Semidefinite bounds for nonbinary codes based on quadruples

Litjens, B.; Polak, S.; Schrijver, A.

DOI
10.1007/s10623-016-0216-5

Publication date
2017

Document Version
Final published version

Published in
Designs, Codes and Cryptography

Des. Codes Cryptogr. (2017) 84:87–100
DOI 10.1007/s10623-016-0216-5

Semidefinite bounds for nonbinary codes based on quadruples

Bart Litjens[1] · **Sven Polak**[1] · **Alexander Schrijver**[1]

Received: 30 December 2015 / Revised: 21 April 2016 / Accepted: 25 April 2016 /
Published online: 11 May 2016

Abstract For nonnegative integers q, n, d, let $A_q(n, d)$ denote the maximum cardinality of a code of length n over an alphabet $[q]$ with q letters and with minimum distance at least d. We consider the following upper bound on $A_q(n, d)$. For any k, let $\mathcal{C}_k$ be the collection of codes of cardinality at most k. Then $A_q(n, d)$ is at most the maximum value of $\sum_{v\in[q]^n} x(\{v\})$, where x is a function $\mathcal{C}_4 \to \mathbb{R}_+$ such that $x(\emptyset) = 1$ and $x(C) = 0$ if C has minimum distance less than d, and such that the $\mathcal{C}_2\times\mathcal{C}_2$ matrix $(x(C\cup C'))_{C,C'\in\mathcal{C}_2}$ is positive semidefinite. By the symmetry of the problem, we can apply representation theory to reduce the problem to a semidefinite programming problem with order bounded by a polynomial in n. It yields the new upper bounds $A_4(6, 3) \le 176$, $A_4(7, 3) \le 596$, $A_4(7, 4) \le 155$, $A_5(7, 4) \le 489$, and $A_5(7, 5) \le 87$.

Keywords Code · Nonbinary code · Upper bounds · Semidefinite programming · Delsarte

Mathematics Subject Classification 94B65 · 05E10 · 90C22 · 20C30

1 Introduction

Let $\mathbb{Z}_+$ denote the set of nonnegative integers, and denote $[m] = \{1, \dots, m\}$, for any $m \in \mathbb{Z}_+$. Fixing $n, q \in \mathbb{Z}_+$, a *code* is a subset of $[q]^n$. So $[q]$ serves as the alphabet and n as the word length. We will assume throughout that $q \ge 2$. (If you prefer $\{0, 1, \dots, q-1\}$ as alphabet, take the letters mod q.) While this paper is mainly meant to handle the case $q \ge 3$, the results also hold for $q = 2$.

For $v, w \in [q]^n$, the *(Hamming) distance* $d_H(v, w)$ is equal to the number of $i \in [n]$ with $v_i \ne w_i$. The *minimum distance* of a code C is the minimum of $d_H(v, w)$ taken over distinct

This is one of several papers published in *Designs, Codes and Cryptography* comprising the special issue in honor of Andries Brouwer's 65th birthday.

✉ Alexander Schrijver
lex@cwi.nl

[1] Korteweg-De Vries Institute for Mathematics, University of Amsterdam, Amsterdam, The Netherlands

$v, w \in C$. Then $A_q(n, d)$ denotes the maximum cardinality of a code with minimum distance at least d. We will study the following upper bound on $A_q(n, d)$, sharpening Delsarte's classical linear programming bound [4].

For $k \in \mathbb{Z}_+$, let $\mathcal{C}_k$ be the collection of subsets C of $[q]^n$ with $|C| \leq k$. For each $x : \mathcal{C}_4 \to \mathbb{R}$ define the $\mathcal{C}_2 \times \mathcal{C}_2$ matrix $M(x)$ by

$$M(x)_{C,C'} := x(C \cup C') \tag{1}$$

for $C, C' \in \mathcal{C}_2$. Then define

$$B_q(n, d) := \max_x \sum_{w \in [q]^n} x(\{w\}), \text{ where } x : \mathcal{C}_4 \to \mathbb{R}_+ \text{ satisfies} \tag{2}$$

(i) $x(\emptyset) = 1$,
(ii) $x(C) = 0$ if the minimum distance of C is less than d,
(iii) $M(x)$ is positive semidefinite.

Proposition 1 $A_q(n, d) \leq B_q(n, d)$.

Proof Let $D \subseteq [q]^n$ have minimum distance at least d and satisfy $|D| = A_q(n, d)$. Define $x : \mathcal{C}_4 \to \mathbb{R}$ by $x(C) = 1$ if $C \subseteq D$ and $x(C) = 0$ otherwise. Then x satisfies the conditions: (iii) follows from the fact that for this x one has $M(x)_{C,C'} = x(C)x(C')$ for all $C, C' \in \mathcal{C}_2$. Moreover, $\sum_{w \in [q]^n} x(\{w\}) = |D| = A_q(n, d)$. □

The optimization problem (2) is huge, but, with methods from representation theory, can be reduced to a size bounded by a polynomial in n, with entries (i.e., coefficients) being polynomials in q. This makes it possible to solve (2) by semidefinite programming for some moderate values of n, d, and q, leading to improvements of best known upper bounds for $A_q(n, d)$.

To explain the reduction, let H be the wreath product $S_q^n \rtimes S_n$. For each k, the group H acts naturally on $\mathcal{C}_k$, maintaining minimum distances and cardinalities of elements of $\mathcal{C}_k$ (being codes). Then we can assume that x is invariant under the H-action on $\mathcal{C}_4$. That is, we can assume that $x(C) = x(D)$ whenever $C, D \in \mathcal{C}_2$ and $D = g \cdot C$ for some $g \in H$. Indeed, (2)(i)(ii)(iii) are maintained under replacing x by $g \cdot x$. (Note that $M(g \cdot x)$ is obtained from $M(x)$ by simultaneously permuting rows and columns.) Moreover, the objective function does not change by this action. Hence the optimum x can be replaced by the average of all $g \cdot x$ (over all $g \in H$), by the convexity of the set of positive semidefinite matrices. This makes the optimum solution H-invariant.

Let Ω be the set of H-orbits on $\mathcal{C}_4$. Note that Ω is bounded by a polynomial in n (independently of q). As there exists an H-invariant optimum solution, we can replace, for each $\omega \in \Omega$ and $C \in \omega$, each variable $x(C)$ by a variable $y(\omega)$. In this way we obtain $M(y)$.

Then $M(y)$ is invariant under the action of H on its rows and columns, induced from the action of H on $\mathcal{C}_2$. Hence $M(y)$ can be block-diagonalized by $M(y) \mapsto U^{\mathsf{T}} M(y) U$, where U is a matrix independent of y. The entries in each block are linear functions of the variables $y(\omega)$. There are several equal (or equivalent) blocks. Taking one block from each such class gives a matrix of order polynomial in n with numbers that are polynomials in q. The issue crucial for us is that the original matrix $M(y)$ is positive semidefinite if and only if each of the blocks is positive semidefinite.

In this paper we will describe the blocks that reduce the problem. With this, we found the following improvements on the known bounds for $A_q(n, d)$, with thanks to Hans D. Mittelmann for his help in solving the larger-sized problems.

q	n	d	Best lower bound known	New upper bound	Best upper bound previously known
4	6	3	164	176	179
4	7	3	512	596	614
4	7	4	128	155	169
5	7	4	250	489	545
5	7	5	53	87	108

The best upper bounds previously known for $A_4(6, 3)$ and $A_4(7, 3)$ are Delsarte's linear programming bound [4]; the other three best upper bounds previously known were given by Gijswijt, Schrijver, and Tanaka [7]. We refer to the most invaluable tables maintained by Andries Brouwer [3] with the best known lower and upper bounds for the size of error-correcting codes (see also Bogdanova, Brouwer, Kapralov, and Östergård [1] and Bogdanova and Östergård [2] for studies of bounds for codes over alphabets of size $q = 4$ and $q = 5$, respectively).

