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

Denote by $\text{Aut}(q, n)$ the set of permutations of $q^n$ that preserve the Hamming distance. It is not hard to see that $\text{Aut}(q, n)$ consists of the permutations of $q^n$ obtained by permuting the $n$ coordinates followed by independently permuting the alphabet $q$ at each of the $n$ coordinates. If we consider the action of $\text{Aut}(q, n)$ on the set $q^n \times q^n$, 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

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

∗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 $\text{Aut}(q, n)$ on ordered triples of words, which will lead to a noncommutative algebra $A_{q,n}$ 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 $A_{q,n}$ 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 $(x, y, z) \in q^n \times q^n \times q^n$ we associate the four-tuple

$$d(x, y, z) := (i, j, t, p),$$

where

$$i := d(x, y),$$

$$j := d(x, z),$$

$$t := |\{v \mid x_v \neq y_v \text{ and } x_v \neq z_v\}|,$$

$$p := |\{v \mid x_v \neq y_v = z_v\}|.$$

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

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

and will index various objects defined below.

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

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

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

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

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

**Proposition 2.** The sets $X_{i, j, t, p}, (i, j, t, p) \in I(q, n)$ are the orbits of $q^n \times q^n \times q^n$ under the action of $\text{Aut}(q, n)$.
Proof. Let $x, y, z \in \mathbb{Q}^n$ and let $(i, j, t, p) = d(x, y, z)$. Since the Hamming distances $i, j, i + j - t - p$ and the number $t - p = |\{v \mid x_v \neq y_v \neq z_v \neq x_v\}|$ are unchanged when permuting the coordinates or permuting the elements of $q$ at any coordinate, we have $d(x, y, z) = d(\pi(x), \pi(y), \pi(z))$ for any $\pi \in \text{Aut}(q, n)$.

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

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

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

(5)

Let $A_{q,n}$ be the set of matrices

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

(6)

where $x_{i,j}^{t,p} \in \mathbb{C}$. From Proposition 2 it follows that $A_{q,n}$ is the set of matrices that are stable under permutations $\pi \in \text{Aut}_0(q, n)$ of the rows and columns. Hence $A_{q,n}$ 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 $A_{q,n}$ and hence

$$\dim A_{q,n} = \binom{n + 4}{4}.$$

(7)

by Proposition 1. Note that the algebra $A_{q,n}$ contains the Bose–Mesner algebra since

$$A_k = \sum_{(i,j,t,p) \in I(q,n)} M_{i,j}^{t,p}.$$

(8)

Although it is not needed for the remainder of this paper, we would like to point out here, that $A_{q,n}$ coincides with the Terwilliger algebra (see [7]) of the nonbinary Hamming scheme $H(n, q)$ (with respect to 0). The Terwilliger algebra $T(q, n)$ 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

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

(9)

for $i = 0, 1, \ldots, n$. 3
Proposition 3. The algebras \( A_{q,n} \) and \( T_{q,n} \) coincide.

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

\[
B_i := E_i^* A_1 E_i^*, \\
C_i := E_i^* A_1 E_{i+1}^*, \\
D_i := E_i^* A_1 E_{i-1}^*.
\]

Observe that:

\[
(B_i)_{x,y} = 1 \quad \text{if and only if} \quad |S(x)| = i, d(x,y) = 1, |S(y)| = i, S(x) = S(y),
\]

\[
(C_i)_{x,y} = 1 \quad \text{if and only if} \quad |S(x)| = i, d(x,y) = 1, |S(y)| = i + 1, |S(x)\Delta S(y)| = 1,
\]

\[
(D_i)_{x,y} = 1 \quad \text{if and only if} \quad |S(x)| = i, d(x,y) = 1, |S(y)| = i - 1, |S(x)\Delta S(y)| = 1.
\]

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

\[
A_{i,j}^{t,p} := (D_i D_{i-1} \cdots D_{t+1})(C_i C_{t+1} \cdots C_{j-1})(B_j)^{t-p}.
\]

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

\[
x = d_i, d_{i-1}, \ldots, d_t = c_t, c_{t+1}, \ldots, c_j = b_0, \ldots, b_{t-p} = y \in q^n
\]

where any two consecutive words have Hamming distance 1, the \( b_k \) have equal support of cardinality \( j \), and \( |S(d_k)| = k, |S(c_k)| = k \) for all \( k \). Hence for \( x, y \in q^n \) the following holds.

