New code upper bounds from the Terwilliger algebra and semidefinite programming

Alexander Schrijver

***Abstract*— We give a new upper bound on the maximum size $A(n,d)$ of a binary code of word length n and minimum distance at least d. It is based on block-diagonalising the Terwilliger algebra of the Hamming cube. The bound strengthens the Delsarte bound, and can be calculated with semidefinite programming in time bounded by a polynomial in n. We show that it improves a number of known upper bounds for concrete values of n and d.**

From this we also derive a new upper bound on the maximum size $A(n,d,w)$ of a binary code of word length n, minimum distance at least d, and constant weight w, again strengthening the Delsarte bound and yielding several improved upper bounds for concrete values of n, d, and w.

***Index Terms*— block-diagonalisation, codes, constant-weight codes, Delsarte bound, semidefinite programming, Terwilliger algebra, upper bounds.**

I. Description of the method

We present a new upper bound on $A(n,d)$, the maximum size of a binary code of word length n and minimum distance at least d. The bound is based on block-diagonalising the (non-commutative) Terwilliger algebra of the Hamming cube and on semidefinite programming. The bound refines the Delsarte bound [4], which is based on diagonalising the (commutative) Bose-Mesner algebra of the Hamming cube and on linear programming. We describe the approach in this section, and go over to the details in Section II.

Taking a tensor product of the algebra, this approach also yields a new upper bound on $A(n,d,w)$, the maximum size of a binary code of word length n, minimum distance at least d, and constant weight w. This bound strengthens the Delsarte bound for constant-weight codes. We describe this method in Section III.

Fix a nonnegative integer n, and let $\mathcal{P}$ be the collection of all subsets of $\{1,\dots,n\}$. We identify code words in $\{0,1\}^n$ with their support. So a code C is a subset of $\mathcal{P}$. The *Hamming distance* of $X,Y\in\mathcal{P}$ is equal to $|X\triangle Y|$. The *minimum distance* of a code C is the minimum Hamming distance of distinct elements of C. For finite sets U and V, a $U\times V$ *matrix* is a matrix whose rows and columns are indexed by U and V, respectively.

For background on coding theory and association schemes we refer to MacWilliams and Sloane [9]. However, most of this paper is self-contained. While we will mention below a theorem on the existence of a block-diagonalisation of a C$*$-algebra, we prove this theorem for the algebras concerned by displaying an explicit block-diagonalisation.

CWI and University of Amsterdam. *Mailing address:* CWI, Kruislaan 413, 1098 SJ Amsterdam, The Netherlands. *Email:* `lex@cwi.nl`

A. The Terwilliger algebra

We first describe the Terwilliger algebra of the Hamming cube, in a form convenient for our purposes. For background we refer to our notes in Subsection I-C.

For nonnegative integers i,j,t, let $M_{i,j}^t$ be the $\mathcal{P}\times\mathcal{P}$ matrix with

$$(1)\qquad (M_{i,j}^t)_{X,Y} := \begin{cases} 1 & \text{if } |X|=i, |Y|=j, |X\cap Y|=t,\\ 0 & \text{otherwise,}\end{cases}$$

for $X,Y\in\mathcal{P}$. So $(M_{i,j}^t)^\mathsf{T} = M_{j,i}^t$. It is trivial but useful to note that if $|X|=i$ and $|Y|=j$, then $|X\cap Y|=t$ is equivalent to $|X\triangle Y| = i+j-2t$.

Let $\mathcal{A}_n$ be the set of matrices

$$(2)\qquad \sum_{i,j,t=0}^{n} x_{i,j}^t M_{i,j}^t$$

with $x_{i,j}^t\in\mathbb{C}$. It is easy to check that $\mathcal{A}_n$ is a *C$*$-algebra*: it is closed under addition, scalar and matrix multiplication, and taking the adjoint. (Matrix multiplication follows from the fact that $M_{i,j}^t M_{j',k}^s = \mathbf{0}$ if $j\neq j'$, and that for $X,Z\in\mathcal{P}$ then the number of $Y\in\mathcal{P}$ with $|Y|=j$, $|X\cap Y|=t$, $|Y\cap Z|=s$ only depends on $|X|$, $|Z|$, and $|X\cap Z|$. So $M_{i,j}^t M_{j,k}^s$ is a linear combination of $M_{i,k}^u$ for $u=0,\dots,n$.)

This algebra is called the *Terwilliger algebra* [14] of the *Hamming cube* $H(n,2)$. It has dimension

$$(3)\qquad \dim\mathcal{A}_n = \binom{n+3}{3},$$

since it is the number of triples (i,j,t) with $M_{i,j}^t\neq\mathbf{0}$, which is equal to the number of triples (a,b,t) with $a+b+t\le n$.

Since $\mathcal{A}_n$ is a C$*$-algebra and since $\mathcal{A}_n$ contains the identity matrix, there exists a unitary $\mathcal{P}\times\mathcal{P}$ matrix U (that is, $U^*U=I$) and positive integers $p_0,q_0,\dots,p_m,q_m$ (for some m) such that $U^*\mathcal{A}_nU$ is equal to the collection of all block-diagonal matrices

$$(4)\qquad \begin{pmatrix} C_0 & 0 & \cdots & 0\\ 0 & C_1 & \cdots & 0\\ \vdots & \vdots & \ddots & 0\\ 0 & 0 & \cdots & C_m\end{pmatrix}$$

(for later purposes, we start the numbering at 0), where each C_k is a block-diagonal matrix with q_k repeated, identical blocks of order p_k:

$$(5) \qquad C_k = \begin{pmatrix} B_k & 0 & \cdots & 0 \\ 0 & B_k & \cdots & 0 \\ \vdots & \vdots & \ddots & 0 \\ 0 & 0 & \cdots & B_k \end{pmatrix}.$$

So $p_0^2+\cdots+p_m^2 = \dim(\mathcal{A}_n) = \binom{n+3}{3}$ and $p_0q_0+\cdots+p_mq_m = 2^n$.

By deleting copies of blocks, we see that $\mathcal{A}_n$ is (as a C$*$-algebra) isomorphic to the direct sum

$$(6) \qquad \bigoplus_{k=0}^{m} \mathbb{C}^{p_k\times p_k} = \{ \begin{pmatrix} B_0 & 0 & \cdots & 0 \\ 0 & B_1 & \cdots & 0 \\ \vdots & \vdots & \ddots & 0 \\ 0 & 0 & \cdots & B_m \end{pmatrix} \mid B_k \in \mathbb{C}^{p_k\times p_k} \text{ for } k=0,\ldots,m\}.$$

The isomorphism maintains positive semidefiniteness of matrices. The number m and the block sizes p_k and block multiplicities q_k are (up to permutation of the indices k) uniquely determined by the C$*$-algebra.

