Mutually unbiased bases: polynomial optimization and symmetry

Sander Gribling, IRIF

Based on joint work with Sven Polak (CWI)

arXiv:2111.05698
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**

\[
\begin{align*}
\left\{ \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right\}, & \quad \left\{ \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix} \right\}, \\
\left\{ \frac{1}{\sqrt{2}} \begin{pmatrix} i \\ 1 \end{pmatrix}, \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ i \end{pmatrix} \right\}.
\end{align*}
\]
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

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

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.

  \[
  (\text{Since } |u_1^* v_j|^2 = 1/d \text{ then describes the probability of outcome } v_j)
  \]

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 ˙Zyczkowski (2010).

Listed as one of ‘Five Open Problems in Quantum Information Theory’ [Horodecki-Rudnicki-˙Zyczkowski‘22]: **prize EUR 2022!**
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 $M(e) := ee^* - I_d / d$. Then, $	ext{Tr}(M(u)M(v)) = |u^*v|^2 - 1/d$. MUBs $\Rightarrow$ orthogonal subspaces. $\Rightarrow$ at most $(d^2 - 1) / (d - 1) = d + 1$ MUBs in dimension $d$. 

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

Then,

$$\text{Tr}(M(u)M(v)) = |u^*v|^2 - 1/d.$$
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 \(\rightarrow\) dim-(\(d\)-1) subspace of traceless Hermitian \(d \times d\) matrices.

Then,

\[
\text{Tr}(M(u)M(v)) = |u^*v|^2 - 1/d.
\]

MUBs \(\rightarrow\) **orthogonal** subspaces.

\(\Rightarrow\) at most \((d^2 - 1)/(d - 1) = d + 1\) MUBs in dimension \(d\).
Known results (constructions)

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

\[\text{No set of } d + 1 \text{ MUBs is known when } d \neq p^n.\]

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 $26^2 = 2^213^2$ 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)

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

*Figure: Finite affine plane of order 3, source: Wiki*
Known results (finite geometry)

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

<table>
<thead>
<tr>
<th>MUBs</th>
<th>Finite affine plane</th>
</tr>
</thead>
<tbody>
<tr>
<td>( d + 1 ) orthonormal bases unit vectors</td>
<td>( d + 1 ) equivalence classes of ( d ) parallel lines lines contain ( d ) points</td>
</tr>
</tbody>
</table>
Known results (finite geometry)

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

<table>
<thead>
<tr>
<th>MUBs</th>
<th>Finite affine plane</th>
</tr>
</thead>
<tbody>
<tr>
<td>$d + 1$ orthonormal bases unit vectors</td>
<td>$d + 1$ equivalence classes of $d$ parallel lines</td>
</tr>
<tr>
<td>$\langle e, f \rangle = 1/d$</td>
<td>lines contain $d$ points</td>
</tr>
<tr>
<td></td>
<td>$</td>
</tr>
</tbody>
</table>
Known results (finite geometry)

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

**MUBs**

<table>
<thead>
<tr>
<th>$d + 1$ orthonormal bases</th>
<th>$d + 1$ equivalence classes of $d$ parallel lines</th>
</tr>
</thead>
<tbody>
<tr>
<td>unit vectors</td>
<td>lines contain $d$ points</td>
</tr>
<tr>
<td>$</td>
<td>\langle e, f \rangle</td>
</tr>
<tr>
<td>Exist if $d = p^n$</td>
<td>Exist if $d = p^n$</td>
</tr>
</tbody>
</table>

**Finite affine plane**
Known results (finite geometry)

Theorem (Bruck-Ryser‘49)

If \( d \equiv 1, 2 \pmod{4} \) 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 $d \equiv 1, 2 \mod 4$ 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 $d \equiv 2 \mod 4$ and $d$ is not a sum of two squares, then there does not exist a complete set of MUBs with $uu^* \in \mathbb{Q}^{d \times d} + i\mathbb{Q}^{d \times d}$ for all basis elements $u$. 

