Mutually unbiased bases: polynomial optimization and symmetry

Sven Polak

Joint work with Sander Gribling (IRIF Paris)

arXiv:2111.05698
Mutually unbiased bases

Definition

Two orthonormal bases $B, B'$ of $\mathbb{C}^d$ are \textit{mutually unbiased} if

$$|e^*f|^2 = \frac{1}{d} \quad \forall e \in B, f \in B'.$$
Mutually unbiased bases

Definition

Two orthonormal bases $B, B'$ of $\mathbb{C}^d$ are mutually unbiased if

$$|e^* f|^2 = \frac{1}{d} \quad \forall e \in B, f \in B'.$$

Question

Do there exist $k$ mutually unbiased bases in dimension $d$?
Mutually unbiased bases

Definition

Two orthonormal bases $B, B'$ of $\mathbb{C}^d$ are mutually unbiased if

$$|e^*f|^2 = \frac{1}{d} \quad \forall e \in B, f \in B'.$$

Question

Do there exist $k$ mutually unbiased bases in dimension $d$?

Example

There exist 3 mutually unbiased bases (MUBs) in dimension 2:

$$\left\{ \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right\}, \quad \left\{ \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix} \right\}, \quad \left\{ \frac{1}{\sqrt{2}} \begin{pmatrix} i \\ 1 \end{pmatrix}, \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ i \end{pmatrix} \right\}.$$
Mutually unbiased bases yield complementary measurements.

- If outcome in \( \{u_i\}_{i \in [d]} \) is deterministic (say \( u_1 \)), then the outcome in \( \{v_j\}_{j \in [d]} \) is uniformly random.

Applications in cryptography, quantum information theory.

See the survey ‘On mutually unbiased bases’.

(Durt, Englert, Bengtsson, Žyczkowski ’10).
Known results

- Known: $k \leq d + 1$, attained if $d$ is a prime power.
  (Ivanovic '81, Wooters-Fields '89)

What about $d = 6$? Not known if there exist $\geq 3$ MUBs in $\mathbb{C}^6$.

Lower bound: if $\exists k$ MUBs in $\mathbb{C}^d_1$ and $\mathbb{C}^d_2$, then $\exists k$ MUBs in $\mathbb{C}^{d_1 \cdot d_2}$.

Not best possible: for $d = 26$, a construction of $6 > 2^{2^{13}}$ MUBs is known. (Wocjan-Beth '05)

Question: $\exists d + 1$ MUBs in $\mathbb{C}^d \iff \exists$ affine plane of order $d$?
Known results

- Known: $k \leq d + 1$, attained if $d$ is a prime power.
  (Ivanovic '81, Wooters-Fields '89)
- What about $d = 6$? Not known if there exist $\geq 3$ MUBs in $\mathbb{C}^6$.

An affine plane of order 3
Known results

- Known: $k \leq d + 1$, attained if $d$ is a prime power. 
  (Ivanovic '81, Wooters-Fields '89)
- What about $d = 6$? Not known if there exist $> 3$ MUBs in $\mathbb{C}^6$.
- Lower bound: if $\exists k$ MUBs in $\mathbb{C}^{d_1}$ and $\mathbb{C}^{d_2}$, then $\exists k$ MUBs in $\mathbb{C}^{d_1d_2}$.

An affine plane of order 3
Known results

- Known: \( k \leq d + 1 \), attained if \( d \) is a prime power.  
  \((\text{Ivanovic '81, Wooters-Fields '89})\)
- What about \( d = 6 \)? Not known if there exist \( > 3 \) MUBs in \( \mathbb{C}^6 \).
- Lower bound: if \( \exists k \) MUBs in \( \mathbb{C}^{d_1} \) and \( \mathbb{C}^{d_2} \), then \( \exists k \) MUBs in \( \mathbb{C}^{d_1 \cdot d_2} \).
  - Not best possible: for \( d = 26^2 = 2^2 \cdot 13^2 \) a construction of \( 6 > 2^2 + 1 \) MUBs is known.  
  \((\text{Wocjan-Beth '05})\)
Known results

- Known: $k \leq d + 1$, attained if $d$ is a prime power.  
  \footnotesize{(Ivanovic '81, Wooters-Fields '89)}

- What about $d = 6$? Not known if there exist $> 3$ MUBs in $\mathbb{C}^6$.

- Lower bound: if $\exists k$ MUBs in $\mathbb{C}^{d_1}$ and $\mathbb{C}^{d_2}$, then $\exists k$ MUBs in $\mathbb{C}^{d_1 d_2}$.
  - Not best possible: for $d = 26^2 = 2^2 \cdot 13^2$ a construction of $6 > 2^2 + 1$ MUBs is known. \footnotesize{(Wocjan-Beth '05)}

- Question: $\exists d + 1$ MUBs in $\mathbb{C}^d \iff \exists$ affine plane of order $d$?

An affine plane of order 3
**Upper bound**

If there are $k$ MUBs in dimension $d$, then $k \leq d + 1$.

