




New lower bounds on crossing numbers of $K_{m,n}$ from semidefinite programming

Daniel Brosch^{1,2} · Sven C. Polak^{2,3} 

Received: 14 July 2022 / Accepted: 3 October 2023 / Published online: 20 November 2023
© The Author(s) 2023

Abstract

In this paper, we use semidefinite programming and representation theory to compute new lower bounds on the crossing number of the complete bipartite graph $K_{m,n}$, extending a method from de Klerk et al. (SIAM J Discrete Math 20:189–202, 2006) and the subsequent reduction by De Klerk, Pasechnik and Schrijver (Math Prog Ser A and B 109:613–624, 2007). We exploit the full symmetry of the problem using a novel decomposition technique. This results in a full block-diagonalization of the underlying matrix algebra, which we use to improve bounds on several concrete instances. Our results imply that $\text{cr}(K_{10,n}) \geq 4.87057n^2 - 10n$, $\text{cr}(K_{11,n}) \geq 5.99939n^2 - 12.5n$, $\text{cr}(K_{12,n}) \geq 7.25579n^2 - 15n$, $\text{cr}(K_{13,n}) \geq 8.65675n^2 - 18n$ for all n . The latter three bounds are computed using a new and well-performing relaxation of the original semidefinite programming bound. This new relaxation is obtained by only requiring one small matrix block to be positive semidefinite.

Keywords Crossing numbers · Complete bipartite graph · Semidefinite programming · Symmetry reduction · Block-diagonalization

Mathematics Subject Classification 05C10 · 68R10 · 90C22 · 05E10

1 Introduction

Computing the crossing number $\text{cr}(K_{m,n})$ of the complete bipartite graph $K_{m,n}$ is a long-standing open problem, which goes back to Turán in the 1940s. In 1956,

✉ Sven C. Polak
s.c.polak@tilburguniversity.edu

Daniel Brosch
daniel.brosch@aau.at

¹ University of Klagenfurt, Klagenfurt, Austria

² Tilburg University, Tilburg, The Netherlands

³ Centrum Wiskunde & Informatica, Amsterdam, The Netherlands

Zarankiewicz [28] conjectured that $\text{cr}(K_{m,n}) = Z(m, n)$, where $Z(m, n)$ is the Zarankiewicz number

$$Z(m, n) := \lfloor \frac{m-1}{2} \rfloor \lfloor \frac{m}{2} \rfloor \lfloor \frac{n-1}{2} \rfloor \lfloor \frac{n}{2} \rfloor = \lfloor \frac{1}{4}(m-1)^2 \rfloor \lfloor \frac{1}{4}(n-1)^2 \rfloor.$$

Zarankiewicz claimed to have a proof for his conjecture, but this turned out to be false. The conjecture thus remains a notorious open problem. As Erdős and Guy [9] wrote in 1973: ‘Almost all questions that one can ask about crossing numbers remain unsolved’, which is still true today. It is known that $\text{cr}(K_{m,n}) \leq Z(m, n)$, by exhibiting an explicit drawing of $K_{m,n}$ in the plane with $Z(m, n)$ crossings—see Fig. 1 for an example.

In this paper, we use semidefinite programming and representation theory to prove the following lower bounds.

Theorem 1 For all integers n ,

$$\begin{aligned} \text{cr}(K_{10,n}) &\geq 4.87057n^2 - 10n, \\ \text{cr}(K_{11,n}) &\geq 5.99939n^2 - 12.5n, \\ \text{cr}(K_{12,n}) &\geq 7.25579n^2 - 15n, \\ \text{cr}(K_{13,n}) &\geq 8.65675n^2 - 18n. \end{aligned}$$

This theorem and Corollary 1 below yield the best known lower bounds on all fixed $\text{cr}(K_{m,n})$ with $m, n \geq 10$. The best previously known lower bounds for $m, n \geq 10$ are $\text{cr}(K_{m,n}) \geq \frac{(m-1)m}{72}(3.86760n^2 - 8n)$, cf. [6]. For an overview of known results regarding Zarankiewicz’s conjecture, see the survey by Székely [26], or the survey about crossing numbers by Schaefer [23].

We now sketch how these lower bounds are derived. For $m \in \mathbb{N}$, let Z_m be the set of permutations of $[m] := \{1, \dots, m\}$ consisting of a single orbit, i.e., Z_m is the set of all m -cycles from S_m and $|Z_m| = (m - 1)!$. Let $K_{m,n}$ have colour classes $\{1, \dots, m\}$ and $\{b_1, \dots, b_n\}$. For any given drawing of $K_{m,n}$ in the plane, define $\gamma(b_i)$ to be the cyclic permutation $(1, i_2, \dots, i_m) \in Z_m$ with the property that the edges leaving b_i in clockwise order go to $1, i_2, \dots, i_m$ (Table 1).

Let Q be the $Z_m \times Z_m$ matrix with for any $\sigma, \tau \in Z_m$, the entry $Q_{\sigma,\tau}$ is equal to the minimum number of crossings in any drawing of $K_{m,2}$ with $\gamma(b_1) = \sigma$ and $\gamma(b_2) = \tau$.

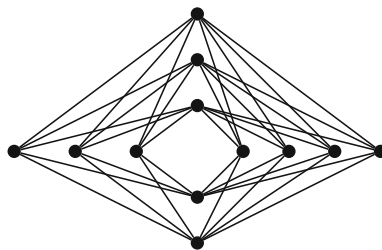


Fig. 1 Optimal drawing of $K_{7,5}$

Table 1 Some of our new lower bounds on $cr(K_{n,n})$

n	Best previously known lower bound	New lower bound	$Z(n, n)$
10	384	388	400
11	581	589	625
12	846	865	900
13	1192	1229	1296

This matrix was defined in [5] and later also used in [6]. An algorithm to compute $Q_{\sigma,\tau}$ was used by Kleitman [15] and more details were described by Woodall [27]. For example, $Q_{\sigma,\sigma} = \lfloor \frac{1}{4}(m-1)^2 \rfloor$ for all $\sigma \in Z_m$. Let $\mathbf{1} \in \mathbb{R}^{Z_m}$ denote the all-ones vector. Consider the following quadratic program.

$$q_m := \min \left\{ x^T Q x \mid x \in \mathbb{R}_{\geq 0}^{Z_m}, x^T \mathbf{1} = 1 \right\}. \tag{1}$$

Theorem 2 (De Klerk et al. [5]) $cr(K_{m,n}) \geq \frac{1}{2}n^2 q_m - \frac{1}{2}n \lfloor \frac{1}{4}(m-1)^2 \rfloor$ for all m, n .

Proof Suppose a drawing of $K_{m,n}$ with $cr(K_{m,n})$ crossings is given. For each $\sigma \in Z_m$, let c_σ be the number of vertices b_i with $\gamma(b_i) = \sigma$. We view c as a vector in \mathbb{R}^{Z_m} and define $x := n^{-1}c$. Then x satisfies the conditions in (1), so $q_m \leq x^T Q x$. For $i, j \in [n]$ let $d_{i,j}$ be the number of crossings of edges leaving b_i with edges leaving b_j . By definition of Q , if $i \neq j$, then $d_{i,j} \geq Q_{\gamma(b_i),\gamma(b_j)}$. This implies

$$\begin{aligned} \frac{1}{2}n^2 q_m &\leq \frac{1}{2}n^2 x^T Q x = \frac{1}{2}c^T Q c = \frac{1}{2} \sum_{i,j=1}^n Q_{\gamma(b_i),\gamma(b_j)} \leq \sum_{i < j} d_{i,j} + \frac{1}{2} \sum_{i=1}^n Q_{\gamma(b_i),\gamma(b_i)} \\ &\leq cr(K_{m,n}) + \frac{1}{2}n \lfloor \frac{1}{4}(m-1)^2 \rfloor, \end{aligned}$$

where the last inequality follows from $Q_{\sigma,\sigma} = \lfloor \frac{1}{4}(m-1)^2 \rfloor$ for all $\sigma \in Z_m$. (In fact, the last inequality is an equality as one may assume that in an optimal drawing edges incident to a common vertex do not cross, cf. [10].) \square

The following semidefinite programming parameter α_m is a lower bound on q_m .

$$\alpha_m := \min \left\{ \langle Q, X \rangle \mid X \in \mathbb{R}_{\geq 0}^{Z_m \times Z_m}, \langle J, X \rangle = 1, X \succeq 0 \right\}. \tag{2}$$

Here $X \succeq 0$ means ‘ X symmetric and positive semidefinite’. It is clear that $q_m \geq \alpha_m$, as any feasible x for q_m gives a feasible $X = xx^T$ for α_m with the same objective value. The values α_m for $m \leq 7$ were computed by De Klerk, Maharry, Pasechnik, Richter, and Salazar [5]. Dobre and Vera [7] computed a better lower bound on q_7 using semidefinite approximations of the copositive cone. The values α_8 and α_9 were computed by De Klerk, Pasechnik and Schrijver [6], who used the regular $*$ -representation to reduce the semidefinite programs in size. The regular $*$ -representation found several applications (see, e.g., [17] for an application in coding theory). In this paper, we

Table 2 The full semidefinite bound α_m from (2) and our relaxation β_m which is described in Sect. 4. We solved the SDPs with multiple precision versions of SDPA [19], and then rounded the dual solutions to rational feasible dual solutions, see Sect. 5.5

m	α_m	$\frac{8\alpha_m}{k(k-1)}$	β_m	$\frac{8\beta_m}{m(m-1)}$
4	1.0000000000	0.6667	1.0000000000	0.6667
5	1.9472135954	0.7789	1.9270509831	0.7708
6	2.9519183588	0.7872	2.9519183588	0.7872
7	4.3593154948	0.8303	4.3107391257	0.8210
8	5.8599856417	0.8371	5.8284271247	0.8326
9	7.7352125975	0.8595	7.6527560430	0.8503
10	9.7411403685	0.8659	9.6866252078	0.8610
11			11.9987919703	0.8726
12			14.5115811776	0.8794
13			17.3135089904	0.8878

The bold values correspond to the newly computed values

show how a full block-diagonalization can be obtained, where we exploit properties of the representation theory of the symmetric group for computational efficiency. This allows us to compute the value α_{10} .

