new inequalities some of the known bounds on $A(n, d)$ for $n \leq 28$ are improved.**

***Index Terms*—$A(n, d)$, holes, Johnson bound, linear programming bound.**

I. Introduction

Let $\mathcal{F}_2 = \{0, 1\}$ and let $\mathcal{F}_2^n$ denote the set of all binary words of length n. For $x, y \in \mathcal{F}_2^n$, $d(x, y)$ denote the Hamming distance between x and y and $W(x) = d(x, \mathbf{0})$ is the weight of x, where $\mathbf{0}$ denote the all-zeros word. For a code $\mathcal{C}$, we denote the minimum Hamming distance (or minimum distance, in short) of $\mathcal{C}$ by $d(\mathcal{C})$, i.e.,

$$d(\mathcal{C}) = \min_{c_1, c_2 \in \mathcal{C}, c_1 \neq c_2} d(c_1, c_2).$$

An $(n, M, 2\delta+i)$ code $\mathcal{C}$, $i \in \{1, 2\}$, is a binary code of length n, minimum distance $2\delta + i$, and M codewords. The code $\mathcal{C}_e$ is the *extended code* of $\mathcal{C}$, i.e., $\mathcal{C}_e$ is obtained from $\mathcal{C}$ by adding an even parity bit to each codeword of $\mathcal{C}$. Clearly, all codewords of $\mathcal{C}_e$ have even weight and if $d(C) = 2\delta + 1$ then $d(\mathcal{C}_e) = 2\delta + 2$.

Let $A(n, d)$ denote the maximum number of codewords in a binary code of length n and minimum Hamming distance d. $A(n, d)$ is a basic quantity in coding theory. Lower bounds on $A(n, d)$ are obtained by constructions. For survey on the known lower bounds the reader is referred to [12]. In this paper we consider upper bounds on $A(n, d)$. We only have to consider the case where the minimum distance d is odd because of the well-known result proved by using the extended code.

Lemma 1: $A(n+1, d+1) = A(n, d)$ for odd d. □

The most basic upper bound on $A(n, d)$, $d = 2\delta + 1$, is the sphere packing bound, also known as the Hamming bound.

Theorem 1:

$$A(n, 2\delta+1) \leq \frac{2^n}{\sum_{i=0}^{\delta} \binom{n}{i}}. \qquad \square$$

Codes which attain the sphere packing bound are called perfect codes and the only perfect codes are

- $(n, 2^n, 1)$ codes for each $n \geq 1$;
- $(2k+1, 2, 2k+1)$ repetition codes for each $k \geq 0$;
- $(2^k - 1, 2^{2^k - k - 1}, 3)$ codes for each $k \geq 2$;
- the $(23, 4096, 7)$ Golay code.

Johnson [9] has improved the sphere-packing bound. In his theorem, he used the quantity $A(n, d, w)$, which is the maximum number of codewords in a binary code of length n, constant weight w, and minimum distance d.

Theorem 2:

$$A(n, 2\delta+1) \leq \frac{2^n}{\sum_{i=0}^{\delta} \binom{n}{i} + \frac{\binom{n}{\delta+1} - \binom{2\delta+1}{\delta} A(n, 2\delta+2, 2\delta+1)}{A(n, 2\delta+2, \delta+1)}}. \qquad \square$$

Since $A(n, 2k, k) = \lfloor \frac{n}{k} \rfloor$ we have the following.

Corollary 1:

$$A(n, 2\delta+1) \leq \frac{2^n}{\sum_{i=0}^{\delta} \binom{n}{i} + \frac{\binom{n}{\delta+1} - \binom{2\delta+1}{\delta} A(n, 2\delta+2, 2\delta+1)}{\lfloor \frac{n}{\delta+1} \rfloor}}. \qquad \square$$

Codes which attain the Johnson bound are called nearly perfect codes and the only nearly perfect codes are the perfect codes and the following codes:

- $(2^k - 2, 2^{2^k - k - 2}, 3)$ codes for each $k \geq 2$;
- $(2^k - 1, 2^{2^k - 2k}, 5)$ punctured Preparata codes for each even $k \geq 4$.

All the results concerning perfect codes, nearly perfect codes, and bounds on $A(n, d)$ given above are summarized in [5] and [13]. Johnson [9] also provided an improvement of his bound, but it works only for small values of n for any given d. We will consider it later in the Appendix.

Another bound on $A(n, d)$ is the Plotkin bound [14] given in the following theorem.

Theorem 3:

- If d is even and $2d > n$ then $A(n, d) \leq 2\lfloor \frac{d}{2d-n} \rfloor$.
- $A(2d, d) \leq 4d$.
- If d is odd and $2d+1 > n$ then $A(n, d) \leq 2\lfloor \frac{d+1}{2d+1-n} \rfloor$.
- $A(2d+1, d) \leq 4d + 4$. □

Manuscript received May 20, 2000. The work of T. Etzion was supported in part by the Israeli Science Foundation under Grant 88/99. The work of S. Litsyn was supported in part by the Binational Science Foundation under Grant 1999099.

B. Mounits is with the Department of Mathematics, Technion–Israel Institute of Technology, Haifa 32000, Israel (e-mail: mounitsb@tx.technion.ac.il).

T. Etzion is with the Department of Computer Science, Technion–Israel Institute of Technology, Haifa 32000, Israel (e-mail: etzion@cs.technion.ac.il).

S. Litsyn is with the Department of Electrical Engineering–Systems, Tel-Aviv University, Tel-Aviv, Israel (e-mail: litsyn@eng.tau.ac.il).

Communicated by P. Solé, Associate Editor for Coding Theory.

Publisher Item Identifier S 0018-9448(02)01939-9.

It was proved by Levenshtein [11] that the Plotkin bound is attained with equality for many parameters. His construction is based on the existence of Hadamard matrices and since it is conjectured that Hadamard matrices exist for all orders divisible by 4, it is also conjectured that for all parameters there are codes that attain the Plotkin bound with equality.

