

# Mutually unbiased bases: polynomial optimization and symmetry

Sander Gribling and Sven Polak

Department of Econometrics and Operations Research, Tilburg University, Tilburg, The Netherlands

A set of  $k$  orthonormal bases of  $\mathbb{C}^d$  is called mutually unbiased if  $|\langle e, f \rangle|^2 = 1/d$  whenever  $e$  and  $f$  are basis vectors in distinct bases. A natural question is for which pairs  $(d, k)$  there exist  $k$  mutually unbiased bases in dimension  $d$ . The (well-known) upper bound  $k \leq d + 1$  is attained when  $d$  is a power of a prime. For all other dimensions it is an open problem whether the bound can be attained. Navascués, Pironio, and Acín showed how to reformulate the existence question in terms of the existence of a certain  $C^*$ -algebra. This naturally leads to a noncommutative polynomial optimization problem and an associated hierarchy of semidefinite programs. The problem has a symmetry coming from the wreath product of  $S_d$  and  $S_k$ .

We exploit this symmetry (analytically) to reduce the size of the semidefinite programs making them (numerically) tractable. A key step is a novel explicit decomposition of the  $S_d \wr S_k$ -module  $\mathbb{C}^{([d] \times [k])^t}$  into irreducible modules. We present numerical results for small  $d, k$  and low levels of the hierarchy. In particular, we obtain sum-of-squares proofs for the (well-known) fact that there do not exist  $d + 2$  mutually unbiased bases in dimensions  $d = 2, 3, 4, 5, 6, 7, 8$ . Moreover, our numerical results indicate that a sum-of-squares refutation, in the above-mentioned framework, of the existence of more than 3 MUBs in dimension 6 requires polynomials of total degree at least 12.

## 1 Introduction

Let  $d \in \mathbb{N}_{\geq 2}$ . A set of  $k$  orthonormal bases of  $\mathbb{C}^d$  is called *mutually unbiased* if

$$|\langle e, f \rangle|^2 = \frac{1}{d} \quad (*)$$

whenever  $e$  and  $f$  are basis vectors in *distinct* bases. A natural question is for which pairs  $(d, k)$  there exist  $k$  mutually unbiased bases in dimension  $d$ . A dimension counting argument shows that there can be at most  $d + 1$  mutually unbiased bases (MUBs) in dimension  $d$ .<sup>1</sup> No other general upper bounds are known. When  $d$  is a power of a prime number it is known that there exist  $d + 1$  MUBs [Iva81, WF89]. However, for all  $d$  that are not a power of a prime the question is wide open. Even for the first such number, dimension 6, it is not known whether there exist more than 3 such bases, despite extensive numerical search [BW09]. It is known however that certain sets of 3 MUBs are *maximal*, i.e., they can not be extended, see [Gra04]. Zauner conjectured that there do not exist 4 MUBs in dimension 6 [Zau99]. Recently, this (widely believed) conjecture was highlighted as one of five important open problems in quantum information theory [HRidZ22].

We mention some other constructions of sets of MUBs. If  $k$  MUBs exist in dimensions  $d_1$  and  $d_2$ , then  $k$  MUBs exist in dimension  $d_1 d_2$ . Hence, if  $d = p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k}$  for prime numbers  $p_1, \dots, p_k$  and

Sander Gribling: s.j.gribling@tilburguniversity.edu

Sven Polak: s.c.polak@tilburguniversity.edu

<sup>1</sup>To see this, consider the map  $u \mapsto uu^* - I_d/d$  between unit vectors in  $\mathbb{C}^d$  and traceless Hermitian  $d \times d$  matrices. This map sends  $k$  MUBs to  $k$  pairwise-orthogonal  $(d - 1)$ -dimensional subspaces of the  $(d^2 - 1)$ -dimensional space of traceless Hermitian  $d \times d$  matrices. Hence  $k \leq \frac{d^2 - 1}{d - 1} = d + 1$ .

integers  $n_1, \dots, n_k$  with  $p_1^{n_1} < p_2^{n_2} < \dots < p_k^{n_k}$ , then there exist at least  $p_1^{n_1} + 1$  MUBs in dimension  $d$ . This strategy of “reducing to prime-powers” does not always lead to the largest number of MUBs in a given non-prime power dimension. An alternative construction was proposed in [WB05]:  $k$  mutually orthogonal Latin squares of order  $n$  can be used to construct  $k+2$  MUBs in dimension  $n^2$ . For dimension  $d = 26^2 = 2^2 13^2$  this yields 6 MUBs (instead of  $2^2 + 1$ ). Finally, for any dimension  $d$ , if there exist  $d$  MUBs, then there exist  $d+1$  MUBs [Wei13].

**Applications of mutually unbiased bases.** A main feature of a collection of MUBs is that if one prepares a state in one of the bases, the measurements of this state with respect to another basis are predicted to occur uniformly at random. This property gives rise to many applications of MUBs in quantum information theory, for example in tomography algorithms [WF89], cryptographic protocols [BB84], and entanglement detection [SHB<sup>+</sup>12]. We refer to [BBE<sup>+</sup>07] for an excellent survey on mutually unbiased bases. Our work is motivated by Zauner’s conjecture on the existence of MUBs in dimension 6. From the perspective of applications, a construction of 7 MUBs in dimension 6 would yield optimal schemes in several settings. A proof of non-existence could help us understand what is special about the number/dimension 6. In the area of combinatorial designs the same number plays a special role, for instance there does not exist a finite affine plane of order 6 [BR49], nor a pair of mutually orthogonal Latin squares of order 6 [Tar01]. We refer to, e.g., [Woo06] for a discussion about the connections between MUBs and certain combinatorial designs.

**$C^*$ -algebraic formulation.** Navascués, Pironio, and Acín [NPA12] gave a  $C^*$ -algebraic formulation of the above problem:  $k$  MUBs exist in dimension  $d$  if and only if a certain  $C^*$ -algebra has a representation with  $I \neq 0$ . We describe this formulation in detail in Section 3. It can be viewed from the perspective of tracial noncommutative polynomial optimization and this leads to semidefinite programming relaxations. Proving infeasibility of such a relaxation would prove non-existence of  $k$  MUBs in dimension  $d$ . Here we follow this approach and exploit the symmetries in the resulting semidefinite programs.

**Symmetry in semidefinite programming.** Symmetry is widely used in semidefinite programming and polynomial optimization [BGSV12]. The usage of symmetry goes back to Delsarte [Del73], who formulated a linear programming bound for codes which was later shown [Sch79] to be a symmetry-reduced version of a slight strengthening of Lovász’  $\vartheta$ -function. Symmetry in semidefinite programs can be used to reduce their size by block-diagonalizing the involved matrix  $*$ -algebras. Indeed, it is a consequence of Schur’s lemma that a complex matrix  $*$ -algebra  $\mathcal{A}$  is  $*$ -isomorphic to a direct sum of full matrix algebras. That is, there exists a  $*$ -isomorphism  $\phi$  such that

$$\phi(\mathcal{A}) = \bigoplus_{i=1}^k \mathbb{C}^{m_i \times m_i}. \quad (1)$$

Constructing this  $*$ -isomorphism is often challenging. For numerical methods to do so, see [MKKK10, KDP11, RMMB21]. Via the regular  $*$ -representation one can obtain a representation of  $\mathcal{A}$  in an (often) smaller matrix algebra [KPS07]. We focus on the setting where the algebra consists of matrices that are invariant under a permutation action of a (finite) group. That is, we consider the matrix  $*$ -algebra  $\mathcal{A} = (\mathbb{C}^{Z \times Z})^G$  of  $G$ -invariant  $Z \times Z$  matrices where the group  $G$  acts on the set  $Z$ . In this setting one can construct the  $*$ -isomorphism from (1) explicitly. To do so, one needs to decompose the  $G$ -module  $\mathbb{C}^Z$  into a direct sum of irreducible  $G$ -modules (see Section 2.3 for the general theory). Group invariance has been used previously in (commutative) polynomial optimization, see for example [GP04, RTJAL13]. More generally, group symmetry in semidefinite programs has applications in many areas, for example in coding theory [Sch05], combinatorics [KPS07, KPS09, KS10], and in geometry [BV08]. Finding the  $*$ -isomorphism (i.e., the decomposition of  $\mathbb{C}^Z$ ) remains challenging even in the group-invariance setting.

Below we first discuss the symmetry that is present in the problem of determining the largest number of MUBs in a given dimension (the MUB problem), and then we give an overview of some of the prior work and our results.

**The symmetry in the MUB problem.** For  $n \in \mathbb{N}$ , let  $S_n$  be the symmetric group on  $n$  elements. The MUB property  $(*)$  of a set of  $k$  MUBs in dimension  $d$  is naturally invariant under relabeling the bases

(an  $S_k$  action) and, for each basis, relabeling the basis elements ( $S_d$  actions). These actions together precisely define an action of the wreath product  $S_d \wr S_k$ . One can show that the  $C^*$ -algebraic formulation and the related semidefinite programming (SDP) relaxations are invariant under this action. Since SDPs are convex, we may thus restrict our attention to solutions that are invariant under the  $S_d \wr S_k$  action. By reducing the number of variables, it yields a first reduction in the complexity of the semidefinite programs. It also implies that the matrix variables in the semidefinite program are group-invariant; by (1) this allows a second reduction in the complexity of the semidefinite programs. Constructing the  $*$ -isomorphism  $\phi$  analytically is the main contribution of our work, see Section 6.

**Symmetry reductions involving the wreath product.** In this paper we exploit group symmetry where the group is a wreath product of symmetric groups. Elements of the wreath product  $S_d \wr S_k$  are of the form  $(\alpha, \beta) = ((\alpha_1, \dots, \alpha_k), \beta)$  where  $\alpha_i \in S_d$  for each  $i \in [k]$  and  $\beta \in S_k$ . There are two canonical actions of the wreath product of  $S_d \wr S_k$  (cf., e.g., [CSST13]). The first action is an action on  $[d]^k$  defined as follows:

$$((\alpha_1, \dots, \alpha_k), \beta) \cdot (z_i)_{i \in [k]} = (\alpha_{\beta^{-1}(i)} \cdot z_{\beta^{-1}(i)})_{i \in [k]} \quad \text{for } (z_i)_{i \in [k]} \in [d]^k.$$

This action is also called the primitive action of  $S_d \wr S_k$  on  $[d]^k$  and is used extensively in coding theory related SDPs: see the fundamental work of Schrijver [Sch05] and subsequent works that rely on representation theory [Gij09, LPS17]. The symmetry reduction for the primitive action is by now well understood, see for example [Pol19] for a general exposition of reducing semidefinite programs invariant under  $G \wr S_n$  acting on  $V^{\otimes n}$  (where  $G$  acts on  $V$ ). In this paper we study a second canonical action of  $S_d \wr S_k$ , which is an action on  $[d] \times [k]$ . It is defined as follows:

$$((\alpha_1, \dots, \alpha_k), \beta) \cdot (i, j) = (\alpha_{\beta(j)}(i), \beta(j)) \quad \text{for } (i, j) \in [d] \times [k].$$

This action is known as the imprimitive action of  $S_d \wr S_k$  on  $[d] \times [k]$ . We give an analytic decomposition of  $\mathbb{C}^{([d] \times [k])^t}$  into  $S_d \wr S_k$ -irreducible submodules (for fixed  $t$ ), which is a new result for  $t > 1$ . For  $t = 1$  the separate actions of  $S_d$  on  $\mathbb{C}^{[d]}$  and  $S_k$  on  $\mathbb{C}^{[k]}$  are transitive and the analytic decomposition can be obtained for example from [CSST13, Thrm. 3.1.1].

**Representation theory of the wreath product  $S_d \wr S_k$ .** It is classical theory to describe the irreducible modules for wreath products of finite groups, see for example [Ker71, Mac80]. In particular, the irreducible modules for the wreath product  $S_d \wr S_k$  are known. However, as mentioned before, decomposing an arbitrary wreath-product-module into its irreducible components often remains challenging. Recently, certain “permutation modules” for wreath products have been studied (see Section 7 for their definition), and methods to derive the multiplicities of the irreducible modules in these modules have been given [CT03, Gre19]. However, in general there is no explicit description of the homomorphisms from the irreducible modules to the permutation modules (which is what we need for our symmetry reduction), see [Gre19] for a partial description. Our symmetry reduction involves constructing explicit homomorphisms for “L-shaped” permutation modules.

**Related prior work.** In [BW10] the MUB problem is considered from the perspective of solving a system of polynomial equations in commutative variables. The authors show that both techniques based on Gröbner bases and techniques based on polynomial optimization can be used to rule out the existence of certain MUBs in small dimensions. An advantage of this approach is its flexibility: one can for example fix a set of MUBs and ask whether it can be extended to a larger set of MUBs. A disadvantage is the number of variables (one per real variable). Noncommutative polynomial optimization was used in [NPA12] and also in [ABMP18]. The latter gives a reformulation of the MUB problem in terms of a game based on quantum random access codes: a certain winning probability is achievable if and only if there exist  $k$  MUBs in dimension  $d$ . They then use an SDP hierarchy of upper bounds on the winning probability due to Navascués and Vértesi [NV15] and numerically exploit the symmetry in the corresponding SDPs. Using this approach they rule out the existence of  $d + 2$  MUBs in dimensions  $d = 3, 4$ . A symmetry reduction for their SDPs can be obtained by decomposing certain modules of the wreath product  $S_d \wr S_k$ , just as in our case. However, the moment matrices appearing in their approach have a different index set from our moment matrices, hence our symmetry reduction is not directly applicable. We leave it to future work to combine our analytical symmetry reduction with their approach.

**Contributions.** We obtain a novel explicit decomposition of the  $S_d \wr S_k$ -module  $\mathbb{C}^{([d] \times [k])^t}$  into irreducible modules. In particular, this allows us to obtain the analytic symmetry reduction of the SDP relaxations coming from the  $C^*$ -algebraic formulation of Navascués, Pironio, and Acín [NPA12]. For fixed  $t \in \mathbb{N}$ , the size of the symmetry reduced SDP is independent of  $d$  and  $k$  whenever  $d, k \geq 2t$ . We provide an implementation of the symmetry reduced SDPs and use it to obtain numerical sum-of-squares certificates for the non-existence of  $d+2$  MUBs in dimensions  $d = 2, 3, 4, 5, 6, 7, 8$ . Moreover, our numerical results indicate that a sum-of-squares refutation (in the context of [NPA12]) of the existence of more than 3 MUBs in dimension 6 requires polynomials of total degree at least 12. See Table 1 for an overview of these numerical results. We use the SDP-solvers SDPA-DD or SDPA-GMP [Nak10, YFF<sup>+</sup>12] (when a solver returns an unknown result status we use a higher-precision solver).

| $d$ | $k$ | $t$ | size= $(dk)^{\lfloor t \rfloor}$ | #vars | #linear constraints | block sizes |      | result     |
|-----|-----|-----|----------------------------------|-------|---------------------|-------------|------|------------|
|     |     |     |                                  |       |                     | sum         | max  |            |
| 2   | 4   | 4.5 | 4096                             | 7     | 8                   | 472         | 85   | infeasible |
| 3   | 5   | 4.5 | 50625                            | 7     | 2                   | 1259        | 142  | infeasible |
| 4   | 6   | 5   | 7962624                          | 38    | 2                   | 6374        | 389  | infeasible |
| 5   | 7   | 5   | 52521875                         | 38    | 2                   | 6732        | 389  | infeasible |
| 6   | 8   | 5   | 254803968                        | 38    | 2                   | 6820        | 389  | infeasible |
| 7   | 9   | 5   | 992436543                        | 38    | 2                   | 6830        | 389  | infeasible |
| 8   | 10  | 5   | 3276800000                       | 38    | 2                   | 6831        | 389  | infeasible |
| 6   | 4   | 5.5 | 7962624                          | 43    | 3                   | 8049        | 577  | feasible   |
| 6   | 7   | 5.5 | 130691232                        | 62    | 3                   | 18538       | 1107 | feasible   |

Table 1: For various  $d, k, t$ , we give the number of rows of the original  $t$ -th level SDP, and for the symmetry reduced SDP the number of variables, the number of linear constraints on the variables, the sum and max of the block sizes, and the solver status.

**Implementation.** We use the programming language Julia to compute the symmetry-reduced semidefinite programs. The code is available here:

<https://github.com/MutuallyUnbiasedBases/>

Our code roughly consists of two parts. We first compute a representative set (cf. Proposition 2.2) for the representation at hand. We do this both for the action of  $S_d \wr S_k$  on (homogeneous) noncommutative polynomials in variables  $x_{i,j}$  with  $i \in [d], j \in [k]$ , and for the action of  $S_k$  on (homogeneous) noncommutative polynomials in variables  $x_1, \dots, x_k$ . This first part does not use the additional structure present in the MUB problem and is therefore also applicable to other problems that exhibit the same symmetry. The second part then consists of computing the entries of the symmetry-reduced SDP. For this we do use the specific structure of the MUB problem (and the previously computed representative set), see Section 8.1 for more details.

## 1.1 Organization

In Section 2 we provide preliminaries about (noncommutative) polynomial optimization and the general framework of symmetry reductions of group-invariant semidefinite programs. In Section 3 we state the  $C^*$ -algebraic formulation of the MUB problem of Navascués, Pironio, and Acín, and we discuss properties of the related semidefinite programming relaxations. To introduce the well-known representation theory of the symmetric group, we provide in Section 4 the symmetry reduction of noncommutative polynomial optimization problems in variables  $x_1, \dots, x_k$  that are invariant under the action of  $S_k$ . We present this from the perspective of representation theory (Sections 4.1 and 4.2), but we also illustrate the theory in Section 4.3 by presenting a small example (degree-2 polynomials in  $x_1, x_2, x_3$ ) in the language of noncommutative polynomials: the symmetry reduction amounts to choosing a suitable basis of the space of polynomials.

The symmetry reduction of  $S_k$  serves as a first step towards that of  $S_d \wr S_k$  in two ways. First, it can be viewed as a special case of the full  $S_d \wr S_k$  action on the variables  $x_{i,j}$  ( $i \in [d], j \in [k]$ ) by restricting to polynomials in the variables  $x_{1,j}$  ( $j \in [k]$ ). We can thus use it to symmetry-reduce a relaxation of the SDPs presented in Section 3.1 where we restrict to polynomials in  $x_{1,j}$  ( $j \in [k]$ ), in Section 8 we will

see that these relaxations sometimes already exclude the existence of MUBs. Second, the representation theory of  $S_d \wr S_k$  naturally builds on that of the symmetric group. Indeed, in Section 5 we describe known (irreducible)  $S_d \wr S_k$ -modules that can be constructed from (irreducible) modules for the symmetric group.

Our main result, the analytic symmetry reduction of the  $S_d \wr S_k$ -invariant semidefinite programs, is obtained in Section 6. At a high level, we obtain our symmetry reduction by decomposing the  $S_d \wr S_k$ -module  $\mathbb{C}\langle x \rangle_{=t}$  given by (homogeneous) degree- $t$  polynomials in the variables  $x_{i,j}$  ( $i \in [d], j \in [k]$ ) into irreducible modules. We do so by first decomposing  $\mathbb{C}\langle x \rangle_{=t}$  into orbits, we then relate these orbits to known modules of  $S_d \wr S_k$ . It turns out that these modules have a special structure (cf. Remark 6.1) which allows us to give an explicit decomposition of them into irreducible modules. To illustrate the (rather technical) theory, we give the explicit symmetry-reduction for the case  $d = 2, k = 3, t = 2$  in the language of noncommutative polynomials in Section 6.5. In Section 7 we relate the results of Section 6 to the literature: we show they can be viewed as a novel explicit decomposition of an “L-shaped” permutation module into irreducible  $S_d \wr S_k$ -modules.

Finally, in Section 8 we provide numerical results obtained using our symmetry reduction.

## 2 Preliminaries on polynomial optimization & symmetry

The use of sum-of-squares and moment techniques for polynomial optimization problems goes back to the works of Parrilo and Lasserre [Par00, Las01]. We refer to, e.g., [Las09, Lau09] for more information about commutative polynomial optimization. In the noncommutative setting such techniques were first introduced for eigenvalue optimization by Navascués, Pironio, and Acín [PNA10]. The extension to the tracial setting can be found in [BCKP13, KP16]. The method of symmetry reduction of group-invariant matrix algebras that we describe in Section 2.3 is well known, see for example [Gij09] and [Pol19] for complete proofs of the statements we use here.

### 2.1 Noncommutative polynomial optimization

We use  $\mathbb{R}\langle x_1, \dots, x_n \rangle$  to denote the ring of noncommutative polynomials in variables  $x_i$  for  $i \in [n]$ . Whenever the number of variables is clear from context, we abbreviate  $\mathbb{R}\langle x_1, \dots, x_n \rangle$  to  $\mathbb{R}\langle x \rangle$ . We equip  $\mathbb{R}\langle x \rangle$  with an involution  $*$  (a linear map) which acts on a monomial  $x_{i_1}x_{i_2} \cdots x_{i_\ell} \in \langle x \rangle$  by reversing the order of the variables:  $(x_{i_1}x_{i_2} \cdots x_{i_\ell})^* = x_{i_\ell}x_{i_{\ell-1}} \cdots x_{i_1}$ . In particular, we have  $x_i^* = x_i$  for all  $i$ . A polynomial  $p$  is Hermitian if  $p^* = p$ . Let  $S$  be a set of Hermitian noncommutative polynomials. The matrix positivity domain associated to  $S$  is

$$\mathcal{D}(S) = \cup_{d \in \mathbb{N}} \{ (X_1, \dots, X_n) \in (\mathbb{H}^d)^n : g(\mathbf{X}) \succeq 0 \text{ for all } g \in S \}$$

where  $\mathbb{H}^d$  is the space of Hermitian  $d \times d$  matrices and for a  $C^*$ -algebra  $\mathcal{A}$  we let

$$\mathcal{D}_{\mathcal{A}}(S) := \{ (X_1, \dots, X_n) \in \mathcal{A}^n : X_i^* = X_i \text{ for } i \in [n], g(\mathbf{X}) \succeq 0 \text{ for all } g \in S \}$$

be its  $C^*$ -algebraic analogue. One similarly defines a matrix variety and its  $C^*$ -algebraic analogue for a set  $T$  of noncommutative polynomials:

$$\begin{aligned} \mathcal{V}(T) &= \cup_{d \in \mathbb{N}} \{ (X_1, \dots, X_n) \in (\mathbb{H}^d)^n : h(\mathbf{X}) = 0 \text{ for all } h \in T \} \\ \mathcal{V}_{\mathcal{A}}(T) &= \{ (X_1, \dots, X_n) \in \mathcal{A}^n : X_i^* = X_i \text{ for } i \in [n], h(\mathbf{X}) = 0 \text{ for all } h \in T \}. \end{aligned}$$

A tracial polynomial optimization problem over  $\mathcal{D}_{\mathcal{A}}(S) \cap \mathcal{V}_{\mathcal{A}}(T)$  can be written as

$$\inf_{\mathcal{A}, \tau, \mathbf{X}} \{ \tau(f(\mathbf{X})) : \tau \text{ is a tracial state on } \mathcal{A}, \mathbf{X} \in \mathcal{D}_{\mathcal{A}}(S) \cap \mathcal{V}_{\mathcal{A}}(T) \}. \quad (2)$$

A fundamental result in the theory of noncommutative polynomial optimization is a reformulation of the above in terms of linear functionals acting on the vector space of polynomials in noncommutative variables  $x_1, \dots, x_n$ . That is, one considers the following (related) problem

$$\inf \{ L(f) : L \in \mathbb{R}\langle x \rangle^* \text{ tracial}, L(1) = 1, L \geq 0 \text{ on } \mathcal{M}(S), L = 0 \text{ on } \mathcal{I}(T) \}. \quad (3)$$

Here  $\mathcal{M}(S)$  is the *quadratic module* associated to the set  $S$ , i.e., the cone of polynomials generated by polynomials of the form  $p^*gp$  for  $g \in S, p \in \mathbb{R}\langle x \rangle$ , and  $\mathcal{I}(T)$  is the *ideal* associated to  $T$ , i.e., the vector

space of polynomials of the form  $ph$  for  $h \in T$ ,  $p \in \mathbb{R}\langle x \rangle$ . The problems (2) and (3) are equivalent whenever the Minkowski sum  $\mathcal{M}(S) + \mathcal{I}(T)$  is *Archimedean*<sup>2</sup>. Proofs of this equivalence can be found in [NPA12, BCKP13]. One obtains a hierarchy of lower bounds by considering polynomials of degree at most  $2t$  (for  $t \in \mathbb{N}$ ):

$$f_t = \inf \{ L(f) : L \in \mathbb{R}\langle x \rangle_{2t}^* \text{ tracial, } L(1) = 1, L \geq 0 \text{ on } \mathcal{M}(S)_{2t}, L = 0 \text{ on } \mathcal{I}(T)_{2t} \}, \quad (4)$$

where

$$\begin{aligned} \mathcal{M}(S)_{2t} &= \text{cone}\{p^*gp : g \in S, p \in \mathbb{R}\langle x \rangle, \deg(p^*gp) \leq 2t\}, \\ \mathcal{I}(T)_{2t} &= \text{cone}\{ph : h \in T, p \in \mathbb{R}\langle x \rangle, \deg(ph) \leq 2t\}. \end{aligned}$$

This hierarchy converges to Eq. (3) whenever  $\mathcal{M}(S) + \mathcal{I}(T)$  is Archimedean. Each relaxation  $f_t$  can be expressed as a semidefinite program (cf. Eq. (7)).

