SEMIDEFINITE PROGRAMMING FOR PERMUTATION CODES

MATHIEU BOGAERTS AND PETER DUKES

Abstract. We initiate study of the Terwilliger algebra and related semidefinite programming techniques for the conjugacy scheme of the symmetric group \( \text{Sym}(n) \). In particular, we compute orbits of ordered pairs on \( \text{Sym}(n) \) acted upon by conjugation, explore a block diagonalization of the associated algebra, and obtain improved upper bounds on the size \( M(n,d) \) of permutation codes of lengths up to 7. For instance, these techniques detect the nonexistence of the projective plane of order six via \( M(6,5) < 30 \) and yield a new best bound \( M(7,4) \leq 535 \) for a challenging open case. Each of these represents an improvement on earlier Delsarte linear programming results.

1. Introduction and notation

Consider the symmetric group \( \text{Sym}(n) \) on \( [n] := \{1, \ldots, n\} \). Let \( D \) be a collection of conjugacy classes of \( \text{Sym}(n) \). A subset \( \Gamma \subseteq \text{Sym}(n) \) is an \((n,D)\)-permutation code if, for any two distinct elements \( \phi, \psi \in \Gamma \), their quotient \( \phi \psi^{-1} \) belongs to a class in \( D \). Note that the order of the terms is not important, since permutations are conjugate with their inverses.

The Hamming distance between \( \phi \) and \( \psi \) in \( \text{Sym}(n) \), denoted \( d_H(\phi, \psi) \), is the number of non-fixed points of \( \phi \psi^{-1} \). Equivalently, if \( \phi \) and \( \psi \) are written in single-line notation, \( d_H(\phi, \psi) \) counts the number of disagreements between corresponding positions. It follows that \( d_H \) is a metric for \( \text{Sym}(n) \). To the best of our knowledge, this metric was first considered by Farahat in [9].

In most investigations of permutation codes, the set \( D \) of admissible conjugacy classes reflects this metric and is instead taken as some subset \( D \subseteq [n] \). This interpretation for \( D \) is that all conjugacy classes with \( n-d \) one-cycles, \( d \in D \), are allowed for quotients \( \phi \psi^{-1} \). In other words, in this context, an \((n,D)\)-permutation code \( \Gamma \) is a subset of \( \text{Sym}(n) \) with all nonzero Hamming distances belonging to \( D \). Based on the coding applications discussed below, the standard choice for \( D \) is the interval \( \{d, d+1, \ldots, n\} \) for some minimum distance \( d \).

Let \( M(n,D) \) denote the maximum size of an \((n,D)\)-permutation code. When \( D = \{d, d+1, \ldots, n\} \), this is simply written \( M(n,d) \). Early work determining some

Date: December 7, 2012.
2000 Mathematics Subject Classification. 05E10, 05E30 (primary), 94B65 (secondary).
Key words and phrases. symmetric group, permutation code, Terwilliger algebra, semidefinite programming.
Research of Peter Dukes is supported by NSERC.
bounds and values for $M(n, D)$ began in the late 1970s in [7, 11], where the term ‘permutation array’ was used. Around 2000, permutation codes enjoyed a revival of interest with the discovery in [4, 10] of their applications to trellis codes. Then, the survey article [3] observed connections with permutation polynomials and also initiated the first serious computational attack on lower bounds on $M(n, d)$. A probabilistic lower bound appears in [15]. Meanwhile, linear programming (LP) upper bounds were investigated, first in [17], and then subsequently in [2, 8]. A growing body of related work has emerged, including constant composition codes, injection codes, and study of the packing and covering radii.

The LP bound rests on Delsarte’s theory of association schemes [6] applied to the conjugacy scheme of $\text{Sym}(n)$. More details follow in Section 2. In various combinatorial settings (block designs and binary codes, for instance) Delsarte LP bounds have been successfully improved using semidefinite programming (SDP). In general, the sizes of matrices required for this SDP tend to grow impractically large. So the most successful applications of SDP to designs and codes usually begin with an attack on the algebraic structure. In a little more detail, block diagonalizations of certain matrix algebras are desired in order to scale the computations. This is the content of Dion Gijswijt’s dissertation [12].

For a finite set $X$, we use $M_X(\mathbb{C})$ or $\mathbb{C}^{X \times X}$ to denote the algebra of $|X| \times |X|$ matrices with rows and columns indexed by $X$. (Some canonical ordering of $X$ is usually assumed, leading to the more standard notation $M_n(\mathbb{C})$ or $\mathbb{C}^{n \times n}$; which we also use.) The $(x, y)$-entry of matrix $A \in M_X(\mathbb{C})$ is here denoted $A(x, y)$. All linear spans and generated sub-algebras $\langle A_1, A_2, \ldots \rangle$ are over $\mathbb{C}$, unless otherwise noted. The conjugate transpose $A^\top$ of $A$ is denoted $A^*$ and as usual $A$ is Hermitian if $A^* = A$. A sub-$\mathbb{C}$-algebra of $M_X(\mathbb{C})$ closed under this Hermitian conjugate is called a $\mathbb{C}^*$- (matrix) algebra.

2. BOSE-MESNER AND TERWILLIGER ALGEBRAS

An $d$-class association scheme on a finite set $X$ is a list of binary relations $R_0, \ldots, R_d$ on $X$ such that $R_0$ is the identity relation, the relations partition $X^2$, and the following regularity condition holds: given $x$ and $y$ with $(x, y) \in R_k$, the number of $z \in X$ for which both $(x, z) \in R_i$ and $(z, y) \in R_j$ is a constant depending only on $i, j, k \in \{0, \ldots, d\}$. These values $p^k_{ij}$ are called the structure constants or intersection numbers of the scheme. Here, we are mainly interested in symmetric schemes in which each relation $R_i$ is symmetric and thus $p^k_{ij} = p^k_{ji}$. Chris Godsil’s notes [13] offer a readily available and comprehensive reference on association schemes.

