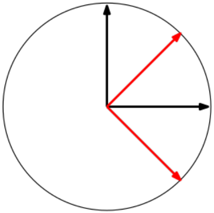
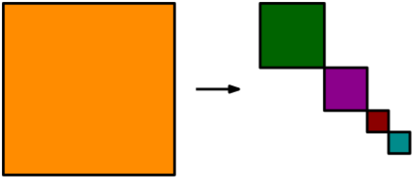
Mutually unbiased bases: polynomial optimization and symmetry

Sander Gribling, IRIF





Based on joint work with Sven Polak (CWI)
`arXiv:2111.05698`

INSTITUT
DE RECHERCHE
EN INFORMATIQUE
FONDAMENTALE

Mutually unbiased bases (MUBs)

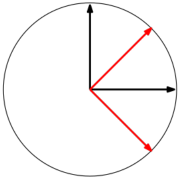
Definition

Let $d \in \mathbb{N}_{\geq 2}$. A set of k orthonormal bases of $\mathbb{C}^d$ is *mutually unbiased* if for every pair of basis vectors e, f from *distinct* bases we have

$$|\langle e, f \rangle|^2 = \frac{1}{d}.$$

Example: 3 MUBs in dimension 2

$$\left\{ \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right\}, \left\{ \tfrac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \tfrac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix} \right\},$$
$$\left\{ \tfrac{1}{\sqrt{2}} \begin{pmatrix} \mathbf{i} \\ 1 \end{pmatrix}, \tfrac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ \mathbf{i} \end{pmatrix} \right\}.$$



Mutually unbiased bases (MUBs)

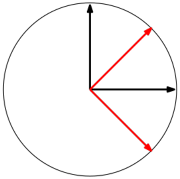
Definition

Let $d \in \mathbb{N}_{\geq 2}$. A set of k orthonormal bases of $\mathbb{C}^d$ is *mutually unbiased* if for every pair of basis vectors e, f from *distinct* bases we have

$$|\langle e, f \rangle|^2 = \frac{1}{d}.$$

Example: 3 MUBs in dimension 2

$$\left\{ \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right\}, \left\{ \tfrac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \tfrac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix} \right\},$$
$$\left\{ \tfrac{1}{\sqrt{2}} \begin{pmatrix} \mathbf{i} \\ 1 \end{pmatrix}, \tfrac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ \mathbf{i} \end{pmatrix} \right\}.$$



Question: *what is the largest number of MUBs in dimension d?*

Why are MUBs useful?

MUBs yield *complementary* measurements:

- If the outcome with respect to $\{u_i\}_{i\in[d]}$ is deterministic (say u_1), then the outcome with respect to a MUB $\{v_j\}_{j\in[d]}$ is uniformly random.
  (Since $|u_1^* v_j|^2 = 1/d$ then describes the probability of outcome v_j)

Why are MUBs useful?

MUBs yield *complementary* measurements:

- If the outcome with respect to $\{u_i\}_{i\in[d]}$ is deterministic (say u_1), then the outcome with respect to a MUB $\{v_j\}_{j\in[d]}$ is uniformly random.
  (Since $|u_1^* v_j|^2 = 1/d$ then describes the probability of outcome v_j)

This makes MUBs useful for, e.g., cryptography.
Other application: tomography (next slide).

Why are MUBs useful?

MUBs yield *complementary* measurements:

- If the outcome with respect to $\{u_i\}_{i \in [d]}$ is deterministic (say u_1), then the outcome with respect to a MUB $\{v_j\}_{j \in [d]}$ is uniformly random.
  (Since $|u_1^* v_j|^2 = 1/d$ then describes the probability of outcome v_j)

This makes MUBs useful for, e.g., cryptography.
Other application: tomography (next slide).

For much more information, see the excellent survey **"On mutually unbiased bases"** of Durt, Englert, Bengtsson, and Życzkowski (2010).

Why are MUBs useful?

MUBs yield *complementary* measurements:

- If the outcome with respect to $\{u_i\}_{i\in[d]}$ is deterministic (say u_1), then the outcome with respect to a MUB $\{v_j\}_{j\in[d]}$ is uniformly random.
  (Since $|u_1^* v_j|^2 = 1/d$ then describes the probability of outcome v_j)

This makes MUBs useful for, e.g., cryptography.
Other application: tomography (next slide).

For much more information, see the excellent survey **"On mutually unbiased bases"** of Durt, Englert, Bengtsson, and Życzkowski (2010).

Listed as one of 'Five Open Problems in Quantum Information Theory' [Horodecki-Rudnicki-Życzkowski'22]: **prize** EUR 2022!

Known results (obstructions)

- A dimension-counting argument shows there can be at most $d+1$ MUBs in dimension d.

Known results (obstructions)

- A dimension-counting argument shows there can be at most $d+1$ MUBs in dimension d.

Proof. For a vector $e \in \mathbb{C}^d$, define

$$M(e) := ee^* - I_d/d.$$

Known results (obstructions)

- A dimension-counting argument shows there can be at most $d + 1$ MUBs in dimension d.

Proof. For a vector $e \in \mathbb{C}^d$, define

$$M(e) := ee^* - I_d/d.$$

ONB $\longrightarrow$ dim-(d-1) subspace of traceless Hermitian $d \times d$ matrices.

Known results (obstructions)

- A dimension-counting argument shows there can be at most $d+1$ MUBs in dimension d.

Proof. For a vector $e \in \mathbb{C}^d$, define

$$M(e) := ee^* - I_d/d.$$

ONB $\longrightarrow$ dim-(d-1) subspace of traceless Hermitian $d \times d$ matrices.

Then,

$$\mathrm{Tr}(M(u)M(v)) = |u^*v|^2 - 1/d.$$

Known results (obstructions)

- A dimension-counting argument shows there can be at most $d+1$ MUBs in dimension d.

Proof. For a vector $e \in \mathbb{C}^d$, define

$$M(e) := ee^* - I_d/d.$$

ONB $\longrightarrow$ dim-(d-1) subspace of traceless Hermitian $d \times d$ matrices.

Then,

$$\mathrm{Tr}(M(u)M(v)) = |u^* v|^2 - 1/d.$$

MUBs $\longrightarrow$ *orthogonal* subspaces.

$\Longrightarrow$ at most $(d^2-1)/(d-1) = d+1$ MUBs in dimension d. $\square$

Known results (constructions)

- $d + 1$ MUBs exist in dimension d when d is prime [Ivanovic'81], or when $d = p^n$ for p prime [Wootters-Fields'89]

Known results (constructions)

- $d+1$ MUBs exist in dimension d when d is prime [Ivanovic'81], or when $d = p^n$ for p prime [Wootters-Fields'89]

No set of $d+1$ MUBs is known when $d \neq p^n$.

Known results (constructions)

- $d + 1$ MUBs exist in dimension d when d is prime [Ivanovic'81], or when $d = p^n$ for p prime [Wootters-Fields'89]

No set of $d + 1$ MUBs is known when $d \neq p^n$.

Other constructions:

- Taking tensor products: If k MUBs exist in dimensions d_1 and d_2, then k MUBs exist in dimension $d_1 d_2$.

Known results (constructions)

- $d + 1$ MUBs exist in dimension d when d is prime [Ivanovic'81], or when $d = p^n$ for p prime [Wootters-Fields'89]

No set of $d + 1$ MUBs is known when $d \neq p^n$.

Other constructions:

- Taking tensor products: If k MUBs exist in dimensions d_1 and d_2, then k MUBs exist in dimension $d_1 d_2$.
- k mutually orthogonal Latin squares of order n yield $k + 2$ MUBs in dimension n^2. [Wocjan-Beth'05]
    - For $d = 26^2$ this yields 6 MUBs (instead of $2^2 + 1$ which one would expect from $26^2 = 2^2 13^2$ and the tensor-product strategy).