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

and

\[
(A_{i,j}^{t,p})_{x,y} > 0 \quad \text{if} \quad |S(x)| = i, |S(y)| = j,
\]

\[
d(x,y) = i + j - t - p \quad \text{and} \quad |S(x)\Delta S(y)| = i + j - 2t.
\]

To see (14) one may take for \( d_k \) the zero-one word with support \( \{i + 1 - k, \ldots, i\} \), for \( c_k \) the zero-one word with support \( \{i + 1 - k, \ldots, i + k - t\} \) and for \( b_k \) 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 \( A_{q,n} \) is not contained in \( T_{q,n} \), and let \( M_{i,j}^{t,p} \) be a matrix not in \( T_{q,n} \) with \( t \) maximal and (secondly) \( p \) maximal. If we write

\[
A_{i,j}^{t,p} = \sum_{t',p'} x_{i,j}^{t',p'} M_{i,j}^{t',p'},
\]

then...
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. \( \square \)

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

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

(16)

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

\[
L_k^V := \{ x \in \mathbb{R}^{2^V} | C_{i,k}^V x = 0, x_I = 0 \text{ if } |I| \neq k \},
\]

(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

\[
\dim L_k^V = \binom{m}{k} - \binom{m}{k-1}.
\]

(18)

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

\[
(C_{i,k}^V b) \ast C_{i,k}^V b' = \begin{cases} \binom{m-2k}{i-k} b' & \text{if } k = k', \\ 0 & \text{otherwise.} \end{cases}
\]

(19)

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

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

(20)

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

**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]. \( \square \)
We will now describe the block-diagonalisation of \( A_{q,n} \). Let \( \phi := e^{2\pi i/q} \) be a primitive \((q - 1)\)-th root of unity. Let

\[
\mathcal{U} := \{(a, k, i, a, b) \mid a, k, i \text{ are integers satisfying } 0 \leq a \leq k \leq i \leq n + a - k, \quad a \in \mathbb{Q}^n \text{ satisfies } |S(a)| = a, a_v \neq q - 1 \text{ for } v = 1, \ldots, n, \\
b \in B_{n-a}^k \}
\]

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

\[
\Psi_{a,b}^{a,k,i}(x) := \begin{cases} (q - 1)^{-\frac{1}{2}i} (n + a - 2k)^{-\frac{1}{2}} \phi(a,x) (C_{i-a, k-a}^{S(a)}) (S(x) \setminus S(a)) & \text{if } S(a) \subseteq S(x), \\
0 & \text{otherwise}, 
\end{cases}
\]

for any \( x \in \mathbb{Q}^n \). Here \( \langle x, y \rangle := \sum_{v=0}^{n} x_v y_v \in \mathbb{Z}_{\geq 0} \) for any \( x, y \in \mathbb{Q}^n \). Observe that \( \Psi_{a,b}^{a,k,i}(x) = 0 \) if \( |S(x)| \neq i \). We have:

**Proposition 5.** The vectors \( \Psi_{a,b}^{a,k,i} \), \((a, k, i, a, b) \in \mathcal{U} \) form an orthonormal base of \( \mathbb{Q}^n \).

**Proof.** The number \( |\mathcal{U}| \) of vectors \( \Psi_{a,b}^{a,k,i} \) equals \( q^n \) since:

\[
\sum_{0 \leq a \leq k \leq i \leq n + a - k} \binom{n}{a} (q - 2)^a \left[ \binom{n - a}{k - a} - \binom{n - a}{k - a - 1} \right] 
\]

\[
= \sum_{i=0}^{n} \sum_{a=0}^{\min(i, n + a - i)} \binom{n}{a} (q - 2)^a \left[ \binom{n - a}{k - a} - \binom{n - a}{k - a - 1} \right] 
\]

\[
= \sum_{i=0}^{n} \sum_{a=0}^{i} \binom{n}{a} (q - 2)^a \binom{n - a}{i - a} 
\]

\[
= \sum_{i=0}^{n} \binom{n}{i} \sum_{a=0}^{i} (q - 2)^a \binom{i}{a} 
\]

\[
= \sum_{i=0}^{n} \binom{n}{i} (q - 1)^i = q^n.
\]