1.1 Comparison with earlier bounds

The bound $B_q(n, d)$ described above is a sharpening of Delsarte's classical linear programming bound [4]. The value of the Delsarte bound is equal to our bound after replacing $\mathcal{C}_4$ and $\mathcal{C}_2$ by $\mathcal{C}_2$ and $\mathcal{C}_1$, respectively, which generally yields a less strict bound.

We can add to (2) the condition that, for each $D \in \mathcal{C}_4$, the $S(D) \times S(D)$ matrix

$$(x(C \cup C'))_{C,C' \in S(D)} \text{ is positive semidefinite,} \tag{3}$$

where $S(D) := \{C \in \mathcal{C}_4 \mid C \supseteq D, |D| + 2|C \setminus D| \leq 4\}$. (So (iii) in (2) is the case $D = \emptyset$.) Also the addition of (3) allows a reduction of the optimization problem to polynomial size as above. (It can be seen that adding (3) for $|D| = 2$ suffices.) For $q = 2$ we obtain in this way the bound given by Gijswijt et al. [6]. Our present description gives a more conceptual and representation-theoretic approach to the method of [6].

A bound intermediate to the Delsarte bound and the currently investigated bound is based on considering functions $x : \mathcal{C}_3 \to \mathbb{R}_+$ and the related matrices—see Schrijver [9] for binary codes and Gijswijt et al. [7] for nonbinary codes.

2 Preliminaries on representation theory

We assume some familiarity with classical representation theory, in particular of the symmetric group S_n and of finite groups in general. In this section we give a brief review, also to settle some notation and terminology. We refer to Sagan [8] for background.

A group G *acts* on a set X if there is a group homomorphism $G \to S_X$, where S_X is the group of bijections $X \to X$. The image of $g \in G$ in S_X is indicated by $g \cdot$. If X is a linear space, the bijections are assumed to be linear functions. The action of G on a set X induces an action of G on the linear space $\mathbb{C}^X$, by $(g \cdot f)(x) := f(g^{-1} \cdot x)$ for all $g \in G$, $f \in \mathbb{C}^X$, and $x \in X$. If any group G acts on X, then X^G denotes the set of elements of X invariant under the action of G.

Let $m \in \mathbb{Z}_+$ and let G be a finite group acting unitarily on $V = \mathbb{C}^m$ (meaning that for each $g \in G$ there is a unitary $m \times m$ matrix U such that $g \cdot x = Ux$ for all $x \in \mathbb{C}^m$). Then V can be decomposed uniquely as direct sum of the G-isotypical components $V_1, \ldots, V_k$.

For distinct i, j, V_i and V_j are orthogonal (with respect to the inner product $\langle x, y\rangle = x^*y$ for $x, y \in \mathbb{C}^m$, where x^* is the conjugate transpose of x). Next, each V_i is a direct sum $V_{i,1} \oplus \cdots \oplus V_{i,m_i}$ of mutually G-isomorphic, irreducible G-modules, in such a way that $V_{i,j}$ and $V_{i,j'}$ are orthogonal for distinct j, j'. (This decomposition is generally not unique.) For each $i \leq k$ and $j \leq m_i$, choose a nonzero $u_{i,j} \in V_{i,j}$ such that for each i and all j, $j' \leq m_i$ there exists a G-isomorphism $V_{i,j} \to V_{i,j'}$ bringing $u_{i,j}$ to $u_{i,j'}$. For each $i \leq k$, let U_i be the matrix $[u_{i,1}, \ldots, u_{i,m_i}]$, considering the $u_{i,j}$ as columns. We call any matrix set $\{U_1, \ldots, U_k\}$ that can be obtained in this way *representative* for the action of G on $\mathbb{C}^m$. It has the property that the function

$$\Phi : (\mathbb{C}^{m\times m})^G \to \bigoplus_{i=1}^{k} \mathbb{C}^{m_i \times m_i} \quad \text{with} \quad \Phi(X) := \bigoplus_{i=1}^{k} U_i^* X U_i \tag{4}$$

for $X \in (\mathbb{C}^{m\times m})^G$ is bijective. So $\sum_i m_i^2$ is equal to the dimension of $(\mathbb{C}^{m\times m})^G$ (and hence can be considerably smaller than m).

Another important property of a representative matrix set is that any $X \in (\mathbb{C}^{m\times m})^G$ is positive semidefinite if and only if $\Phi(X)$ is positive semidefinite. (A positive semidefinite matrix is a Hermitian matrix with all eigenvalues nonnegative.)

In our applications below, throughout G is acting real-orthogonally on a vector space $V = \mathbb{R}^m$; that is, for each $g \in G$ there is a real orthogonal $m \times m$ matrix U with $g \cdot x = Ux$ for each $x \in \mathbb{C}^m$.

Moreover, as it turns out, for the cases considered in the present paper the matrices U_i can be taken real-valued (which is computationally convenient). This implies that $\Phi(X) = \bigoplus_{i=1}^{k} U_i^{\mathsf{T}} X U_i$ for $X \in (\mathbb{R}^{m\times m})^G$ and $\Phi((\mathbb{R}^{m\times m})^G) = \bigoplus_{i=1}^{k} \mathbb{R}^{m_i \otimes m_i}$. Moreover, a matrix $X \in \mathbb{R}^{m\times m}$ is positive semidefinite if and only if $U_i^{\mathsf{T}} X U_i$ is positive semidefinite for each $i = 1, \ldots, k$. For later reference we state that, since for all i, j, $V_{i,j}$ is the linear space spanned by $G \cdot u_{i,j}$,

$$\mathbb{R}^m = \bigoplus_{i=1}^{k} \bigoplus_{j=1}^{m_i} \mathbb{R}G \cdot u_{i,j}. \tag{5}$$

It will turn out to be convenient to consider the columns of the matrices U_i as elements of the dual space $(\mathbb{R}^m)^*$ (by taking the standard inner product). Then each U_i is an ordered set of linear functions on $\mathbb{R}^m$. (The order plays a role in describing a representative matrix set for the action of the wreath product $G^n \rtimes S_n$ on $V^{\otimes n}$.)

2.1 A representative set for the action of S_n on $V^{\otimes n}$

Classical representation theory of the symmetric group yields a representative set for the natural action of S_n on $V^{\otimes n}$, where V is a finite-dimensional vector space, which we will describe now.

For $n \in \mathbb{Z}_+$, $\lambda \vdash n$ means that λ is equal to $(\lambda_1, \ldots, \lambda_t)$ for some t, with $\lambda_1 \geq \cdots \geq \lambda_t > 0$ integer and $\lambda_1 + \cdots + \lambda_t = n$. The number t is called the *height* of λ. The *Young shape* $Y(\lambda)$ of λ is the set

$$Y(\lambda) := \big\{(i, j) \in \mathbb{Z}_+^2 \mid 1 \leq j \leq t, 1 \leq i \leq \lambda_j\big\}. \tag{6}$$

For any $j_0 \leq t$, the set of elements (i, j_0) in $Y(\lambda)$ is called the j_0-*th row* of $Y(\lambda)$. Let R_λ be the group of permutations π of $Y(\lambda)$ with $\pi(Z) = Z$ for each row Z of $Y(\lambda)$. For any

$i_0 \leq \lambda_1$, the set of elements (i_0, j) in $Y(\lambda)$ is called the *i_0-th column* of $Y(\lambda)$. Let C_λ be the group of permutations π of $Y(\lambda)$ with $\pi(Z) = Z$ for each column Z of $Y(\lambda)$.