## 2.2 Group-invariant polynomial optimization problems.

Let  $G$  be a finite group acting on  $[n]$ . We let  $G$  act on noncommutative variables  $x_1, \dots, x_n$  by letting  $G$  act on the indices:  $\sigma \cdot x_i = x_{\sigma(i)}$  for all  $\sigma \in G, i \in [n]$ . We extend the action of  $G$  to monomials by letting  $\sigma$  act on each of the variables, e.g.,  $\sigma \cdot (x_i x_j) = x_{\sigma(i)} x_{\sigma(j)}$ , and we further extend it linearly to  $\mathbb{R}\langle x \rangle = \mathbb{R}\langle x_1, \dots, x_n \rangle$ . We define its action on  $n$ -tuples  $(x_1, \dots, x_n) \in \mathcal{A}^n$  similarly:  $\sigma \cdot (x_1, \dots, x_n) = (x_{\sigma(1)}, \dots, x_{\sigma(n)})$ . For  $\sigma \in G$  and  $L \in \mathbb{R}\langle x \rangle^*$  we define  $\sigma \cdot L$  via  $\sigma \cdot L(p) = L(\sigma \cdot p)$  for all  $p \in \mathbb{R}\langle x \rangle$ , this defines an action of  $G$  on  $\mathbb{R}\langle x \rangle^*$ . We say  $L \in \mathbb{R}\langle x \rangle^*$  is  $G$ -invariant if  $\sigma \cdot L = L$ , i.e., if  $L(p) = L(\sigma \cdot p)$  for all  $\sigma \in G$  and  $p \in \mathbb{R}\langle x \rangle$ . Let  $\mathbb{R}\langle x \rangle^G$  be the subspace of  $G$ -invariant polynomials.

In the polynomial optimization problems that we consider, there will be a finite group  $G$  such that the objective  $f$  is invariant under the action of  $G$  (i.e.,  $f \in \mathbb{R}\langle x \rangle^G$ ) and such that whenever  $L$  is feasible for the moment relaxation (4), then also  $\sigma \cdot L$  is feasible for every  $\sigma \in G$ . Note that  $\sigma \cdot L$  will have the same objective value  $\sigma \cdot L(f) = L(f)$  since  $f$  is  $G$ -invariant. As the feasible region in (4) is convex and  $G$  is finite, it is easy to verify that the linear functional  $\bar{L} = \frac{1}{|G|} \sum_{\sigma \in G} \sigma \cdot L$  is a  $G$ -invariant feasible solution with the same value. Hence we may assume that the optimum  $L$  in (4) is  $G$ -invariant. Note that  $G$ -invariant linear functionals are completely determined by their values on  $\mathbb{R}\langle x \rangle^G$ . This gives a first reduction in the size of the SDP by reducing the number of variables. As mentioned before, a second reduction can be obtained by exploiting the group invariance of the algebra generated by the matrix variables in the SDP. In the next section we recall the general theory.

## 2.3 Symmetry reduction of group-invariant matrix algebras

Let  $G$  be a finite group. If  $G$  acts on a finite-dimensional complex vector space  $V$ , we call  $V$  a  $G$ -module.<sup>3</sup> Suppose that  $V$  is equipped with a  $G$ -invariant inner product  $\langle \cdot, \cdot \rangle$ . Let  $\text{End}_G(V)$  be the space of  $G$ -invariant endomorphisms on  $V$ , that is, the space of linear maps  $A : V \rightarrow V$  that are  $G$ -invariant:  $A(g \cdot v) = g \cdot (Av)$  for all  $v \in V$  and  $g \in G$ . The space  $\text{End}_G(V)$  forms an algebra with multiplication given by function composition. We recall how to block-diagonalize  $\text{End}_G(V)$ .

If  $U \subseteq V$  is a  $G$ -invariant subspace of a  $G$ -module  $V$ , then  $U$  is a *submodule* of  $V$ . A module  $V \neq \{0\}$  is irreducible if the only submodules of  $V$  are  $\{0\}$  and  $V$ . Two  $G$ -modules  $V$  and  $W$  are  $G$ -isomorphic if there exists a bijection  $\psi : V \rightarrow W$  that respects the group action  $g \cdot \psi(v) = \psi(g \cdot v)$  for all  $v \in V$ ,  $g \in G$ . A  $G$ -module  $V$  can then be decomposed as

$$V = \bigoplus_{i=1}^k \bigoplus_{j=1}^{m_i} V_{i,j} \quad (5)$$

where the  $V_{i,j}$  are irreducible  $G$ -modules and  $V_{i,j}$  and  $V_{i',j'}$  are  $G$ -isomorphic if and only if  $i' = i$ . One can show that  $\text{End}_G(V)$  is  $*$ -isomorphic to the matrix algebra  $\bigoplus_{i=1}^k \mathbb{C}^{m_i \times m_i}$  (a  $*$ -isomorphism between

<sup>2</sup> $\mathcal{M}(S) + \mathcal{I}(T)$  is Archimedean whenever there exists an  $R \in \mathbb{R}$  such that  $R^2 - \sum_{i \in [n]} x_i^* x_i \in \mathcal{M}(S) + \mathcal{I}(T)$ . This property will hold for the polynomial optimization problems we consider in this work.

<sup>3</sup>A *group action* of a group  $G$  on a set  $Z$  is a map  $G \times Z \rightarrow Z : (g, z) \mapsto g \cdot z$  which satisfies  $1 \cdot z = z$  and  $g_1 \cdot (g_2 \cdot z) = (g_1 g_2) \cdot z$  for all  $g_1, g_2 \in G$  and  $z \in Z$ . When  $Z$  is a (complex) linear space, we additionally assume  $g \cdot (z_1 + z_2) = g \cdot z_1 + g \cdot z_2$  and  $g \cdot (\alpha z) = \alpha(g \cdot z)$  for each  $z_1, z_2 \in Z$ ,  $g \in G$  and  $\alpha \in \mathbb{C}$ .

two matrix algebras is an isomorphism that preserves the  $*$ -operation, i.e., the conjugate transpose). Here we will use a slightly weaker result: there exists a linear bijection  $\Phi : \text{End}_G(V) \rightarrow \bigoplus_{i=1}^k \mathbb{C}^{m_i \times m_i}$  such that for all  $A \in \text{End}_G(V)$ ,  $A \succeq 0$  if and only if  $\Phi(A) \succeq 0$ . (In general the  $\Phi$  we construct will not be a  $*$ -isomorphism.)

**Definition 2.1** (Representative set). *Let  $V$  be a  $G$ -module with a decomposition into irreducible  $G$ -modules  $V_{i,j}$  as in (5). For each  $i \in [k]$ , choose vectors  $u_{i,j} \in V_{i,j}$  for  $j \in [m_i]$  in such a way that for each  $j, \ell \in [m_i]$  there exists a  $G$ -isomorphism from  $V_{i,j}$  to  $V_{i,\ell}$  that maps  $u_{i,j}$  to  $u_{i,\ell}$ . Let  $U_i = (u_{i,1}, \dots, u_{i,m_i})$ . Then  $\{U_1, \dots, U_k\}$  forms a representative set for the action of  $G$  on  $V$ .*

The term *symmetry adapted basis* is sometimes used to denote a basis respecting the decomposition of  $V$  into  $G$ -modules, cf. [FS92]. A representative set contains one ‘representative’ basis element of each irreducible module, cf. [LPS17]. The term *symmetry basis* is also used in the literature to denote the set of consisting of all  $u_{i,j}$  forming a representative set, cf. [BR21].

We then have the following (which is well-known general theory; a proof of the theorem in this exact form can be found in [Pol19]):

**Proposition 2.2.** *Let  $G$  be a finite group and let  $V$  be a finite-dimensional  $G$ -module with a decomposition as in (5). Let  $\{U_1, \dots, U_k\}$  be a representative set for the action of  $G$  on  $V$ . Define the map  $\Phi : \text{End}_G(V) \rightarrow \bigoplus_{i=1}^k \mathbb{C}^{m_i \times m_i}$  as*

$$A \mapsto \bigoplus_{i=1}^k (\langle u_{i,j}, Au_{i,\ell} \rangle)_{j,\ell \in [m_i]}.$$

*Then  $\Phi$  is a bijection and for all  $A \in \text{End}_G(V)$ , we have  $A \succeq 0$  if and only if  $\Phi(A) \succeq 0$ .*

The complex vector spaces  $V$  studied in this paper all have the form  $V = \mathbb{C}^Z$ , where  $Z$  is a finite set on which  $G$  acts (hence  $G$  acts on  $V = \mathbb{C}^Z$  via permutation matrices). In this case  $\text{End}_G(V)$  is naturally isomorphic to  $(\mathbb{C}^{Z \times Z})^G$ , the space of complex  $Z \times Z$ -matrices which are invariant under the simultaneous action of  $G$  on their rows and columns. Any representative set  $\{U_1, \dots, U_k\}$  as in Definition 2.1 then consists of  $m_i$ -tuples  $U_i$  of vectors contained in  $\mathbb{C}^Z$ , so we can view  $U_i$  as a  $(Z \times m_i)$ -matrix. Moreover, each representative set  $\{U_1, \dots, U_k\}$  determined in this paper consists of real matrices. In that case  $\Phi$  is even a block-diagonalization “over  $\mathbb{R}$ ”, i.e.,  $\Phi$  provides a bijection between  $(\mathbb{R}^{Z \times Z})^G$  and  $\bigoplus_{i=1}^k \mathbb{R}^{m_i \times m_i}$  such that  $A \succeq 0$  if and only if  $\Phi(A) \succeq 0$ .

Finally, note that if  $\{U_1^1, \dots, U_{k_1}^1\}$  and  $\{U_1^2, \dots, U_{k_2}^2\}$  are representative sets for the actions of  $G_1$  and  $G_2$  on  $V_1$  and  $V_2$  respectively, then

$$\{U_i^1 \otimes U_j^2 \mid i \in [k_1], j \in [k_2]\} \tag{6}$$

is a representative set for the action of  $G_1 \times G_2$  on  $V_1 \otimes V_2$ .

### 3 MUB-algebra

One can consider an orthonormal basis of  $\mathbb{C}^d$  as being defined by vectors  $u_1, \dots, u_d \in \mathbb{C}^d$  or by the associated rank-1 orthogonal projectors  $P_1, \dots, P_d \in \mathbb{C}^{d \times d}$  (where  $P_i = u_i u_i^*$  for all  $i$ ). Here we take the second perspective and consider the algebra generated by the projectors arising from (pairwise) mutually unbiased bases. Let  $\{u_1, \dots, u_d\}$  and  $\{v_1, \dots, v_d\}$  form two orthonormal bases of  $\mathbb{C}^d$  and set  $P_i = u_i u_i^*$ ,  $Q_i = v_i v_i^*$  for all  $i \in [d]$ . Then the following holds:

- (i)  $P_i^* = P_i = P_i^2$  for all  $i \in [d]$ , since  $(u_i u_i^*)^* = u_i u_i^* = \langle u_i, u_i \rangle u_i u_i^* = (u_i u_i^*)^2$ ,
- (ii)  $P_i P_j = \delta_{i,j} P_i$  for all  $i, j \in [d]$ , since  $u_i u_i^* u_j u_j^* = \langle u_i, u_j \rangle u_i u_j^* = \delta_{i,j} u_i u_i^*$ ,
- (iii)  $\sum_{i=1}^d P_i = I$ , since for any  $j \in [d]$  we have  $(\sum_{i=1}^d u_i u_i^*) u_j = \sum_{i \in [d]} \langle u_i, u_j \rangle u_i = u_j$ ,
- (iv)  $P_i Q_j P_i = \frac{1}{d} P_i$  for all  $i, j \in [d]$ , since  $u_i u_i^* v_j v_j^* u_i u_i^* = |\langle u_i, v_j \rangle|^2 u_i u_i^* = \frac{1}{d} u_i u_i^*$ ,

(v)  $[P_i U P_i, P_i V P_i] = P_i U P_i V P_i - P_i V P_i U P_i = 0$  for all  $i \in [d], U, V \in \mathbb{C}^{d \times d}$ , since

$$u_i u_i^* U u_i u_i^* V u_i u_i^* = \langle u_i, U u_i \rangle \langle u_i, V u_i \rangle u_i u_i^* = u_i u_i^* V u_i u_i^* U u_i u_i^*.$$

The above conditions generalize naturally to  $k$  pairwise mutually unbiased bases. Note however that the  $P_i$ 's and  $Q_j$ 's are  $d \times d$  matrices. In order to use noncommutative polynomial optimization techniques, we need to relax the condition that the operators are of size  $d \times d$ . We require the following  $C^*$ -algebraic formulation:

**Definition 3.1** (MUB-algebra). *We call a  $C^*$ -algebra  $\mathcal{A}$  a  $(d, k)$ -MUB-algebra if it contains Hermitian elements  $X_{i,j}$  for  $i \in [d], j \in [k]$  that satisfy the following conditions:*

- (i)  $X_{i,j} X_{i',j} = \delta_{i,i'} X_{i,j}$  for all  $i, i' \in [d], j \in [k]$ ,
- (ii)  $\sum_{i \in [d]} X_{i,j} = I$  for all  $j \in [k]$ ,
- (iii)  $X_{i,j} X_{i',j'} = \frac{1}{d} X_{i,j}$  for all  $i, i' \in [d], j, j' \in [k]$  with  $j \neq j'$ ,
- (iv)  $[X_{i,j} U X_{i,j}, X_{i,j} V X_{i,j}] = 0$  for all  $i \in [d], j \in [k]$  and  $U, V \in \langle \mathbf{X} \rangle$ , where  $\langle \mathbf{X} \rangle$  denotes the set of monomials in  $X_{i,j}$ .<sup>4</sup>

We have shown above that if there exist  $k$  mutually unbiased bases in dimension  $d$ , then there exists a  $(d, k)$ -MUB-algebra. Navascués, Pironio, and Acín showed the converse in [NPA12]: if a  $(d, k)$ -MUB-algebra exists with  $I \neq 0$ , then there exist  $k$  mutually unbiased bases in dimension  $d$ .

**Theorem 3.2** ([NPA12]). *There exists a set of  $k$  MUBs in dimension  $d$  if and only if there exists a  $(d, k)$ -MUB-algebra with  $I \neq 0$ .*

We provide a slightly simpler proof (which is inspired by the proof in [NPA12]) of the “only if”-direction in Appendix A. In [NPA12] the authors suggest to use noncommutative polynomial optimization techniques to determine the existence of a  $(d, k)$ -MUB-algebra. We use *tracial* noncommutative polynomial optimization to do so, that is, we use the following simple corollary.

**Corollary 3.3.** *There exists a set of  $k$  MUBs in dimension  $d$  if and only if there exists a  $(d, k)$ -MUB-algebra equipped with a tracial state  $\tau$  for which  $\tau(X_{i,j}) = 1$  for all  $i \in [d], j \in [k]$ .*

In other words, there exist  $k$  MUBs in dimension  $d$  if and only if the following problem is feasible

$$\inf\{0 : \exists C^*\text{-alg. } \mathcal{A} \text{ with tracial state } \tau, \text{ with Herm. } X_{i,j} \in \mathcal{A} \text{ (for } i \in [d], j \in [k]) \text{ satisfying (i)–(iv) and } \tau(X_{i,j}) = 1\},$$

where for any set  $\mathcal{F}$ , feasibility of the optimization problem  $\inf\{0 : \exists a \in \mathcal{F}\}$  means that  $\mathcal{F}$  is nonempty. We now rephrase the above feasibility problem as a tracial optimization problem in the variables  $x_{i,j}$  where  $i \in [d], j \in [k]$ . Let  $\mathcal{I}_{\text{MUB}}$  be the ideal generated by the relations (i) to (iv) of Definition 3.1. Then the above feasibility problem can be equivalently formulated as

$$\inf\{0 : \exists L \in \mathbb{R}\langle x \rangle^* \text{ s.t. } L \text{ is tracial, positive, } L = 0 \text{ on } \mathcal{I}_{\text{MUB}}, \text{ and } L(x_{i,j}) = 1 \text{ for all } i \in [d], j \in [k]\}.$$

(To see the equivalence, a tracial state  $\tau$  defines a feasible solution  $L$  by restricting to the algebra generated by the  $x_{i,j}$ . Conversely, applying the GNS construction to a feasible solution  $L$  yields a  $C^*$ -algebra  $\mathcal{A}$  with the desired properties.)

**Theorem 3.4.** *There exist  $k$  MUBs in dimension  $d$  if and only if there exists a positive tracial linear functional  $L \in \mathbb{R}\langle x \rangle^*$  that satisfies  $L = 0$  on  $\mathcal{I}_{\text{MUB}}$  and  $L(x_{i,j}) = 1$  for all  $i \in [d], j \in [k]$ .*

<sup>4</sup>The proof of Theorem 3.2 only uses  $U, V \in \langle \mathbf{X} \rangle_3$ , i.e., monomials in  $X_{i,j}$  of degree  $\leq 3$ .



### 3.1 Semidefinite programming relaxation

Theorem 3.4 gives rise to an infinite-dimensional semidefinite program since positivity of a linear functional  $L \in \mathbb{R}\langle x \rangle^*$  can be expressed in terms of positive semidefiniteness of its moment matrix:

$$L(p^*p) \geq 0 \text{ for all } p \in \mathbb{R}\langle x \rangle \iff M(L) := (L(u^*v))_{u,v \in \langle x \rangle} \succeq 0. \quad (7)$$

We then obtain (finite-dimensional) relaxations by considering linear functionals acting on polynomials of bounded degree. We define the following semidefinite programs for  $t \in \mathbb{N}$ :

$$\begin{aligned} \text{sdp}(d, k, t) = \inf \{ & 0 : \exists L \in \mathbb{R}\langle x \rangle_{2t}^* \text{ s.t. } L \text{ is tracial,} \\ & L = 0 \text{ on } \mathcal{I}_{\text{MUB}, 2t}, \\ & L(p^*p) \geq 0 \text{ for all } p \in \mathbb{R}\langle x \rangle_t, \\ & L(x_{i,j}) = 1 \text{ for all } i \in [d], j \in [k] \}. \end{aligned}$$

Also, we define  $\text{sdp}(d, k, t + \frac{1}{2})$  by restricting in the definition of  $\text{sdp}(d, k, t + 1)$  to polynomials of degree  $2t + 1$  and for the positivity condition to polynomials of the form  $p = x_{i,j}\tilde{p}$  where  $\tilde{p} \in \mathbb{R}\langle x \rangle_t$  (where we view  $\tilde{p}^*x_{i,j}\tilde{p} = \tilde{p}^*x_{i,j}\tilde{p}$  as a polynomial of degree  $2t + 1$ ). That is, for  $t \in \mathbb{N}$ , we define

$$\begin{aligned} \text{sdp}(d, k, t + \frac{1}{2}) = \inf \{ & 0 : \exists L \in \mathbb{R}\langle x \rangle_{2t+1}^* \text{ s.t. } L \text{ is tracial,} \\ & L = 0 \text{ on } \mathcal{I}_{\text{MUB}, 2t+1}, \\ & L(p^*x_{i,j}p) \geq 0 \text{ for all } p \in \mathbb{R}\langle x \rangle_t, i \in [d], j \in [k], \\ & L(x_{i,j}) = 1 \text{ for all } i \in [d], j \in [k] \}. \end{aligned}$$

These relaxations become tighter as  $t$  grows. Indeed, if  $L \in \mathbb{R}\langle x \rangle_{2t+2}^*$  is feasible for  $\text{sdp}(d, k, t + 1)$ , then the restriction of  $L$  to degree  $2t + 1$  polynomials is feasible for  $\text{sdp}(d, k, t + \frac{1}{2})$  (using  $x_{i,j}^2 = x_{i,j}$ ). Similarly, if  $L \in \mathbb{R}\langle x \rangle_{2t+1}^*$  is feasible for  $\text{sdp}(d, k, t + \frac{1}{2})$ , then for any polynomial  $p \in \mathbb{R}\langle x \rangle_t$  and  $j \in [k]$  we have  $L(p^*p) = \sum_{i \in [d]} L(p^*x_{i,j}p) \geq 0$ , and therefore the restriction of  $L$  to degree  $2t$  polynomials is feasible for  $\text{sdp}(d, k, t)$ . We also have the following:

**Lemma 3.5.** *Let  $t \in \mathbb{N}$ . Then if  $\text{sdp}(d, k, t)$  is infeasible, there do not exist  $k$  MUBs in dimension  $d$ .*

Its converse holds in the following sense (its proof is standard, we include it for completeness):

**Lemma 3.6.** *If there do not exist  $k$  MUBs in dimension  $d$ , then there exists a  $t_0 \in \mathbb{N}$  such that  $\text{sdp}(d, k, t)$  is infeasible for all  $t \geq t_0$ .*

*Proof.* Indeed, towards a contradiction, suppose  $\text{sdp}(d, k, t)$  is feasible for all  $t \in \mathbb{N}$ . For each  $t \in \mathbb{N}$ , let  $L_t \in \mathbb{R}\langle x \rangle_{2t}^*$  be a feasible solution for  $\text{sdp}(d, k, t)$ . We can extend  $L_t$  to a linear functional  $\widetilde{L}_t$  on  $\mathbb{R}\langle x \rangle$  by defining  $\widetilde{L}_t(w) = 0$  for all monomials  $w \in \langle x \rangle$  with  $|w| > 2t$ . The Archimedeanity of  $\mathcal{I}_{\text{MUB}}$  and the fact that  $L_t(1) = d$  for all  $t$  together imply that  $|\widetilde{L}_t(w)| \leq dR^{|w|}$  for all monomials  $w \in \langle x \rangle$  and all  $t \in \mathbb{N}$ , where  $R \in \mathbb{R}$  is such that  $R^2 - \sum_{i,j} x_{i,j}^2 \in \mathcal{M}(\emptyset) + \mathcal{I}_{\text{MUB}}$ . The Banach-Alaoglu theorem then ensures the existence of a subsequence of the sequence  $\{\widetilde{L}_t\}_{t \in \mathbb{N}}$  that converges pointwise to  $L \in \mathbb{R}\langle x \rangle^*$ . This  $L$  is then a positive tracial linear functional and it is zero on  $\mathcal{I}_{\text{MUB}}$ . Theorem 3.4 then shows that there exist  $k$  MUBs in dimension  $d$ .  $\square$

In  $\text{sdp}(d, k, t)$  it suffices to enforce  $L(p^*p) \geq 0$  for all *homogeneous* polynomials of degree  $t$ . Indeed, for  $p = \sum_{w \in \langle x \rangle_t} p_w w \in \mathbb{R}\langle x \rangle_t$ , define its homogenization  $p_{\text{hom}} = \sum_{w \in \langle x \rangle_t} p_w (\sum_{i=1}^d x_{i,1})^{t-|w|} w$ . One then has  $L(p^*p) = L(p_{\text{hom}}^* p_{\text{hom}})$  since  $\mathcal{I}_{\text{MUB}, 2t}$  contains generators of the form  $1 - \sum_{i=1}^d x_{i,j}$  (and  $L$  is tracial). The analogous statement holds for  $\text{sdp}(d, k, t + \frac{1}{2})$ .

**Lemma 3.7.** *Let  $t \in \mathbb{N}$  and let  $L \in \mathbb{R}\langle x \rangle_{2t}^*$  be a tracial linear functional such that  $L = 0$  on the truncated ideal generated by the polynomial  $1 - \sum_{i=1}^d x_{i,1}$ . Then, if  $L(q^*q) \geq 0$  for all homogeneous polynomials  $q$  of degree  $t$ , then  $L(p^*p) \geq 0$  for all polynomials  $p$  of degree at most  $t$ .*

**Certificates of infeasibility.** For  $d, k, t \in \mathbb{N}$ , the dual of  $\text{sdp}(d, k, t)$  is

$$\text{sdp}^*(d, k, t) := \sup \left\{ \sum_{i \in [d], j \in [k]} \lambda_{i,j} : - \sum_{i,j} \lambda_{i,j} x_{i,j} \in \mathcal{M}(1)_{2t} + \mathcal{I}_{\text{MUB}, 2t} \right\}.$$

The program  $\text{sdp}^*(d, k, t)$  is strictly feasible. Indeed, the relations  $x_{i,j} = x_{i,j}^2$  show that the point  $(\lambda_{i,j})_{i \in [d], j \in [k]}$  given by  $\lambda_{i,j} = -1 + \delta_{i,j}$  is feasible whenever  $|\delta_{i,j}| \leq 1$  for all  $i \in [d], j \in [k]$ . Hence, if  $\text{sdp}(d, k, t)$  is infeasible, there exists a feasible solution  $(\lambda_{i,j})$  for  $\text{sdp}^*(d, k, t)$  with  $\sum_{i,j} \lambda_{i,j} > 0$ . For the half-integer levels  $\text{sdp}(d, k, t + \frac{1}{2})$  the dual is formed analogously with  $\mathcal{M}(1)_{2t}$  replaced by  $\mathcal{M}(\{x_{i,j} : i \in [d], j \in [k]\})_{2t+1}$  and  $\mathcal{I}_{\text{MUB}, 2t}$  replaced by  $\mathcal{I}_{\text{MUB}, 2t+1}$  (the same point is strictly feasible).