Example 2.1. Consider $X = G$, a finite group. The relations $R_i$ are indexed by the conjugacy classes of $G$, where $R_0$ corresponds with the trivial conjugacy class. Declare $(g, h)$ in $R_i$ if and only if $gh^{-1}$ belongs to the $i$th conjugacy class. The fact that these $R_i$ partition $G^2$ is clear. A character sum can compute the structure constants (see below). This is the conjugacy scheme on $G$. 
Let \(|X| = N\). Define the \(N \times N\) zero-one matrices \(A_0, \ldots, A_d \in M_X(\mathbb{C})\) by

\[
A_i(x, y) = \begin{cases} 
1 & \text{if } (x, y) \in R_i, \\
0 & \text{otherwise}.
\end{cases}
\]

We have \(A_0 = I\) and \(A_0 + \cdots + A_d = J\), the all ones matrix. And from the definition of the structure constants,

\[
(2.1) \quad A_iA_j = \sum_{k=0}^{d} p_{ij}^k A_k.
\]

From this it follows that \(\langle A_0, \ldots, A_d \rangle\) is a commutative \(\mathbb{C}^*\)-matrix sub-algebra of \(M_X(\mathbb{C})\) of dimension \(d + 1\). This is the Bose-Mesner algebra \(\mathfrak{A}\) of the scheme.

From spectral theory, \(\mathfrak{A}\) also has a basis of orthogonal idempotents \(E_0, \ldots, E_d\) with \(E_0 + \cdots + E_d = I\). It is convenient to index \(E_0 = \frac{1}{N}J\), which is evidently one of the idempotents.

The Hadamard or entrywise product of matrices \(A, B \in \mathbb{C}^{N \times N}\) is \(A \circ B\) with \((A \circ B)(i, j) = A(i, j)B(i, j)\). For the Bose-Mesner algebra, we have the dual relations

\[
A_i \circ A_j = \delta_{ij}A_i \quad \text{and} \quad E_iE_j = \delta_{ij}E_i.
\]

In particular, since \(\mathfrak{A}\) is closed under \(\circ\), a parallel version of (2.1) exists; namely,

\[
E_i \circ E_j = \frac{1}{N} \sum_{k=0}^{d} q_{ij}^k E_k
\]

for some positive reals \(q_{ij}^k\). These are called the Krein parameters for the scheme.

The basis change matrices between \((A_0, \ldots, A_d)\) and \((E_0, \ldots, E_d)\) are denoted by \(P\) and \(\frac{1}{N}Q\); explicitly, the entries are given by

\[
A_i = \sum_{j=0}^{d} P(i, j)E_j \quad \text{and} \quad E_i = \frac{1}{N} \sum_{j=0}^{d} Q(i, j)A_j.
\]

The \(E_j\) being projections imply that the entries \(P(i, j)\) are the eigenvalues of the matrices \(A_i\), with the column space of \(E_j\) as the associated eigenspace. For this reason, the matrices \(P, Q\) are called, respectively, the first and second eigenmatrix. They are of course related by \(Q = NP^{-1}\).

For a subset \(Y \subseteq X\), its indicator vector is \(1_Y \in \{0, 1\}^X\), with \(1_Y(x) = 1\) if and only if \(x \in Y\). The inner distribution of a nonempty \(Y\) is \(a = (a_0, \ldots, a_d)\), where

\[
a_i = \frac{1}{|Y|} 1_Y^\top A_i 1_Y = \frac{1}{|Y|} |Y^2 \cap R_i|.
\]

The following observation leads to the famous Delsarte LP bound for cliques in association schemes.

**Theorem 2.2** ((Delsarte, [6])). The inner distribution \(a\) of a nonempty subset of points in an association scheme with second eigenmatrix \(Q\) satisfies \(aQ \geq 0\).
Now consider a pointed set \((X, x)\) with \(x \in X\). Define diagonal zero-one matrices \(E'_0, \ldots, E'_d\) in \(M_X(\mathbb{C})\) by

\[
E'_i(y, y) = \begin{cases} 
1 & \text{if } (x, y) \in R_i, \\
0 & \text{otherwise.}
\end{cases}
\]

Observe that, by analogy with the Bose-Mesner idempotents, these are projections with \(E'_0\) of rank one and \(E'_0 + \cdots + E'_d = I\).

The algebra \(\mathcal{A} = \langle A_i, E'_i \rangle\) obtained by extending \(\mathcal{A}\) by these \(E'_i\) is called the subconstituent or Terwilliger algebra of the scheme with respect to \(x\). Unlike \(\mathcal{A}\), the algebra \(\mathcal{A}\) is not in general commutative.

Completing the duality, we have \(A'_0, \ldots, A'_d\) with

\[
A'_i(y, y) = NE_i(x, y).
\]

After this introduction, we are now interested exclusively in the conjugacy scheme on \(\text{Sym}(n)\). Recall that the conjugacy classes (and irreducible characters) of \(\text{Sym}(n)\) are in correspondence with the integer partitions of \(n\). For a fixed \(n\), we will use \(m\) to denote the number of partitions, and index the conjugacy classes as \(C_0, \ldots, C_{m-1}\), with \(C_0 = \{\text{id}\}\) consisting only of the identity permutation. For any fixed \(\theta \in C_k\), we have

\[
p^k_{ij} = |\{(\phi, \psi) \in C_i \times C_j : \phi \psi = \theta\}|.
\]

Alternatively, as stated in [14],

\[
p^k_{ij} = \frac{|C_i||C_j|}{n!} \sum_{\chi} \frac{\chi(\phi_i)\chi(\phi_j)\chi(\phi_k)}{\chi(\text{id})},
\]

where the sum is over all \(m\) irreducible characters, and where \(\phi_i\) is a representative in class \(i\), etc.