A *λ-tableau* is a function $\tau : Y(\lambda) \to \mathbb{Z}_+$. We put $\tau \sim \tau'$ for λ-tableaux τ, τ' if $\tau' = \tau r$ for some $r \in R_\lambda$. A λ-tableau is *semistandard* if in each row the entries are nondecreasing and in each column the entries are increasing. Let $T_{\lambda,m}$ denote the collection of semistandard λ-tableaux with entries in $[m]$. Note that $T_{\lambda,m} \neq \emptyset$ if and only if λ has height at most m.

Let $B = (B(1), \ldots, B(m))$ be an ordered basis of V^*. For $\tau \in T_{\lambda,m}$, define the following element of $(V^*)^{\otimes n}$:

$$u_{\tau,B} := \sum_{\tau' \sim \tau} \sum_{c \in C_\lambda} \operatorname{sgn}(c) \bigotimes_{y \in Y(\lambda)} B(\tau' c(y)), \tag{7}$$

where we order the Young shape $Y(\lambda)$ by concatenating its rows. Then the matrix set

$$\{[u_{\tau,B} \mid \tau \in T_{\lambda,m}] \quad | \quad \lambda \vdash n\} \tag{8}$$

is representative for the natural action of S_n on $V^{\otimes n}$.

3 Reduction of the optimization problem

In this section we describe reducing the optimization problem (2) conceptually. In Sect. 4 we consider the reduction computationally. For the remainder of this paper we fix n and q.

We consider the natural action of $H = S_q^n \rtimes S_n$ on $\mathbb{R}^{\mathcal{C}_2}$. If $U_1, \ldots, U_k$ form a representative set of matrices for this action, then with (4) we obtain a reduction of the size of the optimization problem to polynomial size. To make this reduction explicit in order to apply semidefinite programming, we need to express each $m_i \times m_i$ matrix $U_i^\mathsf{T} M(y) U_i$ as an explicit matrix in which each entry is a linear combination of the variables $y(\omega)$ for $\omega \in \Omega$ (the set of H-orbits of $\mathcal{C}_4$).

For $\omega \in \Omega$, let N_ω be the $\mathcal{C}_2 \times \mathcal{C}_2$ matrix with 0, 1 entries satisfying

$$(N_\omega)_{\{\alpha,\beta\},\{\gamma,\delta\}} = 1 \text{ if and only if } \{\alpha, \beta, \gamma, \delta\} \in \omega \tag{9}$$

for $\alpha, \beta, \gamma, \delta \in [q]^n$. Then

$$U_i^\mathsf{T} M(y) U_i = \sum_\omega y(\omega) U_i^\mathsf{T} N_\omega U_i. \tag{10}$$

So to get the reduction, we need to obtain the matrices $U_i^\mathsf{T} N_\omega U_i$ explicitly, for each $\omega \in \Omega$ and for each $i = 1, \ldots, k$. We do this in a number of steps.

We first describe in Sect. 3.1 a representative set for the natural action of S_q on $\mathbb{R}^{q \times q}$. From this we derive, in Sect. 3.2, with the help of the representative set for the action of S_n on $V^{\otimes n}$ described in Sect. 2.1, a representative set for the action of the wreath product $H = S_q^n \rtimes S_n$ on the set $([q]^n)^2$ of *ordered* pairs of words in $[q]^n$, in other words, on $\mathbb{R}^{([q]^n)^2} \cong (\mathbb{R}^{q \times q})^{\otimes n}$. From this we derive in Sect. 3.3 a representative set for the action of H on the set $\mathcal{C}_2 \setminus \{\emptyset\}$ of *unordered* pairs $\{v, w\}$ (including singleton) of words v, w in $[q]^n$. Then in Sect. 3.4 we derive a representative set for the action of H on the set $\mathcal{C}_2^d \setminus \{\emptyset\}$, where $\mathcal{C}_2^d$ is the set of codes in $\mathcal{C}_2$ of minimum distance at least d. (So each singleton word belongs to $\mathcal{C}_2^d$.) Finally, in Sect. 3.4 we include the empty set $\emptyset$, by an easy representation-theoretic argument.

3.1 A representative set for the action of S_q on $\mathbb{R}^{q\times q}$

We now consider the natural action of S_q on $\mathbb{R}^{q\times q}$. Let e_j be the j-th unit basis vector in $\mathbb{R}^q$, I_q be the $q\times q$ identity matrix, J_q be the all-one $q\times q$ matrix, $\mathbf{1}$ be the all-one column vector in $\mathbb{R}^q$, $N := (e_1 - e_2)\mathbf{1}^\mathsf{T}$, and $E_{i,j} := e_i e_j^\mathsf{T}$. We furthermore define the following matrices, where we consider matrices in $\mathbb{R}^{q\times q}$ as *columns* of the matrices B_i:

$$\begin{aligned}
B_1 &:= [I_q, J_q - I_q],\\
B_2 &:= [E_{1,1} - E_{2,2}, N - N^\mathsf{T}, N + N^\mathsf{T} - 2(E_{1,1} - E_{2,2})],\\
B_3 &:= [E_{1,2} + E_{2,3} + E_{3,1} - E_{2,1} - E_{3,2} - E_{1,3}],\\
B_4 &:= [E_{1,3} - E_{3,2} + E_{2,4} - E_{4,1} + E_{3,1} - E_{2,3} + E_{4,2} - E_{1,4}].
\end{aligned} \tag{11}$$

The matrices in $\mathbb{R}^{q\times q}$ will in fact be taken as elements of the dual space $(\mathbb{R}^{q\times q})^*$ (by taking the inner product), so that they are elements of the algebra $\mathcal{O}(\mathbb{R}^{q\times q})$ of polynomials on the linear space $\mathbb{R}^{q\times q}$.

Then $\{B_1, \ldots, B_4\}$ is representative for the natural action of S_q on $\mathbb{R}^{q\times q}$, if $q \geq 4$. If $q \leq 3$, we delete B_4, and if $q = 2$ we moreover delete B_3 and the last column of B_2 (as this column is 0 if $q = 2$). We give a proof in Appendix 1.

If $q \geq 4$, set $k = 4, m_1 = 2, m_2 := 3, m_3 := 1$, and $m_4 := 1$. If $q = 3$, set $k = 3, m_1 = 2$, $m_2 := 3$, and $m_3 := 1$. If $q = 2$, set $k = 2$, $m_1 = 2$, and $m_2 := 2$. For the remainder of this paper we fix $k, m_1, \ldots, m_k$, and $B_1, \ldots, B_k$.

3.2 A representative set for the action of H on $(\mathbb{R}^{q\times q})^{\otimes n}$

Recall that $H = S_q^n \rtimes S_n$ and that we have fixed $k, m_1, \ldots, m_k$, and $B_1, \ldots, B_k$ in Sect. 3.1.

We next consider the action of H on the set $([q]^n)^2$ of *ordered* pairs of code words. For that, we derive a representative set for the natural action of H on $(\mathbb{R}^{q\times q})^{\otimes n} \cong \mathbb{R}^{([q]^n)^2}$ from the results described in Sects. 2.1 and 3.1.

Let $\boldsymbol{N}$ be the collection of all k-tuples $(n_1, \ldots, n_k)$ of nonnegative integers adding up to n. For $\boldsymbol{n} = (n_1, \ldots, n_k) \in \boldsymbol{N}$, let $\boldsymbol{\lambda} \vdash \boldsymbol{n}$ mean that $\boldsymbol{\lambda} = (\lambda_1, \ldots, \lambda_k)$ with $\lambda_i \vdash n_i$ for $i = 1, \ldots, k$. (So each λ_i is equal to $(\lambda_{i,1}, \ldots, \lambda_{i,t})$ for some t.)