A full symmetry reduction for computing α_m has been developed before by Hymabaccus and Pasechnik [13]. Their method can be used to decompose representations of finite groups exactly. Due to the generic nature of their algorithm, they work with representation matrices instead of vectors in the representative sets. This costs a lot of memory (and time), so they only reach α_7 with their method. In the crossing number case, the coefficients in their block-diagonalization contain irrational numbers, potentially leading to rounding issues in floating-point computations. An advantage of our approach is, apart from being more memory and time efficient, that it results in an exact block-diagonalization with integer coefficients.

Our symmetry reduction consists of three steps. First, we use classical representation theory of the symmetric group S_m to decompose a well-known permutation module. Secondly, we use an elementary but crucial observation given in Proposition 1, to transform this decomposition into a decomposition of \mathbb{R}^{Z_m} as S_m -module. Proposition 1 has potential for a wide array of applications, for example, it can also be directly applied to a problem in coding theory, which we describe in Remark 1 below. The third and final step in our block-diagonalization takes into account a separate $\{\pm 1\}$ -action, in Proposition 3.

Inspired by our symmetry reduction, we also formulate a new relaxation of α_m , which we call β_m . The value β_m is obtained from (2) by only requiring that one specified block, which is described in Sect. 4 below, in the block-diagonalization is positive semidefinite instead of the full matrix X . So $\beta_m \leq \alpha_m$, and our experiments show that the new bound β_m is remarkably close to α_m . We give a combinatorial description of the vectors which underly the block-diagonalization of β_m in Proposition 4. Also, we compute the value β_m for $m \leq 13$. The values are provided in Table 2. Inserting our newly computed values $\alpha_{10}, \beta_{11}, \beta_{12}, \beta_{13}$ in Theorem 2 instead of q_k (using the fact that $\beta_k \leq \alpha_k \leq q_k$), we directly obtain our new bounds in Theorem 1.

1.1 Outline of the paper

In Sect. 2 we explain the consequences of Theorem 1: we investigate to which bounds it leads and relate these bounds to the literature. In Sect. 3 we explain how the symmetry can be used to significantly reduce the problem: we develop a full block-diagonalization. To do this, we use representation theory from the symmetric group and linear algebra. After that, we explain in Sect. 4 how our new relaxation β_m of α_m is defined, which is inspired by the symmetry reduction. We give a combinatorial description of the vectors which underly the block-diagonalization of β_m . Finally, in Sect. 5 we give details about our computations. Here we explain how β_m can be computed in practice: using the dual description in combination with an iterative procedure, we are able to compute β_m for $m \leq 13$ up to high precision on a desktop computer.

2 Derived lower bounds

Suppose that $2 \leq k \leq m$ and that $n \in \mathbb{N}$. There are $\binom{m}{k}$ distinct copies of $K_{k,n}$ in $K_{m,n}$, and in any drawing of $K_{m,n}$, each crossing appears in $\binom{m-2}{k-2}$ distinct copies of $K_{k,n}$. This implies that

$$\text{cr}(K_{m,n}) \geq \frac{\text{cr}(K_{k,n}) \binom{m}{k}}{\binom{m-2}{k-2}} = \frac{\text{cr}(K_{k,n}) \cdot m(m-1)}{k(k-1)}. \tag{3}$$

So any lower bound on q_k gives lower bounds on $\text{cr}(K_{m,n})$ for all $m \geq k$ and all n . Combining (3) with our new lower bounds $\alpha_{10}, \beta_{11}, \beta_{12}, \beta_{13}$ presented in Table 2 gives the following.

Corollary 1 *For all integers n we have*

- for all $m \geq 10$, $\text{cr}(K_{m,n}) \geq 0.0541m(m-1)n^2 - \frac{1}{9}m(m-1)n$,*
- for all $m \geq 11$, $\text{cr}(K_{m,n}) \geq 0.0545m(m-1)n^2 - \frac{5}{44}m(m-1)n$,*
- for all $m \geq 12$, $\text{cr}(K_{m,n}) \geq 0.0549m(m-1)n^2 - \frac{5}{44}m(m-1)n$,*
- for all $m \geq 13$, $\text{cr}(K_{m,n}) \geq 0.0554m(m-1)n^2 - \frac{3}{26}m(m-1)n$.*

Proof By Theorem 2, we have $\text{cr}(K_{k,n}) \geq \frac{1}{2}n^2q_k - \frac{1}{2}n \lfloor \frac{1}{4}(k-1)^2 \rfloor$ for all k, n . We also have $q_k \geq \alpha_k \geq \beta_k$ for all k , hence the inequality holds upon replacing q_k by α_k or β_k . Combining this equation with our computed values $\alpha_{10}, \beta_{11}, \beta_{12}, \beta_{13}$ results in lower bounds on $\text{cr}(K_{10,n}), \text{cr}(K_{11,n}), \text{cr}(K_{12,n})$ and $\text{cr}(K_{13,n})$, respectively. Inserting these lower bounds in equation (3) for $\text{cr}(K_{k,n})$ yields the corollary.

The lower bounds also allow to give statements about limits, using the following lemma.

Lemma 1 (De Klerk et al. [5]) $\lim_{n \rightarrow \infty} \frac{\text{cr}(K_{m,n})}{Z(m,n)} \geq \frac{8q_k}{k(k-1)} \frac{m}{m-1}$ for all $k \leq m$.

Proof First, note that the limit exists: the sequence $(\text{cr}(K_{m,n})/\binom{n}{2})_{n \in \mathbb{N}}$ for fixed m is nondecreasing (by the same calculation as in (3) but now applied to n instead of m) and bounded (using $\text{cr}(K_{m,n}) \leq Z_{m,n}$), hence has a limit. For fixed m , both $Z_{m,n}$ and $\binom{n}{2}$ grow quadratically in n , so the limit $\frac{\text{cr}(K_{m,n})}{Z(m,n)}$ exists too. The lemma now follows from an elementary calculation using the bounds previously given. By Theorem 2, we have $\text{cr}(K_{k,n}) \geq \frac{1}{2}n^2q_k - \frac{1}{2}n \lfloor \frac{1}{4}(k-1)^2 \rfloor$ for all k, n . Now, we use (3) and find, for $m \geq k$:

$$\begin{aligned} \lim_{n \rightarrow \infty} \frac{\text{cr}(K_{m,n})}{Z(m,n)} &\geq \lim_{n \rightarrow \infty} \frac{m(m-1)(\frac{1}{2}n^2q_k - \frac{1}{2}n \lfloor \frac{1}{4}(k-1)^2 \rfloor)}{k(k-1)Z_{m,n}} \\ &= \lim_{n \rightarrow \infty} \frac{m(m-1)(\frac{1}{2}n^2q_k - \frac{1}{2}n \lfloor \frac{1}{4}(k-1)^2 \rfloor)}{k(k-1) \lfloor \frac{1}{4}(m-1)^2 \rfloor \lfloor \frac{1}{4}(n-1)^2 \rfloor} \\ &= \frac{2q_k}{k(k-1) \lfloor \frac{1}{4}(m-1)^2 \rfloor} \geq \frac{8q_k}{k(k-1)} \frac{m}{m-1}. \end{aligned}$$

□

As $q_k \geq \alpha_k \geq \beta_k$, the lemma also holds upon replacing q_k by α_k or β_k . So our computed values $\alpha_{10}, \beta_{11}, \beta_{12}, \beta_{13}$ give asymptotic lower bounds on $\lim_{n \rightarrow \infty} \frac{\text{cr}(K_{m,n})}{Z(m,n)}$ for $m \geq k$. In the following lemma, we provide the lower bound for $m \geq 13$, using our computed value β_{13} . The lower bounds for $m = 10, 11, 12$ are displayed in Table 2.

Corollary 2 For all $m \geq 13$, $\lim_{n \rightarrow \infty} \frac{\text{cr}(K_{m,n})}{Z(m,n)} \geq 0.8878 \frac{m}{m-1}$.

A direct result of this corollary is

$$\lim_{n \rightarrow \infty} \frac{\text{cr}(K_{n,n})}{Z(n,n)} \geq 0.8878. \tag{4}$$

The previously best known published lower bound on $\lim_{n \rightarrow \infty} \frac{\text{cr}(K_{n,n})}{Z(n,n)}$ is 0.8594 (which follows using α_9), cf. De Klerk et al. [6]. Norin and Zwols obtained a lower bound of 0.905 using flag algebras which they presented at a workshop [20]. This bound is stronger than our bound in (4) but however remains unpublished. In [1], Balogh, Lidický and Salazar prove very strong asymptotic lower bounds on the crossing number of the complete graph using flag algebras. It might be possible to improve upon (4) and Norin and Zwols’ bound by using a similar approach considering high levels in the flag algebra hierarchy.