### 3.2 Group-invariance of the MUB problem

As mentioned before, the MUB property  $(*)$  of a set of orthonormal bases is preserved under permuting the bases, and under permuting the basis vectors within a single basis. Together these two permutation actions give rise to an action on sets of orthonormal bases of the *wreath product* of  $S_d$  and  $S_k$ . Here we recall the definition of this group and its action on noncommutative polynomials in variables  $x_{i,j}$  where  $i \in [d], j \in [k]$ .

Let  $d, k \in \mathbb{N}$ . Then the wreath product of  $S_d$  and  $S_k$  is a group denoted as  $S_d \wr S_k$ . The group  $S_d \wr S_k$  is a finite group with  $k!(d!)^k$  elements. Each element is of the form  $(\alpha, \beta) = ((\alpha_1, \dots, \alpha_k), \beta)$  where  $\alpha_i \in S_d$  for each  $i \in [k]$  and  $\beta \in S_k$ . The product of  $(\alpha, \beta)$  and  $(\eta, \zeta)$  is defined as

$$(\alpha, \beta)(\eta, \zeta) = (\alpha(\beta * \eta), \beta\zeta)$$

where  $\beta * \eta = (\eta_{\beta^{-1}(1)}, \dots, \eta_{\beta^{-1}(k)})$ .<sup>5</sup> We define the following action of  $S_d \wr S_k$  on noncommutative variables  $x_{i,j}$  indexed by pairs  $(i, j) \in [d] \times [k]$ : for  $(\alpha, \beta) \in S_d \wr S_k$  we set

$$(\alpha, \beta)x_{i,j} = x_{\alpha_{\beta(j)}(i), \beta(j)}.$$

This induces an action of  $S_d \wr S_k$  on noncommutative polynomials in variables  $x_{i,j}$  for  $i \in [d], j \in [k]$ .

**Group-invariance of the SDP relaxations.** The above action on monomials makes  $\text{sdp}(d, k, t)$  group-invariant for the group  $G = S_d \wr S_k$  and  $\text{sdp}(d, k, t + \frac{1}{2})$  group-invariant for a suitable subgroup  $G$  of  $S_d \wr S_k$  that we describe below. Following the discussion in Section 2.2, this allows us to restrict to  $G$ -invariant  $L$  in the definition of  $\text{sdp}(d, k, t)$  and  $\text{sdp}(d, k, t + \frac{1}{2})$ .

For level  $t$ , the rows and columns of the moment matrix are indexed by the monomials in  $\mathbb{R}\langle x_{i,j} \mid i \in [d], j \in [k] \rangle_{=t}$ . We identify this index set with  $Z := ([d] \times [k])^t$ . The moment matrix is invariant under the simultaneous action of the wreath product  $G := S_d \wr S_k$  on its rows and columns. By Proposition 2.2, to block diagonalize the moment matrix it suffices to find a representative set for the action of  $G$  on  $\mathbb{C}^Z$ . We do so in Section 6.

For level  $t + \frac{1}{2}$ , we have  $dk$  localizing moment matrices (one for each  $x_{i,j}$ ). By symmetry these moment matrices are all positive semidefinite if and only if the moment matrix expressing  $L(p^* x_{1,1} p) \geq 0$  for each  $p \in \mathbb{R}\langle x_{i,j} \mid i \in [d], j \in [k] \rangle_{=t}$  is positive semidefinite. This moment matrix is indexed by the monomials in  $x_{1,1} \mathbb{R}\langle x_{i,j} \mid i \in [d], j \in [k] \rangle_{=t}$ . It can be seen that this set is a module for  $G := S_{d-1} \times (S_d \wr S_{k-1})$ , where  $S_{d-1}$  permutes the indices  $2, \dots, d$  corresponding to  $k = 1$  (i.e., the basis elements in the first basis), and where  $S_d \wr S_{k-1}$  acts on the variables  $x_{i,j}$  with  $i \in [d], j \in \{2, \dots, k\}$ . We show in Section 6.4 that we can obtain a representative set for this case from Eq. (6) in combination with already derived representative sets for  $S_{d-1}$ -modules (cf. Sec. 4) and  $S_d \wr S_{k-1}$ -modules (cf. Sec. 6).

## 4 Representative set for the action of $S_k$ on $[k]^t$

Here we give a representative set for the action of  $S_k$  on homogeneous degree- $t$  polynomials in noncommutative variables  $x_1, \dots, x_k$ . This serves as a first step towards the decomposition of the  $S_d \wr S_k$ -invariant

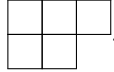
<sup>5</sup>Equivalently, the wreath product  $S_d \wr S_k$  is the semidirect product  $(S_d)^k \rtimes_\phi S_k$  where the homomorphism  $\phi : S_k \rightarrow \text{Aut}(S_d)^k$  comes from the natural action of  $S_k$  on  $(S_d)^k$ , i.e., we have  $\phi(\beta)(\eta) := \tau * \eta = (\eta_{\tau^{-1}(1)}, \dots, \eta_{\tau^{-1}(k)})$ , for  $\beta \in S_k$  and  $\eta \in (S_d)^k$ .

SDPs mentioned above in two ways. First, one can obtain  $S_k$ -invariant relaxations of  $\text{sdp}(d, k, t)$  by only considering polynomials in the variables  $x_{1,j}$  for  $j \in [k]$ . The representative set we describe here allows one to symmetry reduce such SDPs. These relaxations are sometimes sufficient to detect non-existence of MUBs, see Section 8. Second, the construction of a representative set for the  $S_d \wr S_k$ -action on  $([d] \times [k])^t$  builds on the representation theory of the symmetric group. The representative set we construct here applies more broadly to polynomial optimization problems in noncommutative variables  $x_1, \dots, x_k$  that are  $S_k$ -invariant.

We first provide the necessary preliminaries about the representation theory of the symmetric group. For a more detailed overview we refer the reader to, e.g., Sagan [Sag01] (whose notation we follow). In Section 4.2 we then construct a representative set for the action of  $S_k$  on  $[k]^t$ . In Section 4.3 we conclude this preliminary section with an example that illustrates the representation theory in the language of polynomials: we show how to apply the theory to the case of homogeneous quadratic polynomials in three variables ( $k = 3, t = 2$ ).

#### 4.1 Preliminaries on the representation theory of $S_k$

**Notation.** Let  $k \in \mathbb{N}$ . A *composition*  $\mathbf{k}$  of  $k$  is a sequence  $\mathbf{k} = (k_1, k_2, \dots, k_h)$  of nonnegative integers for which  $\sum_{i=1}^h k_i = k$ . A *partition*  $\lambda$  of  $k$ , denoted  $\lambda \vdash k$ , is a nonincreasing sequence  $\lambda = (\lambda_1, \lambda_2, \dots, \lambda_h)$  of positive integers for which  $\sum_{i=1}^h \lambda_i = k$ . We call  $h$  the *height* of  $\lambda$ , denoted  $\text{height}(\lambda)$ . The *shape* or *Ferrers diagram* of  $\lambda$  is an array containing  $k$  cells divided in  $\text{height}(\lambda)$  rows such that the  $i$ th row has  $\lambda_i$  cells. As an example, the shape of  $(3, 2) \vdash 5$  is



A *generalized Young tableau of shape*  $\lambda$  is an array  $\tau$  of shape  $\lambda \vdash k$  with the cells filled with positive integers. For brevity, we simply call  $\tau$  a *tableau*. The integers appearing in  $\tau$  are called its *content*. The content defines a composition  $\mu = (n_1, n_2, \dots, n_\ell)$  of  $k$  where  $n_i$  is the number of repetitions of  $i$  in  $\tau$  and  $\ell$  is the largest integer appearing in  $\tau$ . By concatenating its rows, the tableau  $\tau$  defines a  $k$ -dimensional vector,  $\text{vec}(\tau) \in [\ell]^k$ , and therefore we may view  $\tau$  as a function from  $[k]$  to  $[\ell]$  (when its shape is clear). We can (equivalently) express the numbers  $n_i$  in terms of the function  $\tau : [k] \rightarrow [\ell]$  as  $|\tau^{-1}(i)| = n_i$  for all  $i \in [\ell]$ . Continuing the above example, we can fill the shape  $(3, 2) \vdash 5$  with the integers 1, 2, 3, 4, 5 to obtain a (generalized Young) tableau  $\tau$  that we can express as an array, a row-vector, or a function

$$\tau = \begin{array}{|c|c|c|} \hline 1 & 4 & 2 \\ \hline 3 & 5 & \\ \hline \end{array}, \quad \text{vec}(\tau) = (1, 4, 2, 3, 5) \in [5]^5, \quad \begin{array}{c|ccccc} i & 1 & 2 & 3 & 4 & 5 \\ \hline \tau(i) & 1 & 4 & 2 & 3 & 5 \end{array},$$

its content defines the composition  $(1, 1, 1, 1, 1)$ , which we abbreviate as  $(1^5)$ . Two generalized Young tableaux  $\tau, \tau'$  of the same shape are *row-equivalent*, denoted  $\tau \sim \tau'$ , if tableau  $\tau'$  can be obtained from  $\tau$  by permuting its rows. Given a generalized Young tableau  $\tau$ , we define the corresponding *tabloid*  $\{\tau\}$  as  $\{\tau\} = \{\tau' : \tau' \sim \tau\}$ . The tabloid corresponding to the above example is

$$\{\tau\} = \frac{\overline{1 \ 2 \ 4}}{\overline{3 \ 5}}. \quad (8)$$

For tabloids we use only horizontal lines to indicate that the order within a row does not matter. By convention we display the elements in a row of a tabloid in non-decreasing order. Given a tableau  $\tau$  of shape  $\lambda \vdash k$  with content  $(1^k)$ , we let  $C_\tau$  be its *column stabilizer*, i.e., the subgroup of  $S_k$  that leaves the content of columns invariant. The column stabilizer of our example  $\tau$  is  $C_\tau = S_{\{1,3\}} \times S_{\{4,5\}} \times S_{\{2\}}$ .

A generalized Young tableau is *semistandard* if its rows are (weakly) increasing and its columns are strictly increasing. We let  $\hat{T}_{\lambda\mu}$  be the set of tableaux of shape  $\lambda$  and content  $\mu$  and we let  $T_{\lambda\mu}$  be its subset of semistandard tableaux. We often use the content

$$\mu_r := (k - r, \underbrace{1, \dots, 1}_{r \text{ times}}),$$

where the integer  $k$  is clear from context. Continuing our example, when  $\mu = (3, 2)$  the set of semistandard Young tableaux is empty when the height of  $\lambda$  is at least 3 (since we only have two distinct elements

with which to fill the first column). A complete list of semistandard Young tableaux for  $\mu = (3, 2)$  thus corresponds to the three partitions  $\lambda = (5)$ ,  $(4, 1)$ , and  $(3, 2)$ :

$$\lambda = (5) : \begin{array}{|c|c|c|c|c|} \hline 1 & 1 & 1 & 2 & 2 \\ \hline \end{array}, \quad \lambda = (4, 1) : \begin{array}{|c|c|c|c|} \hline 1 & 1 & 1 & 2 \\ \hline 2 & & & \\ \hline \end{array}, \quad \lambda = (3, 2) : \begin{array}{|c|c|c|} \hline 1 & 1 & 1 \\ \hline 2 & 2 & \\ \hline \end{array}. \quad (9)$$

**Permutation module and Specht modules.** Two important  $S_k$ -modules are permutation modules and Specht modules. Let  $\lambda \vdash k$  and consider tableaux with content  $(1^k) = \{1, 2, \dots, k\}$ . The *permutation module*  $M^\lambda$  consists of the vector space of tabloids of shape  $\lambda$  with content  $(1^k)$ . The action of  $S_k$  on  $M^\lambda$  is defined through its action on tableaux. A permutation  $\pi \in S_k$  acts on a tableau  $\tau$  as  $(\pi\tau)(i) = \pi(\tau(i))$ , this induces an action on tabloids:  $\pi\{\tau\} = \{\pi\tau\}$ . For example, for the permutation  $\pi = (1\ 3)$  and the tabloid  $\tau$  from Eq. (8) we have

$$\pi\{\tau\} = (1\ 3) \frac{\overline{1\ 2\ 4}}{\underline{3\ 5}} = \frac{\overline{2\ 3\ 4}}{\underline{1\ 5}}.$$

A linear combination of tabloids is called a *polytabloid* and the Specht modules are defined in terms of special polytabloids. Given a tableau  $\tau$  of shape  $\lambda$  with content  $(1^k)$ , let  $\kappa_\tau = \sum_{\pi \in C_\tau} \text{sign}(\pi)\pi$  and define the polytabloid  $e_\tau = \kappa_\tau\{\tau\}$ , that is,

$$e_\tau = \sum_{\pi \in C_\tau} \text{sign}(\pi)\pi\{\tau\}.$$

The *Specht module*  $S^\lambda$  is the submodule of  $M^\lambda$  spanned by the polytabloids  $e_\tau$  where  $\tau \in T_{\lambda, (1^k)}$ . The Specht module is a cyclic module and hence it is generated by any of the polytabloids  $e_\tau$ . From now on we will use as (*canonical*) *generating element* of  $S^\lambda$  the polytabloid  $e_t$  corresponding to the tableau  $t$  that satisfies  $t(i) = i$  for  $i \in [k]$ . The Specht modules are the irreducible modules of  $S_k$ .

**Decomposition of a permutation module into Specht modules.** We next give the decomposition of a permutation module  $M^\mu$  into Specht modules (see, e.g., [Sag01]). Given a semistandard tableau  $\tau \in T_{\lambda\mu}$  and a tabloid  $\{t'\}$  of shape  $\lambda$  with content  $(1^k)$ , we define the element<sup>6</sup>

$$\tau \cdot \{t'\} := \sum_{\tau' \sim \tau} \{\tau' * t'\} \in M^\mu$$

of shape  $\mu$  and content  $(1^k)$  by letting the  $a$ -th row of the tabloid  $\{\tau' * t'\}$  contain all indices  $i \in [k]$  for which  $\tau'((t')^{-1}(i)) = a$  (for  $a = 1, \dots, \text{height}(\mu)$ ). Note that  $\{\tau' * t'\}$  is well defined: the tableau  $t'$  has content  $(1^k)$ , the tableau  $\tau'$  has content  $\mu$  so there are exactly  $\mu_a$  elements  $i \in [k]$  for which  $\tau'((t')^{-1}(i)) = a$ . Moreover, the polytabloid  $\tau \cdot \{t'\}$  does not depend on the choice of representative of the equivalence class  $\{t'\}$  and hence it is also well defined.<sup>7</sup>

For the (unique) semistandard tableau  $\tau$  of shape  $(4, 1)$  with content  $(3, 2)$  and the tableau  $t$  of shape  $(4, 1)$  and content  $(1^5)$  corresponding to  $t(i) = i$ , we have

$$\{\tau * t\} = \left\{ \begin{array}{|c|c|c|c|} \hline 1 & 1 & 1 & 2 \\ \hline 2 & & & \\ \hline \end{array} * \begin{array}{|c|c|c|c|} \hline 1 & 2 & 3 & 4 \\ \hline 5 & & & \\ \hline \end{array} \right\} = \frac{\overline{1\ 2\ 3}}{\underline{4\ 5}},$$

and

$$\tau \cdot \{t\} = \begin{array}{|c|c|c|c|} \hline 1 & 1 & 1 & 2 \\ \hline 2 & & & \\ \hline \end{array} \cdot \frac{\overline{1\ 2\ 3\ 4}}{\underline{5}} = \frac{\overline{1\ 2\ 3}}{\underline{4\ 5}} + \frac{\overline{1\ 2\ 4}}{\underline{3\ 5}} + \frac{\overline{1\ 3\ 4}}{\underline{2\ 5}} + \frac{\overline{2\ 3\ 4}}{\underline{1\ 5}}.$$

<sup>6</sup>Note that we deviate here from the notation of [Sag01] where  $\theta_\tau$  is used for the map from  $S^\lambda$  to  $\mathbb{C}[\widetilde{T}_{\lambda\mu}]$ . The latter is isomorphic to  $M^\mu$  and our  $\tau \cdot \{t'\}$  corresponds to the composition of  $\theta_\tau$  and this isomorphism, applied to  $\{t'\}$ .

<sup>7</sup>To see this, suppose that  $t \sim t'$ , i.e.,  $t' = t \circ \pi$ , where  $\pi \in S_{\lambda_1} \times S_{\lambda_2} \times \dots \times S_{\lambda_{\text{height}(\lambda)}}$ . Then  $\{\tau * t'\}$  has on the  $a$ th row the indices  $i \in [k]$  for which  $a = \tau((t')^{-1}(i)) = \tau(\pi^{-1}t^{-1}(i)) = \tau'(t^{-1}(i))$ , where  $\tau' = \tau \circ \pi^{-1} \sim \tau$ , and hence  $\{\tau * t'\} = \{\tau' * t\}$ . To conclude the argument observe that  $\pi$  simply permutes the elements of  $\{\tau' : \tau' \sim \tau\}$ .

The action of  $\tau$  on tabloids is extended linearly to polytabloids  $e_t$  (which are linear combinations of tabloids  $\{t'\}$ ) and then to all of  $S^\lambda$ . In this way,  $\tau \cdot S^\lambda$  becomes a submodule of  $M^\mu$ . The decomposition of a permutation module  $M^\mu$  into Specht modules is now given as (see, e.g., [Sag01]):

$$M^\mu = \bigoplus_{\lambda \vdash k} \left( \bigoplus_{\tau \in T_{\lambda\mu}} \tau \cdot S^\lambda \right). \quad (10)$$

From Eq. (9) it follows that  $M^{(3,2)}$  decomposes as a direct sum of three Specht modules:

$$M^{(3,2)} = \begin{array}{|c|c|c|c|c|} \hline 1 & 1 & 1 & 2 & 2 \\ \hline \end{array} \cdot S^{(5)} \oplus \begin{array}{|c|c|c|c|} \hline 1 & 1 & 1 & 2 \\ \hline 2 & & & \end{array} \cdot S^{(4,1)} \oplus \begin{array}{|c|c|c|} \hline 1 & 1 & 1 \\ \hline 2 & 2 & \end{array} \cdot S^{(3,2)}.$$

The generating element of  $\tau \cdot S^\lambda$  in  $M^\mu$  is obtained by acting with  $\tau$  on the generating element  $e_t$  of  $S^\lambda$ . That is, we use as generating element of the  $\tau$ -th copy of  $S^\lambda$  the vector

$$v_\tau := \tau \cdot e_t = \tau \cdot \sum_{c \in C_t} \text{sign}(c) \{ct\} = \sum_{\tau' \sim \tau} \sum_{c \in C_t} \text{sign}(c) \{\tau' * (ct)\}.$$

## 4.2 Representative set

We now consider the setting of noncommutative polynomials in variables  $x_1, \dots, x_k$  with symmetry coming from  $S_k$ . Let  $t \in \mathbb{N}$  and let  $V := \mathbb{C}^{[k]^t}$ . Let  $S_k$  act naturally on  $[k]^t$  and hence on  $V$ . We obtain a first decomposition of  $V$  by restricting to  $S_k$ -orbits. The elements of  $[k]^t/S_k$  correspond bijectively to *set partitions*  $P = \{P_1, P_2, \dots, P_{|P|}\}$  of  $[t]$  in at most  $k$  parts (i.e.,  $|P| \leq k$  and  $\bigsqcup_{i=1}^{|P|} P_i = [t]$ ). Each  $P_i$  represents a set of indices that are assigned the same  $j \in [k]$ , and distinct  $P_i$  and  $P_{i'}$  are assigned distinct  $j, j' \in [k]$  respectively. Throughout we let  $r = |P|$  denote the number of sets in the set partition  $P$ . We then have a first decomposition

$$V = \bigoplus_{P \in [k]^t/S_k} V_P \quad (11)$$

where  $V_P$  is the vector space spanned by  $w \in P$ . For  $r \in [k]$ , recall that  $\mu_r \vdash k$  is the partition  $\mu_r := (k-r, 1, \dots, 1)$ . Then, for a  $P \in [k]^t/S_k$  with  $P = \{P_1, \dots, P_r\}$  we have a natural bijection between  $w \in P$  and tabloids of shape  $\mu_r$  and content  $(1^k)$ :

$$w \xrightarrow{\phi_P} \begin{array}{c} \overline{i \ \cdots \ j} \\ w(1) \\ \overline{w(2)} \\ \vdots \\ \overline{w(r)} \end{array}$$

here the first row contains all elements in  $[k] \setminus \{w(1), \dots, w(r)\}$ . This bijection respects the action of  $S_k$ , and therefore we see that  $V_P$  is isomorphic to the permutation module  $M^{\mu_r}$ :  $V_P \cong M^{\mu_r}$ . Combining the decompositions in Eqs. (10) and (11) gives the decomposition of  $V$  into irreducible  $S_k$ -modules:

$$V = \bigoplus_{P \in [k]^t/S_k} \phi_P^{-1} M^{\mu_r} = \bigoplus_{\lambda \vdash k} \left( \bigoplus_{P \in [k]^t/S_k} \bigoplus_{\tau \in T_{\lambda\mu_r}} \phi_P^{-1}(\tau \cdot S^\lambda) \right).$$

Note that in the above equation we allow  $T_{\lambda\mu_r}$  to be empty: it is non-empty only if there exists a semistandard tableau of shape  $\lambda$  and content  $\mu_r$ . Given the shape of  $\mu_r$ ,  $T_{\lambda\mu_r}$  is non-empty if the first row of  $\lambda$  has size at least  $k-r$  and the height of  $\lambda$  is at most  $r+1$ . This decomposition of  $V$  gives rise to a representative set for the action of  $S_k$  on  $V$ . Indeed, for a partition  $\lambda \vdash k$ , define

$$U_\lambda := (u_{\tau,P} \mid P \in [k]^t/S_k, \tau \in T_{\lambda\mu_r})$$

where

$$u_{\tau,P} := \phi_P^{-1}(v_\tau) = \sum_{\tau' \sim \tau} \sum_{c \in C_t} \text{sgn}(c) \phi_P^{-1}(\{\tau' * ct\}). \quad (12)$$

Then the set  $\{U_\lambda \mid \lambda \vdash k, \text{height}(\lambda) \leq \min\{k, t+1\}\}$  is representative for the action of  $S_k$  on  $V = \mathbb{C}^{[k]^t}$ . Indeed, we have shown above that the corresponding irreducible submodules decompose  $V$ , moreover, by construction the  $(\tau, P)$ -th copy of  $S^\lambda$  is isomorphic to  $S^\lambda$  and its generating element is chosen according to this isomorphism. This shows that the elements of  $U_\lambda$  satisfy the conditions of Definition 2.1.

**The dimension of  $\text{End}_{S_k}(\mathbb{C}^{[k]^t})$ .** Recall that the sum of the squares of the block sizes equals  $\dim(\text{End}_{S_k}(\mathbb{C}^{[k]^t}))$ . One can show that the latter equals the number of orbits of pairs  $(m_1, m_2)$  where  $m_1$  and  $m_2$  are non-commutative monomials of degree exactly  $t$ . Orbits of pairs  $(m_1, m_2)$  naturally correspond to orbits of length- $2t$  monomials  $m$  via  $m = m_1^* m_2$ . Hence the dimension of the above space of  $S_k$ -invariant endomorphisms equals the dimension of the space of  $S_k$ -invariant noncommutative polynomials of degree exactly  $2t$ . As we have seen before (cf.  $V_P$ ), this equals the number of set partitions of  $[2t]$  in at most  $k$  parts. When  $k \geq 2t$ , this number is independent of  $k$  and simply becomes the number of set partitions of a set of  $2t$  elements. The number of set partitions of a set of  $t$  elements is known as the  $t$ -th *Bell number*. The sequence of Bell numbers  $\{B_t\}_{t \in \mathbb{Z}_{\geq 0}}$  is known in the online encyclopedia of integer sequences as sequence A000110; its first ten elements are 1, 1, 2, 5, 15, 52, 203, 877, 4140, 21147. The sequence can be generated via the recurrence relation  $B_t = \sum_{j=0}^{t-1} \binom{t-1}{j} B_j$ . We emphasize that for  $k \geq 2t$  the sum of the squares of the block sizes of the symmetry reduced SDP equals  $B_{2t}$  and is thus independent of  $k$ .