So far, this is all standard C$*$-algebra theory, but we will need this block-diagonalisation of the Terwilliger algebra $\mathcal{A}_n$ more explicitly. In Section II we will specify a matrix U with the required properties. It will turn out that U can be taken real, that $m = \lfloor \frac{n}{2} \rfloor$, and that, for $k = 0, \ldots, \lfloor \frac{n}{2} \rfloor$, there is a block B_k of order $p_k = n-2k+1$ and multiplicity $q_k = \binom{n}{k} - \binom{n}{k-1}$. (One may check that indeed $\sum_{k=0}^{\lfloor \frac{n}{2} \rfloor}(n-2k+1)^2 = \binom{n+3}{3}$ (cf. (48) below) and $\sum_{k=0}^{\lfloor \frac{n}{2} \rfloor}\left(\binom{n}{k} - \binom{n}{k-1}\right)(n-2k+1) = 2^n$ (cf. (41) below).)

To describe the image of (2) in (6), define, for $i,j,k,t \in \{0,\ldots,n\}$:

$$(7) \qquad \beta^t_{i,j,k} := \sum_{u=0}^{n}(-1)^{u-t}\binom{u}{t}\binom{n-2k}{u-k}\binom{n-k-u}{i-u}\binom{n-k-u}{j-u}.$$

In Theorem 1 (concluding Section II) we will see that, for $k = 0, \ldots, \lfloor \frac{n}{2} \rfloor$, the kth block B_k of the image (6) of (2) is the following $(n-2k+1)\times(n-2k+1)$ matrix:

$$(8) \qquad \left(\sum_t \binom{n-2k}{i-k}^{-\frac{1}{2}} \binom{n-2k}{j-k}^{-\frac{1}{2}} \beta^t_{i,j,k} x^t_{i,j} \right)_{i,j=k}^{n-k}.$$

B. Application to coding

Let $C \subseteq \mathcal{P}$ be any code. It will be convenient to assume $\emptyset \neq C \neq \mathcal{P}$.

Let Π be the set of (distance-preserving) automorphisms π of $\mathcal{P}$ with $\emptyset \in \pi(C)$, and let Π' be the set of automorphisms π of $\mathcal{P}$ with $\emptyset \notin \pi(C)$. Let $\chi^{\pi(C)}$ denote the incidence vector of $\pi(C)$ in $\{0,1\}^{\mathcal{P}}$ (taken as *column* vector). Define the $\mathcal{P}\times\mathcal{P}$ matrices R and R' by:

$$(9) \qquad R := \sum_{\pi\in\Pi} |\Pi|^{-1}\chi^{\pi(C)}(\chi^{\pi(C)})^{\mathsf{T}} \text{ and}$$
$$R' := \sum_{\pi\in\Pi'} |\Pi'|^{-1}\chi^{\pi(C)}(\chi^{\pi(C)})^{\mathsf{T}}.$$

As R and R' are sums of positive semidefinite matrices, they are positive semidefinite. Moreover, R and R' belong to $\mathcal{A}_n$. To see this, define

$$(10) \qquad x^t_{i,j} := \frac{1}{|C|\binom{n}{i-t,j-t,t}}\lambda^t_{i,j},$$

where $\binom{a}{b_1,\ldots,b_m}$ denotes the number of pairwise disjoint subsets of a set of size a, of sizes $b_1,\ldots,b_m$ respectively, and where

(11) $\lambda^t_{i,j}$:= the number of triples $(X,Y,Z) \in C^3$ with $|X\triangle Y| = i$, $|X\triangle Z| = j$, and $|(X\triangle Y)\cap(X\triangle Z)| = t$.

We set $x^t_{i,j} = 0$ if $\binom{n}{i-t,j-t,t} = 0$.

Then

Proposition 1:

$$(12) \qquad R = \sum_{i,j,t} x^t_{i,j} M^t_{i,j} \text{ and}$$
$$R' = \frac{|C|}{2^n - |C|}\sum_{i,j,t}(x^0_{i+j-2t,0} - x^t_{i,j})M^t_{i,j}.$$

Proof: Consider any $X \in \mathcal{P}$, and let Π_X be the set of automorphisms π of $\mathcal{P}$ with $\pi(X) = \emptyset$. So $|\Pi_X| = n!$. Let

$$(13) \qquad R_X := \sum_{\pi\in\Pi_X} |\Pi_X|^{-1}\chi^{\pi(C)}(\chi^{\pi(C)})^{\mathsf{T}}.$$

As the value of $(R_X)_{Y,Z}$ only depends on $|X\triangle Y|$, $|X\triangle Z|$, and $|(X\triangle Y)\cap(X\triangle Z)|$, we know that R_X belongs to $\mathcal{A}_n$. In fact,

$$(14) \qquad R_X = \sum_{i,j,t}\binom{n}{i-t,j-t,t}^{-1}\lambda^{t,X}_{i,j}M^t_{i,j},$$

where $\lambda^{t,X}_{i,j}$ is the number of pairs $(Y,Z) \in C^2$ with $|X\triangle Y| = i$, $|X\triangle Z| = j$, and $|(X\triangle Y)\cap(X\triangle Z)| = t$.

Equation (14) follows from the fact that for any $\pi \in \Pi_X$ and for all i,j,t, the number of 1's of $\chi^{\pi(C)}(\chi^{\pi(C)})^{\mathsf{T}}$ in positions where $M^t_{i,j}$ is 1, is equal to $\lambda^{t,X}_{i,j}$. As there are $\binom{n}{i-t,j-t,t}$ such positions, we obtain (14).

Now $R = \sum_{X\in C}|C|^{-1}R_X$ and $R' = \sum_{X\in\mathcal{P}\setminus C}(2^n - |C|)^{-1}R_X$. Moreover,

$$(15) \qquad \sum_{X\in C}\lambda^{t,X}_{i,j} = \lambda^t_{i,j}$$

and

$$(16) \qquad \sum_{X\in\mathcal{P}\setminus C}\lambda^{t,X}_{i,j} = \binom{i+j-2t}{i-t}\binom{n-i-j+2t}{t}\lambda^0_{i+j-2t,0} - \lambda^t_{i,j}.$$

The latter expression follows from

(17) $$\sum_{X\in\mathcal{P}} \lambda_{i,j}^{t,X} = \binom{i+j-2t}{i-t}\binom{n-i-j+2t}{t}\lambda_{i+j-2t,0}^{0},$$

which holds since for any pair $(Y,Z)\in C^2$ with $|Y\triangle Z| = i+j-2t$, the number of sets $X\in\mathcal{P}$ with $|X\triangle Y| = i$, $|X\triangle Z| = j$, and $|(X\triangle Y)\cap(X\triangle Z)| = t$ is equal to $\binom{i+j-2t}{i-t}\binom{n-i-j+2t}{t}$.