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

**Theorem (Bruck-Ryser‘49)**
If \( d \equiv 1, 2 \mod 4 \) 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 \( d \equiv 2 \mod 4 \) and \( d \) is not a sum of two squares, then there does not exist a complete set of MUBs with \( uu^* \in \mathbb{Q}^{d \times d} + i \mathbb{Q}^{d \times d} \) 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 $d \iff$ 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 $d \iff$ 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 $d \iff$ 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]:
   \[
   \min f_1(x)^2 \quad \text{s.t.} \quad f_i(x) = 0 \text{ for } i = 2, \ldots, N.
   \]
   → 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 $d \iff$ there exists a $(d, k)$-MUB-algebra.

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

[Aguilar-Borka la-Mironowicz-Paw lowski‘18] formulate a game based on quantum random access codes: the $(k, 2)$-d→1$pQRAC$ game.
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 $d \iff$ 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 $d$ $\iff$ 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

   $\iff k$ MUBs exist in dim $d$. 

---

8
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 $d$ $\iff$ 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
   $\iff k$ MUBs exist in dim $d$.
   [Aguilar-Borkała-Mironowicz-Pawłowski‘18] formulate a game based on quantum random access codes: the $(k, 2)^d \rightarrow 1$ pQRAC game
Our contributions

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

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 $d = 2, 3, 4, 5, 6, 7, 8$. 

...
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.

- 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 $d = 2, 3, 4, 5, 6, 7, 8$. 

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 $ee^*$. 

A set of $k$ MUBs $\{\{u_i, j\} \mid i \in [d], j \in [k]\}$ corresponds to a set of rank-1 $d$-by-$d$ projectors $X_{i, j} = u_{i, j} u_{i, j}^*$ satisfying the following relations:

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. $[X_{i, j}, UX_{i, j}, VX_{i, j}] = 0$ for all $i \in [d], j \in [k]$ and $U, V \in \langle X \rangle$.

Theorem (Navascu´es-Pironio-Ac ´ın'12)

There exist $k$ MUBs in dimension $d$ ⇔ 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:
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 \( d \times d \) 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:

\[
\begin{align*}
\text{Definition} & \\
\text{A C}\ast\text{-algebra } \mathcal{A} \text{ is a } (d, k)-\text{MUB-algebra if it contains Herm. elements } X_{i,j} \text{ for } i \in [d], j \in [k] \text{ that satisfy the following relations:} \\
& \begin{align*}
1. & \quad X_{i,j}X_{i',j} = \delta_{i,i'}X_{i,j} \quad \text{for all } i, i' \in [d], j \in [k], \\
2. & \quad \sum_{i \in [d]} X_{i,j} = I \quad \text{for all } j \in [k], \\
3. & \quad X_{i,j}X_{i',j'}X_{i,j} = \frac{1}{d}X_{i,j} \quad \text{for all } i, i' \in [d], j, j' \in [k] \text{ with } j \neq j',
\end{align*}
\end{align*}
\]
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 $U, V \in \langle X \rangle$.

Theorem (Navascués-Pironio-Acin'12)

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

Strategy: show non-existence of $k$ MUBs by proving infeasibility of SDP relaxations!
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 $A$ 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 $U, V \in \langle X \rangle$.

**Theorem (Navascués-Pironio-Acín’12)**

There exist $k$ MUBs in dimension $d$ $\iff$ 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 $U, V \in \langle X \rangle$.

Theorem (Navascués-Pironio-Acín‘12)
There exist $k$ MUBs in dimension $d \iff$ 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 \( U, V \in \langle X \rangle \).

**Theorem (Navascués-Pironio-Acín‘12)**

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

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

\[
Z_{i,j} := d \left[ X_{1,2}X_{a,1}X_{i,j}X_{b,1}X_{1,2} \right]_{a,b \in [d]}. 
\]
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. \( [X_{i,j} U X_{i,j}, X_{i,j} V X_{i,j}] = 0 \) for all \( i \in [d], j \in [k] \) and \( U, V \in \langle X \rangle \).