For $\boldsymbol{\lambda} \vdash \boldsymbol{n}$ define

$$W_{\boldsymbol{\lambda}} := T_{\lambda_1,m_1} \times \cdots \times T_{\lambda_k,m_k}, \tag{12}$$

and for $\boldsymbol{\tau} = (\tau_1, \ldots, \tau_k) \in W_{\boldsymbol{\lambda}}$ define

$$v_{\boldsymbol{\tau}} := \bigotimes_{i=1}^{k} u_{\tau_i,B_i}. \tag{13}$$

Proposition 2 *The matrix set*

$$\{[v_{\boldsymbol{\tau}} \mid \boldsymbol{\tau} \in W_{\boldsymbol{\lambda}}] \quad \mid \boldsymbol{n} \in \boldsymbol{N}, \boldsymbol{\lambda} \vdash \boldsymbol{n}\} \tag{14}$$

is representative for the action of $S_q^n \rtimes S_n$ on $(\mathbb{R}^{q\times q})^{\otimes n}$.

Proof Let L_i denote the linear space spanned by $B_i(1), \ldots, B_i(m_i)$. Then

$$(\mathbb{R}^{q\times q})^{\otimes n} \overset{\text{by (5)}}{=} \left(\bigoplus_{i=1}^{k}\bigoplus_{j=1}^{m_i}\mathbb{R}S_q\cdot B_i(j)\right)^{\otimes n} = \mathbb{R}S_n\cdot\bigoplus_{\boldsymbol{n}\in N}\bigotimes_{i=1}^{k}\left(\bigoplus_{j=1}^{m_i}\mathbb{R}S_q\cdot B_i(j)\right)^{\otimes n_i}$$

$$= \mathbb{R}S_n\cdot\mathbb{R}S_q^{\otimes n}\cdot\bigoplus_{\boldsymbol{n}\in N}\bigotimes_{i=1}^{k}L_i^{\otimes n_i} \overset{\text{by (5)}}{=} \mathbb{R}H\cdot\bigoplus_{\boldsymbol{n}\in N}\bigotimes_{i=1}^{k}\bigoplus_{\lambda_i\vdash n_i}\bigoplus_{\tau_i\in T_{\lambda_i,m_i}}\mathbb{R}S_{n_i}\cdot u_{\tau_i,B_i}$$

$$= \bigoplus_{\boldsymbol{n}\in N}\bigoplus_{\boldsymbol{\lambda}\vdash\boldsymbol{n}}\bigoplus_{\boldsymbol{\tau}\in W_{\boldsymbol{\lambda}}}\mathbb{R}H\cdot v_{\boldsymbol{\tau}}. \tag{15}$$

Now for each $\boldsymbol{n}, \boldsymbol{\lambda}$ and $\boldsymbol{\tau}, \boldsymbol{\sigma} \in W_{\boldsymbol{\lambda}}$, there is an H-isomorphism $\mathbb{R}H\cdot v_{\boldsymbol{\tau}} \to \mathbb{R}H\cdot v_{\boldsymbol{\sigma}}$ bringing $v_{\boldsymbol{\tau}}$ to $v_{\boldsymbol{\sigma}}$, since for each $i = 1, \ldots, k$, setting $H_i := S_q^{n_i} \rtimes S_{n_i}$, there is an H_i-isomorphism $\mathbb{R}H_i\cdot u_{\tau_i,B_i} \to \mathbb{R}H_i\cdot u_{\sigma_i,B_i}$. Hence (where $\mathrm{Sym}_t(X) := (X^{\otimes t})^{S_t}$ for any $t \in \mathbb{Z}_+$ and linear space X, with the natural action of S_t on $X^{\otimes t}$)

$$\begin{aligned}
\dim((\mathbb{R}^{q\times q})^{\otimes n}\otimes(\mathbb{R}^{q\times q})^{\otimes n})^H &\geq \sum_{\boldsymbol{n}\in N}\sum_{\boldsymbol{\lambda}\vdash\boldsymbol{n}}|W_{\boldsymbol{\lambda}}|^2 = \sum_{\boldsymbol{n}\in N}\sum_{\boldsymbol{\lambda}\vdash\boldsymbol{n}}\prod_{i=1}^{k}|T_{\lambda_i,m_i}|^2\\
&= \sum_{\boldsymbol{n}\in N}\prod_{i=1}^{k}\sum_{\lambda_i\vdash n_i}|T_{\lambda_i,m_i}|^2\\
&\overset{\text{by (8)}}{=} \sum_{\boldsymbol{n}\in N}\prod_{i=1}^{k}\dim\mathrm{Sym}_{n_i}(\mathbb{R}^{m_i}\otimes\mathbb{R}^{m_i})\\
&= \sum_{\boldsymbol{n}\in N}\prod_{i=1}^{k}\tbinom{m_i^2+n_i-1}{n_i-1} = \tbinom{\sum_{i=1}^{k}m_i^2+n-1}{n-1}\\
&= \dim\mathrm{Sym}_n(((\mathbb{R}^{q\times q})\otimes(\mathbb{R}^{q\times q}))^{S_q})\\
&= \dim((\mathbb{R}^{q\times q})^{\otimes n}\otimes(\mathbb{R}^{q\times q})^{\otimes n})^H
\end{aligned} \tag{16}$$

as $\sum_{i=1}^{k}m_i^2 = \dim(\mathbb{R}^{q\times q}\otimes\mathbb{R}^{q\times q})^{S_q}$. So we have equality throughout in (16), and hence each $\mathbb{R}H\cdot v_{\boldsymbol{\tau}}$ is irreducible, and if $\boldsymbol{\lambda} \neq \boldsymbol{\lambda}'$, then for each $\boldsymbol{\tau} \in W_{\boldsymbol{\lambda}}$ and $\boldsymbol{\tau}' \in W_{\boldsymbol{\lambda}'}$, $\mathbb{R}H\cdot v_{\boldsymbol{\tau}}$ and $\mathbb{R}H\cdot v_{\boldsymbol{\tau}'}$ are not H-isomorphic. □

3.3 Unordered pairs

We now go over from the set $([q]^n)^2$ of ordered pairs of code words to the set $\mathcal{C}_2 \setminus \{\emptyset\}$ of unordered pairs (including singletons) of code words. For this we consider the action of the group S_2 on $\mathbb{R}^{[q]^n\times[q]^n} \cong \mathbb{R}^{([q]^n)^2} \cong (\mathbb{R}^{q\times q})^{\otimes n}$, where the nonidentity element σ in S_2 acts as taking the transpose. The actions of S_2 and H commute.

Let F be the $(\mathcal{C}_2 \setminus \{\emptyset\}) \times ([q]^n)^2$ matrix with 0, 1 entries satisfying

$$F_{\{\alpha,\beta\},(\gamma,\delta)} = 1 \text{if and only if} \{\gamma,\delta\} = \{\alpha,\beta\}, \tag{17}$$

for $\alpha, \beta, \gamma, \delta \in [q]^n$. Then the function $x \mapsto Fx$ is an H-isomorphism $(\mathbb{R}^{([q]^n)^2})^{S_2} \to \mathbb{R}^{\mathcal{C}_2\setminus\{\emptyset\}}$.