Since $|\Pi| = |C|n!$ and $|\Pi'| = (2^n - |C|)n!$, and since

(18) $$\binom{n}{i-t,j-t,t}^{-1}\binom{i+j-2t}{i-t}\binom{n-i-j+2t}{t} = \binom{n}{i+j-2t}^{-1},$$

(14) gives (12). ■

The positive semidefiniteness of R and R' is by (8) equivalent to:

(19) for each $k = 0,\dots,\lfloor\frac{n}{2}\rfloor$, the matrices

$$\left(\sum_{t=0}^{n}\beta_{i,j,k}^{t}x_{i,j}^{t}\right)_{i,j=k}^{n-k}$$

and

$$\left(\sum_{t=0}^{n}\beta_{i,j,k}^{t}(x_{i+j-2t,0}^{0} - x_{i,j}^{t})\right)_{i,j=k}^{n-k}$$

are positive semidefinite.

(We have deleted the factor $\binom{n-2k}{i-k}^{-\frac{1}{2}}\binom{n-2k}{j-k}^{-\frac{1}{2}}$ as it makes the coefficients integer, while positive semidefiniteness is maintained.)

The $x_{i,j}^{t}$'s moreover satisfy the following constraints, where (iv) holds if C has minimum distance at least d:

(20)
(i) $x_{0,0}^{0} = 1$,
(ii) $0 \le x_{i,j}^{t} \le x_{i,0}^{0}$ and $x_{i,0}^{0} + x_{j,0}^{0} \le 1 + x_{i,j}^{t}$ for all $i,j,t\in\{0,\dots,n\}$,
(iii) $x_{i,j}^{t} = x_{i',j'}^{t'}$ if $(i',j',i'+j'-2t')$ is a permutation of $(i,j,i+j-2t)$,
(iv) $x_{i,j}^{t} = 0$ if $\{i,j,i+j-2t\}\cap\{1,\dots,d-1\}\neq\emptyset$.

(Condition (ii) follows from the fact that each row of R and R' is nonnegative and is dominated by its diagonal entry (by (9)). Conditions (iii) and (iv) follow from the fact that $\lambda_{i,j}^{t}$ is equal to the number of triples (X,Y,Z) in C^3 with $|X\triangle Y| = i$, $|X\triangle Z| = j$, and $|Y\triangle Z| = i+j-2t$, as follows directly from (11).)

Moreover,

(21) $$|C| = \sum_{i=0}^{n}\binom{n}{i}x_{i,0}^{0},$$

since $|C|^2 = \sum_{i=0}^{n}\lambda_{i,0}^{0}$. Hence we obtain an upper bound on $A(n,d)$ by considering the $x_{i,j}^{t}$ as variables, and by

(22) maximizing $\sum_{i=0}^{n}\binom{n}{i}x_{i,0}^{0}$ subject to conditions (19) and (20).

This is a semidefinite programming problem with $O(n^3)$ variables, and it can be solved in time polynomial in n. (A generic form of a semidefinite programming problem is: given $c_1,\dots,c_t\in\mathbb{R}$ and real symmetric matrices $A_0,\dots,A_t,B$ (of equal dimensions), find $x_1,\dots,x_t\in\mathbb{R}$ that maximize $\sum_i c_ix_i$ subject to the condition that $(\sum_i x_iA_i)-B$ is positive semidefinite. If all A_i and B are diagonal matrices, we have a linear programming problem. Under certain conditions (which are satisfied in the present case), semidefinite programming problems can be solved in polynomial time. For background on semidefinite programming we refer to Todd [15] and Wright [17].)

One may reduce the number of variables by using the well-known facts that if d is odd then $A(n,d) = A(n+1,d+1)$ and that if d is even then $A(n,d)$ is attained by a code with all code words having even Hamming weights. So one can put $x_{i,j}^{t} = 0$ if i or j is odd.

The method gives, in the range $n\le 28$, the new upper bounds on $A(n,d)$ given in Table I (cf. the tables given by Best, Brouwer, MacWilliams, Odlyzko, and Sloane [3] and Agrell, Vardy, and Zeger [2]; $A(25,8)\le 5557$ and $A(26,10)\le 989$ were shown by Mounits, Etzion, and Litsyn [11], $A(22,10)\ge 64$ by Östergård [12], and $A(25,10)\ge 192$ and $A(26,10)\ge 384$ by Elssel and Zimmermann [5] (see also Andries Brouwer's website http://www.win.tue.nl/∼aeb/codes/binary-1.html)).

n	d	best lower bound known	new upper bound	best upper bound previously known	Delsarte bound
19	6	1024	1280	1288	1289
23	6	8192	13766	13774	13775
25	6	16384	47998	48148	48148
19	8	128	142	144	145
20	8	256	274	279	290
25	8	4096	5477	5557	6474
27	8	8192	17768	17804	18189
28	8	16384	32151	32204	32206
22	10	64	87	88	95
25	10	192	503	549	551
26	10	384	886	989	1040

TABLE I
NEW UPPER BOUNDS ON $A(n,d)$

Our computations were done by the algorithm SDPT3 version 3.02 (cf. Tütüncü, Toh, and Todd [16]), which is available through the web on the NEOS Server for Optimization (http://www-neos.mcs.anl.gov/neos/server-solvers.html#SDP). The answers have been confirmed by the algorithm DSDP version 5.5, available on the same server.

We note that the new bound is stronger than the Delsarte bound, which is equal to the maximum value of $\sum_i\binom{n}{i}x_{i,0}^{0}$ subject to the condition that $x_{i,0}^{0}\ge 0$ for all i and $x_{i,0}^{0} = 0$ if $1\le i\le d-1$, and to the condition that

(23) $$\sum_{i,j,t} x_{i+j-2t,0}^{0}M_{i,j}^{t} \text{ is positive semidefinite.}$$

(This matrix belongs to the Bose-Mesner algebra, which is a subalgebra of $\mathcal{A}_n$.) The latter condition is equivalent to the Delsarte inequalities (involving the Krawtchouk polynomial). (Then the variables different from the $x^0_{i,0}$ are superfluous and can be deleted.) Condition (23) is a consequence of the positive semidefiniteness of the matrices

$$(24)\qquad \sum_{i,j,t} x^t_{i,j} M^t_{i,j} \text{ and } \sum_{i,j,t} (x^0_{i+j-2t,0} - x^t_{i,j}) M^t_{i,j},$$

which is, as we saw, equivalent to (19).