The Bose-Mesner algebra \(\mathcal{A}\) is a commutative sub-algebra of \(M_n(\mathbb{C})\). Its eigenvalues are obtained nearly directly from the character table of \(\text{Sym}(n)\).

**Lemma 2.3** (Tarnanen, [17]). The second eigenvalue matrix \(Q\) for the conjugacy scheme on \(\text{Sym}(n)\) is given by

\[
Q(i, j) = \chi_j(\text{id})\chi_j(\phi_i),
\]

where \(0 \leq i, j < m\) index both the conjugacy classes and irreducible characters.

The idempotents and Krein parameters of this conjugacy scheme are also expressible via the irreducible characters, but we omit the details.

The linear programming bound of Theorem 2.2 now becomes

\[
\begin{align*}
\text{maximize:} & \quad a_0 + a_1 + \cdots + a_{m-1} \\
\text{subject to:} & \quad \sum_{0 \leq i < m} a_i \chi_k(\phi_i) \geq 0 \quad \text{for } 0 \leq k < m, \\
& \quad a_0 = 1, a_i \geq 0, \\
& \quad a_i = 0 \quad \text{if } d_H(\text{id}, \phi_i) \notin D.
\end{align*}
\]
Given \( n \) and \( D \), let \( M_{LP} \) denote this maximum value. Then

\[
M(n, D) \leq M_{LP}.
\]

This was used with some success in [2, 17] to obtain some upper bound \( s \) on permutation codes with \( n < 15 \). Additionally, the LP led to a general upper bound on \( M(n, 4) \) in [8].

When extending to the Terwilliger algebra in this setting, it is natural to take \( \text{id} \in \text{Sym}(n) \) as the distinguished element. We have

\[
E'_i(\phi, \phi) = \begin{cases} 
1 & \text{if } \phi \in C_i, \\
0 & \text{otherwise}.
\end{cases}
\]

The products \( E'_i A_k E'_j \) are supported on the \( C_i \times C_j \) block. This offers a natural decomposition of the Terwilliger algebra in general. Note that \( E'_i A_k E'_j \) is the zero matrix if and only if \( p_{ij} = 0 \).

3. ISOMETRIES, ORBITS, AND THE CENTRALIZER ALGEBRA

Consider the automorphism group \( \text{Aut}(A) \) of the Bose-Mesner algebra of \( \text{Sym}(n) \). On one hand, this is the intersection of the automorphism groups of the graphs whose adjacency matrices are the zero-one generators \( A_i, 0 \leq i < m = p(n) \). Alternatively, this is also the group of isometries of \( \text{Sym}(n) \), when endowed with the Hamming distance metric \( d_H \). Let us also denote this group by \( \text{Iso}(n) \).

Let \( \mathcal{L} \) and \( \mathcal{R} \) denote the group actions of left and right multiplication by \( \text{Sym}(n) \), acting on itself. Let \( \mathcal{I} \) be the (involutorial) group action generated by inversion \( \phi \mapsto \phi^{-1} \) on \( \text{Sym}(n) \). That these actions induce all isometries appears in [9], and is discussed further in [2].

**Lemma 3.1.** \( \text{Aut}(A) = \text{Iso}(n) = (\mathcal{L} \times \mathcal{R}) \rtimes \mathcal{I} \cong \text{Sym}(n) \rtimes 2 \).

Let \( \text{Iso}_1(n) \) be the subgroup of isometries which fixes the identity element. Its action on \( \text{Sym}(n) \) is generated by conjugations \( \mathcal{C} \) and inversion \( \mathcal{I} \). These actions commute, and therefore \( \text{Iso}_1(n) = \mathcal{C} \times \mathcal{I} \cong \text{Sym}(n) \times 2 \).

For the extension to the Terwilliger algebra \( \mathcal{T} \), we are concerned with how \( \text{Iso}_1(n) \) acts on pairs of permutations. In what follows, sums indexed by ‘\( \chi \)’ are to be taken over all irreducible characters \( \chi \) of \( \text{Sym}(n) \).

**Proposition 3.2.** The number of orbits of \( \text{Sym}(n)^2 \), acted on by conjugation and inversion is given by

\[
b_n = \frac{1}{2n} \sum_{\alpha \in \text{Sym}(n)} \left[ \left( \sum_{\chi} \chi^2(\alpha) \right)^2 + \left( \sum_{\chi} \chi(\alpha) \right)^3 \right].
\]
Proof. We use Burnside’s orbit counting lemma to obtain

\[ b_n = \frac{1}{|C \times I|} \sum_{g \in C \times I} |\text{fix}(g)| = \frac{1}{2n!} \left[ \sum_{\alpha \in \text{Sym}(n)} |\{ (\phi, \psi) : \alpha(\phi, \psi)\alpha^{-1} = (\phi, \psi) \}| + \sum_{\alpha \in \text{Sym}(n)} |\{ (\phi, \psi) : \alpha(\phi, \psi)\alpha^{-1} = (\phi^{-1}, \psi^{-1}) \}| \right] \]

\[ = \frac{1}{2n!} \left[ \sum_{\alpha \in \text{Sym}(n)} |\{ \phi : \alpha\phi\alpha^{-1} = \phi \}|^2 + \sum_{\alpha \in \text{Sym}(n)} |\{ \phi : \alpha\phi\alpha^{-1} = \phi^{-1} \}|^2 \right]. \]