Now note that each $B_i(j)$, as matrix in $\mathbb{R}^{q\times q}$, is S_2-invariant (i.e., symmetric) except for $B_2(2)$ and $B_3(1)$, while $\sigma\cdot B_2(2) = -B_2(2)$ and $\sigma\cdot B_3(1) = -B_3(1)$ (as $B_2(2)$ and $B_3(1)$ are skew-symmetric). So for any $\boldsymbol{n} \in N$, $\boldsymbol{\lambda} \vdash \boldsymbol{n}$, and $\boldsymbol{\tau} \in W_{\boldsymbol{\lambda}}$, we have

$$\sigma \cdot v_{\boldsymbol{\tau}} = (-1)^{|\tau_2^{-1}(2)|+|\tau_3^{-1}(1)|} v_{\boldsymbol{\tau}}. \tag{18}$$

Therefore, let $W'_{\boldsymbol{\lambda}}$ be the set of those $\boldsymbol{\tau} \in W_{\boldsymbol{\lambda}}$ with $|\tau_2^{-1}(2)| + |\tau_3^{-1}(1)|$ even. Then the matrix set

$$\{[v_{\boldsymbol{\tau}} \mid \boldsymbol{\tau} \in W'_{\boldsymbol{\lambda}}] \mid \boldsymbol{n} \in \boldsymbol{N}, \boldsymbol{\lambda} \vdash \boldsymbol{n}\} \tag{19}$$

is representative for the action of H on $(\mathbb{R}^{([q]^n)^2})^{S_2}$. Hence the matrix set

$$\{[Fv_{\boldsymbol{\tau}} \mid \boldsymbol{\tau} \in W'_{\boldsymbol{\lambda}}] \mid \boldsymbol{n} \in \boldsymbol{N}, \boldsymbol{\lambda} \vdash \boldsymbol{n}\} \tag{20}$$

is representative for the action of H on $\mathbb{R}^{\mathcal{C}_2 \setminus \{\emptyset\}}$.

3.4 Restriction to pairs of words at distance at least d

Let $d \in \mathbb{Z}_+$, and let $\mathcal{C}_2^d$ be the collection of elements of $\mathcal{C}_2$ of minimum distance at least d. Note that each singleton code word belongs to $\mathcal{C}_2^d$, and that H acts on $\mathcal{C}_2^d$. From (20) we derive a representative set for the action of H on $\mathbb{R}^{\mathcal{C}_2^d \setminus \{\emptyset\}}$.

To see this, let for each $t \in \mathbb{Z}_+$, L_t be the subspace of $\mathbb{R}^{\mathcal{C}_2}$ spanned by the elements $e_{\{\alpha,\beta\}}$ with $\alpha, \beta \in [q]^n$ and $d_H(\alpha, \beta) = t$. (For any $Z \in \mathcal{C}_2$, e_Z denotes the unit base vector in $\mathbb{R}^{\mathcal{C}_2^d}$ for coordinate Z.)

Then for any $\boldsymbol{n} \in \boldsymbol{N}$, $\boldsymbol{\lambda} \vdash \boldsymbol{n}$, and $\boldsymbol{\tau} \in W'_{\boldsymbol{\lambda}}$, the irreducible representation $H \cdot Fv_{\boldsymbol{\tau}}$ is contained in L_t, where

$$t := n - |\tau_1^{-1}(1)| - |\tau_2^{-1}(1)|, \tag{21}$$

since $B_1(1) = I_q$ and $B_2(1) = E_{1,1} - E_{2,2}$ are the only two entries $B_i(j)$ in the B_i that have nonzeros on the diagonal of the matrix $B_i(j)$. Let $W''_{\boldsymbol{\lambda}}$ be the set of those $\boldsymbol{\tau}$ in $W'_{\boldsymbol{\lambda}}$ with

$$n - |\tau_1^{-1}(1)| - |\tau_2^{-1}(1)| \in \{0, d, d+1, \ldots, n\}. \tag{22}$$

Then a representative set for the action of H on $\mathcal{C}_2^d \setminus \{\emptyset\}$ is

$$\left\{[Fv_{\boldsymbol{\tau}} \mid \boldsymbol{\tau} \in W''_{\boldsymbol{\lambda}}] \mid \boldsymbol{n} \in \boldsymbol{N}, \boldsymbol{\lambda} \vdash \boldsymbol{n}\right\}. \tag{23}$$

3.5 Adding $\emptyset$

To obtain a representative set for the action of H on $\mathcal{C}_2^d$, note that H acts trivially on $\emptyset$. So $e_\emptyset$ belongs to the H-isotypical component of $\mathbb{R}^{\mathcal{C}_2}$ that consists of H-invariant elements. Now the H-isotypical component of $\mathbb{R}^{\mathcal{C}_2 \setminus \{\emptyset\}}$ that consists of the H-invariant elements corresponds to the matrix in the representative set indexed by indexed by $\boldsymbol{n} = (n, 0, 0, 0)$ and $\boldsymbol{\lambda} = ((n), (), (), ())$, where $() \vdash 0$. So to obtain a representative set for $\mathbb{R}^{\mathcal{C}_2}$, we just add $e_\emptyset$ as column to this matrix.

4 How to compute $(Fv_{\boldsymbol{\tau}})^{\mathsf{T}} N_{\boldsymbol{\omega}} Fv_{\boldsymbol{\sigma}}$

We now have a reduction of the original problem to blocks with coefficients $(Fv_{\boldsymbol{\tau}})^{\mathsf{T}} N_\omega Fv_{\boldsymbol{\sigma}}$, for $\boldsymbol{n} \in \boldsymbol{N}$, $\boldsymbol{\lambda} \vdash \boldsymbol{n}$, $\boldsymbol{\tau}, \boldsymbol{\sigma} \in W_{\boldsymbol{\lambda}}$, and $\omega \in \Omega$. The number and orders of these blocks are bounded by a polynomial in n, but computing these coefficients still must be reduced in time, since the order of F, $v_{\boldsymbol{\tau}}$, $v_{\boldsymbol{\sigma}}$, and N_ω is exponential in n.

Fix $\boldsymbol{n} \in \boldsymbol{N}$, $\boldsymbol{\lambda} \vdash \boldsymbol{n}$, and $\boldsymbol{\tau}, \boldsymbol{\sigma} \in W_{\boldsymbol{\lambda}}$. For any $\omega \in \Omega$, let $L_\omega := F^{\mathsf{T}} N_\omega F$. So L_ω is a $([q]^n \times [q]^n) \times ([q]^n \times [q]^n)$ matrix with 0,1 entries satisfying

$$(L_\omega)_{(\alpha,\beta),(\gamma,\delta)} = 1 \text{ if and only if } \{\alpha, \beta, \gamma, \delta\} \in \omega, \tag{24}$$

for all $\alpha, \beta, \gamma, \delta \in [q]^n$. By definition of L_ω,

$$(F v_{\boldsymbol{\tau}})^{\mathsf{T}} N_\omega F v_{\boldsymbol{\sigma}} = v_{\boldsymbol{\tau}}^{\mathsf{T}} L_\omega v_{\boldsymbol{\sigma}}. \tag{25}$$

So it suffices to evaluate the latter value.

Let Π be the collection of partitions of $\{1, 2, 3, 4\}$ into at most q parts. There is the following bijection between Π and the set of orbits of the action of S_q on $[q]^4$.

For each word $w \in [q]^4$, let part(w) be the partition $P \in \Pi$ such that i and j belong to the same class of P if and only if $w_i = w_j$ (for $i, j = 1, \ldots, 4$). Then two elements $v, w \in [q]^4$ belong to the same S_q-orbit if and only if part(v) = part(w). Note that $|\Pi| = 8$ if $q = 2$, $|\Pi| = 14$ if $q = 3$, and $|\Pi| = 15$ if $q \geq 4$. (In all cases, $|\Pi| = \dim(\mathbb{R}^{q\times q})^{S_q} = \sum_{i=1}^{k} m_i^2$.)

For $P \in \Pi$, let

$$d_P := \sum_{\substack{i_1,\ldots,i_4 \in [q] \\ \text{part} i_1 \cdots i_4 = P}} e_{i_1} e_{i_2}^{\mathsf{T}} \otimes e_{i_3} e_{i_4}^{\mathsf{T}}, \tag{26}$$

where each e_i is a unit basis column vector in $\mathbb{R}^q$, so that $e_i e_j^{\mathsf{T}}$ is a matrix in $\mathbb{R}^{q\times q}$. Then $D := \{d_P \mid P \in \Pi\}$ is a basis of $(\mathbb{R}^{q\times q} \otimes \mathbb{R}^{q\times q})^{S_q}$. Let D^* be the dual basis.