A sharpening of the bound can be obtained by adding the conditions (for appropriate i)

$$(25)\qquad \tbinom{n}{i} x^0_{i,0} \leq A^*(n,d,i),$$

where $A^*(n,d,i)$ is any upper bound on the maximum size of a constant-weight code of word length n, minimum distance at least d, and constant weight i. Adding these constraints to the new bound seems less effective than adding them to the Delsarte bound, as the new bound implicitly contains the Delsarte bound for the Johnson schemes. Using known upper bounds $A^*(n,d,i)$, we did not obtain in this way any improvement in the above table.

C. Some background

Above we have introduced the Terwilliger algebra of the Hamming cube in a way that is convenient for our purposes, which differs slightly from the usual (but equivalent) definition. In the usual terminology, we consider the Terwilliger algebra $T = T(\mathbf{0})$ of the Hamming cube $H(n,2)$ with respect to $\mathbf{0}$. This is the algebra generated by the $\mathcal{P} \times \mathcal{P}$ 0,1 matrices A_d and E^*_d for $d = 0, \ldots, n$, where $(A_d)_{X,Y} = 1 \iff |X \triangle Y| = d$, and $(E^*_d)_{X,Y} = 1 \iff X = Y$ and $|X| = d$. Then $M^t_{i,j} = E^*_i A_{i+j-2t} E^*_j$ for all i,j,t. Conversely, $A_d = \sum_{i,j,t; i+j-2t=d} M^t_{i,j}$ and $E^*_d = M^d_{d,d}$ for each d. So $T(\mathbf{0})$ coincides with our algebra $\mathcal{A}_n$.

Basic properties of the Terwilliger algebra of the Hamming cube were found by Go [6]. In particular, Go identified the irreducible T-modules of the algebra, which implies the block sizes and block multiplicities of $\mathcal{A}_n$. Go also described bases for these modules. Our paper needs, and gives, a more explicit description of these bases. It also yields an explicit decomposition of the Terwilliger algebra into irreducible constituents.

The present research roots in two basic papers presenting eigenvalue techniques to obtain upper bounds: Delsarte [4], giving a bound on codes based on association schemes, and Lovász [7], giving a bound on the Shannon capacity of a graph. It was shown by McEliece, Rodemich, and Rumsey [10] and Schrijver [13] that the Delsarte bound is a special case of (a close variant of) the Lovász bound. (This is not to say that the Lovász bound supersedes the Delsarte bound: essential in the latter bound is a reduction of the 2^n-vertex graph problem to a linear programming problem of order n.) An extension of the Lovász bound based on 'matrix cuts' was given by Lovász and Schrijver [8]. Applying a variant of matrix cuts to the coding problem leads to considering the Terwilliger algebra as above.

II. Block-diagonalisation of the Terwilliger algebra

In this section we show that (8) indeed describes the block-diagonalisation of $\mathcal{A}_n$. For $k = 0, \ldots, \lfloor \frac{n}{2} \rfloor$, let L_k be the linear space

$$(26)\qquad L_k := \{b \in \mathbb{R}^{\mathcal{P}} \mid M^{k-1}_{k-1,k} b = 0, \text{ and } b_X = 0 \text{ if } |X| \neq k\}.$$

Then

$$(27)\qquad M^i_{i,k} b = 0 \text{ for all } i < k \text{ and } b \in L_k,$$

since $M^i_{i,k-1} M^{k-1}_{k-1,k} = (k-i) M^i_{i,k}$.

The dimension of L_k is given by:

$$(28)\qquad \dim L_k = \tbinom{n}{k} - \tbinom{n}{k-1},$$

since:

Proposition 2: For each $k \leq \lfloor \frac{n}{2} \rfloor$, $M^{k-1}_{k-1,k}$ has rank $\binom{n}{k-1}$.

Proof: We have

$$(29)\qquad M^{k-1}_{k-1,k} M^{k-1}_{k,k-1} = M^{k-2}_{k-1,k-2} M^{k-2}_{k-2,k-1} + (n-2k+2) M^{k-1}_{k-1,k-1}.$$

As $M^{k-2}_{k-1,k-2} M^{k-2}_{k-2,k-1}$ is positive semidefinite, as $n - 2k + 2 > 0$, and as $M^{k-1}_{k-1,k-1}$ is positive semidefinite of rank $\binom{n}{k-1}$, we know that $M^{k-1}_{k-1,k} M^{k-1}_{k,k-1}$ has rank $\binom{n}{k-1}$. Hence also $M^{k-1}_{k-1,k}$ has rank $\binom{n}{k-1}$. ■

The following formula is basic to our results (note that $c^{\mathsf{T}} b = 0$ if $c \in L_l$, $b \in L_k$, and $l \neq k$):

Proposition 3: For $i,j,k,l,t \in \{0, \ldots, n\}$ with $k, l \leq \lfloor \frac{n}{2} \rfloor$, and for $c \in L_l$, $b \in L_k$:

$$(30)\qquad c^{\mathsf{T}} M^l_{l,i} M^t_{i,j} M^k_{j,k} b = \beta^t_{i,j,k} c^{\mathsf{T}} b.$$

Proof: First we have for each $s \in \{0, \ldots, n\}$:

$$(31)\qquad M^s_{l,s} M^s_{s,k} = \sum_{p=0}^{n} \tbinom{p}{s} M^p_{l,k},$$

since the entry of this matrix in position (X,Y), with $|X| = l$ and $|Y| = k$, is equal to the number of common subsets of X and Y of size s.

Equation (31) implies for all $l,k,p \in \{0, \ldots, n\}$:

$$(32)\qquad M^p_{l,k} = \sum_{s=0}^{n} (-1)^{s-p} \tbinom{s}{p} M^s_{l,s} M^s_{s,k},$$

since

$$\text{(33)}\quad \sum_{s=0}^{n}(-1)^{s-p}\binom{s}{p}M^s_{l,s}M^s_{s,k} = \sum_{s=0}^{n}(-1)^{s-p}\binom{s}{p}\sum_{t=0}^{n}\binom{t}{s}M^t_{l,k} = \sum_{t=0}^{n}\sum_{s=0}^{n}(-1)^{s-p}\binom{s}{p}\binom{t}{s}M^t_{l,k} = \sum_{t=0}^{n}\delta_{t,p}M^t_{l,k} = M^p_{l,k},$$

where $\delta_{t,p}=1$ if $t=p$, and $\delta_{t,p}=0$ else.

Equation (32) implies that for all $l,k,p \in \{0,\dots,n\}$ and $b \in L_k$:

$$\text{(34)}\quad M^p_{l,k}b = (-1)^{k-p}\binom{k}{p}M^k_{l,k}b,$$

since $M^s_{l,s}M^s_{s,k}b = 0$ if $s \neq k$: if $s<k$ then $M^s_{s,k}b=0$ (by (27)) and if $s>k$ then $M^s_{s,k}=\mathbf{0}$.