When someone is given specific, relatively small values, of n and d, the best method to find upper bound on $A(n,\, d)$ is the linear programming bound. We will discuss this bound in details at a later stage. However, the computation of this bound is not tractable for large values of n. Therefore, for fixed d and large values of n, the best known upper bound on $A(n,\, d)$ is the Johnson bound.

The paper is organized as follows. In Section II, we prove a new upper bound on $A(n,\, 2\delta+1)$. It is given by the following inequality:

$$A(n,\, 2\delta+1) \leq \frac{2^n}{\sum_{i=0}^{\delta}\binom{n}{i} + \frac{\binom{n+1}{\delta+2}-\binom{2\delta+2}{\delta+2}A(n+1,\, 2\delta+2,\, 2\delta+2)}{A(n+1,\, 2\delta+2,\, \delta+2)}}.$$

In Section III, we first prove that the new bound is always at least as good as the Johnson bound. Then we show that for each $\delta \geq 1$ there exist infinitely many values of n for which the new bound is better than the Johnson bound. In Section IV, we give a set of new inequalities for the linear programming bound, which are added to the known inequalities. Using this new set of inequalities we give 13 new upper bounds on $A(n,\, d)$ for $n \leq 28$ and $d \leq 10$. Finally, in the Appendix we discuss the improvement of Johnson to his bound and show that our bound has a similar improvement.

II. The New Bound

Let $\mathcal{C}$ be an $(n, M, 2\delta{+}1)$ code, for which $M{=}A(n, 2\delta{+}1)$, and $\mathcal{C}_e$ be its extended $(n+1,\, M,\, 2\delta+2)$ code. Without loss of generality we assume that **0** is a codeword of $\mathcal{C}$. We say that a word $x \in \mathcal{F}_2^n(\mathcal{F}_2^{n+1})$ is covered by a codeword $c \in \mathcal{C}(\mathcal{C}_e)$ if $d(x,\, c) \leq \delta$. For a word $x \in \mathcal{F}_2^n$, $d(x,\, \mathcal{C})$ stands for the Hamming distance between x and $\mathcal{C}$, i.e., $d(x,\, \mathcal{C}) = \min_{c\in\mathcal{C}}\, d(x,\, c)$. A word $h \in \mathcal{F}_2^n$ is called a *hole* if $d(h,\, C) > \delta$. The number of holes of weight i, with respect to $\mathcal{C}$, is denoted by $H_i(\mathcal{C})$, and $A_i(\mathcal{C})$ stands for the number of codewords with weight i in $\mathcal{C}$. We will write A_i instead of $A_i(\mathcal{C})$ if the code $\mathcal{C}$ is understood from the context. Let $H(\mathcal{C})$ be the total number of holes with respect to $\mathcal{C}$. Finally, we define $NH(c, \mathcal{C}, \Delta)$ to be the number of holes at distance Δ from a codeword c in a code $\mathcal{C}$, $NC(h,\, \mathcal{C},\, \Delta)$ to be the number of codewords of $\mathcal{C}$ at distance Δ from a hole h, and $H(C,\, \Delta)$ to be the number of holes at distance Δ from $\mathcal{C}$. Similar definitions are given for $\mathcal{C}_e$.

Lemma 2:

$$H_{\delta+1}(\mathcal{C}) = \binom{n}{\delta+1} - \binom{2\delta+1}{\delta+1}A_{2\delta+1}(\mathcal{C}).$$

Proof: The total number of words of weight $\delta+1$ in $\mathcal{F}_2^n$ is $\binom{n}{\delta+1}$. Words of weight $\delta+1$ can be covered only by codewords of weight $2\delta{+}1$ of $\mathcal{C}$. A codeword of weight $2\delta{+}1$ covers $\binom{2\delta+1}{\delta+1}$ words of weight $\delta{+}1$. Finally, two codewords $c_1,\, c_2 \in \mathcal{C}$ cannot cover the same word and hence

$$H_{\delta+1}(\mathcal{C}) = \binom{n}{\delta+1} - \binom{2\delta+1}{\delta+1}A_{2\delta+1}(\mathcal{C}). \qquad \square$$

Lemma 3:

$$H_{\delta+2}(\mathcal{C}) = \binom{n}{\delta+2} - \binom{2\delta+1}{\delta+2}A_{2\delta+1}(\mathcal{C}) - \binom{2\delta+2}{\delta+2}A_{2\delta+2}(\mathcal{C}).$$

Proof: The total number of words of weight $\delta+2$ in $\mathcal{F}_2^n$ is $\binom{n}{\delta+2}$. Words of weight $\delta+2$ can be covered either by codewords of weight $2\delta+2$ or by codewords of weight $2\delta+1$. A codeword of weight $2\delta{+}2$ covers $\binom{2\delta+2}{\delta+2}$ words of weight $\delta{+}2$. A codeword of weight $2\delta+1$ covers $\binom{2\delta+1}{\delta+2}$ words of weight $\delta{+}2$. Finally, two codewords $c_1,\, c_2 \in \mathcal{C}$ cannot cover the same word and hence

$$H_{\delta+2}(\mathcal{C}) = \binom{n}{\delta+2} - \binom{2\delta+1}{\delta+2}A_{2\delta+1}(\mathcal{C}) - \binom{2\delta+2}{\delta+2}A_{2\delta+2}(\mathcal{C}).$$

$\square$

Lemma 4:

$$H_{\delta+2}(\mathcal{C}_e) = H_{\delta+1}(\mathcal{C}) + H_{\delta+2}(\mathcal{C}).$$

Proof: If w_1 is a hole of weight $\delta+1$ with respect to $\mathcal{C}$ then clearly $w_1 1$ is a hole of weight $\delta+2$ with respect to $\mathcal{C}_e$ and if w_2 is a hole of weight $\delta+2$ with respect to $\mathcal{C}$ then $w_2 0$ is a hole of weight $\delta+2$ with respect to $\mathcal{C}_e$. Therefore,

$$H_{\delta+2}(\mathcal{C}_e) \geq H_{\delta+1}(\mathcal{C}) + H_{\delta+2}(\mathcal{C}). \qquad (1)$$

Let hb be a hole of weight $\delta+2$ with respect to $\mathcal{C}_e$, where $h \in \mathcal{F}_2^n$ and $b \in \mathcal{F}_2$, i.e., $d(hb,\, \mathcal{C}_e) > \delta$. Therefore, $d(h,\, \mathcal{C}) \geq \delta$. We claim that h is a hole with respect to $\mathcal{C}$. We distinguish between two cases.