Both terms in the sum are connected with interesting class functions on $\text{Sym}(n)$. The first term is just the sum of squared centralizers. Recall that orthonormality of the irreducible characters implies that for an element $\alpha \in \text{Sym}(n)$,

\[ \sum_{\chi} \chi(\alpha)^2 = |C(\alpha)|, \]

the (size of the) centralizer of $\alpha$. So the first of our two summation terms can be rewritten

\[ \sum_{\alpha \in \text{Sym}(n)} \left( \sum_{\chi} \chi^2(\alpha) \right)^2. \]

For the second sum, observe that the condition $\alpha\phi\alpha^{-1} = \phi^{-1}$ is equivalent to $(\alpha\phi)^2 = \alpha^2$. So for a fixed $\alpha$, the number of such $\phi$ is simply the number of square roots of $\alpha^2$ in $\text{Sym}(n)$. As an aside, this counting problem for general groups $G$ was connected long ago (see [18]) with the ‘Frobenius-Schur indicator’

\[ s(\chi) = \frac{1}{|G|} \sum_{g \in G} \chi(g^2). \]

For our purposes, all irreducible representations of $\text{Sym}(n)$ are real and therefore $s(\chi)$ is always 1. The number of square roots of an element $\beta$ reduces in this case to the basic character sum $\sum_{\chi} \chi(\beta)$. For $\beta = \alpha^2$, the term we seek becomes

\[ \sum_{\alpha \in \text{Sym}(n)} \left( \sum_{\chi} \chi(\alpha^2) \right)^2 = \sum_{\beta \in \text{Sym}(n)} \left( \sum_{\chi} \chi(\beta) \right) \left( \sum_{\chi} \chi(\beta) \right)^2 \]

\[ = \sum_{\alpha \in \text{Sym}(n)} \left( \sum_{\chi} \chi(\alpha) \right)^3. \]

Combining (3.1) and (3.2) completes the proof. □

Now consider $\text{Iso}_1^+(n) \cong \text{Sym}(n) \times 2 \times 2$, acting on $\text{Sym}(n)^2$ by conjugation, inversion, and the ‘coordinate swaps’ $(\phi, \psi) \mapsto (\psi, \phi)$. A small extension of Proposition 3.2 also yields a character sum formula to count orbits for this action.
Proposition 3.3. The number of orbits of \( \text{Sym}(n)^2 \), acted on by conjugation, inversion, and coordinate swaps, is given by

\[
b^*_n = \frac{1}{2} \left( b_n + \frac{1}{n!} \sum_{\alpha \in \text{Sym}(n)} \left( \sum_{\chi} \chi(\alpha) \right) \left( \sum_{\chi} \chi^2(\alpha) \right) \right),
\]

where \( b_n \) is as in Proposition 3.2.

Proof. New sums not already present in the proof of Proposition 3.2 count, for a fixed \( \alpha \),

\[
|\{ (\phi, \psi) : \alpha(\phi, \psi)\alpha^{-1} = (\psi, \phi) \}| \quad \text{and} \quad |\{ (\phi, \psi) : \alpha(\phi, \psi)\alpha^{-1} = (\psi^{-1}, \phi^{-1}) \}|.
\]

Since conjugacy by \( \alpha \) is a bijection, it follows that each of these is counted simply by the centralizer of \( \alpha^2 \). Alternatively, we may count, over all \( \beta \in \text{Sym}(n) \), the number of square roots of \( \beta \) times the size of the centralizer of \( \beta \). Using the expressions in the previous proof,

\[
\sum_{\alpha \in \text{Sym}(n)} |C(\alpha^2)| = \sum_{\beta \in \text{Sym}(n)} \left( \sum_{\chi} \chi(\beta) \right) \left( \sum_{\chi} \chi^2(\beta) \right).
\]

This, along with earlier terms, finishes the orbit count. \( \square \)

Table 1 contains some small values of \( b_n \) and \( b^*_n \).

| \( n \) | \( n! \) | \( b_n \) | \( b^*_n \) |
|---|---|---|---|
| 4 | 24 | 43 | 28 |
| 5 | 120 | 155 | 93 |
| 6 | 720 | 761 | 425 |
| 7 | 5040 | 4043 | 2151 |
| 8 | 40320 | 27190 | 14016 |

Let \( O_1, \ldots, O_M \) denote the orbits of \( \text{Sym}(n)^2 \) under \( \text{Iso}_1(n) \cong \text{Sym}(n) \times 2 \). Define the corresponding zero-one matrices \( B_1, \ldots, B_M \in M_{n!}(\mathbb{C}) \) by

\[
B_l(\phi, \psi) = \begin{cases} 
1 & \text{if } (\phi, \psi) \in O_l, \\
0 & \text{otherwise.}
\end{cases}
\]

Put \( \mathcal{B} = \langle B_l : l = 1, \ldots, M \rangle \) and observe that by Proposition 3.2 we have \( \dim(\mathcal{B}) = b_n \).

