Advances in Mathematics of Communications
Volume 1, No. 2, 2007, 173–195
Web site: http://www.aimSciences.org

NEW UPPER BOUNDS ON CODES VIA ASSOCIATION SCHEMES AND LINEAR PROGRAMMING

Beniamin Mounits

Centrum voor Wiskunde en Informatica
Kruislaan 413, 1098 SJ
P.O. Box 94079
1090 GB Amsterdam, The Netherlands

Tuvi Etzion

Department of Computer Science
Technion, Haifa 32000, Israel

Simon Litsyn

School of Electrical Engineering
Tel Aviv University, Tel Aviv 69978, Israel

(Communicated by Eimear Byrne)

Abstract. Let $A(n,d)$ denote the maximum number of codewords in a binary code of length n and minimum Hamming distance d. Upper and lower bounds on $A(n,d)$ have been a subject for extensive research. In this paper we examine upper bounds on $A(n,d)$ as a special case of bounds on the size of subsets in metric association scheme. We will first obtain general bounds on the size of such subsets, apply these bounds to the binary Hamming scheme, and use linear programming to further improve the bounds. We show that the sphere packing bound and the Johnson bound as well as other bounds are special cases of one of the bounds obtained from association schemes. Specific bounds on $A(n,d)$ as well as on the sizes of constant weight codes are also discussed.

1. Introduction

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 usually obtained by constructions. For a survey on the known lower bounds the reader is referred to [12]. For a new asymptotic lower bound and a survey of previous results the reader is referred to [9].

In this work we consider upper bounds on $A(n,d)$. The most basic upper bound on $A(n,d)$, $d = 2e+1$ or $d = 2e+2$, is the sphere packing bound, also known as the Hamming bound:

$$A(n,d) \leq \frac{2^n}{\sum_{i=0}^{e} \binom{n}{i}} \ . \tag{1}$$

2000 *Mathematics Subject Classification:* Primary: 94B65; Secondary: 05E30.
Key words and phrases: Bounds on codes, association schemes, linear programming.
The research of the first and the second author was supported in part by grant no. 263/04 of the Israeli Science Foundation. The research of the third author was supported in part by grant no. 533/03 of the Israeli Science Foundation.

Johnson [10] has improved the sphere packing bound. In his theorem, Johnson 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:

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

In [15] a new bound was obtained:

$$A(n,2e+1) \leq \frac{2^n}{\sum_{i=0}^{e}\binom{n}{i} + \frac{\binom{n+1}{e+2}-\binom{2e+2}{e+2}A(n+1,2e+2,2e+2)}{A(n+1,2e+2,e+2)}} . \tag{3}$$

This bound 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. This bound will be called the improved Johnson bound. Considering distance $2e+1$ in the last two bounds is not restrictive as we have that $A(n+1,2e+2) = A(n,2e+1)$. This result is proved by considering the extended code, i.e., the code obtained by adding a parity check to each codeword. If an even parity is added, then the resulting code is an *even weight code*, i.e., a code whose codewords have even weight.

For given specific values of n and d, usually, to obtain a good upper bound on $A(n,d)$ one has to use linear programming [5, 3, 4, 15, 17].

In this paper we will use a more general approach to obtain bounds on $A(n,d)$. We will first obtain general bounds on the sizes of codes in any metric association scheme. We will translate these bounds to the binary Hamming scheme and obtain specific bounds for the binary Hamming scheme. These bounds depend on the distance distribution of the code and we optimize the bound by using linear programming.

The rest of the paper is organized as follows. In Section 2 we give the necessary background needed in association schemes. In Section 3 we present our main theorem that the inner distribution of the holes of the code is uniquely determined by the inner distribution of the code. This will lead to a sequence of upper bounds on subsets of the association scheme. We show that the sphere packing bound, the Johnson bound, as well as other bounds are special cases of one of these bounds. In Section 4 we derive some values on the number of holes with certain properties in the binary Hamming scheme . We combine these values with our main theorem to obtain some new upper bounds in the binary Hamming scheme. These bounds include some values from the inner distribution of the code. To further improve these bounds we use linear programming, optimizing the variables from the inner distribution. In Section 5 we summarize the new explicit bounds on $A(n,d)$ and $A(n,d,w)$.

2. Association schemes, codes, and holes

An *association scheme* with n *classes* consists of a finite set X of v points together with $n+1$ relations
$R_0, R_1, \ldots, R_n$ defined on X which satisfy:

- Each R_i is symmetric, i.e., $(x,y) \in R_i$ implies $(y,x) \in R_i$.
- For every $x, y \in X$, $(x,y) \in R_i$ for exactly one i.
- $R_0 = \{(x,x) \ : \ x \in X\}$ is the identity relation.

- If $(x, y) \in R_k$, then the number of $z \in X$ such that $(x, z) \in R_i$ and $(y, z) \in R_j$ is a constant $p^k_{i,j}$ (called *intersection number*) depending on i, j, k but not on the particular choice of x and y.

Let Γ be a connected graph with v vertices, with no loops or multiple edges, and let X be the set of vertices. The *distance* $d(x, y)$ between $x, y \in X$ is the number of edges in the shortest path between x and y. The maximum distance, say n, between any two vertices is called the *diameter* of the graph. The graph Γ is called *distance-regular* if, for any $x, y \in X$ with $d(x, y) = k$, the number of $z \in X$ such that $d(x, z) = i$ and $d(y, z) = j$ is a constant $p^k_{i,j}$ independent of the choice of x and y. Clearly, we obtain an association scheme with n classes from a distance-regular graph with diameter n. This scheme is called a *metric scheme*.

We also denote $p^0_{i,i} = v_i$ and $|X| = v$; v_i is called the *valency* of R_i and it is the number of points in X at distance i from any point $x \in X$. It is easy to verify that, for any association scheme, the following conditions hold:

$$p^i_{i,0} = 1,\ p^j_{i,0} = 0 \text{ and } p^0_{i,j} = 0 \text{ for } i \neq j. \tag{4}$$

$$\sum_{j=0}^{n} p^k_{i,j} = v_i \text{ and } p^k_{i,j} v_k = p^i_{k,j} v_i. \tag{5}$$

Let $(X, \mathcal{R})$ be a metric association scheme with a distance function $d(\cdot, \cdot)$ defined on a set X, and a set $\mathcal{R}$ with n relations, i.e. $\mathcal{R} = \{R_0, R_1, \cdots, R_n\}$, where $R_i = \{(x, y) \ :\ x, y \in X,\ d(x, y) = i\}$. By the triangle inequality we have that

$$p^k_{i,j} = 0, \text{ if } i + j < k \text{ or } i + k < j \text{ or } j + k < i. \tag{6}$$

A nonempty subset C of X is called a *code*. Let d be the *minimum distance* of C, i.e., $d = \min_{c_1, c_2 \in C} d(c_1, c_2)$. C is called an e-code for $e = \lfloor \frac{d-1}{2} \rfloor$, as it is capable of correcting e errors; C is also called an (n, d) code. For a point $x \in X$, $d(x, C)$ is the distance between x and C, i.e., $d(x, C) = \min_{c \in C} d(x, c)$. The *inner distribution* of C is the $(n + 1)$-tuple of rational numbers $\{A_0, A_1, \cdots, A_n\}$, where

$$A_i = \frac{1}{|C|} |R_i \cap (C \times C)|$$

is the average number of codewords which are at distance i from any given codeword $c \in C$. It is clear that $A_0 = 1$ and $A_i \geq 0,\ i = 1, 2, \cdots, n$. For any given $c \in C$, $A_i(c)$ denotes the number of codewords at distance i from c. Thus we have another useful expression for A_i:

$$\sum_{c \in C} A_i(c) = |R_i \cap (C \times C)| = |C| A_i\ . \tag{7}$$

The *e-sphere* about a point x consists of all points which are within distance e from x. These points are said to be *covered* by x. The *volume* of such a sphere, $V(n, e)$, is the size of the sphere, i.e.,

$$V(n, e) = \sum_{i=0}^{e} v_i\ .$$

For a given e-code C, we define the set of *holes* H of C to be $H = \{h \in X : d(h, C) > e\}$. We will be interested in the case $e \geq 1$. The non-normalized inner

distribution of H is the $(n+1)$-tuple of rational numbers $\{L_0, L_1, \cdots, L_n\}$, where

$$L_i = |R_i \cap (H \times H)|.$$

For any given $h \in H$, $L_i(h)$ denotes the number of holes at distance i from h.

We can partition X into two subsets H and E, where $E = \{x \in X \ : \ 0 \leq d(x, C) \leq e\}$ and $|E| = |C| \sum_{j=0}^{e} v_j$. Thus, we have

$$|H| = |X \setminus E| = v - |C| \sum_{j=0}^{e} v_j = v - |C| V(n, e). \tag{8}$$

3. Upper bounds derived from inner distribution

Let C be an e-code in a metric association scheme $(X, \mathcal{R})$. In this section we show a method to obtain upper bounds on the size of C. We will prove that the sphere packing bound, the Johnson bound, and the improved Johnson bound, are obtained by the new method. Moreover, this method can be applied with various sets of parameters. Each parameter set will lead to a new bound. Unfortunately, some of the bounds are weak, but fortunately some bounds can be used to obtain new bounds on the sizes of codes in some schemes. The bounds are obtained by computing the sum $\sum_{i=0}^{n} q_i L_i$, where $\{q_i\}$ is any sequence of real numbers, in two different ways. Different bounds can be obtained by using different sequences.