However, in order to prove asymptotic bounds it is also worthwhile to further investigate the quadratic programming hierarchy from De Klerk et al. [5] which we consider in this paper. One might hope to prove lower bounds t_k on α_k such that $8t_k/(k(k-1)) \rightarrow 1$ as $k \rightarrow \infty$, thereby proving $\lim_{n \rightarrow \infty} \frac{\text{cr}(K_{n,n})}{Z(n,n)} = 1$, i.e., asymptotically proving Zarankiewicz’ conjecture. Figure 2 gives rise to the question whether $8\beta_k/(k(k-1)) \rightarrow 1$ as $k \rightarrow \infty$.

In Fig. 2, the increases are larger for odd k than for even k , a trend which was already noted in [6]. We now see that this trend continues for some larger k . As noted in [6], this is reminiscent of the fact that Zarankiewicz’s conjecture holds for $K_{2m,n}$ if it holds for $K_{2m-1,n}$.

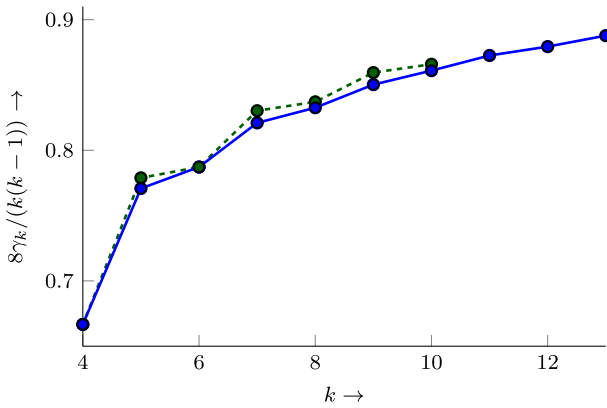


Fig. 2 We have the lower bound $\lim_{n \rightarrow \infty} \text{cr}(K_{m,n})/Z(m,n) \geq (8\gamma_k/(k(k-1)))m/(m-1)$ for each $m \geq k$ and $\gamma_k \in \{\alpha_k, \beta_k\}$. The values $8\alpha_k/(k(k-1))$ are plotted in green (connected by the green dashed line) and the values $8\beta_k/(k(k-1))$ are plotted in blue (colour figure online).

3 Exploiting the symmetry of the problem

Recall that Z_m is the set of permutations of $[m]$ consisting of a single orbit, i.e., Z_m is the set of all m -cycles from S_m and $|Z_m| = (m-1)!$. The group $G_m := S_m \times \{\pm 1\}$ acts on Z_m via

$$(\pi, \varepsilon) \cdot \sigma = \pi \sigma^\varepsilon \pi^{-1},$$

for $\sigma \in Z_m$, $(\pi, \varepsilon) \in G_m = S_m \times \{\pm 1\}$. If X is any optimum solution for the program (2) defining α_m , also $g \cdot X$ with $(g \cdot X)_{\sigma, \tau} = X_{g \cdot \sigma, g \cdot \tau}$ is feasible for all $g \in G_m$: the matrix $g \cdot X$ is obtained from X by simultaneously permuting rows and columns, which preserves positive semidefiniteness, entrywise nonnegativeness and the total sum of the entries. Moreover, the objective values corresponding to X and $g \cdot X$ are the same: Indeed, as $g \cdot Q = Q$ for all $g \in G_m$, one has $\langle Q, X \rangle = \langle g \cdot Q, g \cdot X \rangle = \langle Q, g \cdot X \rangle$. As G_m is a finite group and the feasible region in (2) is convex, we can replace any optimum solution X by the group average $(1/|G_m|) \sum_{g \in G_m} g \cdot X$ to obtain a G_m -invariant optimum solution. So we may assume our optimum solution is G_m -invariant, i.e., its entries are constant on G_m -orbits of $Z_m \times Z_m$. Hence the number of variables is the cardinality of $\Omega_m := (Z_m \times Z_m)/G_m$ (where G_m acts on both copies of Z_m simultaneously). The set Ω_m is also known as the set of *orbitals* of G_m acting on Z_m , and $|\Omega_m|$ as the rank of the action of G_m , see, e.g., [4]. The number of variables can be reduced further since X is symmetric, so the value of X on the orbit of (σ, τ) is the same as the value of X on the orbit of (τ, σ) . We write Ω'_m to be the collection of these ‘symmetric’ G_m -orbits on $Z_m \times Z_m$, in which orbits of (σ, τ) and (τ, σ) are identified. This gives a significant reduction in the number of variables which was already used in [5].

It is also possible to reduce the size of the matrix X in the semidefinite programming formulation. In [6], the regular $*$ -representation was used, which reduced checking

whether a G_m -invariant matrix X is positive semidefinite into checking whether a matrix of order $|\Omega_m| \times |\Omega_m|$ is positive semidefinite. In this paper, we will reduce the matrix X further, by developing a full *block-diagonalization*. For any finite group G acting on a vector space V , we write V^G for the subspace of V of G -invariant elements. The block-diagonalization is a bijective linear map

$$\Phi : \left(\mathbb{C}^{Z_m \times Z_m}\right)^{G_m} \rightarrow \bigoplus_{i=1}^k \mathbb{C}^{m_i \times m_i}, \tag{5}$$

for some integer k and integers m_i for $i \in [k]$, such that $X \in \left(\mathbb{C}^{Z_m \times Z_m}\right)^{G_m}$ is positive semidefinite if and only if $\Phi(X)$ is positive semidefinite. It has the property that $\sum_{i=1}^k m_i^2 = |(Z_m \times Z_m)/G_m| = |\Omega_m|$, which is considerably smaller than $|Z_m|^2$.

3.1 Preliminaries on representation theory

We here describe the preliminaries on representation theory which we will use throughout the paper, based on a combination of the notation and definitions used in references [3, 8, 18, 22]. If G is a finite group acting on a complex vector space V of finite dimension, V is called a G -module. Any G -invariant subspace of V is called a *submodule*. If V and W are G -modules, a G -homomorphism is a linear map $\psi : V \rightarrow W$ with $g \cdot \psi(v) = \psi(g \cdot v)$ for all $g \in G$ and $v \in V$. The modules V and W are *equivalent* (or G -isomorphic) if there is a bijective G -homomorphism (called a G -isomorphism) from V to W . A G -module V is *irreducible* if $V \neq 0$ and its only nonzero submodule is V . The *centralizer algebra* of the action of G on V , denoted by $\text{End}_G(V)$, is the algebra of G -homomorphisms $V \rightarrow V$.

Let again G be a finite group acting on a complex finite dimensional vector space V . Then one can decompose $V = \bigoplus_{i=1}^k \bigoplus_{j=1}^{m_i} V_{i,j}$, for some unique number k and numbers m_1, \dots, m_k (which are unique up to permutation), such that the $V_{i,j}$ are irreducible submodules of V with the property that $V_{i,j}$ is isomorphic to $V_{i',j'}$ if and only if $i = i'$.

Definition 1 (Representative set) For each $i \leq k$ and $j \leq m_i$ let $u_{i,j} \in V_{i,j}$ be a nonzero vector, such that for each $i \leq k$ and $j, j' \leq m_i$ there exists a G -isomorphism from $V_{i,j}$ to $V_{i,j'}$ which maps $u_{i,j}$ to $u_{i,j'}$. Define, for each $i \leq k$, the tuple $U_i := (u_{i,1}, \dots, u_{i,m_i})$. Call any set $\{U_1, \dots, U_k\}$ obtained in this way a *representative set* for the action of G on V .

We can view the U_i as matrices by seeing the vectors $u_{i,j}$ (for $j = 1, \dots, m_i$) as its columns, and we will do so depending on the context.

The space V has a G -invariant inner product $\langle \cdot, \cdot \rangle$. Let $\{U_1, \dots, U_k\}$ be any representative set for the action of G on V , and define the map $\Phi : \text{End}_G(V) \rightarrow \bigoplus_{i=1}^k \mathbb{C}^{m_i \times m_i}$ which maps $A \mapsto \bigoplus_{i=1}^k (\langle Au_{i,j'}, u_{i,j} \rangle)_{j,j'=1}^{m_i}$. This map is linear and bijective, and it has the property that $A \geq 0$ if and only if $\Phi(A) \geq 0$. This follows from classical representation theory. For a proof, see e.g., [21, Proposition 2.4.4]. We apply it to the

following. Suppose that G is a finite group acting on a finite set Z , hence on the vector space $V := \mathbb{C}^Z$. Then $\text{End}_G(V)$ can be naturally identified with $(\mathbb{C}^{Z \times Z})^G$, and the map Φ becomes

$$\Phi: (\mathbb{C}^{Z \times Z})^G \rightarrow \bigoplus_{i=1}^k \mathbb{C}^{m_i \times m_i} \quad \text{with} \quad A \mapsto \bigoplus_{i=1}^k U_i^* A U_i. \tag{6}$$

It will turn out that all representative sets in this paper consist of real matrices. So we can replace \mathbb{C} by \mathbb{R} in the above equation: Φ is a linear bijective map $(\mathbb{R}^{Z \times Z})^G \rightarrow \bigoplus_{i=1}^k \mathbb{R}^{m_i \times m_i}$ such that $A \geq 0$ if and only if $\Phi(A) \geq 0$ for all $A \in (\mathbb{R}^{Z \times Z})^G$.