Alternatively, \( \mathcal{B} = \text{End}_G(X) \), where \( X = \text{Sym}(n) \) and \( G = \text{Iso}_1(n) \). For \( \alpha \in \text{Sym}(n) \), consider the zero-one matrix \( \tilde{\alpha} \in M_{n!}(\mathbb{C}) \) with

\[
\tilde{\alpha}(\phi, \psi) = \begin{cases} 
1 & \text{if } \alpha^{-1}\phi\alpha = \psi, \\
0 & \text{otherwise.}
\end{cases}
\]
Then $\alpha \mapsto \hat{\alpha}$ is the conjugacy representation. Define the action of inversion similarly

$$\hat{\iota}(\phi, \psi) = \begin{cases} 1 & \text{if } \phi^{-1} = \psi, \\ 0 & \text{otherwise}. \end{cases}$$

Let $\hat{\mathcal{R}} = \langle \hat{\iota}, \hat{\alpha} : \alpha \in \text{Sym}(n) \rangle$. The following rephrases the earlier definition of orbits under $\text{Iso}_1(n)$ in terms of matrix algebras.

**Proposition 3.4.** $\mathcal{B}$ is the centralizer algebra of $\mathcal{R}$.

Since conjugacy classes of $\text{Sym}(n)$ are left invariant by both conjugation and inversion, the orbits under $\text{Iso}_1(n)$ admit a classification according to conjugacy classes. In other words, each matrix $B_l$ is supported on some block $C_i \times C_j$. The sum of all such $B_l$ supported on a given block is, when restricted to that block, the all-ones matrix $J$.

With notation from Section 2, we recall that the ‘restricted’ Bose-Mesner algebra $E'[AE]$ has conjugation-invariant generators supported on the $C_i \times C_j$ block. So it follows that $\mathcal{T}$ is a sub-$\mathbb{C}$-algebra of $\mathcal{B}$. The reverse inclusion seems reasonable, but much more difficult to prove. Indeed, the dimensions in Table 1 grow much faster than the number of generators for $\mathcal{T}$.

**Conjecture 3.5.** For the conjugacy scheme of $\text{Sym}(n)$, the Terwilliger algebra has as a basis the zero-one matrices $B_i$, $i = 1, \ldots, M$, defined via orbits of $\text{Sym}(n)^2$ under $\text{Iso}_1(n)$. That is, as $\mathbb{C}$-algebras, we have $\mathcal{T} = \mathcal{B}$.

Conjecture 3.5 was verified up to $n = 5$ in [1]. We have extended this verification to $n = 6$ but leave the general problem to future work.

Fortunately, the center of $\mathcal{B}$ is reasonably easy to describle. The following appears in [15] for general groups; here (and from now on) we are interested in $G = \text{Iso}_1(n) \cong \text{Sym}(n) \times 2$.

**Proposition 3.6.** The primitive central idempotents of $\mathcal{B}$ are given by

$$\epsilon_k = \frac{\chi_k(\text{id})}{2n!} \sum_{\gamma \in G} \chi_k(\gamma) \hat{\gamma},$$

where $0 \leq k < 2m$ indexes the irreducible characters of $G$.

Since the $\epsilon_k$ commute, they have a common basis of eigenvectors. Consider a unitary matrix $U \in M_{n!}(\mathbb{C})$ which has orthonormal eigenvectors of the $\epsilon_k$, organized by columns. Then $U \mathcal{B} U^\top$ is block-diagonalized by simple blocks. Our goal later, in Section 5, is to decompose these simple blocks into basic blocks. For now, though, we have sufficient background to introduce semidefinite programming for permutation codes.

### 4. Semidefinite Programming

Let $\Gamma$ be a subset of $\text{Sym}(n)$, and recall that $1_\Gamma$ is the $n! \times 1$ zero-one indicator vector of $\Gamma$. 
Define now the subgroup $\Pi$ of $\Iso(n)$ consisting of all isometries $t$ such that $\text{id} \in t(\Gamma)$. Let $\Pi'$ denote the complement of this subgroup, consisting of all $t' \in \Iso(n)$ with $\text{id} \not\in t'(\Gamma)$. It is clear that $|\Pi| = 2n!|\Gamma|$, while $|\Pi'| = 2n!(n! - |\Gamma|)$. This defines two matrices

$$R_\Gamma = \frac{1}{|\Pi|} \sum_{t \in \Pi} 1_{t(\Gamma)} \cdot 1_{t(\Gamma)}^T$$

and

$$R'_\Gamma = \frac{1}{|\Pi'|} \sum_{t' \in \Pi'} 1_{t'(\Gamma)} \cdot 1_{t'(\Gamma)}^T$$

which are roughly analogous to the inner distribution vector $a$ of Section 2.

By construction, both $R_\Gamma$ and $R'_\Gamma$ are positive semidefinite (symmetric) matrices. And the trace of $R_\Gamma$ gives the cardinality of $\Gamma$. The $(\text{id}, \text{id})$-entry of $R_\Gamma$ is always 1, since $\text{id}$ appears in all copies under $\Pi$. The $(\text{id}, \text{id})$-entry equals the $(\phi, \phi)$-entry in $R_\Gamma$, and, $R_\Gamma$ being symmetric, it is also equal to the $(\phi, \text{id})$-entry. Since $\Iso(n)$ is transitive on $\Sym(n)$, one has the following formula and lemma.

$$R_\Gamma(\phi, \psi) + \frac{n! - |\Gamma|}{|\Gamma|} R'_\Gamma(\phi, \psi) = R_\Gamma(\phi\psi^{-1}, \phi\psi^{-1}) = R_\Gamma(\text{id}, \phi\psi^{-1}).$$

(In particular, the matrix $R_\Gamma + \frac{n! - |\Gamma|}{|\Gamma|} R'_\Gamma$ has a diagonal of 1.)

**Lemma 4.1.** Consider an entry $(\phi, \psi) \in \Sym(n)^2$. If no quotient in $\Gamma$ belongs to the same conjugacy class as $\phi\psi^{-1}$, then $R_\Gamma(\phi, \psi) = R'_\Gamma(\phi, \psi) = 0$.