3.1. The main theorem.

In the first theorem we will prove that the inner distribution of the holes is uniquely determined by the inner distribution of C. Each value L_i, $0 \leq i \leq n$, is determined by the valency of the relation R_i, the size of X, the size of C, the size of an e-sphere, the inner distribution of the code, and the intersection numbers of the scheme.

Theorem 3.1. *If C is an e-code of X with inner distribution $\{A_i\}_{i=0}^{n}$, then for each i, $0 \leq i \leq n$,*

$$L_i = v_i \left(v - 2|C|V(n, e)\right) + |C| U(C, i) \ ,$$

where

$$U(C, i) = \sum_{k=0}^{n} \sum_{\ell=0}^{n} \sum_{m=0}^{e} \sum_{j=0}^{e} p_{\ell,m}^{k} p_{i,j}^{\ell} A_k \ . \tag{9}$$

Proof. The number of ordered pairs of points from X at distance i is

$$|R_i \cap (X \times X)| = \sum_{x \in X} v_i = v v_i. \tag{10}$$

Since X can be partitioned into two subsets E and H, it follows that $X \times X$ can be partitioned into two subsets $E \times E$ and $X \times H \cup H \times X$.

Therefore, we have an alternative way to compute $|R_i \cap (X \times X)|$.

- For a given k, $0 \leq k \leq n$, let $c, c' \in C$ be two codewords such that $d(c, c') = k$. First, we count the number of pairs (x, x') such that $d(c, x) = m$, $d(c', x') = j$, $0 \leq m, j \leq e$, and $d(x, x') = i$. Clearly, $x, x' \in E$. For a given ℓ, $0 \leq \ell \leq n$, the number of points $x \in E$ such that $d(c, x) = m$ and $d(c', x) = \ell$ is $p_{\ell,m}^{k}$. The number of points $x' \in E$ such that $d(x, x') = i$ and $d(c', x') = j$ is $p_{i,j}^{\ell}$. Hence, the number of pairs (x, x') is $\sum_{\ell=0}^{n} p_{\ell,m}^{k} p_{i,j}^{\ell}$. Thus, the number of pairs (x, x') such that $0 \leq d(c, x) \leq e$ and $0 \leq d(c', x') \leq e$ is

$$\sum_{m=0}^{e}\sum_{j=0}^{e}\sum_{\ell=0}^{n} p_{\ell,m}^{k} p_{i,j}^{\ell} \ .$$

Summing on all pairs $c, c' \in C$, and by using (7) we obtain

$$|R_i \cap (E \times E)| = \sum_{c\in C}\sum_{k=0}^{n} A_k(c) \sum_{m=0}^{e}\sum_{j=0}^{e}\sum_{\ell=0}^{n} p_{\ell,m}^{k} p_{i,j}^{\ell} = |C| \sum_{k=0}^{n}\sum_{\ell=0}^{n}\sum_{m=0}^{e}\sum_{j=0}^{e} p_{\ell,m}^{k} p_{i,j}^{\ell} A_k \ . \tag{11}$$

- One can easily verify that

$$|\{(h,x) \in H \times X \ : \ d(h,x) = i\}| = \sum_{h\in H} v_i$$

and for any given sets A, B, D such that $B \subseteq A$

$$|D \cap (A \times B \cup B \times A)| = |D \cap (A \times B)| + |D \cap (B \times A)| - |D \cap (B \times B)|.$$

Therefore,

$$|R_i \cap (X \times H \cup H \times X)| = 2\sum_{h\in H} v_i - L_i = 2|H|v_i - L_i. \tag{12}$$

From (10)-(12) it follows that

$$vv_i = |C| \sum_{k=0}^{n}\sum_{\ell=0}^{n}\sum_{m=0}^{e}\sum_{j=0}^{e} p_{\ell,m}^{k} p_{i,j}^{\ell} A_k + 2|H|v_i - L_i.$$

The claim of the theorem follows after substituting (8) in $|H|$ and simple algebraic manipulations. □

Corollary 1. *Let C be an e-code with inner distribution $\{A_i\}_{i=0}^{n}$ and let $\{q_i\}_{i=0}^{n}$ be a sequence of real numbers. Then*

$$\sum_{i=0}^{n} q_i L_i = v \sum_{i=0}^{n} q_i v_i + |C| \sum_{i=0}^{n} q_i \left(U(C,i) - 2V(n,e)v_i\right). \tag{13}$$

where $U(C,i)$ is given by (9).

3.2. Generalization of the known bounds. First, we will prove that some of the well known bounds in the binary Hamming scheme can be obtained from Corollary 1. Moreover, these bounds are now generalized to any metric association scheme as our corollary is not specific to any scheme. First, we will give some general results. For a hole h let $NC(h,C,k)$ be the number of codewords in C at distance k from h.

Lemma 3.2. *For each i, $0 \le i \le n$, the following holds*

$$L_i = \sum_{h\in H} \left(v_i - \sum_{k=e+1}^{e+i} NC(h,C,k) \sum_{j=0}^{e} p_{i,j}^{k} \right).$$

Proof. The number of points at distance i from hole h in X is v_i. The number of points at distance i from h in E is $\sum_{k=e+1}^{e+i} NC(h,C,k) \sum_{j=0}^{e} p_{i,j}^{k}$. Hence, the number of points at distance i from h in H is $v_i - \sum_{k=e+1}^{e+i} NC(h,C,k) \sum_{j=0}^{e} p_{i,j}^{k}$. □

Given a sequence $\{q_i\}$, by using Lemma 3.2 and (8) we estimate $\sum_{i=0}^{n} q_i L_i$ in the following way.

$$\begin{aligned}\sum_{i=0}^{n} q_i L_i &= \sum_{i=0}^{n} q_i \sum_{h\in H}\left(v_i - \sum_{k=e+1}^{e+i} NC(h,C,k)\sum_{j=0}^{e} p_{i,j}^{k}\right)\\ &= \sum_{h\in H}\left(\sum_{i=0}^{n} q_i v_i - \sum_{i=0}^{n} q_i \sum_{k=e+1}^{e+i} NC(h,C,k)\sum_{j=0}^{e} p_{i,j}^{k}\right)\\ &\geq (v-|C|V(n,e))\left(\sum_{i=0}^{n} q_i v_i - \xi(C,\{q_i\})\right), \qquad (14)\end{aligned}$$

where

$$\xi(C,\{q_i\}) = \max_{h\in H}\left\{\sum_{i=0}^{n} q_i \sum_{k=e+1}^{e+i} NC(h,C,k)\sum_{j=0}^{e} p_{i,j}^{k}\right\}. \qquad (15)$$

By combining (13) and (14) we obtain

Theorem 3.3. *If C is an e-code with inner distribution $\{A_i\}_{i=0}^{n}$, then*

$$|C| \leq \frac{v}{V(n,e) + \frac{\sum_{i=0}^{n} q_i (V(n,e)v_i - U(C,i))}{\xi(C,\{q_i\})}} \qquad (16)$$

provided $\xi(C,\{q_i\})$ is not zero, where $\xi(C,\{q_i\})$ is given by (15) and $U(C,i)$ is given by (9).

Lemma 3.4. *For any given e-code C with inner distribution $\{A_i\}_{i=0}^{n}$,*

$$U(C,0) = V(n,e)\ ,$$

$$U(C,1) = V(n,e)v_1 - p_{1,e}^{e+1} v_{e+1} + p_{1,e}^{e+1} p_{e+1,e}^{2e+1} A_{2e+1}\ , \qquad (17)$$

$$\begin{aligned}U(C,2) &= V(n,e)v_2 - (p_{2,e-1}^{e+1} + p_{2,e}^{e+1})v_{e+1} - p_{2,e}^{e+2} v_{e+2}\\ &\quad + \left(p_{e+1,e}^{2e+1}\left(p_{2,e-1}^{e+1} + p_{2,e}^{e+1}\right) + \left(p_{e+2,e-1}^{2e+1} + p_{e+2,e}^{2e+1}\right) p_{2,e}^{e+2}\right) A_{2e+1}\\ &\quad + p_{e+2,e}^{2e+2} p_{2,e}^{e+2} A_{2e+2}\ . \qquad (18)\end{aligned}$$

Proof. Since $A_0 = 1$, $A_k = 0$ for $1 \leq k \leq 2e$, the claim follows by evaluating (9) using (4)-(6). □

3.2.1. *The sphere packing bound.* The sphere packing bound is given in the following theorem.

Theorem 3.5. *For any given e-code C,*

$$|C| \leq \frac{v}{V(n,e)}\ .$$

Proof. The result is obtained by taking the sequence $q_0 = 1$ and $q_i = 0$ for $1 \leq i \leq n$ in Corollary 1. □

3.2.2. *The Johnson bound.* The Johnson bound is an improvement of the sphere packing bound. It was given in [10] for the binary Hamming scheme and in [7] for general distance regular graphs. The Johnson bound is given in the following theorem.