**Theorem (Navascués-Pironio-Acín‘12)**

There exist \( k \) MUBs in dimension \( d \) \( \iff \) 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

\[
Z_{i,j} := d \begin{bmatrix} X_{1,2} X_{a,1} X_{i,j} X_{b,1} X_{1,2} \end{bmatrix}_{a,b \in [d]}
\]

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 $U, V \in \langle X \rangle.$

Theorem (Navascués-Pironio-Acín‘12)

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

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

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

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:

1. A permutation $\tau \in S_k$ of the labels of the bases.
2. 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 $S_d \wr S_k$.

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 $x_{i,j}$:

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

The resulting SDP-relaxations inherit this symmetry.
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:**

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

where $\tau \ast \pi = (\pi_{\tau^{-1}(1)}, \ldots, \pi_{\tau^{-1}(k)})$. 
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 \( x_{i,j} \):

\[
(\sigma, \tau) \cdot x_{i,j} = x_{\sigma^{-1}(\tau(j))(i), \tau(j)}.
\]

- The resulting SDP-relaxations inherit this symmetry.
Symmetry reductions of SDPs

Based on Artin-Wedderburn theory:

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

Based on *Artin-Wedderburn theory*:

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

- Size reduction of an SDP when applied to the matrix $\star$-algebra generated by the objective and constraint matrices.
Symmetry reductions of SDPs

Based on Artin-Wedderburn theory:

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

▶ Size reduction of an SDP when applied to the matrix \( \ast \)-algebra generated by the objective and constraint matrices.

Example

\[
\begin{pmatrix}
a & b & b \\
b & c & d \\
b & d & c
\end{pmatrix} \succeq 0 \iff \begin{pmatrix}
a & \sqrt{2}b & 0 \\
\sqrt{2}b & c + d & 0 \\
0 & 0 & c - d
\end{pmatrix} \succeq 0
\]
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 $Z$. 

Example (continued)

\[
\begin{pmatrix} a & b & b \\
 b & c & d \\
 b & d & c \end{pmatrix} \preceq 0 \iff \begin{pmatrix} a & \sqrt{2} & b \\
 0 & c + d \\
 \sqrt{2} & 0 & 0 \end{pmatrix} \preceq 0
\]

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

**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)

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

The group $S_2$ acts on the last two rows/columns.
Symmetry reductions of SDPs: group invariance

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

**Example (continued)**

\[
\begin{pmatrix}
a & b & b \\
b & c & d \\
b & d & c
\end{pmatrix} \succeq 0 \iff \begin{pmatrix}
a & \sqrt{2}b & 0 \\
\sqrt{2}b & c + d & 0 \\
0 & 0 & c - d
\end{pmatrix} \succeq 0
\]

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

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

where \( k \) and \( m_i \) are such that

\[
\mathbb{C}^{Z \times Z} = \bigoplus_{i=1}^{k} \bigoplus_{j=1}^{m_i} V_i, j.
\]

for irreducible \( G \)-modules \( V_i, j \) such that

\[
V_i, j \cong V_i', j' \text{ iff } i = i'.
\]
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 $\ast$-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 \( (\mathbb{C}^{Z \times Z})^G \rightarrow \bigoplus_{i=1}^k \mathbb{C}^{m_i \times m_i} \) is given by

\[
A \mapsto \bigoplus_{i=1}^k \left( \langle u_{i,j}, Au_{i,j'} \rangle \right)_{j,j'=1}^{m_i}
\]

