New upper bounds for nonbinary codes based on the Terwilliger algebra and semidefinite programming

Dion Gijswijt*, Alexander Schrijver†, Hajime Tanaka‡

March 23, 2005

Abstract

We give a new upper bound on the maximum size $A_q(n,d)$ of a code of word length n and minimum Hamming distance at least d over the alphabet of $q \geq 3$ letters. By block-diagonalizing the Terwilliger algebra of the nonbinary Hamming scheme, the bound can be calculated in time polynomial in n using semidefinite programming. For $q = 3,4,5$ this gives several improved upper bounds for concrete values of n and d. This work is related to [6], where a similar approach is used to derive upper bounds for binary codes.

Keywords: codes, nonbinary codes, upper bounds, Delsarte bound, Terwilliger algebra, block-diagonalisation, semidefinite programming.

Fix integers $n \geq 1$ and $q \geq 2$, and fix an alphabet $\mathbf{q} = \{0, 1, \ldots, q-1\}$. We will consider q-ary codes of length n, that is subsets of $\mathbf{q}^n$. The Hamming distance $d(\mathbf{x}, \mathbf{y})$ of two words $\mathbf{x}$ and $\mathbf{y}$ is defined as the number of positions in which $\mathbf{x}$ and $\mathbf{y}$ differ. For a word $\mathbf{x} \in \mathbf{q}^n$, we denote the *support* of $\mathbf{x}$ by $S(\mathbf{x}) := \{v \mid \mathbf{x}_v \neq 0\}$. Note that $|S(\mathbf{x})| = d(\mathbf{x}, \mathbf{0})$, where $\mathbf{0}$ is the all-zero word.

Denote by $\mathrm{Aut}(q,n)$ the set of permutations of $\mathbf{q}^n$ that preserve the Hamming distance. It is not hard to see that $\mathrm{Aut}(q,n)$ consists of the permutations of $\mathbf{q}^n$ obtained by permuting the n coordinates followed by independently permuting the alphabet $\mathbf{q}$ at each of the n coordinates. If we consider the action of $\mathrm{Aut}(q,n)$ on the set $\mathbf{q}^n \times \mathbf{q}^n$, the orbits form an association scheme known as the nonbinary Hamming scheme $H(n,q)$, with association matrices $A_0, A_1, \ldots, A_n$ defined by

$$(A_i)_{\mathbf{x},\mathbf{y}} := \begin{cases} 1 & \text{if } d(\mathbf{x},\mathbf{y}) = i, \\ 0 & \text{otherwise,} \end{cases} \tag{1}$$

*Department of Mathematics, University of Amsterdam, Plantage Muidergracht 24, 1018 TV Amsterdam, The Netherlands (gijswijt@science.uva.nl).

†CWI and University of Amsterdam. Mailing adress: CWI, Kruislaan 413,1098 SJ Amsterdam, The Netherlands (lex@cwi.nl).

‡Division of Mathematics, Graduate School of Information Sciences, Tohoku University, Sendai, Japan (htanaka@ims.is.tohoku.ac.jp).

for $i = 0, 1, \ldots, n$. The association matrices span a commutative algebra called the Bose–Mesner algebra of the scheme. Diagonalizing the Bose–Mesner algebra yields the well-known linear programming bound of Delsarte [5], which gives a good upper bound on $A_q(n, d)$.

Here we will consider the action of $\mathrm{Aut}(q, n)$ on ordered triples of words, which will lead to a noncommutative algebra $\mathcal{A}_{q,n}$ containing the Bose–Mesner algebra. It turns out that the algebra coincides with the Terwilliger algebra [7] of $H(n, q)$. In section 3 it is shown how the algebra $\mathcal{A}_{q,n}$ can be used to obtain a new upper bound on $A_q(n, d)$. The bound is based on semidefinite programming and can be computed in time polynomial in n by using the block-diagonalisation constructed in section 2. The approach we follow is similar to the one in [6], which deals with binary codes. In fact we will use results from that paper to obtain our block-diagonalisation.

1 The Terwilliger algebra

To each ordered triple $(\mathbf{x}, \mathbf{y}, \mathbf{z}) \in \mathbf{q}^n \times \mathbf{q}^n \times \mathbf{q}^n$ we associate the four-tuple

$$\begin{aligned} d(\mathbf{x}, \mathbf{y}, \mathbf{z}) \quad := \quad & (i, j, t, p), \text{ where} \\ & i := d(\mathbf{x}, \mathbf{y}), \\ & j := d(\mathbf{x}, \mathbf{z}), \\ & t := |\{v \mid \mathbf{x}_v \neq \mathbf{y}_v \text{ and } \mathbf{x}_v \neq \mathbf{z}_v\}|, \\ & p := |\{v \mid \mathbf{x}_v \neq \mathbf{y}_v = \mathbf{z}_v\}|. \end{aligned} \tag{2}$$

Note that $d(\mathbf{y}, \mathbf{z}) = i + j - t - p$ and $|\{v \mid \mathbf{x}_v \neq \mathbf{y}_v \neq \mathbf{z}_v \neq \mathbf{x}_v\}| = t - p$. The set of four-tuples (i, j, t, p) that occur as $d(\mathbf{x}, \mathbf{y}, \mathbf{z})$ for some $\mathbf{x}, \mathbf{y}, \mathbf{z} \in \mathbf{q}^n$ is given by

$$\mathcal{I}(q, n) := \{(i, j, t, p) \mid 0 \leq p \leq t \leq i, j \text{ and } i + j \leq n + t\}, \tag{3}$$

and will index various objects defined below.