Next, we have the key connection with the centralizer algebra $\mathfrak{B}$ discussed in Section 3.

**Proposition 4.2.** The two matrices $R_\Gamma$ and $R'_\Gamma$ belong to the algebra $\mathfrak{B}$.

**Proof.** Recall that $\{B_l\}$ are the zero-one matrices representing the orbits $\{O_l\}$ of $\Sym(n)^2$ under the action of $\Iso_1(n)$. With the convention that $O_1 = \{(\text{id}, \text{id})\}$, one has $R_\Gamma = B_1 + \sum_l a_l B_l$, where the coefficients $a_l$ are explicitly determined by the formula

$$a_l = \frac{|\{(\mu, \nu) \in \Gamma \times \Gamma : (\theta^{-1}\mu, \theta^{-1}\nu) \in O_l\}|}{|\Gamma| |O_l|}.$$ 

Observe that $0 \leq a_l \leq 1$.

Let $I_1$ denote the subset of indices $l \neq 1$ such that $O_l$ contains elements of type $(\text{id}, \phi)$, $(\phi, \text{id})$ or $(\phi, \phi)$, and let $I_2$ be the complementary set $\{2 \ldots M\} \setminus I_1$.

With some rearranging and (4.1), it follows easily that

$$\frac{n! - |\Gamma|}{|\Gamma|} R'_\Gamma = (I - B_1) + \sum_l a_l B'_l,$$

where the matrices $B'_l$ are defined by $B'_l = -B_l$ if $l \in I_2$ and by the following expression if $l \in I_1$:

$$B'_l(\phi, \psi) = \begin{cases} 
1 & \text{if } (\phi\psi^{-1}, \text{id}) \in O_l, \\
-1 & \text{if } \phi = \psi \text{ and } (\phi, \text{id}) \in O_l, \\
0 & \text{otherwise.}
\end{cases}$$

In both cases, we have the required matrices expressed as linear combinations of the $\{B_l\}$. \hfill $\square$
We now summarize the above facts concerning \( R_\Gamma \) and \( R_\Gamma' \).

**Proposition 4.3.** Let \( D \subseteq [0, n] \). For any \((n, D)\)-permutation code \( \Gamma \subseteq \text{Sym}(n) \), we have

\[
\begin{align*}
|\Gamma| &= \text{Tr}(R_\Gamma) \\
R_\Gamma &= B_1 + \sum_{i} a_i B_i \succeq 0 \\
R'_\Gamma &= I - B_1 + \sum_{j} a_j B'_j \succeq 0 \\
R_\Gamma(\text{id}, \text{id}) &= 1 \\
R'_\Gamma(\text{id}, \text{id}) &= 0 \\
R_\Gamma(\phi, \psi) &= R'_\Gamma(\phi, \psi) = 0 \quad \text{if } d_H(\phi, \psi) \notin D
\end{align*}
\]

From this, the following SDP system is obtained, considering the coefficients \( a_i \) as variables in \([0, 1]\):

\[
\begin{align*}
\text{maximize:} & \quad \text{Tr}(R_1) \\
\text{subject to:} & \quad R_1 = B_1 + \sum_{i} a_i B_i \succeq 0 \\
& \quad R_2 = I - B_1 + \sum_{i} a_i B'_i \succeq 0, \quad 0 \leq a_i \leq 1 \\
& \quad R_1(\text{id}, \text{id}) = 1, \\
& \quad R_2(\text{id}, \text{id}) = 0, \\
& \quad R_1(\phi, \psi) = R_2(\phi, \psi) = 0 \quad \text{if } d_H(\phi, \psi) \notin D.
\end{align*}
\]

Given \( n \) and \( D \), let \( M_{SDP} \) denote the maximum value of this program. Then

\[ M(n, D) \leq M_{SDP}. \]

**Table 2.** LP and SDP bounds for \( \text{Sym}(6) \)

| \( D \) | \( M_{SDP} \) | \( M_{LP} \) | \( \Pi_{4 \notin D}d \) | \( D \) | \( M_{SDP} \) | \( M_{LP} \) | \( \Pi_{4 \notin D}d \) |
|---|---|---|---|---|---|---|---|
| \( \emptyset \) | 1 | 1 | 1 | \{4, 5, 6\} | 120 | 120 | 120 |
| \{6\} | 6 | 6 | 6 | \{3, 5, 6\} | 56 | 60 | 90 |
| \{5\} | 12 | 15 | 5 | \{2, 5, 6\} | 27 | 30 | 60 |
| \{4\} | 7 | 12 | 4 | \{3, 4, 6\} | 39 | 48 | 72 |
| \{3\} | 5 | 6 | 3 | \{2, 4, 6\} | 48 | 48 | 48 |
| \{2\} | 2 | 2 | 2 | \{2, 3, 6\} | 20 | 36 | 36 |
| \{5, 6\} | 25 | 30 | 30 | \{3, 4, 5\} | 60 | 60 | 60 |
| \{4, 6\} | 35 | 48 | 24 | \{2, 4, 5\} | 24 | 30 | 80 |
| \{3, 6\} | 18 | 24 | 18 | \{2, 3, 5\} | 14 | 15 | 30 |
| \{2, 6\} | 9 | 12 | 12 | \{2, 3, 4\} | 24 | 24 | 24 |
| \{4, 5\} | 20 | 20 | 20 | \{3, 4, 5, 6\} | 360 | 360 | 360 |
| \{3, 5\} | 14 | 15 | 15 | \{2, 4, 5, 6\} | 120 | 120 | 240 |
| \{2, 5\} | 12 | 15 | 10 | \{2, 3, 5, 6\} | 56 | 60 | 180 |
| \{3, 4\} | 15 | 24 | 12 | \{2, 3, 4, 6\} | 48 | 48 | 144 |
| \{2, 4\} | 8 | 12 | 8 | \{2, 3, 4, 5\} | 120 | 120 | 120 |
| \{2, 3\} | 6 | 6 | 6 | \{2, 3, 4, 5, 6\} | 720 | 720 | 720 |

Recall that the matrices \( B_i \) have size \( n! \times n! \). So presently, we can only directly consider this SDP problem for \( n \leq 6 \). Since permutation codes are well understood
for $n \leq 5$, our main contribution at this stage is a table of SDP bounds for $n = 6$. For $n \geq 7$, it is necessary to consider an equivalent SDP obtained via block-diagonalization of the algebra $\mathfrak{B}$. That is the topic of the next section.