We calculate the inner product of \( \Psi_{a,b}^{a,k,i} \) and \( \Psi_{a',b'}^{a',k',i'} \). 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:

\[
\langle \Psi_{a,b}^{a,k,i}, \Psi_{a',b'}^{a',k',i} \rangle = (q - 1)^{-i} \binom{n + a - 2k}{i - k}^{-\frac{1}{2}} \binom{n + a' - 2k'}{i - k'}^{-\frac{1}{2}} 
\]

\[
\sum_{x} \phi(a,x) - (a', x) (C_{i-a, k-a}^{S(a)}) (S(x) \setminus S(a)) \cdot (C_{i-a', k'-a}^{S(a')})(S(x) \setminus S(a')), 
\]

\[(24)\]
where the sum ranges over all $x \in q^i$ with $|S(x)| = i$ and $S(x) \supseteq S(a) \cup S(a')$. If $a_j \neq a'_j$ for some $j$, then the inner product equals zero, since we can factor out $\sum_{x_j=1}^{q-1} \phi_{x_j}(a_j-a'_j) = 0$. So we may assume that $a = a'$ (and hence $a = a'$), which simplifies the righthand side of (24) to
\[
\left(\frac{n + a - 2k}{i - k}\right)^{-\frac{1}{2}} \left(\frac{n + a - 2k}{j - k}\right)^{-\frac{1}{2}} (C_{i-a,k-a}^a)_{i-a,k-a} b_1. \tag{25}
\]

Now by Proposition 4 we conclude that $\langle \Psi_{a,b}^{a,k,i}, \Psi_{a,b'}^{a,k',i} \rangle$ is nonzero only if $b = b'$ and $k = k'$, in which case the inner product equals 1. \hfill \Box

**Proposition 6.** For $(i, j, t, p) \in I(q, n)$ and $(a, k, i', A, b) \in \mathcal{V}$ we have:
\[
M_{i,j}^{t,p} \Psi_{a,b}^{a,k,i} = \delta_{i,i'} \left(\frac{n + a - 2k}{i - k}\right)^{-\frac{1}{2}} \left(\frac{n + a - 2k}{j - k}\right)^{-\frac{1}{2}} \alpha(i, j, t, p, a, k) \Psi_{a,b}^{a,k,i}, \tag{26}
\]

where
\[
\alpha(i, j, t, p, a, k) := \beta_{i-a, j-a, k-a}^n \sum_{g=0}^{p} (-1)^{a-g} \binom{a}{g} (t-a) (q-2)^{t-a-p+g}. \tag{27}
\]

**Proof.** Clearly, both sides of (26) are zero if $i \neq i'$, hence we may assume that $i = i'$. We calculate $(M_{i,j}^{t,p} \Psi_{a,b}^{a,k,i})(y)$. We may assume that $|S(y)| = j$, since otherwise both sides of (26) have a zero in position $y$. We have:
\[
(M_{i,j}^{t,p} \Psi_{a,b}^{a,k,i})(y) = \sum_{x \in q^i} (M_{i,j}^{t,p})_{y,x} \Psi_{a,b}^{a,k,i}(x) \tag{28}
\]
\[
= (q-1)^{-\frac{1}{2}} \left(\frac{n + a - 2k}{i - k}\right)^{-\frac{1}{2}} \sum_{x} \phi(x,a) (C_{i-a,k-a}^a)(S(x) \setminus S(a)),
\]
where the last sum is over all $x \in q^i$ with $|S(x)| = i$, $S(x) \supseteq S(a)$, $|S(x) \cap S(y)| = t$ and $|\{v \mid x_v = y_v \neq 0\}| = p$. If $v \in S(a) \setminus S(y)$ we can factor out $\sum_{x=1}^{q-1} \phi_{x_v}(a_v-a_v) = 0$, implying that both sides of (26) have a zero at position $y$. Hence we may assume that $S(y) \supseteq S(a)$. Now the support of each word $x$ in this sum can be split into five parts $U, U', V, V', W$, where
\[
U = \{v \in S(a) \mid x_v = y_v\}, \tag{29}
\]
\[
U' = S(a) \setminus U,
\]
\[
V = \{v \in S(y) \setminus S(a) \mid x_v = y_v\},
\]
\[
V' = ((S(y) \setminus S(a)) \cap S(x)) \setminus V \text{ and}
\]
\[
W = S(x) \setminus S(y).
\]
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:

\[
(q - 1)^{-\frac{1}{2}} \left( \binom{n + a - 2k}{i - k} \right)^{-\frac{1}{2}} \sum_{g=0}^{p} \sum_{U,U',V,V',W} (C_{i-a,k-a}^S)(V \cup V' \cup W) \prod_{v \in U} \phi^{a,y} \prod_{v \in U'} -\phi^{a,y} \prod_{v \in V} 1 \prod_{v \in V'} (q - 2) \prod_{v \in W} (q - 1),
\]

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

\[
(q - 1)^{-\frac{1}{2}} \left( \binom{n + a - 2k}{i - k} \right)^{-\frac{1}{2}} (q - 1)^{i-t} \sum_{g=0}^{p} \binom{a}{g} \left( \frac{t - a}{p - g} \right) (-1)^{a-g} (q - 2)^{t-a-p+g}.
\]

\[
(q - 1)^{i-t} \phi^{(a,y)} \sum_{T} (C_{i-a,k-a}^S)(T),
\]

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

\[
(q - 1)^{-\frac{1}{2}} \left( \binom{n + a - 2k}{i - k} \right)^{-\frac{1}{2}} (q - 1)^{i-t} \sum_{g=0}^{p} \binom{a}{g} \left( \frac{t - a}{p - g} \right) (-1)^{a-g} (q - 2)^{t-a-p+g}.
\]

\[
\phi^{(a,y)} \left( \binom{n + a - 2k}{j - k} \right)^{-1} \beta_{i-a,j-a,k-a}^{a,t-a} (C_{j-a,k-a}^S)(y) \setminus S(a),
\]

which equals

\[
\Psi_{a,b}^{a,k,j}(y) \cdot \beta_{i-a,j-a,k-a}^{a,t-a} \left( \binom{n + a - 2k}{i - k} \right)^{-\frac{1}{2}} \left( \binom{n + a - 2k}{j - k} \right)^{-\frac{1}{2}} (q - 1)^{\frac{1}{2}(i+j)-t}. \]

\[
\sum_{g=0}^{p} (-1)^{a-g} \binom{a}{g} \left( \frac{t - a}{p - g} \right) (q - 2)^{t-a-p+g}.
\]

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

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

This implies
**Proposition 7.** The matrix \( U \) gives a block-diagonalisation of \( A_{q,n} \).

**Proof.** Equation (34) implies that each matrix \( \tilde{M}_{t,p}^{i,j} \) 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 \((a, b)\) such that \( a \in q^n \) satisfies \(|S(a)| = a, a_v \neq q - 1\) for \( v = 1, \ldots, n \), and \( b \in S_{k-a}^n \), 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 \( U^* A_{q,n} U \). 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 \( A_{q,n} \), which is \( \binom{n+2}{4} \). This follows from

\[
\sum_{0 \leq a \leq k \leq n+a-k} (n + a + 1 - 2k)^2
= n \sum_{a=0}^n \sum_{k=a}^n (n + a + 1 - 2k)^2
= \sum_{a \equiv n(2)} (1^2 + 3^2 + \cdots + (n + 1 - a)^2) + \sum_{a \not\equiv n(2)} (2^2 + 4^2 + \cdots + (n + 1 - a)^2)
= \sum_{a \equiv n(2)} \binom{n+1-a+2}{3} + \sum_{a \not\equiv n(2)} \binom{n+1-a+2}{3}
= \sum_{a=0}^n \frac{n-a+3}{3} = \binom{n+4}{4}.
\]

(35)

\( \square \)

### 3 Application to coding

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

\[
R_x := |\text{Aut}_0(q,n)|^{-1} \sum_{\pi \in \text{Aut}_0(q,n)} \chi^{\pi(\sigma_x(C))}(\chi^{\pi(\sigma_x(C))})^T.
\]

(36)