Representation theory of the symmetric group. A partition λ of n is a sequence of integers $\lambda_1 \geq \dots \geq \lambda_h > 0$ with $\lambda_1 + \dots + \lambda_h = n$ for some $h \in \mathbb{N}$ which is called the *height* of λ . We write $\lambda \vdash n$ to denote that λ is a partition of n . The (*Young*) *shape* of $\lambda \vdash n$ is an array consisting of n boxes divided into h rows where for each $1 \leq i \leq h$, the i -th row contains λ_i boxes. As an example, consider the shape corresponding to $(4, 1, 1) \vdash 6$:



A *Young tableau* of shape λ is a filling τ of the boxes of the Young shape λ with the integers $1, \dots, n$, where each number appears once. Two Young tableaux t, t' of shape $\lambda \vdash n$ are (*row*) *equivalent*, written as $t \sim t'$ if corresponding rows of the two tableaux contain the same elements. A *tabloid* of shape λ is an equivalence class of tableaux: $\{t\} = \{t' : t' \sim t\}$. We denote a tabloid by an array with lines between the rows, e.g.,

$$\left\{ \begin{array}{|c|c|} \hline 1 & 3 \\ \hline 2 & \\ \hline \end{array}, \begin{array}{|c|c|} \hline 3 & 1 \\ \hline 2 & \\ \hline \end{array} \right\} = \frac{1 \ 3}{2}.$$

Any permutation $\pi \in S_n$ acts on a tableau $t = t_{i,j}$ by acting on its content, i.e., $\pi t = (\pi(t_{i,j}))$. The *column stabilizer* C_t of a tableau τ is the subgroup of S_n which leaves the columns of t invariant. The action of $\pi \in S_n$ on a tableau t extends to a well-defined action on tabloids via $\pi\{t\} = \{\pi t\}$. For each $\lambda \vdash n$ the *permutation module* M^λ corresponding to λ is defined as

$$M^\lambda = \mathbb{C}\{\{t_1\}, \dots, \{t_k\}\},$$

where $\{t_1\}, \dots, \{t_k\}$ is a complete set of λ -tabloids. For any tableau t , we the associated *polytabloid* is $e_t := \sum_{c \in C_t} \text{sgn}(c)c\{t\}$. The *Specht module* S^λ corresponding to λ is the submodule of M^λ spanned by the polytabloids e_t , where t is a tableau of shape λ . The module S^λ is irreducible, and it is generated by any given polytabloid: $S^\lambda = \mathbb{C}S_n \cdot e_t$ for any fixed λ -tableau t .

A *generalized Young tableau* of shape $\lambda \vdash n$ is a (Young) shape filled with integers, where we allow repeated entries. Depending on the context, we often omit the word

‘generalized’. A generalized Young tableau is *standard* if its rows and columns are strictly increasing, and *semistandard* if its rows are nondecreasing and its columns are strictly increasing. We say that a generalized tableau of shape $\lambda \vdash n$ has *content* $\mu = (\mu_1, \dots, \mu_h) \vdash n$ if it contains μ_i times the integer i , for all $1 \leq i \leq h$. If T is any tableau of shape λ and content μ , the map

$$\vartheta_T : M^\lambda \rightarrow M^\mu, \quad \{t\} \mapsto \sum_{T' \sim T} t[T'] \quad (\text{extended linearly to } M^\lambda),$$

where $\{t\}$ is any tabloid in M^λ , and where

$$t[T'] := \{\text{tableau with entry } t_{i,j} \text{ in its } T'_{i,j} \text{-th row}\},$$

is an S_n -homomorphism. Moreover, a basis of $\text{Hom}(S^\lambda, M^\mu)$ is given by (cf. Sagan [22])

$$\{\vartheta_T \mid T \text{ semistandard of shape } \lambda \text{ and content } \mu\}.$$

Unless specified otherwise, we from now on assume that t is the λ -tableau containing the integers $1, \dots, n$ in this order from left to right, from top to bottom. Sometimes we write t_λ instead of t . It follows that a representative set for the action of S_n on M^μ is given by

$$\{(\vartheta_T(e_{t_\lambda}) \mid T \text{ semistandard of shape } \lambda \text{ and content } \mu) \mid \lambda \vdash n\}. \tag{7}$$

Induced representations. Let G be a finite group, and H a subgroup of G . Let $R = \{r_1, \dots, r_t\}$ be a full set of representatives for the left cosets of H in G , so $|R| = [G : H]$. If V is an H -module, the *induced* module $\text{Ind}_H^G(V)$ is defined as follows. The elements of $\text{Ind}_H^G(V)$ are (formal) sums of the form

$$\lambda_1(r_1, v_1) + \dots + \lambda_t(r_t, v_t) \quad \text{for } v_1, \dots, v_t \in V, \lambda_1, \dots, \lambda_t \in \mathbb{C}.$$

(So as vector space $\text{Ind}_H^G(V) = \bigoplus_{r \in R} rV$.) The action of an element $g \in G$ on (r_i, v) is defined via $g \cdot (r_i, v) = (r_j, h \cdot v)$, where $r_j \in R$ and $h \in H$ are uniquely determined by the equation $gr_i = r_jh$.

3.2 The block-diagonalization for computing α_k

We aim to decompose the space \mathbb{C}^{Z^m} as a G_m -module. The derivation will consist of three steps.

1. Derive a representative set of matrices for the action of S_m on $M^{(1^m)}$ from the elementary representation theory of the symmetric group.

2. There is a natural surjective G -homomorphism $f : M^{(1^m)} \rightarrow \mathbb{C}^{Z_m}$. For each matrix in the representative set for the action of S_m on $M^{(1^m)}$, construct a new matrix consisting of a minimal linearly independent set of columns of the original matrix after applying the map f . The new matrices together form a representative set for the action of S_m on \mathbb{C}^{Z_m} , as we will show.

In general: suppose G is a finite group acting on finite dimensional vector spaces V and W , and $f : V \rightarrow W$ is a surjective G -homomorphism. We show how to derive a representative set for the action of G on W from a representative set for the action of G on V .

3. Use the additional $S_2 \cong \{\pm 1\}$ -action to finally obtain a representative set for the action of $S_m \times S_2$ on \mathbb{C}^{Z_m} .

In general: suppose that H is a finite group acting on a complex finite dimensional vector space V , and that also S_2 acts on V . We show how to derive a representative set for the action of $H \times S_2$ on V from a representative set for the action of H on V , provided that the H - and S_2 -actions on V commute.

So we first consider the action of the subgroup $S_m \cong S_m \times \{+1\} < S_m \times \{\pm 1\}$ acting on Z_m by conjugation, and give an algorithm to determine a representative set for this action. Afterwards, we consider the additional $S_2 \cong \{\pm 1\}$ -action to reduce the representative set further.

3.2.1 The S_m -action on Z_m

The starting point to find a representative set for the action of S_m on \mathbb{C}^{Z_m} is a representative set for the action of S_m on $M^{(1^m)}$ given in (7). We consider the natural projection

$$f : M^{(1^m)} \rightarrow \mathbb{C}^{Z_m}, \tag{8}$$

mapping a tabloid which is filled row-wise with i_1 up to i_m to the indicator vector in \mathbb{C}^{Z_m} corresponding to $(i_1 i_2 \dots i_m)$.

The map f is linear and surjective, and it respects the S_m -action, as for each $\pi \in S_m$ we have

$$f \left(\pi \cdot \begin{pmatrix} \overline{i_1} \\ \overline{i_2} \\ \vdots \\ \overline{i_m} \end{pmatrix} \right) = f \left(\begin{pmatrix} \overline{\pi(i_1)} \\ \overline{\pi(i_2)} \\ \vdots \\ \overline{\pi(i_m)} \end{pmatrix} \right) = (\pi(i_1) \dots \pi(i_m)) = \pi(i_1 \dots i_m)\pi^{-1} = \pi f \left(\begin{pmatrix} \overline{i_1} \\ \overline{i_2} \\ \vdots \\ \overline{i_m} \end{pmatrix} \right) \pi^{-1}.$$

We now use the following fact (which follows from elementary representation theory, see, e.g., [14, 25]) to derive a representative set for the action of S_m on \mathbb{C}^{Z_m} .

Proposition 1 *Suppose that a finite group G acts on two finite-dimensional complex vector spaces V and W , and suppose that $f : V \rightarrow W$ is a surjective G -homomorphism. Let $\{U_1, \dots, U_k\}$ be a representative set for the action of G on V , with $U_i = (u_{i,j} \mid j = 1, \dots, m_i)$. Then the set $\{U'_1, \dots, U'_k\}$ is representative for the*

action of G on W , where U'_i (for $i \in [k]$) is a tuple consisting of a minimal spanning set among the $f(u_{i,j})$, with $j = 1, \dots, m_i$.