**Proof.** For each $e \in \mathbb{C}^d$, define $M(e) := ee^* - I_d/d$. Then

$$M(e) \in \mathcal{M} := \{ X \in \mathbb{C}^{d \times d} \mid X^* = X, \text{trace}(X) = 0 \}.$$  

- Orthonormal basis gives $(d - 1)$-dim subspace of $\mathcal{M}$.
- For $u, v \in \mathbb{C}^d$:
  $$\text{trace}(M(u)M(v)) = |u^* v|^2 - 1/d,$$
  so MUBs give orthogonal subspaces of $\mathcal{M}$.
- Hence $k \leq \dim(\mathcal{M})/(d - 1) = \frac{d^2 - 1}{d - 1} = d + 1$.  

\[\square\]
MUBs and polynomial optimization

Approach 1: commutative

\[ \exists k \text{ MUBs in dim } d \iff \text{a system of polynomial equations } \{f_1(x) = 0, \ldots, f_N(x) = 0\} \text{ in } 2kd^2 \text{ real variables has a real solution.} \]
MUBs and polynomial optimization

**Approach 1: commutative**

\[ \exists k \text{ MUBs in dim } d \iff \text{a system of polynomial equations } \{ f_1(x) = 0, \ldots, f_N(x) = 0 \} \text{ in } 2kd^2 \text{ real variables has a real solution.} \]

▶ No solution if 1 in ideal generated by \( f_1, \ldots, f_N \). \( \rightsquigarrow \) Gröbner bases
Approach 1: commutative

\[ \exists k \text{ MUBs in dim } d \iff \text{a system of polynomial equations} \]
\[ \{ f_1(x) = 0, \ldots, f_N(x) = 0 \} \text{ in } 2kd^2 \text{ real variables has a real solution.} \]

- No solution if 1 in ideal generated by \( f_1, \ldots, f_N \). \( \sim \) Gröbner bases
- Optimization: \( \min \{ f_1(x)^2 \mid f_2(x) = 0, \ldots, f_N(x) = 0 \} \).
  - Lasserre hierarchy of lower bounds in polynomial optimization.

（Brierly, Weigert '10）
MUBs and polynomial optimization

**Approach 1: commutative**

\[ \exists k \text{ MUBs in dim } d \iff \text{a system of polynomial equations } \{ f_1(x) = 0, \ldots, f_N(x) = 0 \} \text{ in } 2kd^2 \text{ real variables has a real solution.} \]

- No solution if 1 in ideal generated by \( f_1, \ldots, f_N \). ⇔ Gröbner bases
- Optimization: \( \min \{ f_1(x)^2 \mid f_2(x) = 0, \ldots, f_N(x) = 0 \} \).
  - Lasserre hierarchy of lower bounds in polynomial optimization.

(Brierly, Weigert '10)

**Approach 2: noncommutative**

- \( \exists k \text{ MUBs in dimension } d \iff \exists (d, k)-\text{MUB } C^*\text{-algebra.} \)

(Navascués, Pironio, Acín '12)

\[ \implies \text{problem in } dk \text{ noncommutative real variables.} \]
MUBs and polynomial optimization

Approach 1: commutative

\[ \exists k \text{ MUBs in dim } d \iff \text{a system of polynomial equations} \]
\[ \{ f_1(x) = 0, \ldots, f_N(x) = 0 \} \text{ in } 2kd^2 \text{ real variables has a real solution.} \]

- No solution if 1 in ideal generated by \( f_1, \ldots, f_N \). \( \leadsto \) Gröbner bases
- Optimization: \( \min \{ f_1(x)^2 \mid f_2(x) = 0, \ldots, f_N(x) = 0 \} \).
  - Lasserre hierarchy of lower bounds in polynomial optimization.

(Brierly, Weigert ’10)

Approach 2: noncommutative

- \( \exists k \text{ MUBs in dimension } d \iff \exists (d, k)-\text{MUB } C^*-\text{algebra.} \)
  (Navascués, Pironio, Acín ’12)

\( \leadsto \) problem in \( dk \) noncommutative real variables.

- Quantum random access codes and nonlocal games.
  \( \leadsto \) no \( d + 2 \) MUBs for \( d = 3, 4 \). (Aguilar, Borkała, Mironowicz, Pawłowski ’18)
Our contributions

SDPs resulting from characterization of Navascués, Pironio, Acín are symmetric under an action of the wreath product $S_d \wr S_k = S_d^k \rtimes S_k$.

▶ We fully exploit this symmetry to reduce the SDPs.

Main contribution

Explicit decomposition of the $S_d \wr S_k$-module $\mathbb{C}^{([d] \times [k])^t}$ into irreducibles.
Our contributions

SDPs resulting from characterization of Navascués, Pironio, Acín are symmetric under an action of the wreath product \( S_d \wr S_k = S_d^k \rtimes S_k \).

\( \blacktriangleright \) We fully exploit this symmetry to reduce the SDPs.

Main contribution

Explicit decomposition of the \( S_d \wr S_k \)-module \( \mathbb{C}^([d] \times [k])^t \) into irreducibles.

\( \blacktriangleright \) We compute several levels of the hierarchy.

\( \blacktriangleright \) Up to level 5.5 for \((d, k) = (6, 7)\).