Theorem 3.6. *For any given $(n, 2e+1)$ code C with inner distribution $\{A_i\}_{i=0}^n$,*

$$|C| \le \frac{v}{V(n,e) + \frac{v_{e+1} - p_{e+1,e}^{2e+1} A_{2e+1}}{\max_{h \in H}\{NC(h,C,e+1)\}}} \ . \tag{19}$$

Proof. Let $q_0 = 0$, $q_1 = 1$ and $q_i = 0$ for $2 \le i \le n$. Since in (15), $q_i \ne 0$ only for $i = 1$ and $p_{i,j}^k \ne 0$ only for $i = 1$, $j = e$, and $k = e+1$, by (6), we have

$$\xi(C, \{q_i\}) = p_{1,e}^{e+1} \max_{h \in H} \{NC(h, C, e+1)\} \ . \tag{20}$$

The theorem is obtained by substituting (17) and (20) in (16). □

For the binary Hamming scheme, by substituting

$$A_{2e+1} \le A(n, 2e+2, 2e+1)$$

and

$$\max_{h \in H} \{NC(h, C, e+1)\} \le A(n, 2e+2, e+1)$$

in (19) we obtain the Johnson bound (2).

3.2.3. *Improved Johnson bound.* The improved Johnson bound is given in the following theorem.

Theorem 3.7. *For any given $(n, 2e+1)$ code C with inner distribution $\{A_i\}_{i=0}^n$,*

$$|C| \le \frac{v}{V(n,e) + \frac{v_{e+1} + v_{e+2} - \gamma}{\max_{h \in H}\{NC(h,C,e+1) + NC(h,C,e+2)\}}} \ , \tag{21}$$

where

$$\gamma = (p_{e+1,e}^{2e+1} + p_{e+2,e-1}^{2e+1} + p_{e+2,e}^{2e+1}) A_{2e+1} + p_{e+2,e}^{2e+2} A_{2e+2} \ .$$

Proof. Let $q_0 = 0$, $q_1 = \frac{p_{2,e}^{e+2} - p_{2,e-1}^{e+1} - p_{2,e}^{e+1}}{p_{1,e}^{e+1}}$, $q_2 = 1$ and $q_i = 0$ for $3 \le i \le n$. Again, since only q_1 and q_2 are nonzero, by (15) we have

$$\xi(C, \{q_i\}) = p_{2,e}^{e+2} \max_{h \in H} \{NC(h, C, e+1) + NC(h, C, e+2)\} \ . \tag{22}$$

The theorem is obtained by substituting (17), (18), and (22) in (16). □

For the binary Hamming scheme we have $\gamma = \binom{2e+2}{e+2}(A_{2e+1} + A_{2e+2})$, $v_{e+1} + v_{e+2} = \binom{n+1}{e+2}$, and $\max_{h \in H} \{NC(h, C, e+1) + NC(h, C, e+2)\} \le A(n+1, 2e+2, e+2)$. By substituting in (21) we obtain

$$|C| \le \frac{2^n}{\sum_{i=0}^e \binom{n}{i} + \frac{\binom{n+1}{e+2} - \binom{2e+2}{e+2}(A_{2e+1} + A_{2e+2})}{A(n+1, 2e+2, e+2)}} \ . \tag{23}$$

By substituting $A_{2e+1} + A_{2e+2} \le A(n+1, 2e+2, 2e+2)$ in (23) we obtain the improved Johnson bound (3).

4. New bounds in the binary Hamming scheme

In this section we will apply Corollary 1 to obtain new bounds in the binary Hamming scheme. In any sequence $\{q_i\}$ that we have used for the known bounds the nonzero elements had small indices. Now, we will use sequences in which the nonzero elements have large indices. We will obtain new bounds on the size of a code which depend on a few coefficients from inner distribution of the code. For a more explicit analytic bound we will use linear programming to obtain bounds on these coefficients. The "code" which attains the linear programming bound on these coefficients might be smaller or larger than the explicit analytic bound. If this is the case then we will try to improve the analytic bound by using linear programming again with an additional constraint.

The computations that will be done in this section involve computing some of the intersection numbers in the binary Hamming scheme. It is easy to see that, for the binary Hamming scheme,

$$p_{i,j}^k = \begin{cases} \binom{k}{\frac{i-j+k}{2}}\binom{n-k}{\frac{i+j-k}{2}} & \text{if } i+j-k \text{ is even,} \\ 0 & \text{if } i+j-k \text{ is odd.} \end{cases}$$

4.1. Bounds derived from inner distribution.

In this subsection we will use Corollary 1 with sequences whose nonzero elements have large indices. First, for a given t, $0 \le t \le e$, we will compute the number of holes, for which there is a codeword at distance $n-t$. Let

$$K_{n-t} = \{h \in H \ : \ NC(h, C, n-t) = 1\}$$

be the set of holes, for which there is a codeword at distance $n-t$. Note that, for any hole $h \in H$, we have $NC(h, C, n-t) \in \{0, 1\}$, where $0 \le t \le e$.

Lemma 4.1. *For each t, $0 \le t \le e$,*

$$|K_{n-t}| = |C| \left(v_{n-t} - \sum_{i=0}^{e+t} A_{n-i} \sum_{j=0}^{e} p_{n-t,j}^{n-i} \right). \tag{24}$$

Proof. The number of vectors at distance $n-t$ from a codeword c is v_{n-t}. Similar to the proof of Lemma 3.2, $\sum_{i=0}^{e+t} A_{n-i}(c) \sum_{j=0}^{e} p_{n-t,j}^{n-i}$ is the number of vectors in E at distance $n-t$ from c. Hence,

$$|K_{n-t}| = \sum_{c \in C} \left(v_{n-t} - \sum_{i=0}^{e+t} A_{n-i}(c) \sum_{j=0}^{e} p_{n-t,j}^{n-i} \right) = |C| \left(v_{n-t} - \sum_{i=0}^{e+t} A_{n-i} \sum_{j=0}^{e} p_{n-t,j}^{n-i} \right).$$

□

Theorem 4.2. *If C is an $(n, 2e+1)$ code with inner distribution $\{A_i\}_{i=0}^n$ then*

$$|C| \le \frac{2^n}{2\sum_{i=0}^{e}\binom{n}{i} + \frac{\binom{n}{e}\left(\frac{n-e}{e+1} - \left\lfloor \frac{n-e}{e+1} \right\rfloor\right)}{\left\lfloor \frac{n}{e+1} \right\rfloor} - \frac{S_1(e,n)}{(e+1)\left\lfloor \frac{n}{e+1} \right\rfloor}},$$

where

$$S_1(e,n) = \sum_{i=n-1}^{n} U(C,i) - (e+1)\left(\frac{n+1}{e+1} - \lfloor\frac{n}{e+1}\rfloor\right)\sum_{t=0}^{e-1}\sum_{i=0}^{e+t} A_{n-i}\sum_{j=0}^{e} p_{n-t,j}^{n-i}$$
$$-(e+1)\left(\lfloor\frac{n+1}{e+1}\rfloor - \lfloor\frac{n}{e+1}\rfloor\right)\sum_{i=0}^{2e} A_{n-i}\sum_{j=0}^{e} p_{n-e,j}^{n-i}\ ,$$

where $U(C,n-1)$ and $U(C,n)$ are given by (9).

Proof. For any given hole h we distinguish between three mutually exclusive cases:

1. If there exists a codeword c such that $n-(e-1) \le d(c,h) \le n$ then

$$L_{n-1}(h) + L_n(h) = 0\ . \tag{25}$$

2. Assume there exists a codeword c such that $d(c,h) = n-e$. Without loss of generality we can assume that h is the all-ones vector and hence c is a codeword with weight e. Therefore, the all-zeroes vector is not a hole and there are at most $n-e$ potential holes with weight one. These potential holes can be covered only by codewords with weight $e+1$. On these $n-e$ coordinates there are at most $A(n-e,2e+2,e+1) = \lfloor\frac{n-e}{e+1}\rfloor$ codewords with weight $e+1$, each one covers exactly $e+1$ potential holes with weight one. Therefore,

$$L_{n-1}(h) + L_n(h) \ge n-e-(e+1)\lfloor\frac{n-e}{e+1}\rfloor\ . \tag{26}$$

3. If there is no codeword c such that $n-e \le d(c,h) \le n$ then similarly we have

$$L_{n-1}(h) + L_n(h) \ge n+1-(e+1)A(n,2e+2,e+1) = n+1-(e+1)\lfloor\frac{n}{e+1}\rfloor. \tag{27}$$

We sum (25), (26), and (27), over all the holes and use (24) to obtain

$$L_{n-1}+L_n = \sum_{h\in H}(L_{n-1}(h)+L_n(h)) \ge \sum_{t=0}^{e-1}|K_{n-t}|\cdot 0 + |K_{n-e}|\cdot\left(n-e-(e+1)\lfloor\frac{n-e}{e+1}\rfloor\right)$$
$$+\left(|H| - \sum_{t=0}^{e}|K_{n-t}|\right)\cdot\left(n+1-(e+1)\lfloor\frac{n}{e+1}\rfloor\right)$$
$$= |C|\left(\binom{n}{e} - \sum_{i=0}^{2e} A_{n-i}\sum_{j=0}^{e} p_{n-e,j}^{n-i}\right)\left(n-e-(e+1)\lfloor\frac{n-e}{e+1}\rfloor\right)$$
$$+\left(2^n - |C|V(n,e) - |C|\sum_{t=0}^{e}\left(\binom{n}{t} - \sum_{i=0}^{e+t} A_{n-i}\sum_{j=0}^{e} p_{n-t,j}^{n-i}\right)\right)\left(n+1-(e+1)\lfloor\frac{n}{e+1}\rfloor\right)\ .$$