Proof For each $i \in [k]$, let $s_i \in \mathbb{N}$ and $\ell_1^{(i)}, \dots, \ell_{s_i}^{(i)} \in [m_i]$ be such that

$$U'_i = (f(u_{i,\ell_1^{(i)}}), \dots, f(u_{i,\ell_{s_i}^{(i)}}))$$

is the chosen tuple consisting of a minimal spanning set among the $f(u_{i,j})$ for $j = 1, \dots, m_i$. Define

$$V' := \bigoplus_{i=1}^k \bigoplus_{j=1}^{s_i} \mathbb{C}G u_{i,\ell_j^{(i)}} \subseteq V,$$

i.e., V' is the restriction of the direct sum decomposition of V to the components corresponding to the chosen minimal spanning sets.

The restriction $f' : V' \rightarrow W$ of f to V' is a bijection. Surjectivity of f' is clear, as the image of f is W and is spanned by the $f(u_{i,\ell_j^{(i)}})$ ($i \in [k], j \in [s_i]$). If f' is not injective, then $\text{Ker}(f')$ contains an irreducible submodule M of V' . Schur's lemma implies that the projection of M onto the components $\bigoplus_{j=1}^{s_i} \mathbb{C}G u_{i,\ell_j^{(i)}}$ is zero for all but one $i \in [k]$. Any nonzero element of M now gives rise to a nontrivial linear combination of the $u_{i,\ell_j^{(i)}}$ that is in the kernel of f (for the i for which the projection of M onto $\bigoplus_{j=1}^{s_i} \mathbb{C}G u_{i,\ell_j^{(i)}}$ is nonzero) contradicting the fact that the $f(u_{i,\ell_j^{(i)}})$ ($j = 1, \dots, s_i$) are linearly independent. So f' is indeed a bijection.

Since by definition the set $\{(u_{i,\ell_j^{(i)}} \mid j = 1, \dots, s_i) \mid i = 1, \dots, k\}$ is representative for the action of G on V' , the set

$$\{U'_1, \dots, U'_m\} = \left\{ \left(f' \left(u_{i,\ell_j^{(i)}} \right) \mid j = 1, \dots, s_i \right) \mid i = 1, \dots, k \right\}$$

is representative for the action of G on W , as was needed to prove. □

Recall that a representative set for the action of S_m on $M^{(1^m)}$ is given by

$$\{\vartheta_T(e_t) \mid T \text{ semistandard of shape } \lambda \text{ and content } (1^m)\}.$$

Note that any semistandard tableaux of shape $\lambda \vdash m$ and content (1^m) is standard. Consider for each $\lambda \vdash n$ a tuple U_λ consisting of a minimal spanning set among the vectors

$$\{f(\vartheta_T(e_t)) \mid T \text{ standard of shape } \lambda \text{ and content } (1^m)\} \subseteq \mathbb{C}Z^m. \tag{9}$$

Corollary 3 *The set $\{U_\lambda \mid \lambda \vdash n\}$ is representative for the action of S_m on \mathbb{C}^{Z_m} .*

Proof Apply Proposition 1 with $V = M^{(1^m)}$, $W = \mathbb{C}^{Z_m}$, and f from (8). □

We note that it is useful to maintain for each λ a list of the Young tableaux which give rise to the minimal spanning set among the vectors in (9). They can help to compute the coefficients in the block-diagonalizations more efficiently (but still exponential in m), see Sect. 5.2.

Remark 1 Proposition 1 has a wide potential for application. For instance, for computing bounds on the cardinality of error-correcting codes, a block-diagonalization for matrices indexed by ordered k -tuples of codewords can be obtained using existing tools [11, 21]. With Proposition 1, one may further reduce this into a block-diagonalization for matrices indexed by *unordered* sets of codewords of size $\leq k$.

Discussion about finding the minimal spanning set faster. It is also natural to identify \mathbb{C}^{Z_m} with $M^{(1^m)}/(\mathbb{Z}/m\mathbb{Z})$, where $\mathbb{Z}/m\mathbb{Z}$ permutes the rows of a tabloid in $M^{(1^m)}$ cyclically. Brosch [3] developed a fast method in the context of flag algebras to decompose any module M^μ/F , where F is a group acting on the rows of μ via permutations. However, the computational results presented in this paper can be obtained without this speed-up: we can compute the representative set for α_k for $k \leq 10$ using the method from Proposition 1, and the representative set for our new relaxation β_k is described explicitly in Sect. 4.

The method of Brosch [3] allows to avoid working with the vectors $\vartheta_T(e_t)$ explicitly, which is desirable given the high dimension of $M^{(1^m)}$. The key observation is

$$\text{Hom}(S^\lambda, M^{(1^m)}/(\mathbb{Z}/m\mathbb{Z})) = \mathcal{R}_{\mathbb{Z}/m\mathbb{Z}}(\text{Hom}(S^\lambda, M^{(1^m)})),$$

by identifying the quotient $M^{(1^m)}/(\mathbb{Z}/m\mathbb{Z})$ with the elements v in $M^{(1^m)}$ with $\sigma(v) = v$ for all $\sigma \in \mathbb{Z}/m\mathbb{Z}$. Here $\mathcal{R}_{\mathbb{Z}/m\mathbb{Z}}$ denotes the *Reynolds operator* of $\mathbb{Z}/m\mathbb{Z}$ on $\text{Hom}(S^\lambda, M^{(1^m)})$, which averages over the group

$$\mathcal{R}_{\mathbb{Z}/m\mathbb{Z}}(\vartheta_T) := \frac{1}{m} \sum_{\sigma \in \mathbb{Z}/m\mathbb{Z}} \sigma(\vartheta_T).$$

The action of $\mathbb{Z}/m\mathbb{Z}$ on homomorphisms ϑ_T is given by $\sigma(\vartheta_T) = \vartheta_{\sigma(T)}$, where σ is applied to T entrywise. The method of [3] results in a matrix representation of $\mathcal{R}_{\mathbb{Z}/m\mathbb{Z}}$ in the semistandard basis, so that one can choose the homomorphisms corresponding to a spanning set of rows to find a basis of $\text{Hom}(S^\lambda, M^{(1^m)}/(\mathbb{Z}/m\mathbb{Z}))$. The advantage is that one works in a space of dimension $\dim(\text{Hom}(S^\lambda, M^{(1^m)}))$ instead of $\dim(M^{(1^m)}) = m!$.

As mentioned before, knowing the description of the columns $\vartheta_T(e_t)$ of the representative set in terms of tableaux is useful for the computations, see Sect. 5.2.

The multiplicities of the irreducible representations. It can be shown that the module \mathbb{C}^{Z_m} is S_m -isomorphic to a module which has been described in the literature. This

allows us to immediately obtain the multiplicities of the irreducible representations of \mathbb{C}^{Z_m} as an S_m -module.

Proposition 2 *As S_m -modules, we have $\mathbb{C}^{Z_m} \cong \text{Ind}_{\mathbb{Z}/m\mathbb{Z}}^{S_m} 1$.*

Proof Define the map $\phi : \mathbb{C}^{Z_m} \rightarrow \text{Ind}_{\mathbb{Z}/m\mathbb{Z}}^{S_m} 1$ by mapping the standard basis vector e_σ corresponding to $\sigma = (\sigma_1 \sigma_2 \dots \sigma_m) \in Z_m$ with $\sigma_1 = 1$ to the basis element $(r, 1)$ in $\text{Ind}_{\mathbb{Z}/m\mathbb{Z}}^{S_m} 1$, where r is the permutation which maps i to σ_i for each $i \in [m]$. Then

$$\phi(\pi \cdot e_\sigma) = \phi(e_{\pi\sigma\pi^{-1}}) = \phi(e_{(\pi\sigma_1 \pi\sigma_2 \dots \pi\sigma_m)}) = (\overline{\pi r}, 1) = \pi \cdot \phi(e_\sigma), \tag{10}$$

for each $\pi \in S_m$, where $\overline{\pi r}$ is the representative of the class of the permutation πr with $\overline{\pi r}(1) = 1$. So ϕ respects the S_m -action. As ϕ is also a bijection between the bases of \mathbb{C}^{Z_m} and $\text{Ind}_{\mathbb{Z}/m\mathbb{Z}}^{S_m} 1$, its linear extension is an S_m -isomorphism. \square

It is known [16] that

$$\text{Ind}_{\mathbb{Z}/m\mathbb{Z}}^{S_m} 1 \cong \bigoplus_{\lambda \vdash m} a_\lambda S^\lambda, \tag{11}$$

where a_λ is the number of standard tableaux T of shape λ with $c(T) = 0 \pmod m$, where

$$c(T) \text{ is the sum of all } a \text{ in } T \text{ for which } a + 1 \text{ appears in a row strictly below } a \text{'s row.} \tag{12}$$

So it is not hard to determine the multiplicities of the irreducible representations of \mathbb{C}^{Z_m} as S_m -module. We however need the decomposition explicitly, to obtain an explicit representative set.

3.2.2 The $S_2 \cong \{\pm 1\}$ -action on Z_m

The S_m -action and the $S_2 \cong \{\pm 1\}$ -action on \mathbb{C}^{Z_m} commute. This enables us to compute a representative set for the action of $S_m \times S_2$ on \mathbb{C}^{Z_m} , starting with a given representative set for the action of S_m on Z_m . We first state the setting in a general form, and then prove a proposition which allows us to derive the full symmetry reduction.