\( \blacktriangleright \) Numerical SOS-certificates that no \( d + 2 \) MUBs exist in dimensions \( d = 2, 3, 4, 5, 6, 7, 8 \).
If \{u^{(1)}_1, \ldots, u^{(1)}_d\}, \ldots, \{u^{(k)}_1, \ldots, u^{(k)}_d\} are \(k\) MUBs in \(\mathbb{C}^d\), define
\[X_{i,j} = u^{(j)}_i (u^{(j)}_i)^*\] for all \(i \in [d], j \in [k]\).
If \( \{u_1^{(1)}, \ldots, u_d^{(1)}\}, \ldots, \{u_1^{(k)}, \ldots, u_d^{(k)}\} \) are \( k \) MUBs in \( \mathbb{C}^d \), define
\[
X_{i,j} = u_i^{(j)}(u_i^{(j)})^* \quad \text{for all } i \in [d], j \in [k].
\]

Relations

The \( X_{i,j} \) are rank-1 projectors with:

1. \( X_{i,j}X_{\ell,j} = \delta_{i,\ell}X_{i,j} \) for all \( i, \ell \in [d], j \in [k] \).

\[
\Downarrow \quad X_{i,j}X_{\ell,j} = u_i^{(j)}(u_i^{(j)})^*u_\ell^{(j)}(u_\ell^{(j)})^* = \delta_{i,\ell}X_{i,j}.
\]
If \( \{ u_1^{(1)}, \ldots, u_d^{(1)} \}, \ldots, \{ u_1^{(k)}, \ldots, u_d^{(k)} \} \) are \( k \) MUBs in \( \mathbb{C}^d \), define

\[
X_{i,j} = u_i^{(j)}(u_i^{(j)})^* \text{ for all } i \in [d], j \in [k].
\]

**Relations**

The \( X_{i,j} \) are rank-1 projectors with:

1. \( X_{i,j}X_{\ell,j} = \delta_{i,\ell}X_{i,j} \text{ for all } i, \ell \in [d], j \in [k]. \)

\( \Rightarrow \ X_{i,j}X_{\ell,j} = u_i^{(j)}(u_i^{(j)})^*u_\ell^{(j)}(u_\ell^{(j)})^* = \delta_{i,\ell}X_{i,j}. \)

2. \( \sum_{i \in [d]} X_{i,j} = I \text{ for all } j \in [k]. \)

3. \( X_{i,j}X_{\ell,m}X_{i,j} = \frac{1}{d}X_{i,j} \text{ for all } i, \ell \in [d], j, m \in [k] \text{ with } j \neq m. \)

4. \( [X_{i,j}UX_{i,j}, X_{i,j}VX_{i,j}] = 0 \text{ for all } i \in [d], j \in [k], U, V \in \mathbb{C}^{d \times d}. \)
If \( \{u_1^{(1)}, \ldots, u_d^{(1)}\}, \ldots, \{u_1^{(k)}, \ldots, u_d^{(k)}\} \) are \( k \) MUBs in \( \mathbb{C}^d \), define
\[
X_{i,j} = u_i^{(j)}(u_i^{(j)})^* \quad \text{for all } i \in [d], j \in [k].
\]

Relations

The \( X_{i,j} \) are rank-1 projectors with:

1. \( X_{i,j}X_{\ell,j} = \delta_{i,\ell}X_{i,j} \) for all \( i, \ell \in [d], j \in [k] \).

\[
\Downarrow \quad X_{i,j}X_{\ell,j} = u_i^{(j)}(u_i^{(j)})^*u_{\ell}^{(j)}(u_{\ell}^{(j)})^* = \delta_{i,\ell}X_{i,j}.
\]

2. \( \sum_{i \in [d]} X_{i,j} = I \) for all \( j \in [k] \).

3. \( X_{i,j}X_{\ell,m}X_{i,j} = \frac{1}{d}X_{i,j} \) for all \( i, \ell \in [d], j, m \in [k] \) with \( j \neq m \).

4. \( [X_{i,j}UX_{i,j}, X_{i,j}VX_{i,j}] = 0 \) for all \( i \in [d], j \in [k], U, V \in \mathbb{C}^{d \times d} \).

Theorem (Navascués, Pironio, Acín ’12)

\[ \exists k \text{ MUBs in dimension } d \iff \exists \text{ } C^*-\text{algebra } \mathcal{A} \text{ with self-adjoint operators } X_{i,j} \in \mathcal{A} \text{ satisfying } 1-4 \]
MUB-algebra

If \( \{u^{(1)}_1, \ldots, u^{(1)}_d\}, \ldots, \{u^{(k)}_1, \ldots, u^{(k)}_d\} \) are \( k \) MUBs in \( \mathbb{C}^d \), define

\[
X_{i,j} = u^{(j)}_i (u^{(j)}_i)^* \quad \text{for all } i \in [d], j \in [k].
\]

Relations

The \( X_{i,j} \) are rank-1 projectors with:

1. \( X_{i,j} X_{\ell,j} = \delta_{i,\ell} X_{i,j} \) for all \( i, \ell \in [d], j \in [k] \).

\[
\Downarrow \quad X_{i,j} X_{\ell,j} = u^{(j)}_i (u^{(j)}_i)^* u^{(j)}_\ell (u^{(j)}_\ell)^* = \delta_{i,\ell} X_{i,j}.
\]

2. \( \sum_{i \in [d]} X_{i,j} = I \) for all \( j \in [k] \).

3. \( X_{i,j} X_{\ell,m} X_{i,j} = \frac{1}{d} X_{i,j} \) for all \( i, \ell \in [d], j, m \in [k] \) with \( j \neq m \).

4. \( [X_{i,j} UX_{i,j}, X_{i,j} VX_{i,j}] = 0 \) for all \( i \in [d], j \in [k], U, V \in \mathbb{C}^{d \times d} \).