By Corollary 1, we have

$$L_{n-1}+L_n = 2^n(n+1) + |C|\left(U(C,n-1)+U(C,n)-2V(n,e)(n+1)\right),$$

and hence

$$2^n(e+1)\lfloor\frac{n}{e+1}\rfloor \ge |C|(2V(n,e)(n+1) - U(C,n-1) - U(C,n) + \binom{n}{e}\left(n-e-(e+1)\lfloor\frac{n-e}{e+1}\rfloor\right)$$
$$-2V(n,e)\left(n+1-(e+1)\lfloor\frac{n}{e+1}\rfloor\right) - \sum_{i=0}^{2e} A_{n-i}\sum_{j=0}^{e} p_{n-e,j}^{n-i}\left(n-e-(e+1)\lfloor\frac{n-e}{e+1}\rfloor\right)$$
$$+\sum_{t=0}^{e}\sum_{i=0}^{e+t} A_{n-i}\sum_{j=0}^{e} p_{n-t,j}^{n-i}\left(n+1-(e+1)\lfloor\frac{n}{e+1}\rfloor\right))$$

$$= |C|(2V(n,e)(e+1)\lfloor\frac{n}{e+1}\rfloor + (e+1)\binom{n}{e}\left(\frac{n-e}{e+1} - \lfloor\frac{n-e}{e+1}\rfloor\right)$$

$$-U(C,n-1) - U(C,n) + \sum_{t=0}^{e-1}\sum_{i=0}^{e+t} A_{n-i}\sum_{j=0}^{e} p_{n-t,j}^{n-i}\left(\frac{n+1}{e+1} - \lfloor\frac{n}{e+1}\rfloor\right)(e+1)$$

$$+\sum_{i=0}^{2e} A_{n-i}\sum_{j=0}^{e} p_{n-e,j}^{n-i}\left(e+1+(e+1)\lfloor\frac{n-e}{e+1}\rfloor - (e+1)\lfloor\frac{n}{e+1}\rfloor\right)).$$

The theorem follows now by elementary algebraic manipulation on the last formula. □

Corollary 2. *If n is even and C is an $(n,3)$ code with inner distribution $\{A_i\}_{i=0}^n$ then*

$$|C| \le \frac{2^n}{2n+3-\frac{S_1(1,n)}{n}} ,$$

where

$$S_1(1,n) = 6(A_{n-3}+A_{n-2}) + 3n(A_{n-1}+A_n) .$$

Theorem 4.3. *If C is an $(n,2e+1)$ code with inner distribution $\{A_i\}_{i=0}^n$ then*

$$|C| \le \frac{2^n}{2\sum_{i=0}^{e}\binom{n}{i} + \phi - \frac{S_2(e,n)}{\binom{e+2}{2}A(n+1,2e+2,e+2)}} ,$$

where

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

$$S_2(e,n) = \sum_{i=n-2}^{n} U(C,i) - \left(V(n,2) - \binom{e+2}{2}A(n+1,2e+2,e+2)\right)\sum_{t=0}^{e-2}\sum_{i=0}^{e+t} A_{n-i}\sum_{j=0}^{e} p_{n-t,j}^{n-i}$$

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

$$\times \sum_{t=e-1}^{e}\sum_{i=0}^{e+t} A_{n-i}\sum_{j=0}^{e} p_{n-t,j}^{n-i} ,$$

where $U(C,n-2)$, $U(C,n-1)$, and $U(C,n)$ are given by (9).

Proof. For any given hole h we distinguish between four mutually exclusive cases:

1. If there exists a codeword $c \in C$ such that $n-(e-2) \le d(c,h) \le n$ then

$$L_{n-2}(h) + L_{n-1}(h) + L_n(h) = 0 . \tag{28}$$

2. If there exists a codeword $c \in C$ such that $d(c,h) = n-e+1$ then

$$L_{n-2}(h)+L_{n-1}(h)+L_n(h) \ge \binom{n-e+1}{2} - \binom{e+2}{2}A(n-e+1,2e+2,e+2). \tag{29}$$

3. Assume there exists a codeword $c \in C$ such that $d(c,h) = n-e$. Without loss of generality we can assume that h is the all-ones vector and hence c is a codeword with weight e. Therefore, the all-zeroes vector is not a hole and there are at most $n-e$ potential holes with weight one and $\binom{n-e}{2}$ potential holes with weight two. A codeword with weight $e+2$ covers $\binom{e+2}{2}$ potential holes with weight two. There are $NC(h,C,n-(e+2))$ such codewords and

they cover $\binom{e+2}{2}NC(h,C,n-(e+2))$ potential holes. Similarly codewords with weight $e+1$ cover $(e+1+\binom{e+1}{2})NC(h,C,n-(e+1))$ potential holes with weight less or equal two. Note, that if $c' \in C$ has weight $e+1$ or $e+2$ then its support is disjoint from the support of c since $d(c,c') > 2e$. Therefore, $NC(h,C,n-e-1)+NC(h,C,n-e-2) \leq A(n-e+1,2e+2,e+2)$. Since no other codewords can cover holes with weight less or equal two, we have that

$$L_{n-2}(h)+L_{n-1}(h)+L_n(h) \geq \binom{n-e+1}{2} - \binom{e+2}{2} A(n-e+1,2e+2,e+2)\,. \tag{30}$$

4. If there is no codeword c such that $n-e \leq d(c,h) \leq n$ then similarly we have

$$L_{n-2}(h)+L_{n-1}(h)+L_n(h) \geq 1+\binom{n+1}{2} - \binom{e+2}{2} A(n+1,2e+2,e+2). \tag{31}$$

Similar to the proof of Theorem 4.2 we sum (28), (29), (30), and (31), over all the holes, use (24) to obtain

$$L_{n-2}+L_{n-1}+L_n = \sum_{h\in H} (L_{n-2}(h)+L_{n-1}(h)+L_n(h)) \geq$$

$$|C| \sum_{t=e-1}^{e} \left(\binom{n}{t} - \sum_{i=0}^{e+t} A_{n-i} \sum_{j=0}^{e} p_{n-t,j}^{n-i} \right) \left(\binom{n-e+1}{2} - \binom{e+2}{2} A(n-(e-1),2e+2,e+2) \right)$$

$$+ \left(2^n - |C|V(n,e) - |C| \sum_{t=0}^{e} \left(\binom{n}{t} - \sum_{i=0}^{e+t} A_{n-i} \sum_{j=0}^{e} p_{n-t,j}^{n-i} \right) \right)$$

$$\times \left(1 + \binom{n+1}{2} - \binom{e+2}{2} A(n+1,2e+2,e+2) \right).$$

By Corollary 1, we have

$$L_{n-2}+L_{n-1}+L_n = 2^n \left(\binom{n+1}{2} + 1 \right) + |C| \left(\sum_{i=n-2}^{n} U(C,i) - 2V(n,e)(\binom{n+1}{2}+1)) \right),$$

and hence as in the proof of Theorem 4.2 we have

$$2^n \binom{e+2}{2} A(n+1,2e+2,e+2) \geq |C|(2V(n,e)\binom{e+2}{2} A(n+1,2e+2,e+2) - \sum_{i=n-2}^{n} U(C,i)$$

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

$$+ \sum_{t=0}^{e-2} \sum_{i=0}^{e+t} A_{n-i} \sum_{j=0}^{e} p_{n-t,j}^{n-i} \left(1+n+\binom{n}{2} - \binom{e+2}{2} A(n+1,2e+2,e+2) \right)$$

$$+ \sum_{t=e-1}^{e} \sum_{i=0}^{e+t} A_{n-i} \sum_{j=0}^{e} p_{n-t,j}^{n-i} (1+e(n-e)+\binom{e+1}{2} - \binom{e+2}{2} (A(n+1,2e+2,e+2)$$

$$-A(n-e+1,2e+2,e+2)))).$$

The theorem follows now by elementary algebraic manipulation on the last formula. □

Corollary 3. *If C is an $(n,3)$ code with inner distribution $\{A_i\}_{i=0}^n$ then*

$$|C| \leq \frac{2^n}{2n+2+\frac{(n+1)\left(\frac{n(n-1)}{6}-A(n,4,3)\right)}{A(n+1,4,3)}-\frac{S_2(1,n)}{3A(n+1,4,3)}} \ ,$$

where

$$S_2(1,n) = 12(A_{n-4}+A_{n-3})+(3(n-1)+6(A(n+1,4,3)-A(n,4,3)))(A_{n-2}+A_{n-1}) \\ +3(n+1)(A(n+1,4,3)-A(n,4,3))A_n \ .$$

4.2. THE LINEAR PROGRAMMING BOUND. One of the most common methods to obtain upper bounds on $A(n,d)$ is to apply the linear programming bound of Delsarte [5, 6]. Likewise, the general technique of linear programming can be used to bound any combination of the coefficients of the inner distribution as will be done in the next subsection. We will proceed in describing the method similarly to the description in Best and Brouwer [3].