Proposition 1. *For $n \geq 1$ and $q \geq 3$, $|\mathcal{I}(q, n)| = \binom{n+4}{4}$.*

Proof. If we substitute $p' := p$, $t' := t - p$, $i' := i - t$ and $j' := j - t$, then the integer solutions of $0 \leq p \leq t \leq i, j, \quad i + j \leq n + t$ are in bijection with the integer solutions of $0 \leq p', t', i', j', \quad p' + t' + i' + j' \leq n$. □

The integers i, j, t, p parametrize the ordered triples of words up to symmetry. That is, if we define

$$X_{i,j,t,p} := \{(\mathbf{x}, \mathbf{y}, \mathbf{z}) \in \mathbf{q}^n \times \mathbf{q}^n \times \mathbf{q}^n \mid d(\mathbf{x}, \mathbf{y}, \mathbf{z}) = (i, j, t, p)\}, \tag{4}$$

for $(i, j, t, p) \in \mathcal{I}(q, n)$, we have the following.

Proposition 2. *The sets $X_{i,j,t,p}$, $(i, j, t, p) \in \mathcal{I}(q, n)$ are the orbits of $\mathbf{q}^n \times \mathbf{q}^n \times \mathbf{q}^n$ under the action of $\mathrm{Aut}(q, n)$.*

Proof. Let $\mathbf{x}, \mathbf{y}, \mathbf{z} \in \mathbf{q}^n$ and let $(i, j, t, p) = d(\mathbf{x}, \mathbf{y}, \mathbf{z})$. Since the Hamming distances $i, j, i + j - t - p$ and the number $t - p = |\{v \mid \mathbf{x}_v \neq \mathbf{y}_v \neq \mathbf{z}_v \neq \mathbf{x}_v\}|$ are unchanged when permuting the coordinates or permuting the elements of $\mathbf{q}$ at any coordinate, we have $d(\mathbf{x}, \mathbf{y}, \mathbf{z}) = d(\pi(\mathbf{x}), \pi(\mathbf{y}), \pi(\mathbf{z}))$ for any $\pi \in \text{Aut}(q, n)$.

Hence it suffices to show that there is an automorphism π such that $(\pi(\mathbf{x}), \pi(\mathbf{y}), \pi(\mathbf{z}))$ only depends upon i, j, t and p. By permuting $\mathbf{q}$ at the coordinates in the support of $\mathbf{x}$, we may assume that $\mathbf{x} = \mathbf{0}$. Let $A := \{v \mid \mathbf{y}_v \neq 0, \mathbf{z}_v = 0\}$, $B := \{v \mid \mathbf{y}_v = 0, \mathbf{z}_v \neq 0\}$, $C := \{v \mid \mathbf{y}_v \neq 0, \mathbf{z}_v \neq 0, \mathbf{y}_v \neq \mathbf{z}_v\}$ and $D := \{v \mid \mathbf{y}_v = \mathbf{z}_v \neq 0\}$. Note that $|A| = i - t$, $|B| = j - t$, $|C| = t - p$ and $|D| = p$. By permuting coordinates, we may assume that $A = \{1, 2, \ldots, i - t\}$, $B = \{i - t + 1, \ldots, i + j - 2t\}$, $C = \{i + j - 2t + 1, \ldots, i + j - t - p\}$ and $D = \{i + j - t - p + 1, \ldots, i + j - t\}$. Now by permuting $\mathbf{q}$ at each of the points in $A \cup B \cup C \cup D$, we can accomplish that $\mathbf{y}_v = 1$ for $v \in A \cup C \cup D$ and $\mathbf{z}_v = 2$ for $v \in B \cup C$ and $\mathbf{z}_v = 1$ for $v \in D$. $\square$

Denote the stabilizer of $\mathbf{0}$ in $\text{Aut}(q, n)$ by $\text{Aut}_0(q, n)$. For $(i, j, t, p) \in \mathcal{I}(q, n)$, let $M_{i,j}^{t,p}$ be the $\mathbf{q}^n \times \mathbf{q}^n$ matrix defined by:

$$(M_{i,j}^{t,p})_{\mathbf{x},\mathbf{y}} := \begin{cases} 1 & \text{if } |S(\mathbf{x})| = i,\ |S(\mathbf{y})| = j,\ |S(\mathbf{x}) \cap S(\mathbf{y})| = t,\ |\{v \mid \mathbf{x}_v = \mathbf{y}_v \neq 0\}| = p, \\ 0 & \text{otherwise.} \end{cases} \tag{5}$$

Let $\mathcal{A}_{q,n}$ be the set of matrices

$$\sum_{(i,j,t,p) \in \mathcal{I}(q,n)} x_{i,j}^{t,p} M_{i,j}^{t,p}, \tag{6}$$

where $x_{i,j}^{t,p} \in \mathbb{C}$. From Proposition 2 it follows that $\mathcal{A}_{q,n}$ is the set of matrices that are stable under permutations $\pi \in \text{Aut}_0(q, n)$ of the rows and columns. Hence $\mathcal{A}_{q,n}$ is a complex matrix algebra called the *centralizer algebra* (cf. [1]) of $\text{Aut}_0(q, n)$. The $M_{i,j}^{t,p}$ constitute a basis for $\mathcal{A}_{q,n}$ and hence

$$\dim \mathcal{A}_{q,n} = \binom{n+4}{4}, \tag{7}$$

by Proposition 1. Note that the algebra $\mathcal{A}_{q,n}$ contains the Bose–Mesner algebra since

$$A_k = \sum_{\substack{(i,j,t,p) \in \mathcal{I}(q,n) \\ i+j-t-p=k}} M_{i,j}^{t,p}. \tag{8}$$

Although it is not needed for the remainder of this paper, we would like to point out here, that $\mathcal{A}_{q,n}$ coincides with the Terwilliger algebra (see [7]) of the nonbinary Hamming scheme $H(n, q)$ (with respect to $\mathbf{0}$). The Terwilliger algebra $\mathcal{T}(q, n)$ is the complex matrix algebra generated by the association matrices $A_0, A_1, \ldots, A_n$ of the Hamming scheme and the diagonal matrices $E_0^*, E_1^*, \ldots, E_n^*$ defined by

$$(E_i^*)_{\mathbf{x},\mathbf{x}} := \begin{cases} 1 & \text{if } |S(\mathbf{x})| = i, \\ 0 & \text{otherwise,} \end{cases} \tag{9}$$

for $i = 0, 1, \ldots, n$.