Theorem (Navascués, Pironio, Acín ’12)

\( \exists k \) MUBs in dimension \( d \) \( \iff \)

\( \exists \mathbb{C}^*\)-algebra \( \mathcal{A} \) with self-adjoint operators \( X_{i,j} \in \mathcal{A} \) satisfying 1-4

with linear \( \tau : \mathcal{A} \rightarrow \mathbb{R} \) which is positive \( \tau(a^*a) \geq 0 \) and tracial \( \tau(ab) = \tau(ba) \) for all \( a, b \in \mathcal{A} \).
SDP formulation

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

**Level \( t \) bound**

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

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

Level \( t \) bound

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

Positivity condition gives SDP:

\[
L(p^*p) \geq 0 \text{ for all } p \in \mathbb{R}\langle x\rangle_{=t} \iff M_t(L) := (L(u^*v))_{u,v \in \langle x\rangle_{=t}} \succeq 0
\]
SDP formulation

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

Level \( t \) bound

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

Positivity condition gives SDP:

\[ L(p^*p) \geq 0 \text{ for all } p \in \mathbb{R}\langle x \rangle_{=t} \iff M_t(L) := (L(u^*v))_{u,v} \in \langle x \rangle_{=t} \succeq 0 \]

Certificates

\[ \text{sdp}(d, k, t) \text{ infeasible } \implies \text{ no } k \text{ MUBs in } \mathbb{C}^d. \]
\[ \text{No } k \text{ MUBs in } \mathbb{C}^d \implies \exists t \text{ with sdp}(d, k, t) \text{ infeasible.} \]
Suppose: $G$ finite group, acting on $[d] \times [k]$, hence on $\mathbb{R}\langle x \rangle$, s.t.

$$p \in I_{\text{MUB}} \implies \sigma \cdot p \in I_{\text{MUB}} ~ \forall \sigma \in G.$$
Group-invariant problem

Suppose: $G$ finite group, acting on $[d] \times [k]$, hence on $\mathbb{R} \langle x \rangle$, s.t.

$$ p \in \mathcal{I}_{MUB} \implies \sigma \cdot p \in \mathcal{I}_{MUB}, \quad \forall \sigma \in G. $$

Then $L$ feasible $\implies \sigma \cdot L \in \mathbb{R} \langle x \rangle^* \text{ feasible, with } \sigma \cdot L(p) = L(\sigma \cdot p)$. 
Suppose: $G$ finite group, acting on $[d] \times [k]$, hence on $\mathbb{R}\langle x \rangle$, s.t.

$$p \in \mathcal{I}_{\text{MUB}} \implies \sigma \cdot p \in \mathcal{I}_{\text{MUB}} \quad \forall \sigma \in G.$$ 

Then $L$ feasible $\implies \sigma \cdot L \in \mathbb{R}\langle x \rangle^*$ feasible, with $\sigma \cdot L(p) = L(\sigma \cdot p)$.

Indeed:

1. $M(\sigma \cdot L) \succeq 0$
   $$\downarrow \quad M(\sigma \cdot L)_{u,v} = \sigma \cdot L(u^* v) = L(\sigma(u^*)\sigma(v)) = M(L)_{\sigma \cdot u, \sigma \cdot v}$$
2. $\sigma \cdot L = 0$ on $\mathcal{I}_{\text{MUB}}$
3. $\sigma \cdot L$ is tracial.
   $$\downarrow \quad \sigma \cdot L(ab) = L(\sigma(ab)) = L(\sigma(a)\sigma(b)) = L(\sigma(b)\sigma(a)) = \sigma \cdot L(ba).$$
Group-invariant problem

Suppose: $G$ finite group, acting on $[d] \times [k]$, hence on $\mathbb{R}\langle x \rangle$, s.t.

$$ p \in \mathcal{I}_{\text{MUB}} \implies \sigma \cdot p \in \mathcal{I}_{\text{MUB}} \quad \forall \sigma \in G. $$

Then $L$ feasible $\implies \sigma \cdot L \in \mathbb{R}\langle x \rangle^*$ feasible, with $\sigma \cdot L(p) = L(\sigma \cdot p)$.

Indeed:

- $M(\sigma \cdot L) \succeq 0$
  - $M(\sigma \cdot L)_{u,v} = \sigma \cdot L(u^*v) = L(\sigma(u^*)\sigma(v)) = M(L)_{\sigma \cdot u, \sigma \cdot v}$

- $\sigma \cdot L = 0$ on $\mathcal{I}_{\text{MUB}}$

- $\sigma \cdot L$ is tracial.
  - $\sigma \cdot L(ab) = L(\sigma(ab)) = L(\sigma(a)\sigma(b)) = L(\sigma(b)\sigma(a)) = \sigma \cdot L(ba)$.

$$ \implies L^G := \frac{1}{|G|} \sum_{\sigma \in G} \sigma \cdot L \text{ is feasible, and } G\text{-invariant.} $$

Assumption

Optimum $L$ is $G$-invariant. $\Rightarrow$ significant reduction in number of variables
The symmetry of the problem

Suppose \( \{u_1^{(1)}, \ldots, u_d^{(1)}\}, \ldots, \{u_1^{(k)}, \ldots, u_d^{(k)}\} \) are \( k \) MUBs in \( \mathbb{C}^d \).
The symmetry of the problem

Suppose \( \{u_1^{(1)}, \ldots, u_d^{(1)}\}, \ldots, \{u_1^{(k)}, \ldots, u_d^{(k)}\} \) are \( k \) MUBs in \( \mathbb{C}^d \).