Case 1) $b = 0$, i.e., the weight of h is $\delta+2$. If h is not a hole then there exists a codeword $x \in \mathcal{C}$ such that $d(x,\, h) = \delta$, and since $d(\mathcal{C}) = 2\delta+1$, $W(h) = \delta+2$, it follows that $W(x) = 2\delta+2$. Therefore, $x0 \in \mathcal{C}_e$, $d(x0,\, hb) = \delta$, and hb is not a hole with respect to $\mathcal{C}_e$, which is a contradiction.

Case 2) $b = 1$, i.e., the weight of h is $\delta+1$. If h is not a hole then there exists a codeword $x \in \mathcal{C}$ such that $d(x,\, h) = \delta$, and since $d(\mathcal{C}) = 2\delta{+}1$ it follows that $W(x) = 2\delta{+}1$. Therefore, $x1 \in \mathcal{C}_e$, $d(x1,\, hb) = \delta$, and hb is not a hole with respect to $\mathcal{C}_e$, which is a contradiction.

Both cases imply that h is a hole and hence

$$H_{\delta+2}(\mathcal{C}_e) \leq H_{\delta+1}(\mathcal{C}) + H_{\delta+2}(\mathcal{C}). \qquad (2)$$

Equations (1) and (2) imply that

$$H_{\delta+2}(\mathcal{C}_e) = H_{\delta+1}(\mathcal{C}) + H_{\delta+2}(\mathcal{C}). \qquad \square$$

Lemma 5:

$$H_{\delta+2}(\mathcal{C}_e) \geq \binom{n+1}{\delta+2} - \binom{2\delta+2}{\delta+2}A(n+1,\, 2\delta+2,\, 2\delta+2).$$

Proof: By Lemmas 2–4

$$\begin{aligned} H_{\delta+2}(\mathcal{C}_e) &= H_{\delta+1}(\mathcal{C}) + H_{\delta+2}(\mathcal{C}) \\ &= \binom{n}{\delta+1} - \binom{2\delta+1}{\delta+1} A_{2\delta+1}(\mathcal{C}) + \binom{n}{\delta+2} \\ &\quad - \binom{2\delta+1}{\delta+2} A_{2\delta+1}(\mathcal{C}) - \binom{2\delta+2}{\delta+2} A_{2\delta+2}(\mathcal{C}) \end{aligned}$$

and hence

$$H_{\delta+2}(\mathcal{C}_e) = \binom{n+1}{\delta+2} - \binom{2\delta+2}{\delta+2}[A_{2\delta+1}(\mathcal{C}) + A_{2\delta+2}(\mathcal{C})]. \tag{3}$$

It is easily verified that

$$\begin{aligned} &A_{2\delta+1}(\mathcal{C}) + A_{2\delta+2}(\mathcal{C}) \\ &\qquad = A_{2\delta+2}(\mathcal{C}_e) \leq A(n+1, 2\delta+2, 2\delta+2) \end{aligned} \tag{4}$$

and, therefore, by (3) and (4) we have

$$H_{\delta+2}(\mathcal{C}_e) \geq \binom{n+1}{\delta+2} - \binom{2\delta+2}{\delta+2} A(n+1, 2\delta+2, 2\delta+2). \quad \square$$

Corollary 2: If $c \in \mathcal{C}_e$ then

$$NH(c, \mathcal{C}_e, \delta+2) \geq \binom{n+1}{\delta+2} - \binom{2\delta+2}{\delta+2} A(n+1, 2\delta+2, 2\delta+2). \quad \square$$

Lemma 6: If for a hole h with respect to $\mathcal{C}_e$ there exists a codeword $c_1 \in \mathcal{C}_e$ such that $d(h, c_1) = \delta + 2$, then $d(h, \mathcal{C}_e) = \delta + 2$.

Proof: Clearly, $d(h, \mathcal{C}_e) \leq \delta+2$. To complete the proof we only have to show that $d(h, \mathcal{C}_e) \neq \delta+1$. Assume the contrary, i.e., that there exists a codeword $c_2 \in \mathcal{C}_e$ such that $d(h, c_2) = \delta+1$. But this implies that $d(c_1, c_2)$ is odd which is a contradiction since all codewords of $\mathcal{C}_e$ have even weight. □

Lemma 7:

$$H(\mathcal{C}_e, \delta+2) \leq 2^n - M \sum_{i=0}^{\delta} \binom{n}{i}.$$

Proof: Clearly,

$$H(C) = 2^n - M \sum_{i=0}^{\delta} \binom{n}{i}.$$

By Lemma 4, each hole of the form hb, $h \in \mathcal{F}_2^n$, $b \in \mathcal{F}$, with respect to $\mathcal{C}_e$, for which $d(hb, x) = \delta + 2$, for some $x \in \mathcal{C}_e$, is obtained from a hole h of $\mathcal{C}$. To complete the proof we only have to show that if hb is a hole for which $d(hb, y) = \delta + 2$, for some $y \in \mathcal{C}_e$, then $h\bar{b}$, where $\bar{b}$ stands for the binary complement of b, is not a hole for which $d(h\bar{b}, z) = \delta + 2$, for some $z \in \mathcal{C}_e$. Assume the contrary, i.e., that there exist two codewords $c_1, c_2 \in \mathcal{C}_e$ such that $d(hb, c_1) = \delta + 2$ and $d(h\bar{b}, c_2) = \delta + 2$. But this implies that $d(c_1, c_2)$ is odd which is a contradiction since all codewords of $\mathcal{C}_e$ have even weight.