**Computing the coefficients of the block-diagonalized SDP.** To compute the coefficients of the block-diagonalized semidefinite program we may use the following formula. Fix a partition  $\lambda \vdash k$  and  $u_{\tau, P}, u_{\sigma, Q} \in U_\lambda$ , then for any  $A \in \text{End}_{S_k}(V)$  we have,

$$\begin{aligned} \langle u_{\tau, P}, A u_{\sigma, Q} \rangle &= \sum_{\substack{\tau' \sim \tau, \\ \sigma' \sim \sigma}} \sum_{c, c' \in C_t} \text{sgn}(cc') A_{\phi_P^{-1}(\tau' * \{ct\}), \phi_Q^{-1}(\sigma' * \{c't\})} \\ &= \sum_{\substack{\tau' \sim \tau, \\ \sigma' \sim \sigma}} \sum_{c, c' \in C_t} \text{sgn}(cc') A_{\phi_P^{-1}(\tau' * \{t\}), \phi_Q^{-1}(\sigma' * \{c^{-1}c't\})} = |C_t| \sum_{\substack{\tau' \sim \tau, \\ \sigma' \sim \sigma}} \sum_{c \in C_t} \text{sgn}(c) A_{\phi_P^{-1}(\tau' * \{t\}), \phi_Q^{-1}(\sigma' * \{ct\})} \end{aligned} \quad (13)$$

where in the last equality we use the group structure of  $C_t$ .

At first glance, even for fixed level  $t$ , Eq. (13) could take time exponential in  $k$  to evaluate since the number of terms can be exponentially large (take for instance  $\lambda = (t^k/t)$ ). However, one can show that it is possible to compute these inner products in time polynomial in  $k$  (for fixed level  $t$ ). Define commutative variables  $z_{i,j}$  for  $i \in [r_P + 1], j \in [r_Q + 1]$ . Let  $f_{\tau, \sigma}$  be the polynomial

$$f_{\tau, \sigma}(z) = \sum_{\substack{\tau' \sim \tau, \\ \sigma' \sim \sigma}} \sum_{c, c' \in C_\lambda} \text{sgn}(cc') \prod_{y \in [k]} z_{c \cdot \tau'(y), c' \cdot \sigma'(y)}.$$

Consider a monomial  $m = \prod_{y \in [k]} z_{i_y, j_y}$ . A variable  $z_{i,j}$  for  $i, j > 1$  appears in  $m$  if  $P_{i-1}$  and  $Q_{j-1}$  are assigned the same element in  $[k]$ , and hence  $m$  represents an  $S_k$ -orbit of  $[k]^t \times [k]^t$ . The coefficient of  $m$  in  $f_{\tau, \sigma}$  thus counts the number of  $c, c' \in C_t$  and  $\tau' \sim \tau, \sigma' \sim \sigma$  for which  $(\phi_P^{-1}(\tau' * \{ct\}), \phi_Q^{-1}(\sigma' * \{c't\}))$  are  $S_k$ -equivalent. It was shown in [Gij09, Sec. 3] that  $f_{\tau, \sigma}$  can be expressed as a linear combination of monomials in time polynomial in  $k$ , assuming the height of  $\tau, \sigma$  is fixed (which holds in our case since  $\max\{r_P + 1, r_Q + 1\} \leq t + 1$ ). See also [LPS17, Prop. 3] for a different proof.

### 4.3 An example: homogeneous quadratic polynomials

To illustrate the concepts developed in the previous sections, we show how to use representation theory to block-diagonalize moment matrices indexed by homogenous quadratic polynomials in three variables that are invariant under the action of  $S_3$ . We express the concepts in the language of polynomials. (This example corresponds to the case  $k = 3$  and  $t = 2$ .)

For any  $L \in \mathbb{R}\langle x_1, x_2, x_3 \rangle_{=4}^*$ , we write  $M(L)$  for the moment matrix whose rows and columns are indexed by elements of  $\langle x_1, x_2, x_3 \rangle_{=2}$ . We show how to block-diagonalize the algebra of such matrices  $M(L)$  that are invariant under the simultaneous action of  $S_3$  on their rows and columns. We can identify this algebra with  $(\mathbb{C}^{[3]^2 \times [3]^2})^{S_3} = \text{End}_{S_3}(\mathbb{C}^{[3]^2})$ , the algebra of  $[3]^2 \times [3]^2$ -matrices that are invariant under the same action. As discussed in Section 2.3, block-diagonalizing this algebra amounts to decomposing

the  $S_3$ -module  $V := \mathbb{C}^{[3]^2}$  into irreducible modules. This module can be identified with the space of trivariate homogeneous quadratics

$$\mathbb{C}^{[3]^2} \simeq \mathbb{C}\langle x_1, x_2, x_3 \rangle_{=2}$$

where the group  $S_3$  acts on this space by permuting the indices of  $x_1, x_2, x_3$ .

We now follow the recipe provided in Section 4.2 to obtain this decomposition. The first step is to decompose  $V$  into orbits of  $S_3$ . A permutation  $\sigma \in S_3$  maps a monomial  $x_i x_j$  to  $x_{\sigma(i)} x_{\sigma(j)}$ . It is then not hard to see that we have only two orbits: one formed by monomials with  $i = j$  and one where  $i \neq j$ . This corresponds to Eq. (11) from the previous section: we write

$$V = \mathbb{C}^{[3]^2} \cong \mathbb{C}\langle x_1, x_2, x_3 \rangle_2 = V_{11} \oplus V_{12},$$

where  $V_{11} = \text{span}\{x_i^2 : i \in [3]\}$  and  $V_{12} = \text{span}\{x_i x_j : i, j \in [3] \text{ with } i \neq j\}$ .

In the language of the previous section, the space  $V_{11}$  corresponds to the partition  $P = \{\{1, 2\}\}$  of  $[t] = [2]$ , or the  $S_3$  orbit of  $(1, 1) \in [k]^t$ . We have  $V_{11} \cong M^{\mu_1}$  where the natural bijection between elements in this orbit and tabloids of shape  $\mu_1 = (2, 1) \vdash 3$  and content  $(1^3)$  is as follows:

$$x_1^2 \leftrightarrow \overline{\frac{2 \quad 3}{1}}, \quad x_2^2 \leftrightarrow \overline{\frac{1 \quad 3}{2}}, \quad x_3^2 \leftrightarrow \overline{\frac{1 \quad 2}{3}}.$$

Similarly, the space  $V_{12}$  corresponds to the partition  $P = \{\{1\}, \{2\}\}$  of  $[t] = [2]$ , or the  $S_3$  orbit of  $(1, 2) \in [k]^t$ . We have  $V_{12} \cong M^{\mu_2}$  where the bijection between elements in this orbit and tabloids of shape  $\mu_2 = (1, 1, 1) \vdash 3$  and content  $(1^3)$  is given by:

$$x_i x_j \leftrightarrow \overline{\frac{k}{\frac{i}{j}}}, \quad \text{for } i \neq j \in [3] \text{ and } k \text{ the remaining element } \neq i, j \text{ in } [3].$$

The advantage of identifying the orbits with these permutation modules is that we can use the representation theory of the symmetric group to further decompose  $V_{11}$  and  $V_{12}$  into irreducible modules. Here we translate the theory to the language of polynomials. The irreducible modules of  $S_k$  are indexed by all partitions  $\lambda$  of  $k$ , which for the case  $k = 3$  amounts to the partitions  $(3)$ ,  $(2, 1)$  and  $(1, 1, 1)$ . The blocks of the block-diagonalized algebra will be labeled by these partitions and we can thus already note that there will be three blocks.

As a concrete example, we compute one of the representative elements that correspond to the decomposition of  $V_{11}$ . Following Eq. (10), the space  $V_{11}$  decomposes as

$$\bigoplus_{\lambda \vdash 3} \bigoplus_{\tau \in T_{\lambda, \mu_1}} \phi_{11}^{-1}(\tau \cdot S^\lambda).$$

This decomposition is labeled by partitions  $\lambda \vdash 3$  and semistandard tableaux  $\tau \in T_{\lambda, \mu_1}$ . In this small example this reduces to a decomposition into two parts: there are unique semistandard tableaux with content  $\mu_1 = (2, 1)$  for the partitions  $(3)$  and  $(2, 1)$ :

$$\lambda = (3) : \begin{array}{|c|c|c|} \hline 1 & 1 & 2 \\ \hline \end{array}; \quad \lambda = (2, 1) : \begin{array}{|c|c|} \hline 1 & 1 \\ \hline 2 & \\ \hline \end{array}.$$

There is no semistandard tableau of shape  $(1, 1, 1)$  with content  $(2, 1)$ . In the language of the previous section,  $V_{11}$  corresponds to the partition  $P = \{\{1, 2\}\}$ . We show how to compute the representative element  $u_{\tau, P}$  for this  $P$  and the semistandard tableau corresponding to the partition  $(2, 1)$ . We have

$$\begin{aligned} u_{\tau, P} &= \sum_{\tau' \sim \tau} \sum_{c \in C_t} \text{sgn}(c) \phi_P^{-1}(\tau' * \{ct\}) \\ &= \phi_{11}^{-1}(\tau * \{t\}) + \text{sgn}((13)) \phi_{11}^{-1}(\tau * \{(13)t\}) \\ &= \phi_{11}^{-1} \left( \overline{\frac{1 \quad 2}{3}} \right) - \phi_{11}^{-1} \left( \overline{\frac{3 \quad 2}{1}} \right) = x_3 x_3 - x_1 x_1, \end{aligned}$$

where for the second equality we use that there is a unique tableau that is row-equivalent to  $\tau$  (namely  $\tau$  itself) and the column-stabilizer corresponding to this shape (and its standard labeling  $t$ ) consists of the identity permutation and the permutation  $(13)$ . For completeness we mention that the other representative element corresponding to  $V_{11}$ , the one associated to  $\tau = \begin{array}{|c|c|c|} \hline 1 & 1 & 2 \\ \hline \end{array}$ , is  $x_1x_1 + x_2x_2 + x_3x_3$ .

For the space  $V_{12}$  one can do the same, the space corresponds to the partition  $P = \{\{1\}, \{2\}\}$  of  $[t] = [2]$ , or the  $S_3$  orbit of  $(1, 2) \in [k]^t$ . One computes representative elements  $u_{\tau, P}$  for each of the  $\phi_P^{-1}(\tau \cdot S^\lambda)$  with  $P = \{\{1\}, \{2\}\}$  via the procedure illustrated above where we now have the following semistandard tableaux for the three choices of partitions  $\lambda$ :

$$\lambda = (3) : \begin{array}{|c|c|c|} \hline 1 & 2 & 3 \\ \hline \end{array} ; \quad \lambda = (2, 1) : \begin{array}{|c|c|} \hline 1 & 2 \\ \hline 3 & \\ \hline \end{array}, \quad \begin{array}{|c|c|} \hline 1 & 3 \\ \hline 2 & \\ \hline \end{array} ; \quad \lambda = (1, 1, 1) : \begin{array}{|c|} \hline 1 \\ \hline 2 \\ \hline 3 \\ \hline \end{array}.$$

A representative set for the action of  $S_3$  on  $\mathbb{C}^{[3]^2}$  is then denoted by  $\{U_\lambda \mid \lambda \vdash 3, \text{height}(\lambda) \leq 3\}$ , and it is obtained by grouping the representative elements for  $V_{11}$  and  $V_{12}$  according to their partition  $\lambda$ . For example, both  $V_{11}$  and  $V_{12}$  contain a single irreducible sub-module that is isomorphic to  $S^{(3)}$  and thus  $U_{(3)}$  contains two elements; these correspond to the polynomials

$$\sum_{i \in [3]} x_i x_i \text{ and } \sum_{\substack{(i,j) \in [3] \\ i \neq j}} x_i x_j.$$

Formally, we can view the representative set as a collection of matrices by identifying a polynomial with its (column) vector of coefficients;  $U_{(3)}$  is a  $9 \times 2$  matrix. The remaining two matrices,  $U_{(2,1)}$  and  $U_{(1,1,1)}$  have columns corresponding to the following polynomials:

$$\begin{aligned} U_{(2,1)} : & \quad x_3x_3 - x_1x_1, \quad x_2x_3 - x_2x_1 + x_1x_3 - x_3x_1, \quad x_3x_2 - x_1x_2 + x_3x_1 - x_1x_3, \\ U_{(1,1,1)} : & \quad x_1x_2 + x_2x_3 + x_3x_1 - x_2x_1 - x_1x_3 - x_3x_2. \end{aligned}$$

Having computed the representative set, we finally obtain a block-diagonalization of  $(\mathbb{C}^{[3]^2 \times [3]^2})^{S_3}$  by computing (cf. Proposition 2.2 and Eq. (12))

$$U_{(3)}^\top M(L) U_{(3)} \oplus U_{(2,1)}^\top M(L) U_{(2,1)} \oplus U_{(1,1,1)}^\top M(L) U_{(1,1,1)}.$$

The matrices  $U$  technically contain coefficient vectors of polynomials and the moment matrix  $M(L)$  contains the values of  $L$  on monomials, but by viewing the columns of each representative matrix  $U_\lambda$  as a polynomial, we can compute the  $\ell j$ -th entry  $U_{\lambda, \ell}^\top M(L) U_{\lambda, j}$  of the block corresponding to  $\lambda$  by expanding  $L(U_{\lambda, \ell}^* U_{\lambda, j})$ . Here  $U_{\lambda, j}$  and  $U_{\lambda, \ell}$  are the polynomials corresponding to columns  $j$  and  $\ell$  of  $U_\lambda$ , respectively. As an example, we display the  $(1, 2)$ -entry of the block corresponding to  $U_{(3)}$ :

$$\begin{aligned} U_{(3), 1}^\top M(L) U_{(3), 2} &= L\left(U_{(3), 1}^* U_{(3), 2}\right) = L\left(\left(\sum_{i \in [3]} x_i x_i\right)^* \left(\sum_{\substack{(i,j) \in [3] \\ i \neq j}} x_i x_j\right)\right) \\ &= 6(L(x_1x_1x_1x_2) + L(x_1x_1x_2x_1) + L(x_1x_1x_2x_3)), \end{aligned}$$

where for the last equality we use that  $L$  is constant on orbits. This allows us to express the entry as a linear combination of the linear functional evaluated at orbit representatives (here we use as orbit representative the lexicographically smallest element in the  $S_3$ -orbit).<sup>8</sup>

## 5 Preliminaries on the representation theory of $S_d \wr S_k$

The irreducible modules of  $S_d \wr S_k$  are well known, see for example [Ker71, Mac80]. Here we collect the necessary definitions and constructions that lead to the irreducible modules for the wreath product of  $S_d \wr S_k$ .

<sup>8</sup>For completeness we mention that the case  $t = 2$  and general  $k$  was studied in [LPS17, Sec. 3.1, App. 2], where a representative set for the action of  $S_k$  on  $[k]^2$  together with the explicit formulas in the corresponding block-diagonalization are given.



**Notation.** In the representation theory of  $S_k$  partitions and compositions play a large role, for the wreath product we moreover need the notion of *multipartitions*. Let  $\ell \in \mathbb{N}$ , then an  $\ell$ -multipartition of  $k$  is an  $\ell$ -tuple  $\underline{\Lambda} = (\Lambda^1, \dots, \Lambda^\ell)$  such that each  $\Lambda^a$  is a partition and  $\sum_{a \in [\ell]} |\Lambda^a| = k$ . We write  $\underline{\Lambda} \vdash k$  and, throughout, underline each symbol that corresponds to an  $\ell$ -multipartition. To an  $\ell$ -multipartition  $\underline{\Lambda}$  we associate the  $\ell$ -composition  $|\underline{\Lambda}| = (|\Lambda^1|, \dots, |\Lambda^\ell|)$  of  $k$ .

**Induction.** Two natural modules of  $S_d \wr S_k$  involve the notion of induction which we recall here for general groups for convenience and to fix notation. Let  $G$  be a group and  $H$  be a subgroup of  $G$ . If  $V$  is a module of  $H$ , we define the *induced module*  $V \uparrow_H^G$  as follows. Let  $R := \{r_1, \dots, r_s\}$  be a set consisting of representatives of the (left) cosets of  $H$  in  $G$ , so  $|R| = [G : H]$ . Then the elements of  $V \uparrow_H^G$  are sums of the form  $\alpha_1(r_1, v_1) + \dots + \alpha_s(r_s, v_s)$ , for  $v_1, \dots, v_s \in V$  and scalars  $\alpha_1, \dots, \alpha_s \in \mathbb{C}$ . An element  $g \in G$  acts on an element  $(r_i, v)$  via  $g(r_i, v) = (r_j, hv)$ , where  $r_j \in R$  and  $h \in H$  are the unique elements such that  $gr_i = r_j h$ . This action is extended linearly to  $V \uparrow_H^G$ .

**Basic constructions of modules.** Modules of  $S_d$  and  $S_k$  can be used to construct modules for  $S_d \wr S_k$ . We list some essential constructions. Let  $X$  be an  $S_d$ -module. We define an  $S_d \wr S_k$ -module  $X^{\boxtimes k}$  as follows: as vector space it equals  $X^{\otimes k}$  and the action of an element  $(\alpha, \beta) = (\alpha_1, \dots, \alpha_k; \beta) \in S_d \wr S_k$  on a rank-1 tensor  $\otimes_{i \in [k]} x_i$  is

$$(\alpha_1, \dots, \alpha_k; \beta) \bigotimes_{i \in [k]} x_i = \bigotimes_{i \in [k]} \alpha_i x_{\beta^{-1}(i)}.$$

A similar construction can be used to create a module for the wreath product between  $S_d$  and a *Young subgroup* of  $S_k$ . A Young subgroup of  $S_k$  associated to an  $\ell$ -composition  $\mathbf{k}$  of  $k$  is the subgroup  $S_{\mathbf{k}} := S_{\{1, \dots, k_1\}} \times \dots \times S_{\{1 + \sum_{a < \ell} k_a, k\}}$  of  $S_k$ . For  $S_d$ -modules  $X_1, \dots, X_\ell$  we define the  $S_d \wr S_{\mathbf{k}}$ -module  $(X_1, \dots, X_\ell)^{\boxtimes \mathbf{k}}$  as follows:

$$(X_1, \dots, X_\ell)^{\boxtimes \mathbf{k}} := X_1^{\boxtimes k_1} \otimes X_2^{\boxtimes k_2} \otimes \dots \otimes X_\ell^{\boxtimes k_\ell},$$

where  $(\alpha, \beta) = (\alpha_1, \dots, \alpha_k, \beta) \in S_d \wr S_{\mathbf{k}}$  acts on an element  $\otimes_{i \in [k]} x_i$  as

$$(\alpha; \beta) \bigotimes_{i \in [k]} x_i = \bigotimes_{i \in [k]} \alpha_i x_{\beta^{-1}(i)}. \quad (14)$$

In what follows, it will be convenient to work with a module that is closely related to the above  $S_d \wr S_{\mathbf{k}}$ -module, but where the tensor legs are permuted. For a tuple  $\mathbf{j} \in [\ell]^k$  we consider the Young subgroup  $S_{\mathbf{j}} := S_{j^{-1}(1)} \times \dots \times S_{j^{-1}(\ell)}$  and we define the  $S_d \wr S_{\mathbf{j}}$ -module

$$(X_1, \dots, X_\ell)^{\boxtimes \mathbf{k}(\mathbf{j})}_{\mathbf{j}}$$

which equals  $\bigotimes_{i \in [k]} X_{j(i)}$  as vector space. The  $S_d \wr S_{\mathbf{j}}$  action is defined by identifying, for each  $a \in [\ell]$ , the module  $(X_1, \dots, X_\ell)^{\boxtimes \mathbf{k}}_{\mathbf{j}}$  restricted to the coordinates for which  $j(i) = a$  with the  $S_d \wr S_{j^{-1}(a)}$ -module  $X_a^{\boxtimes k_a}$ . That is,  $(\alpha, \beta) \in S_d \wr S_{\mathbf{j}}$  acts on an element  $\otimes_{i \in [k]} x_i$  exactly as in (14). The following construction is used to combine  $S_d \wr S_{\mathbf{k}}$ -modules and  $S_k$ -modules.

**Definition 5.1.** Let  $H$  be a subgroup of  $S_k$ ,  $G$  a subgroup of  $S_d$ ,  $Y$  an  $H$ -module, and  $Z$  a  $(G \wr H)$ -module. Then define  $Z \circ Y := Z \otimes Y$  as vector space, with action  $(\alpha, \beta)(x, y) = ((\alpha, \beta)x, \beta y)$ , so that  $Z \circ Y$  is a  $(G \wr H)$ -module.<sup>9</sup>

**Analogues of Specht modules for  $S_d \wr S_k$ .** In what follows, let  $\nu_1, \dots, \nu_\ell \vdash d$  be a complete list of partitions of  $d$ , sorted lexicographically. So  $\ell$  is the number of partitions of  $d$ . For induction, we use  $d \wr k$  as shorthand for  $S_d \wr S_k$  (and similarly for  $d \wr \mathbf{j}$  and  $d \wr |\Lambda|$ ). Using the above constructions, one can define an analogue of Specht modules for the wreath product  $S_d \wr S_k$ .

<sup>9</sup> Alternatively, it holds that  $Z \circ Y = Z \otimes \text{Inf}_H^{G \wr H} Y$ , where the *inflation*  $\text{Inf}_H^{G \wr H} Y$  of  $Y$  from  $H$  to  $G \wr H$  is  $Y$  as vector space, with action  $(\alpha, \beta)y = \beta y$ .

**Definition 5.2.** For an  $\ell$ -multipartition  $\underline{\Lambda}$  of  $k$ , the Specht module  $S^{\underline{\Lambda}}$  is defined as

$$S^{\underline{\Lambda}} := \left[ (S^{\nu_1}, \dots, S^{\nu_\ell})^{\boxtimes |\underline{\Lambda}|} \odot (S^{\Lambda^1} \boxtimes \dots \boxtimes S^{\Lambda^\ell}) \right] \uparrow_{d|\underline{\Lambda}|}^{dk},$$

and for  $\mathbf{j} \in [\ell]^k$  with  $\mathbf{j}^{-1}(a) = |\Lambda^a|$  (for all  $a \in [\ell]$ ) we define the module  $S_{\mathbf{j}}^{\underline{\Lambda}}$  as

$$S_{\mathbf{j}}^{\underline{\Lambda}} := \left[ (S^{\nu_1}, \dots, S^{\nu_\ell})_{\mathbf{j}}^{\boxtimes |\underline{\Lambda}|} \odot (S^{\Lambda^1} \boxtimes \dots \boxtimes S^{\Lambda^\ell}) \right] \uparrow_{d\mathbf{j}}^{dk}.$$

The modules  $S^{\underline{\Lambda}}$  form a complete set of irreducible  $S_d \wr S_k$ -modules (cf. [Mac80, CT03]) and therefore can be used to decompose any (finite-dimensional)  $S_d \wr S_k$ -module. Observe that  $S^{\underline{\Lambda}} = S_{\mathbf{j}}^{\underline{\Lambda}}$  for the  $k$ -tuple  $\mathbf{j}$  for which, for each  $a \in [\ell]$  with  $|\Lambda^a| > 0$ , we have  $\mathbf{j}^{-1}(a) = \{1 + \sum_{j < a} |\Lambda^j|, \dots, \sum_{j \leq a} |\Lambda^j|\}$ . Below in Lemma 5.3 we show that in fact for every  $\mathbf{j}$  with  $|\mathbf{j}^{-1}(a)| = |\Lambda^a|$  we have that  $S^{\underline{\Lambda}}$  and  $S_{\mathbf{j}}^{\underline{\Lambda}}$  are  $S_d \wr S_k$ -isomorphic. We first describe the generating elements of  $S_{\mathbf{j}}^{\underline{\Lambda}}$ .