Proposition 3. *The algebras $\mathcal{A}_{q,n}$ and $\mathcal{T}_{q,n}$ coincide.*

Proof. Since $\mathcal{A}_{q,n}$ contains the matrices A_k and the matrices $E_k^* = M_{k,k}^{k,k}$ for $k = 0, 1, \ldots, n$, it follows that $\mathcal{T}_{q,n}$ is a subalgebra of $\mathcal{A}_{q,n}$. To show the reverse inclusion, define the zero-one matrices $B_i, C_i, D_i \in \mathcal{T}_{q,n}$ by

$$\begin{aligned} B_i &:= E_i^* A_1 E_i^*, \\ C_i &:= E_i^* A_1 E_{i+1}^*, \\ D_i &:= E_i^* A_1 E_{i-1}^*. \end{aligned} \tag{10}$$

Observe that:

$$\begin{aligned} (B_i)_{\mathbf{x},\mathbf{y}} &= 1 \quad \text{if and only if} \\ &\quad |S(\mathbf{x})| = i, d(\mathbf{x},\mathbf{y}) = 1, |S(\mathbf{y})| = i, S(\mathbf{x}) = S(\mathbf{y}), \\ (C_i)_{\mathbf{x},\mathbf{y}} &= 1 \quad \text{if and only if} \\ &\quad |S(\mathbf{x})| = i, d(\mathbf{x},\mathbf{y}) = 1, |S(\mathbf{y})| = i+1, |S(\mathbf{x})\Delta S(\mathbf{y})| = 1, \\ (D_i)_{\mathbf{x},\mathbf{y}} &= 1 \quad \text{if and only if} \\ &\quad |S(\mathbf{x})| = i, d(\mathbf{x},\mathbf{y}) = 1, |S(\mathbf{y})| = i-1, |S(\mathbf{x})\Delta S(\mathbf{y})| = 1. \end{aligned} \tag{11}$$

For given $(i, j, t, p) \in \mathcal{I}(q, n)$, let $A_{i,j}^{t,p} \in \mathcal{T}_{q,n}$ be given by

$$A_{i,j}^{t,p} := (D_i D_{i-1} \cdots D_{t+1})(C_t C_{t+1} \cdots C_{j-1})(B_j)^{t-p}. \tag{12}$$

Then for words $\mathbf{x}, \mathbf{y} \in \mathbf{q}^n$, the entry $(A_{i,j}^{t,p})_{\mathbf{x},\mathbf{y}}$ counts the number of $(i + j - t - p + 3)$-tuples

$$\mathbf{x} = \mathbf{d}_i, \mathbf{d}_{i-1}, \ldots, \mathbf{d}_t = \mathbf{c}_t, \mathbf{c}_{t+1}, \ldots, \mathbf{c}_j = \mathbf{b}_0, \ldots, \mathbf{b}_{t-p} = \mathbf{y} \in \mathbf{q}^n$$

where any two consecutive words have Hamming distance 1, the $\mathbf{b}_k$ have equal support of cardinality j, and $|S(\mathbf{d}_k)| = k$, $|S(\mathbf{c}_k)| = k$ for all k. Hence for $\mathbf{x}, \mathbf{y} \in \mathbf{q}^n$ the following holds.

$$(A_{i,j}^{t,p})_{\mathbf{x},\mathbf{y}} = 0 \quad \text{if } d(\mathbf{x},\mathbf{y}) > i + j - t - p \text{ or } |S(\mathbf{x})\Delta S(\mathbf{y})| > i + j - 2t \tag{13}$$

and

$$\begin{aligned} (A_{i,j}^{t,p})_{\mathbf{x},\mathbf{y}} > 0 \quad &\text{if } |S(\mathbf{x})| = i,\ |S(\mathbf{y})| = j, \\ &d(\mathbf{x},\mathbf{y}) = i + j - t - p \text{ and } |S(\mathbf{x})\Delta S(\mathbf{y})| = i + j - 2t. \end{aligned} \tag{14}$$

To see (14) one may take for $\mathbf{d}_k$ the zero-one word with support $\{i + 1 - k, \ldots, i\}$, for $\mathbf{c}_k$ the zero-one word with support $\{i + 1 - t, \ldots, i + k - t\}$ and for $\mathbf{b}_k$ the word with support $\{i + 1 - t, \ldots, i + j - t\}$ where the first k nonzero entries are 2 and the other nonzero entries are 1.

Now suppose that $\mathcal{A}_{q,n}$ is not contained in $\mathcal{T}_{q,n}$, and let $M_{i,j}^{t,p}$ be a matrix not in $\mathcal{T}_{q,n}$ with t maximal and (secondly) p maximal. If we write

$$A_{i,j}^{t,p} = \sum_{t',p'} x_{i,j}^{t',p'} M_{i,j}^{t',p'}, \tag{15}$$

then by (13) $x_{i,j}^{t',p'} = 0$ if $t' + p' < t + p$ or $t' < t$ implying that $A_{i,j}^{t,p} - x_{i,j}^{t,p} M_{i,j}^{t,p} \in \mathcal{T}_{q,n}$ by the maximality assumption. Therefore since $x_{i,j}^{t,p} > 0$ by (14), also $M_{i,j}^{t,p}$ belongs to $\mathcal{T}_{q,n}$, a contradiction. □

2 Block-diagonalisation of the Terwilliger algebra

In this section we give an explicit block-diagonalisation of the algebra $\mathcal{A}_{q,n}$. The block-diagonalisation can be seen as an extension of the block-diagonalisation in the binary case as given in [6]. In fact, we will use some results of this paper, summarized in Proposition 4 below.

For a finite set V of cardinality m and nonnegative integers i, j, define the $2^V \times 2^V$ matrix $C_{i,j}^V$ by

$$(C_{i,j}^V)_{I,J} := \begin{cases} 1 & \text{if } |I| = i,\ |J| = j,\ I \subseteq J \text{ or } J \subseteq I, \\ 0 & \text{otherwise.} \end{cases} \tag{16}$$

For $k = 0, \ldots, \lfloor \frac{m}{2} \rfloor$ define the linear space L_k^V by

$$L_k^V := \{x \in \mathbf{R}^{2^V} \mid C_{k-1,k}^V x = 0,\ x_I = 0 \text{ if } |I| \neq k\}, \tag{17}$$

and let B_k^V be an orthonormal base of L_k^V.