Thus,

$$H(\mathcal{C}_e, \delta+2) \leq H(C) = 2^n - M \sum_{i=0}^{\delta} \binom{n}{i}. \quad \square$$

Theorem 4:

$$A(n, 2\delta+1) \leq \frac{2^n}{\sum_{i=0}^{\delta} \binom{n}{i} + \frac{\binom{n+1}{\delta+2} - \binom{2\delta+2}{\delta+2} A(n+1, 2\delta+2, 2\delta+2)}{A(n+1, 2\delta+2, \delta+2)}}.$$

Proof: By Corollary 2 we have

$$\begin{aligned} &\sum_{c \in \mathcal{C}_e} NH(c, \mathcal{C}_e, \delta+2) \\ &\qquad \geq M\left(\binom{n+1}{\delta+2} - \binom{2\delta+2}{\delta+2} A(n+1, 2\delta+2, 2\delta+2)\right). \end{aligned} \tag{5}$$

We also have that for each hole h with respect to $\mathcal{C}_e$

$$NC(h, \mathcal{C}_e, \delta+2) \leq A(n+1, 2\delta+2, \delta+2). \tag{6}$$

By Lemmas 6, 7, and (6) we have

$$\begin{aligned} &\sum_{h,\, d(h, \mathcal{C}_e) = \delta+2} NC(h, \mathcal{C}_e, \delta+2) \\ &\qquad \leq \left(2^n - M \sum_{i=0}^{\delta} \binom{n}{i}\right) A(n+1, 2\delta+2, \delta+2) \end{aligned} \tag{7}$$

and

$$\sum_{c \in \mathcal{C}_e} NH(c, \mathcal{C}_e, \delta+2) = \sum_{h, d(h, \mathcal{C}_e) = \delta+2} NC(h, \mathcal{C}_e, \delta+2) \tag{8}$$

since each pair $\{c, h\}$, where $c \in \mathcal{C}_e$, and $d(h, \mathcal{C}_e) = \delta + 2$, is counted exactly once on each side of the equation.

We substitute (5) and (7) into (8) and use the initial assumption that $M = A(n, 2\delta + 1)$ to obtain

$$\begin{aligned} &A(n, 2\delta+1)\left(\binom{n+1}{\delta+2} - \binom{2\delta+2}{\delta+2} A(n+1, 2\delta+2, 2\delta+2)\right) \\ &\quad \leq \left(2^n - A(n, 2\delta+1) \sum_{i=0}^{\delta} \binom{n}{i}\right) A(n+1, 2\delta+2, \delta+2) \end{aligned}$$

which implies the claim of the theorem. □

III. Comparison With the Johnson Bound

In this section, we will examine the bound given in Theorem 4 in Section II. We will first prove that the bound is at least as good as the Johnson bound and then we will show that for each δ there exist infinitely many values of n for which the new bound is better than the Johnson bound. Let $J(n, \delta)$ denote the Johnson upper bound on $A(n, 2\delta+1)$ and $HL(n, \delta)$ denote the new upper bound on $A(n, 2\delta + 1)$, i.e.,

$$J(n, \delta) = \frac{2^n}{\sum_{i=0}^{\delta} \binom{n}{i} + \frac{\binom{n}{\delta+1} - \binom{2\delta+1}{\delta} A(n, 2\delta+2, 2\delta+1)}{A(n, 2\delta+2, \delta+1)}}$$

and

$$HL(n, \delta) = \frac{2^n}{\sum_{i=0}^{\delta} \binom{n}{i} + \frac{\binom{n+1}{\delta+2} - \binom{2\delta+2}{\delta+2} A(n+1, 2\delta+2, 2\delta+2)}{A(n+1, 2\delta+2, \delta+2)}}.$$

To prove the next theorem we need the following lemma which is one of the Johnson bounds for constant-weight codes [10].

Lemma 8: $A(n, d, w) \leq \lfloor \frac{n}{w} A(n-1, d, w-1) \rfloor$. □

In the next theorem we prove that our new bound is at least as good as the Johnson bound.

Theorem 5: $HL(n, \delta) \leq J(n, \delta)$.

Proof: We use Lemma 8 and obtain the following equalities and inequalities:

$$\frac{\binom{n}{\delta+1} - \binom{2\delta+1}{\delta} A(n, 2\delta+2, 2\delta+1)}{A(n, 2\delta+2, \delta+1)}$$

$$= \frac{\frac{n+1}{\delta+2}\left(\binom{n}{\delta+1} - \binom{2\delta+1}{\delta+1} A(n, 2\delta+2, 2\delta+1)\right)}{\frac{n+1}{\delta+2} A(n, 2\delta+2, \delta+1)}$$

$$\leq \frac{\binom{n+1}{\delta+2} - \binom{2\delta+2}{\delta+2} \frac{n+1}{2\delta+2} A(n, 2\delta+2, 2\delta+1)}{A(n+1, 2\delta+2, \delta+2)}$$

$$\leq \frac{\binom{n+1}{\delta+2} - \binom{2\delta+2}{\delta+2} A(n+1, 2\delta+2, 2\delta+2)}{A(n+1, 2\delta+2, \delta+2)}$$

and since

$$\frac{\binom{n}{\delta+1} - \binom{2\delta+1}{\delta} A(n, 2\delta+2, 2\delta+1)}{A(n, 2\delta+2, \delta+1)}$$

is always nonnegative we have that $HL(n, \delta) \leq J(n, \delta)$. □

In a similar way to the proof of Theorem 5 we prove the following result.