For  $\mathbf{j} \in [\ell]^k$  the canonical generating element of  $S_{\mathbf{j}}^{\underline{\Lambda}}$  is obtained by combining the generating elements of the respective Specht modules of  $S_d$  and  $S_k$  as follows. We define for  $i \in [k]$  and  $a \in [\ell]$

$$v_i = \kappa_{t_{\mathbf{j}(i)}} \{t_{\mathbf{j}(i)}\}, \quad u_a = \kappa_{t_{\Lambda^a}} \{t_{\Lambda^a}\}$$

where  $t_{\mathbf{j}(i)}$  is the usual fixed tableau of shape  $\nu_{\mathbf{j}(i)}$  and where  $t_{\Lambda^a} : \mathbf{j}^{-1}(a) \rightarrow \mathbf{j}^{-1}(a)$  is the standard tableau of shape  $\Lambda^a$ . Throughout, as coset representatives of  $S_d \wr S_{\mathbf{j}}$  in  $S_d \wr S_k$  we consider the elements  $(\mathbf{id}, b) \in S_d \wr S_k$  for which  $b \in S_k$  is an increasing function on each  $\mathbf{j}^{-1}(a)$ , i.e.,  $b$  is such that if  $i, i' \in \mathbf{j}^{-1}(a)$  with  $i < i'$  then  $b(i) < b(i')$ . The canonical generating element of  $S_{\mathbf{j}}^{\underline{\Lambda}}$  is the vector  $((\mathbf{id}, \mathbf{id}), (\bigotimes_{i \in [k]} v_i) \otimes (\bigotimes_{a \in [\ell]} u_a))$ . To emphasize the difference between  $S_d$ - and  $S_k$ -modules we write

$$((\mathbf{id}, \mathbf{id}), (v_1, \dots, v_k; u_1, \dots, u_\ell)) := ((\mathbf{id}, \mathbf{id}), (\bigotimes_{i \in [k]} v_i) \otimes (\bigotimes_{a \in [\ell]} u_a)).$$

**Lemma 5.3.** Let  $\underline{\Lambda}$  be an  $\ell$ -multipartition of  $k$  and let  $\mathbf{j} \in [\ell]^k$  be such that  $|\mathbf{j}^{-1}(a)| = |\Lambda^a|$  for all  $a \in [\ell]$ . Then the  $S_d \wr S_k$ -module  $S^{\underline{\Lambda}}$  is isomorphic to the  $S_d \wr S_k$ -module  $S_{\mathbf{j}}^{\underline{\Lambda}}$ .

*Proof.* For  $a \in [\ell]$  with  $|\Lambda^a| > 0$ , let  $I_a := \{1 + \sum_{j < a} |\Lambda^j|, \dots, \sum_{j \leq a} |\Lambda^j|\}$ . Let  $\pi \in S_k$  be the permutation that maps the  $t$ -th smallest element in  $I_a$  to the  $t$ -th smallest element in  $\mathbf{j}^{-1}(a)$  for each  $a \in [\ell]$  and  $t \in [|\Lambda^a|]$ . We show this permutation defines an isomorphism between  $S^{\underline{\Lambda}}$  and  $S_{\mathbf{j}}^{\underline{\Lambda}}$ :

$$((\mathbf{id}, b), (v_1, \dots, v_k; u_1, \dots, u_\ell)) \xrightarrow{\phi} ((\mathbf{id}, b\pi^{-1}), (v_{\pi^{-1}(1)}, \dots, v_{\pi^{-1}(k)}; \pi u_1, \dots, \pi u_\ell))$$

Observe that  $(\mathbf{id}, b\pi^{-1})$  is indeed a coset representative of  $S_d \wr S_{\mathbf{j}}$  in  $S_d \wr S_k$ :  $b\pi^{-1} \in S_k$  and for  $i, i' \in \mathbf{j}^{-1}(a)$  with  $i < i'$  we have  $\pi^{-1}(i) < \pi^{-1}(i')$  and therefore  $b\pi^{-1}(i) < b\pi^{-1}(i')$ . Moreover, the set of coset representatives  $(\mathbf{id}, b)$  of  $S_d \wr S_{|\underline{\Lambda}|}$  is mapped bijectively to the set of coset representatives of  $S_d \wr S_{\mathbf{j}}$  in  $S_d \wr S_k$ . Finally, for each coset the map is bijective (since it acts as a permutation).

We now show that the  $S_d \wr S_k$  action is preserved. Let  $(\alpha, \beta) \in S_d \wr S_k$ . By definition

$$(\alpha, \beta)((\mathbf{id}, b), (v_1, \dots, v_k; u_1, \dots, u_\ell)) = ((\mathbf{id}, \tilde{b}), (\tilde{\alpha}_1 v_{\tilde{\beta}^{-1}(1)}, \dots, \tilde{\alpha}_k v_{\tilde{\beta}^{-1}(k)}; \tilde{\beta} u_1, \dots, \tilde{\beta} u_\ell))$$

where  $(\mathbf{id}, \tilde{b})$  is the unique coset representative such that  $(\alpha, \beta)(\mathbf{id}, b) = (\mathbf{id}, \tilde{b})(\tilde{\alpha}, \tilde{\beta})$  with  $(\tilde{\alpha}, \tilde{\beta}) \in S_d \wr S_{|\underline{\Lambda}|}$ . Hence

$$\begin{aligned} & \phi((\alpha, \beta)((\mathbf{id}, b), (v_1, \dots, v_k; u_1, \dots, u_\ell))) \\ &= ((\mathbf{id}, \tilde{b}\pi^{-1}), (\tilde{\alpha}_{\pi^{-1}(1)} v_{\tilde{\beta}^{-1}\pi^{-1}(1)}, \dots, \tilde{\alpha}_{\pi^{-1}(k)} v_{\tilde{\beta}^{-1}\pi^{-1}(k)}; \pi \tilde{\beta} u_1, \dots, \pi \tilde{\beta} u_\ell)). \end{aligned}$$

On the other hand, using that  $(\alpha, \beta)(\mathbf{id}, b) = (\mathbf{id}, \tilde{b})(\tilde{\alpha}, \tilde{\beta})$  one can verify that  $(\alpha, \beta)(\mathbf{id}, b\pi^{-1}) = (\mathbf{id}, \tilde{b}\pi^{-1})(\pi \tilde{\alpha}, \pi \tilde{\beta}\pi^{-1})$ . Then we have

$$\begin{aligned} & (\alpha, \beta)\phi((\mathbf{id}, b), (v_1, \dots, v_k; u_1, \dots, u_\ell)) \\ &= (\alpha, \beta)((\mathbf{id}, b\pi^{-1}), (v_{\pi^{-1}(1)}, \dots, v_{\pi^{-1}(k)}; \pi u_1, \dots, \pi u_\ell)) \\ &= ((\mathbf{id}, \tilde{b}\pi^{-1}), (\pi \tilde{\alpha}, \pi \tilde{\beta}\pi^{-1})(v_{\pi^{-1}(1)}, \dots, v_{\pi^{-1}(k)}; \pi u_1, \dots, \pi u_\ell)) \\ &= ((\mathbf{id}, \tilde{b}\pi^{-1}), (\tilde{\alpha}_{\pi^{-1}(1)} v_{\tilde{\beta}^{-1}\pi^{-1}(1)}, \dots, \tilde{\alpha}_{\pi^{-1}(k)} v_{\tilde{\beta}^{-1}\pi^{-1}(k)}; \pi \tilde{\beta} u_1, \dots, \pi \tilde{\beta} u_\ell)). \end{aligned}$$

So  $\phi$  respects the  $S_d \wr S_k$ -action. □

## 6 Representative set for the action of $S_d \wr S_k$ on $([d] \times [k])^t$

We now turn our attention to the setting of noncommutative polynomials in variables  $x_{i,j}$  with  $i \in [d], j \in [k]$ . We consider the natural action of the wreath product  $S_d \wr S_k$  on such polynomials. We construct a representative set for the action of  $S_d \wr S_k$  on  $\mathbb{C}^{([d] \times [k])^t}$ .

As before, we start by decomposing  $\mathbb{C}^{([d] \times [k])^t}$  using the equivalence classes  $([d] \times [k])^t / (S_d \wr S_k)$ . Such an equivalence class corresponds to a pair  $(P, \mathbf{Q})$  where  $P = \{P_1, \dots, P_r\}$  is a set partition of  $[t]$  in at most  $k$  parts and  $\mathbf{Q} = (Q_1, \dots, Q_r)$  where each  $Q_i$  is a set partition of  $P_i$  in at most  $d$  parts. This gives a first decomposition of our vector space:

$$\mathbb{C}^{([d] \times [k])^t} = \bigoplus_{(P, \mathbf{Q}) \in ([d] \times [k])^t / (S_d \wr S_k)} V_{P, \mathbf{Q}} \quad (15)$$

where  $V_{P, \mathbf{Q}}$  is the vector space spanned by elements in the equivalence class  $(P, \mathbf{Q})$ . For  $P$  and  $\mathbf{Q} = (Q_1, \dots, Q_r)$ , set  $q_i := |Q_i|$  for each  $i \in [r]$ . The vector space  $V_{P, \mathbf{Q}}$  is spanned by monomials  $x_{i_1, j_1} \cdots x_{i_t, j_t}$  for which the set partition  $P$  is used to assign *distinct* bases ( $j_a$ 's) to variables in the monomial and the set partition  $Q_i$  of  $P_i$  is then used to assign  $q_i = |Q_i|$  *distinct* basis elements ( $i_a$ 's) to the variables in  $P_i$ . Below in Section 6.1 we use the representation theory of the symmetric group to obtain a decomposition of each of the  $S_d \wr S_k$ -modules  $V_{P, \mathbf{Q}}$ . In Section 6.2, we show that this is in fact a decomposition into *irreducible*  $S_d \wr S_k$ -modules by constructing isomorphisms to Specht modules  $S^\Delta$ . In Section 6.3 we give an explicit description of the representative set. We conclude the section with a worked out example of one representative element in the language of polynomials, see Section 6.5.

### 6.1 $V_{P, \mathbf{Q}}$ is a module for $S_d \wr S_k$

We give a natural interpretation of  $V_{P, \mathbf{Q}}$  in terms of tabloids. In what follows we use the partitions  $\mu_r^{(k)} = (k - r, 1^r)$  and  $\mu_q^{(d)} = (d - q, 1^q)$ . Consider the vector space

$$W := (M^{\mu_{q_1}^{(d)}} \otimes \dots \otimes M^{\mu_{q_r}^{(d)}}) \otimes M^{\mu_r^{(k)}}.$$

The standard basis vectors of  $W$  are naturally associated to tuples of standard basis vectors  $v_i \in M^{\mu_{q_i}^{(d)}}$  ( $i \in [r]$ ) and  $w \in M^{\mu_r^{(k)}}$  and we will use the notation

$$(v_1, \dots, v_r; w) := v_1 \otimes \dots \otimes v_r \otimes w.$$

We define an  $S_d \wr S_k$ -action on  $W$  by letting  $(\alpha, \beta) \in S_d \wr S_k$  act on such a vector as

$$(\alpha, \beta)(v_1, \dots, v_r; w) = (\alpha_{\beta w(1)} v_1, \dots, \alpha_{\beta w(r)} v_r; \beta w). \quad (16)$$

Here, for ease of notation, we use the convention that for integers  $0 \leq r < k$ , a tabloid  $w$  of shape  $\mu_r^{(k)}$  has content

$$w = \begin{array}{c} \overline{i \ \cdots \ j} \\ w(1) \\ \overline{w(2)} \\ \vdots \\ \overline{w(r)} \end{array}. \quad (17)$$

**Remark 6.1.** We emphasize the difference between the module  $W$  and the construction of  $S_d \wr S_k$ -modules described in Section 5: the action  $(\alpha; \beta) \otimes_{i \in [k]} x_i = \otimes_{i \in [k]} \alpha_i x_{\beta^{-1}(i)}$  described in Eq. (14) permutes the tensor legs and then applies  $\alpha_i$  to the  $i$ th leg, whereas the action described in Eq. (16) instead permutes the  $\alpha_i$  but leaves the tensor legs fixed. To define the action on  $W$  we require the “L-shape” of the tabloid  $w$  from (17). The fact that the tensor legs are not permuted by the  $S_d \wr S_k$ -action on  $W$  will be crucial in deriving our decomposition.

**Lemma 6.2.** *We have  $V_{P,Q} \cong W$  as  $S_d \wr S_k$ -modules.*

*Proof.* We construct an explicit  $S_d \wr S_k$ -isomorphism. Let  $\phi : V_{P,Q} \rightarrow W$  be the map that sends a monomial  $x_{i_1,j_1} \cdots x_{i_t,j_t}$  in  $V_{P,Q}$  to the standard basis vector  $(v_1, \dots, v_r; w)$  where  $w \in M^{\mu_r^{(k)}}$  is the tabloid for which  $w(i) \in [k]$  is the label of the basis assigned to the monomials corresponding to  $P_i$ , and similarly  $v_i(j) \in [d]$  is the basis element assigned to the monomials corresponding to the  $j$ th set in the set partition  $Q_i$ . The map  $\phi$  is a bijection between the standard basis elements of  $V_{P,Q}$  and the standard basis elements of  $W$  and we extend it linearly to all of  $V_{P,Q}$ . It remains to show that  $\phi$  is  $S_d \wr S_k$ -equivariant. Let  $x_{i_1,j_1} \cdots x_{i_t,j_t} \in V_{P,Q}$ , define  $(v_1, \dots, v_r; w) = \phi(x_{i_1,j_1} \cdots x_{i_t,j_t})$ , and let  $(\alpha, \beta) \in S_d \wr S_k$ . We show that  $\phi((\alpha, \beta)(x_{i_1,j_1} \cdots x_{i_t,j_t}))$  agrees with Eq. (16). Recall that

$$(\alpha, \beta)(x_{i_1,j_1} \cdots x_{i_t,j_t}) = x_{\alpha_{\beta(j_1)}(i_1), \beta(j_1)} \cdots x_{\alpha_{\beta(j_t)}(i_t), \beta(j_t)}$$

and therefore the assignment of bases and basis elements after the action of  $(\alpha, \beta)$  is as follows: the monomials corresponding to  $P_i$  are assigned basis  $\beta(w(i))$  and the monomials corresponding to the  $j$ th set in the set partition  $Q_i$  are assigned basis element  $\alpha_{\beta(w(i))}v_i(j)$ . This shows that indeed

$$\begin{aligned} \phi((\alpha, \beta)(x_{i_1,j_1} \cdots x_{i_t,j_t})) &= (\alpha_{\beta w(1)}v_1, \dots, \alpha_{\beta w(r)}v_r; \beta w) \\ &= (\alpha, \beta)(v_1, \dots, v_r; w) = (\alpha, \beta)\phi(x_{i_1,j_1} \cdots x_{i_t,j_t}). \end{aligned} \quad \square$$

We now use known results from the representation theory of the symmetric group to obtain a decomposition of  $W$ . Recall that  $\nu_1, \dots, \nu_\ell \vdash d$  is a complete list of partitions of  $d$ , sorted lexicographically, and hence that  $\ell$  is the number of partitions of  $d$ . For  $\mathbf{j} \in [\ell]^r$ , let

$$T_{\mathbf{j}, \mathbf{q}}^d = \bigtimes_{i \in [r]} T_{\nu_{j(i)}, \mu_{q_i}^{(d)}}. \quad (18)$$

For each  $\sigma \in T_{\mathbf{j}, \mathbf{q}}^d$  we define an  $S_d \wr S_k$ -submodule of  $W$ :

$$W_\sigma := (\sigma_1 \cdot S^{\nu_{j(1)}} \otimes \dots \otimes \sigma_r \cdot S^{\nu_{j(r)}}) \otimes M^{\mu_r^{(k)}}.$$

Applying Eq. (10) to each of the first  $r$  coordinates of  $W$  shows the following.

**Lemma 6.3.** *We have  $W = \bigoplus_{\mathbf{j} \in [\ell]^r} \bigoplus_{\sigma \in T_{\mathbf{j}, \mathbf{q}}^d} W_\sigma$ .*

We proceed by viewing the above module  $W_\sigma$  as an induced module, where the induction is from a group that corresponds to  $\mathbf{j}$ . The  $r$ -tuple  $\mathbf{j}$  naturally gives rise to a Young subgroup of  $S_r$ . We would like to associate a subgroup of  $S_k$  to it. We do this by first extending  $\mathbf{j}$  to a  $k$ -tuple  $\tilde{\mathbf{j}} = (j(1), \dots, j(r), \underbrace{1, \dots, 1}_{k-r \text{ times}}) \in [\ell]^k$  and then associating a Young subgroup to it. Concretely, to the  $r$ -tuple  $\mathbf{j}$  we associate the following Young subgroup of  $S_k$ : let  $\tilde{\mathbf{j}} = (j(1), \dots, j(r), \underbrace{1, \dots, 1}_{k-r \text{ times}}) \in [\ell]^k$  and define<sup>10</sup>

$$S_{\mathbf{j}} := S_{\tilde{\mathbf{j}}} = S_{j^{-1}(1) \cup \{k-r+1, \dots, k\}} \times S_{j^{-1}(2)} \times \dots \times S_{j^{-1}(\ell)}. \quad (19)$$

We define partitions  $\gamma^a$  for  $a \in [\ell]$  as

$$\gamma^a = \begin{cases} (k-r, 1^{|j^{-1}(1)|}) & \text{if } a = 1, \\ (1^{|j^{-1}(a)|}) & \text{if } a \geq 2. \end{cases} \quad (20)$$

We next consider the permutation modules  $M^{\gamma^a}$ . For  $a \geq 2$  we index the rows of tabloids in  $M^{\gamma^a}$  with  $\mathbf{j}^{-1}(a)$  and we let these tabloids have content  $\mathbf{j}^{-1}(a)$ . For  $M^{\gamma^1}$  we index the last  $|j^{-1}(1)|$  rows using  $\mathbf{j}^{-1}(1)$  and we let tabloids in  $M^{\gamma^1}$  have content  $\tilde{\mathbf{j}}^{-1}(1)$ . We then define the  $S_d \wr S_j$ -module

$$(\sigma_1 \cdot S^{\nu_{j(1)}} \otimes \dots \otimes \sigma_r \cdot S^{\nu_{j(r)}}) \otimes (M^{\gamma^1} \otimes \dots \otimes M^{\gamma^\ell})$$

---

<sup>10</sup>The choice of 1's on the last  $k-r$  coordinates might seem arbitrary, but it is motivated by the fact that  $\nu_1 = (d)$  and  $S^{(d)}$  is the trivial representation of  $S_d$ .

where the action of  $(\alpha, \beta) \in S_d \wr S_j$  is defined on a standard basis vector  $(v_1, \dots, v_r; w_1, \dots, w_\ell)$  as follows

$$(\alpha, \beta)(v_1, \dots, v_r; w_1, \dots, w_\ell) = (\alpha_{\beta w(1)} v_1, \dots, \alpha_{\beta w(r)} v_r; \beta w_1, \dots, \beta w_\ell)$$

where  $w : [r] \rightarrow [k]$  is such that the row of  $w_1, \dots, w_\ell$  that is indexed with  $i \in [r]$  has content  $w(i)$ . This  $S_d \wr S_j$ -module is naturally isomorphic to a tensor product of an  $S_d \wr S_{\tilde{j}^{-1}(1)}$ -module and  $S_d \wr S_{j^{-1}(a)}$ -modules (for  $a \geq 2$ ):

$$(\sigma_1 \cdot S^{\nu_{j(1)}} \otimes \dots \otimes \sigma_r \cdot S^{\nu_{j(r)}}) \otimes (M^{\gamma^1} \otimes \dots \otimes M^{\gamma^\ell}) \cong \bigotimes_{a \in [\ell]} \left( \left( \bigotimes_{i \in j^{-1}(a)} \sigma_i \cdot S^{\nu_a} \right) \otimes M^{\gamma^a} \right) \quad (21)$$

**Lemma 6.4.** For  $j \in [\ell]^r$  and  $\sigma \in T_{j,q}^d$ , as  $S_d \wr S_k$ -modules, we have

$$W_\sigma \cong \left[ (\sigma_1 \cdot S^{\nu_{j(1)}} \otimes \dots \otimes \sigma_r \cdot S^{\nu_{j(r)}}) \otimes (M^{\gamma^1} \otimes \dots \otimes M^{\gamma^\ell}) \right] \uparrow_{d,j}^{dk} =: W'_\sigma$$

*Proof.* We construct an explicit  $S_d \wr S_k$ -isomorphism  $\phi : W_\sigma \rightarrow W'_\sigma$ . For each standard basis element  $(v_1, \dots, v_r; w) \in W_\sigma$  we construct an element

$$\phi(v_1, \dots, v_r; w) = ((\mathbf{id}, b), (v_1, \dots, v_r; w_1, \dots, w_\ell)),$$

where  $(\mathbf{id}, b)$  is a coset representative of  $S_d \wr S_j$  in  $S_d \wr S_k$ . As coset representatives we take the elements  $(\mathbf{id}, b)$  for which  $b \in S_k$  is such that  $b(i) > b(i')$  whenever  $i > i'$  and either  $i, i' \in \tilde{j}^{-1}(1)$  or there exists an  $a \in [\ell]_{\geq 2}$  such that  $i, i' \in j^{-1}(a)$ . The coset representative  $b$  and  $\ell$ -tuple of tabloids  $(w_1, \dots, w_\ell)$  where  $w_a \in M^{\gamma^a}$  ( $a \in [\ell]$ ) are uniquely defined by the condition

$$w(i) = b(w_{j(i)}(i)) \quad \text{for } i \in [r]. \quad (22)$$

This defines a bijection between the basis elements of  $W_\sigma$  and those of  $W'_\sigma$ , and we extend  $\phi$  linearly to all of  $W_\sigma$ . It remains to show that  $\phi$  respects the group action.

Let  $(\alpha, \beta) \in S_d \wr S_k$  and let  $(v_1, \dots, v_r; w) \in W_\sigma$ . Let  $(\mathbf{id}, \tilde{b})$  be the coset representative for which  $(\alpha, \beta)(\mathbf{id}, b) \in (\mathbf{id}, \tilde{b}) \cdot S_d \wr S_j$  and let  $(\tilde{\alpha}, \tilde{\beta})$  be such that

$$(\alpha, \beta)(\mathbf{id}, b) = (\mathbf{id}, \tilde{b})(\tilde{\alpha}, \tilde{\beta}).$$

Note that  $\tilde{\alpha}$ ,  $\tilde{\beta}$  and  $\tilde{b}$  are such that  $\tilde{\beta} = \tilde{b}^{-1} \beta b \in S_j$  and  $\alpha_i = \tilde{\alpha}_{\tilde{b}^{-1}(i)}$  for all  $i \in [k]$ . In particular,  $\tilde{\alpha}_i = \alpha_{\tilde{b}(i)}$  for all  $i \in [k]$ . Then we have

$$\begin{aligned} (\alpha, \beta)\phi(v_1, \dots, v_r; w) &= (\alpha, \beta)((\mathbf{id}, b), (v_1, \dots, v_r; w_1, \dots, w_\ell)) \\ &= ((\mathbf{id}, \tilde{b}), (\tilde{\alpha}, \tilde{\beta})(v_1, \dots, v_r; w_1, \dots, w_\ell)) \\ &= ((\mathbf{id}, \tilde{b}), (\tilde{\alpha}_{\tilde{\beta}u(1)} v_1, \dots, \tilde{\alpha}_{\tilde{\beta}u(r)} v_r; \tilde{\beta} w_1, \dots, \tilde{\beta} w_\ell)) \\ &= ((\mathbf{id}, \tilde{b}), (\alpha_{\tilde{b}\tilde{\beta}u(1)} v_1, \dots, \alpha_{\tilde{b}\tilde{\beta}u(r)} v_r; \tilde{\beta} w_1, \dots, \tilde{\beta} w_\ell)) \\ &= ((\mathbf{id}, \tilde{b}), (\alpha_{\beta bu(1)} v_1, \dots, \alpha_{\beta bu(r)} v_r; \tilde{\beta} w_1, \dots, \tilde{\beta} w_\ell)) \end{aligned}$$

where  $u : [r] \rightarrow [k]$  is the function such that the row of  $w_1, \dots, w_\ell$  that is indexed with  $i \in [r]$  has content  $u(i)$ . On the other hand, we have

$$\begin{aligned} \phi((\alpha, \beta)(v_1, \dots, v_r; w)) &= \phi(\alpha_{\beta w(1)} v_1, \dots, \alpha_{\beta w(r)} v_r; \beta w) \\ &= ((\mathbf{id}, \tilde{b}), (\alpha_{\beta w(1)} v_1, \dots, \alpha_{\beta w(r)} v_r; \tilde{\beta} w_1, \dots, \tilde{\beta} w_\ell)) \\ &= ((\mathbf{id}, \tilde{b}), (\alpha_{\beta bu(1)} v_1, \dots, \alpha_{\beta bu(r)} v_r; \tilde{\beta} w_1, \dots, \tilde{\beta} w_\ell)) \end{aligned}$$

where for the second to last step we use that  $\beta w(i) = \beta b(w_{j(i)}(i)) = \tilde{b}\tilde{\beta}(w_{j(i)}(i))$  for  $i \in [r]$ , and for the last step we use Eq. (22).  $\square$

We then obtain our final decomposition by decomposing the permutation modules  $M^{\gamma^a}$  as in Eq. (10) to obtain  $S_d \wr S_k$ -modules  $W_{\sigma, \tau}$ : let  $\underline{\Lambda}$  be an  $\ell$ -multipartition of  $|\underline{\gamma}|$  and define

$$\mathbf{T}_{\underline{\Lambda}, \underline{\gamma}}^k := \bigotimes_{a \in [\ell]} T_{\Lambda^a, \gamma^a}. \quad (23)$$

For each  $\sigma \in \mathbf{T}_{j, q}^d$  and  $\tau \in \mathbf{T}_{\underline{\Lambda}, \underline{\gamma}}^k$  we define an  $S_d \wr S_k$ -submodule of  $W'_\sigma$ :

$$W_{\sigma, \tau} := \left[ (\sigma_1 \cdot S^{\nu_{j(1)}} \otimes \dots \otimes \sigma_r \cdot S^{\nu_{j(r)}}) \otimes (\tau_1 \cdot S^{\Lambda^1} \otimes \dots \otimes \tau_\ell \cdot S^{\Lambda^\ell}) \right] \uparrow_{d, j}^{dk}$$

**Lemma 6.5.** *We have  $W'_\sigma = \bigoplus_{\underline{\Lambda} \vdash |\underline{\gamma}|} \bigoplus_{\tau \in \mathbf{T}_{\underline{\Lambda}, \underline{\gamma}}^k} W_{\sigma, \tau}$ .*

*Proof.* This follows by applying Eq. (10) to each of the modules  $M^{\gamma^a}$ .  $\square$

Combining Lemmas 6.3 and 6.5 this shows the following:

**Corollary 6.6.** *We have  $W \cong \bigoplus_{j \in [\ell]^r} \bigoplus_{\sigma \in \mathbf{T}_{j, q}^d} \bigoplus_{\underline{\Lambda} \vdash |\underline{\gamma}|} \bigoplus_{\tau \in \mathbf{T}_{\underline{\Lambda}, \underline{\gamma}}^k} W_{\sigma, \tau}$ .*

In the next section we provide the necessary lemmas that allow us to show this is in fact a decomposition of  $W$  into *irreducible* submodules.