Next define the matrices \( R \) and \( R' \) by:

\[
R := |C|^{-1} \sum_{x \in C} R_x, \quad (37)
R' := (q^n - |C|)^{-1} \sum_{x \in q^n \setminus C} R_x.
\]
As the $R_x$, and hence also $R$ and $R'$, are convex combinations of positive semidefinite matrices, they are positive semidefinite. By construction, the matrices $R_x$, and hence the matrices $R$ and $R'$ are invariant under permutations $\pi \in \text{Aut}_0(q,n)$ of the rows and columns and hence they are elements of the algebra $\mathcal{A}_{q,n}$. Write

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

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

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

**Proof.** The matrix

$$S := |C|R + (q^n - |C|)R' = |\text{Aut}_0(q,n)|^{-1} \sum_{\sigma \in \text{Aut}(q,n)} \chi_\sigma(C)(\chi_\sigma(C))^T \quad (40)$$

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

$$S = \sum_k y_k A_k. \quad (41)$$

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

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

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

$$(q^n - |C|)R' = S - |C|R = \sum_k |C| x_{k,0}^{0,0} A_k - |C| \sum_{(i,j,t,p)} x_{i,j}^{t,p} M_{i,j}^{t,p} = \sum_k \left( x_{k,0}^{0,0} - \sum_{i+j-t-p = k} x_{i,j}^{t,p} M_{i,j}^{t,p} \right) = \sum_{(i,j,t,p)} (x_{i+j-t-p,0}^{0,0} - x_{i,j}^{t,p}) M_{i,j}^{t,p},$$

which proves the proposition. \qed

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

\[
\text{for all } a, k \text{ with } 0 \leq a \leq k \leq n + a - k, \text{ the matrices } \\
\left( \sum_{t,p} \alpha(i, j, t, p, a, k)x_{i,j}^{t,p} \right)_{i,j=k}^{n+a-k} \\
\text{and} \\
\left( \sum_{t,p} \alpha(i, j, t, p, a, k)(x_{i+j-t-p,0}^{0,0} - x_{i,j}^{t,p}) \right)_{i,j=k}^{n+a-k}
\]

are positive semidefinite.

Define the numbers

\[
\lambda_{i,j}^{t,p} := |(C \times C \times C) \cap X_{i,j,t,p}|, \\
\gamma_{i,j}^{t,p} := |\{0\} \times q^n \times q^n) \cap X_{i,j,t,p}|
\]

be the number of nonzero entries of \( M_{i,j}^{t,p} \). A simple calculation yields:

\[
\gamma_{i,j}^{t,p} = (q - 1)^{i+j-t}(q - 2)^{t-p}\left(\begin{array}{c}
\frac{n}{p} \\
t-p
\end{array}\right).
\]

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 \( \langle M, N \rangle := \text{tr}(M^*N) \) the standard innerproduct on the space of complex \( q^n \times q^n \) matrices. Observe that the matrices \( M_{i,j}^{t,p} \) are pairwise orthogonal and that

\[
\langle M_{i,j}^{t,p}, M_{i,j}^{t,p} \rangle = \gamma_{i,j}^{t,p} \text{ for } (i, j, t, p) \in I(q, n). 
\]

Hence

\[
\frac{1}{|C|} \sum_{x \in C} \langle Rx, M_{i,j}^{t,p} \rangle = \frac{|\{x\} \times C \times C) \cap X_{i,j,t,p}|}{|\gamma_{i,j}^{t,p}|} \\
= \frac{1}{|C|} \lambda_{i,j}^{t,p}
\]

implies that

\[
R = \frac{1}{|C|} \sum_{(i,j,t,p) \in I(q,n)} \lambda_{i,j}^{t,p}(\gamma_{i,j}^{t,p})^{-1}M_{i,j}^{t,p}.
\]

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 $d$:

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

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 $M = \chi^{\sigma(C)}(\chi^{\sigma(C)})^T$ then $0 \leq M_{x,y} \leq M_{x,x}$ for any $x, y \in q^n$ and $\sigma \in \text{Aut}(q,n)$.