Equation (34) implies

$$\text{(35)}\quad M^p_{p,j}M^k_{j,k}b = \binom{n-k-p}{j-p}M^k_{p,k}b,$$

since

$$\text{(36)}\quad M^p_{p,j}M^k_{j,k}b = \sum_{t=0}^{n}\binom{n-p-k+t}{n-j}M^t_{p,k}b = \sum_{t=0}^{n}\binom{n-p-k+t}{n-j}(-1)^{k-t}\binom{k}{t}M^k_{p,k}b = \binom{n-k-p}{j-p}M^k_{p,k}b.$$

We finally obtain (30) (using (32) and three times (35)):

$$\text{(37)}\quad c^\mathsf{T}M^l_{l,i}M^t_{i,j}M^k_{j,k}b = \sum_{p=0}^{n}(-1)^{t-p}\binom{p}{t}c^\mathsf{T}M^l_{l,i}M^p_{i,p}M^p_{p,j}M^k_{j,k}b = \sum_{p=0}^{n}(-1)^{t-p}\binom{p}{t}\binom{n-l-p}{i-p}\binom{n-k-p}{j-p}c^\mathsf{T}M^l_{l,p}M^k_{p,k}b = \sum_{p=0}^{n}(-1)^{t-p}\binom{p}{t}\binom{n-l-p}{i-p}\binom{n-k-p}{j-p}\binom{n-l-k}{n-p-k}c^\mathsf{T}M^k_{l,k}b.$$

By (27), the latter expression is nonzero only if $l=k$, in which case it is equal to $\beta^t_{i,j,k}c^\mathsf{T}b$. Since $c^\mathsf{T}b=0$ if $l\neq k$, this proves the proposition. ∎

This implies:

Proposition 4: For $i,j,k,l \in \{0,\dots,n\}$ with $k,l \leq \lfloor\frac{n}{2}\rfloor$, and for $c\in L_l$, $b \in L_k$:

$$\text{(38)}\quad c^\mathsf{T}M^l_{l,i}M^k_{j,k}b = \begin{cases}\binom{n-2k}{i-k}c^\mathsf{T}b & \text{if } l=k,\ i=j,\\ 0 & \text{otherwise.}\end{cases}$$

Proof: Since $M^l_{l,i}M^k_{j,k}=\mathbf{0}$ if $i\neq j$, we can assume $i=j$. Then

$$\text{(39)}\quad c^\mathsf{T}M^l_{l,i}M^k_{i,k}b = c^\mathsf{T}M^l_{l,i}M^i_{i,i}M^k_{i,k}b.$$

If $l \neq k$, this is 0 by (30). If $l=k$, then, again by (30), it is equal to $\beta^i_{i,i,k}c^\mathsf{T}b = \binom{n-2k}{i-k}c^\mathsf{T}b$. ∎

For each $k=0,\dots,\lfloor\frac{n}{2}\rfloor$, choose an orthonormal basis $\mathcal{B}_k$ of L_k. By (28), $|\mathcal{B}_k| = \binom{n}{k}-\binom{n}{k-1}$. Let

$$\text{(40)}\quad V := \{(k,b,i) \mid k\in\{0,\dots,\lfloor\tfrac{n}{2}\rfloor\}, b\in\mathcal{B}_k, i\in\{k,k+1,\dots,n-k\}\}.$$

Then

$$\text{(41)}\quad |V| = 2^n,$$

since

$$\text{(42)}\quad |V| = \sum_{i=0}^{n}\sum_{k=0}^{\min\{i,n-i\}}\left(\binom{n}{k}-\binom{n}{k-1}\right) = \sum_{i=0}^{n}\binom{n}{\min\{i,n-i\}} = \sum_{i=0}^{n}\binom{n}{i} = 2^n.$$

For each $(k,b,i)\in V$, define $u_{k,b,i}\in\mathbb{R}^{\mathcal{P}}$ by

$$\text{(43)}\quad u_{k,b,i} := \binom{n-2k}{i-k}^{-\frac{1}{2}}M^k_{i,k}b.$$

With (41), Proposition 4 implies that the $u_{k,b,i}$'s form an orthonormal basis for $\mathbb{R}^{\mathcal{P}}$. Let U be the $\mathcal{P}\times V$ matrix whose (k,b,i)-th column equals $u_{k,b,i}$, for $(k,b,i)\in V$. Then for each triple i,j,t, the matrix $\widetilde{M^t_{i,j}} := U^\mathsf{T}M^t_{i,j}U$ is in block-diagonal form. This will follow from:

Proposition 5: For $(l,c,i'),(k,b,j') \in V$ and $i,j,t \in \{0,\dots,n\}$:

$$\text{(44)}\quad (\widetilde{M^t_{i,j}})_{(l,c,i'),(k,b,j')} = \begin{cases}\binom{n-2k}{i-k}^{-\frac{1}{2}}\binom{n-2k}{j-k}^{-\frac{1}{2}}\beta^t_{i,j,k} & \text{if } l=k, i=i', j=j',\\ & \text{and } b=c,\\ 0 & \text{otherwise.}\end{cases}$$

Proof: We have

$$\text{(45)}\quad (\widetilde{M^t_{i,j}})_{(l,c,i'),(k,b,j')} = u^\mathsf{T}_{l,c,i'}M^t_{i,j}u_{k,b,j'} = \binom{n-2l}{i'-l}^{-\frac{1}{2}}\binom{n-2k}{j'-k}^{-\frac{1}{2}}c^\mathsf{T}M^l_{l,i'}M^t_{i,j}M^k_{j',k}b.$$

This is 0 if $i'\neq i$ or $j'\neq j$. So we can assume that $i=i'$ and $j=j'$. Then (30) and (45) imply (44). ∎

This implies that each matrix in $U^\mathsf{T}\mathcal{A}_nU$ is a block-diagonal matrix determined by the partition of V into the classes

$$\text{(46)}\quad V_{k,b} := \{(k,b,i) \mid k\leq i\leq n-k\},$$

for $k=0,\dots,\lfloor\frac{n}{2}\rfloor$ and $b\in\mathcal{B}_k$. Indeed, if $(l,c,i'),(k,b,j')\in V$ then $(\widetilde{M^t_{i,j}})_{(l,c,i'),(k,b,j')}=0$ if $l\neq k$ or $c\neq b$.