Known results (constructions)

- $d + 1$ MUBs exist in dimension d when d is prime [Ivanovic'81], or when $d = p^n$ for p prime [Wootters-Fields'89]

No set of $d + 1$ MUBs is known when $d \neq p^n$.

Other constructions:

- Taking tensor products: If k MUBs exist in dimensions d_1 and d_2, then k MUBs exist in dimension $d_1 d_2$.
- k mutually orthogonal Latin squares of order n yield $k + 2$ MUBs in dimension n^2. [Wocjan-Beth'05]
  - For $d = 26^2$ this yields 6 MUBs (instead of $2^2 + 1$ which one would expect from $26^2 = 2^2 13^2$ and the tensor-product strategy).
- If there exist d MUBs, then there exist $d + 1$ MUBs [Weiner'13]

Known results (constructions)

- $d+1$ MUBs exist in dimension d when d is prime [Ivanovic'81], or when $d = p^n$ for p prime [Wootters-Fields'89]

No set of $d+1$ MUBs is known when $d \neq p^n$.

Other constructions:

- Taking tensor products: If k MUBs exist in dimensions d_1 and d_2, then k MUBs exist in dimension $d_1 d_2$.
- k mutually orthogonal Latin squares of order n yield $k+2$ MUBs in dimension n^2. [Wocjan-Beth'05]
  - For $d = 26^2$ this yields 6 MUBs (instead of 2^2+1 which one would expect from $26^2 = 2^2 13^2$ and the tensor-product strategy).
- If there exist d MUBs, then there exist $d+1$ MUBs [Weiner'13]

Widely believed that no more than 3 MUBs exist in dimension 6, but no formal proof (yet).

Known results (finite geometry)

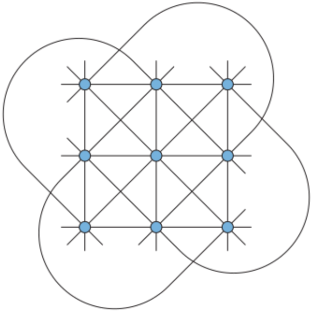


Figure: Finite affine plane of order 3, source: Wiki

Known results (finite geometry)

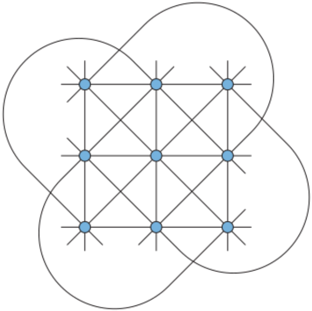


Figure: Finite affine plane of order 3, source: Wiki

MUBs	**Finite affine plane**
$d+1$ orthonormal bases	$d+1$ equivalence classes of d parallel lines

Known results (finite geometry)

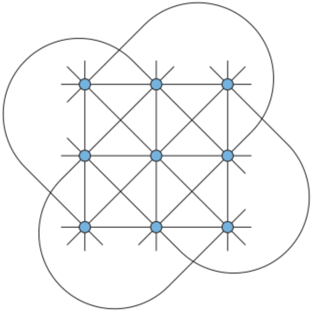


Figure: Finite affine plane of order 3, source: Wiki

MUBs	Finite affine plane
$d+1$ orthonormal bases	$d+1$ equivalence classes of d parallel lines
unit vectors	lines contain d points

Known results (finite geometry)

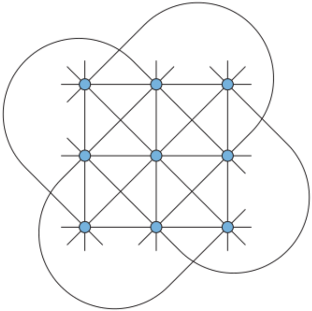


Figure: Finite affine plane of order 3, source: Wiki

MUBs	**Finite affine plane**
$d+1$ orthonormal bases	$d+1$ equivalence classes of d parallel lines
unit vectors	lines contain d points
$\|\langle e, f \rangle\| = 1/d$	$\|\ell \cap k\| = 1$

Known results (finite geometry)

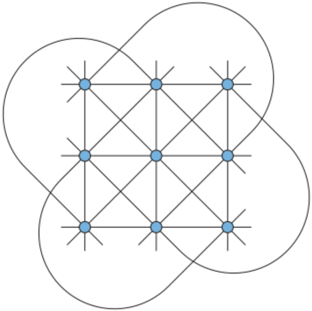


Figure: Finite affine plane of order 3, source: Wiki

MUBs	**Finite affine plane**
$d+1$ orthonormal bases	$d+1$ equivalence classes of d parallel lines
unit vectors	lines contain d points
$\lvert\langle e, f\rangle\rvert = 1/d$	$\lvert\ell \cap k\rvert = 1$
Exist if $d = p^n$	Exist if $d = p^n$

Known results (finite geometry)

Theorem (Bruck-Ryser'49)

If $d \equiv 1, 2 \bmod 4$ and d is not the sum of two squares, then there does not exist a finite affine plane of order d.

Implies that no finite affine plane of order 6 exists.

Known results (finite geometry)

Theorem (Bruck-Ryser'49)

If $d \equiv 1, 2 \bmod 4$ and d is not the sum of two squares, then there does not exist a finite affine plane of order d.

Implies that no finite affine plane of order 6 exists.

No such proof of non-existence is known for MUBs. Similar techniques only lead to:

Weak analogue for MUBs

If $d \equiv 2 \bmod 4$ and d is not a sum of two squares, then there does not exist a complete set of MUBs with $uu^* \in \mathbb{Q}^{d \times d} + \mathbf{i}\,\mathbb{Q}^{d \times d}$ for all basis elements u.

Known results (finite geometry)

Theorem (Bruck-Ryser'49)

If $d \equiv 1, 2 \bmod 4$ and d is not the sum of two squares, then there does not exist a finite affine plane of order d.

Implies that no finite affine plane of order 6 exists.

No such proof of non-existence is known for MUBs. Similar techniques only lead to:

Weak analogue for MUBs

If $d \equiv 2 \bmod 4$ and d is not a sum of two squares, then there does not exist a complete set of MUBs with $uu^* \in \mathbb{Q}^{d\times d} + \mathbf{i}\,\mathbb{Q}^{d\times d}$ for all basis elements u.

Proof uses sum of squares (of integers) and such MUBs to build an integral solution to $dx^2 = y^2 + z^2$.

Prior work using polynomials/SDPs

Approach 1: $\exists k$ MUBs in dim $d \Leftrightarrow$ a system $\{f_1(x) = 0, \ldots, f_N(x) = 0\}$ of polynomial equations in $2kd^2$ real variables has a real solution.

Prior work using polynomials/SDPs

Approach 1: $\exists k$ MUBs in dim $d \Leftrightarrow$ a system $\{f_1(x) = 0, \ldots, f_N(x) = 0\}$ of polynomial equations in $2kd^2$ real variables has a real solution.

1. *weak Nullstellensatz:*
   Non-existence if 1 lies in the ideal generated by $f_1, \ldots, f_N$

Prior work using polynomials/SDPs

Approach 1: $\exists k$ MUBs in dim $d \Leftrightarrow$ a system $\{f_1(x) = 0, \ldots, f_N(x) = 0\}$ of polynomial equations in $2kd^2$ real variables has a real solution.