Lemma 9:

$$HL(n, \delta) \leq \frac{2^n}{\sum_{i=0}^{\delta} \binom{n}{i} + \frac{\binom{n}{\delta+1} - \binom{2\delta+1}{\delta} A(n, 2\delta+2, 2\delta+1)}{\frac{\delta+2}{n+1}\left\lfloor \frac{n+1}{\delta+2} \left\lfloor \frac{n}{\delta+1} \right\rfloor \right\rfloor}}. \quad (9)$$

Proof: As in Theorem 5, we obtain the following equalities and inequalities:

$$\frac{\binom{n}{\delta+1} - \binom{2\delta+1}{\delta} A(n, 2\delta+2, 2\delta+1)}{\frac{\delta+2}{n+1}\left\lfloor \frac{n+1}{\delta+2} \left\lfloor \frac{n}{\delta+1} \right\rfloor \right\rfloor}$$

$$= \frac{\frac{n+1}{\delta+2}\left(\binom{n}{\delta+1} - \binom{2\delta+1}{\delta+1} A(n, 2\delta+2, 2\delta+1)\right)}{\frac{n+1}{\delta+2}\frac{\delta+2}{n+1}\left\lfloor \frac{n+1}{\delta+2} A(n, 2\delta+2, \delta+1)\right\rfloor}$$

$$\leq \frac{\binom{n+1}{\delta+2} - \binom{2\delta+2}{\delta+2} \frac{n+1}{2\delta+2} A(n, 2\delta+2, 2\delta+1)}{A(n+1, 2\delta+2, \delta+2)}$$

$$\leq \frac{\binom{n+1}{\delta+2} - \binom{2\delta+2}{\delta+2} A(n+1, 2\delta+2, 2\delta+2)}{A(n+1, 2\delta+2, \delta+2)}.$$

Therefore,

$$HL(n, \delta) \leq \frac{2^n}{\sum_{i=0}^{\delta} \binom{n}{i} + \frac{\binom{n}{\delta+1} - \binom{2\delta+1}{\delta} A(n, 2\delta+2, 2\delta+1)}{\frac{\delta+2}{n+1}\left\lfloor \frac{n+1}{\delta+2} \left\lfloor \frac{n}{\delta+1} \right\rfloor \right\rfloor}}. \quad □$$

The next lemma will be used to substitute the denominator of (9).

Lemma 10: If $n = (\delta+1)((\delta+2)k+2)$, for any given $\delta > 0$ and $k > 0$ then

$$\frac{\delta+2}{n+1}\left\lfloor \frac{n+1}{\delta+2} \left\lfloor \frac{n}{\delta+1} \right\rfloor \right\rfloor = \frac{n}{\delta+1} - \frac{\delta}{n+1}.$$

Proof: The proof of the claim follows from the sequence of equalities given below

$$\frac{\delta+2}{n+1}\left\lfloor \frac{n+1}{\delta+2} \left\lfloor \frac{n}{\delta+1} \right\rfloor \right\rfloor$$

$$= \frac{\delta+2}{n+1}\left\lfloor \frac{n+1}{\delta+2}((\delta+2)k+2) \right\rfloor$$

$$= \frac{\delta+2}{n+1}\left\lfloor (n+1)k + \frac{2n}{\delta+2} + \frac{2}{\delta+2} \right\rfloor$$

$$= \frac{\delta+2}{n+1}\left\lfloor (n+1)k + 2(\delta+1)k + 3 + \frac{\delta}{\delta+2} \right\rfloor$$

$$= \frac{\delta+2}{n+1}((n+1)k + 2(\delta+1)k + 3)$$

$$= (\delta+2)k + 2 - \frac{\delta}{n+1} = \frac{n}{\delta+1} - \frac{\delta}{n+1}. \quad □$$

Finally, before our main theorem we need the following lemma.

Lemma 11: If $n = (\delta+1)((\delta+2)k+2)$, for any given $\delta > 0$ and $k > 0$ then

$$\binom{n}{\delta+1} - \binom{2\delta+1}{\delta} A(n, 2\delta+2, 2\delta+1) > 0.$$

Proof: Let $\mathcal{C}$ be an optimal constant-weight code of length n, weight $2\delta+1$, and minimum distance $2\delta+2$. Each word of weight $2\delta+1$ covers $\binom{2\delta+1}{\delta}$ words of weight $\delta+1$ within distance δ. Therefore,

$$\mathcal{H} = \binom{n}{\delta+1} - \binom{2\delta+1}{\delta} A(n, 2\delta+2, 2\delta+1)$$

is the total number of words of weight $\delta+1$ not covered by $\mathcal{C}$ within distance δ. It is well known (see [13, Ch. 2]) that $\mathcal{H} = 0$ implies that $\delta+1$ divides $n-\delta$. Since, $\delta+1$ does not divide $n-\delta$ it follows that $\mathcal{H} > 0$. □

We now intend to prove the main theorem of this section, i.e., for any given minimum distance greater than 2, there exist infinitely many lengths for which the new bound is better than the Johnson bound. In fact, we will show for these values that the difference between the two bounds is exponential with the length.

Theorem 6: For any given $\delta > 0$ and integer $k > 0$ let $n_k = (\delta+1)((\delta+2)k+2)$. There exist infinitely many values of k for which $HL(n_k, \delta) < \lfloor J(n_k, \delta) \rfloor$.

Proof: Using Lemmas 9 and 10 we have the expression at the top of the following page.

By Lemma 11, the numerator is a positive integer. The denominator is clearly a positive polynomial in n_k. Therefore, the expression tends to infinity as $k \to \infty$. □

As a simple example of the superiority of the new bound over the Johnson bound we can compare them for small values of d