The group \( G = S_d \rtimes S_k \) acts on the \( X_{i,j} = u_i^{(j)}(u_i^{(j)})^* \) via:

\[
(\sigma_1, \ldots, \sigma_k; \pi) \cdot X_{i,j} = X_{\sigma_{\pi(j)}(i), \pi(j)}, \quad (i \in [d], j \in [k]), \text{ respecting } \mathcal{I}_{\text{MUB}}.
\]
The symmetry of the problem

Suppose \( \{ u_1^{(1)}, \ldots, u_d^{(1)} \}, \ldots, \{ u_1^{(k)}, \ldots, u_d^{(k)} \} \) are \( k \) MUBs in \( \mathbb{C}^d \).

The group \( G = S_d \wr S_k \) acts on the \( X_{i,j} = u_i^{(j)}(u_i^{(j)})^* \) via:

\[
(\sigma_1, \ldots, \sigma_k; \pi) \cdot X_{i,j} = X_{\sigma_1^{\pi(j)}, \sigma_2^{\pi(j)}, \ldots, \sigma_k^{\pi(j)}}(i, \pi(j)), \quad (i \in [d], j \in [k]), \text{ respecting } I_{\text{MUB}}.
\]

Example of \( G \)-invariant \( L \)

Let \( t = 1 \). Then \( M(L)_{1} \) contains monomials of length 2. Up to \( S_d \wr S_k \):

\[
L(x_1,1x_1,1) = L(x_1,1) = 1,
\]

\[
L(x_1,1x_1,2) = L(x_1,1x_1,2x_1,1) = 1/d,
\]

\[
L(x_1,1x_2,1) = 0.
\]
Approach: reduction via block-diagonalization

Symmetric problems have symmetric solutions in a matrix algebra. Then there exists a reduction to matrix blocks. (Artin-Wedderburn)

Challenge: obtain reduction, no general recipe.

Approach: study representation theory of group leaving the problem invariant.
Artin-Wedderburn

Every (unital) complex matrix $\mathcal{A}$ is $\ast$-isomorphic to a direct sum of full matrix $\ast$-algebras.

$$\mathcal{A} \cong \bigoplus_{i=1}^{k} \mathbb{C}^{m_i \times m_i}.$$ 

The $m_i$ depend on the “commutativity” of $\mathcal{A}$. Small example:

$$\begin{pmatrix} a & b & b & b \\ b & c & d & d \\ b & d & c & d \\ b & d & d & c \end{pmatrix} \succeq 0 \iff \begin{pmatrix} a & 3b \\ 3b & 3c + 6d \\ \end{pmatrix} \begin{pmatrix} 2c - 2d \end{pmatrix} \succeq 0.$$
**Block-diagonalization**

**Artin-Wedderburn**

Every (unital) complex matrix $*$-algebra $\mathcal{A}$ is $*$-isomorphic to a direct sum of full matrix $*$-algebras.

$$\mathcal{A} \cong k \bigoplus_{i=1}^{k} \mathbb{C}^{m_i \times m_i}. $$

The $m_i$ depend on the “commutativity” of $\mathcal{A}$. Small example:

$$\begin{pmatrix}
  a & b & b & b \\
  b & c & d & d \\
  b & d & c & d \\
  b & d & d & c
\end{pmatrix} \succeq 0 \iff \begin{pmatrix}
  a & 3b \\
  3b & 3c + 6d \\
  2c - 2d
\end{pmatrix} \succeq 0.$$

**Applications in**

- Coding theory (Schrijver ’05)
- Other areas of combinatorics (survey De Klerk, ’10)
- Polynomial optimization (Gatermann, Parrilo ’04, Riener, Theobald, Andrén, Lasserre ’13)
Let $G$ be a finite group acting on a finite set $Z$. Decompose $\mathbb{C}^Z$ as:

$$V = \bigoplus_{i=1}^{k} \bigoplus_{j=1}^{m_i} V_{i,j},$$

for irreducible $G$-modules $V_{i,j}$ with $V_{i,j} \cong V_{i',j'}$ iff $i = i'$. 
Let $G$ be a finite group acting on a finite set $Z$. Decompose $\mathbb{C}^Z$ as:

$$V = \bigoplus_{i=1}^{k} \bigoplus_{j=1}^{m_i} V_{i,j},$$

for irreducible $G$-modules $V_{i,j}$ with $V_{i,j} \cong V_{i',j'}$ iff $i = i'$. Choose nonzero $u_{i,j} \in V_{i,j}$ s.t. for all $i \in [k], j, j' \in [m_i]$ there is a $G$-isomorphism $V_{i,j} \to V_{i,j'}$ mapping $u_{i,j}$ to $u_{i,j'}$. Define the map

$$\Phi : \left( \mathbb{C}^Z \times Z \right)^G \to \bigoplus_{i=1}^{k} \mathbb{C}^{m_i \times m_i},$$

$$A \mapsto \bigoplus_{i=1}^{k} \left( \langle u_{i,j'}, Au_{i,j} \rangle \right)_{j,j' \in [m_i]}$$
Let $G$ be a finite group acting on a finite set $Z$. Decompose $\mathbb{C}^Z$ as:

$$V = \bigoplus_{i=1}^{k} \bigoplus_{j=1}^{m_i} V_{i,j},$$

for irreducible $G$-modules $V_{i,j}$ with $V_{i,j} \cong V_{i',j'}$ iff $i = i'$. Choose nonzero $u_{i,j} \in V_{i,j}$ s.t. for all $i \in [k]$, $j, j' \in [m_i]$ there is a $G$-isomorphism $V_{i,j} \rightarrow V_{i,j'}$ mapping $u_{i,j}$ to $u_{i,j'}$. Define the map

$$\Phi : \left( \mathbb{C}^{Z \times Z} \right)^G \rightarrow \bigoplus_{i=1}^{k} \mathbb{C}^{m_i \times m_i},$$