1. *weak Nullstellensatz:*
   Non-existence if 1 lies in the ideal generated by $f_1, \ldots, f_N$
2. [Brierly-Weigert'10]:

$$\min f_1(x)^2 \quad \text{s.t.} \quad f_i(x) = 0 \text{ for } i = 2, \ldots, N.$$

$\rightarrow$ Apply polynomial optimization techniques (Lasserre)

Prior work using polynomials/SDPs

Approach 2: Noncommutative polynomial optimization formulations.

1. Use a C^*-algebra formulation of NPA:

Theorem (Navascués-Pironio-Acín'12)

There exist k MUBs in dimension $d \Leftrightarrow$ there exists a (d, k)-MUB-algebra.

Prior work using polynomials/SDPs

Approach 2: Noncommutative polynomial optimization formulations.

1. Use a C^*-algebra formulation of NPA:

Theorem (Navascués-Pironio-Acín'12)

There exist k MUBs in dimension $d \Leftrightarrow$ there exists a (d, k)-MUB-algebra.

Uses kd noncommutative variables! (vs $2kd^2$ real vars previously)

Prior work using polynomials/SDPs

Approach 2: Noncommutative polynomial optimization formulations.

1. Use a C^*-algebra formulation of NPA:

Theorem (Navascués-Pironio-Acín'12)

There exist k MUBs in dimension $d \Leftrightarrow$ there exists a (d, k)-MUB-algebra.

Uses kd noncommutative variables! (vs $2kd^2$ real vars previously)

2. Construct a nonlocal game such that value p is attained $\Leftrightarrow$ k MUBs exist in dim d.

Prior work using polynomials/SDPs

Approach 2: Noncommutative polynomial optimization formulations.

1. Use a C^*-algebra formulation of NPA:

Theorem (Navascués-Pironio-Acín'12)

There exist k MUBs in dimension $d \Leftrightarrow$ there exists a (d, k)-MUB-algebra.

Uses kd noncommutative variables! (vs $2kd^2$ real vars previously)

2. Construct a nonlocal game such that value p is attained
   $\Leftrightarrow$ k MUBs exist in dim d.
   [Aguilar-Borkała-Mironowicz-Pawłowski'18] formulate a game based on quantum random access codes: the $(k, 2)^d \to 1$ *pQRAC game*

Our contributions

The C^*-algebraic formulation of Navascués, Pironio, and Acín (2012) is symmetric under an action of the wreath product $S_d \wr S_k$.

Our contributions

The C^*-algebraic formulation of Navascués, Pironio, and Acín (2012) is symmetric under an action of the wreath product $S_d \wr S_k$.

- We give the full symmetry reduction of the SDP-relaxations of their formulation.

Our contributions

The C^*-algebraic formulation of Navascués, Pironio, and Acín (2012) is symmetric under an action of the wreath product $S_d \wr S_k$.

- We give the full symmetry reduction of the SDP-relaxations of their formulation.

Main contribution: an explicit decomposition of certain “L-shaped” “permutation” modules for $S_d \wr S_k$ into irreducible “Specht” modules.

Our contributions

The C^*-algebraic formulation of Navascués, Pironio, and Acín (2012) is symmetric under an action of the wreath product $S_d \wr S_k$.

- We give the full symmetry reduction of the SDP-relaxations of their formulation.

Main contribution: an explicit decomposition of certain "L-shaped" "permutation" modules for $S_d \wr S_k$ into irreducible "Specht" modules.

- This allows us to compute high(er) levels of the hierarchy. (Currently up to level 5.5 for $(d, k) = (6, 7)$).

Our contributions

The C^*-algebraic formulation of Navascués, Pironio, and Acín (2012) is symmetric under an action of the wreath product $S_d \wr S_k$.

- We give the full symmetry reduction of the SDP-relaxations of their formulation.

Main contribution: an explicit decomposition of certain "L-shaped" "permutation" modules for $S_d \wr S_k$ into irreducible "Specht" modules.

- This allows us to compute high(er) levels of the hierarchy. (Currently up to level 5.5 for $(d, k) = (6, 7)$).
- (Numerical) Sum-of-Squares proof that no $d + 2$ MUBs exist in dimensions $d = 2, 3, 4, 5, 6, 7, 8$.

MUB-algebra

- A unit vector e corresponds to a rank-1 projector ee^*.

MUB-algebra

- A unit vector e corresponds to a rank-1 projector ee^*.
- A set of k MUBs $\{\{u_{i,j}\}_{i\in[d]} : j \in [k]\}$ corresponds to a set of rank-1 d-by-d projectors $X_{i,j} = u_{i,j}u_{i,j}^*$ satisfying the following relations:

MUB-algebra

- A unit vector e corresponds to a rank-1 projector ee^*.
- A set of k MUBs $\{\{u_{i,j}\}_{i\in[d]} : j \in [k]\}$ corresponds to a set of rank-1 d-by-d projectors $X_{i,j} = u_{i,j}u_{i,j}^*$ satisfying the following relations:

Definition

A C^*-algebra $\mathcal{A}$ is a (d,k)-*MUB-algebra* if it contains Herm. elements $X_{i,j}$ for $i \in [d], j \in [k]$ that satisfy the following relations:

1. $X_{i,j}X_{i',j} = \delta_{i,i'}X_{i,j}$ for all $i, i' \in [d], j \in [k]$,

MUB-algebra

- A unit vector e corresponds to a rank-1 projector ee^*.
- A set of k MUBs $\{\{u_{i,j}\}_{i\in[d]} : j \in [k]\}$ corresponds to a set of rank-1 d-by-d projectors $X_{i,j} = u_{i,j}u_{i,j}^*$ satisfying the following relations:

Definition

A C^*-algebra $\mathcal{A}$ is a (d,k)-*MUB-algebra* if it contains Herm. elements $X_{i,j}$ for $i \in [d], j \in [k]$ that satisfy the following relations:

1. $X_{i,j}X_{i',j} = \delta_{i,i'}X_{i,j}$ for all $i, i' \in [d], j \in [k]$,
2. $\sum_{i\in[d]} X_{i,j} = I$ for all $j \in [k]$,

MUB-algebra

- A unit vector e corresponds to a rank-1 projector ee^*.
- A set of k MUBs $\{\{u_{i,j}\}_{i\in[d]} : j \in [k]\}$ corresponds to a set of rank-1 d-by-d projectors $X_{i,j} = u_{i,j}u_{i,j}^*$ satisfying the following relations:

Definition

A C^*-algebra $\mathcal{A}$ is a (d,k)-*MUB-algebra* if it contains Herm. elements $X_{i,j}$ for $i \in [d], j \in [k]$ that satisfy the following relations:

1. $X_{i,j}X_{i',j} = \delta_{i,i'}X_{i,j}$ for all $i, i' \in [d], j \in [k]$,
2. $\sum_{i\in[d]} X_{i,j} = I$ for all $j \in [k]$,
3. $X_{i,j}X_{i',j'}X_{i,j} = \frac{1}{d}X_{i,j}$ for all $i, i' \in [d], j, j' \in [k]$ with $j \neq j'$,

MUB-algebra

- A unit vector e corresponds to a rank-1 projector ee^*.
- A set of k MUBs $\{\{u_{i,j}\}_{i\in[d]} : j \in [k]\}$ corresponds to a set of rank-1 d-by-d projectors $X_{i,j} = u_{i,j}u_{i,j}^*$ satisfying the following relations:

Definition

A C^*-algebra $\mathcal{A}$ is a (d,k)-*MUB-algebra* if it contains Herm. elements $X_{i,j}$ for $i \in [d], j \in [k]$ that satisfy the following relations:

1. $X_{i,j}X_{i',j} = \delta_{i,i'}X_{i,j}$ for all $i, i' \in [d], j \in [k]$,
2. $\sum_{i\in[d]} X_{i,j} = I$ for all $j \in [k]$,
3. $X_{i,j}X_{i',j'}X_{i,j} = \frac{1}{d}X_{i,j}$ for all $i, i' \in [d], j, j' \in [k]$ with $j \neq j'$,
4. $[X_{i,j}UX_{i,j}, X_{i,j}VX_{i,j}] = 0$ for all $i \in [d], j \in [k]$ and $U, V \in \langle \mathbf{X} \rangle$.