$$\begin{aligned}
J(n_k, \delta) - HL(n_k, \delta) &= \frac{2^{n_k}}{\sum_{i=0}^{\delta}\binom{n_k}{i} + \frac{\binom{n_k}{\delta+1} - \binom{2\delta+1}{\delta}A(n_k, 2\delta+2, 2\delta+1)}{A(n_k, 2\delta+2, \delta+1)}} - \frac{2^{n_k}}{\sum_{i=0}^{\delta}\binom{n_k}{i} + \frac{\binom{n_k+1}{\delta+2} - \binom{2\delta+2}{\delta+2}A(n_k+1, 2\delta+2, 2\delta+2)}{A(n_k+1, 2\delta+2, \delta+2)}} \\
&\geq \frac{2^{n_k}}{\sum_{i=0}^{\delta}\binom{n_k}{i} + \frac{\binom{n_k}{\delta+1} - \binom{2\delta+1}{\delta}A(n_k, 2\delta+2, 2\delta+1)}{A(n_k, 2\delta+2, \delta+1)}} - \frac{2^{n_k}}{\sum_{i=0}^{\delta}\binom{n_k}{i} + \frac{\binom{n_k}{\delta+1} - \binom{2\delta+1}{\delta}A(n_k, 2\delta+2, 2\delta+1)}{\frac{\delta+2}{n_k+1}\left\lfloor \frac{n_k+1}{\delta+2}\left\lfloor \frac{n_k}{\delta+1}\right\rfloor\right\rfloor}} \\
&= 2^{n_k}\left(\frac{1}{\sum_{i=0}^{\delta}\binom{n_k}{i} + \frac{\binom{n_k}{\delta+1} - \binom{2\delta+1}{\delta}A(n_k, 2\delta+2, 2\delta+1)}{\left\lfloor\frac{n_k}{\delta+1}\right\rfloor}} - \frac{1}{\sum_{i=0}^{\delta}\binom{n_k}{i} + \frac{\binom{n_k}{\delta+1} - \binom{2\delta+1}{\delta}A(n_k, 2\delta+2, 2\delta+1)}{\left\lfloor\frac{n_k}{\delta+1}\right\rfloor - \frac{\delta}{n_k+1}}}\right) \\
&= 2^{n_k}\left(\frac{\frac{\binom{n_k}{\delta+1} - \binom{2\delta+1}{\delta}A(n_k, 2\delta+2, 2\delta+1)}{\left\lfloor\frac{n_k}{\delta+1}\right\rfloor - \frac{\delta}{n_k+1}} - \frac{\binom{n_k}{\delta+1} - \binom{2\delta+1}{\delta}A(n_k, 2\delta+2, 2\delta+1)}{\left\lfloor\frac{n_k}{\delta+1}\right\rfloor}}{\left(\sum_{i=0}^{\delta}\binom{n_k}{i} + \frac{\binom{n_k}{\delta+1} - \binom{2\delta+1}{\delta}A(n_k, 2\delta+2, 2\delta+1)}{\left\lfloor\frac{n_k}{\delta+1}\right\rfloor}\right)\left(\sum_{i=0}^{\delta}\binom{n_k}{i} + \frac{\binom{n_k}{\delta+1} - \binom{2\delta+1}{\delta}A(n_k, 2\delta+2, 2\delta+1)}{\left\lfloor\frac{n_k}{\delta+1}\right\rfloor - \frac{\delta}{n_k+1}}\right)}\right) \\
&\geq 2^{n_k}\left(\frac{\binom{n_k}{\delta+1} - \binom{2\delta+1}{\delta}A(n_k, 2\delta+2, 2\delta+1)}{\frac{n_k+1}{\delta}\left(\left\lfloor\frac{n_k}{\delta+1}\right\rfloor - \frac{\delta}{n_k+1}\right)\left\lfloor\frac{n_k}{\delta+1}\right\rfloor\left(\sum_{i=0}^{\delta}\binom{n_k}{i} + \frac{\binom{n_k}{\delta+1} - \binom{2\delta+1}{\delta}A(n_k, 2\delta+2, 2\delta+1)}{\left\lfloor\frac{n_k}{\delta+1}\right\rfloor - \frac{\delta}{n_k+1}}\right)^2}\right).
\end{aligned}$$

and n. In most cases, the new bound is superior. For example, $J(21, 9) = 181$ while $HL(21, 9) = 130$. Of course, the best upper bound for such small values of d and n is given by the linear programming bound discussed in the next section.

Finally, we ask which codes attain the new bound. Clearly, all perfect codes and nearly perfect codes attain this bound as it is at least as good as the Johnson bound. For some small values of n and d, we found that the new bound is equal to the Plotkin bound and there exist codes which attain them. We conjecture that there are no more codes which attain the new bound.

IV. The Linear Programming Bound

One of the most effective methods to obtain upper bounds on $A(n, d)$ for specific relatively small values of n and d is to apply the linear programming bound.

The *distance distribution* of an (n, M, d) code $\mathcal{C}$ is defined as the sequence

$$B_i = |\{(c_1, c_2) \in \mathcal{C} \times \mathcal{C}: d(c_1, c_2) = i\}|/|\mathcal{C}|$$

for $0 \leq i \leq n$. The linear programming bound was introduced by Delsarte [6], who showed that the distance distribution of any code satisfies

$$\sum_{i=0}^{n} B_i P_k(i) \geq 0$$

for $0 \leq k \leq n$, where $P_k(x)$ is the *Krawtchouk polynomial* of degree k, given by

$$P_k(x) = \sum_{j=0}^{k}(-1)^j\binom{x}{j}\binom{n-x}{k-j}.$$

By Lemma 1 it would be sufficient to consider only even values of d, while assuming that $B_i = 0$ except for $B_0 = 1$, B_d, $B_{d+2}, \ldots, B_{2\lfloor n/2\rfloor}$. This leads to the following theorem.

Theorem 7: For every positive even integer d

$$A(n, d) \leq 1 + \lfloor \max\left(B_d + B_{d+2} + \cdots + B_{2\lfloor n/2\rfloor}\right)\rfloor \quad (10)$$

subject to the constraints

$$\begin{aligned}
&0 \leq B_i \leq A(n, d, i), && i = d, d+2, \ldots, 2\lfloor n/2\rfloor \\
&\sum_{j=d/2}^{\lfloor n/2\rfloor} B_{2j}P_k(2j) \geq -\binom{n}{k}, && k = 1, 2, \ldots, \lfloor n/2\rfloor. \quad (11)
\end{aligned}$$

□

In some cases, the right-hand side of (11) can be slightly increased, as in the following theorem proved in [4].

Theorem 8: The distance distribution of an (n, M, d) code of odd size M satisfies

$$\sum_{j=d/2}^{\lfloor n/2\rfloor} B_{2j}P_k(2j) \geq \frac{1-M}{M}\binom{n}{k}, \qquad k = 1, 2, \ldots, \lfloor n/2\rfloor.$$

If $M \equiv 2(\mathrm{mod} 4)$, then there exists $l \in \{0, \ldots, n\}$ such that

$$\sum_{j=d/2}^{\lfloor n/2\rfloor} B_{2j}P_k(2j) \geq \frac{(2-M)\binom{n}{k} + 2P_k(l)}{M}, \quad k = 1, \ldots, \lfloor n/2\rfloor.$$

In some cases, some more constraints were added to obtain some specific bounds [4], [15], [8].