**Proposition 6.7.** *For  $j \in [\ell]^r$ ,  $\sigma \in \mathbf{T}_{j, q}^d$ ,  $\tau \in \mathbf{T}_{\underline{\Lambda}, \underline{\gamma}}^k$ , we have  $W_{\sigma, \tau} \cong S_j^\underline{\Lambda} \cong S^\underline{\Lambda}$  as  $S_d \wr S_k$ -modules.*

*Proof.* Recall that in Lemma 5.3 we have already shown that  $S_j^\underline{\Lambda}$  is  $S_d \wr S_k$ -isomorphic to  $S^\underline{\Lambda}$ . It thus remains to show that  $W_{\sigma, \tau}$  is  $S_d \wr S_k$ -isomorphic to  $S_j^\underline{\Lambda}$ . Since induction preserves isomorphism, it suffices to show that the respective  $S_d \wr S_j$ -modules are  $S_d \wr S_j$ -isomorphic. That is, after grouping on both sides the  $j^{-1}(a)$  coordinates (cf. (21)), it suffices to show

$$\bigotimes_{a \in [\ell]} \left( \left( \bigotimes_{i \in j^{-1}(a)} \sigma_i \cdot S^{\nu_a} \right) \otimes \tau_a \cdot S^{\Lambda^a} \right) \cong \bigotimes_{a \in [\ell]} \left( (S^{\nu_a})^{\tilde{\boxtimes} |\gamma^a|} \otimes S^{\Lambda^a} \right)$$

as  $S_d \wr S_j$ -modules. We do so separately for each  $a \in [\ell]$ . For  $a \geq 2$ , we have that  $\tau_a \cdot S^{\Lambda^a} \subseteq M^{(1^{|\gamma^a|})}$  and the  $S_d \wr S_{j^{-1}(a)}$ -isomorphism follows from Lemmas 6.9 and 6.10. For  $a = 1$  and thus  $\nu_1 = (d)$ , we have  $\tau_1 \cdot S^{\Lambda^1} \subseteq M^{(k-r, 1^{j^{-1}(1)|})}$  and the  $S_d \wr S_j$ -isomorphism follows from Lemma 6.11.  $\square$

To obtain a representative set for the action of  $S_d \wr S_k$  on  $W$  it will be useful to group the terms in the decomposition of  $W$  from Corollary 6.6 per Specht module  $S^\underline{\Lambda}$ . That is, we rearrange the direct sum as follows

$$W \cong \bigoplus_{\underline{\Lambda} \vdash k} \left( \bigoplus_{\substack{j \in [\ell]^r: \\ |j^{-1}(a)| = |\Lambda^a| \text{ for } a \geq 2}} \bigoplus_{\tau \in \mathbf{T}_{\underline{\Lambda}, \underline{\gamma}}^k} \bigoplus_{\sigma \in \mathbf{T}_{j, q}^d} W_{\sigma, \tau} \right).$$

## 6.2 $W_{\sigma, \tau}$ is isomorphic to a Specht module

We first consider the setting where all  $S_d$ -modules are isomorphic to  $S^\nu$  for a single  $\nu \vdash d$  and on the last coordinate we have the module  $M^{(1^k)}$ . That is, for  $\sigma_i \in T_{\nu, \mu_i}$  (for arbitrary  $\mu_i \vdash d$ ) we consider the  $S_d \wr S_k$ -module

$$M_1 = \left( \bigotimes_{i \in [k]} \sigma_i \cdot S^\nu \right) \otimes M^{(1^k)}$$

with the action from (16). We show  $M_1$  is isomorphic to the  $S_d \wr S_k$ -module  $M_2 = (S^\nu)^{\tilde{\boxtimes} r} \otimes M^{(1^k)}$ .

**Lemma 6.8.** *As  $S_d \wr S_k$ -modules we have  $M_1 \cong M_2$ .*

*Proof.* We construct an  $S_d \wr S_k$ -isomorphism  $\phi : M_1 \rightarrow M_2$ . As a standard basis of  $M_1$  we consider the vectors of the form  $(\sigma_1 \cdot v_1, \dots, \sigma_k \cdot v_k; w) \in M_1$  where  $v_1, \dots, v_k$  are standard basis vectors of  $S^\nu$  and  $w \in M^{(1^k)}$  is a tabloid (this forms a basis since the  $\sigma_i$  provide bijections between  $S^\nu$  and  $\sigma_i \cdot S^\nu$ ). For such a basis vector we define

$$\phi(\sigma_1 \cdot v_1, \dots, \sigma_k \cdot v_k; w) = (v_{w^{-1}(1)}, \dots, v_{w^{-1}(k)}; w).$$

This defines a bijection between the standard basis of  $M_1$  and the standard basis of  $M_2$ . We extend  $\phi$  linearly to the vector space  $M_1$ . Recall that for  $(\alpha, \beta) \in S_d \wr S_k$  we have

$$\begin{aligned} (\alpha, \beta)(\sigma_1 \cdot v_1, \dots, \sigma_k \cdot v_k; w) &= (\alpha_{\beta w(1)} \sigma_1 \cdot v_1, \dots, \alpha_{\beta w(k)} \sigma_k \cdot v_k; \beta w) \\ &= (\sigma_1 \cdot \alpha_{\beta w(1)} v_1, \dots, \sigma_k \cdot \alpha_{\beta w(k)} v_k; \beta w), \end{aligned}$$

and hence

$$\begin{aligned} \phi((\alpha, \beta)(\sigma_1 \cdot v_1, \dots, \sigma_k \cdot v_k; w)) &= (\alpha_{\beta w((\beta w)^{-1}(1))} v_{(\beta w)^{-1}(1)}, \dots, \alpha_{\beta w((\beta w)^{-1}(k))} v_{(\beta w)^{-1}(k)}; \beta w) \\ &= (\alpha_1 v_{(\beta w)^{-1}(1)}, \dots, \alpha_k v_{(\beta w)^{-1}(k)}; \beta w). \end{aligned}$$

On the other hand

$$\begin{aligned} (\alpha, \beta)\phi(\sigma_1 \cdot v_1, \dots, \sigma_k \cdot v_k; w) &= (\alpha, \beta)(v_{w^{-1}(1)}, \dots, v_{w^{-1}(k)}; w) \\ &= (\alpha_1 v_{w^{-1}\beta^{-1}(1)}, \dots, \alpha_k v_{w^{-1}\beta^{-1}(k)}; \beta w). \end{aligned}$$

In other words,  $\phi$  is  $S_d \wr S_k$ -equivariant. □

We now restrict the isomorphism from the above lemma to an  $S_d \wr S_k$ -submodule to obtain:

**Lemma 6.9.** *For  $i \in [k]$ , let  $\lambda_i \vdash k$  and  $\sigma_i \in T_{\nu, \lambda_i}$ . For  $\Lambda \vdash k$  and  $\tau \in T_{\Lambda, (1^k)}$ , we have*

$$\left( \bigotimes_{i \in [k]} \sigma_i \cdot S^\nu \right) \otimes \tau \cdot S^\Lambda \cong (S^\nu)^{\boxtimes k} \otimes \tau \cdot S^\Lambda.$$

*Proof.* Let  $\phi$  be the  $S_d \wr S_k$ -isomorphism from the proof of Lemma 6.8. By restricting  $\phi$  to  $\left( \bigotimes_{i \in [k]} \sigma_i \cdot S^\nu \right) \otimes \tau \cdot S^\Lambda$  (an  $S_d \wr S_k$ -submodule of its domain) we obtain an  $S_d \wr S_k$ -isomorphism between  $\left( \bigotimes_{i \in [k]} \sigma_i \cdot S^\nu \right) \otimes \tau \cdot S^\Lambda$  and  $\phi \left( \left( \bigotimes_{i \in [k]} \sigma_i \cdot S^\nu \right) \otimes \tau \cdot S^\Lambda \right)$ . It remains to show that the image is in fact  $(S^\nu)^{\boxtimes k} \otimes \tau \cdot S^\Lambda$ . Let  $e_\nu \in S^\nu$  and  $e_\Lambda \in S^\Lambda$  be the respective generating elements. We first show that  $\phi(e_\nu, \dots, e_\nu; e_\Lambda) \in (S^\nu)^{\boxtimes k} \otimes \tau \cdot S^\Lambda$ . Recall that  $\tau \cdot e_\Lambda = \sum_{\tau' \sim \tau} \sum_{c \in C_{t_\Lambda}} \text{sign}(c) \tau' * c\{t_\Lambda\}$ . Using the linearity of  $\phi$ , we have

$$\begin{aligned} &\phi(\sigma_1 \cdot e_\nu, \dots, \sigma_k \cdot e_\nu; \tau \cdot e_\Lambda) \\ &= \sum_{\tau' \sim \tau} \sum_{c \in C_{t_\Lambda}} \text{sign}(c) \phi(\sigma_1 \cdot e_\nu, \dots, \sigma_k \cdot e_\nu; \tau' * c\{t_\Lambda\}) = \sum_{\tau' \sim \tau} \sum_{c \in C_{t_\Lambda}} \text{sign}(c) (e_\nu, \dots, e_\nu; \tau' * c\{t_\Lambda\}) \\ &= (e_\nu, \dots, e_\nu; \sum_{\tau' \sim \tau} \sum_{c \in C_{t_\Lambda}} \text{sign}(c) \tau' * c\{t_\Lambda\}) = (e_\nu, \dots, e_\nu; \tau \cdot e_\Lambda) \in (S^\nu)^{\boxtimes k} \otimes \tau \cdot S^\Lambda. \end{aligned}$$

In other words, the generating element of  $\left( \bigotimes_{i \in [k]} \sigma_i \cdot S^\nu \right) \otimes \tau \cdot S^\Lambda$  is mapped to the generating element of  $(S^\nu)^{\boxtimes k} \otimes \tau \cdot S^\Lambda$ . Since  $\phi$  is  $S_d \wr S_k$ -equivariant, this shows that

$$\phi \left( \left( \bigotimes_{i \in [k]} \sigma_i \cdot S^\nu \right) \otimes \tau \cdot S^\Lambda \right) = (S^\nu)^{\boxtimes k} \otimes \tau \cdot S^\Lambda. \quad \square$$

Finally, we show that  $\tau$  can be removed, by using  $\mu = (1^k)$  in the proposition below.

**Lemma 6.10.** For  $\Lambda, \mu \vdash k$  and  $\tau \in T_{\Lambda, \mu}$ , we have  $(S^\nu)^{\boxtimes k} \circ \tau \cdot S^\Lambda \cong (S^\nu)^{\boxtimes k} \circ S^\Lambda$ .

*Proof.* Let  $v_1, \dots, v_k$  be basis elements of  $S^\nu$  and let  $w$  be a basis vector of  $S^\Lambda$ . We define  $\phi(v_1, \dots, v_k; \tau \cdot w) = (v_1, \dots, v_k; w)$ . Since  $\tau$  forms a linear bijection between  $S^\Lambda$  and  $\tau \cdot S^\Lambda$ , this provides a linear bijection between  $(S^\nu)^{\boxtimes k} \circ \tau \cdot S^\Lambda$  and  $(S^\nu)^{\boxtimes k} \circ S^\Lambda$ . Moreover,  $\phi$  is  $S_d \wr S_k$ -equivariant since  $\tau$  is  $S_k$ -equivariant.  $\square$

We finally consider the case  $\nu = (d)$  and  $\Lambda = (k - r, 1^r)$  (for some  $r < k$ ). Recall that if  $M$  is an  $S_k$ -module, it also is an  $S_d \wr S_k$ -module via  $(\alpha, \beta)m = \beta m$  for  $m \in M$  and  $(\alpha, \beta) \in S_d \wr S_k$ . By taking a tensor product with sufficiently many copies of the standard basis element  $\overline{1 \cdots d}$  of  $S^{(d)}$ , one can show the following.

**Lemma 6.11.** For  $\Lambda \vdash k$  and  $\tau \in T_{\Lambda, (k-r, 1^r)}$ , we have

$$\left( \bigotimes_{i \in [r]} \sigma_i \cdot S^{(d)} \right) \otimes \tau \cdot S^\Lambda \cong (S^{(d)})^{\boxtimes k} \circ \tau \cdot S^\Lambda \cong (S^{(d)})^{\boxtimes k} \circ S^\Lambda \cong S^\Lambda.$$

### 6.3 Decomposing $\mathbb{C}^{([d] \times [k])^t}$ into Specht modules

Combining the results from the previous sections, we obtain a decomposition of  $\mathbb{C}^{([d] \times [k])^t}$  into irreducible modules. We have

$$\mathbb{C}^{([d] \times [k])^t} = \bigoplus_{(P, \mathbf{Q}) \in ([d] \times [k])^t / (S_d \wr S_k)} \phi_{P, \mathbf{Q}} \bigoplus_{\underline{\Lambda} \vdash k} \left( \bigoplus_{\substack{j \in [\ell]^r: \\ |j^{-1}(a)| = |\Lambda^a| \text{ for } a \geq 2}} \bigoplus_{\tau \in T_{\underline{\Lambda}, \underline{\gamma}}^k} \bigoplus_{\sigma \in T_{j, \mathbf{q}}^d} W_{\sigma, \tau} \right) \quad (24)$$

where  $\phi_{P, \mathbf{Q}}$  is the isomorphism provided in Lemma 6.2,  $r = |P|$ ,  $q_i = |Q_i|$ .

From this decomposition we derive an explicit representative set by selecting for each  $W_{\sigma, \tau}$  the canonical generating element as the representative element (and grouping them according to  $\underline{\Lambda}$ ). The representative vectors  $u_{(\sigma, \tau), (P, \mathbf{Q})}$  will be constructed from pairs  $(\sigma, \tau)$  and  $(P, \mathbf{Q})$  appearing in the above decomposition. We now give precise definitions.

**Representative elements.** Fix a pair  $(P, \mathbf{Q})$  where  $P = \{P_1, \dots, P_r\}$  is a set partition of  $[t]$  into at most  $k$  parts and  $\mathbf{Q} = (Q_1, \dots, Q_r)$ , where each  $Q_i$  is a set partition of  $P_i$  in at most  $d$  parts. Let  $j \in [\ell]^r$ ,  $\mathbf{q} = (q_1, \dots, q_r) = (|Q_1|, \dots, |Q_r|)$ ,  $\underline{\Lambda} \vdash |\underline{\gamma}|$  where  $\underline{\gamma}$  is defined in Eq. (20), and  $\sigma \in T_{j, \mathbf{q}}^d$  and  $\tau \in T_{\underline{\Lambda}, \underline{\gamma}}^k$ . The representative vector corresponding to  $(\sigma, \tau)$  and  $(P, \mathbf{Q})$  is equal to

$$u_{(\sigma, \tau), (P, \mathbf{Q})} := \phi_{P, \mathbf{Q}}^{-1}((\mathbf{id}, \mathbf{id}), (\sigma_1 \cdot v_1, \dots, \sigma_r \cdot v_r; \tau_1 \cdot u_1, \dots, \tau_\ell \cdot u_\ell)),$$

where the vector  $((\mathbf{id}, \mathbf{id}), (v; u))$  is the generating element of  $S_j^\Lambda$  described in Section 5. Explicitly, we have

$$u_{(\sigma, \tau), (P, \mathbf{Q})} = \phi_{P, \mathbf{Q}}^{-1} \left( \left( \bigotimes_{i=1}^r \sigma_i \cdot e_{\nu_{j(i)}} \right) \otimes \left( \bigotimes_{a=1}^\ell \tau_a \cdot e_{\Lambda^a} \right) \right).$$

The next step is to describe these vectors explicitly as vectors in  $\mathbb{C}^{([d] \times [k])^t}$ . Note that

$$V_{Q_1} \otimes \dots \otimes V_{Q_r} \otimes V_P \cong V_{P, \mathbf{Q}} \subseteq \mathbb{C}^{([d] \times [k])^t},$$

via the isomorphism given by  $w_1 \otimes \dots \otimes w_r \otimes u \mapsto \text{Perm}_P(w_1 \otimes \dots \otimes w_r) \otimes u$ . Here  $\text{Perm}_P$  is the permutation matrix which permutes the coordinates of  $w_1 \otimes \dots \otimes w_r$  (which is a vector in  $\mathbb{C}^{[d]^t}$ ) in such a way that  $w_i$  corresponds to the coordinates given by  $P_i$ . Then

$$\phi_{P, \mathbf{Q}}^{-1}((\mathbf{id}, \mathbf{id}), (v_1, \dots, v_r; u_1, \dots, u_\ell)) = \text{Perm}_P(\phi_{Q_1}^{-1}(v_1) \otimes \dots \otimes \phi_{Q_r}^{-1}(v_r)) \otimes \phi_P^{-1}(u_1 \otimes \dots \otimes u_\ell),$$

where  $\phi_P : V_P \rightarrow M^{\mu_r}$  is the isomorphism from Section 4.2 and we identify  $\left[ \bigotimes_{a \in [\ell]} M^{\gamma^a} \right] \uparrow_{d, j}^{d, k}$  with  $M^{\mu_r^{(k)}}$  (cf. Lemma 6.4).



**The dimension of  $\text{End}_{S_d \wr S_k}(\mathbb{C}^{([d] \times [k])^t})$ .** As in Section 4.2, we note that  $\dim(\text{End}_{S_d \wr S_k}(\mathbb{C}^{([d] \times [k])^t}))$  equals the dimension of the space of  $S_d \wr S_k$ -invariant noncommutative polynomials of degree exactly  $2t$ . In other words, it equals the number of pairs  $(P, \{Q_1, \dots, Q_r\})$  where  $P$  is a set partition of  $[2t]$  which determines the assignment of bases (to the  $k$ -part) with  $|P| = r$ , and  $Q_i$  is a set partition of  $P_i$  which determines the assignment of the basis elements (to the  $d$ -part). When  $d, k \geq 2t$ , this number is independent of  $k$  and  $d$  and simply becomes the number of pairs of set partitions  $(P, P')$  of a set of  $2t$  elements with the property that the set partition  $P'$  is a refinement of  $P$ . The sequence of numbers  $(C_n)_{n \geq 0}$  such that  $C_n$  is the number of pairs of set partitions  $(P, P')$  with  $P$  a set partition of  $[n]$  and  $P'$  a refinement of  $P$  is known in the online encyclopedia of integer sequences as sequence A000258; its first ten elements are 1, 1, 3, 12, 60, 358, 2471, 19302, 167894, 1606137. We emphasize that for  $d, k \geq 2t$ , the size of the symmetry reduced SDP thus becomes independent of  $d$  and  $k$ .

#### 6.4 Representative set for the $S_{d-1} \times (S_d \wr S_{k-1})$ action on $(1, 1) \times ([d] \times [k])^t$

We will now give a representative set useful for the case  $t + \frac{1}{2}$ , as discussed in Section 3.2. We naturally identify  $x_{1,1} \mathbb{R}\langle x_{i,j} : i \in [d], j \in [k] \rangle_{=t}$  with  $\mathbb{C}^{(1,1) \times ([d] \times [k])^t}$ . Recall that this set is a module for  $G := S_{d-1} \times (S_d \wr S_{k-1})$ , where  $S_{d-1}$  permutes the indices  $2, \dots, d$  corresponding to  $k = 1$ , and where  $S_d \wr S_{k-1}$  acts on the indices  $(i, j)$  with  $i \in [d]$ ,  $j \in \{2, \dots, k\}$ .

As before, we start by decomposing  $\mathbb{C}^{(1,1) \times ([d] \times [k])^t}$  using the equivalence classes  $((1, 1) \times ([d] \times [k])^t) / (S_{d-1} \times (S_d \wr S_{k-1}))$ . Such an equivalence class corresponds to a pair  $(P, \mathbf{Q})$  where  $P = \{P_1, \dots, P_r\}$  is a set partition of  $[t + 1]$  in at most  $k$  parts and  $\mathbf{Q} = (Q_1, \dots, Q_r)$  where each  $Q_i$  is a set partition of  $P_i$  in at most  $d$  parts. This gives a first decomposition of our vector space:

$$\mathbb{C}^{(1,1) \times ([d] \times [k])^t} = \bigoplus_{(P, \mathbf{Q}) \in ((1,1) \times ([d] \times [k])^t) / (S_{d-1} \times (S_d \wr S_{k-1}))} V_{P, \mathbf{Q}}$$

In the decomposition, we may assume that  $1 \in P_1$  (and hence gets assigned basis 1) and that  $1 \in Q_1^{(1)}$  (and hence gets assigned basis element 1). We then have that  $V_{P, \mathbf{Q}}$  is  $S_{d-1} \times (S_d \wr S_{k-1})$ -isomorphic to the tensor product  $V_1 \otimes V_2$ , where

$$V_1 := M^{\mu_{q_1-1}^{(d-1)}}, \quad V_2 := (M^{\mu_{q_2}^{(d)}} \otimes \dots \otimes M^{\mu_{q_r}^{(d)}}) \otimes M^{\mu_{r-1}^{(k)}}.$$

The group  $G_1 := S_{d-1}$  acts on  $V_1$ , and  $G_2 := S_d \wr S_{k-1}$  acts on  $V_2$ . To obtain a representative set for the action of  $G_1 \times G_2$  on  $V_1 \otimes V_2$ , we use Eq. (6) to combine representative sets for the actions of  $G_1$  and  $G_2$  on  $V_1$  and  $V_2$  from Sections 4 and 6, respectively. One then obtains a representative set for the  $G$ -action on  $\mathbb{C}^{(1,1) \times ([d] \times [k])^t}$  by combining the representative sets of all  $V_{P, \mathbf{Q}}$ .

#### 6.5 An example: homogeneous quadratic polynomials

To illustrate the theory developed in Section 6, we show how to compute one particular representative element. We consider homogeneous quadratic polynomials in variables  $x_{i,j}$ , where  $i \in [d]$  and  $j \in [k]$ , that are invariant under the action of  $S_d \wr S_k$ . We express the concepts in the language of polynomials. In this example we take  $d = 2$ ,  $k = 3$  and  $t = 2$ .

We first decompose the space of polynomials into  $S_d \wr S_k$ -invariant subspaces corresponding to orbits of monomials. In this example we consider the orbit

$$\{x_{i_1, j_1} x_{i_2, j_2} \mid i_1, i_2 \in [d], j_1, j_2 \in [k] \text{ with } j_1 \neq j_2\}.$$

This orbit corresponds to the tuple of partitions  $(P, \mathbf{Q}) = (\{\{1\}, \{2\}\}, (\{\{1\}\}, \{\{2\}\}))$ . Here  $P$  is a partition of  $[t]$  and  $\mathbf{Q}$  is a tuple of set partitions  $\mathbf{Q} = (Q_1, \dots, Q_{|P|})$  where each  $Q_i$  is a set partition of  $P_i$  in at most  $d$  parts. The corresponding subspace is

$$V_{P, \mathbf{Q}} = \text{Span}\{x_{i_1, j_1} x_{i_2, j_2} \mid i_1, i_2 \in [d], j_1, j_2 \in [k] \text{ with } j_1 \neq j_2\}.$$

We have seen that, in order to decompose  $V_{P, \mathbf{Q}}$ , we consider  $\ell$ -multipartitions of  $k = 3$ , where we recall that  $\ell$  is the number of partitions of  $d$ . In this example  $d = 2$  and therefore  $\ell = 2$ . For this example we take the  $\ell$ -multipartition  $\underline{\Lambda} = ((1), (1, 1))$ . The rows and columns of the block indexed by  $\underline{\Lambda}$  in the

block diagonalization are indexed by tuples  $(\sigma, \tau), (P, Q)$ , where  $\sigma$  is an element of  $T_{j,q}^d$  and  $\tau$  is an element of  $T_{\underline{\Lambda}, \underline{\gamma}}^k$ .