Proposition 4. *Let i, j, k, t, m be nonnegative integers satisfying $k, t \leq i, j$, $i + j \leq m + 2t$ and $k \leq \lfloor \frac{m}{2} \rfloor$. Let V be a set of cardinality m and let $b \in L_k^V$.*

i. We have

$$\dim L_k^V = \binom{m}{k} - \binom{m}{k-1}. \tag{18}$$

ii. For any nonnegative integer $k' \leq \lfloor \frac{m}{2} \rfloor$ and $b' \in L_{k'}^V$

$$(C_{i,k}^V b)^{\mathsf{T}} C_{i,k'}^V b' = \begin{cases} \binom{m-2k}{i-k} b^{\mathsf{T}} b' & \text{if } k = k', \\ 0 & \text{otherwise.} \end{cases} \tag{19}$$

iii. For any set $Y \subseteq V$ of cardinality j

$$\sum_{\substack{U \subseteq V \\ |U| = i \\ |U \cap Y| = t}} (C_{i,k}^V b)_U = \beta_{i,j,k}^{m,t} \binom{m-2k}{j-k}^{-1} (C_{j,k}^V b)_Y, \tag{20}$$

where $\beta_{i,j,k}^{m,t} := \sum_{u=0}^{m} (-1)^{t-u} \binom{u}{t} \binom{m-2k}{m-k-u} \binom{m-k-u}{i-u} \binom{m-k-u}{j-u}$.

Proof. See [6] for a proof. Although part *iii* is not explicitly stated there, it can be derived from equations (36) and (39) in [6]. □

We will now describe the block-diagonalisation of $\mathcal{A}_{q,n}$. Let $\phi := e^{\frac{2\pi i}{q-1}}$ be a primitive $(q-1)$-th root of unity. Let

$$\begin{aligned}\mathcal{V} \ := \ \{(a,k,i,\mathbf{a},b) \mid \\ & a,k,i \text{ are integers satisfying } 0 \le a \le k \le i \le n+a-k, \\ & \mathbf{a} \in \mathbf{q}^n \text{ satisfies } |S(\mathbf{a})| = a, \mathbf{a}_v \neq q-1 \text{ for } v = 1,\ldots,n, \\ & b \in B_{k-a}^{\overline{S(\mathbf{a})}}\},\end{aligned} \tag{21}$$

where $\overline{U} := \{1,2,\ldots,n\} \setminus U$ for any set $U \subseteq \{1,2,\ldots,n\}$. For each tuple $(a,k,i,\mathbf{a},b)$ in $\mathcal{V}$, define the vector $\Psi_{\mathbf{a},b}^{a,k,i} \in \mathbb{C}^{\mathbf{q}^n}$ by

$$\Psi_{\mathbf{a},b}^{a,k,i}(\mathbf{x}) := \begin{cases} (q-1)^{-\frac{1}{2}i}\binom{n+a-2k}{i-k}^{-\frac{1}{2}}\phi^{\langle \mathbf{a},\mathbf{x}\rangle}(C_{i-a,k-a}^{\overline{S(\mathbf{a})}}b)(S(\mathbf{x})\setminus S(\mathbf{a})) & \text{if } S(\mathbf{a}) \subseteq S(\mathbf{x}), \\ 0 & \text{otherwise,} \end{cases} \tag{22}$$

for any $\mathbf{x} \in \mathbf{q}^n$. Here $\langle \mathbf{x},\mathbf{y}\rangle := \sum_{v=0}^{n} \mathbf{x}_v\mathbf{y}_v \in \mathbf{Z}_{\ge 0}$ for any $\mathbf{x},\mathbf{y} \in \mathbf{q}^n$. Observe that $\Psi_{\mathbf{a},b}^{a,k,i}(\mathbf{x}) = 0$ if $|S(\mathbf{x})| \neq i$. We have:

Proposition 5. *The vectors* $\Psi_{\mathbf{a},b}^{a,k,i}$, $(a,k,i,\mathbf{a},b) \in \mathcal{V}$ *form an orthonormal base of* $\mathbf{q}^n$.

Proof. The number $|\mathcal{V}|$ of vectors $\Psi_{\mathbf{a},b}^{a,k,i}$ equals q^n since:

$$\begin{aligned}\sum_{\substack{a,k,i \\ 0\le a\le k\le i\le n+a-k}} & \binom{n}{a}(q-2)^a\left[\binom{n-a}{k-a} - \binom{n-a}{k-a-1}\right] \\ &= \sum_{i=0}^{n}\sum_{a=0}^{i}\sum_{k=a}^{\min(i,n+a-i)}\binom{n}{a}(q-2)^a\left[\binom{n-a}{k-a} - \binom{n-a}{k-a-1}\right] \\ &= \sum_{i=0}^{n}\sum_{a=0}^{i}\binom{n}{a}(q-2)^a\binom{n-a}{i-a} \\ &= \sum_{i=0}^{n}\binom{n}{i}\sum_{a=0}^{i}(q-2)^a\binom{i}{a} \\ &= \sum_{i=0}^{n}\binom{n}{i}(q-1)^i = q^n.\end{aligned} \tag{23}$$