Recall that, throughout this section, we only deal with the binary Hamming scheme. If C is an $(n,2e+1)$ code with inner distribution $\{A_i\}_{i=0}^n$, the non-normalized *dual inner distribution* $\{B_i\}_{i=0}^n$ is defined by

$$B_k = \sum_{i=0}^{n} A_i P_k(i), \tag{32}$$

where

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

is the Krawtchouk polynomial of degree k. It was proved by Delsarte [6] that $B_k \geq 0$ for $0 \leq k \leq n$. Since the Krawtchouk polynomials satisfy the following orthogonality relation [11]

$$\sum_{k=0}^{n} P_k(i)P_j(k) = 2^n \delta_{ij} \ ,$$

we have (see [3])

$$\sum_{k=0}^{n} B_k P_j(k) = \sum_{k=0}^{n}\sum_{i=0}^{n} A_i P_k(i) P_j(k) = \sum_{i=0}^{n} A_i \sum_{k=0}^{n} P_k(i)P_j(k) = 2^n A_j \ . \tag{33}$$

Since $P_0(i) \equiv 1$ it follows from (32) that

$$B_0 = \sum_{i=0}^{n} A_i = |C| \ .$$

Therefore, by (33) and since $A_j = 0$ for $1 \leq j \leq 2e$, $0 \leq A_j \leq A(n,2e+2,j)$ for $2e+1 \leq j \leq n$, we have:

Theorem 4.4.

$$A(n,2e+1) \leq \lfloor max\{B_0\} \rfloor \ ,$$

subject to constraints

$$\sum_{k=0}^{n} B_k = 2^n,$$

$$\sum_{k=0}^{n} B_k P_j(k) = 0 \ for\ 1 \le j \le 2e,$$

$$0 \le \sum_{k=0}^{n} B_k P_j(k) \le 2^n A(n, 2e+2, j) \ for\ 2e+1 \le j \le n.$$

and $B_k \ge 0$ *for* $0 \le k \le n$.

If C is an even weight code, we can reduce the number of variables and linear constraints from $n+1$ to $\lceil (n+1)/2 \rceil$, using the following properties of the Krawtchouk polynomials [11]:

$$P_{n-k}(i) = (-1)^i P_k(i) \tag{34}$$

$$P_k(i) = (-1)^k P_k(n-i). \tag{35}$$

Since in the even weight code $A_i = 0$ for odd i we obtain from (32) and (34)

$$B_{n-k} = \sum_{i=0}^{\lfloor n/2 \rfloor} A_{2i} P_{n-k}(2i) = \sum_{i=0}^{\lfloor n/2 \rfloor} A_{2i} P_k(2i) = B_k. \tag{36}$$

If n is an odd integer then by (33), (36), and (35) we have

$$\begin{aligned} 2^n A_k = \sum_{j=0}^{n} B_j P_k(j) &= \sum_{j=0}^{(n-1)/2} B_j P_k(j) + \sum_{j=(n+1)/2}^{n} B_j P_k(j) \\ &= \sum_{j=0}^{(n-1)/2} B_j (P_k(j) + P_k(n-j)) = (1 + (-1)^k) \sum_{j=0}^{(n-1)/2} B_j P_k(j)\ . \end{aligned}$$

Similarly, if n is an even integer, then

$$\begin{aligned} 2^n A_k = \sum_{j=0}^{n} B_j P_k(j) &= \sum_{j=0}^{(n-2)/2} B_j P_k(j) + B_{n/2} P_k(n/2) + \sum_{j=(n+2)/2}^{n} B_j P_k(j) \\ &= (1 + (-1)^k) \sum_{j=0}^{n/2} \hat{B}_j P_k(j), \end{aligned}$$

where $\hat{B}_j = B_j$ for $0 \le j \le (n-2)/2$ and $\hat{B}_{n/2} = \frac{1}{2} B_{n/2}$. Therefore we have

Lemma 4.5. *If C is an $(n, 2e+2)$ even weight code with inner distribution $\{A_i\}_{i=0}^n$, then for any integer k, $0 \le k \le \lfloor n/2 \rfloor$,*

$$\sum_{j=0}^{\lfloor n/2 \rfloor} \hat{B}_j P_{2k}(j) = 2^{n-1} A_{2k},$$

where $\hat{B}_j = B_j$ for $0 \le j \le \lfloor n/2 \rfloor - 1$ and

$$\hat{B}_{\lfloor n/2 \rfloor} = \begin{cases} B_{(n-1)/2} & \text{if } n \text{ is odd}\ , \\ \frac{1}{2} B_{n/2} & \text{if } n \text{ is even}\ . \end{cases}$$

Since any code with even distance can be made an even weight code, we have

Corollary 4.

$$A(n, 2e+2) \leq \lfloor max\{\hat{B}_0\} \rfloor \ ,$$

subject to constraints

$$\sum_{k=0}^{\lfloor n/2 \rfloor} \hat{B}_k = 2^{n-1},$$

$$\sum_{k=0}^{\lfloor n/2 \rfloor} \hat{B}_k P_{2j}(k) = 0 \ for \ 1 \leq j \leq e,$$

$$0 \leq \sum_{k=0}^{\lfloor n/2 \rfloor} \hat{B}_k P_{2j}(k) \leq 2^{n-1} A(n, 2e+2, 2j) \ for \ e+1 \leq j \leq \lfloor n/2 \rfloor \ ,$$

and $\hat{B}_k \geq 0$ *for* $0 \leq k \leq \lfloor n/2 \rfloor$.

In some cases we will add more constraints to obtain some specific bounds as in [4], [8], [15], [19].

4.3. BOUNDS ON $A(n,3)$ DERIVED BY LINEAR PROGRAMMING. Corollaries 2 and 3 do not give an explicit bound on $A(n,3)$. To obtain explicit bounds from these two corollaries we will use linear programming to find upper bounds on $S_1(1,n)$ and $S_2(1,n)$ of the $(n,3)$ code C. Since we now wish to analyze an even weight code, it follows that we have to take the extended code of C. Hence, we will have to make small appropriate changes when we use Corollaries 2 and 3.

Lemma 4.6. *If C is an even weight $(n,4)$ code, $n \equiv 11 \ (mod \ 12)$, with inner distribution $\{A_i\}_{i=0}^n$, then*

$$6A_{n-3} + 3(n-1)A_{n-1} \leq \frac{(n-2)(n-1)(n+4)}{n+2} \ . \tag{37}$$

Proof. Let C be an even weight $(n,4)$ code, $n \equiv 11 \ (mod \ 12)$. Its inner distribution $\{A_i\}_{i=0}^n$ must satisfy

$$\begin{cases} A_0 = 1, \\ A_2 = 0, \\ A_{n-3} + (A(n,4,3) - A(n-1,4,3))A_{n-1} \leq A(n,4,3), \end{cases}$$

where the values of $A(n,4,3)$ are given by Theorem 5.1 and the last inequality is clearly valid for even weight $(n,4)$ codes [2].

Our goal is to maximize $6A_{n-3} + 3(n-1)A_{n-1}$. By Lemma 4.5 it is equivalent to solve the following linear programming problem:

maximize $6\sum_{j=0}^{(n-1)/2} B_j \left(P_{n-3}(j) + \frac{n-1}{2} P_{n-1}(j)\right)$,

subject to

$$\begin{cases} \sum_{j=0}^{(n-1)/2} B_j = 2^{n-1}, \\ \sum_{j=0}^{(n-1)/2} B_j P_2(j) = 0, \\ \sum_{j=0}^{(n-1)/2} B_j \left(P_{n-3}(j) + \frac{n-3}{2} P_{n-1}(j)\right) \leq \frac{n^2-n-8}{6} \cdot 2^{n-1} \ , \end{cases}$$

and $B_j \geq 0$, for $0 \leq j \leq (n-1)/2$.

We will solve this linear programming problem by using the simplex method (we will use the definitions as in [13]). We will add a slack variable to convert the problem into standard form. Denote $g(j) = -\left(P_{n-3}(j) + \frac{n-1}{2}P_{n-1}(j)\right)$ and $f(j) = P_{n-3}(j) + \frac{n-3}{2}P_{n-1}(j)$. The standard form of the problem is:

minimize $6\sum_{j=0}^{(n-1)/2} g(j)x_j$

subject to $Ax = b$

and $x \geq 0$,

where

$$A = \begin{pmatrix} 1 & 1 & \cdots & 1 & 1 & 1 & 0 \\ P_2(0) & P_2(1) & \cdots & P_2((n-5)/2) & P_2((n-3)/2) & P_2((n-1)/2) & 0 \\ f(0) & f(1) & \cdots & f((n-5)/2) & f((n-3)/2) & f((n-1)/2) & 1 \end{pmatrix},$$

$x = (x_0, x_1, \cdots, x_{(n-1)/2}, x_{(n+1)/2})^T$, $x_j = B_j$ for $0 \leq j \leq (n-1)/2$, and $b = 2^{n-1}(1, 0, \frac{n^2-n-8}{6})^T$.