To describe  $T_{j,q}^d$ , we first need  $j$  and  $q$ . Throughout this section we have  $r = |P|$ , so in this case  $r = 2$ . In the final decomposition in Eq. (24), we have  $j \in [\ell]^r = [2]^2$ , where  $|j^{-1}(2)| = |\Lambda^2| = 2$ , so  $j = (2, 2)$ . Furthermore, we have  $q = (|Q_1|, \dots, |Q_r|) = (|Q_1|, |Q_2|) = (1, 1)$ . The collection  $T_{j,q}^d$  is a tuple of sets of semistandard tableaux (cf. Eq (18)), one set for each set in  $P$  ( $r = |P|$ ), where the content is defined by the size of the corresponding partition in  $Q$ , and the shape is  $\nu_{j(i)}$ , for  $i = 1, \dots, r$ , which is determined by  $\underline{\Lambda}$  as  $j$  is determined by  $\underline{\Lambda}$ . Formally, we have (cf. Eq. (18))

$$T_{j,q}^d = T_{(2,2),(1,1)}^2 = \bigtimes_{i \in [r]} T_{\nu_{j(i)}, \mu_{q_i}^{(d)}} = T_{(1,1), \mu_1^{(2)}} \times T_{(1,1), \mu_1^{(2)}} = \left\{ \begin{bmatrix} 1 \\ 2 \end{bmatrix} \right\} \times \left\{ \begin{bmatrix} 1 \\ 2 \end{bmatrix} \right\},$$

which consists of only one element:  $\sigma = \left( \begin{bmatrix} 1 \\ 2 \end{bmatrix}, \begin{bmatrix} 1 \\ 2 \end{bmatrix} \right)$ .

Similarly, to describe  $T_{\underline{\Lambda}, \underline{\gamma}}^k$ , we first describe  $\underline{\gamma}$ . The tuple  $j$  is via Eq. (20) associated with the multipartition  $\underline{\gamma} = ((k-r, 0), (1, 1)) = ((1), (1, 1))$ . The collection  $T_{\underline{\Lambda}, \underline{\gamma}}^k$  is a tuple of sets of semistandard tableaux (cf. Eq (23)), one set for each partition in the multipartition  $\underline{\Lambda}$ , where the content is defined by the size of the corresponding partition in  $\underline{\gamma}$ . Formally, we have (cf. Eq. (23))

$$T_{\underline{\Lambda}, \underline{\gamma}}^k = \bigtimes_{a \in [\ell]} T_{\Lambda^a, \gamma^a} = T_{(1), (1)} \times T_{(1,1), (1,1)} = \left\{ \begin{bmatrix} 1 \\ 1 \end{bmatrix} \right\} \times \left\{ \begin{bmatrix} 1 \\ 2 \end{bmatrix} \right\},$$

which consists of one element, namely  $\tau = \left( \begin{bmatrix} 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 2 \end{bmatrix} \right)$ . We have now defined  $(\sigma, \tau)$  and  $(P, Q)$ , so we are ready to compute the representative element  $u_{(\sigma, \tau), (P, Q)}$ . We have

$$\begin{aligned} u_{(\sigma, \tau), (P, Q)} &= \phi_{P, Q}^{-1} \left( \left( \bigotimes_{i=1}^r \sigma_i \cdot e_{\nu_{j(i)}} \right) \otimes \left( \bigotimes_{a=1}^{\ell} \tau_a \cdot e_{\Lambda^a} \right) \right) \\ &= \phi_{P, Q}^{-1} \left( \left( \left( \begin{bmatrix} 1 \\ 2 \end{bmatrix} - \begin{bmatrix} 2 \\ 1 \end{bmatrix} \right) \otimes \left( \begin{bmatrix} 1 \\ 2 \end{bmatrix} - \begin{bmatrix} 2 \\ 1 \end{bmatrix} \right) \right) \otimes \left( \begin{bmatrix} 1 \\ 1 \end{bmatrix} \otimes \left( \begin{bmatrix} 1 \\ 2 \end{bmatrix} - \begin{bmatrix} 2 \\ 1 \end{bmatrix} \right) \right) \right) \\ &= \text{Perm}_P \left( \phi_{\{1\}}^{-1} \left( \begin{bmatrix} 1 \\ 2 \end{bmatrix} - \begin{bmatrix} 2 \\ 1 \end{bmatrix} \right) \otimes \phi_{\{2\}}^{-1} \left( \begin{bmatrix} 1 \\ 2 \end{bmatrix} - \begin{bmatrix} 2 \\ 1 \end{bmatrix} \right) \right) \otimes \phi_{\{1\}, \{2\}}^{-1} \left( \begin{bmatrix} 1 \\ 1 \end{bmatrix} \otimes \left( \begin{bmatrix} 1 \\ 2 \end{bmatrix} - \begin{bmatrix} 2 \\ 1 \end{bmatrix} \right) \right) \end{aligned}$$

As in the discussion below Lemma 6.3, we identify  $\left[ \bigotimes_{a \in [\ell]} M^{\gamma^a} \right]_{dj}^{dk}$  with  $M^{\mu_r^{(k)}}$ . In our case,  $S_j = S_{\{3\}} \times S_{\{1,2\}}$ , cf. Eq. (19), so the element

$$\left( \begin{bmatrix} 1 \\ 1 \end{bmatrix} \otimes \left( \begin{bmatrix} 1 \\ 2 \end{bmatrix} - \begin{bmatrix} 2 \\ 1 \end{bmatrix} \right) \right) \text{ is identified with } \frac{\overline{3}}{\underline{2}} - \frac{\overline{3}}{\underline{1}} \in M^{\mu_2^{(3)}}.$$

Therefore we find

$$\begin{aligned} u_{(\sigma, \tau), (P, Q)} &= \text{Perm}_P \left( \phi_{\{1\}}^{-1} \left( \begin{bmatrix} 1 \\ 2 \end{bmatrix} - \begin{bmatrix} 2 \\ 1 \end{bmatrix} \right) \otimes \phi_{\{2\}}^{-1} \left( \begin{bmatrix} 1 \\ 2 \end{bmatrix} - \begin{bmatrix} 2 \\ 1 \end{bmatrix} \right) \right) \otimes \phi_{\{1\}, \{2\}}^{-1} \left( \frac{\overline{3}}{\underline{2}} - \frac{\overline{3}}{\underline{1}} \right) \\ &= \text{Perm}_P \left( \underbrace{(y_2 - y_1)(y_2 - y_1)}_{\text{'d-part'}} \otimes \underbrace{(z_1 z_2 - z_2 z_1)}_{\text{'k-part'}} \right) \\ &= x_{2,1} x_{2,2} - x_{1,1} x_{2,2} - x_{2,1} x_{1,2} + x_{1,1} x_{1,2} - x_{2,2} x_{2,1} + x_{1,2} x_{2,1} + x_{2,2} x_{1,1} - x_{1,2} x_{1,1}. \end{aligned}$$

In this case,  $\text{Perm}_P$  can be viewed as identifying  $x_{i,j} = y_i z_j$ , where  $i \in [d]$  and  $j \in [k]$ . The other representative elements are computed in an analogous way, by considering different tuples of set partitions  $(P, Q)$ ,  $\ell$ -multipartitions  $\underline{\Lambda}$ , and tuples of Young tableaux  $\sigma$  and  $\tau$ .

## 7 $V_{P,Q}$ is isomorphic to a permutation module $M^\mu$ .

Here we show that the  $S_d \wr S_k$ -modules  $V_{P,Q}$  from Eq. (15) can alternatively be viewed as a generalization of permutation modules to the wreath product setting. Our decomposition of  $V_{P,Q}$  can thus be viewed as an explicit decomposition of such a permutation module in Specht modules, or alternatively, as a characterization of the space of homomorphisms from Specht modules to such permutation modules.

Analogously to Definition 5.2 for Specht modules, we use the following definition of a permutation module for  $S_d \wr S_k$ ; these modules were named permutation modules e.g. in [Gre19].

**Definition 7.1.** For an  $\ell$ -multipartition  $\underline{\mu}$  of  $k$ , the permutation module  $M^\mu$  is defined as

$$M^\mu := \left[ (M^{\nu_1}, \dots, M^{\nu_\ell})^{\boxtimes |\underline{\mu}|} \otimes (M^{\mu^1} \boxtimes \dots \boxtimes M^{\mu^\ell}) \right] \uparrow_{d|\underline{\mu}|}^{dk}.$$

Standard basis elements of  $M^\mu$  are of the form  $((\mathbf{id}, b), (v_1 \otimes \dots \otimes v_k \otimes u_1 \otimes \dots \otimes u_\ell))$  where  $(\mathbf{id}, b)$  is a coset representative,  $v_1 \otimes \dots \otimes v_k$  is an element of  $(M^{\nu_1}, \dots, M^{\nu_\ell})^{\boxtimes |\underline{\mu}|}$ , and for each  $a \in [\ell]$ ,  $u_a$  is a tabloid in  $M^{\mu^a}$  with content  $I_a := \{1 + \sum_{j < a} |\mu^j|, \dots, \sum_{j \leq a} |\mu^j|\}$  (if  $|\mu^a| > 0$ ). To make the distinction between  $S_d$ -modules and  $S_k$ -modules more apparent we will write  $(v_1, \dots, v_k; u_1, \dots, u_\ell)$  to denote the vector  $v_1 \otimes \dots \otimes v_k \otimes u_1 \otimes \dots \otimes u_\ell$ . That is, we write standard basis vectors of  $M^\mu$  as  $((\mathbf{id}, b), (v_1, \dots, v_k; u_1, \dots, u_\ell))$ .

### 7.1 The isomorphism

Given  $P$  and  $Q = (Q_1, \dots, Q_r)$ , set  $q_i := |Q_i|$  for each  $i \in [r]$ . Recall that in the vector space  $V_{P,Q}$  the set partition  $P$  is used to assign *distinct* bases ( $j$ 's) to variables in the monomial  $x_{i_1, j_1} \dots x_{i_t, j_t}$ . The set partition  $Q_i$  of  $P_i$  is then used to assign  $q_i = |Q_i|$  *distinct* basis elements ( $i$ 's) to the variables in  $P_i$ . We now show how to interpret  $V_{P,Q}$  as a permutation module.

For each  $j \in [t-r]$ , let  $n_j = |\{i \in [r] : s_i = j\}|$ . Define the  $\ell$ -multipartition  $\underline{\mu} = (\mu^1, \dots, \mu^\ell)$  by

$$\mu^a = \begin{cases} (k-r) & \text{if } a = 1 \\ (1^{n_j}) & \text{if } \nu_a = \mu_j^{(d)} \text{ for some } j \in [t-r] \\ () & \text{otherwise.} \end{cases}$$

Note that  $\sum_{j \in [t-r]} n_j = r$  and  $\mu^1 = (k-r)$ , so  $\underline{\mu}$  is an  $\ell$ -multipartition of  $k$ .

**Lemma 7.2.** We have  $V_{P,Q} \cong M^\mu$ .

*Proof.* For this proof it will be notationally convenient to change the order of the partitions of  $d$  in  $M^\mu$ : we assume  $\nu_j = \mu_j^{(d)}$  for  $j \in [t-r]$  and we let  $\nu_\ell = (d)$ . Correspondingly, we then have  $\mu^j = (1^{n_j})$  for  $j \in [t-r]$  and  $\mu^\ell = (k-r)$ . Changing the order of the partitions of  $d$  leads to an  $S_d \wr S_k$ -isomorphic module, which, with abuse of notation, we will denote with  $M^\mu$  as well. We consider  $S_d \wr S_{|\underline{\mu}|}$  as a subgroup of  $S_d \wr S_k$ . As coset representatives we take the elements  $(\mathbf{id}, b)$  where  $b \in S_k$  is such that  $b(i) > b(i')$  whenever there exists a  $a \in [\ell]$  such that  $i, i' \in I_a$  and  $i > i'$ .

We first define a bijection between monomials in  $V_{P,Q}$  and basis vectors in  $M^\mu$ . Recall that

$$I_j = I(\underline{\mu})_j = \left\{ 1 + \sum_{i < j} |\mu^i|, \dots, |\mu^j| + \sum_{i < j} |\mu^i| \right\} = \left\{ 1 + \sum_{i < j} n_i, \dots, n_j + \sum_{i < j} n_i \right\}.$$

Then, without loss of generality, we may label the  $P_i$ 's and corresponding  $Q_i$ 's in such a way that  $|Q_i| = n_j$  if  $i \in I_j$  (each  $i \in [t]$  is contained in exactly one such  $I_j$ ). Given a monomial  $x_{i_1, j_1} \dots x_{i_t, j_t}$  in  $V_{P,Q}$ , we define the following basis vector in  $M^\mu$ . The assignment of bases to  $P_1, \dots, P_r$  uniquely determines a coset representative  $b$  and an  $\ell$ -tuple  $(u_1, \dots, u_\ell)$  of tabloids where each  $u_a : I_a \rightarrow I_a$  has shape  $\mu^a$ : for  $j \in [t-r]$  the tabloid  $u_j$  is such that if  $i \in I_j$ , then  $P_i$  is assigned basis  $b(u_j(i))$ , and finally

we let  $u_\ell$  be the tabloid of shape  $(k-r)$  with content  $I_\ell$ . For  $i \in I_j$  define a tabloid  $v_i$  of shape  $\mu_j^{(d)}$  as

$$v_i = \frac{\overline{\dots}}{\overline{\frac{w^1_{u_j^{-1}(i)}}{\vdots}} \overline{\frac{w^j_{u_j^{-1}(i)}}{\vdots}}}$$

where  $w_{u_j^{-1}(i)}^{j'} \in [d]$  is the basis element assigned to the  $j'$ -th set in  $Q_{u_j^{-1}(i)}$ . We let  $v_{r+1}, \dots, v_k$  equal the tabloid of shape  $(d)$  with content  $(1^d)$ . Combining the above, to a monomial  $x_{i_1, j_1} \cdots x_{i_t, j_t}$  in  $V_{P, Q}$ , we associate the basis vector

$$((\mathbf{id}, b), (v_1, \dots, v_k; u_1, \dots, u_\ell)) \in M^\mu. \quad (25)$$

This construction defines a (linear) bijection  $\phi$  between  $V_{P, Q}$  and  $M^\mu$ . To conclude the proof we show that  $\phi$  respects the  $S_d \wr S_k$ -action.

Let us first consider the  $S_d \wr S_k$ -action on the element  $\phi(x_{i_1, j_1} \cdots x_{i_t, j_t})$  shown in (25). Let  $(\alpha, \beta) \in S_d \wr S_k$ . Let  $(\mathbf{id}, \tilde{b})$  be the coset representative for which  $(\alpha, \beta)(\mathbf{id}, b) \in (\mathbf{id}, \tilde{b}) \cdot S_d \wr S_{|\underline{\mu}|}$  and let  $(\tilde{\alpha}, \tilde{\beta})$  be such that

$$(\alpha, \beta)(\mathbf{id}, b) = (\mathbf{id}, \tilde{b})(\tilde{\alpha}, \tilde{\beta}). \quad (26)$$

Note that  $\tilde{\alpha}, \tilde{\beta}$  and  $\tilde{b}$  are such that  $\tilde{\beta} = \tilde{b}^{-1}\beta b \in S_{|\underline{\mu}|}$  and  $\alpha_i = \tilde{\alpha}_{\tilde{b}^{-1}(i)}$  for all  $i \in [k]$ . In particular,  $\tilde{\alpha}_i = \alpha_{\tilde{b}(i)}$  for all  $i \in [k]$ . Then we have

$$\begin{aligned} (\alpha, \beta)((\mathbf{id}, b), (v_1, \dots, v_k; u_1, \dots, u_\ell)) &= ((\mathbf{id}, \tilde{b}), (\tilde{\alpha}, \tilde{\beta})(v_1, \dots, v_k; u_1, \dots, u_\ell)) \\ &= ((\mathbf{id}, \tilde{b}), (\tilde{\alpha}_1 v_{\tilde{\beta}^{-1}(1)}, \dots, \tilde{\alpha}_k v_{\tilde{\beta}^{-1}(k)}; \tilde{\beta} u_1, \dots, \tilde{\beta} u_\ell)) \\ &= ((\mathbf{id}, \tilde{b}), (\alpha_{\tilde{b}(1)} v_{\tilde{\beta}^{-1}(1)}, \dots, \alpha_{\tilde{b}(k)} v_{\tilde{\beta}^{-1}(k)}; \tilde{\beta} u_1, \dots, \tilde{\beta} u_\ell)). \end{aligned} \quad (27)$$

On the other hand, for the corresponding element  $x_{i_1, j_1} \cdots x_{i_t, j_t} \in V_{P, Q}$  we have

$$(\alpha, \beta)x_{i_1, j_1} \cdots x_{i_t, j_t} = x_{\alpha_{\beta(j_1)}(i_1), \beta(j_1)} \cdots x_{\alpha_{\beta(j_t)}(i_t), \beta(j_t)}.$$

We will use the above identity to express  $\phi((\alpha, \beta)x_{i_1, j_1} \cdots x_{i_t, j_t})$  in terms of  $\phi(x_{i_1, j_1} \cdots x_{i_t, j_t})$ . For  $i \in [r]$  let  $j \in [t-r]$  be the unique index such that  $i \in I_j$ , then  $P_i$  is assigned basis

$$\beta(b(u_j(i))) = \tilde{b}(\tilde{\beta}(u_j(i))) = \tilde{b}(\tilde{u}_j(i)),$$

where we used the definition of  $\tilde{b}, \tilde{\alpha}, \tilde{\beta}$  from (26) and we let  $\tilde{u}_a = \tilde{\beta} u_a$  for each  $a \in [\ell]$ . For each  $i \in [k-r]$  we have that  $\tilde{v}_{i+r}$  is the tabloid of shape  $(d)$  with content  $(1^d)$ , and therefore  $\tilde{v}_{i+r} = v_{\tilde{\beta}^{-1}(i+r)}$  where we use that  $\tilde{\beta} \in S_{|\underline{\mu}|}$ . For  $j \in [t-r]$  and  $i \in I_j$  we now consider the content of  $\tilde{v}_i$ . By definition it corresponds to the assignment of basis elements to the  $j$  sets in

$$Q_{\tilde{u}_j^{-1}(i)} = Q_{(\tilde{\beta} u_j)^{-1}(i)} = Q_{u_j^{-1}(\tilde{\beta}^{-1}(i))}.$$

It follows that the content of  $\tilde{v}_i$  is the content of  $v_{\tilde{\beta}^{-1}(i)}$ . All variables corresponding to  $Q_{\tilde{u}_j^{-1}(i)}$  are assigned basis  $\tilde{b}\tilde{u}_j(\tilde{u}_j^{-1}(i)) = \tilde{b}(i)$  from which it follows that  $\alpha_{\tilde{b}(i)}$  is applied to  $v_{\tilde{\beta}^{-1}(i)}$ . That is,

$$\tilde{v}_i = \frac{\overline{\dots}}{\overline{\frac{w^1_{\tilde{u}_j^{-1}(i)}}{\vdots}} \overline{\frac{w^j_{\tilde{u}_j^{-1}(i)}}{\vdots}}} = \frac{\overline{\dots}}{\overline{\frac{\alpha_{\tilde{b}(i)} w^1_{u_j^{-1}(i)}}{\vdots}} \overline{\frac{\alpha_{\tilde{b}(i)} w^j_{u_j^{-1}(i)}}{\vdots}}} = \alpha_{\tilde{b}(i)} v_{\tilde{\beta}^{-1}(i)}.$$

This shows, using (27), that

$$\begin{aligned} \phi((\alpha, \beta)x_{i_1, j_1} \cdots x_{i_t, j_t}) &= ((\mathbf{id}, \tilde{b}), (\alpha_{\tilde{b}(1)} v_{\tilde{\beta}^{-1}(1)}, \dots, \alpha_{\tilde{b}(k)} v_{\tilde{\beta}^{-1}(k)}; \tilde{\beta} u_1, \dots, \tilde{\beta} u_\ell)) \\ &= (\alpha, \beta)\phi(x_{i_1, j_1} \cdots x_{i_t, j_t}), \end{aligned}$$

which means that  $\phi$  respects the action of  $S_d \wr S_k$ . □

## 8 Computational results

Using the representative sets obtained in Sections 4 and 6 we can symmetry reduce  $\text{sdp}(d, k, t)$ . That is, we use the representative sets and Proposition 2.2 to obtain equivalent SDPs of smaller size. We furthermore use the  $S_d \wr S_k$ -invariance of feasible solutions, the MUB relations, and the tracial property to reduce the number of variables. We present computational results for (moderately) small  $d, k, t$  in Section 8.2.<sup>11</sup>

### 8.1 How to determine the value of $L$ on monomials

An essential step in generating our SDPs is to decide which variables to use, i.e., for which  $S_d \wr S_k$ -orbits should we include a variable? For this we construct a list  $\mathcal{L}$  of values  $L(w)$  to use as variables as follows. Let  $\mathcal{R} = \{p_1, \dots, p_m\}$  be a list of representatives for the  $S_d \wr S_k$ -orbits of monomials in  $\mathbb{R}\langle x_{i,j} \mid i \in [d], j \in [k] \rangle_{=2t}$ . We order the monomials in the following way: we view  $([d] \times [k])^t$  as  $[k]^t \times [d]^t$  and then use the *graded lexicographic order*, i.e., for two monomials  $q, p$  we have  $q \leq p$  if  $\deg(q) < \deg(p)$  or if  $\deg(q) = \deg(p)$  and  $q$  precedes  $p$  in the lexicographic order. This is a well ordering of the noncommutative monomials and any monomial is preceded by only finitely many other monomials. Then, as long as  $\mathcal{R}$  is not empty, we remove the last monomial  $p$  from  $\mathcal{R}$  and express  $L(p)$  as a linear combination of values  $L(q)$  using substitutions coming from the relations in  $\mathcal{I}_{\text{MUB}}$  in the following order:

1. If a sequence  $x_{i,j}x_{i',j}$  occurs we use (i), i.e.  $x_{i,j}x_{i',j} = \delta_{i,i'}x_{i,j}$ , to reduce the degree.
2. If a base occurs once we use the  $S_d \wr S_k$ -invariance of  $L$  and the POVM constraint (ii) to reduce the degree by one.
3. If a base occurs more than once but at least one of its elements occurs only once, we take the largest such basis element, say  $x_{i,j}$ , and we replace it by  $I - \sum_{i' \neq i} x_{i',j}$ . This gives  $L(p) = L(p_0) - \sum_{i' \neq i} L(p_{i'})$  where  $p_{i'}$  corresponds to replacing  $x_{i,j}$  by the identity if  $i' = 0$  and by  $x_{i',j}$  if  $i' > 0$ . Using the  $S_d \wr S_k$ -invariance of  $L$  we have  $L(p) = L(p_{i'})$  whenever  $x_{i',j}$  does not occur elsewhere in  $p$ . This expresses  $L(p)$  as a linear combination of ( $L$  of) a monomial of lower degree  $p_0$  and monomials  $p_{i'}$  for which the number of basis elements occurring only once is reduced by one.
4. If a sequence  $x_{i,j}x_{i',j'}x_{i,j}$  occurs, we use (iii) to reduce the degree by two.
5. If a sequence  $x_{i,j}ux_{i,j}vx_{i,j}$  occurs, we use (iv) if  $x_{i,j}vx_{i,j}ux_{i,j}$  results in a monomial that is smaller in the lexicographic order or that can be reduced by (iii).

For each monomial  $q$  we moreover use the tracial property of  $L$ , and the  $S_d \wr S_k$ -invariance of  $L$  to reduce to a lexicographically smallest representative. If  $q$  was not present in  $\mathcal{R}$ , we add it to  $\mathcal{R}$ . If none of the above substitutions can be applied to  $p$ , then we add  $L(p)$  to the list of variables  $\mathcal{L}$ .