3.2.3 Representative set of $H \times S_2$ -action

Let H be a finite group acting on a finite-dimensional complex vector space V and suppose a representative set $\{U_1, \dots, U_k\}$ where $U_i = (u_{i,1}, \dots, u_{i,m_i})$ (for $i \leq k$) for the action of H on V is given. Suppose that also $S_2 = \{1, \eta\}$ acts on V , and that the actions of H and S_2 on V commute. Let $L_\pm := \{x \mid x = \pm \eta x\}$, so that L_+ and L_- are the eigenspaces of η . We show to obtain a representative set for the action of $H \times S_2$ on V , generalizing [12, Section 3.4] (which considers S_2 -actions on a finite set Z).

Proposition 3 *A representative set for the action of $H \times S_2$ on V is the set $\{U_1^+, U_1^-, \dots, U_k^+, U_k^-\}$, where U_i^+ is a tuple consisting of a linearly independent subset among the vectors $u_{i,j}^+ := u_{i,j} + \eta \cdot u_{i,j}$ (for $j = 1, \dots, m_i$), and U_i^- is a tuple consisting of a linearly independent subset among the vectors $u_{i,j}^- := u_{i,j} - \eta \cdot u_{i,j}$ (for $j = 1, \dots, m_i$).*

Proof Since the actions of H and S_2 on V commute, both L_+ and L_- are $H \times S_2$ -invariant subspaces of V . The maps $f^+ : V \rightarrow L_+$ and $f^- : V \rightarrow L_-$ given by $f^+(v) = (I + \eta)v$ and $f^-(v) = (I - \eta)v$ are surjective $H \times S_2$ -homomorphisms. From Proposition 1 it now follows that $\{U_1^+, \dots, U_k^+\}$ and $\{U_1^-, \dots, U_k^-\}$ are representative sets for the actions of $H \times S_2$ on L_+ and L_- , respectively.

Note that $V = L_+ \oplus L_-$. Also, if $W_1 \subseteq L_+$ and $W_2 \subseteq L_-$, are irreducible $H \times S_2$ -modules, then they are non-isomorphic: indeed, if $\psi : W_1 \rightarrow W_2$ were an $H \times S_2$ -isomorphism, then for each $x \in W_1$ we have $\psi(x) = \psi(\eta x) = \eta\psi(x)$, as $x \in L_+$, but also $\psi(x) = -\eta\psi(x)$, as $\psi(x) \in L_-$, so $\psi(x) = 0$. So the union $\{U_1^+, \dots, U_k^+\} \cup \{U_1^-, \dots, U_k^-\}$ of representative sets for the actions of $H \times S_2$ on L_+ and L_- is a representative set for the action of $H \times S_2$ on V . \square

For our semidefinite program this means that, in the block-diagonalization for the action of S_m on \mathbb{C}^{Z_m} , the block corresponding to the matrix U_λ will split into two blocks in the block-diagonalization for the action of $S_m \times S_2$ on \mathbb{C}^{Z_m} : one corresponding to U_λ^+ and one corresponding to U_λ^- .

4 The relaxation β_m

When computing α_m , we use the symmetry reduction from the previous section and require that all blocks in the block-diagonalization of X are positive semidefinite. As α_m is a minimization problem, only requiring one block to be positive semidefinite will yield a lower bound on α_m . From our computer experiments it follows that one small block seems ‘special’: only requiring this block to be positive semidefinite yields a remarkably good lower bound on α_m . It is the block corresponding to U_λ^- , where $\lambda = (m - 2, 1, 1) \vdash m$. This observation gives rise to a new relaxation β_m of α_m , in which we only require the mentioned block to be positive semidefinite. The primal of the program β_m is

$$\beta_m = \min \left\{ \langle Q, X \rangle \mid X \in \mathbb{R}_{\geq 0}^{Z_m \times Z_m}, \langle J, X \rangle = 1, (U_\lambda^-)^T X U_\lambda^- \geq 0 \right\}, \tag{13}$$

where $\lambda = (m - 2, 1, 1)$. It turns out that we can explicitly describe the columns of the matrix U_λ^- using Young tableaux. We first describe the matrix U_λ . Define the tableau

$$M_i := \begin{array}{|c|c|c|c|c|} \hline & & \cdot & & \\ \hline 2 & & & & \\ \hline i & & & & \\ \hline \end{array}, \quad \text{for } i \in \{3, \dots, m\}.$$

Proposition 4 *The matrix U_λ can be taken to consist of the columns $f(\vartheta_{M_i}(e_i))$ for $i = 3, \dots, \lfloor \frac{m+1}{2} \rfloor + 1$.*

5 Computation

In this section, we comment on the computation. First we explain how we compute the entries of Q , taking into account its symmetries. After that, we describe how to compute the entries in the block-diagonalizations more efficiently. Then we give the dual semidefinite program of β_m , which has nice features: a small matrix block which is required to be positive semidefinite, and few variables. However, it has $|\Omega'_m|$ linear constraints, which is a very large number.¹ In the final section we explain how we computed β_m using this dual description in practice.

5.1 Computing the matrix Q with Dijkstra’s algorithm

To compute the entries of the matrix Q , we follow Woodall [27]. Construct a graph Γ_m with vertex set Z_m , and $\{\sigma, \gamma\}$ is an edge if γ can be obtained from σ by one transposition of adjacent elements of σ . Then the entry $Q_{\sigma,\tau}$ is equal to the length of a shortest path from σ to τ^{-1} in Γ_m , which can be computed with Dijkstra’s shortest path algorithm. We only apply Dijkstra with the source node $\sigma = (12\dots m)$, as we only want the value of $Q_{\sigma,\tau}$ on G_m -orbits of $Z_m \times Z_m$.

A speed-up inside Dijkstra algorithm which takes into account symmetry is based on the observation that $\sigma = (12\dots m)$ is fixed by the elements $(\sigma, 1)$ and $(\rho, -1)$ of G_m , where ρ is such that $\rho\sigma^{-1}\rho^{-1} = \sigma$. So the subgroup H_m of G_m generated by these two elements fixes σ , and hence has the property that $Q_{\sigma,h\cdot\tau} = Q_{h\cdot\sigma,h\cdot\tau} = Q_{\sigma,\tau}$ for any $h \in H_m$ and $\tau \in Z_m$. We represent each H_m -orbit of Z_m by its lexicographically smallest element. We maintain a priority queue S of elements with their distances, and a set L of visited orbit representatives of Z_m under H_m , and a distance $d := 0$. The priority queue S initially consists of $(12\dots m)$ with distance 0, and L consists of $\sigma = (12\dots m)$.

As long as there are orbits in S , we pop the element τ from S with the smallest distance, increase d by 1, and check all cycles in Z_m reachable from τ with one swap of adjacent elements in τ . These cycles are replaced with the unique representatives of their orbits, and the new orbit representatives are added to L , as well as to the queue S with distance d . This is repeated until S is empty.

5.2 Computing the inner products

Let $\lambda \vdash m$ and $u_{T_1} = f(\vartheta_{T_1}(e_{\lambda}))$, $u_{T_2} = f(\vartheta_{T_2}(e_{\lambda}))$ be columns of U_λ . Let $X \in (\mathbb{C}^{Z_m \times Z_m})^{G_m}$. The inner products are of the form

$$((1 + \eta) \cdot u_{T_1})^\top X ((1 + \eta) \cdot u_{T_2}) \quad \text{or} \quad ((1 - \eta) \cdot u_{T_1})^\top X ((1 - \eta) \cdot u_{T_2}).$$

By symmetry one has $(\eta \cdot u_{T_1})^\top X (\eta \cdot u_{T_2}) = u_{T_1}^\top X u_{T_2}$ and $(\eta \cdot u_{T_1})^\top X u_{T_2} = u_{T_1}^\top X (\eta \cdot u_{T_2})$. So to compute the inner products, we must compute expressions of the form

¹ Recall that $\Omega_m := (Z_m \times Z_m)/G_m$ is the collection of nonempty G_m -orbits of $Z_m \times Z_m$, and Ω'_m is the collection of nonempty G_m -orbits on $Z_m \times Z_m$ in which additionally orbits of $(\sigma, \tau) \in Z_m \times Z_m$ and (τ, σ) are identified.

$u_{T_1}^\top Xu_{T_2}$ and $(\eta \cdot u_{T_1})^\top Xu_{T_2}$. Note that

$$u_{T_1}^\top Xu_{T_2} = \sum_{T'_1 \sim T_1, T'_2 \sim T_2} \sum_{c, c' \in C_t} \text{sgn}(cc') x_{\omega(f(t[cT'_1]), f(t[c'T'_2]))}, \tag{15}$$

where f from (8) maps a tabloid to the corresponding m -cycle in Z_m , and $\omega(\sigma, \tau) \in \Omega'_m$ denotes the orbit of $(\sigma, \tau) \in Z_m \times Z_m$. If we have (15), then one can also obtain $(\eta \cdot u_{T_1})^\top Xu_{T_2}$ from it by replacing each variable $x_{\omega(f(t[cT'_1]), f(t[c'T'_2]))}$ by $x_{\omega(\eta \cdot f(t[cT'_1]), f(t[c'T'_2]))}$. So we now focus on computing (15). One can compute the inner products by using (15) (and we succeeded to compute α_{10} in that way). We now describe a method which is faster in practice and which we used in our implementation. Since $|\Omega'_m|$ is exponential in m , one cannot hope for a running time polynomial in m . Let $Y(\lambda)$ be the set of (row,column)-coordinates indicating the boxes of λ . Define the polynomial

$$p_{T_1, T_2}(Z) := \sum_{T'_1 \sim T_1, T'_2 \sim T_2} \sum_{c, c' \in C_t} \text{sign}(cc') \prod_{y \in Y(\lambda)} z_{cT'_1(y), c'T'_2(y)}, \tag{16}$$

for $Z = (z_{j,h})_{j,h=1}^m \in \mathbb{R}^{m \times m}$. One can express p_{T_1, T_2} as a linear combination of monomials with the algorithms of [11] or [18]. This allows to compute the inner product fast in many instances for error-correcting codes (see e.g., [11, 21]). The method was generalized to be applicable to arbitrary permutation modules in the setting of flag algebras (cf. [3]).