For any $(\alpha, \beta, \gamma, \delta) \in ([q]^n)^4$, let

$$\psi(\alpha, \beta, \gamma, \delta) := \prod_{i=1}^{n} d^*_{\text{part}(\alpha_i \beta_i \gamma_i \delta_i)}, \tag{27}$$

which is a degree n polynomial on $(\mathbb{R}^{q\times q} \otimes \mathbb{R}^{q\times q})^{S_q}$. Then $\psi(\alpha, \beta, \gamma, \delta) = \psi(\alpha', \beta', \gamma', \delta')$ if and only if $(\alpha, \beta, \gamma, \delta)$ and $(\alpha', \beta', \gamma', \delta')$ belong to the same H-orbit on $([q]^n)^4$. So this gives a bijection between the set Q of degree n monomials expressed in the dual basis D^* and the set of H-orbits on $([q]^n)^4 \cong ([q]^4)^n$. The function $([q]^n)^4 \to \mathcal{C}_4$ with $(\alpha_1, \ldots, \alpha_4) \mapsto \{\alpha_1, \ldots, \alpha_4\}$ then gives a surjective function $\omega : Q \to \Omega \setminus \{\{\emptyset\}\}$.

For any $\mu \in Q$, define

$$K_\mu := \sum_{\substack{d_1,\ldots,d_n \in D \\ d_1^* \cdots d_n^* = \mu}} \bigotimes_{j=1}^{n} d_j. \tag{28}$$

Lemma 1 *For each $\omega \in \Omega$: $L_\omega = \sum_{\substack{\mu \in Q \\ \omega(\mu) = \omega}} K_\mu$.*

Proof Choose $\alpha, \beta, \gamma, \delta \in [q]^n$. Then

$$\begin{aligned} \sum_{\substack{\mu \in Q \\ \omega(\mu) = \omega}} (K_\mu)_{(\alpha,\beta),(\gamma,\delta)} &= \sum_{\substack{\mu \in Q \\ \omega(\mu) = \omega}} \sum_{\substack{P_1,\ldots,P_n \in \Pi \\ d^*_{P_1} \cdots d^*_{P_n} = \mu}} \left(\bigotimes_{i=1}^{n} d_{P_i} \right)_{\alpha,\beta,\gamma,\delta} \\ &= \sum_{\substack{\mu \in Q \\ \omega(\mu) = \omega}} \sum_{\substack{P_1,\ldots,P_n \in \Pi \\ d^*_{P_1} \cdots d^*_{P_n} = \mu}} \prod_{i=1}^{n} (d_{P_i})_{\alpha_i,\beta_i,\gamma_i,\delta_i}. \end{aligned} \tag{29}$$

Now the latter value is 1 if $\omega(d^*_{\mathrm{part}(\alpha_1\beta_1\gamma_1\delta_1)}\cdots d^*_{\mathrm{part}(\alpha_n\beta_n\delta_n\gamma_n)}) = \omega$, and is 0 otherwise. So it is equal to $(L_\omega)_{(\alpha,\beta),(\gamma,\delta)}$. □

By this lemma, it suffices to compute $v_{\boldsymbol{\tau}}^{\mathsf{T}} K_\mu v_{\boldsymbol{\sigma}}$ for each $\mu \in Q$. To this end, define the following degree n polynomial on $W := (\mathbb{R}^{q\times q} \otimes \mathbb{R}^{q\times q})^{S_q}$:

$$p_{\boldsymbol{\tau},\boldsymbol{\sigma}} := \prod_{i=1}^{k} \sum_{\substack{\tau_i'\sim\tau_i \\ \sigma_i'\sim\sigma_i}} \sum_{c_i,c_i'\in C_{\lambda_i}} \mathrm{sgn}(c_i c_i') \prod_{y\in Y(\lambda_i)} B_i(\tau_i' c_i(y)) \otimes B_i(\sigma_i' c_i'(y)). \tag{30}$$

This polynomial can be computed (i.e., expressed as linear combination of monomials in $B_i(j) \otimes B_i(h)$) in time bounded by a polynomial in n (Gijswijt [5], see Appendix 2 in Sect. 1 below).

Lemma 2 $\sum_{\mu\in Q} (v_{\boldsymbol{\tau}}^{\mathsf{T}} K_\mu v_{\boldsymbol{\sigma}})\mu = p_{\boldsymbol{\tau},\boldsymbol{\sigma}}$.

Proof We can write for each $\mu \in Q$:

$$v_{\boldsymbol{\tau}}^{\mathsf{T}} K_\mu v_{\boldsymbol{\sigma}} = (v_{\boldsymbol{\tau}} \otimes v_{\boldsymbol{\sigma}})(K_\mu), \tag{31}$$

using the fact that $v_{\boldsymbol{\tau}}, v_{\boldsymbol{\sigma}} \in ((\mathbb{R}^{q\times q})^{\otimes n})^*$ and $K_\mu \in (\mathbb{R}^{q\times q})^{\otimes n} \otimes (\mathbb{R}^{q\times q})^{\otimes n}$. So it suffices to show

$$\sum_{\mu\in Q} (v_{\boldsymbol{\tau}} \otimes v_{\boldsymbol{\sigma}})(K_\mu)\mu = p_{\boldsymbol{\tau},\boldsymbol{\sigma}}. \tag{32}$$

Consider any $f = f_1 \cdots f_n$ with $f_j \in W^*$ for $j = 1, \ldots, n$. Then

$$f = \sum_{\mu\in Q} \left(\bigotimes_{j=1}^{n} f_j \right)(K_\mu)\,\mu. \tag{33}$$

Indeed,

$$\begin{aligned} \sum_{\mu\in Q} \left(\bigotimes_{j=1}^{n} f_j \right)(K_\mu)\,\mu &= \sum_{\substack{d_1,\ldots,d_n\in D \\ d_1^*\cdots d_n^*=\mu}} \left(\bigotimes_{j=1}^{n} f_j \right)\left(\bigotimes_{j=1}^{n} d_j \right)\mu \\ &= \sum_{d_1,\ldots,d_n\in D} \prod_{j=1}^{n} f_j(d_j) d_j^* = \prod_{j=1}^{n} \sum_{d\in D} f_j(d) d^* \\ &= \prod_{j=1}^{n} f_j = f. \end{aligned} \tag{34}$$

Applying (33) to each term f of $p_{\boldsymbol{\tau},\boldsymbol{\sigma}}$ as given by (30) we obtain (32), in view of (7) and (13). □

So $v_{\boldsymbol{\tau}}^{\mathsf{T}} K_\mu v_{\boldsymbol{\sigma}}$ can be computed by expressing the polynomial $p_{\boldsymbol{\tau},\boldsymbol{\sigma}}$ as linear combination of monomials $\mu \in Q$, which are products of linear functions in D^*. So it suffices to express each $B_i(j) \otimes B_i(h)$ as linear function into the basis D^*, that is, to calculate the numbers $(B_i(j) \otimes B_i(h))(d_P)$ for all $i = 1, \ldots, k$, $j, h = 1, \ldots, m_i$, and $P \in \Pi$—see Appendix 3 (Sect. 1 below).