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

**Key fact**

For all $A \in \left( \mathbb{C}^{Z \times Z} \right)^G$ we have $A \succeq 0 \iff \Phi(A) \succeq 0$. 
Symmetry reduction

Recall: \( \text{sdp}(d, k, t) = \inf \{ 0 : \exists L \in \mathbb{R} \langle x \rangle_{2t}^* \text{ s.t. } L \text{ is tracial, } G\text{-invariant, } \)
\[ L = 0 \text{ on } \mathcal{I}_{\text{MUB},2t}, \quad L(I) = d, \]
\[ M_t(L) := (L(u^* v))_{u,v \in \langle x \rangle_{=t}} \geq 0 \} \).

In our case \( Z = \langle x \rangle_{=t} \cong ([d] \times [k])^t \) and \( G = S_d \wr S_k \).
Recall: $\text{sdp}(d, k, t) = \inf \{ 0 : \exists \ L \in \mathbb{R}\langle \mathbf{x} \rangle_{2t}^* \text{ s.t. } L \text{ is tracial, } G\text{-invariant, }$
$ L = 0 \text{ on } \mathcal{I}_{\text{MUB},2t}, L(I) = d,$
$ M_t(L) := (L(u^* v))_{u,v \in \langle \mathbf{x} \rangle_{=t}} \succeq 0 \}.$

In our case $Z = \langle \mathbf{x} \rangle_{=t} \simeq ([d] \times [k])^t$ and $G = S_d \wr S_k.$

First decomposition from $G$-orbits: $\mathbb{C}^Z = \bigoplus_{(P,Q)} V_{P,Q},$ where

- $P = \{ P_1, \ldots, P_r \}$ is a set partition of $[t]$ in $\leq k$ parts,
- $Q = \{ Q_1, \ldots, Q_r \}$ where $Q_i$ is a set partition of $P_i$ in $\leq d$ parts.
Symmetry reduction

Recall: \( \text{sdp}(d, k, t) = \inf \{ 0 : \exists L \in \mathbb{R}\langle x \rangle_{2t}^* \text{ s.t. } L \text{ is tracial}, G\text{-invariant}, \)
\[
L = 0 \text{ on } \mathcal{I}_{\text{MUB},2t}, L(I) = d,
\]
\[
M_t(L) := (L(u^* v))_{u,v \in \langle x \rangle_{=t}} \succeq 0 \}.
\]

In our case \( Z = \langle x \rangle_{=t} \simeq ([d] \times [k])^t \) and \( G = S_d \wr S_k \).

First decomposition from \( G \)-orbits: \( \mathbb{C}^Z = \bigoplus_{(P,Q)} V_{P,Q} \), where
\begin{itemize}
  \item \( P = \{P_1, \ldots, P_r\} \) is a set partition of \([t]\) in \( \leq k \) parts,
  \item \( Q = \{Q_1, \ldots, Q_r\} \) where \( Q_i \) is a set partition of \( P_i \) in \( \leq d \) parts.
\end{itemize}

Example of \((P, Q)\) for \( t = 4\):
\[
P = \{\{1, 3, 4\}, \{2\}\}, \ Q = \{Q_1, Q_2\} \text{ with } Q_1 = \{\{1, 3\}, \{4\}\}, \ Q_2 = \{2\}
\]
\[
V_{P,Q} := \text{span of monomials with indices } (i, j) (a, \ell) (i, j) (b, j)
\]
Decomposing $V_P$ with $S_k$-action: ‘L-shapes’

First consider $S_k$-action on monomials in $x_1, \ldots, x_k$.

$S_k$-orbit of $\langle x \rangle = t \xleftarrow{1:1} P = \{P_1, \ldots, P_r\}$ set partition of $[t]$ in $\leq k$ parts.
Decomposing $V_P$ with $S_k$-action: ‘L-shapes’

First consider $S_k$-action on monomials in $x_1, \ldots, x_k$.

$S_k$-orbit of $\langle x \rangle = t \stackrel{1:1}{\longleftrightarrow} P = \{P_1, \ldots, P_r\}$ set partition of $[t]$ in $\leq k$ parts.

$V_P$ is a permutation module $M^{\mu_r}$ for the partition $\mu_r = (k - r, 1, \ldots, 1)$:

Identify monomial in $V_P$ (with $w_j \in [k]$ assigned to $P_j$) with tabloid

\[
\begin{array}{c}
\cdots \\
\vdots \\
w_1 \\
w_2 \\
\vdots \\
w_r \\
\end{array}
\quad \leftrightarrow \quad \begin{array}{c}
\cdots \\
3 \\
7 \\
4 \\
\end{array}
\]

Example: $x_3 x_7 x_3 x_7 x_4 \leftrightarrow \begin{array}{c}
\cdots \\
3 \\
7 \\
4 \\
\end{array}$

Decomposition follows directly from known representation theory of $S_k$.\[ V_P = M^{\mu_r} = \bigoplus_{\lambda \vdash k} \bigoplus_{\tau \in T_{\lambda, \mu_r}} \lambda \cdot S_{\lambda}. \] (e.g., Sagan '01)
Decomposing $V_P$ with $S_k$-action: ‘L-shapes’

First consider $S_k$-action on monomials in $x_1, \ldots, x_k$.