Let

$$T = \begin{pmatrix} t_{11} & t_{12} & t_{13} \\ t_{21} & t_{22} & t_{23} \\ t_{31} & t_{32} & t_{33} \end{pmatrix} = \begin{pmatrix} -\frac{6}{(n+1)(n+2)(n-3)} & 0 & \frac{6}{(n+1)(n+2)(n-3)} \\ \frac{(n-1)^2 n}{8(n+2)(n-3)} & \frac{1}{4} & \frac{-3(n-1)}{4(n+2)(n-3)} \\ \frac{-(n^2-6n-19)n}{8(n+1)(n+2)} & -\frac{1}{4} & \frac{3(n+3)}{4(n+1)(n+2)} \end{pmatrix},$$

$\tilde{A} = TA$, and $\tilde{b} = Tb$. Hence, we have the following linear programming problem:

minimize $6\sum_{j=0}^{(n-1)/2} g(j)x_j$

subject to $\tilde{A}x = \tilde{b}$

and $x \geq 0$,

where

$$\tilde{A} = \begin{pmatrix} 1 & c_{11} & \cdots & c_{1k} & \cdots & c_{1(n-5)/2} & 0 & 0 & t_{13} \\ 0 & c_{21} & \cdots & c_{2k} & \cdots & c_{2(n-5)/2} & 1 & 0 & t_{23} \\ 0 & c_{31} & \cdots & c_{3k} & \cdots & c_{3(n-5)/2} & 0 & 1 & t_{33} \end{pmatrix}, \quad \tilde{b} = 2^{n-1} \begin{pmatrix} \frac{n^2-n-14}{(n-3)(n+1)(n+2)} \\ \frac{n-1}{(n-3)(n+2)} \\ \frac{n^2+n-3}{(n+1)(n+2)} \end{pmatrix},$$

$$c_{1k} = \begin{cases} \frac{(n+2-2k)(n+1-2k)(n-3-2k)}{(n+2)(n+1)(n-3)} & \text{if } k \text{ is even} \\ \frac{-(n+3-2k)(n-1-2k)(n-2-2k)}{(n+2)(n+1)(n-3)} & \text{if } k \text{ is odd} \end{cases}$$

$$c_{2k} = \begin{cases} \frac{k(n+1-2k)(7+2k-2n-2kn+n^2)}{4(n+2)(n-3)} & \text{if } k \text{ is even} \\ \frac{(n-1-2k)(n-k)(-7+2k-2kn+n^2)}{4(n+2)(n-3)} & \text{if } k \text{ is odd} \end{cases}$$

$$c_{3k} = \begin{cases} \frac{-k(n-3-2k)(7-6k+6n-2kn+n^2)}{4(n+2)(n+1)} & \text{if } k \text{ is even} \\ \frac{-(n+3-2k)(n-k)(-7-6k-2kn+n^2)}{4(n+2)(n+1)} & \text{if } k \text{ is odd.} \end{cases}$$

Thus we have the following basic feasible solution:

$$x = 2^{n-1}\left(\frac{n^2-n-14}{(n-3)(n+1)(n+2)}, 0, 0, \cdots, 0, \frac{n-1}{(n-3)(n+2)}, \frac{n^2+n-3}{(n+1)(n+2)}, 0\right)^T.$$

We want to show that this solution is optimal. We will use the *Optimality Condition Theorem* [13, p. 43]. In our case, the solution is optimal if the following $\frac{n+3}{2}$ conditions hold:

$$t_{13} \cdot g(0) + t_{23} \cdot g((n-3)/2) + t_{33} \cdot g((n-1)/2) \le 0 \tag{38}$$

and

$$c_{1k} \cdot g(0) + c_{2k} \cdot g((n-3)/2) + c_{3k} \cdot g((n-1)/2) - g(k) \le 0, \tag{39}$$

for $0 \le k \le (n-1)/2$.

First,

$$g(0) = -\binom{n+1}{3},\ g((n-3)/2) = -4,\ g((n-1)/2) = 0,$$

$$t_{13} \cdot g(0) + t_{23} \cdot g((n-3)/2) + c_{33} \cdot g((n-1)/2) = -\frac{n-1}{n+2} < 0,$$

and therefore condition (38) is satisfied.
Next, for even k we have

$$c_{1k} \cdot g(0) + c_{2k} \cdot g((n-3)/2) + c_{3k} \cdot g((n-1)/2) - g(k) = -\frac{k(n+1-2k)(n-3-2k)}{n+2},$$

and for odd k we have

$$c_{1k} \cdot g(0) + c_{2k} \cdot g((n-3)/2) + c_{3k} \cdot g((n-1)/2) - g(k) = \frac{(k-n)(n+3-2k)(n-1-2k)}{n+2}.$$

Since $n \equiv 11 (mod\ 12)$, these expressions are not positive and, therefore, condition (39) is satisfied.
The optimal value of the objective function in the linear programming problem is

$$-6 \cdot 2^{n-1}\left(\frac{n^2-n-14}{(n-3)(n+1)(n+2)} \cdot \binom{n+1}{3} + \frac{4(n-1)}{(n-3)(n+2)}\right) = -2^{n-1}\frac{(n-2)(n-1)(n+4)}{n+2},$$

which implies

$$6A_{n-3} + 3(n-1)A_{n-1} \le \frac{(n-2)(n-1)(n+4)}{n+2}.$$

□

By linear programming in Lemma 4.6, the "code" C which attains the maximum of $6A_{n-3} + 3(n-1)A_{n-1}$ has size

$$B_0 = \frac{n^2-n-14}{(n-3)(n+1)(n+2)}2^{n-1} = \frac{2^{n-1}}{n+1+\frac{8}{n+2}+\frac{32(n+4)}{(n+2)(n^2-n-14)}}.$$

By substituting (37) in Corollary 2 for $n \equiv 11(mod\ 12)$ we infer that

$$A(n-1,3) \leq \frac{2^{n-1}}{n+1+\frac{8}{n+2}}.$$

Therefore, we would like to know if a code with size greater than $\frac{n^2-n-14}{(n-3)(n+1)(n+2)}2^{n-1}$ can exist, subject to the constraints in Lemma 4.6. Among all codes with size greater than $\frac{n^2-n-14}{(n-3)(n+1)(n+2)}2^{n-1}$ we are interested in those for which $6A_{n-3}+3(n-1)A_{n-1}$ is maximum.

Theorem 4.7. *If* $m \equiv 10\ (mod\ 12)$ *then*

$$A(m,3) \leq \frac{2^m}{m+2+\frac{8}{m+3}\left(1+\frac{48(m+5)}{m^3+8m^2+5m-126+(m+3)\sqrt{m^4+10m^3+5m^2-292m+484}}\right)}.$$

Proof. Let $n \equiv 11\ (mod\ 12)$ and consider the following linear programming problem:

maximize $6\sum_{j=0}^{(n-1)/2} B_j\left(P_{n-3}(j)+\frac{n-1}{2}P_{n-1}(j)\right)$

subject to

$$\begin{cases} \sum_{j=0}^{(n-1)/2} B_j = 2^{n-1}, \\ \sum_{j=0}^{(n-1)/2} B_j P_2(j) = 0, \\ \sum_{j=0}^{(n-1)/2} B_j\left(P_{n-3}(j)+\frac{n-3}{2}P_{n-1}(j)\right) \leq \frac{n^2-n-8}{6}\cdot 2^{n-1}, \\ B_0 \geq \left(\frac{n^2-n-14}{(n-3)(n+1)(n+2)}+\tau\right)2^{n-1}, \end{cases}$$

and $B_j \geq 0$, $0 \leq j \leq (n-1)/2$,
where τ is nonnegative parameter.

Again, we will solve this linear programming problem by using the simplex method. We will add a slack variable and a surplus variable to convert the problem into standard form. Denote $g(j) = -\left(P_{n-3}(j)+\frac{n-1}{2}P_{n-1}(j)\right)$ and $f(j) = P_{n-3}(j)+\frac{n-3}{2}P_{n-1}(j)$. The standard form of the problem is:

minimize $6\sum_{j=0}^{(n-1)/2} g(j)x_j$

subject to $Ax = b$

and $x \geq 0$,

where

$$A = \begin{pmatrix} 1 & 1 & \cdots & 1 & 1 & 1 & 0 & 0 \\ P_2(0) & P_2(1) & \cdots & P_2((n-5)/2) & P_2((n-3)/2) & P_2((n-1)/2) & 0 & 0 \\ f(0) & f(1) & \cdots & f((n-5)/2) & f((n-3)/2) & f((n-1)/2) & 1 & 0 \\ 1 & 0 & \cdots & 0 & 0 & 0 & 0 & -1 \end{pmatrix},$$

$x = (x_0, x_1, \cdots, x_{(n-1)/2}, x_{(n+1)/2}, x_{(n+3)/2})^T$, $x_j = B_j$ for $0 \leq j \leq (n-1)/2$, and $b = 2^{n-1}(1, 0, \frac{n^2-n-8}{6}, \left(\frac{n^2-n-14}{(n-3)(n+1)(n+2)}+\tau\right))^T$.