MUB-algebra

- A unit vector e corresponds to a rank-1 projector ee^*.
- A set of k MUBs $\{\{u_{i,j}\}_{i\in[d]} : j \in [k]\}$ corresponds to a set of rank-1 d-by-d projectors $X_{i,j} = u_{i,j}u_{i,j}^*$ satisfying the following relations:

Definition

A C^*-algebra $\mathcal{A}$ is a (d,k)-*MUB-algebra* if it contains Herm. elements $X_{i,j}$ for $i \in [d], j \in [k]$ that satisfy the following relations:

1. $X_{i,j}X_{i',j} = \delta_{i,i'}X_{i,j}$ for all $i, i' \in [d], j \in [k]$,
2. $\sum_{i\in[d]} X_{i,j} = I$ for all $j \in [k]$,
3. $X_{i,j}X_{i',j'}X_{i,j} = \frac{1}{d}X_{i,j}$ for all $i, i' \in [d], j, j' \in [k]$ with $j \neq j'$,
4. $[X_{i,j}UX_{i,j}, X_{i,j}VX_{i,j}] = 0$ for all $i \in [d], j \in [k]$ and $U, V \in \langle \mathbf{X} \rangle$.

Theorem (Navascués-Pironio-Acín'12)

There exist k MUBs in dimension d $\Leftrightarrow$ there exists a (d,k)-MUB-algebra.

MUB-algebra

- A unit vector e corresponds to a rank-1 projector ee^*.
- A set of k MUBs $\{\{u_{i,j}\}_{i\in[d]} : j \in [k]\}$ corresponds to a set of rank-1 d-by-d projectors $X_{i,j} = u_{i,j}u_{i,j}^*$ satisfying the following relations:

Definition

A C^*-algebra $\mathcal{A}$ is a (d,k)-*MUB-algebra* if it contains Herm. elements $X_{i,j}$ for $i \in [d], j \in [k]$ that satisfy the following relations:

1. $X_{i,j}X_{i',j} = \delta_{i,i'}X_{i,j}$ for all $i, i' \in [d], j \in [k]$,
2. $\sum_{i\in[d]} X_{i,j} = I$ for all $j \in [k]$,
3. $X_{i,j}X_{i',j'}X_{i,j} = \frac{1}{d}X_{i,j}$ for all $i, i' \in [d], j, j' \in [k]$ with $j \neq j'$,
4. $[X_{i,j}UX_{i,j}, X_{i,j}VX_{i,j}] = 0$ for all $i \in [d], j \in [k]$ and $U, V \in \langle \mathbf{X} \rangle$.

Theorem (Navascués-Pironio-Acín‘12)

There exist k MUBs in dimension $d \Leftrightarrow$ there exists a (d,k)-MUB-algebra.

- **Strategy:** show non-existence of k MUBs by proving infeasibility of SDP relaxations!

MUB-algebra (proof sketch)

Definition (recap of relations)

1. $X_{i,j}X_{\ell,j} = \delta_{i,\ell}X_{i,j}$ for all $i, \ell \in [d], j \in [k]$,
2. $\sum_{i\in[d]} X_{i,j} = I$ for all $j \in [k]$,
3. $X_{i,j}X_{i',j'}X_{i,j} = \frac{1}{d}X_{i,j}$ for all $i, i' \in [d], j, j' \in [k]$ with $j \neq j'$,
4. $[X_{i,j}UX_{i,j}, X_{i,j}VX_{i,j}] = 0$ for all $i \in [d], j \in [k]$ and $U, V \in \langle \mathbf{X} \rangle$.

Theorem (Navascués-Pironio-Acín'12)

There exist k MUBs in dimension $d \Leftrightarrow$ there exists a (d, k)-MUB-algebra.

Proof sketch.

MUB-algebra (proof sketch)

Definition (recap of relations)

1. $X_{i,j}X_{\ell,j} = \delta_{i,\ell}X_{i,j}$ for all $i, \ell \in [d], j \in [k]$,
2. $\sum_{i\in[d]} X_{i,j} = I$ for all $j \in [k]$,
3. $X_{i,j}X_{i',j'}X_{i,j} = \frac{1}{d}X_{i,j}$ for all $i, i' \in [d], j, j' \in [k]$ with $j \neq j'$,
4. $[X_{i,j}UX_{i,j}, X_{i,j}VX_{i,j}] = 0$ for all $i \in [d], j \in [k]$ and $U, V \in \langle \mathbf{X} \rangle$.

Theorem (Navascués-Pironio-Acín'12)

There exist k MUBs in dimension d $\Leftrightarrow$ there exists a (d, k)-MUB-algebra.

Proof sketch. For all $i \in [d], j \in [k]$, define $Z_{i,j} \in M_d(\mathcal{A})$ as

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

MUB-algebra (proof sketch)

Definition (recap of relations)

1. $X_{i,j}X_{\ell,j} = \delta_{i,\ell}X_{i,j}$ for all $i, \ell \in [d], j \in [k]$,
2. $\sum_{i \in [d]} X_{i,j} = I$ for all $j \in [k]$,
3. $X_{i,j}X_{i',j'}X_{i,j} = \frac{1}{d}X_{i,j}$ for all $i, i' \in [d], j, j' \in [k]$ with $j \neq j'$,
4. $[X_{i,j}UX_{i,j}, X_{i,j}VX_{i,j}] = 0$ for all $i \in [d], j \in [k]$ and $U, V \in \langle \mathbf{X} \rangle$.

Theorem (Navascués-Pironio-Acín'12)

There exist k MUBs in dimension $d \Leftrightarrow$ there exists a (d, k)-MUB-algebra.

Proof sketch. For all $i \in [d], j \in [k]$, define $Z_{i,j} \in M_d(\mathcal{A})$ as

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

Show the $Z_{i,j}$ satisfy 1. & 3. using the relations for the $X_{i,j}$.

MUB-algebra (proof sketch)

Definition (recap of relations)

1. $X_{i,j}X_{\ell,j} = \delta_{i,\ell}X_{i,j}$ for all $i, \ell \in [d], j \in [k]$,
2. $\sum_{i\in[d]} X_{i,j} = I$ for all $j \in [k]$,
3. $X_{i,j}X_{i',j'}X_{i,j} = \frac{1}{d}X_{i,j}$ for all $i, i' \in [d], j, j' \in [k]$ with $j \neq j'$,
4. $[X_{i,j}UX_{i,j}, X_{i,j}VX_{i,j}] = 0$ for all $i \in [d], j \in [k]$ and $U, V \in \langle \mathbf{X} \rangle$.

Theorem (Navascués-Pironio-Acín'12)

There exist k MUBs in dimension $d \Leftrightarrow$ there exists a (d, k)-MUB-algebra.

Proof sketch. For all $i \in [d], j \in [k]$, define $Z_{i,j} \in M_d(\mathcal{A})$ as

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

Show the $Z_{i,j}$ satisfy 1. & 3. using the relations for the $X_{i,j}$. Finally, use 4. to simultaneously diagonalize the entries of the $Z_{i,j}$. □

The symmetry

A set of k MUBs $\{\{u_{i,j}\}_{i\in[d]} : j \in [k]\}$ remains a set of k MUBs under the following two actions:

The symmetry

A set of k MUBs $\{\{u_{i,j}\}_{i\in[d]} : j \in [k]\}$ remains a set of k MUBs under the following two actions:

- A permutation $\tau \in S_k$ of the labels of the bases.