We calculate the inner product of $\Psi_{\mathbf{a},b}^{a,k,i}$ and $\Psi_{\mathbf{a}',b'}^{a',k',i'}$. If $i \neq i'$ then the inner product is zero since the two vectors have disjoint support. So we may assume that $i' = i$. We obtain:

$$\begin{aligned}\left\langle \Psi_{\mathbf{a},b}^{a,k,i}, \Psi_{\mathbf{a}',b'}^{a',k',i}\right\rangle = (q-1)^{-i}\binom{n+a-2k}{i-k}^{-\frac{1}{2}}\binom{n+a'-2k'}{i-k'}^{-\frac{1}{2}}\cdot \\ \sum_{\mathbf{x}}\phi^{\langle \mathbf{a},\mathbf{x}\rangle - \langle \mathbf{a}',\mathbf{x}\rangle}(C_{i-a,k-a}^{\overline{S(\mathbf{a})}}b)(S(\mathbf{x})\setminus S(\mathbf{a}))\cdot(C_{i-a',k'-a'}^{\overline{S(\mathbf{a}')}}b')(S(\mathbf{x})\setminus S(\mathbf{a}')),\end{aligned} \tag{24}$$

where the sum ranges over all $\mathbf{x} \in \mathbf{q}^n$ with $|S(\mathbf{x})| = i$ and $S(\mathbf{x}) \supseteq S(\mathbf{a}) \cup S(\mathbf{a}')$. If $\mathbf{a}_j \neq \mathbf{a}'_j$ for some j, then the inner product equals zero, since we can factor out $\sum_{x_j=1}^{q-1} \phi^{x_j(\mathbf{a}_j - \mathbf{a}'_j)} = 0$. So we may assume that $\mathbf{a} = \mathbf{a}'$ (and hence $a = a'$), which simplifies the righthand side of (24) to

$$\binom{n+a-2k}{i-k}^{-\frac{1}{2}} \binom{n+a-2k'}{i-k'}^{-\frac{1}{2}} (C^{\overline{S(\mathbf{a})}}_{i-a,k-a} b)^{\mathsf{T}} C^{\overline{S(\mathbf{a})}}_{i-a,k'-a} b'. \tag{25}$$

Now by Proposition 4 we conclude that $\left\langle \Psi^{a,k,i}_{\mathbf{a},b}, \Psi^{a,k',i}_{\mathbf{a},b'} \right\rangle$ is nonzero only if $b = b'$ and $k = k'$, in which case the inner product equals 1. □

Proposition 6. *For $(i,j,t,p) \in \mathcal{I}(q,n)$ and $(a,k,i',A,b) \in \mathcal{V}$ we have:*

$$M^{t,p}_{j,i} \Psi^{a,k,i'}_{\mathbf{a},b} = \delta_{i,i'} \binom{n+a-2k}{i-k}^{-\frac{1}{2}} \binom{n+a-2k}{j-k}^{-\frac{1}{2}} \alpha(i,j,t,p,a,k) \Psi^{a,k,j}_{\mathbf{a},b}, \tag{26}$$

where

$$\alpha(i,j,t,p,a,k) := \beta^{n-a,t-a}_{i-a,j-a,k-a} (q-1)^{\frac{1}{2}(i+j)-t} \sum_{g=0}^{p} (-1)^{a-g} \binom{a}{g} \binom{t-a}{p-g} (q-2)^{t-a-p+g}. \tag{27}$$

Proof. Clearly, both sides of (26) are zero if $i \neq i'$, hence we may assume that $i = i'$. We calculate $(M^{t,p}_{j,i} \Psi^{a,k,i}_{\mathbf{a},b})(\mathbf{y})$. We may assume that $|S(\mathbf{y})| = j$, since otherwise both sides of (26) have a zero in position $\mathbf{y}$. We have:

$$\begin{aligned} (M^{t,p}_{j,i} \Psi^{a,k,i}_{\mathbf{a},b})(\mathbf{y}) &= \sum_{\mathbf{x} \in \mathbf{q}^n} (M^{t,p}_{j,i})_{\mathbf{y},\mathbf{x}} \Psi^{a,k,i}_{\mathbf{a},b}(\mathbf{x}) \qquad (28) \\ &= (q-1)^{-\frac{1}{2}i} \binom{n+a-2k}{i-k}^{-\frac{1}{2}} \sum_{\mathbf{x}} \phi^{\langle \mathbf{x},\mathbf{a} \rangle} (C^{\overline{S(\mathbf{a})}}_{i-a,k-a} b)(S(\mathbf{x}) \setminus S(\mathbf{a})), \end{aligned}$$

where the last sum is over all $\mathbf{x} \in \mathbf{q}^n$ with $|S(\mathbf{x})| = i$, $S(\mathbf{x}) \supseteq S(\mathbf{a})$, $|S(\mathbf{x}) \cap S(\mathbf{y})| = t$ and $|\{v \mid \mathbf{x}_v = \mathbf{y}_v \neq 0\}| = p$. If $v \in S(\mathbf{a}) \setminus S(\mathbf{y})$ we can factor out $\sum_{l=1}^{q-1} \phi^{l\mathbf{a}_v} = 0$, implying that both sides of (26) have a zero at position $\mathbf{y}$. Hence we may assume that $S(\mathbf{y}) \supseteq S(\mathbf{a})$. Now the support of each word $\mathbf{x}$ in this sum can be split into five parts U, U', V, V', W, where

$$\begin{aligned} U &= \{v \in S(\mathbf{a}) \mid \mathbf{x}_v = \mathbf{y}_v\} \qquad (29) \\ U' &= S(\mathbf{a}) \setminus U, \\ V &= \{v \in S(\mathbf{y}) \setminus S(\mathbf{a}) \mid \mathbf{x}_v = \mathbf{y}_v\}, \\ V' &= ((S(\mathbf{y}) \setminus S(\mathbf{a})) \cap S(\mathbf{x})) \setminus V \text{ and} \\ W &= S(\mathbf{x}) \setminus S(\mathbf{y}). \end{aligned}$$