We finally consider the entries in the row and column for $\emptyset$ in the matrix associated with $\boldsymbol{\lambda} = ((n), (), (), ())$ (cf. Sect. 3.5). Trivially, $e_\emptyset^\mathsf{T} M(x) e_\emptyset = (M(x))_{\emptyset,\emptyset} = x(\emptyset)$, which is set to 1 in the optimization problem. Any $\boldsymbol{\tau} \in W_{\boldsymbol{\lambda}}$ is determined by the number t of 2's in the row of the Young shape $Y((n))$. Then

$$v_{\boldsymbol{\tau}} = \sum_{\substack{u,w\in[q]^n \\ d_H(u,w)=t}} e_{(u,w)} \quad \text{and hence} \quad F v_{\boldsymbol{\tau}} = \sum_{\substack{u,w\in[q]^n \\ d_H(u,w)=t}} e_{\{u,w\}}. \tag{35}$$

Hence, as $\emptyset \cup \{u, w\} = \{u, w\}$,

$$e_\emptyset^\mathsf{T} M(x) F v_{\boldsymbol{\tau}} = \sum_{\substack{u,w\in[q]^n \\ d_H(u,w)=t}} x(\{u, w\}) = \binom{n}{t} q^n (q-1)^t y(\omega), \tag{36}$$

where ω is the H-orbit of $\mathcal{C}_4$ consisting of all pairs $\{\alpha, \beta\}$ with $d_H(\alpha, \beta) = t$.

Acknowledgements We are very grateful to Hans D. Mittelmann for his help in solving the larger semidefinite programming problems, and to the referee for helpful suggestions as to the presentation of the paper. The research leading to these results has received funding from the European Research Council under the European Union's Seventh Framework Programme (FP7/2007-2013)/ERC Grant Agreement n° 339109.

Appendix 1: The representative set $\{B_1, \ldots, B_k\}$ for the action of S_q on $\mathbb{C}^{q\times q}$

In this section we show that the matrix set $\{B_1, \ldots, B_k\}$ as given in (11) is representative for the natural action of S_q on $\mathbb{C}^{q\times q}$. For $a \in \mathbb{C}^q$, let Δ_a be the $q \times q$ diagonal matrix with diagonal a, and let $\mathbf{1}$ be the all-one column vector in $\mathbb{C}^q$. Define

$$\begin{aligned}
V_{1,1} &:= \{\lambda I_q \mid \lambda \in \mathbb{C}\},\\
V_{1,2} &:= \{\lambda(J_q - I_q) \mid \lambda \in \mathbb{C}\},\\
V_{2,1} &:= \{\Delta_a \mid a \in \mathbb{C}^q, a^\mathsf{T}\mathbf{1} = 0\},\\
V_{2,2} &:= \{a\mathbf{1}^\mathsf{T} - \mathbf{1}a^\mathsf{T} \mid a \in \mathbb{C}^q, a^\mathsf{T}\mathbf{1} = 0\},\\
V_{2,3} &:= \{a\mathbf{1}^\mathsf{T} + \mathbf{1}a^\mathsf{T} - 2\Delta_a \mid a \in \mathbb{C}^q, a^\mathsf{T}\mathbf{1} = 0\},\\
V_{3,1} &:= \{X \in \mathbb{C}^{q\times q} \mid X \text{ skew-symmetric}, X\mathbf{1} = 0\},\\
V_{4,1} &:= \{X \in \mathbb{C}^{q\times q} \mid X \text{ symmetric}, X\mathbf{1} = 0, X_{i,i} = 0 \text{ for all } i \in [q]\}.
\end{aligned} \tag{37}$$

Observe that each $V_{i,j}$ is S_q-stable, and that $V_{i,j}$ and $V_{i',j'}$ are orthogonal whenever $(i, j) \neq (i', j')$ (with respect to the inner product $X, Y \mapsto \mathrm{tr}(X^*Y)$). Moreover $\lambda I_q \mapsto \lambda(J_q - I_q)$ gives an S_q-isomorphism $V_{1,1} \to V_{1,2}$, $\Delta_a \mapsto a\mathbf{1}^\mathsf{T} - \mathbf{1}a^\mathsf{T}$ gives an S_q-isomorphism $V_{2,1} \to V_{2,2}$, and $\Delta_a \mapsto a\mathbf{1}^\mathsf{T} + \mathbf{1}a^\mathsf{T} - 2\Delta_a$ gives an S_q-isomorphism $V_{2,1} \to V_{2,3}$.

Let $q \geq 4$. Then $\dim(V_{i,j}) > 0$ for all i, j. Set, as before, $m_1 = 2, m_2 = 3, m_3 = m_4 = 1$. Then $\sum_{i=1}^4 m_i^2 = 15$, which is equal to the number of partitions of $\{1, 2, 3, 4\}$, hence to the dimension of $(\mathbb{C}^{q\times q} \otimes \mathbb{C}^{q\times q})^{S_q}$. This implies that the $V_{i,j}$ in fact form an orthogonal *decomposition* of $\mathbb{C}^{q\times q}$ into *irreducible* representations and that $V_{i,j}$ and $V_{i',j'}$ are equivalent

representations if and *only if* $i = i'$ (as any further representation, or decomposition, or equivalence would yield that the sum of the squares of the multiplicities of the irreducible representations is strictly larger than 15, contradicting the fact that Φ in (4) is bijective).

Now $B_{1,1}$ and $B_{1,2}$ are the elements of $V_{1,1}$ and $V_{1,2}$ with $\lambda = 1$. Moreover, $B_{2,1}$, $B_{2,2}$, and $B_{2,3}$ are the elements of $V_{2,1}$, $V_{2,2}$, and $V_{2,3}$ with $a = e_1 - e_2$. Finally, $B_{3,1}$ and $B_{4,1}$ are nonzero elements of $V_{3,1}$ and $V_{4,1}$ (they can be chosen arbitrarily). This implies that $\{B_1, \ldots, B_4\}$ is a representative matrix set.

If $q = 3$, then $\dim(V_{4,1}) = 0$, while the dimension of $(\mathbb{C}^{3\times 3} \otimes \mathbb{C}^{3\times 3})^{S_3}$ is equal to the number of partitions of $\{1, 2, 3, 4\}$ into at most 3 classes, which is $2^2 + 3^2 + 1^2 = 14$. If $q = 2$, then moreover $\dim(V_{2,3}) = \dim(V_{3,1}) = 0$, while the dimension of $(\mathbb{C}^{2\times 2} \otimes \mathbb{C}^{2\times 2})^{S_2}$ is equal to the number of partitions of $\{1, 2, 3, 4\}$ into at most 2 classes, which is $2^2 + 2^2 = 8$. Similarly as above, this implies that also for $q \leq 3$, $B_1, \ldots, B_k$ form a representative matrix set.

Appendix 2: Computation of $p_{\tau,\sigma}$

For any $n, m \in \mathbb{Z}_+$, $\lambda \vdash n$, and $\tau, \sigma \in T_{\lambda,m}$, define the polynomial $p_{\tau,\sigma} \in \mathbb{R}[x_{j,h} \mid j, h = 1, \ldots, m]$ by

$$p_{\tau,\sigma}(X) := \sum_{\substack{\tau'\sim\tau \\ \sigma'\sim\sigma}} \sum_{c,c'\in C_\lambda} \operatorname{sgn}(cc') \prod_{y\in Y(\lambda)} x_{\tau' c(y),\sigma' c'(y)}, \tag{38}$$

for $X = (x_{j,h})_{j,h=1}^m \in \mathbb{R}^{m\times m}$.

Proposition 3 *Expressing $p_{\tau,\sigma}$ as a linear combination of monomials can be done in polynomial time, for fixed m.*

Proof First observe that

$$\begin{aligned} p_{\tau,\sigma}(X) &= |C_\lambda| \sum_{\substack{\tau'\sim\tau \\ \sigma'\sim\sigma}} \sum_{c\in C_\lambda} \operatorname{sgn}(c) \prod_{y\in Y_\lambda} x_{\tau'(y),\sigma' c(y)} \\ &= |C_\lambda| \sum_{\substack{\tau'\sim\tau \\ \sigma'\sim\sigma}} \prod_{j=1}^{\lambda_1} \det((x_{\tau'(i,j),\sigma'(i',j)})_{i,i'=1}^{\lambda_j^*}). \end{aligned} \tag{39}$$

(λ^* is the dual partition of λ; that is, λ_j^* is the height of column j.)