$S_k$-orbit of $\langle x \rangle \mapsto P = \{P_1, \ldots, P_r\}$ set partition of $[t]$ in $\leq k$ parts.

$V_P$ is a permutation module $M^{\mu_r}$ for the partition $\mu_r = (k - r, 1, \ldots, 1)$: Identify monomial in $V_P$ (with $w_j \in [k]$ assigned to $P_j$) with tabloid

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

Example: $x_3x_7x_3x_7x_4 \mapsto \begin{array}{cccc}
\cdots \\
3 \\
7 \\
4 \\
\end{array}$

Decomposition follows directly from known representation theory of $S_k$.

\[
V_P = M^{\mu_r} = \bigoplus_{\lambda \vdash k} \left( \bigoplus_{\tau \in T_{\lambda, \mu_r}} \tau \cdot S^{\lambda} \right).
\]

(e.g., Sagan '01)
Decomposing $V_{P,Q}$ with $S_d \wr S_k$-action

Monomials in $V_{P,Q}$ correspond to tensor products of tabloids.

As before: if $w(j) \in [k]$ assigned to $P_j$ \[ \rightarrow \quad w = \]

if $v^i(j) \in [d]$ assigned to the $j$-th set in $Q_i$ \[ \rightarrow \quad v_i = \]
Decomposing $V_{P,Q}$ with $S_d \wr S_k$-action

Monomials in $V_{P,Q}$ correspond to tensor products of tabloids.

As before: if $w(j) \in [k]$ assigned to $P_j$ \quad $w = \ldots \ldots \ldots \ldots$

if $v^i(j) \in [d]$ assigned to the $j$-th set in $Q_i$ \quad $v_i = \ldots \ldots \ldots \ldots$

$S_d \wr S_k$-action is $(\sigma_1, \ldots, \sigma_k; \tau) \cdot \left( \bigotimes_{i \in [r]} v_i \otimes w \right) = \left( \bigotimes_{i \in [r]} \sigma_{\tau w(i)} v_i \right) \otimes \tau w$
The irreducible ‘Specht’ modules of $S_d \wr S_k$ are known, but the action looks different:

$$(\sigma_1, \ldots, \sigma_k; \tau) \cdot \bigotimes_{i \in [k]} v_i = \bigotimes_{i \in [k]} \sigma_i \cdot v_{\tau^{-1}(i)}.$$
The irreducible ‘Specht’ modules of $S_d \wr S_k$ are known, but the action looks different:

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

We decompose $V_{P, Q}$ by separately decomposing each permutation module for $S_d$ or $S_k$. 

Key step: We show that the modules in our decomposition are isomorphic to known ‘Specht’ modules $S^\lambda$.

Link to literature: $V_{P, Q} \approx M_\gamma$, for known ‘permutation’ module $M_\gamma$.

Multiplicities of $S^\lambda$ in $M_\gamma$ can be derived from the literature, explicit embeddings not available.
Decomposing $V_{P,Q}$ with $S_d \wr S_k$-action – II

The irreducible ‘Specht’ modules of $S_d \wr S_k$ are known, but the action looks different:

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

- We decompose $V_{P,Q}$ by separately decomposing each permutation module for $S_d$ or $S_k$.
- **Key step:** We show that the modules in our decomposition are isomorphic to known ‘Specht’ modules $S^\lambda$. 

▶ Link to literature: $V_{P,Q} \cong M_{\gamma}$, for known ‘permutation’ module $M_{\gamma}$.

▶ Multiplicities of $S^\lambda$ in $M_{\gamma}$ can be derived from the literature, explicit embeddings not available.
Decomposing $V_P, Q$ with $S_d \wr S_k$-action – II

The irreducible ‘Specht’ modules of $S_d \wr S_k$ are known, but the action looks different:

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

- We decompose $V_P, Q$ by separately decomposing each permutation module for $S_d$ or $S_k$.
- Key step: We show that the modules in our decomposition are isomorphic to known ‘Specht’ modules $S^\lambda$.
- Link to literature: $V_P, Q \cong M^\gamma$, for known ‘permutation’ module $M^\gamma$.
  - Multiplicities of $S^\lambda$ in $M^\gamma$ can be derived from the literature,
  - Explicit embeddings not available.
Computational results – full hierarchy

- \( \sum m_i^2 \) obtained from reduction for \( d, k \geq 2t \) is entry 2t of OEIS A000258: 1, 3, 12, 60, 358, 2471, 19302, 167894, 1606137.
Computational results – full hierarchy

- $\sum m_i^2$ obtained from reduction for $d, k \geq 2t$ is entry $2t$ of OEIS A000258: 1, 3, 12, 60, 358, 2471, 19302, 167894, 1606137.