There is a one-to-one correspondence between S_m -orbits of pairs of tabloids $(t[cT_1], t[c'T_2])$ and monomials $\prod_{y \in Y(\lambda)} z_{cT'_1(y), c'T'_2(y)}$ via their *overlap*, i.e., the numbers of elements of each row of the first tabloid which appear in each row of the second. The overlap of two tabloids $\{t_1\}$ and $\{t_2\}$ can be described by a monomial $\prod_{i,j=1}^m z_{i,j}^{(|\{t_1\}_i \cap \{t_2\}_j|)}$, where m is the number of parts of λ and $\{t\}_i$ denotes the set of elements in the i -th row of a tabloid $\{t\}$. So to compute (15), we can compute (16), and then replace each monomial of degree m in the variables $z_{i,j}$ by the variable $x_{\omega(t[cT_1], t[c'T_2])}$, where $(t[cT_1], t[c'T_2])$ is any element in the S_m -orbit of pairs of tabloids corresponding to the monomial in $z_{i,j}$.

Computing (16). We here state the method from [11], which is easy to implement and uses only methods for addition, multiplication, and differentiation of polynomials. Given two generalized Young tableaux T_1, T_2 , define

$$\begin{aligned} r(s, j) &:= \text{number of } s\text{'s in row } j \text{ of } T_1, & u(s, j) &:= \text{number of } s\text{'s in row } j \text{ of } T_2, \\ d_{s \rightarrow j} &:= \sum_{i=1}^m x_{s,i} \frac{\partial}{\partial x_{j,i}}, \text{ and} & d_{j \rightarrow s}^* &:= \sum_{i=1}^m x_{i,s} \frac{\partial}{\partial x_{i,j}}. \end{aligned}$$

Also, define the polynomial $P_\lambda(Z) := \prod_{k=1}^m \left(k! \det \left((z_{i,j})^k_{i,j=1} \right) \right)^{\lambda_k - \lambda_{k+1}}$ in variables $z_{i,j}$, where $i, j \in [m]$ and $\lambda_{m+1} := 0$. Then it holds [11, Theorem 7] that

$$p_{T_1, T_2}(X) = \left(\prod_{j=1}^{m-1} \prod_{s=j+1}^m \frac{1}{r(s, j)! u(s, j)!} (d_{s \rightarrow j})^{r(s, j)} (d_{j \rightarrow s}^*)^{u(s, j)} \right) \cdot P_\lambda(Z).$$

5.3 The dual semidefinite program

First, note that the dual of the original semidefinite program α_m is

$$\alpha_m = \max \left\{ t \mid Q - tJ - Y \succeq 0, Y \in \mathbb{R}_{\geq 0}^{Z_m \times Z_m} \right\}. \tag{17}$$

To show that this is indeed an equality, one needs to show that strong duality holds. This is indeed the case, as the primal (2) is strictly feasible (set $X = aJ + bI$, where $a = \frac{1}{2((m-1)!)^2}$ and $b = \frac{1}{2(m-1)!}$), while the dual is feasible with $t = 0$ and $Y = Q - \Delta(Q)$, where $\Delta(Q)$ is a matrix which is zero outside the diagonal and which has the same diagonal entries as Q .

We now describe the dual of β_m . The primal of the program β_m is

$$\beta_m = \min \left\{ \langle Q, X \rangle \mid X \in \mathbb{R}_{\geq 0}^{Z_m \times Z_m}, \langle J, X \rangle = 1, U_\lambda^\top X U_\lambda \succeq 0 \right\}, \tag{18}$$

where $\lambda = (m - 2, 1, 1)$. For each $\omega \in \Omega'_m$, let K_ω be the indicator matrix of ω , i.e., the $(Z_m \times Z_m)$ -matrix with $(K_\omega)_{\sigma, \tau} = 1$ if $(\sigma, \tau) \in \omega$ and $(K_\omega)_{\sigma, \tau} = 0$ otherwise. As X is G_m -invariant, we may write $X = \sum_{\omega \in \Omega'_m} K_\omega x_\omega$. We define for each $\omega \in \Omega'_m$ the constant matrix $A_\omega := U_\lambda^\top K_\omega U_\lambda$. Let q_ω denote the common value of $Q_{(\sigma, \tau)}$ for $(\sigma, \tau) \in \omega$. So we may rewrite (18) as

$$\beta_m = \min \left\{ \sum_{\omega \in \Omega'_m} |\omega| x_\omega q_\omega : x_\omega \geq 0 \forall \omega \in \Omega'_m, \sum_{\omega \in \Omega'_m} |\omega| x_\omega = 1, \sum_{\omega \in \Omega'_m} x_\omega A_\omega \succeq 0 \right\}.$$

The dual of this semidefinite program is (again strong duality holds)

$$\beta_m = \max \left\{ t : Y \in \mathbb{R}^{\lfloor \frac{m-1}{2} \rfloor \times \lfloor \frac{m-1}{2} \rfloor}, Y \succeq 0, \forall \omega \in \Omega'_m : \langle Y, A_\omega \rangle + |\omega| t \leq |\omega| q_\omega \right\}. \tag{19}$$

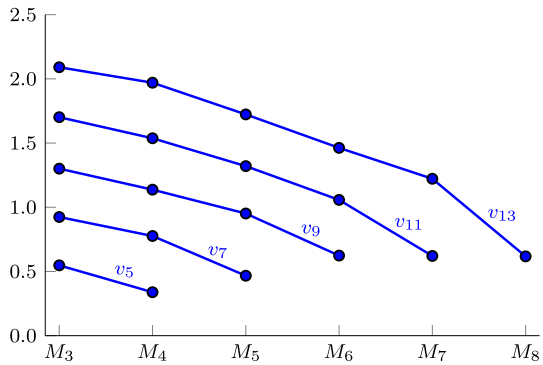
This dual has few variables and only a very small matrix block which is required to be positive semidefinite. The main difficulty is that there are many linear constraints, as can be seen in Table 3.

Remark 2 We observed some structure in the optimal solutions Y of the dual (19) for β_m computationally. Up to $m = 13$, the rank of the optimal Y is one if m is odd, and 2 if m is even (and $m > 4$). Furthermore, the eigenvector of the cases where m is odd

Table 3 The number of variables in our SDP is $|\Omega'_m| = \sum m_i(m_i + 1)/2$, and for the block sizes m_i we have $\sum m_i^2 = |\Omega_m| = |(Z_m \times Z_m)/G_m|$. The block sizes are given in the format (block size) multiplicity

m	$ \Omega_m $	$ \Omega'_m $	block sizes m_i for α_m	$\sum m_i$
4	3	3	1^3	3
5	8	7	$2^1 1^4$	6
6	20	17	$2^3 1^8$	14
7	78	56	$3^6 2^4 1^8$	34
8	380	239	$7^2 5^2 4^9 3^7 2^4 1^9$	98
9	2438	1366	$12^8 11^2 9^6 7^3 6^5 5^2 4^2 3 1 6 1 5$	294
10	18,744	9848	$38^2 34^1 31^1 29^1 28^1 26^3 24^2 22^4 20^5 18^3 16^4 14^6 13^1 12^2 10^4 9^1 8^7 6^8 4^7 3^2 7 1^3$	952
11	166,870	85,058	$105^4 80^2 60^6 56^4 55^2 54^2 50^8 45^6 44^2 40^6 34^2 30^6 29^2 26^2 25^2 24^2 20^6 16^2 15^2 11^4 10^8 6^4 5 1 4 2 1^2$	3246
12	1,670,114	840,906	$327^1 317^1 243^1 241^2 238^1 234^4 199^1 191^1 187^1 177^1 176^1 172^1 169^1 163^1 162^2 155^2 150^1 147^1 146^4 144^1 137^2$ $133^2 132^1 128^1 127^1 121^1 117^3 113^1 110^1 106^1 102^1 98^3 93^2 91^1 90^2 87^4 86^2 84^1 83^1 82^2 81^1 79^1 77^1 75^1 74^1$ $72^4 71^2 68^1 66^1 64^2 59^4 56^2 50^1 49^1 47^2 45^1 44^3 41^2 37^3 36^1 34^1 32^2 29^1 26^1 25^1 24^1 19^2 17^3 16^1 14^5 13^4 12^3 10^1 9^4$ $7^5 6^1 5^3 4^1 3^1 2^5 1^2$	11,698
13	18,446,184	9,244,958		

Fig. 3 The vectors $v_m \in \mathbb{R}^{\lfloor \frac{m-1}{2} \rfloor}$ such that the optimal solution of the dual (19) of β_m is given by $Y = \frac{1}{(m-1)!} v_m v_m^T$. Note that v_m can be indexed by M_i ($i = 3, \dots, \lfloor \frac{m-1}{2} \rfloor + 1$) as in Proposition 4. Each plotted function corresponds to the coefficients of one v_m , where a point at position (M_i, x) signifies that the coordinate of v_m corresponding to M_i is x



behaves similarly for each m , as can be seen in Fig. 3. This gives us some hope that the optimal solutions can be constructed analytically, potentially leading to improved bounds for bigger m in the future.