Analogous to the proof of Lemma 4.6 we obtain the following optimal basic feasible solution

$$x = 2^{n-1} \begin{pmatrix} \frac{n^2-n-14}{(n-3)(n+1)(n+2)} + \tau \\ \\ \frac{n+2}{(n-4)}\tau \\ \\ 0 \\ \vdots \\ 0 \\ \\ \frac{(n-1)(4n-16-\tau(n^4-3n^3-9n^2+17n+30))}{4(n-4)(n-3)(n+2)} \\ \\ \frac{4n^3-12n^2-28n+48+\tau(n^5-18n^3-26n^2+17n+26)}{4(n-4)(n+1)(n+2)} \\ \\ 0 \\ 0 \end{pmatrix}.$$

Since $B_j \geq 0$, $0 \leq j \leq (n-1)/2$, it follows that $0 \leq \tau \leq \frac{4(n-4)}{(n-3)(n+2)(n^2-2n-5)}$.

The optimal value of the objective function in the linear programming problem is:

$$-2^{n-1}\frac{(n-1)((n-4)(n-2)(n+4)-6\tau(n-3)(n+1)(n+2))}{(n-4)(n+2)},$$

which implies

$$6A_{n-3} + 3(n-1)A_{n-1} \leq \frac{(n-2)(n-1)(n+4)}{n+2} - 6\tau\frac{(n-1)(n-3)(n+1)}{n-4}\ . \tag{40}$$

Note that for $\tau = 0$ the value of the objective function coincides with the one found in Lemma 4.6. By substituting (40) in Corollary 2 for $n \equiv 11 (mod\ 12)$ we infer that

$$A(n-1,3) \leq \frac{2^{n-1}}{n+1+\frac{8}{n+2}+6\tau\frac{(n-3)(n+1)}{n-4}}. \tag{41}$$

By linear programming, the "code" C which attains the maximum of $6A_{n-3} + 3(n-1)A_{n-1}$ has size

$$B_0 = \left(\frac{n^2-n-14}{(n-3)(n+1)(n+2)} + \tau\right)2^{n-1}\ . \tag{42}$$

It is easy to see that the RHS of (41) is continuous monotonic decreasing function of τ and the RHS of (42) is a continuous monotonic increasing function of τ on the interval $[0, \frac{4(n-4)}{(n-3)(n+2)(n^2-2n-5)}]$. Therefore, upper bounds on $A(n-1,3)$ are obtained as long as

$$\left(\frac{n^2-n-14}{(n-3)(n+1)(n+2)} + \tau\right)2^{n-1} \leq \frac{2^{n-1}}{n+1+\frac{8}{n+2}+6\tau\frac{(n-3)(n+1)}{n-4}}\ . \tag{43}$$

Hence, we maximize τ in the given interval, such that (43) is satisfied, and obtain τ^*,

(44)
$$\tau^* = \frac{64(n-4)(n+4)}{(n-3)(n+1)(n+2)(n^3+5n^2-8n-124+(n+2)\sqrt{n^4+6n^3-19n^2-276n+772})}.$$

Since we are interested in $n \equiv 11(mod\ 12)$, one can verify that $\tau^* \in [0, \frac{4(n-4)}{(n-3)(n+2)(n^2-2n-5)}]$ for $n \geq 11$. The theorem follows by substituting (44) in (41).

□

We turn our attention to $S_2(1,n)$.

Lemma 4.8. *If C is an even weight $(n,4)$ code, $n \equiv 10$ $(mod\ 12)$, with inner distribution $\{A_i\}_{i=0}^n$, then*

$$12A_{n-4} + (4n-10)A_{n-2} + \frac{n(n-4)}{2}A_n \leq \frac{n(n^2-4n+2)}{2}\ . \tag{45}$$

Proof. Let C be an even weight $(n,4)$ code, $n \equiv 10$ $(mod\ 12)$. Its inner distribution $\{A_i\}_{i=0}^n$ must satisfy

$$\begin{cases} A_0 = 1, \\ A_2 = 0, \\ A_n \geq 0. \end{cases}$$

Our goal is to maximize $12A_{n-4} + (4n-10)A_{n-2} + \frac{n(n-4)}{2}A_n$. By lemma 4.5 it is equivalent to solve the following linear programming problem:

maximize $\sum_{j=0}^{n/2} \hat{B}_j \left(12P_{n-4}(j) + (4n-10)P_{n-2}(j) + \frac{n(n-4)}{2}P_n(j)\right)$,

subject to

$$\begin{cases} \sum_{j=0}^{n/2} \hat{B}_j = 2^{n-1}, \\ \sum_{j=0}^{n/2} \hat{B}_j P_2(j) = 0, \\ \sum_{j=0}^{n/2} \hat{B}_j P_n(j) \geq 0\ , \end{cases}$$

and $\hat{B}_j \geq 0$, for $0 \leq j \leq \frac{n}{2}$.

We will solve this linear programming problem similar to the solution in Lemma 4.6 (a complete solution appears in [16]). The optimal value of the objective function in the linear programming problem is $2^{n-1}\frac{1}{2}n(n^2-4n+2)$, which implies

$$12A_{n-4} + (4n-10)A_{n-2} + \frac{n(n-4)}{2}A_n \leq \frac{n(n^2-4n+2)}{2}\ .$$

□

By linear programming in Lemma 4.8, the "code" C which attains the maximum of $12A_{n-4} + (4n-10)A_{n-2} + \frac{n(n-4)}{2}A_n$ has size

$$\hat{B}_0 = \frac{2^{n-1}}{n+2}\ .$$

By substituting (45) in Corollary 3 for $n \equiv 10(mod\ 12)$ we infer that

$$A(n-1,3) \leq \frac{2^{n-1}}{n+2+\frac{4}{(n-1)^2-3}} \ .$$

Therefore, there is no code with cardinality $\frac{2^{n-1}}{n+2}$. Hence, we will search for a code with cardinality at most $\frac{2^{n-1}}{n+2+\frac{4}{(n-1)^2-3}}$ subject to the constraints in Lemma 4.8. Among all codes with the size at most $\frac{2^{n-1}}{n+2+\frac{4}{(n-1)^2-3}}$, we are interested in those for which $12A_{n-4}+(4n-10)A_{n-2}+\frac{n(n-4)}{2}A_n$ is maximum.

Theorem 4.9. *If* $m \equiv 9\ (mod\ 12)$ *then*

$$A(m,3) \leq \frac{2^m}{m+3+\frac{4}{m^2-3}\left(1+\frac{16(m-1)^2}{m^3-5m^2+13m-13+\sqrt{m^6-10m^5+51m^4-156m^3+427m^2-594m+297}}\right)} \ .$$

Proof. Let $n \equiv 10\ (mod\ 12)$ and consider the following linear programming problem:

maximize $\sum_{j=0}^{n/2} \hat{B}_j \left(12P_{n-4}(j)+(4n-10)P_{n-2}(j)+\frac{n(n-4)}{2}P_n(j)\right)$

subject to

$$\begin{cases} \sum_{j=0}^{n/2} \hat{B}_j = 2^{n-1}, \\ \sum_{j=0}^{n/2} \hat{B}_j P_2(j) = 0, \\ \sum_{j=0}^{n/2} \hat{B}_j P_n(j) \geq 0\ , \\ \hat{B}_0 \leq \left(\frac{1}{n+2}-\tau\right)2^{n-1}\ , \end{cases}$$

and $\hat{B}_j \geq 0$, $0 \leq j \leq \frac{n}{2}$,
where τ is nonnegative parameter.

Analogous to the proof of Theorem 4.7 we obtain

(46)

$$12A_{n-4}+(4n-10)A_{n-2}+\frac{n(n-4)}{2}A_n \leq \frac{n(n^2-4n+2)}{2}-4\tau(n-2)^2(n+2)\ .$$

Note that for $\tau = 0$ the value of the objective function coincides with the one found in Lemma 4.8. By substituting (46) in Corollary 3 for $n \equiv 10(mod\ 12)$ we infer that

$$A(n-1,3) \leq \frac{2^{n-1}}{n+2+\frac{4}{(n-1)^2-3}+8\tau\frac{(n-2)^2(n+2)}{n^2-2n-2}} \ . \tag{47}$$

By linear programming, the "code" C which attains the maximum of $12A_{n-4}+(4n-10)A_{n-2}+\frac{n(n-4)}{2}A_n$ has size

$$B_0 = \left(\frac{1}{n+2}-\tau\right)2^{n-1}. \tag{48}$$

It is easy to see that the RHS of (47) and the RHS of (48) are continuous monotonic decreasing functions of τ, $0 \leq \tau < \frac{1}{n+2}$. Therefore, upper bounds on $A(n-1,3)$ are obtained as long as

$$\left(\frac{1}{n+2}-\tau\right)2^{n-1} \geq \frac{2^{n-1}}{n+2+\frac{4}{(n-1)^2-3}+8\tau\frac{(n-2)^2(n+2)}{n^2-2n-2}} \ . \tag{49}$$

Hence, we maximize τ, such that (49) is satisfied, and obtain τ^*,

$$\tau^* = \frac{8}{(n+2)\left(n^3-8n^2+26n-32+\sqrt{n^6-16n^5+116n^4-480n^3+1316n^2-2176n+1536}\right)} \ . \tag{50}$$

Since we are interested in $n \equiv 10(mod\ 12)$, one can verify that $\tau^* \in [0, \frac{1}{n+2}]$ for $n \geq 10$. The theorem follows by substituting (50) in (47). □

For the specific details of the proofs of Lemma 4.8 and Theorem 4.9 the reader is referred to [16].