If we set $g = |U|$, then $|U'| = a - g$, $|V| = p - g$, $|V'| = t - a - p + g$ and $|W| = i - t$. Hence splitting the sum over g, we obtain:

$$(q-1)^{-\frac{1}{2}i}\binom{n+a-2k}{i-k}^{-\frac{1}{2}}\sum_{g=0}^{p}\sum_{U,U',V,V',W}(C_{i-a,k-a}^{\overline{S(\mathbf{a})}}b)(V\cup V'\cup W)$$
$$\prod_{v\in U}\phi^{\mathbf{a}_v\mathbf{y}_v}\prod_{v\in U'}-\phi^{\mathbf{a}_v\mathbf{y}_v}\prod_{v\in V}1\prod_{v\in V'}(q-2)\prod_{v\in W}(q-1), \quad (30)$$

where U, U', V, V', W are as indicated. Substituting $T = V \cup V' \cup W$, we can rewrite this as

$$(q-1)^{-\frac{1}{2}i}\binom{n+a-2k}{i-k}^{-\frac{1}{2}}\sum_{g=0}^{p}\binom{a}{g}\binom{t-a}{p-g}(-1)^{a-g}(q-2)^{t-a-p+g}\cdot$$
$$(q-1)^{i-t}\phi^{\langle\mathbf{a},\mathbf{y}\rangle}\sum_{T}(C_{i-a,k-a}^{\overline{S(\mathbf{a})}}b)(T), \quad (31)$$

where the sum ranges over all $T \subseteq \overline{S(\mathbf{a})}$ with $|T| = i - a$ and $|T \cap S(\mathbf{y})| = t - a$. Now by Proposition 4 this is equal to

$$(q-1)^{-\frac{1}{2}i}\binom{n+a-2k}{i-k}^{-\frac{1}{2}}(q-1)^{i-t}\sum_{g=0}^{p}\binom{a}{g}\binom{t-a}{p-g}(-1)^{a-g}(q-2)^{t-a-p+g}\cdot$$
$$\phi^{\langle\mathbf{a},\mathbf{y}\rangle}\binom{n+a-2k}{j-k}^{-1}\beta_{i-a,j-a,k-a}^{n-a,t-a}(C_{j-a,k-a}^{\overline{S(\mathbf{a})}}b)(S(\mathbf{y})\setminus S(\mathbf{a})), \quad (32)$$

which equals

$$\Psi_{\mathbf{a},b}^{a,k,j}(\mathbf{y})\cdot\beta_{i-a,j-a,k-a}^{n-a,t-a}\binom{n+a-2k}{i-k}^{-\frac{1}{2}}\binom{n+a-2k}{j-k}^{-\frac{1}{2}}(q-1)^{\frac{1}{2}(i+j)-t}\cdot$$
$$\sum_{g=0}^{p}(-1)^{a-g}\binom{a}{g}\binom{t-a}{p-g}(q-2)^{t-a-p+g}. \quad (33)$$

□

If we define U to be the $\mathbf{q}^n \times \mathcal{V}$ matrix with $\Psi_{\mathbf{a},b}^{a,k,i}$ as the $(a, k, i, \mathbf{a}, b)$-th column, then Proposition 6 shows that for each $(i, j, t, p) \in \mathcal{I}(q, n)$ the matrix $\tilde{M}_{i,j}^{t,p} := U^* M_{i,j}^{t,p} U$ has entries

$$(\tilde{M}_{i,j}^{t,p})_{(a,k,l,\mathbf{a},b),(a',k',l',\mathbf{a}',b')} = \begin{cases}\binom{n+a-2k}{i-k}^{-\frac{1}{2}}\binom{n+a-2k}{j-k}^{-\frac{1}{2}}\alpha(i,j,t,p,a,k) & \text{if } a=a',\ k=k',\ \mathbf{a}=\mathbf{a}',\ b=b' \text{ and } \\ & l=i,\ l'=j, \\ 0 & \text{otherwise.}\end{cases} \quad (34)$$

This implies

Proposition 7. *The matrix U gives a block-diagonalisation of $\mathcal{A}_{q,n}$.*

Proof. Equation (34) implies that each matrix $\tilde{M}_{i,j}^{t,p}$ has a block-diagonal form, where for each pair (a,k) there are $\binom{n}{a}(q-2)^a\left[\binom{n-a}{k-a}-\binom{n-a}{n-a-1}\right]$ copies of an $(n+a+1-2k)\times(n+a+1-2k)$ block on the diagonal. For fixed a,k the copies are indexed by the pairs $(\mathbf{a},b)$ such that $\mathbf{a}\in\mathbf{q}^n$ satisfies $|S(\mathbf{a})|=a$, $\mathbf{a}_v\neq q-1$ for $v=1,\ldots,n$, and $b\in B_{k-a}^{\overline{S(a)}}$, and in each copy the rows and columns in the block are indexed by the integers i with $k\leq i\leq n+a-k$. Hence we need to show that all matrices of this block-diagonal form are in $U^*\mathcal{A}_{q,n}U$. It suffices to show that the dimension $\sum_{0\leq a\leq k\leq n+a-k}(n+a+1-2k)^2$ of the algebra consisting of the matrices in the given block-diagonal form equals the dimension of $\mathcal{A}_{q,n}$, which is $\binom{n+4}{4}$. This follows from

$$
\begin{aligned}
&\sum_{0\leq a\leq k\leq n+a-k}(n+a+1-2k)^2\\
&\quad=\sum_{a=0}^{n}\sum_{k=a}^{\lfloor\frac{n+a}{2}\rfloor}(n+a+1-2k)^2\\
&\quad=\sum_{a\equiv n(2)}(1^2+3^2+\cdots+(n+1-a)^2)+\sum_{a\not\equiv n(2)}(2^2+4^2+\cdots+(n+1-a)^2)\\
&\quad=\sum_{a\equiv n(2)}\binom{n+1-a+2}{3}+\sum_{a\not\equiv n(2)}\binom{n+1-a+2}{3}\\
&\quad=\sum_{a=0}^{n}\binom{n-a+3}{3}=\binom{n+4}{4}.
\end{aligned}
\tag{35}
$$

□

3 Application to coding

Let $C\subseteq\mathbf{q}^n$ be any code. For any automorphism π, denote the characteristic vector of $\pi(C)$ by $\chi^{\pi(C)}$ (taken as a columnvector). For any word $\mathbf{x}\in\mathbf{q}^n$, let $\sigma_{\mathbf{x}}\in\mathrm{Aut}(q,n)$ be any automorphism with $\sigma_{\mathbf{x}}(\mathbf{x})=\mathbf{0}$, and define

$$
R_{\mathbf{x}}:=|\mathrm{Aut}_{\mathbf{0}}(q,n)|^{-1}\sum_{\pi\in\mathrm{Aut}_{\mathbf{0}}(q,n)}\chi^{\pi(\sigma_{\mathbf{x}}(C))}(\chi^{\pi(\sigma_{\mathbf{x}}(C))})^{\mathsf{T}}. \tag{36}
$$