The symmetry

A set of k MUBs $\{\{u_{i,j}\}_{i\in[d]} : j \in [k]\}$ remains a set of k MUBs under the following two actions:

- A permutation $\tau \in S_k$ of the labels of the bases.
- For each j, a permutation $\sigma_j \in S_d$ of the labels of basis elements in $\{u_{i,j}\}_{i\in[d]}$.

The symmetry

A set of k MUBs $\{\{u_{i,j}\}_{i\in[d]} : j \in [k]\}$ remains a set of k MUBs under the following two actions:

- A permutation $\tau \in S_k$ of the labels of the bases.
- For each j, a permutation $\sigma_j \in S_d$ of the labels of basis elements in $\{u_{i,j}\}_{i\in[d]}$.

The group associated to these permutations is the *wreath product* $S_d \wr S_k$.

The group $S_d \wr S_k$

Elements: $(\sigma, \tau) = ((\sigma_1, \ldots, \sigma_k), \tau)$ where each $\sigma_i \in S_d$ and $\tau \in S_k$.
Multiplication:

$$(\sigma, \tau) \cdot (\pi, \rho) = (\sigma(\tau * \pi), \tau\rho)$$

where $\tau * \pi = (\pi_{\tau^{-1}(1)}, \ldots, \pi_{\tau^{-1}(k)})$.

The symmetry

A set of k MUBs $\{\{u_{i,j}\}_{i\in[d]} : j \in [k]\}$ remains a set of k MUBs under the following two actions:

- A permutation $\tau \in S_k$ of the labels of the bases.
- For each j, a permutation $\sigma_j \in S_d$ of the labels of basis elements in $\{u_{i,j}\}_{i\in[d]}$.

The group associated to these permutations is the *wreath product* $S_d \wr S_k$.

The group $S_d \wr S_k$

Elements: $(\sigma, \tau) = ((\sigma_1, \ldots, \sigma_k), \tau)$ where each $\sigma_i \in S_d$ and $\tau \in S_k$.
Multiplication:

$$(\sigma, \tau) \cdot (\pi, \rho) = (\sigma(\tau * \pi), \tau\rho)$$

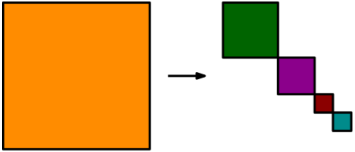
where $\tau * \pi = (\pi_{\tau^{-1}(1)}, \ldots, \pi_{\tau^{-1}(k)})$.

- The relations of a (d, k)-MUB algebra are preserved under the natural $S_d \wr S_k$-action on the NC-variables $x_{i,j}$:

$$(\sigma, \tau) \cdot x_{i,j} = x_{\sigma_{\tau(j)}(i), \tau(j)}.$$

- The resulting SDP-relaxations inherit this symmetry.

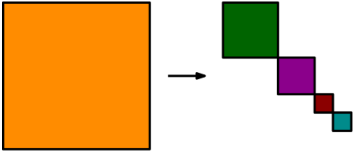
Symmetry reductions of SDPs



Based on *Artin-Wedderburn theory*:

Every (unital) complex matrix $*$-algebra $\mathcal{A}$ is $*$-isomorphic to a direct sum of *full* matrix $*$-algebras: $\mathcal{A} \cong \oplus_{i=1}^{k} \mathbb{C}^{m_i \times m_i}$.

Symmetry reductions of SDPs

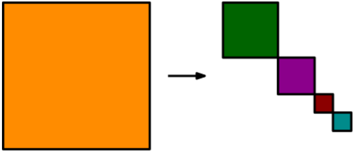


Based on *Artin-Wedderburn theory*:

Every (unital) complex matrix $*$-algebra $\mathcal{A}$ is $*$-isomorphic to a direct sum of *full* matrix $*$-algebras: $\mathcal{A} \cong \oplus_{i=1}^{k} \mathbb{C}^{m_i \times m_i}$.

- Size reduction of an SDP when applied to the matrix $*$-algebra generated by the objective and constraint matrices.

Symmetry reductions of SDPs



Based on *Artin-Wedderburn theory*:

Every (unital) complex matrix $*$-algebra $\mathcal{A}$ is $*$-isomorphic to a direct sum of *full* matrix $*$-algebras: $\mathcal{A} \cong \oplus_{i=1}^{k} \mathbb{C}^{m_i \times m_i}$.

- Size reduction of an SDP when applied to the matrix $*$-algebra generated by the objective and constraint matrices.

Example

$$\begin{pmatrix} a & b & b \\ b & c & d \\ b & d & c \end{pmatrix} \succeq 0 \quad \Longleftrightarrow \quad \begin{pmatrix} a & \sqrt{2}b & 0 \\ \sqrt{2}b & c+d & 0 \\ 0 & 0 & c-d \end{pmatrix} \succeq 0$$

Symmetry reductions of SDPs: group invariance

Group invariant SDPs: $\mathcal{A} = (\mathbb{C}^{Z\times Z})^G$, the algebra of G-invariant $Z \times Z$ matrices, where G is a group acting on the set of indices Z.

Symmetry reductions of SDPs: group invariance

Group invariant SDPs: $\mathcal{A} = (\mathbb{C}^{Z\times Z})^G$, the algebra of G-invariant $Z \times Z$ matrices, where G is a group acting on the set of indices Z.

Example (continued)

$$\begin{pmatrix} a & b & b \\ b & c & d \\ b & d & c \end{pmatrix} \succeq 0 \quad \Longleftrightarrow \quad \begin{pmatrix} a & \sqrt{2}b & 0 \\ \sqrt{2}b & c+d & 0 \\ 0 & 0 & c-d \end{pmatrix} \succeq 0$$

The group S_2 acts on the last two rows/columns.

Symmetry reductions of SDPs: group invariance

Group invariant SDPs: $\mathcal{A} = (\mathbb{C}^{Z \times Z})^G$, the algebra of G-invariant $Z \times Z$ matrices, where G is a group acting on the set of indices Z.

Example (continued)

$$\begin{pmatrix} a & b & b \\ b & c & d \\ b & d & c \end{pmatrix} \succeq 0 \quad \Longleftrightarrow \quad \begin{pmatrix} a & \sqrt{2}b & 0 \\ \sqrt{2}b & c+d & 0 \\ 0 & 0 & c-d \end{pmatrix} \succeq 0$$

The group S_2 acts on the last two rows/columns.

Used in many areas, for example

- Coding theory (e.g. [Schrijver'05]),
- Combinatorics (e.g., survey [de Klerk'10]),
- Polynomial optimization (e.g. [Gatermann-Parrilo'04], [Riener-Theobald-Andrén-Lasserre'13]).

Symmetry reductions of SDPs: group invariance

Let Z be a finite set, G a finite group acting on Z, and $(\mathbb{C}^{Z\times Z})^G$ the $*$-algebra of G-invariant $Z \times Z$ matrices, then

$$(\mathbb{C}^{Z\times Z})^G \cong \bigoplus_{i=1}^{k} \mathbb{C}^{m_i \times m_i},$$

Symmetry reductions of SDPs: group invariance

Let Z be a finite set, G a finite group acting on Z, and $(\mathbb{C}^{Z\times Z})^G$ the $*$-algebra of G-invariant $Z \times Z$ matrices, then

$$(\mathbb{C}^{Z\times Z})^G \cong \bigoplus_{i=1}^{k} \mathbb{C}^{m_i \times m_i},$$

where k and m_i are such that

$$\mathbb{C}^Z = \bigoplus_{i=1}^{k} \left(\bigoplus_{j=1}^{m_i} V_{i,j} \right)$$

for irreducible G-modules $V_{i,j}$ such that $V_{i,j} \cong V_{i',j'}$ iff $i = i'$.