We will prove now that we can add two sets of inequalities to the set of constraints in the linear programming. These sets generalize some constraints given by Best [3].

If the minimum distance of the code is $d = 2\delta$, then no two codewords of weight $n-\delta$ can have common 0's and, therefore, there are at most $\lfloor n/\delta\rfloor$ codewords of weight $n-\delta$. Moreover, if there is a codeword of weight greater than $n-\delta$, then all the other words have weight $n-\delta-1$ or less. The next lemma is a first consequence of these observations.

Lemma 12: If a code $\mathcal{C}$ of length n and minimum Hamming distance $d = 2\delta$ contains a codeword of weight $n - \delta + j$ for some $j > 0$, then all the other codewords have weight $n - \delta - j$ or less. If a code $\mathcal{C}$ of length n and minimum Hamming distance $d=2\delta$ contains a codeword of weight $n-\delta$ then $A_{n-\delta} \leq \frac{n}{\delta}$. □

Averaging Lemma 12 over the codewords we get the following result.

Theorem 9: For a code $\mathcal{C}$ of length n and minimum Hamming distance $d = 2\delta$ we have

$$B_{n-\delta} + \left\lfloor \frac{n}{\delta} \right\rfloor \sum_{i<\delta} B_{n-i} \leq \left\lfloor \frac{n}{\delta} \right\rfloor . \tag{12}$$

□

In the same way we get the following two results.

Lemma 13: If a code $\mathcal{C}$ of length n and minimum Hamming distance $d = 2\delta$ contains a codeword of weight $n - \delta + j$ for some $0 < j < \delta$, then all the other codewords have weight $n - \delta - j$ or less, and furthermore

$$A_{n-\delta-j} \leq A(n - \delta + j,\, 2\delta,\, \delta + j). \qquad \square$$

Theorem 10: For a code C of length n and minimum distance $d = 2\delta$ we have for all i, $0 < i < \delta$

$$\begin{aligned} B_{n-\delta-i} &+ (A(n,\, 2\delta,\, \delta+i) - A(n-\delta+i,\, 2\delta,\, \delta+i))B_{n-\delta+i} \\ &+ A(n,\, 2\delta,\, \delta+i) \sum_{j>i} B_{n-\delta+j} \leq A(n,\, 2\delta,\, \delta+i). \end{aligned}$$

Proof: It suffices to prove that

$$\begin{aligned} A_{n-\delta-i} &+ (A(n,\, 2\delta,\, \delta+i) - A(n-\delta+i,\, 2\delta,\, \delta+i))A_{n-\delta+i} \\ &+ A(n,\, 2\delta,\, \delta+i) \sum_{j>i} A_{n-\delta+j} \leq A(n,\, 2\delta,\, \delta+i). \end{aligned}$$

If $A_{n-\delta+j} > 0$ for any $j > i$, then $A_{n-\delta-i} = A_{n-\delta+i} = 0$ and all the other summands are zeros, and there is nothing to prove. Assume, therefore, that $A_{n-\delta+j} = 0$ for all $j > i$. We know that $A_{n-\delta+i}$ is either 0 or 1: if it is 0, then we claim that $A_{n-\delta-i} \leq A(n,\, 2\delta,\, \delta+i)$, which is clear; if it is 1, then the claim becomes $A_{n-\delta-i} \leq A(n-\delta+i,\, 2\delta,\, \delta+i)$, which is correct by Lemma 13. □

We have used the new constraints of Theorems 9 and 10 in addition to the constraints of Theorems 7 and 8. For upper bounds of $A(n,\, d,\, w)$, we used the updated table in [1]. The new upper bounds which improve on the bounds in [2] are summarized in the following theorem (the values in the parentheses are the best bounds previously known).

Theorem 11:

- $A(21,\, 4) \leq 43\,688(43\,689)$
- $A(22,\, 4) \leq 87\,376(87\,378)$
- $A(23,\, 4) \leq 173\,015(173\,491)$
- $A(25,\, 4) \leq 599\,184(599\,185)$
- $A(26,\, 4) \leq 1\,198\,368(1\,198\,370)$
- $A(27,\, 4) \leq 2\,396\,736(2\,396\,740)$
- $A(28,\, 4) \leq 4\,793\,472(4\,793\,480)$
- $A(26,\, 6) \leq 84\,260(86\,132)$
- $A(27,\, 6) \leq 157\,285(162\,400)$
- $A(25,\, 8) \leq 5557(6425)$
- $A(26,\, 8) \leq 9672(10\,336)$
- $A(28,\, 8) \leq 32\,204(32\,205)$
- $A(26,\, 10) \leq 989(1029)$. □

Appendix

In the appendix, we will prove that the refinement of Johnson to his bound is good only for small values of n. This will be done by showing that each additional term in the refinement becomes negative as n tends to infinity. This will imply that our bound is at least as good as any refinement of the Johnson bound when n is large and better for infinitely many values of n for each δ. Moreover, we show refinements to our bound similar to the refinements of Johnson.

The refinements of the Johnson bound are given by

$$A(n,\, 2\delta+1) \leq \frac{2^n}{\sum\limits_{i=0}^{\delta} \binom{n}{i} + \sum\limits_{i=1}^{t} \frac{J_{\delta+i}}{A(n,\, 2\delta+2,\, \delta+i)}} \tag{13}$$

for each $t \leq \delta$, where $J_{\delta+i}$ is a lower bound on $H_{\delta+i}(\mathcal{C})$ given by

$$\begin{aligned} J_{\delta+i} = \binom{n}{\delta+i} &- T(\delta,\, i) \\ &- \binom{2\delta+2i-1}{\delta+i} A(n,\, 2\delta+2,\, 2\delta+2i-1) \end{aligned} \tag{14}$$

and $T(\delta,\, i) \geq 0$ (see [9]).