- We compute several levels of the hierarchy:

<table>
<thead>
<tr>
<th>$d$</th>
<th>$k$</th>
<th>$t$</th>
<th>$(dk)^[t]$</th>
<th>#vars</th>
<th>#linear constraints</th>
<th>block sizes</th>
<th>result</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>sum</td>
<td>max</td>
</tr>
<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>
</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>
</tr>
<tr>
<td>4</td>
<td>6</td>
<td>5</td>
<td>7962624</td>
<td>43</td>
<td>2</td>
<td>6374</td>
<td>389</td>
</tr>
<tr>
<td>5</td>
<td>7</td>
<td>5</td>
<td>52521875</td>
<td>43</td>
<td>2</td>
<td>6732</td>
<td>389</td>
</tr>
<tr>
<td>6</td>
<td>8</td>
<td>5</td>
<td>254803968</td>
<td>43</td>
<td>2</td>
<td>6820</td>
<td>389</td>
</tr>
<tr>
<td>7</td>
<td>9</td>
<td>5</td>
<td>992436543</td>
<td>43</td>
<td>2</td>
<td>6830</td>
<td>389</td>
</tr>
<tr>
<td>8</td>
<td>10</td>
<td>5</td>
<td>32768000000</td>
<td>43</td>
<td>2</td>
<td>6831</td>
<td>389</td>
</tr>
<tr>
<td>6</td>
<td>10</td>
<td>5.5</td>
<td>7962624</td>
<td>54</td>
<td>3</td>
<td>8049</td>
<td>577</td>
</tr>
<tr>
<td>6</td>
<td>7</td>
<td>4.5</td>
<td>3111696</td>
<td>7</td>
<td>0</td>
<td>1627</td>
<td>146</td>
</tr>
<tr>
<td>6</td>
<td>7</td>
<td>5</td>
<td>130691232</td>
<td>43</td>
<td>2</td>
<td>6749</td>
<td>389</td>
</tr>
<tr>
<td>6</td>
<td>7</td>
<td>5.5</td>
<td>130691232</td>
<td>75</td>
<td>3</td>
<td>18538</td>
<td>1107</td>
</tr>
</tbody>
</table>
Future work

- Improve implementation, run on cluster instead of desktop.
  - Aim: no 7 MUBs in dimension 6.
Future work

- Improve implementation, run on cluster instead of desktop.
  - Aim: no 7 MUBs in dimension 6.
- Partial approaches: subset of blocks or relations from higher levels.

If infeasible, find analytic certificate.

Question: certificate for no \(d + 2\) MUBs in \(C^d\) at level \(t = 5\)?

Can the reduction be computed in polynomial time, for fixed \(t\)?

Symmetry reduction for other semidefinite programming approaches. (e.g., QRAC-formulation of Aguilar, Borka la, Mironowicz, Paw lowski '18)
Future work

- Improve implementation, run on cluster instead of desktop.
  - Aim: no 7 MUBs in dimension 6.
- Partial approaches: subset of blocks or relations from higher levels.
- If infeasible, find analytic certificate.
  - Question: certificate for no $d + 2$ MUBs in $\mathbb{C}^d$ at level $t = 5$?
Future work

- Improve implementation, run on cluster instead of desktop.
  - Aim: no 7 MUBs in dimension 6.
- Partial approaches: subset of blocks or relations from higher levels.
- If infeasible, find analytic certificate.
  - Question: certificate for no \( d + 2 \) MUBs in \( \mathbb{C}^d \) at level \( t = 5 \)?
- Can the reduction be computed in polynomial time, for fixed \( t \)?
Future work

- Improve implementation, run on cluster instead of desktop.
  - Aim: no 7 MUBs in dimension 6.
- Partial approaches: subset of blocks or relations from higher levels.
- If infeasible, find analytic certificate.
  - Question: certificate for no $d + 2$ MUBs in $\mathbb{C}^d$ at level $t = 5$?
- Can the reduction be computed in polynomial time, for fixed $t$?
- Symmetry reduction for other semidefinite programming approaches.
  (e.g., QRAC-formulation of Aguilar, Borkała, Mironowicz, Pawłowski ‘18)
Use only submatrix indexed by monomials $x_{1,j}$ with $j \in [k]$. 
Computational results – $S_k$-part

- Use only submatrix indexed by monomials $x_{1,j}$ with $j \in [k]$.
- Bell numbers: $\sum m_i^2$ obtained from reduction for $k \geq 2t$ is entry $2t$ of OEIS A000110: 1, 2, 5, 15, 52, 203, 877, 4140, 21147, 115975.

<table>
<thead>
<tr>
<th>$d$</th>
<th>$k$</th>
<th>$t$</th>
<th>$k^{[t]}$</th>
<th>#vars</th>
<th>#linear constraints</th>
<th>block sizes</th>
<th>result</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>sum</td>
<td>max</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>4</td>
<td>4.5</td>
<td>256</td>
<td>5</td>
<td>0</td>
<td>48</td>
<td>24</td>
</tr>
<tr>
<td>3</td>
<td>5</td>
<td>4.5</td>
<td>625</td>
<td>5</td>
<td>0</td>
<td>95</td>
<td>32</td>
</tr>
<tr>
<td>4</td>
<td>6</td>
<td>5</td>
<td>7776</td>
<td>17</td>
<td>2</td>
<td>364</td>
<td>70</td>
</tr>
<tr>
<td>5</td>
<td>7</td>
<td>6.5</td>
<td>117649</td>
<td>467</td>
<td>74</td>
<td>3288</td>
<td>640</td>
</tr>
<tr>
<td>6</td>
<td>4</td>
<td>7.5</td>
<td>16384</td>
<td>20</td>
<td>5</td>
<td>586</td>
<td>293</td>
</tr>
<tr>
<td>6</td>
<td>7</td>
<td>6.5</td>
<td>117649</td>
<td>467</td>
<td>74</td>
<td>3288</td>
<td>640</td>
</tr>
</tbody>
</table>