Moreover, for $k \in \{0, \ldots, \lfloor \frac{n}{2} \rfloor\}$, $b, c \in \mathcal{B}_k$, and $i', j' \in \{k, \ldots, n-k\}$ we have by (44)

$$(\widetilde{M}^t_{i,j})_{(k,b,i'),(k,b,j')} = (\widetilde{M}^t_{i,j})_{(k,c,i'),(k,c,j')}. \tag{47}$$

So for each fixed k, the blocks determined by the $V_{k,b}$ (over $b \in \mathcal{B}_k$) are equal.

For each k and each $b \in \mathcal{B}_k$, the block determined by $V_{k,b}$ has size $|V_{k,b}| = n - 2k + 1$. Now

$$\sum_{k=0}^{\lfloor \frac{n}{2} \rfloor} (n-2k+1)^2 = \binom{n+3}{3}. \tag{48}$$

(Proof: Induction on n. It is true for $n = 0$ and $n = 1$. Moreover, $\binom{n+3}{3} - \binom{n+1}{3} = \frac{1}{6}((n+3)(n+2)(n+1) - (n+1)n(n-1)) = \frac{1}{6}((n^3+6n^2+11n+6) - (n^3-n)) = \frac{1}{6}(6n^2+12n+6) = (n+1)^2$.)

As $\binom{n+3}{3}$ is the dimension of $\mathcal{A}_n$ (by (3)), we can conclude that $\mathcal{A}_n$ is (as an algebra) isomorphic to the direct sum

$$\bigoplus_{k=0}^{\lfloor \frac{n}{2} \rfloor} \mathbb{C}^{V_{k,b_k} \times V_{k,b_k}}, \tag{49}$$

where b_k is an arbitrary element of $\mathcal{B}_k$.

In other words, define, for each $k = 0, \ldots, \lfloor \frac{n}{2} \rfloor$,

$$N_k := \{k, k+1, \ldots, n-k\}. \tag{50}$$

Then the kth block B_k belongs to $\mathbb{C}^{N_k \times N_k}$, and (using (44)):

Theorem 1: $\mathcal{A}_n$ is isomorphic to $\bigoplus_{k=0}^{\lfloor \frac{n}{2} \rfloor} \mathbb{C}^{N_k \times N_k}$, where (2) maps in $\mathbb{C}^{N_k \times N_k}$ to matrix

$$\left(\sum_t \binom{n-2k}{i-k}^{-\frac{1}{2}} \binom{n-2k}{j-k}^{-\frac{1}{2}} \beta^t_{i,j,k} x^t_{i,j} \right)_{i,j=k}^{n-k}. \tag{51}$$

III. Constant-weight codes

We now go over to derive a similar bound for constant-weight codes, which is based on considering a tensor product of the algebra $\mathcal{A}_n$. In the previous sections we fixed n, but now it will be convenient to have n as parameter in our notation. Therefore, we will denote the objects $\mathcal{P}$, $M^t_{i,j}$, B_k, $\beta^t_{i,j,k}$, and U by $\mathcal{P}_n$, $M^{t,n}_{i,j}$, B^n_k, $\beta^{t,n}_{i,j,k}$, and U_n, respectively.

A. The algebras $\mathcal{A}_{w,v}$ and $\mathcal{B}_{w,v}$

Choose n and w with $w \leq n$, and define $v := n - w$. Let $\mathcal{A}_{w,v}$ be the C$*$-algebra generated by the tensor products[1] of matrices in $\mathcal{A}_w$ and $\mathcal{A}_v$. So $\mathcal{A}_{w,v}$ is equal to the set of matrices

$$\sum_{i,j,t,i',j',s} z^{t,s}_{i,j,i',j'} M^{t,w}_{i,j} \circ M^{s,v}_{i',j'} \tag{52}$$

with $z^{t,s}_{i,j,i',j'} \in \mathbb{C}$.

The algebra $\mathcal{A}_{w,v}$ can be brought into block-diagonal form by

$$(U_w \circ U_v)^\mathsf{T} \mathcal{A}_{w,v} (U_w \circ U_v), \tag{53}$$

since

$$(U_w \circ U_v)^\mathsf{T} (M^{t,w}_{i,j} \circ M^{s,v}_{i',j'})(U_w \circ U_v) = (U_w^\mathsf{T} M^{t,w}_{i,j} U_w) \circ (U_v^\mathsf{T} M^{s,v}_{i',j'} U_v) \tag{54}$$

for all i, j, i', j', t, s. Then the blocks of $\mathcal{A}_{w,v}$ are spanned by the tensor products $B^w_k \circ B^v_l$ of a block B^w_k of $\mathcal{A}_w$ and a block B^v_l of $\mathcal{A}_v$. Note that $B^w_k \circ B^v_l$ is a $(W_k \times V_l) \times (W_k \times V_l)$ matrix, where we denote

$$W_k := \{k, k+1, \ldots, w-k\} \text{ and } V_l := \{l, l+1, \ldots, v-l\}. \tag{55}$$

By Theorem 1 and by the definition of tensor product, matrix (52) maps in $B^w_k \circ B^v_l$ to the matrix

$$\left(\sum_{t,s} \binom{w-2k}{i-k}^{-\frac{1}{2}} \binom{w-2k}{j-k}^{-\frac{1}{2}} \binom{v-2l}{i'-l}^{-\frac{1}{2}} \binom{v-2l}{j'-l}^{-\frac{1}{2}} \cdot \beta^{t,w}_{i,j,k} \beta^{s,v}_{i',j',l} z^{t,s}_{i,j,i',j'} \right)_{(i,i'),(j,j') \in W_k \times V_l}. \tag{56}$$

We next consider the subalgebra $\mathcal{B}_{w,v}$ of $\mathcal{A}_{w,v}$ consisting of all matrices

$$\sum_{i,j,t,s} y^{t,s}_{i,j} M^{t,w}_{i,j} \circ M^{s,v}_{i,j}, \tag{57}$$

with $y^{t,s}_{i,j} \in \mathbb{C}$. So $\mathcal{B}_{w,v}$ consists of all matrices (52) with $z^{t,s}_{i,j,i',j'} = 0$ if $i \neq i'$ or $j \neq j'$.

The image (56) of (57) in block $B^w_k \circ B^v_l$ has zeros in positions $(i,i'),(j,j')$ with $i \neq i'$ or $j \neq j'$. Deleting these rows and columns, we obtain a block of order $|W_k \cap V_l|$ (of zero order if $W_k \cap V_l = \emptyset$). Then (57) maps in this block to

$$\left(\sum_{t,s} \binom{w-2k}{i-k}^{-\frac{1}{2}} \binom{w-2k}{j-k}^{-\frac{1}{2}} \binom{v-2l}{i-l}^{-\frac{1}{2}} \binom{v-2l}{j-l}^{-\frac{1}{2}} \cdot \beta^{t,w}_{i,j,k} \beta^{s,v}_{i,j,l} y^{t,s}_{i,j} \right)_{i,j \in W_k \cap V_l}, \tag{58}$$

where we have identified any $i \in W_k \cap V_l$ with the pair $(i,i) \in W_k \times V_l$.