Next define the matrices R and R' by:

$$
\begin{aligned}
R &:= |C|^{-1}\sum_{\mathbf{x}\in C}R_{\mathbf{x}}, && (37)\\
R' &:= (q^n-|C|)^{-1}\sum_{\mathbf{x}\in\mathbf{q}^n\setminus C}R_{\mathbf{x}}.
\end{aligned}
$$

As the $R_{\mathbf{x}}$, and hence also R and R', are convex combinations of positive semidefinite matrices, they are positive semidefinite. By construction, the matrices $R_{\mathbf{x}}$, and hence the matrices R and R' are invariant under permutations $\pi \in \mathrm{Aut}_{\mathbf{0}}(q,n)$ of the rows and columns and hence they are elements of the algebra $\mathcal{A}_{q,n}$. Write

$$R = \sum_{(i,j,t,p)} x_{i,j}^{t,p} M_{i,j}^{t,p}. \tag{38}$$

We can express the matrix R' in terms of the coefficients $x_{i,j}^{t,p}$ as follows.

Proposition 8. *The matrix R' is given by*

$$R' = \frac{|C|}{q^n - |C|} \sum_{(i,j,t,p)} (x_{i+j-t-p,0}^{0,0} - x_{i,j}^{t,p}) M_{i,j}^{t,p}. \tag{39}$$

Proof. The matrix

$$S := |C|R + (q^n - |C|)R' = |\mathrm{Aut}_{\mathbf{0}}(q,n)|^{-1} \sum_{\sigma \in \mathrm{Aut}(q,n)} \chi^{\sigma(C)} (\chi^{\sigma(C)})^{\mathsf{T}} \tag{40}$$

is invariant under permutation of the rows and columns by permutations $\sigma \in \mathrm{Aut}(q,n)$ and hence is an element of the Bose–Mesner algebra, say

$$S = \sum_k y_k A_k. \tag{41}$$

Note that for any $\mathbf{y} \in \mathbf{q}^n$ with $|S(\mathbf{y})| = k$, we have

$$y_k = (S)_{\mathbf{y},\mathbf{0}} = |C|(R)_{\mathbf{y},\mathbf{0}} = |C| x_{k,0}^{0,0},$$

since $(R')_{\mathbf{y},\mathbf{0}} = 0$. Hence we have

$$\begin{aligned} (q^n - |C|)R' &= S - |C|R \\ &= \sum_k |C| x_{k,0}^{0,0} A_k - |C| \sum_{(i,j,t,p)} x_{i,j}^{t,p} M_{i,j}^{t,p} \\ &= |C| \sum_k \sum_{i+j-t-p=k} (x_{k,0}^{0,0} - x_{i,j}^{t,p}) M_{i,j}^{t,p} \\ &= |C| \sum_{(i,j,t,p)} (x_{i+j-t-p,0}^{0,0} - x_{i,j}^{t,p}) M_{i,j}^{t,p}, \end{aligned} \tag{42}$$

which proves the proposition. ☐

Using the block-diagonalisation of $\mathcal{A}(n,d)$, the positive semidefiniteness of R and R' is equivalent to:

$$\text{for all } a,k \text{ with } 0 \le a \le k \le n+a-k, \text{ the matrices} \tag{43}$$
$$\left(\sum_{t,p} \alpha(i,j,t,p,a,k) x_{i,j}^{t,p}\right)_{i,j=k}^{n+a-k}$$
$$\text{and}$$
$$\left(\sum_{t,p} \alpha(i,j,t,p,a,k)(x_{i+j-t-p,0}^{0,0} - x_{i,j}^{t,p})\right)_{i,j=k}^{n+a-k}$$
$$\text{are positive semidefinite.}$$

Define the numbers
$$\lambda_{i,j}^{t,p} := |(C \times C \times C) \cap X_{i,j,t,p}|, \tag{44}$$
for $(i,j,t,p) \in \mathcal{I}(q,n)$, and let
$$\gamma_{i,j}^{t,p} := |(\{\mathbf{0}\} \times \mathbf{q}^n \times \mathbf{q}^n) \cap X_{i,j,t,p}| \tag{45}$$
be the number of nonzero entries of $M_{i,j}^{t,p}$. A simple calculation yields:
$$\gamma_{i,j}^{t,p} = (q-1)^{i+j-t}(q-2)^{t-p}\binom{n}{p,t-p,i-t,j-t}. \tag{46}$$

The numbers $x_{i,j}^{t,p}$ can be expressed in terms of the the numbers $\lambda_{i,j}^{t,p}$ as follows.

Proposition 9. $x_{i,j}^{t,p} = (|C|\gamma_{i,j}^{t,p})^{-1}\lambda_{i,j}^{t,p}$.

Proof. Denote by $\langle M,N\rangle := \mathrm{tr}(M^*N)$ the standard innerproduct on the space of complex $\mathbf{q}^n \times \mathbf{q}^n$ matrices. Observe that the matrices $M_{i,j}^{t,p}$ are pairwise orthogonal and that $\left\langle M_{i,j}^{t,p}, M_{i,j}^{t,p}\right\rangle = \gamma_{i,j}^{t,p}$ for $(i,j,t,p) \in \mathcal{I}(q,n)$. Hence

$$\left\langle R, M_{i,j}^{t,p}\right\rangle = \frac{1}{|C|}\sum_{\mathbf{x}\in C}\left\langle R_{\mathbf{x}}, M_{i,j}^{t,p}\right\rangle \tag{47}$$
$$= \frac{1}{|C|}\sum_{\mathbf{x}\in C} |(\{\mathbf{x}\} \times C \times C) \cap X_{i,j,t,p}| \tag{48}$$
$$= \frac{1}{|C|}\lambda_{i,j}^{t,p}$$

implies that
$$R = \frac{1}{|C|}\sum_{(i,j,t,p)\in\mathcal{I}(q,n)} \lambda_{i,j}^{t,p}(\gamma_{i,j}^{t,p})^{-1}M_{i,j}^{t,p}. \tag{49}$$