Since $|C|^2 = \sum_i x_{i,0}^{0,0}$, 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 $O(n^3)$ 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


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

<table>
<thead>
<tr>
<th>$n$</th>
<th>$d$</th>
<th>$n$</th>
<th>$d$</th>
<th>best lower bound known</th>
<th>best upper bound</th>
<th>best upper bound previously known</th>
<th>Delsarte bound</th>
</tr>
</thead>
<tbody>
<tr>
<td>12</td>
<td>4</td>
<td>12</td>
<td>4</td>
<td>4374</td>
<td>6839</td>
<td>7029</td>
<td>7029</td>
</tr>
<tr>
<td>13</td>
<td>4</td>
<td>13</td>
<td>4</td>
<td>8019</td>
<td>19270</td>
<td>19682</td>
<td>19683</td>
</tr>
<tr>
<td>14</td>
<td>4</td>
<td>14</td>
<td>4</td>
<td>24057</td>
<td>54774</td>
<td>59046</td>
<td>59049</td>
</tr>
<tr>
<td>15</td>
<td>4</td>
<td>15</td>
<td>4</td>
<td>72171</td>
<td>149585</td>
<td>153527</td>
<td>153527</td>
</tr>
<tr>
<td>16</td>
<td>4</td>
<td>16</td>
<td>4</td>
<td>216513</td>
<td>424001</td>
<td>434815</td>
<td>434815</td>
</tr>
<tr>
<td>12</td>
<td>5</td>
<td>12</td>
<td>5</td>
<td>729</td>
<td>1557</td>
<td>1562</td>
<td>1562</td>
</tr>
<tr>
<td>13</td>
<td>5</td>
<td>13</td>
<td>5</td>
<td>2187</td>
<td>4078</td>
<td>4163</td>
<td>4163</td>
</tr>
<tr>
<td>14</td>
<td>5</td>
<td>14</td>
<td>5</td>
<td>6561</td>
<td>10624</td>
<td>10736</td>
<td>10736</td>
</tr>
<tr>
<td>15</td>
<td>5</td>
<td>15</td>
<td>5</td>
<td>6561</td>
<td>29213</td>
<td>29524</td>
<td>29524</td>
</tr>
<tr>
<td>13</td>
<td>6</td>
<td>13</td>
<td>6</td>
<td>729</td>
<td>1449</td>
<td>1562</td>
<td>1562</td>
</tr>
<tr>
<td>14</td>
<td>6</td>
<td>14</td>
<td>6</td>
<td>2187</td>
<td>3660</td>
<td>3885</td>
<td>4163</td>
</tr>
<tr>
<td>15</td>
<td>6</td>
<td>15</td>
<td>6</td>
<td>2187</td>
<td>9904</td>
<td>10736</td>
<td>10736</td>
</tr>
<tr>
<td>16</td>
<td>6</td>
<td>16</td>
<td>6</td>
<td>6561</td>
<td>27356</td>
<td>29524</td>
<td>29524</td>
</tr>
<tr>
<td>14</td>
<td>7</td>
<td>14</td>
<td>7</td>
<td>243</td>
<td>805</td>
<td>836</td>
<td>836</td>
</tr>
<tr>
<td>15</td>
<td>7</td>
<td>15</td>
<td>7</td>
<td>729</td>
<td>2204</td>
<td>2268</td>
<td>2268</td>
</tr>
<tr>
<td>16</td>
<td>7</td>
<td>16</td>
<td>7</td>
<td>729</td>
<td>6235</td>
<td>6643</td>
<td>6643</td>
</tr>
<tr>
<td>13</td>
<td>8</td>
<td>13</td>
<td>8</td>
<td>42</td>
<td>95</td>
<td>103</td>
<td>103</td>
</tr>
<tr>
<td>15</td>
<td>8</td>
<td>15</td>
<td>8</td>
<td>243</td>
<td>685</td>
<td>711</td>
<td>712</td>
</tr>
<tr>
<td>16</td>
<td>8</td>
<td>16</td>
<td>8</td>
<td>297</td>
<td>1923</td>
<td>2079</td>
<td>2079</td>
</tr>
<tr>
<td>14</td>
<td>9</td>
<td>14</td>
<td>9</td>
<td>31</td>
<td>62</td>
<td>66</td>
<td>81</td>
</tr>
<tr>
<td>15</td>
<td>9</td>
<td>15</td>
<td>9</td>
<td>81</td>
<td>165</td>
<td>166</td>
<td>166</td>
</tr>
<tr>
<td>16</td>
<td>10</td>
<td>16</td>
<td>10</td>
<td>54</td>
<td>114</td>
<td>117</td>
<td>127</td>
</tr>
</tbody>
</table>
Table 2: New upper bounds on $A_4(n, d)$

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

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

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