We conclude with Table 2, indicating the SDP bounds for $n = 6$ and various distance sets $D$. For comparison, the Delsarte LP bounds $M_{LP}$ are given, along with the quantity $\Pi_{d \in D} d$, which is an upper bound either for $M(n, D)$ or $M(n, D^*)$.

5. Block diagonalization

First, let us recall the notion of $*$-isomorphism. A linear mapping $\kappa : A \to B$ such that for all $(A, B) \in A \times B$, $\kappa(AB) = \kappa(A)\kappa(B)$ and $\kappa(A^*) = \kappa(A)^*$ is called a $*$-homomorphism of algebras. A bijective such mapping is called a $C^*$-isomorphism and the two algebras $A, B$ are $*$-isomorphic. A $*$-isomorphism preserves positive semidefiniteness.

We may regard $\mathfrak{g}$ as a semisimple $G$-module, acted upon by $\mathfrak{B}$. It therefore decomposes as a sum of orthogonal submodules $W_k$, where $W_k$ has columns forming a basis of the eigenspace of the matrix $\epsilon_k$, defined in (3.3), for $0 \leq k < 2m$. Each $W_k$ is a direct sum of $m_k$ submodules: $W_k = V_k^1 \oplus \cdots \oplus V_k^{m_k}$, with $V_k^i \sim V_k^j$ for all $i, j$. Let $d_k$ denote the dimension of $V_k^i$.

Now we would like to decompose each submodule $W_k$ of $\mathfrak{B} = \text{End}_G(\mathfrak{g}) = \bigoplus_k W_k$ into smaller blocks (that we call basic blocks). The method is the following: for each $k$, compute an element $v_k \in W_k$. Then define $U_k := \mathfrak{B}v_k$, that is a linear subspace of $W_k$.

Note that the vector $v_k$ can be obtained as $\epsilon_k x$ for any vector $x$, because $\epsilon_k(\epsilon_k x) = \epsilon_k x$ since $\epsilon_k$ is idempotent. So any non-zero row of $\epsilon_k$ would give an appropriate element of $U_k$.

By Schur’s lemma, the subspace $U_k$ meets each $V_k^i$ in a 1-dimensional subspace. Then for all $B_i \in \mathfrak{B}$, $B_i : U_k \to U_k$ has an action on the basis of $U_k$. If $(u_1, \ldots, u_{m_k})$ is an orthogonal basis of $U_k$, then the basic block $B_{ik} := B_i|_{U_k}$ of $B_i$ can be obtained by:

$$(B_{ik})(j, l) = \frac{\langle B_i u_j, u_l \rangle}{\|u_j\| \|u_l\|}$$

Each basic block $B_{ik}$ is an $m_k \times m_k$ matrix. The matrix $B_i$ has nonzero entries in $(\phi, \psi)$ position if $(\phi, \psi) \in O_i$. The scalar product defining $B_{ik}$ can be written as:

$$\langle B_i u_j, u_l \rangle = \sum_{(\phi, \psi) \in O_i} (u_j)_\phi (u_l)_\psi.$$
Table 3. LP and SDP bounds for Sym(7)

| \( D \) | \( M_{SDP} \) | \( M_{LP} \) | \( \Pi_{d \in Dd} \) | \( D \) | \( M_{SDP} \) | \( M_{LP} \) | \( \Pi_{d \in Dd} \) |
|-------|-------|-------|------|-------|-------|-------|------|
| \( 0 \) | 1     | 1     | 1    | \( \{4,5\} \) | 26    | 60    | 20   |
| \( \{7\} \) | 7     | 7     | 7    | \( \{3,5\} \) | 15    | 15    | 15   |
| \( \{6\} \) | 28    | 30    | 6    | \( \{2,5\} \) | 14    | 15    | 15   |
| \( \{5\} \) | 14    | 15    | 5    | \( \{3,4\} \) | 21    | 26    | 12   |
| \( \{4\} \) | 9     | 12    | 4    | \( \{2,4\} \) | 9     | 12    | 8    |
| \( \{3\} \) | 6     | 8     | 3    | \( \{2,3\} \) | 7     | 9     | 6    |
| \( \{2\} \) | 2     | 2     | 2    | \( \{5,6,7\} \) | 134   | 140   | 210  |
| \( \{6,7\} \) | 42    | 42    | 42   | \( \{4,6,7\} \) | 181   | 205   | 168  |
| \( \{5,7\} \) | 47    | 52    | 35   | \( \{3,6,7\} \) | 70    | 84    | 126  |
| \( \{4,7\} \) | 34    | 46    | 28   | \( \{2,6,7\} \) | 59    | 84    | 84   |
| \( \{3,7\} \) | 27    | 42    | 21   | \( \{4,5,7\} \) | 74    | 93    | 140  |
| \( \{2,7\} \) | 12    | 14    | 14   | \( \{3,5,7\} \) | 54    | 63    | 105  |
| \( \{5,6\} \) | 30    | 30    | 30   | \( \{2,5,7\} \) | 47    | 52    | 70   |
| \( \{4,6\} \) | 47    | 72    | 24   | \( \{3,4,7\} \) | 49    | 84    | 84   |
| \( \{3,6\} \) | 31    | 36    | 18   | \( \{2,4,7\} \) | 36    | 46    | 56   |
| \( \{2,6\} \) | 34    | 48    | 12   | \( \{2,3,7\} \) | 32    | 42    | 42   |