For fixed m, when n grows, there will be several columns of $Y(\lambda)$ that are the same both in τ' and in σ'. More precisely, for given τ', σ' let the 'count function' κ be defined as follows: for $t \in \mathbb{Z}_+$ and $v, w \in [m]^t$, $\kappa(v, w)$ is the number of columns j of height t such that $\tau'(i, j) = v_i$ and $\sigma'(i, j) = w_i$ for all $i = 1, \ldots, t$. Then for each $i \leq h := \text{height}(\lambda)$ and each $s \in [m]$:

$$\begin{aligned} \sum_{t=i}^{h} \sum_{\substack{v,w\in[m]^t \\ v_i=s}} \kappa(v, w) &= \text{number of } s \text{ in row } i \text{ of } \tau, \text{ and} \\ \sum_{t=i}^{h} \sum_{\substack{v,w\in[m]^t \\ w_i=s}} \kappa(v, w) &= \text{number of } s \text{ in row } i \text{ of } \sigma. \end{aligned} \tag{40}$$

For any given function $\kappa : \bigcup_{i=1}^{h} [m]^i \times [m]^i \to \mathbb{Z}_+$ satisfying (40), there are precisely

$$\prod_{t=1}^{h} \frac{(\lambda_t - \lambda_{t+1})!}{\prod_{v,w\in[m]^t} \kappa(v,w)!} \tag{41}$$

pairs $\tau' \sim \tau$ and $\sigma' \sim \sigma$ having count function κ (setting $\lambda_{h+1} := 0$). (Note that (40) implies $\lambda_t - \lambda_{t+1} = \sum_{v,w\in[m]^t} \kappa(v,w)$, for each t, so that for each t, the factor in (41) is a Newton multinomial coefficient.) Hence

$$p_{\tau,\sigma} = |C_\lambda| \sum_{\kappa} \prod_{t=1}^{h} (\lambda_t - \lambda_{t+1})! \prod_{v,w\in[m]^t} \frac{\det((x_{v(i),w(i')})_{i,i'=1}^{t})^{\kappa(v,w)}}{\kappa(v,w)!}, \tag{42}$$

where κ ranges over functions $\kappa : \bigcup_{t=1}^{h} ([m]^t \times [m]^t) \to \mathbb{Z}_+$ satisfying (40). □

Appendix 3: Expressing $B_i(j) \otimes B_i(h)$ into d_P^*

Recall that each $B_i(j)$ is a linear function on $\mathbb{R}^{q\times q}$, and that each d_P is an element of $\mathbb{R}^{q\times q} \otimes \mathbb{R}^{q\times q}$, where P belongs to the set Π of partitions of $\{1,\dots,4\}$ with at most q classes. We express each $B_i(j) \otimes B_i(h)$ in the dual basis $B^* := \{d_P^* \mid P \in \Pi\}$. The coefficient of d_P^* is obtained by evaluating $(B_i(j) \otimes B_i(h))(d_P)$. This is routine, but we display the expressions.

For this, denote any subset X of $\{1,\dots,4\}$ by a string formed by the elements of X, and denote a partition P of $\{1,\dots,4\}$ by a sequence of its classes (for instance, $d^*_{13,2,4}$ denotes the dual variable d_P^* associated with partition $P = \{\{1,3\},\{2\},\{4\}\}$ of $\{1,2,3,4\}$). Then:

$$\begin{aligned}
B_1(1) \otimes B_1(1) &= q d^*_{1234} + q(q-1) d^*_{12,34},\\
B_1(1) \otimes B_1(2) &= q(q-1)(d^*_{123,4} + d^*_{124,3} + (q-2) d^*_{12,3,4}),\\
B_1(2) \otimes B_1(1) &= q(q-1)(d^*_{1,234} + d^*_{134,2} + (q-2) d^*_{1,2,34}),\\
B_1(2) \otimes B_1(2) &= q(q-1)(d^*_{13,24} + d^*_{14,23} + (q-2)(d^*_{13,2,4} + d^*_{14,2,3} + d^*_{1,23,4}\\
&\quad + d^*_{1,24,3} + (q-3) d^*_{1,2,3,4})).\\
B_2(1) \otimes B_2(1) &= 2 d^*_{1234} - 2 d^*_{12,34},\\
B_2(1) \otimes B_2(2) &= 2q(d^*_{123,4} - d^*_{124,3}),\\
B_2(1) \otimes B_2(3) &= 2(q-2)(d^*_{124,3} + d^*_{123,4} - 2 d^*_{12,3,4}),\\
B_2(2) \otimes B_2(1) &= 2q(d^*_{134,2} - d^*_{1,234}),\\
B_2(2) \otimes B_2(2) &= 2q(2 d^*_{13,24} - 2 d^*_{14,23} + (q-2)(d^*_{13,2,4} - d^*_{14,2,3} - d^*_{1,23,4} + d^*_{1,24,3})),\\
B_2(2) \otimes B_2(3) &= 2q(q-2)(d^*_{13,2,4} + d^*_{14,2,3} - d^*_{1,23,4} - d^*_{1,24,3}),\\
B_2(3) \otimes B_2(1) &= 2(q-2)(d^*_{1,234} + d^*_{134,2} - 2 d^*_{1,2,34}),\\
B_2(3) \otimes B_2(2) &= 2q(q-2)(d^*_{13,2,4} - d^*_{14,2,3} + d^*_{1,23,4} - d^*_{1,24,3}),\\
B_2(3) \otimes B_2(3) &= 2(q-2)(2 d^*_{13,24} + 2 d^*_{14,23} + (q-4)(d^*_{13,2,4} + d^*_{14,2,3} + d^*_{1,23,4}\\
&\quad + d^*_{1,24,3}) - 4(q-3) d^*_{1,2,3,4}).\\
B_3(1) \otimes B_3(1) &= 6(d^*_{13,24} - d^*_{14,23} - d^*_{13,2,4} + d^*_{14,2,3} + d^*_{1,23,4} - d^*_{1,24,3}).\\
B_4(1) \otimes B_4(1) &= 8(d^*_{13,24} + d^*_{14,23} - d^*_{13,2,4} - d^*_{14,2,3} - d^*_{1,23,4} - d^*_{1,24,3}) + 16 d^*_{1,2,3,4}.
\end{aligned}$$

References

1. Bogdanova G.T., Brouwer A.E., Kapralov S.N., Östergård P.R.J.: Error-correcting codes over an alphabet of four elements. Discret. Comput. Geom. **23**, 333–342 (2001).
2. Bogdanova G.T., Östergård P.R.J.: Bounds on codes over an alphabet of five elements. Discret. Math. **240**, 13–19 (2001).
3. Brouwer A.E.: Tables of code bounds, see http://www.win.tue.nl/~aeb/ (2015).
4. Delsarte P.: An algebraic approach to the association schemes of coding theory. Philips Research Reports Supplements 1973 No. 10, Philips Research Laboratories, Eindhoven (1973).
5. Gijswijt D.: Block diagonalization for algebra's associated with block codes. arXiv:0910.4515 (2014).
6. Gijswijt D.C., Mittelmann H.D., Schrijver A.: Semidefinite code bounds based on quadruple distances. IEEE Trans. Inf. Theory **58**, 2697–2705 (2012).
7. Gijswijt D., Schrijver A., Tanaka H.: New upper bounds for nonbinary codes based on the Terwilliger algebra and semidefinite programming. J. Comb. Theory A **113**, 1719–1731 (2006).
8. Sagan B.E.: The Symmetric Group: Representations, Combinatorial Algorithms, and Symmetric Functions, Graduate Texts in Mathematics, vol. 203. Springer, New York (2001).
9. Schrijver A.: New code upper bounds from the Terwilliger algebra and semidefinite programming. IEEE Trans. Inf. Theory **51**, 2859–2866 (2005).