Symmetry reductions of SDPs: group invariance

Let Z be a finite set, G a finite group acting on Z, and $(\mathbb{C}^{Z\times Z})^G$ the $*$-algebra of G-invariant $Z \times Z$ matrices, then

$$(\mathbb{C}^{Z\times Z})^G \cong \bigoplus_{i=1}^{k} \mathbb{C}^{m_i \times m_i},$$

where k and m_i are such that

$$\mathbb{C}^Z = \bigoplus_{i=1}^{k} \left(\bigoplus_{j=1}^{m_i} V_{i,j} \right)$$

for irreducible G-modules $V_{i,j}$ such that $V_{i,j} \cong V_{i',j'}$ iff $i = i'$.

An explicit isomorphism $(\mathbb{C}^{Z\times Z})^G \to \bigoplus_{i=1}^{k} \mathbb{C}^{m_i\times m_i}$ is given by

$$A \longmapsto \bigoplus_{i=1}^{k} \big(\langle u_{i,j}, A u_{i,j'}\rangle\big)_{j,j'=1}^{m_i}$$

for (carefully chosen) $u_{i,j} \in V_{i,j}$ for all i, j.

The MUB SDPs

The t-th SDP relaxation of (d, k)-MUB algebras involves matrices indexed by noncommutative monomials of degree exactly t. That is,

$$Z = ([d] \times [k])^t = \{x_{i_1,j_1} \cdots x_{i_t,j_t} : i_1, \ldots, i_t \in [d], j_1, \ldots, j_t \in [k]\}$$

and the $S_d \wr S_k$-action is defined through $(\sigma, \tau) \cdot x_{i,j} = x_{\sigma_{\tau(j)}(i),\tau(j)}$.

The MUB SDPs

The t-th SDP relaxation of (d, k)-MUB algebras involves matrices indexed by noncommutative monomials of degree exactly t. That is,

$$Z = ([d] \times [k])^t = \{x_{i_1,j_1} \cdots x_{i_t,j_t} : i_1, \ldots, i_t \in [d], j_1, \ldots, j_t \in [k]\}$$

and the $S_d \wr S_k$-action is defined through $(\sigma, \tau) \cdot x_{i,j} = x_{\sigma_{\tau(j)}(i), \tau(j)}$.

For integers d, k, t we define

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

The MUB SDPs

The t-th SDP relaxation of (d,k)-MUB algebras involves matrices indexed by noncommutative monomials of degree exactly t. That is,

$$Z = ([d] \times [k])^t = \{x_{i_1,j_1} \cdots x_{i_t,j_t} : i_1, \dots, i_t \in [d], j_1, \dots, j_t \in [k]\}$$

and the $S_d \wr S_k$-action is defined through $(\sigma, \tau) \cdot x_{i,j} = x_{\sigma_{\tau(j)}(i), \tau(j)}$.

For integers d, k, t we define

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

These are indeed semidefinite programs since

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

The MUB SDPs

The t-th SDP relaxation of (d,k)-MUB algebras involves matrices indexed by noncommutative monomials of degree exactly t. That is,

$$Z = ([d]\times[k])^t = \{x_{i_1,j_1}\cdots x_{i_t,j_t} : i_1,\ldots,i_t \in [d], j_1,\ldots,j_t \in [k]\}$$

and the $S_d \wr S_k$-action is defined through $(\sigma,\tau)\cdot x_{i,j} = x_{\sigma_{\tau(j)}(i),\tau(j)}$.

For integers d,k,t we define

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

These are indeed semidefinite programs since

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

Compared to previous slide: $\mathbb{C}^Z = \mathbb{C}^{\langle\mathbf{x}\rangle_{=t}} \simeq \mathbb{C}^{([d]\times[k])^t}$

Symmetry reductions of MUB SDPs

Recall, $(\sigma, \tau) \cdot x_{i,j} = x_{\sigma_{\tau(j)}(i),\tau(j)}$ and

$$Z = ([d] \times [k])^t = \{x_{i_1,j_1} \cdots x_{i_t,j_t} : i_1, \ldots, i_t \in [d], j_1, \ldots, j_t \in [k]\}.$$

Symmetry reductions of MUB SDPs

Recall, $(\sigma, \tau) \cdot x_{i,j} = x_{\sigma_{\tau(j)}(i), \tau(j)}$ and

$$Z = ([d] \times [k])^t = \{x_{i_1,j_1} \cdots x_{i_t,j_t} : i_1, \ldots, i_t \in [d], j_1, \ldots, j_t \in [k]\}.$$

A first decomposition of $\mathbb{C}^Z$ is obtained through the $S_d \wr S_k$-orbits in Z, i.e., through set partitions $P, \mathbf{Q}$ where

- $P = \{P_1, \ldots, P_r\}$ is a set partition of $[t]$,
- $\mathbf{Q} = \{Q_1, \ldots, Q_r\}$ where Q_i is a set partition of P_i.

Symmetry reductions of MUB SDPs

Recall, $(\sigma, \tau) \cdot x_{i,j} = x_{\sigma_{\tau(j)}(i), \tau(j)}$ and

$$Z = ([d] \times [k])^t = \{x_{i_1,j_1} \cdots x_{i_t,j_t} : i_1, \ldots, i_t \in [d], j_1, \ldots, j_t \in [k]\}.$$

A first decomposition of $\mathbb{C}^Z$ is obtained through the $S_d \wr S_k$-orbits in Z, i.e., through set partitions $P, \mathbf{Q}$ where

- $P = \{P_1, \ldots, P_r\}$ is a set partition of $[t]$,
- $\mathbf{Q} = \{Q_1, \ldots, Q_r\}$ where Q_i is a set partition of P_i.

Example:

$t = 4$, $P = \{\{1,3,4\},\{2\}\}$, $\mathbf{Q} = \{Q_1, Q_2\}$ with $Q_1 = \{\{1,3\},\{4\}\}$, $Q_2 = \{2\}$

$V_{P,\mathbf{Q}} :=$ span of monomials with indices:

i_1, j_1	i_3, j_2	i_1, j_1	i_2, j_1

- We have $\mathbb{C}^Z = \bigoplus_{P,\mathbf{Q}} V_{P,\mathbf{Q}}$ as $S_d \wr S_k$-modules.

How does $V_{P,\mathbf{Q}}$ decompose? restricted to S_k-action

Warming-up:

Consider the S_k-action on $x_1, \ldots, x_k$. Then S_k-orbits in $[k]^t$ correspond to set partitions $P = \{P_1, \ldots, P_r\}$ of $[t]$.

How does $V_{P,\mathbf{Q}}$ decompose? restricted to S_k-action

Warming-up:

Consider the S_k-action on $x_1, \ldots, x_k$. Then S_k-orbits in $[k]^t$ correspond to set partitions $P = \{P_1, \ldots, P_r\}$ of $[t]$.

V_P is a *permutation module* M^μ for the partition $\mu = (k - r, \overbrace{1, \ldots, 1}^{r \text{ times}})$:
A monomial in V_P with w_j assigned to P_j is identified with the *tabloid*

$$\begin{array}{l} \hline \cdots\ \cdots\ \cdots \\ \hline w_1 \\ \hline w_2 \\ \hline \vdots \\ \hline w_r \\ \hline \end{array}$$

"L-shape"

How does $V_{P,\mathbf{Q}}$ decompose? restricted to S_k-action

Warming-up:

Consider the S_k-action on $x_1, \ldots, x_k$. Then S_k-orbits in $[k]^t$ correspond to set partitions $P = \{P_1, \ldots, P_r\}$ of $[t]$.