5.4 Iterative procedure to obtain the bounds β_m

To solve (19) on the computer, we follow a cut generation method: First the semidefinite program is solved without the linear constraints. Then:

- All of the constraints are evaluated. (As m grows, this takes up most of the runtime.)
- We add the most violated constraint as a new constraint to the semidefinite program. When there are ties, we choose the most violated constraint that was evaluated first.
- The semidefinite program is solved again.

These steps are repeated, until no constraints are violated anymore. In theory this procedure could take $|\Omega'_m|$ iterations. In practice however, the number of iterations is much smaller, and we are able to compute β_m for $m \leq 13$ up to high precision on a desktop computer—see Table 2.²

5.5 Verifying the bounds

We explain the procedure used to verify our lower bounds. For the bound β_m , the starting point is formulation (19). For the bound α_m , one can derive the following analogous formulation. For $\lambda \vdash m$ and $\varepsilon \in \{\pm 1\}$, let m_λ^ε denote the number of columns of U_λ^ε in the representative set for the action of $S_m \times S_2$ on \mathbb{C}^{Z^m} we derived in Sect. 2. Also, for $\omega \in \Omega'_m$, define the matrix $C_\omega := \bigoplus_{\lambda \vdash m, \varepsilon \in \{\pm 1\}} (U_\lambda^\varepsilon)^T K_\omega U_\lambda^\varepsilon$. Then

$$\alpha_m = \max \left\{ t : Y \in \bigoplus_{\substack{\lambda \vdash n \\ \varepsilon \in \{\pm 1\}}} \mathbb{R}^{m_\lambda^\varepsilon \times m_\lambda^\varepsilon}, Y \geq 0, \forall \omega \in \Omega'_m : \langle Y, C_\omega \rangle + |\omega|t \leq |\omega|q_\omega \right\}. \tag{20}$$

² The julia code used is publicly available via the link: <https://github.com/CrossingBounds/CrossingNumber>.

Note that all our SDP's contain integer data after block-diagonalization, so in the SDP-input there is no rounding. However, the high-precision interior-point solution (t, Y) to (19) or (20) obtained from the solver may exhibit tiny infeasibilities. To obtain a rational feasible solution, we do the following:

- Round t to a rational number t' , and round the eigenvalues λ_i and eigenvectors v_i of Y to rationals $\hat{\lambda}_i$ and rational vectors \hat{v}_i . Construct a new matrix $Y' := \sum_{i'} \hat{\lambda}_{i'} \hat{v}_{i'} \hat{v}_{i'}^T$ from the nonnegative rounded eigenvalues and the corresponding rounded eigenvectors. Then $Y' \succeq 0$.
- Check each of the inequalities (involving only rational numbers) in (19) or (20) using the rational matrix Y' . If the inequality corresponding to ω is violated, replace t' by $(|\omega|q_\omega - \langle Y', C_\omega \rangle)/|\omega|$ so that the inequality is not violated anymore.

In this way, we obtain rational feasible solutions (t', Y') to (19) or (20) and thus guaranteed lower bounds on α_m and β_m . The obtained lower bounds coincide with the approximations of α_m and β_m computed by the solver for all decimals given in Table 2. (At least 40 decimals are correct for all computed bounds except α_{10} using SDPA-GMP [19], and at least 13 decimals are correct for α_{10} using SDPA-DD.)

Acknowledgements The authors thank Sander Gribling, Etienne de Klerk, Monique Laurent, Bart Litjens and Lex Schrijver for useful discussions. The authors also thank the anonymous referees and the editor for their careful reading and valuable comments to improve the content and presentation of the paper, as well as the proofs of Propositions 1 and 3. Most of this research was carried out while D. Brosch was with Tilburg University, Tilburg and S. Polak was with Centrum Wiskunde & Informatica, Amsterdam.

Open Access This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit <http://creativecommons.org/licenses/by/4.0/>.

References

1. Balogh, J., Lidický, B., Salazar, G.: Closing in on Hill's conjecture. *SIAM J. Discrete Math.* **33**, 1261–1276 (2019)
2. Balogh, J., Lidický, B., Norin, S., Pfender, F., Salazar, G., Spiro, S.: Crossing numbers of complete bipartite graphs. *Procedia Computer Science* **223**, 78–87 (2023)
3. Brosch, D.: Symmetry reduction in convex optimization with applications in combinatorics. Ph.D. thesis, Tilburg University (2022)
4. Cameron, P.J.: *Permutation Groups*. Cambridge University Press, Cambridge (1999)
5. de Klerk, E., Maharry, J., Pasechnik, D.V., Richter, R.B., Salazar, G.: Improved bounds for the crossing numbers of $K_{m,n}$ and K_n . *SIAM J. Discrete Math.* **20**, 189–202 (2006)
6. de Klerk, E., Pasechnik, D., Schrijver, A.: Reductions of symmetric semidefinite programs using the regular $*$ -representation. *Math. Program.* **109**, 613–624 (2007)
7. Dobre, C., Vera, J.: Exploiting symmetry in copositive programs via semidefinite hierarchies. *Math. Program. Ser. B* **151**, 659–680 (2015)
8. Gatermann, K., Parrilo, P.A.: Symmetry groups, semidefinite programs, and sums of squares. *J. Pure Appl. Algebra* **192**, 95–128 (2004)
9. Erdős, P., Guy, R.K.: Crossing number problems. *Am. Math. Mon.* **80**, 52–58 (1973)

10. Garey, M.R., Johnson, D.S.: Crossing number is NP-complete. *SIAM J. Algebraic Discrete Methods* **4**, 312–316 (1983)
11. Gijswijt, D.C.: Block diagonalization for algebras associated with block codes, [arXiv:0910.4515](https://arxiv.org/abs/0910.4515) (2009)
12. Gijswijt, D.C., Mittelmann, H.D., Schrijver, A.: Semidefinite code bounds based on quadruple distances. *IEEE Trans. Inf. Theory* **58**, 2697–2705 (2012)
13. Hymabaccuz, K., Pasechnik, D.: Decomposing Linear Representations of Finite Groups, [arXiv:2007.02459](https://arxiv.org/abs/2007.02459) (2020)
14. Isaacs, M.: *Character Theory of Finite Groups*. Academic Press, New York (1976)
15. Kleitman, D.J.: The crossing number of $K_{5,n}$. *J. Comb. Theory* **9**, 315–323 (1970)
16. Kraskiewicz, W., Weyman, J.: Algebra of coinvariants and the action of a Coxeter element. *Bayreuth. Math. Schr.* **63**, 265–284 (2001)
17. Laurent, M.: Strengthened semidefinite programming bounds for codes. *Math. Program.* **109**, 239–261 (2007)
18. Litjens, B.M., Polak, S.C., Schrijver, A.: Semidefinite bounds for nonbinary codes based on quadruples. *Des. Codes Crypt.* **84**(1), 87–100 (2017)
19. Nakata, M.: A numerical evaluation of highly accurate multiple-precision arithmetic version of semidefinite programming solver: SDPA-GMP, -QD and -DD. In: *Proceedings of 2010 IEEE Multi-Conference on Systems and Control*, pp. 29–34 (2010)
20. Norin, S., Zwols, Y.: Presentation at the BIRS Workshop on geometric and topological graph theory (13w5091) (2013). <https://www.birs.ca/events/2013/5-day-workshops/13w5091/videos/watch/201310011538-Norin.html>
21. Polak, S.C.: *New methods in coding theory: error-correcting codes and the Shannon capacity*. Ph.D. thesis, University of Amsterdam (2019)
22. Sagan, B.E.: *The Symmetric Group: Representations, Combinatorial Algorithms, and Symmetric Functions*. Graduate Texts in Mathematics, vol. 203. Springer, New York (2001)
23. Schaefer, M.: The graph crossing number and its variants: a survey. *Electron. J. Comb. DS21* (2022)
24. Schrijver, A.: New code upper bounds from the Terwilliger algebra and semidefinite programming. *IEEE Trans. Inf. Theory* **51**, 2859–2866 (2005)
25. Serre, J.-P.: *Linear Representations of Finite Groups*. Springer Graduate Texts in Mathematics. Springer, New York (1977)
26. Székely, L.A.: Turán’s brick factory problem: the status of the conjectures of Zarankiewicz and Hill. In: Gera, R., et al. (eds.) *Graph Theory*. Springer, New York (2016)
27. Woodall, D.R.: Cyclic-order graphs and Zarankiewicz’s crossing-number conjecture. *J. Graph Theory* **17**, 657–671 (1993)
28. Zarankiewicz, K.: On a problem of P. Turán concerning graphs. *Fundam. Math.* **41**, 137–145 (1954)

Publisher’s Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.