**Example 8.1.** Let  $d, k \geq 3$ . The  $S_d \wr S_k$ -invariance and the POVM constraint can be used to show  $L(x_{1,1}x_{1,2}x_{1,3}) = \frac{1}{d} \sum_{j=1}^d L(x_{j,1}x_{1,2}x_{1,3}) = \frac{1}{d} L(x_{1,2}x_{1,3}) = \frac{1}{d^2}$ . In fact, one has to go to  $t = 3$  (degree 6 monomials) to find a free variable, it corresponds to the monomial  $(x_{1,1}x_{1,2}x_{1,3})^2$ .  $\triangle$

The above algorithm in fact does not capture all the linear relations between the values  $L(w)$  for  $w \in \langle x \rangle_{2t}$  that are implied by  $\mathcal{I}_{\text{MUB}}$ . Indeed, since we are not working with a Gröbner basis of  $\mathcal{I}_{\text{MUB}}$ , the above substitution method does not guarantee that  $L = 0$  on the entire ideal  $\mathcal{I}_{\text{MUB}}$ . Computing a Gröbner basis is in general a costly procedure. We therefore use the above procedure only to generate a list of variables for the semidefinite program. We then search for “additional” linear constraints between these variables by explicitly verifying whether  $L = 0$  on  $\mathcal{I}_{\text{MUB}}$ . That is, using the above procedure, we evaluate  $L(qp)$  for, up to symmetry, all polynomials  $q$  defining  $\mathcal{I}_{\text{MUB}}$  and all monomials  $p$  of degree at most  $2t - \deg(q)$ . If  $L(qp) = 0$  leads to a non-trivial constraint, we add it to the semidefinite program (if it is linearly independent of previously added constraints). In Tables 2 and 3 below the resulting number of “additional” linear constraints is listed in the sixth column.

### 8.2 Tables with computational results

In Table 1 (in the introduction) we presented numerical results obtained by solving  $\text{sdp}(d, k, t)$  for fixed  $d, k, t$  using the symmetry reduction and the above described method of determining the value

<sup>11</sup>Recall, the code used is available at <https://github.com/MutuallyUnbiasedBases/>.

of  $L$  on monomials. The columns list the size (number of rows)  $(dk)^{\lfloor t \rfloor}$  of the SDP before symmetry reduction, the number of variables after symmetry reduction, the number of “additional” linear constraints generated by the procedure in the previous section, and the sum and maximum of the block sizes after symmetry reduction. For the block sizes we moreover use the relations defining  $\mathcal{I}_{\text{MUB}}$  to restrict to a subset of the pairs  $(P, Q)$  for which the moment matrix does not contain zero-rows (using relation (i)), or linearly dependent rows (using relations (i) or (iii)). The last column indicates the solution status as reported by SDPA-GMP, SDPA-DD or SDPA [Nak10, YFF<sup>+</sup>12]. We remark that  $\text{sdp}(2, 4, 4.5)$  is infeasible already due to the “additional” linear constraints: they include  $L(1) = 0$ . Below in Table 2 we show additional numerical results for dimension  $d = 6$  to illustrate the size of the involved SDPs. In Table 3 we present the same computational results for the relaxation of  $\text{sdp}(d, k, t)$  obtained by working only with monomials in  $\mathbb{R}\langle x_{1,j} \mid j \in [k] \rangle_{2t}$ .

| $d$ | $k$ | $t$ | $(dk)^{\lfloor t \rfloor}$ | #vars | #linear constraints | block sizes |      | result   |
|-----|-----|-----|----------------------------|-------|---------------------|-------------|------|----------|
|     |     |     |                            |       |                     | sum         | max  |          |
| 6   | 4   | 4.5 | 331776                     | 7     | 0                   | 994         | 107  | feasible |
| 6   | 4   | 5   | 7962624                    | 27    | 2                   | 3697        | 319  | feasible |
| 6   | 4   | 5.5 | 7962624                    | 43    | 3                   | 8049        | 577  | feasible |
| 6   | 7   | 4.5 | 3111696                    | 7     | 0                   | 1627        | 146  | feasible |
| 6   | 7   | 5   | 130691232                  | 38    | 2                   | 6749        | 389  | feasible |
| 6   | 7   | 5.5 | 130691232                  | 62    | 3                   | 18538       | 1107 | feasible |

Table 2: An overview of results for the reduction of the full  $t$ -th level moment matrix, using the symmetry group  $S_d \wr S_k$  (for level  $t$ ) or  $S_{d-1} \times (S_d \wr S_{k-1})$  (for level  $t + \frac{1}{2}$ ).

| $d$ | $k$ | $t$ | $k^{\lfloor t \rfloor}$ | #vars | #linear constraints | block sizes |     | result            |
|-----|-----|-----|-------------------------|-------|---------------------|-------------|-----|-------------------|
|     |     |     |                         |       |                     | sum         | max |                   |
| 2   | 4   | 4.5 | 256                     | 5     | 0                   | 48          | 24  | <b>infeasible</b> |
| 3   | 5   | 4.5 | 625                     | 5     | 0                   | 95          | 32  | <b>infeasible</b> |
| 4   | 6   | 5   | 7776                    | 17    | 2                   | 364         | 70  | <b>infeasible</b> |
| 5   | 7   | 6.5 | 117649                  | 306   | 49                  | 3288        | 640 | <b>infeasible</b> |
| 6   | 4   | 7.5 | 16384                   | 19    | 5                   | 586         | 293 | feasible          |
| 6   | 7   | 6.5 | 117649                  | 306   | 49                  | 3288        | 640 | feasible          |
| 6   | 8   | 6.5 | 262144                  | 306   | 49                  | 4096        | 707 | feasible          |

Table 3: An overview of the bounds for the submatrix of the  $t$ -th level moment matrix indexed by monomials in  $\mathbb{R}\langle x_{1,j} \mid j \in [k] \rangle_{2t}$ , using the symmetry group  $S_k$  (for level  $t$ ) or  $S_{k-1}$  (for level  $t + \frac{1}{2}$ ).

## Acknowledgements

We thank Stefano Pironio and Erik Woodhead for interesting and useful discussions. In particular, we thank Stefano for pointing out that the substitution procedure in Section 8.1 may miss linear constraints, and that infeasibility for  $(d, k) = (2, 4)$  follows from these linear constraints. We thank Erik for independently checking some of our code used to reduce the number of variables. Sander Gribling was partially supported by the projects QUDATA (ANR-18-CE47-0010) and QOPT (QuantERA ERA-NET Cofund 2022-25). Most of this research was carried out while Sander Gribling was affiliated with Université Paris Cité, IRIF, and Sven Polak was affiliated with Centrum Wiskunde & Informatica, Amsterdam.

## References

- [ABMP18] E.A. Aguilar, J.J. Borkala, P. Mironowicz, and M. Pawłowski. Connections between mutually unbiased bases and quantum random access codes. *Phys. Rev. Lett.*, 121:050501, Jul 2018. arXiv:1709.04898v2. doi:10.1103/PhysRevLett.121.050501.

- [BB84] C. H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing*, pages 175–179, 1984. doi:10.1016/j.tcs.2014.05.025.
- [BBE<sup>+</sup>07] I. Bengtsson, W. Bruzda, A. Ericsson, J.-A. Larsson, W. Tadej, and K. Życzkowski. Mutually unbiased bases and hadamard matrices of order six. *Journal of Mathematical Physics*, 48(5):052106, 2007. doi:10.1063/1.2716990.
- [BCKP13] S. Burgdorf, K. Cafuta, I. Klep, and J. Povh. The tracial moment problem and trace-optimization of polynomials. *Mathematical Programming*, 137(1):557–578, 2013. doi:10.1007/s10107-011-0505-8.
- [BGSV12] C. Bachoc, D.C. Gijswijt, A. Schrijver, and F. Vallentin. Invariant semidefinite programs. In M. F. Anjos and J. B. Lasserre, editors, *Handbook on Semidefinite, Conic and Polynomial Optimization*, pages 219–269. Springer, 2012. doi:10.1007/978-1-4614-0769-0\_9.
- [Bla06] B. Blackadar. *Operator Algebras: Theory of  $C^*$ -Algebras and Von Neumann Algebras*. Encyclopaedia of Mathematical Sciences. Springer, 2006. doi:10.1007/3-540-28517-2.
- [BR49] R. H. Bruck and H. J. Ryser. The nonexistence of certain finite projective planes. *Canadian Journal of Mathematics*, 1(1):88–93, 1949. doi:10.4153/CJM-1949-009-2.
- [BR21] G. Blekherman and C. Riener. Symmetric nonnegative forms and sums of squares. *Discrete & Computational Geometry*, 65:764–799, 2021. doi:10.1007/s00454-020-00208-w.
- [BV08] C. Bachoc and F. Vallentin. New upper bounds for kissing numbers from semidefinite programming. *Journal of the American Mathematical Society*, 21:909–924, 2008. doi:10.1090/S0894-0347-07-00589-9.
- [BW09] S. Brierley and S. Weigert. Constructing mutually unbiased bases in dimension six. *Phys. Rev. A*, 79:052316, May 2009. doi:10.1103/PhysRevA.79.052316.
- [BW10] S. Brierley and S. Weigert. Mutually unbiased bases and semi-definite programming. *Journal of Physics: Conference Series*, 254, 2010. doi:10.1088/1742-6596/254/1/012008.
- [CSST13] T. Ceccherini-Silberstein, F. Scarabotti, and F. Tolli. *Representation Theory and Harmonic Analysis of Wreath Products of Finite Groups*. London Mathematical Society Lecture Note Series (410). Cambridge University Press, 2013. doi:10.1017/CB09781107279087.
- [CT03] J. Chuang and K.M. Tan. Representations of wreath products of algebras. *Mathematical Proceedings of the Cambridge Philosophical Society*, 135(3):395–411, 2003. doi:10.1017/S0305004103006984.
- [Del73] P. Delsarte. An algebraic approach to the association schemes of coding theory. *Philips Research Reports Supplements*, 10, 1973.
- [FS92] A. Fässler and E. Stiefel. *Group Theoretical Methods and Their Applications*. Birkhäuser, Basel, 1992. doi:10.1007/978-1-4612-0395-7.
- [Gij09] D.C. Gijswijt. Block diagonalization for algebra’s associated with block codes. *arXiv:0910.4515*, 2009. doi:10.48550/arXiv.0910.4515.
- [GP04] K. Gatermann and P.A. Parrilo. Symmetry groups, semidefinite programs, and sums of squares. *Journal of Pure and Applied Algebra*, 192(1–3):9–128, 2004. doi:10.1016/j.jpaa.2003.12.011.
- [Gra04] M. Grassl. On SIC-POVMs and MUBs in Dimension 6. In *Proceedings ERATO Conference on Quantum Information Science 2004 (EQIS 2004)*, pages 60–61, 2004. doi:10.48550/arXiv.quant-ph/0406175.
- [Gre19] R. Green. *Some properties of Specht modules for the wreath product of symmetric groups*. PhD thesis, University of Kent, 2019. URL: <https://kar.kent.ac.uk/74164/>.
- [HRidZ22] Paweł Horodecki, Łukasz Rudnicki, and Karol Życzkowski. Five open problems in quantum information theory. *PRX Quantum*, 3:010101, Mar 2022. doi:10.1103/PRXQuantum.3.010101.
- [Iva81] I.D. Ivanović. Geometrical description of quantal state determination. *Journal of Physics A: Mathematical and General*, 14(12):3241–3245, 1981. doi:10.1088/0305-4470/14/12/019.
- [KDP11] E. de Klerk, C. Dobre, and D.V. Pasechnik. Numerical block diagonalization of matrix \*-algebras with application to semidefinite programming. *Mathematical Programming*, 129:91, 2011. doi:10.1007/s10107-011-0461-3.
- [Ker71] A. Kerber. *Representations of Permutation Groups I*. Lecture Notes in Mathematics. Springer-Verlag, 1971. doi:10.1007/BFb0067943.

- [KP16] I. Klep and J. Povh. Constrained trace-optimization of polynomials in freely noncommuting variables. *Journal of Global Optimization*, 64(2):325–348, 2016. doi:10.1007/s10898-015-0308-1.
- [KPS07] E. de Klerk, D. Pasechnik, and A. Schrijver. Reductions of symmetric semidefinite programs using the regular  $*$ -representation. *Mathematical Programming*, 109:613–624, 2007. doi:10.1007/s10107-006-0039-7.
- [KPS09] E. de Klerk, D.V. Pasechnik, and R. Sotirov. On semidefinite programming relaxations of the traveling salesman problem. *SIAM Journal on Optimization*, 19(4):1559–1573, 2009. doi:10.1137/070711141.
- [KS10] E. de Klerk and R. Sotirov. Exploiting group symmetry in semidefinite programming relaxations of the quadratic assignment problem. *Mathematical Programming*, 122(2):225–246, 2010. doi:10.1007/s10107-008-0246-5.
- [Las01] J. B. Lasserre. Global optimization with polynomials and the problem of moments. *SIAM Journal on Optimization*, 11(3):796–817, 2001. doi:10.1137/S1052623400366802.
- [Las09] J. B. Lasserre. *Moments, Positive Polynomials and Their Applications*. Imperial College Press, 2009. doi:10.1142/p665.
- [Lau09] M. Laurent. Sums of squares, moment matrices and optimization over polynomials. In M. Putinar and S. Sullivant, editors, *Emerging Applications of Algebraic Geometry*, pages 157–270. Springer, 2009. doi:10.1007/978-0-387-09686-5\_7.
- [LPS17] B. Litjens, S. Polak, and A. Schrijver. Semidefinite bounds for nonbinary codes based on quadruples. *Designs, Codes and Cryptography*, 84:87–100, 2017. doi:10.1007/s10623-016-0216-5.
- [Mac80] I.G. MacDonald. Polynomial functors and wreath products. *Journal of Pure and Applied Algebra*, 18(2):173–204, 1980. doi:10.1016/0022-4049(80)90128-0.
- [MKKK10] K. Murota, Y. Kanno, M. Kojima, and S. Kojima. A numerical algorithm for block-diagonal decomposition of matrix  $*$ -algebras with application to semidefinite programming. *Japan Journal of Industrial and Applied Mathematics*, 27:125–160, 2010. doi:10.1007/s13160-010-0006-9.
- [Nak10] M. Nakata. A numerical evaluation of highly accurate multiple-precision arithmetic version of semidefinite programming solver: SDPA-GMP, -QD and -DD. In *2010 IEEE International Symposium on Computer-Aided Control System Design*, pages 29–34, 2010. doi:10.1109/CACSD.2010.5612693.
- [NPA12] M. Navascués, S. Pironio, and A. Acín. SDP relaxations for non-commutative polynomial optimization. In M. F. Anjos and J. B. Lasserre, editors, *Handbook on Semidefinite, Conic and Polynomial Optimization*, pages 601–634. Springer, 2012. doi:10.1007/978-1-4614-0769-021.
- [NV15] M. Navascués and T. Vértesi. Bounding the set of finite dimensional quantum correlations. *Phys. Rev. Lett.*, 115:020501, Jul 2015. doi:10.1103/PhysRevLett.115.020501.
- [Par00] P. A. Parrilo. *Structured Semidefinite Programs and Semialgebraic Geometry Methods in Robustness and Optimization*. PhD thesis, Caltech, 2000. doi:10.7907/2K6Y-CH43.
- [PNA10] S. Pironio, M. Navascués, and A. Acín. Convergent relaxations of polynomial optimization problems with noncommuting variables. *SIAM Journal on Optimization*, 20(5):2157–2180, 2010. doi:10.1137/090760155.
- [Pol19] S.C. Polak. *New Methods in Coding Theory: Error-Correcting Codes and the Shannon Capacity*. PhD thesis, University of Amsterdam, 2019. URL: <https://hdl.handle.net/11245.1/393eb25b-c1ba-4c6f-89e8-c439a97358b6>.
- [RMMB21] D. Rosset, F. Montealegre-Mora, and JD Bancal. RepLAB: A Computational/Numerical Approach to Representation Theory. In M.B. Paranjape, R. MacKenzie, Z. Thomova, P. Winternitz, and W. Witzak-Krempa, editors, *Quantum Theory and Symmetries*, CRM Series in Mathematical Physics. Springer, 2021. doi:10.1007/978-3-030-55777-5\_60.
- [RTJAL13] C. Riener, T. Theobald, L. Jansson Andrén, and J.B. Lasserre. Exploiting symmetry in sdp-relaxations for polynomial optimization. *Mathematics of Operations Research*, 38:122–141, 2013. doi:10.1287/moor.1120.0558.
- [Sag01] B.E. Sagan. *The symmetric group*, volume 203 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 2001. doi:10.1007/978-1-4757-6804-6.



- [Sch79] A. Schrijver. A comparison of the Delsarte and Lovász bounds. *IEEE Transactions on Information Theory*, 25(4):425–429, 1979. doi:10.1109/TIT.1979.1056072.
- [Sch05] A. Schrijver. New code upper bounds from the terwilliger algebra and semidefinite programming. *IEEE Transactions on Information Theory*, 51(8):2859–2866, 2005. doi:10.1109/TIT.2005.851748.
- [SHB<sup>+</sup>12] C. Spengler, M. Huber, S. Brierley, T. Adaktylos, and B.C. Hiesmayr. Entanglement detection via mutually unbiased bases. *Phys. Rev. A*, 86:022311, Aug 2012. doi:10.1103/PhysRevA.86.022311.
- [Tar01] Gaston Tarry. Le problème des 36 officiers. *Compte Rendu de l'Association Francaise pour l'Avancement des Sciences*, 2:170–203, 1901.
- [WB05] P. Wocjan and T. Beth. New construction of mutually unbiased bases in square dimensions. *Quantum Inf. Comput.*, 5(2):93–101, 2005. doi:10.26421/QIC5.2-1.
- [Wei13] M. Weiner. A gap for the maximum number of mutually unbiased bases. *Proceedings of the American Mathematical Society*, 141(6):1963–1969, 2013. doi:10.1090/S0002-9939-2013-11487-5.
- [WF89] W.K. Wootters and B.D. Fields. Optimal state-determination by mutually unbiased measurements. *Annals of Physics*, 191(2):363 – 381, 1989. doi:10.1016/0003-4916(89)90322-9.
- [Woo06] W.K. Wootters. Quantum Measurements and Finite Geometry. *Found Phys*, 36:112–126, 2006. doi:10.1007/s10701-005-9008-x.
- [YFF<sup>+</sup>12] M. Yamashita, K. Fujisawa, M. Fukuda, K. Kobayashi, K. Nakata, and M. Nakata. Latest developments in the SDPA Family for solving large-scale SDPs. In M. F. Anjos and J. B. Lasserre, editors, *Handbook on Semidefinite, Conic and Polynomial Optimization*, pages 687–714. Springer, 2012. doi:10.1007/978-1-4614-0769-0\_24.
- [Zau99] G. Zauner. *Quantendesigns: Grundzüge einer nichtkommutativen Designtheorie*. PhD thesis, University of Vienna, 1999. Also published as *Quantum designs: foundations of a noncommutative design theory*, International Journal of Quantum Information 09(01):445–507, 2011. doi:10.1142/S0219749911006776.

## A $C^*$ -algebraic formulation of the MUB problem

The theorem below was proven in [NPA12], we give a slightly simpler proof (inspired by their proof).

**Theorem 3.2** ([NPA12]). *There exists a set of  $k$  MUBs in dimension  $d$  if and only if there exists a  $(d, k)$ -MUB-algebra with  $I \neq 0$ .*

*Proof.* Let  $\{u_{i,1}\}_{i \in [d]}, \{u_{i,2}\}_{i \in [d]}, \dots, \{u_{i,k}\}_{i \in [d]}$  be ONB's of  $\mathbb{C}^d$ . Let  $X_{i,j} = u_{i,j}u_{i,j}^*$  be the rank-1 projector associated to  $u_{i,j}$  for all  $i \in [d], j \in [k]$ . Then the  $C^*$ -algebra  $\mathcal{A} = \mathbb{C}\langle \mathbf{X} \rangle$  generated by the  $X_{i,j}$ , and the Hermitian operators  $X_{i,j}$ , satisfy the relations (i) to (iv).

Conversely, suppose there exist  $\mathcal{A}$  and Hermitian  $X_{i,j} \in \mathcal{A}$  satisfying the relations (i) to (iv). We show how to construct  $k$  mutually unbiased bases in dimension  $d$ . For all  $i \in [d], j \in [k]$ , let  $Z_{ij} \in M_d(\mathcal{A})$  be defined as<sup>12</sup>

$$Z_{i,j} := d \left[ X_{1,2} X_{a,1} X_{i,j} X_{b,1} X_{1,2} \right]_{a,b \in [d]}.$$

Clearly the matrices  $Z_{i,j}$  are Hermitian. We now verify that the matrices  $Z_{ij}$  satisfy the relations (i) and (iii). Let  $i, i' \in [d], j, j' \in [k]$ , we have

$$\begin{aligned} (Z_{i,j} Z_{i',j'})_{a,b} &= d^2 \sum_{c \in [d]} X_{1,2} X_{a,1} X_{i,j} X_{c,1} X_{1,2} X_{c,1} X_{i',j'} X_{b,1} X_{1,2} \\ &\stackrel{(i),(iii)}{=} d^2 \cdot \frac{1}{d} \sum_{c \in [d]} X_{1,2} X_{a,1} X_{i,j} X_{c,1} X_{i',j'} X_{b,1} X_{1,2} \\ &\stackrel{(ii)}{=} d X_{1,2} X_{a,1} X_{i,j} X_{i',j'} X_{b,1} X_{1,2}. \end{aligned}$$

When  $j = j'$  the above shows, together with (i) for the  $X_{i,j}$ 's, that  $Z_{i,j} Z_{i',j} = \delta_{i,i'} Z_{i,j}$ . A similar computation shows that when  $j \neq j'$  we have  $Z_{i,j} Z_{i',j'} Z_{i,j} = \frac{1}{d} Z_{i,j}$ . Finally, using relation (ii) we see that  $\sum_{a,b \in [d]} \sum_{i \in [d]} (Z_{i,j})_{a,b} = d X_{1,2}$ . It follows from (ii) and (iii) for the  $X_{i,j}$ 's that  $X_{1,2} \neq 0$ . Hence  $\sum_{i \in [d]} Z_{i,j} \neq 0$ , and since (iii) holds for the  $Z_{i,j}$ , we therefore have that  $Z_{i,j} \neq 0$  for all  $i, j$ .

Now observe that  $\mathbb{C}\langle X_{1,2} X_{a,1} X_{i,j} X_{b,1} X_{1,2} : a, b, i \in [d], j \in [k] \rangle$  is a commutative  $C^*$ -algebra because of (iv). We will restrict our attention to this sub-algebra and refer to it as  $\mathcal{A}$ . A commutative  $C^*$ -algebra can be viewed as an algebra of continuous functions in the following sense, see, e.g., [Bla06, II.2.2.4]. Using the Gelfand representation, any commutative  $C^*$ -algebra  $\mathcal{A}$  is  $*$ -isomorphic to  $C_0(\hat{\mathcal{A}})$ , where  $\hat{\mathcal{A}}$  is the set of non-zero  $*$ -homomorphisms from  $\mathcal{A}$  to  $\mathbb{C}$  (i.e., the set of characters), and  $C_0(\hat{\mathcal{A}})$  is the set of continuous functions on  $\hat{\mathcal{A}}$  that vanish at infinity ( $\hat{\mathcal{A}}$  is a locally compact Hausdorff space, using the weak- $*$  topology). We may thus write

$$Z_{i,j} := d \left[ \Theta_{a,b}^{i,j}(\hat{a}) \right]_{a,b \in [d]}$$

where  $\Theta_{a,b}^{i,j} \in C_0(\hat{\mathcal{A}})$  and  $\hat{a} \in \hat{\mathcal{A}}$ .

Now for each  $\hat{a} \in \hat{\mathcal{A}}$  define  $Z_{i,j}^{\hat{a}} := d [\Theta_{a,b}^{i,j}(\hat{a})]_{a,b \in [d]}$ . Since the multiplication in  $C_0(\hat{\mathcal{A}})$  is pointwise, the relations (ii) and (iii) also hold for the matrices  $Z_{i,j}^{\hat{a}}$  (for  $i \in [d], j \in [k]$ ). Fix  $i' \in [d], j' \in [k]$ . Since  $Z_{i',j'} \neq 0$  there exists an  $\hat{a}$  such that  $Z_{i',j'}^{\hat{a}} \neq 0$ . Since (iii) holds for the matrices  $Z_{i,j}^{\hat{a}}$  ( $i \in [d], j \in [k]$ ), we know that all of them are non-zero. Together with (i) this implies that each  $Z_{i,j}^{\hat{a}}$  has rank equal to 1. Thus for each  $j \in [k]$ , the projectors  $Z_{i,j}^{\hat{a}}$  ( $i \in [d]$ ) define an orthonormal basis. Relation (iii) for the  $Z_{i,j}$ 's implies that these bases are mutually unbiased.  $\square$

<sup>12</sup>The choice for 1 and 2 here is arbitrary. All that matters is they are fixed and different.