This in fact gives the block-diagonalisation of $\mathcal{B}_{w,v}$. For consider any complex $(W_k \cap V_l) \times (W_k \cap V_l)$ matrix L. Extend L by zeros so as to obtain a $(W_k \times V_l) \times (W_k \times V_l)$ matrix L'. As (56) gives the block-diagonalisation of $\mathcal{A}_{w,v}$, we know that L' is equal to (56) for some $z^{t,s}_{i,j,i',j'}$. Resetting $z^{t,s}_{i,j,i',j'}$

[1]The *tensor product* of an $A \times B$ matrix M and a $C \times D$ matrix N is the $(A \times C) \times (B \times D)$ matrix $M \circ N$ given by $(M \circ N)_{(a,c),(b,d)} := M_{a,b} N_{c,d}$ for $(a,c) \in A \times C$ and $(b,d) \in B \times D$.

to 0 if $i \neq i'$ or $j \neq j'$ does not change L'. Hence L can be given as (58), for $y_{i,j}^{t,s} := z_{i,j,i,j}^{t,s}$.

Incidentally, this implies

$$\dim(\mathcal{B}_{w,v}) = \sum_{k=0}^{\lfloor \frac{w}{2} \rfloor} \sum_{l=0}^{\lfloor \frac{v}{2} \rfloor} |W_k \cap V_l|^2. \tag{59}$$

B. Application to constant-weight coding

We proceed as in Section I. Let $C \subseteq \mathcal{P}_n$ be any constant-weight code of word length n and constant weight w. Fix a set $X \in \mathcal{P}_n$ with $|X| = w$. We will identify $\mathcal{P}_n$ and $\mathcal{P}_w \times \mathcal{P}_v$, by identifying any $Y \in \mathcal{P}_n$ with the pair $(X \setminus Y, Y \setminus X) \in \mathcal{P}_w \times \mathcal{P}_v$.

Let Π be the set of (distance-preserving) automorphisms π of $\mathcal{P}_n$ fixing $\emptyset$ and with $X \in \pi(C)$, and let Π' be the set of automorphisms π of $\mathcal{P}_n$ fixing $\emptyset$ and with $X \notin \pi(C)$. Define the matrices R and R' by:

$$\begin{aligned} R &:= \sum_{\pi \in \Pi} |\Pi|^{-1} \chi^{\pi(C)} (\chi^{\pi(C)})^{\mathsf{T}} \text{ and} \\ R' &:= \sum_{\pi \in \Pi'} |\Pi'|^{-1} \chi^{\pi(C)} (\chi^{\pi(C)})^{\mathsf{T}}. \end{aligned} \tag{60}$$

Again, as R and R' are sums of positive semidefinite matrices, they are positive semidefinite. Moreover, R and R' belong to $\mathcal{B}_{w,v}$, using the identification of $\mathcal{P}_n$ and $\mathcal{P}_w \times \mathcal{P}_v$:

$$\begin{aligned} R &= \sum_{i,j,t,s} y_{i,j}^{t,s} M_{i,j}^{t,w} \circ M_{i,j}^{s,v} \text{ and} \\ R' &= \frac{|C|}{2^n - |C|} \sum_{i,j,t,s} (y_{i+j-t-s,0}^{0,0} - y_{i,j}^{t,s}) M_{i,j}^{t,w} \circ M_{i,j}^{s,v}, \end{aligned} \tag{61}$$

with

$$y_{i,j}^{t,s} := \frac{1}{|C| \binom{w}{i-t,j-t,t} \binom{v}{i-s,j-s,s}} \mu_{i,j}^{t,s}, \tag{62}$$

where

(63) $\mu_{i,j}^{t,s}$:= the number of triples $(X, Y, Z) \in C^3$ with $|X \setminus Y| = i$, $|X \setminus Z| = j$, $|(X \setminus Y) \cap (X \setminus Z)| = t$, and $|(Y \setminus X) \cap (Z \setminus X)| = s$.

The equations in (61) can be proved similarly as Proposition 1.

The positive semidefiniteness of R and R' is by (58) equivalent to:

(64) for each $k = 0, \ldots, \lfloor \frac{w}{2} \rfloor$ and $l = 0, \ldots, \lfloor \frac{v}{2} \rfloor$, the matrices

$$\left(\sum_{t,s} \beta_{i,j,k}^{t,w} \beta_{i,j,l}^{s,v} y_{i,j}^{t,s} \right)_{i,j \in W_k \cap V_l}$$

and

$$\left(\sum_{t,s} \beta_{i,j,k}^{t,w} \beta_{i,j,l}^{s,v} (y_{i+j-t-s,0}^{0,0} - y_{i,j}^{t,s}) \right)_{i,j \in W_k \cap V_l}$$

are positive semidefinite.

The $y_{i,j}^{t,s}$'s moreover satisfy the following constraints, where (iv) holds if C has minimum distance at least d:

(65)
- (i) $y_{0,0}^{0,0} = 1$,
- (ii) $0 \leq y_{i,j}^{t,s} \leq y_{i,0}^{0,0}$ and $y_{i,0}^{0,0} + y_{j,0}^{0,0} \leq 1 + y_{i,j}^{t,s}$ for all $i, j, t, s \in \{0, \ldots, \min\{w, v\}\}$,
- (iii) $y_{i,j}^{t,s} = y_{i',j'}^{t',s'}$ if $t' - s' = t - s$ and $(i', j', i' + j' - t' - s')$ is a permutation of $(i, j, i + j - t - s)$,
- (iv) $y_{i,j}^{t,s} = 0$ if $\{2i, 2j, 2(i + j - t - s)\} \cap \{1, \ldots, d - 1\} \neq \emptyset$.

(Condition (ii) follows from the fact that each row of R and R' is nonnegative and is dominated by its diagonal entry (by (60)). Conditions (iii) and (iv) follow from the fact that $\mu_{i,j}^{t,s}$ is equal to the number of triples (X, Y, Z) in C^3 with $|X \triangle Y| = 2i$, $|X \triangle Z| = 2j$, $|Y \triangle Z| = 2(i + j - t - s)$, and $|X \triangle Y \triangle Z| = w + 2t - 2s$, as follows directly from (63).)