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

$$\text{sdp}(d, k, t) = \exists L \in \mathbb{R}(x)^*_{2t} \text{ s.t. } L \text{ is tracial,}$$

$$L = 0 \text{ on } \mathcal{I}_{\text{MUB},2t},$$

$$L(p^*p) \geq 0 \text{ for all } p \in \mathbb{R}(x)^{t},$$

$$L(x_{i,j}) = 1 \text{ for all } i \in [d], j \in [k].$$
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

$$\text{sdp}(d, k, t) = \exists L \in \mathbb{R}\langle x\rangle_{2t}^* \text{ s.t. } L \text{ is tracial, }$$

$$L = 0 \text{ on } \mathcal{I}_{\text{MUB},2t},$$

$$L(p^* p) \geq 0 \text{ for all } p \in \mathbb{R}\langle x\rangle_t,$$

$$L(x_{i,j}) = 1 \text{ for all } i \in [d], j \in [k].$$

These are indeed semidefinite programs since

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

$$\text{sdp}(d, k, t) = \exists L \in \mathbb{R}\langle x \rangle_{2t}^* \text{ s.t. } L \text{ is tracial,}$$

$$L = 0 \text{ on } \mathcal{I}_{\text{MUB}, 2t},$$

$$L(p^* p) \geq 0 \text{ for all } p \in \mathbb{R}\langle x \rangle_t,$$

$$L(x_{i,j}) = 1 \text{ for all } i \in [d], j \in [k].$$

These are indeed semidefinite programs since

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

Compared to previous slide: $\mathbb{C}^Z = \mathbb{C}\langle x \rangle = \mathbb{C}([d] \times [k])^t$
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 $P, Q$ where

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

Recall, \((\sigma, \tau) \cdot x_{i,j} = x_{\sigma\tau(i),\tau(j)}\) 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 \(P, Q\) where

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

**Example:**

\(t = 4\), \(P = \{\{1, 3, 4\}, \{2\}\}\), \(Q = \{Q_1, Q_2\}\) with \(Q_1 = \{\{1, 3\}, \{4\}\}\), \(Q_2 = \{2\}\)

\[V_{P,Q} := \text{span of monomials with indices: } i_1, j_1 \quad i_3, j_2 \quad i_1, j_1 \quad i_2, j_1\]

- We have \(\mathbb{C}^Z = \bigoplus_{P,Q} V_{P,Q}\) as \(S_d \wr S_k\)-modules.
How does $V_{P,Q}$ 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 $[t]$. 

$V_{P,Q}$ is a permutation module $M_\mu$ for the partition $\mu = (k-r, r \times \underbrace{1, \ldots, 1})$:

A monomial in $V_P$ with $w_j$ assigned to $P_j$ is identified with the tabloid $w_1 \ldots w_r$ "L-shape"

The representation theory of $S_k$ is very well understood (cf. [Sagan'01]).

The irreducible $S_k$-modules are the Specht modules $S_\lambda$ 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 $V_{P,Q}$ 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 $M^\mu$ for the partition $\mu = (k - r, 1, \ldots, 1)$: A monomial in $V_P$ with $w_j$ assigned to $P_j$ is identified with the tabloid

```
  w_1
 /    \   \    \   \    \\
/      \   \    \   \    \\
\w_2
 \    .   .    .   .    \\
\w_r
```

“L-shape”
How does $V_{P,Q}$ 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 $M^\mu$ for the partition $\mu = (k-r,1,\ldots,1)$:
A monomial in $V_P$ with $w_j$ assigned to $P_j$ is identified with the tabloid

\[
\begin{array}{cccc}
  \cdots & \cdots & \cdots & \cdots \\
  w_1 \\
  w_2 \\
  \vdots \\
  w_r \\
\end{array}
\]

“L-shape”

The representation theory of $S_k$ is very well understood (cf. [Sagan‘01]).
The irreducible $S_k$-modules are the Specht modules $S^\lambda$ 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 $V_{P,Q}$ decompose? full $S_d \wr S_k$ action

A monomial in $V_{P,Q}$ corresponds to a tensor product of tabloids:
How does $V_{P,Q}$ decompose? full $S_d \wr S_k$ action

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

- For the set partition $P$, as before:

  \[
  \begin{array}{c}
  \vdots \\
  w(1) \\
  \vdots \\
  w(r)
  \end{array}
  \]

  if $w(j) \in [k]$ assigned to $P_j \rightarrow w = \begin{array}{c}
  w(2) \\
  \vdots \\
  w(r)
  \end{array}$