When $t = 1$, the bound (13) coincides with the Johnson bound. Thus, we have to prove that when n tends to infinity the value of $J_{\delta+i}$, $i \geq 2$, is nonpositive.

It is clear that

$$\binom{n}{\delta+i} \leq \frac{n^{\delta+i}}{(\delta+i)!} \tag{15}$$

and it is shown in [7] that

$$A(n,\, 2\delta,\, w) \geq \frac{n^{w-\delta+1}}{w!}, \qquad \text{as } n \to \infty.$$

Hence,

$$\begin{aligned} &\binom{2\delta+2i-1}{\delta+i} A(n,\, 2\delta+2,\, 2\delta+2i-1) \\ &\qquad \geq \frac{n^{\delta+i}}{(\delta+i)!} \cdot \frac{n^{i-1}}{(\delta+i-1)!}, \qquad \text{as } n \to \infty. \end{aligned} \tag{16}$$

From (14)–(16) we have that $J_{\delta+i}$, $i \geq 2$, becomes negative when n tends to infinity.

Now, we will show that our bound can be also improved similarly to the improvement of the Johnson bound. Very similar to Lemma 4 we can prove the following lemma.

Lemma 14:

$$H(\mathcal{C}_e,\, \delta+2) = H(\mathcal{C},\, \delta+1) + H(\mathcal{C},\, \delta+2). \qquad \square$$

Therefore, we can improve Lemma 7 to obtain

$$A(n,\,2\delta+1) \le \frac{2^n}{\sum\limits_{i=0}^{\delta}\binom{n}{i} + \frac{\binom{n+1}{\delta+2}-\binom{2\delta+2}{\delta+2}A(n+1,\,2\delta+2,\,2\delta+2)}{A(n+1,\,2\delta+2,\,\delta+2)} + \sum\limits_{i=3}^{t}\frac{J_{\delta+i}}{A(n,\,2\delta+2,\,\delta+i)}}.$$

Lemma 15:

$$H(C_e,\,\delta+2) = 2^n - A(n,\,2\delta+1)\sum_{i=0}^{\delta}\binom{n}{i} - \sum_{i=3}^{\delta}H(C,\,\delta+i).$$

□

A lower bound on $H(C,\,\delta+i)$ is given by

$$H(C,\,\delta+i) \ge A(n,\,2\delta+1)\,\frac{J_{\delta+i}}{A(n,\,2\delta+2,\,\delta+i)}.$$

Hence, we have

$$H(C_e,\,\delta+2) \le 2^n - A(n,\,2\delta+1) \cdot\left(\sum_{i=0}^{\delta}\binom{n}{i} + \sum_{i=3}^{\delta}\frac{J_{\delta+i}}{A(n,\,2\delta+2,\,\delta+i)}\right). \quad (17)$$

Therefore, we have the following theorem which improves on the new bound of Theorem 4 for small values of n similarly to the improvements of Johnson on his bound.

Theorem 12: The expression at the top of the page for each $t,\,3 \le t \le \delta$. □

Therefore, the only term in the denominator of the improvements to the Johnson bound which does not appear in the improvements to the new bound is $\frac{J_{\delta+2}}{A(n,\,2\delta+2,\,\delta+2)}$.

Acknowledgment

The authors wish to thank E. Agrell for very helpful discussions and two anonymous referees for their constructive comments.

References

[1] E. Agrell, A. Vardy, and K. Zeger, "Upper bounds for constant-weight codes," *IEEE Trans. Inform. Theory*, vol. 46, pp. 2373–2395, Nov. 2000.

[2] ——, "A table of upper bounds for binary codes," *IEEE Trans. Inform. Theory*, vol. 47, pp. 3004–3006, Nov. 2001.

[3] M. R. Best, "Binary codes with a minimum distance of four," *IEEE Trans. Inform. Theory*, vol. IT-26, pp. 738–742, Nov. 1980.

[4] 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*, vol. IT-24, pp. 81–93, Jan. 1978.

[5] G. Cohen, I. Honkala, S. Litsyn, and A. Lobstein, *Covering Codes*. Amsterdam, The Netherlands: North-Holland, 1997.

[6] Ph. Delsarte, "Bounds for unrestricted codes, by linear programming," *Philips Res. Repts.*, vol. 27, pp. 272–289, June 1972.

[7] R. L. Graham and N. J. A. Sloane, "Lower bounds for constant weight codes," *IEEE Trans. Inform. Theory*, vol. IT-26, pp. 37–43, Jan. 1980.

[8] I. Honkala, "Bounds for binary constant weight and covering codes," Licentiate thesis, Dept. Math., Univ. of Turku, Turku, Finland, Mar. 1987.

[9] S. M. Johnson, "A new upper bound for error-correcting codes," *IRE Trans. Inform. Theory*, vol. IT-8, pp. 203–207, Apr. 1962.

[10] ——, "Upper bounds for constant weight error-correcting codes," *Discr. Math.*, vol. 3, pp. 109–124, 1972.

[11] V. I. Levenshtein, "The application of Hadamard matrices to a problem in coding," *Probl. Kibern.*, vol. 5, pp. 123–136, 1961. English translation in *Probl. Cybernetics*, vol. 5, pp. 166–184, 1964.

[12] S. Litsyn, "An updated table of the best binary codes known," in *Handbook of Coding Theory*, V. S. Pless and W. C. Huffman, Eds. Amsterdam, The Netherlands: Elsevier, 1998, vol. 1, pp. 463–498.

[13] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*. Amsterdam, The Netherlands: North-Holland, 1977.

[14] M. Plotkin, "Binary codes with specified minimum distance," *IRE Trans. Inform. Theory*, vol. IT-6, pp. 445–450, Sept. 1960.

[15] C. L. N. van Pul, "On bounds on codes," Master's thesis, Dept. Math. and Comput. Science, Eindhoven Univ. Technol., Eindhoven, The Netherlands, Aug. 1982.