Now

$$|C| = \sum_{i=0}^{\min\{w,v\}} \tbinom{w}{i} \tbinom{v}{i} y_{i,0}^{0,0}, \tag{66}$$

since $|C|^2 = \sum_{i=0}^{\min\{w,v\}} \mu_{i,0}^{0,0}$. Hence we obtain an upper bound on $A(n, d, w)$ by considering the $y_{i,j}^{t,s}$ as variables, and by

(67) maximizing $\displaystyle\sum_{i=0}^{\min\{w,v\}} \tbinom{w}{i} \tbinom{v}{i} y_{i,0}^{0,0}$ subject to conditions (64) and (65).

This is a semidefinite programming problem with $O(w^4)$ variables, and it can be solved in time polynomial in n. In the range $n \leq 28$, it gives the new bounds given in Table II (cf. the tables given by Best, Brouwer, MacWilliams, Odlyzko, and Sloane [3] and Agrell, Vardy, and Zeger [1], and Erik Agrell's website http://www.s2.chalmers.se/~agrell/bounds/cw.html). Note that it implies the exact value $A(23, 8, 11) = 1288$.

Again, this new bound strengthens the Delsarte bound for constant-weight codes, as can be seen by an argument similar to that given in Section I.

Acknowledgements. I thank Rob Ellis, Dion Gijswijt, Monique Laurent, and Dima Pasechnik for very helpful discussions and comments. I am moreover grateful to the two referees and to the editor, Khaled Abdel-Ghaffar, for useful suggestions as to the presentation of the results.

n	d	w	best lower bound known	new upper bound	best upper bound previously known	Delsarte bound
17	6	7	166	228	234	249
17	6	8	184	280	283	283
18	6	6	132	199	202	204
19	6	8	408	718	734	751
21	6	9	1184	2359	2364	2364
21	6	10	1454	2685	2702	2702
22	6	9	1792	3736	3775	3775
22	6	10	2182	4415	4416	4734
26	6	11	12037	42075	42081	42081
26	6	12	14836	50169	50204	52440
21	8	9	280	314	320	358
21	8	10	336	383	399	464
22	8	9	280	473	493	597
22	8	10	616	634	641	758
22	8	11	672	680	766	805
23	8	9	400	707	796	830
23	8	10	616	1025	1109	1111
23	8	11	1288	1288	1328	1417
24	8	9	640	1041	1143	1160
24	8	10	960	1551	1639	1639
24	8	11	1288	2142	2188	2305
25	8	9	829	1486	1610	1626
25	8	10	1248	2333	2448	2448
25	8	11	1662	3422	3575	3575
25	8	12	2576	4087	4169	4316
26	8	9	883	2108	2160	2282
26	8	10	1519	3496	3719	3719
26	8	11	1988	5225	5315	5416
26	8	12	3070	6741	6834	7634
26	8	13	3588	7080	7164	8030
27	8	10	1597	4986	5260	5260
27	8	11	2295	7833	7837	8381
27	8	13	4094	11981	11991	12883
28	8	10	1820	7016	7368	7368
28	8	12	4916	17011	17299	17299
28	8	13	4805	21152	21739	21739
28	8	14	6090	22710	23268	23268
22	10	10	46	72	73	82
22	10	11	46	80	81	88
24	10	9	56	118	119	119
25	10	11	125	380	388	388
25	10	12	132	434	464	465
26	10	10	130	406	410	412
26	10	11	168	566	581	621
26	10	12	195	702	728	842
26	10	13	210	754	869	897
27	10	10	162	571	577	579
27	10	11	222	882	900	1011
27	10	12	351	1201	1289	1306
27	10	13	405	1419	1460	1479
28	10	11	286	1356	1434	1453
28	10	12	365	1977	1981	1981
25	12	10	28	37	38	40
26	12	11	39	66	69	85
26	12	13	58	91	92	106
27	12	10	39	64	65	83
28	12	10	49	87	99	105

TABLE II

NEW UPPER BOUNDS ON $A(n, d, w)$

REFERENCES

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

[2] E. Agrell, A. Vardy, K. Zeger, "A table of upper bounds for binary codes," *IEEE Trans. Inform. Theory,* vol. IT-47, pp. 3004–3006, November 2001.

[3] M.R. Best, A.E. Brouwer, F.J. MacWilliams, A.M. Odlyzko, N.J.A. Sloane, "Bounds for binary codes of length less than 25," *IEEE Trans. Inform. Theory,* vol. IT-24, pp. 81–93, January 1978.

[4] P. Delsarte, "An algebraic approach to the association schemes of coding theory," *Philips Res. Repts. Suppl.,* no. 10, 1973.

[5] K. Elssel, K.-H. Zimmermann, "Two new nonlinear binary codes," *IEEE Trans. Inform. Theory,* vol IT-51, pp. 1189–1190, March 2005.

[6] J.T. Go, "The Terwilliger algebra of the hypercube," *European J. Combin.,* vol. 23, pp. 399–429, May 2002.

[7] L. Lovász, "On the Shannon capacity of a graph," *IEEE Trans. Inform. Theory,* vol. IT-25, pp. 1–7, January 1979.

[8] L. Lovász, A. Schrijver, "Cones of matrices and set-functions and 0–1 optimization," *SIAM J. Optim.,* vol. 1, pp. 166–190, May 1991.

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

[10] R.J. McEliece, E.R. Rodemich, H.C. Rumsey, Jr, "The Lovász bound and some generalizations," *J. Combin. Inform. System Sci.,* vol. 3 (no. 3), pp. 134–152, 1978.

[11] B. Mounits, T. Etzion, S. Litsyn, "Improved upper bounds on sizes of codes," *IEEE Trans. Inform. Theory,* vol. IT-48, pp. 880–886, April 2002.

[12] P.R.J. Östergård, "Two new four-error-correcting binary codes," preprint, 2003. Available: http://www.hut.fi/∼pat/papers/four.ps

[13] A. Schrijver, "A comparison of the Delsarte and Lovász bounds," *IEEE Trans. Inform. Theory,* vol. IT-25, pp. 425–429, July 1979.

[14] P. Terwilliger, "The subconstituent algebra of an association scheme (Part I)," *J. Algebraic Combin.,* vol. 1, pp. 363–388, December 1992.

[15] M.J. Todd, "Semidefinite optimization," *Acta Numer.,* vol. 10, pp. 515–560, May 2001.

[16] R.H. Tütüncü, K.C. Toh, M.J. Todd, "Solving semidefinite-quadratic-linear programs using SDPT3," *Math. Program., Series B,* vol. 95, pp. 189–217, February 2003.

[17] S.J. Wright, "Nonlinear and semidefinite programming," in: *Trends in Optimization*, Proc. Sympos. Appl. Math., 61, Providence, RI: Amer. Math. Soc., 2004, pp. 115–137.