  “L-shape”
How does $V_{P,Q}$ decompose? full $S_d \wr S_k$ action

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

- For the set partition $P$, as before:

  \[
  \begin{array}{c}
  \vdots \\
  \vdots \\
  w(1) \\
  \vdots \\
  \vdots \\
  \vdots \\
  \vdots \\
  \vdots \\
  w(r)
  \end{array}
  \]

  if $w(j) \in [k]$ assigned to $P_j \rightarrow w = w(2) \cdots$  \[\text{“L-shape”}\]

- For each set partition $Q_i$:

  \[
  \begin{array}{c}
  \vdots \\
  \vdots \\
  e^i(1) \\
  \vdots \\
  \vdots \\
  \vdots \\
  \vdots \\
  \vdots \\
  e^i(|Q_i|)
  \end{array}
  \]

  if $e^i(j) \in [d]$ is assigned to the $j$-th set in $Q_i \rightarrow v_i = e^i(2) \cdots$
How does $V_{P,Q}$ decompose? full $S_d \wr S_k$ action

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

- For the set partition $P$, as before:

  $$w = \begin{array}{c}
  w(1) \\
  \vdots \\
  w(r)
  \end{array}$$

  if $w(j) \in [k]$ assigned to $P_j \rightarrow w = \begin{array}{c}
  w(2) \\
  \vdots \\
  w(r)
  \end{array}$

  “L-shape”

- For each set partition $Q_i$:

  $$v_i = \begin{array}{c}
  e^i(1) \\
  \vdots \\
  e^i(|Q_i|)
  \end{array}$$

  if $e^i(j) \in [d]$ is assigned to the $j$-th set in $Q_i \rightarrow v_i = \begin{array}{c}
  e^i(2) \\
  \vdots \\
  e^i(|Q_i|)
  \end{array}$

What is the $S_d \wr S_k$ action?

$$\left(\sigma, \tau\right) \cdot \left( \bigotimes_{i \in [r]} v_i \right) \otimes w = \left( \bigotimes_{i \in [r]} \sigma_{\tau w(i)} v_i \right) \otimes \tau w$$
How does $V_{P,Q}$ 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 $V_{P,Q}$ 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?

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

Link to literature: We show that $V_{P,Q}$ is isomorphic to a “permutation module” $M_\gamma$.
▶ Multiplicities of $S_\lambda$ in $M_\gamma$ can be found in the literature,
▶ Explicit homomorphisms not (so easily)
How does $V_{P,Q}$ 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 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 $V_{P,Q}$ 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 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:

$$
(s_1, \ldots, s_k; \tau) \cdot \bigotimes_{i \in [k]} x_i = \bigotimes_{i \in [k]} s_i \cdot x_{\tau^{-1}(i)}.
$$

**Key step:** We show that the modules in our decomposition are isomorphic to such “Specht modules”.
How does $V_{P,Q}$ 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 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 $V_{P,Q}$ is isomorphic to a "permutation module" $M^\gamma$. 

How does $V_{P,Q}$ 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 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 $V_{P,Q}$ is isomorphic to a "permutation module" $M^\gamma$.

- Multiplicities of $S^\lambda$ in $M^\gamma$ can be found in the literature,
How does \( V_{P,Q} \) decompose? full \( S_d \wr S_k \) action

- We (carefully) decompose each permutation module for the symmetric group \((S_d \text{ or } S_k)\) into Specht modules.
- Is this 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 \( V_{P,Q} \) is isomorphic to a "permutation module" \( M^\gamma \).

- Multiplicities of \( S^\lambda \) in \( M^\gamma \) 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 $(P, Q)$ where $P$ and $Q$ 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 $(P, Q)$ where $P$ and $Q$ 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 $(P, Q)$ where $P$ and $Q$ 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.