The algebra \( \mathfrak{B} = \bigoplus_{k=0}^{m-1} \mathbb{C}^{m_k \times m_k} \) generated by the diagonal joins of \( B_{ik} \) yields an algebra that is \(*\)-isomorphic to \( \mathfrak{B} \). Let us define the linear mapping

\[
\Phi : B_i \mapsto D_i := \begin{bmatrix}
B_{i1} & 0 & \ldots & 0 \\
0 & B_{i2} & \ldots & 0 \\
\vdots & \vdots & \ddots & 0 \\
0 & 0 & \ldots & B_{im}
\end{bmatrix}
\]

By construction, \( \Phi \) is a \(*\)-isomorphism, inducing the equivalence between the two systems below.
\[
\begin{align*}
\begin{cases}
\text{maximize: } & \text{Tr}(X) \\
\text{subject to: } & X = \sum_i a_i C_i \succeq 0 \\
& 0 \leq a_i \leq 1
\end{cases}
\iff
\begin{cases}
\text{maximize: } & \text{Tr}(X) \\
\text{subject to: } & \Phi(X) = \sum_i a_i \Phi(C_i) \succeq 0 \\
& 0 \leq a_i \leq 1
\end{cases}
\end{align*}
\]

After similar computations as in the previous section, we can report SDP bounds for \( n = 7 \) according to Table 3.

6. Concluding remarks

For \( n \geq 8 \), the number of variables is presently too large for practical implementation of the SDP, even after block-diagonalization. But we are hopeful that \( n = 8 \) can soon be attacked with some new ideas for generating orbits, block-diagonalizing, and possibly constraining the number of variables. In fact, should the SDP eventually scale up to \( n = 10 \), there is a chance that \( M(10, 9) < 90 \) can be proved in this way. Following [4], this represents an opportunity for a possible alternate proof of the nonexistence of projective planes of order 10.

References

[1] J.M.P. Balmaceda and M. Oura, ‘The Terwilliger algebras of the group association schemes of \( S_5 \) and \( A_5 \)’, Kyushu Journal of Mathematics 48 (1994), 221–231.
[2] M. Bogaerts, ‘New upper bounds for the size of permutation codes via linear programming’, Electronic Journal of Combinatorics 17 (2010), #R135.
[3] W. Chu, C.J. Colbourn and P. Dukes, Permutation codes for powerline communication, Designs Codes and Cryptography 32 (2004), 51–64.
[4] C.J. Colbourn, T. Kløve, and A.C.H. Ling, ‘Permutation arrays for powerline communication and mutually orthogonal Latin squares’, IEEE Transactions on Information Theory 50 (2004), 1289–1291.
[5] E. de Klerk, C. Dobre and D.V. Pasechnik, ‘Numerical block diagonalization of matrix *-algebras with application to semidefinite programming’, Mathematical Programming 129 (2011), 91–111.
[6] P. Delsarte, ‘An algebraic approach to the association schemes of coding theory’, Philips Research Reports Supplements No. 10 (1973).
[7] M. Deza and S.A. Vanstone, ‘Bounds for permutation arrays’, Journal of Statistical Planning and Inference 2 (1978), 197–209.
[8] P. Dukes and N. Sawchuck, ‘Bounds on permutation codes of distance four’, Journal of Algebraic Combinatorics 31 (2010), 143-158.
[9] H. Farahat, ‘The symmetric group as a metric space’, Journal of the London Mathematical Society 35 (1960), 215–220.
[10] H.C. Ferreira and A.J. Han Vinck, ‘Interference cancellation with permutation trellis codes’, Vehicular Technology Conference 5 (2000), 2401–2407.
[11] P. Frankl and M. Deza, ‘On the maximum number of permutations with given maximal or minimal distance’, Journal of Combinatorial Theory Series A 22 (1977), 352–360.
[12] D. Gijswijt, ‘Matrix algebras and semidefinite programming techniques for codes’, Ph.D. dissertation, 2005.
[13] C.D. Godsil, ‘Notes on association schemes’, University of Waterloo, 2005.
[14] D. M. Jackson, ‘Counting Cycles in Permutations by Group Characters, With an Application to a Topological Problem’, Transactions of the American Mathematical Society 299 (1987), 785–801.
[15] P. Keevash and C.Y. Ku, ‘A random construction for permutation codes and the covering radius’, Designs Codes and Cryptography 41 (2006), 79–86.
[16] M.A. Naimark and A.I. Stern, *Theory of Group Representations*, Springer-Verlag, New York, 1982.

[17] H. Tarnanen, ‘Upper bounds on permutation codes via linear programming’, *European Journal of Combinatorics* 20 (1999), 101–114.

[18] E.P. Wigner, ‘On representations of certain finite groups’, *American Journal of Mathematics* 63 (1941), 57–63.

Faculté des Sciences Appliquées, Université Libre de Bruxelles, Bruxelles, Belgium

E-mail address: mbogaert@ulb.ac.be

Department of Mathematics and Statistics, University of Victoria, Victoria, BC V8W 3R4, Canada

E-mail address: dukes@uvic.ca