V_P is a *permutation module* M^μ for the partition $\mu = (k - r, \overbrace{1, \ldots, 1}^{r \text{ times}})$:
A monomial in V_P with w_j assigned to P_j is identified with the *tabloid*

$$
\begin{array}{lll}
\hline
\cdots & \cdots & \cdots \\
\hline
w_1 & & \\
\cline{1-1}
w_2 & & \\
\cline{1-1}
\vdots & & \\
\cline{1-1}
w_r & & \\
\cline{1-1}
\end{array}
\qquad\qquad \text{“L-shape”}
$$

The representation theory of S_k is very well understood (cf. [Sagan'01]).
The irreducible S_k-modules are the *Specht modules* S^λ where $\lambda \vdash k$, and

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

How does $V_{P,\mathbf{Q}}$ decompose? full $S_d \wr S_k$ action

A monomial in $V_{P,\mathbf{Q}}$ corresponds to a tensor product of tabloids:

How does $V_{P,\mathbf{Q}}$ decompose? full $S_d \wr S_k$ action

A monomial in $V_{P,\mathbf{Q}}$ corresponds to a tensor product of tabloids:

- For the set partition P, as before:

$$\text{if } w(j) \in [k] \text{ assigned to } P_j \longrightarrow w = \begin{array}{l} \hline \cdots\ \cdots\ \cdots \\ \hline w(1) \\ \hline w(2) \\ \hline \vdots \\ \hline w(r) \\ \hline \end{array} \qquad \text{“L-shape”}$$

How does $V_{P,\mathbf{Q}}$ decompose? full $S_d \wr S_k$ action

A monomial in $V_{P,\mathbf{Q}}$ corresponds to a tensor product of tabloids:

- For the set partition P, as before:

$$\text{if } w(j) \in [k] \text{ assigned to } P_j \longrightarrow w = \begin{array}{l} \hline \cdots \ \cdots \ \cdots \\ \hline w(1) \\ \hline w(2) \\ \hline \vdots \\ \hline w(r) \\ \hline \end{array} \qquad \text{“L-shape”}$$

- For each set partition Q_i:

$$\text{if } e^i(j) \in [d] \text{ is assigned to the } j\text{-th set in } Q_i \longrightarrow v_i = \begin{array}{l} \hline \cdots \ \cdots \ \cdots \\ \hline e^i(1) \\ \hline e^i(2) \\ \hline \vdots \\ \hline e^i(|Q_i|) \\ \hline \end{array}$$

How does $V_{P,\mathbf{Q}}$ decompose? full $S_d \wr S_k$ action

A monomial in $V_{P,\mathbf{Q}}$ corresponds to a tensor product of tabloids:

- For the set partition P, as before:

$$\text{if } w(j) \in [k] \text{ assigned to } P_j \longrightarrow w = \begin{array}{l} \hline \cdots\ \cdots\ \cdots \\ \hline w(1) \\ \hline w(2) \\ \hline \vdots \\ \hline w(r) \\ \hline \end{array} \qquad \text{“L-shape”}$$

- For each set partition Q_i:

$$\text{if } e^i(j) \in [d] \text{ is assigned to the } j\text{-th set in } Q_i \longrightarrow v_i = \begin{array}{l} \hline \cdots\ \cdots\ \cdots \\ \hline e^i(1) \\ \hline e^i(2) \\ \hline \vdots \\ \hline e^i(|Q_i|) \\ \hline \end{array}$$

What is the $S_d \wr S_k$ action?

$$(\sigma, \tau) \cdot \Big(\bigotimes_{i \in [r]} v_i\Big) \otimes w = \Big(\bigotimes_{i \in [r]} \sigma_{\tau w(i)} v_i\Big) \otimes \tau w$$

How does $V_{P,\mathbf{Q}}$ decompose? full $S_d \wr S_k$ action

- We (carefully) decompose each permutation module for the symmetric group (S_d or S_k) into Specht modules.

How does $V_{P,\mathbf{Q}}$ decompose? full $S_d \wr S_k$ action

- We (carefully) decompose each permutation module for the symmetric group (S_d or S_k) into Specht modules.
- Is this is a decomposition into *irreducible* modules?

How does $V_{P,\mathbf{Q}}$ decompose? full $S_d \wr S_k$ action

- We (carefully) decompose each permutation module for the symmetric group (S_d or S_k) into Specht modules.
- Is this is a decomposition into *irreducible* modules?
- The irreducible modules of $S_d \wr S_k$ are known ("Specht modules"), but they involve a seemingly different action:

$$(\sigma_1, \ldots, \sigma_k; \tau) \cdot \bigotimes_{i \in [k]} x_i = \bigotimes_{i \in [k]} \sigma_i \cdot x_{\tau^{-1}(i)}.$$

How does $V_{P,\mathbf{Q}}$ decompose? full $S_d \wr S_k$ action

- We (carefully) decompose each permutation module for the symmetric group (S_d or S_k) into Specht modules.
- Is this is a decomposition into *irreducible* modules?
- The irreducible modules of $S_d \wr S_k$ are known ("Specht modules"), but they involve a seemingly different action:

$$(\sigma_1, \ldots, \sigma_k; \tau) \cdot \bigotimes_{i \in [k]} x_i = \bigotimes_{i \in [k]} \sigma_i \cdot x_{\tau^{-1}(i)}.$$

Key step: We show that the modules in our decomposition are isomorphic to such "Specht modules".

How does $V_{P,\mathbf{Q}}$ decompose? full $S_d \wr S_k$ action

- We (carefully) decompose each permutation module for the symmetric group (S_d or S_k) into Specht modules.
- Is this is a decomposition into *irreducible* modules?
- The irreducible modules of $S_d \wr S_k$ are known ("Specht modules"), but they involve a seemingly different action:

$$(\sigma_1, \ldots, \sigma_k; \tau) \cdot \bigotimes_{i \in [k]} x_i = \bigotimes_{i \in [k]} \sigma_i \cdot x_{\tau^{-1}(i)}.$$

Key step: We show that the modules in our decomposition are isomorphic to such "Specht modules".

Link to literature: We show that $V_{P,\mathbf{Q}}$ is isomorphic to a "permutation module" $M^{\underline{\gamma}}$.

How does $V_{P,\mathbf{Q}}$ decompose? full $S_d \wr S_k$ action

- We (carefully) decompose each permutation module for the symmetric group (S_d or S_k) into Specht modules.
- Is this is a decomposition into *irreducible* modules?
- The irreducible modules of $S_d \wr S_k$ are known ("Specht modules"), but they involve a seemingly different action:

$$(\sigma_1, \ldots, \sigma_k; \tau) \cdot \bigotimes_{i \in [k]} x_i = \bigotimes_{i \in [k]} \sigma_i \cdot x_{\tau^{-1}(i)}.$$

Key step: We show that the modules in our decomposition are isomorphic to such "Specht modules".

Link to literature: We show that $V_{P,\mathbf{Q}}$ is isomorphic to a "permutation module" $M^{\underline{\gamma}}$.