Comparing the coefficients of the $M_{i,j}^{t,p}$ with those in (38) proves the proposition. □

The $x_{i,j}^{t,p}$ satisfy the following linear constraints, where (iv) holds if C has minimum distance at least d:

$$\begin{array}{ll} \text{(i)} & x_{0,0}^{0,0} = 1 \\ \text{(ii)} & 0 \leq x_{i,j}^{t,p} \leq x_{i,0}^{0,0} \\ \text{(iii)} & x_{i,j}^{t,p} = x_{i',j'}^{t',p'} \text{ if } t-p = t'-p' \text{ and} \\ & (i,j,i+j-t-p) \text{ is a permutation of } (i',j',i'+j'-t'-p') \\ \text{(iv)} & x_{i,j}^{t,p} = 0 \text{ if } \{i,j,i+j-t-p\} \cap \{1,2,\ldots,d-1\} \neq \emptyset. \end{array} \tag{50}$$

Here conditions (iii) and (iv) follow from Proposition 9. Condition (ii) follows from $x_{i,0}^{0,0} = x_{i,i}^{i,i}$ and the fact that if $M = \chi^{\sigma(C)}(\chi^{\sigma(C)})^{\mathsf{T}}$ then $0 \leq M_{\mathbf{x},\mathbf{y}} \leq M_{\mathbf{x},\mathbf{x}}$ for any $\mathbf{x},\mathbf{y} \in \mathbf{q}^n$ and $\sigma \in \mathrm{Aut}(q,n)$.

Since $|C|^2 = \sum_i \lambda_{i,0}^{0,0}$, we have $|C| = \sum_i \gamma_{i,0}^{0,0} x_{i,0}^{0,0}$. Hence if we view the $x_{i,j}^{t,p}$ as variables, then maximizing $\sum_i \gamma_{i,0}^{0,0} x_{i,0}^{0,0}$ subject to conditions (50) and (43) yields an upper bound on $A_q(n,d)$. This is a semidefinite programming problem with $O(n^4)$ variables, and can be solved in time polynomial in n.

In the range $n \leq 16$, $n \leq 12$ and $n \leq 11$, the method gives a number of new upper bounds on $A_3(n,d)$, $A_4(n,d)$ and $A_5(n,d)$ respectively, summarized in Table 1, 2 and 3 below (cf. the tables given by Brouwer, Hämäläinen, Östergård and Sloane [4], by Bogdanova, Brouwer, Kapralov and Östergård [2] and by Bogdanova and Östergård [3]).

References

[1] E. Bannai,T. Ito, *Algebraic Combinatorics I: Association Schemes*, The Benjamin/Cumings Publishing Co., Inc., Menlo Park, CA, 1984.

[2] G.T. Bogdanova, A.E. Brouwer, S.N. Kapralov, P.R.J. Östergård, Error-Correcting Codes over an Alphabet of Four Elements, *Designs, Codes and Cryptography* 23 (2001) 333–342.

[3] G.T. Bogdanova, P.R.J. Östergård, Bounds on codes over an alphabet of five elements, *Discrete Mathematics* 240 (2001) 13–19.

[4] A.E. Brouwer, H.O. Hämäläinen, P.R.J. Östergård, N.J.A. Sloane, Bounds on Mixed Binary/Ternary Codes, *IEEE Trans. Inf. Th.* 44 (1998) 140–161.

[5] P. Delsarte, *An Algebraic Approach to the Association Schemes of Coding Theory* [Philips Research Reports Supplements 1973 No. 10], Philips Research Laboratories, Eindhoven, 1973.

[6] A. Schrijver, New code upper bounds from the Terwilliger algebra, *preprint 2004*.

[7] P. Terwilliger, The subconstituent algebra of an association scheme (Part I), *Journal of Algebraic Combinatorics* 1 (1992) 363–388.

Table 1: New upper bounds on $A_3(n,d)$

n	d	best lower bound known	new upper bound	best upper bound previously known	Delsarte bound
12	4	4374	6839	7029	7029
13	4	8019	19270	19682	19683
14	4	24057	54774	59046	59049
15	4	72171	149585	153527	153527
16	4	216513	424001	434815	434815
12	5	729	1557	1562	1562
13	5	2187	4078	4163	4163
14	5	6561	10624	10736	10736
15	5	6561	29213	29524	29524
13	6	729	1449	1562	1562
14	6	2187	3660	3885	4163
15	6	2187	9904	10736	10736
16	6	6561	27356	29524	29524
14	7	243	805	836	836
15	7	729	2204	2268	2268
16	7	729	6235	6643	6643
13	8	42	95	103	103
15	8	243	685	711	712
16	8	297	1923	2079	2079
14	9	31	62	66	81
15	9	81	165	166	166
16	10	54	114	117	127

Table 2: New upper bounds on $A_4(n, d)$

n	d	best lower bound known	new upper bound	best upper bound previously known	Delsarte bound
7	4	128	169	179	179
8	4	320	611	614	614
9	4	1024	2314	2340	2340
10	4	4096	8951	9360	9362
10	5	1024	2045	2048	2145
10	6	256	496	512	512
11	6	1024	1780	2048	2048
12	6	4096	5864	6241	6241
12	7	256	1167	1280	1280

Table 3: New upper bounds on $A_5(n, d)$

n	d	best lower bound known	new upper bound	best upper bound previously known	Delsarte bound
7	4	250	545	554	625
7	5	53	108	125	125
8	5	160	485	554	625
9	5	625	2152	2291	2291
10	5	3125	9559	9672	9672
11	5	15625	44379	44642	44642
10	6	625	1855	1875	1875
11	6	3125	8840	9375	9375