<table>
<thead>
<tr>
<th>$d$</th>
<th>$k$</th>
<th>$t$</th>
<th>$(dk)^{[t]}$</th>
<th>#vars</th>
<th>#linear constr.</th>
<th>block sizes sum</th>
<th>max</th>
<th>result</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>4</td>
<td>4.5</td>
<td>4096</td>
<td>7</td>
<td>8</td>
<td>472</td>
<td>85</td>
<td>infeasible</td>
</tr>
<tr>
<td>3</td>
<td>5</td>
<td>4.5</td>
<td>50625</td>
<td>7</td>
<td>2</td>
<td>1259</td>
<td>142</td>
<td>infeasible</td>
</tr>
<tr>
<td>4</td>
<td>6</td>
<td>5</td>
<td>7962624</td>
<td>38</td>
<td>2</td>
<td>6374</td>
<td>389</td>
<td>infeasible</td>
</tr>
<tr>
<td>5</td>
<td>7</td>
<td>5</td>
<td>52521875</td>
<td>38</td>
<td>2</td>
<td>6732</td>
<td>389</td>
<td>infeasible</td>
</tr>
<tr>
<td>6</td>
<td>8</td>
<td>5</td>
<td>254803968</td>
<td>38</td>
<td>2</td>
<td>6820</td>
<td>389</td>
<td>infeasible</td>
</tr>
<tr>
<td>7</td>
<td>9</td>
<td>5</td>
<td>992436543</td>
<td>38</td>
<td>2</td>
<td>6830</td>
<td>389</td>
<td>infeasible</td>
</tr>
<tr>
<td>8</td>
<td>10</td>
<td>5</td>
<td>3276800000</td>
<td>38</td>
<td>2</td>
<td>6831</td>
<td>389</td>
<td>infeasible</td>
</tr>
<tr>
<td>6</td>
<td>4</td>
<td>5.5</td>
<td>7962624</td>
<td>43</td>
<td>3</td>
<td>8049</td>
<td>577</td>
<td>feasible</td>
</tr>
<tr>
<td>6</td>
<td>7</td>
<td>5.5</td>
<td>130691232</td>
<td>62</td>
<td>3</td>
<td>18538</td>
<td>1107</td>
<td>feasible</td>
</tr>
</tbody>
</table>
Concluding remarks

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

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

SIC-POVM: $d^2$ rank-1 projectors $P_i$ with $\text{Tr}(P_iP_j) = \frac{1}{d+1}$ 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!
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 $\text{poly}(d, k)$ 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 $\text{poly}(d, k)$ for a fixed $t$?
▶ Is there a SIC-POVM analogue of NPA’s result?

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

*Noncommutativity makes things easier!*
How does $V_{P,Q}$ 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 $X^{\tilde{\otimes}k}$ as follows:

**Vector space:** $X^{\otimes k}$

**Action:** $(\sigma_1, \ldots, \sigma_k; \pi)$ acts on an element $x = \bigotimes_{i \in [k]} x_i$ 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 $X^{\tilde{\otimes}k} \otimes Y$:

**Vector space:** $X^{\otimes k} \otimes Y$

**Action:** $(\sigma_1, \ldots, \sigma_k; \pi)$ acts on an element $x \otimes y$ as

$$
(\sigma_1, \ldots, \sigma_k; \pi) \cdot (x \otimes y) = ((\sigma_1, \ldots, \sigma_k; \pi) \cdot x) \otimes (\pi \cdot y)
$$
How does $V_{P,Q}$ decompose?

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

**Permutation module** $M^\lambda$ is defined as

$$M^\lambda := \left[ \bigotimes_{a \in [\ell]} \left( (M^{\nu_a})^{\lambda^a} \otimes M^{\lambda^a} \right) \right]^{d|\lambda|}_{d|\lambda|},$$

**Specht module** $S^\lambda$ is defined as

$$S^\lambda := \left[ \bigotimes_{a \in [\ell]} \left( (S^{\nu_a})^{\lambda^a} \otimes S^{\lambda^a} \right) \right]^{d|\lambda|}_{d|\lambda|}.$$

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

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

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

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