- Multiplicities of $S^{\underline{\lambda}}$ in $M^{\underline{\gamma}}$ can be found in the literature,

How does $V_{P,\mathbf{Q}}$ decompose? full $S_d \wr S_k$ action

- We (carefully) decompose each permutation module for the symmetric group (S_d or S_k) into Specht modules.
- Is this is a decomposition into *irreducible* modules?
- The irreducible modules of $S_d \wr S_k$ are known ("Specht modules"), but they involve a seemingly different action:

$$(\sigma_1, \dots, \sigma_k; \tau) \cdot \bigotimes_{i \in [k]} x_i = \bigotimes_{i \in [k]} \sigma_i \cdot x_{\tau^{-1}(i)}.$$

Key step: We show that the modules in our decomposition are isomorphic to such "Specht modules".

Link to literature: We show that $V_{P,\mathbf{Q}}$ is isomorphic to a "permutation module" $M^{\underline{\gamma}}$.

- Multiplicities of $S^{\underline{\lambda}}$ in $M^{\underline{\gamma}}$ can be found in the literature,
- Explicit homomorphisms not (so easily)

Symmetry reduced SDPs

For t-th order relaxation with the full $S_d \wr S_k$ symmetry we obtain:

- Sum of squares of block-sizes equals the number of pairs $(P, \mathbf{Q})$ where P and $\mathbf{Q}$ are set partitions of $[2t]$.

Symmetry reduced SDPs

For t-th order relaxation with the full $S_d \wr S_k$ symmetry we obtain:

- Sum of squares of block-sizes equals the number of pairs $(P, \mathbf{Q})$ where P and $\mathbf{Q}$ are set partitions of $[2t]$.
- When $d, k \geq 2t$, this is independent of d, k and equals the $2t$-th number in the OEIS sequence `A000258`:
  1, 1, 3, 12, 60, 358, 2471, 19302, 167894, 1606137.

Symmetry reduced SDPs

For t-th order relaxation with the full $S_d \wr S_k$ symmetry we obtain:

- Sum of squares of block-sizes equals the number of pairs $(P, \mathbf{Q})$ where P and $\mathbf{Q}$ are set partitions of $[2t]$.
- When $d, k \geq 2t$, this is independent of d, k and equals the $2t$-th number in the OEIS sequence `A000258`:
  1, 1, 3, 12, 60, 358, 2471, 19302, 167894, 1606137.

d	k	t	$(dk)^{\lfloor t \rfloor}$	#vars	#linear constr.	block sizes sum	block sizes max	result
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

Concluding remarks

- So far, all computations are done on a standard desktop.

Concluding remarks

- So far, all computations are done on a standard desktop.
- If successful (i.e., infeasible), then still considerable amount of work to get an analytic certificate!

Concluding remarks

- So far, all computations are done on a standard desktop.
- If successful (i.e., infeasible), then still considerable amount of work to get an analytic certificate!

Open questions:

- Can the symmetry reduction be computed in time $\mathrm{poly}(d, k)$ for a fixed t?

Concluding remarks

- So far, all computations are done on a standard desktop.
- If successful (i.e., infeasible), then still considerable amount of work to get an analytic certificate!

Open questions:

- Can the symmetry reduction be computed in time $\mathrm{poly}(d, k)$ for a fixed t?
- Is there a SIC-POVM analogue of NPA's result?

Concluding remarks

- So far, all computations are done on a standard desktop.
- If successful (i.e., infeasible), then still considerable amount of work to get an analytic certificate!

Open questions:

- Can the symmetry reduction be computed in time $\mathrm{poly}(d, k)$ for a fixed t?
- Is there a SIC-POVM analogue of NPA's result?
  - **SIC-POVM**: d^2 rank-1 projectors P_i with $\mathrm{Tr}(P_i P_j) = \frac{1}{d+1}$ for $i \neq j$
  - ([Wootters'04] for a discussion of MUBs, SIC-POVMs and finite geometries)

Concluding remarks

- So far, all computations are done on a standard desktop.
- If successful (i.e., infeasible), then still considerable amount of work to get an analytic certificate!

Open questions:

- Can the symmetry reduction be computed in time $\mathrm{poly}(d, k)$ for a fixed t?
- Is there a SIC-POVM analogue of NPA's result?
  - **SIC-POVM**: d^2 rank-1 projectors P_i with $\mathrm{Tr}(P_i P_j) = \frac{1}{d+1}$ for $i \neq j$
  - ([Wootters'04] for a discussion of MUBs, SIC-POVMs and finite geometries)

Noncommutativity makes things easier!

Concluding remarks

- So far, all computations are done on a standard desktop.
- If successful (i.e., infeasible), then still considerable amount of work to get an analytic certificate!

Open questions:

- Can the symmetry reduction be computed in time $\mathrm{poly}(d, k)$ for a fixed t?
- Is there a SIC-POVM analogue of NPA's result?
  - **SIC-POVM**: d^2 rank-1 projectors P_i with $\mathrm{Tr}(P_i P_j) = \frac{1}{d+1}$ for $i \neq j$
  - ([Wootters'04] for a discussion of MUBs, SIC-POVMs and finite geometries)

Noncommutativity makes things easier!

How does $V_{P,\mathbf{Q}}$ decompose?

Modules for $S_d \wr S_k$:

(1) Let X be an S_d-module. We define an $S_d \wr S_k$-module $X^{\tilde{\boxtimes} k}$ as follows:
Vector space: $X^{\otimes k}$
Action: $(\sigma_1, \ldots, \sigma_k; \pi)$ acts on an element $\mathbf{x} = \otimes_{i\in[k]} x_i$ as

$$(\sigma_1, \ldots, \sigma_k; \pi) \cdot \bigotimes_{i\in[k]} x_i = \bigotimes_{i\in[k]} \sigma_i \cdot x_{\pi^{-1}(i)}.$$

(2) Given an S_k-module Y, we define an $S_d \wr S_k$-module $X^{\tilde{\boxtimes} k} \oslash Y$:
Vector space: $X^{\otimes k} \otimes Y$
Action: $(\sigma_1, \ldots, \sigma_k; \pi)$ acts on an element $\mathbf{x} \otimes y$ as

$$(\sigma_1, \ldots, \sigma_k; \pi) \cdot (\mathbf{x} \otimes y) = \big((\sigma_1, \ldots, \sigma_k; \pi) \cdot \mathbf{x}\big) \otimes \big(\pi \cdot y\big)$$

How does $V_{P,\mathbf{Q}}$ decompose?

Let $\nu_1, \ldots, \nu_\ell$ be a complete list of partitions of d, and let $\underline{\lambda} = (\lambda^1, \ldots, \lambda^\ell)$ be an *ℓ-multipartition* of k.

Permutation module $M^{\underline{\lambda}}$ is defined as

$$M^{\underline{\lambda}} := \left[\bigotimes_{a \in [\ell]} \left((M^{\nu_a})^{\tilde{\boxtimes}|\lambda^a|} \oslash M^{\lambda^a} \right) \right] \Big\uparrow_{d \wr |\underline{\lambda}|}^{d \wr k},$$

Specht module $S^{\underline{\lambda}}$ is defined as

$$S^{\underline{\lambda}} := \left[\bigotimes_{a \in [\ell]} \left((S^{\nu_a})^{\tilde{\boxtimes}|\lambda^a|} \oslash S^{\lambda^a} \right) \right] \Big\uparrow_{d \wr |\underline{\lambda}|}^{d \wr k}.$$

The Specht modules form the irreducible modules of $S_d \wr S_k$.

[MacDonald'80,Chuang-Tan'04,Green'19]

- Multiplicities of $S^{\underline{\lambda}}$ in $M^{\underline{\gamma}}$ can be found in the literature,
- Explicit homomorphisms not (so easily)

Main result: we show that $V_{P,\mathbf{Q}} \cong M^{\underline{\gamma}}$ where $\underline{\gamma}$ has an "L-shape", and we give an explicit decomposition of such permutation modules.