5. Summary of explicit new bounds

5.1. Bounds on $A(n,3)$. The known upper bounds on $A(n,3)$ are summarized in the following table:

$$A(n,3) \leq \begin{cases} 2^n/(n+1) & \text{if } n \equiv 3 \text{ or } 7(mod\ 12) \quad (1) \\ 2^n/(n+1+\frac{8}{n-1}) & \text{if } n \equiv 11(mod\ 12) \quad (2) \\ 2^n/(n+2) & \text{if } n \equiv 2 \text{ or } 6(mod\ 12) \quad (2) \\ 2^n/(n+2+\frac{2n+28}{n^2+n-8}) & \text{if } n \equiv 10(mod\ 12) \quad (3) \\ 2^n/(n+3) & \text{if } n \equiv 1(mod\ 4) \quad [3] \\ 2^n/(n+4) & \text{if } n \equiv 0(mod\ 4) \quad [3] \end{cases}$$

Some of these bounds are obtained by using the known bounds on sizes of constant weight codes $A(n,4,3)$ and $A(n,4,4)$ [14].

Theorem 5.1.

$$A(n,4,3) = \begin{cases} \frac{n(n-2)}{6} & \text{if } n \equiv 0 \text{ or } 2(mod\ 6) \\ \frac{n(n-1)}{6} & \text{if } n \equiv 1 \text{ or } 3(mod\ 6) \\ \frac{n^2-2n-2}{6} & \text{if } n \equiv 4(mod\ 6) \\ \frac{n^2-n-8}{6} & \text{if } n \equiv 5(mod\ 6) \ . \end{cases}$$

Theorem 5.2.

$$A(n,4,4) = \begin{cases} \frac{n(n-1)(n-3)}{24} & \text{if } n \equiv 1 \text{ or } 3(mod\ 6) \\ \frac{n(n-1)(n-2)}{24} & \text{if } n \equiv 2 \text{ or } 4(mod\ 6) \\ \frac{n(n^2-3n-6)}{24} & \text{if } n \equiv 0(mod\ 6) \ , \end{cases}$$

$$A(n,4,4) \leq \begin{cases} \frac{n^3-4n^2+n-6}{24} & \text{if } n \equiv 5(mod\ 12) \\ \frac{n^3-4n^2+n-18}{24} & \text{if } n \equiv 11(mod\ 12) \ . \end{cases}$$

In Theorem 4.7 we have improved the bound for $n \equiv 10\ (mod\ 12)$ and obtain that

$$A(n,3) \leq \frac{2^n}{n+2+\frac{8}{n+3}\left(1+\frac{48(n+5)}{n^3+8n^2+5n-126+(n+3)\sqrt{n^4+10n^3+5n^2-292n+484}}\right)}.$$

In Theorem 4.9 we have improved the bound for $n \equiv 9 \ (mod\ 12)$ and obtain that

$$A(n,3) \leq \frac{2^n}{n+3+\frac{4}{n^2-3}\left(1+\frac{16(n-1)^2}{n^3-5n^2+13n-13+\sqrt{n^6-10n^5+51n^4-156n^3+427n^2-594n+297}}\right)}.$$

Some specific bounds which were obtained from Theorems 4.7 and 4.9 are $A(21,3) \leq 87333$ and $A(22,3) \leq 172361$ (compared to 87376 and 173015 in [15]). By maximizing $S_1(e,n)$ defined in Theorem 4.2 subject to constraints of Theorem 4.4 and similarly to the arguments in the proof of Theorem 4.9, we obtain $A(24,5) \leq 47538$ (compared to 47998 in [18]).

5.2. BOUNDS ON $A(n,d,w)$. Our results can be applied to any metric association scheme. As an example we consider the Johnson scheme. In this scheme X is the set of all binary vectors of length n and weight w. Without loss of generality we assume that $w \leq \frac{n}{2}$. The distance between two vectors is defined to be the half of the Hamming distance between them. In this scheme the number of relations is $w+1$. One can verify, that $v = \binom{n}{w}$, $v_i = \binom{w}{i}\binom{n-w}{i}$, and $p_{i,j}^k$ is given by

$$p_{i,j}^k = \sum_{l=0}^{w-k} \binom{w-k}{l}\binom{k}{w-i-l}\binom{k}{w-j-l}\binom{n-w-k}{i+j+l-w}.$$

Denote by $T(w_1,n_1,w_2,n_2,d)$ the maximum number of binary vectors of length n_1+n_2, having mutual Hamming distance of at least d, where each vector has exactly w_1 ones in the first n_1 coordinates and exactly w_2 ones in the last n_2 coordinates. Tables of the best known upper bounds on $T(w_1,n_1,w_2,n_2,d)$ are given in [1].

By substituting

$$\max_{h \in H}\{NC(h,C,e+1)\} \leq T(e+1,w,e+1,n-w,4e+2)$$

in (19), we obtain the following bound.

Theorem 5.3.

$$A(n,4e+2,w) \leq \frac{\binom{n}{w}}{\sum_{i=0}^{e}\binom{w}{i}\binom{n-w}{i}+\frac{\binom{w}{e+1}\binom{n-w}{e+1}-\binom{2e+1}{e}^2\max\{A_{2e+1}\}}{T(e+1,w,e+1,n-w,4e+2)}},$$

where $\max\{A_{2e+1}\}$ *is taken subject to Delsarte's linear constraints for Johnson scheme (see* [14, Theorem 12, p. 666] *).*

By applying Theorem 5.3 for $e=1$ and similarly to the arguments in the proofs of Theorems 4.7 and 4.9 we obtain the following improvements (the values in the parentheses are the best bounds previously known [1], [18]): $A(19,6,7) \leq 519$ (520), $A(22,6,11) \leq 5033$ (5064), $A(26,6,11) \leq 42017$ (42075).

ACKNOWLEDGEMENTS

We would like to thank Avraham Sidi for pointing the material in [13] and the referees for their valuable comments and suggestions.

References

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

[2] M. R. Best, *Binary codes with a minimum distance of four*, IEEE Trans. on Inform. Theory, **26** (1980), 738–742.

[3] M. R. Best, A. E. Brouwer, *The triply shortened binary Hamming code is optimal*, Discrete Mathematics, **17** (1977), 235–245.

[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. on Inform. Theory, **24** (1978), 81–93.

[5] Ph. Delsarte, *Bounds for unrestricted codes, by linear programming*, Philips Res. Reports, **27** (1972), 272–289.

[6] Ph. Delsarte, *An algebraic approach to the association schemes of coding theory*, Philips Research Reports Supplements, **10** (1973).

[7] P. Hammond, *Nearly perfect codes in distance-regular graphs*, Discrete Mathematics, **14** (1976), 41–56.

[8] I. Honkala, "Bounds for Binary Constant Weight and Covering Codes," Licentiate Thesis, Department of Mathematics, Univ. of Turku, Turku, Finland, 1987.

[9] T. Jiang, A. Vardy, *Asymptotic improvement of the Gilbert-Varshamov bound on the size of binary codes*, IEEE Trans. on Inform. Theory, **50** (2004), 1655–1664.

[10] S. M. Johnson, *A new upper bound for error-correcting codes*, IRE Trans. on Inform. Theory, **8** (1962), 203–207.

[11] I. Krasikov, S. Litsyn, *Survey of binary Krawtchouk polynomials*, DIMACS Series in Discrete Mathematics and Theoretical Computer Science, **56** (2001), 199–211.

[12] S. Litsyn, *An updated table of the best binary codes known*, in "Handbook of Coding Theory" (eds. V. S. Pless and W. C. Huffman), Vol. 1, Elsevier, Amsterdam, (1998), 463–498.

[13] D. G. Luenberger, "Linear and Nonlinear Programming," Reading, Addison-Wesley, Massachusetts, 1973.

[14] F. J. MacWilliams, N. J. A. Sloane, "The Theory of Error-Correcting Codes," North-Holland, Amsterdam, 1977.

[15] B. Mounits, T. Etzion and S. Litsyn, *Improved upper bounds on sizes of codes*, IEEE Trans. on Inform. Theory, **48** (2002), 880–886.

[16] B. Mounits, "Bounds on Sizes of Nonlinear Codes," Ph. D thesis, Dept. of Mathematics, Technion - Israel Institute of Technology, Haifa, Israel, 2006.

[17] C. Roos, C. de Vroedt, *Upper bounds for A(n,4) and A(n,6) derived from Delsarte's linear programming bound*, Discrete Mathematics, **40** (1982), 261–276.

[18] A. Schrijver, *New code upper bounds from the Terwilliger algebra and semidefinite programming*, IEEE Trans. on Inform. Theory, **51** (2005), 2859–2866.

[19] C. L. N. van Pul, "On Bounds on Codes," Master's thesis, Dept. of Mathematics and Computing Science, Eindhoven Univ. of Technology, Eindhoven, the Netherlands, 1982.

Received August 2006; revised February 2007.

E-mail address: B.Mounits@cwi.nl
E-mail address: etzion@cs.technion.ac.il
E-mail address: litsyn@eng.tau.ac.il