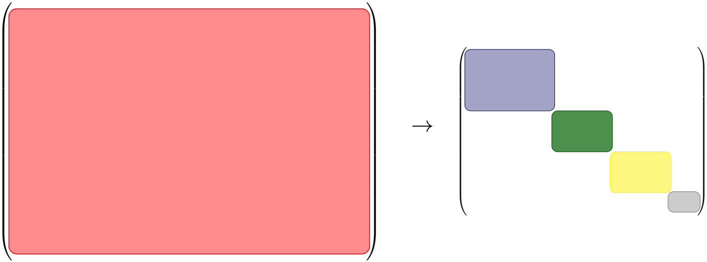
Mutually unbiased bases: polynomial optimization and symmetry

Sven Polak

CWI



Joint work with Sander Gribling (IRIF Paris)

arXiv:2111.05698

Mutually unbiased bases

Definition

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

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

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:

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

Why do so many people study MUBs?

Picture: MS-Tech

Picture: Forest Stearns, Google AI

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.

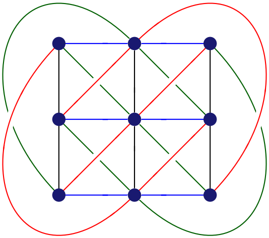
See the survey *'On mutually unbiased bases'*.

(Durt, Englert, Bengtsson, Życzkowski '10).

Known results

- Known: $k \leq d+1$, attained if d is a prime power.

(Ivanovic '81, Wooters-Fields '89)

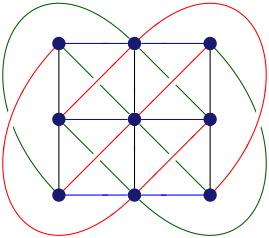


An affine plane of order 3

Known results

- Known: $k \leq d + 1$, attained if d is a prime power.

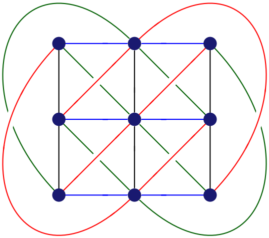
  (Ivanovic '81, Wooters-Fields '89)
- What about $d = 6$? Not known if there exist > 3 MUBs in $\mathbb{C}^6$.



An affine plane of order 3

Known results

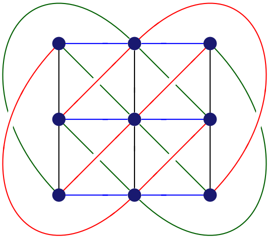
- Known: $k \leq d + 1$, attained if d is a prime power.
  (Ivanovic '81, Wooters-Fields '89)
- What about $d = 6$? Not known if there exist > 3 MUBs in $\mathbb{C}^6$.
- Lower bound: if $\exists\, k$ MUBs in $\mathbb{C}^{d_1}$ and $\mathbb{C}^{d_2}$, then $\exists\, k$ MUBs in $\mathbb{C}^{d_1 d_2}$.



An affine plane of order 3

Known results

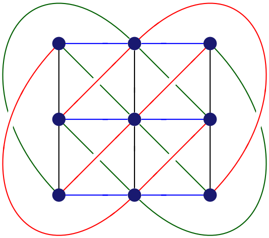
- Known: $k \leq d + 1$, attained if d is a prime power.
  (Ivanovic '81, Wooters-Fields '89)
- What about $d = 6$? Not known if there exist > 3 MUBs in $\mathbb{C}^6$.
- Lower bound: if $\exists\, k$ MUBs in $\mathbb{C}^{d_1}$ and $\mathbb{C}^{d_2}$, then $\exists\, k$ MUBs in $\mathbb{C}^{d_1 d_2}$.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



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 $\mathbb{C}^{d_1 d_2}$.
  - Not best possible: for $d = 26^2 = 2^2 13^2$ a construction of $6 > 2^2 + 1$ MUBs is known. (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

Elementary upper bound

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

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

- Orthonormal basis gives $(d-1)$-dim subspace of $\mathcal{M}$.
- For $u, v \in \mathbb{C}^d$:

  $$\operatorname{trace}(M(u)M(v)) = |u^* v|^2 - 1/d,$$

  so MUBs give orthogonal subspaces of $\mathcal{M}$.
- Hence $k \leq \dim(\mathcal{M})/(d-1) = \frac{d^2-1}{d-1} = d + 1$. □

MUBs and polynomial optimization

Approach 1: commutative

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

MUBs and polynomial optimization

Approach 1: commutative

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

- No solution if 1 in ideal generated by $f_1, \dots, f_N$. $\rightsquigarrow$ Gröbner bases

MUBs and polynomial optimization

Approach 1: commutative

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

- No solution if 1 in ideal generated by $f_1, \ldots, f_N$. $\rightsquigarrow$ 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

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

- No solution if 1 in ideal generated by $f_1, \ldots, f_N$. $\rightsquigarrow$ 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 MUBs in dimension d $\iff$ $\exists$ (d, k)-MUB C^*-algebra.

(Navascués, Pironio, Acín '12)

$\rightsquigarrow$ problem in dk noncommutative real variables.

MUBs and polynomial optimization

Approach 1: commutative

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

- No solution if 1 in ideal generated by $f_1, \ldots, f_N$. $\rightsquigarrow$ 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 MUBs in dimension $d \iff \exists$ (d, k)-MUB C^*-algebra.

  (Navascués, Pironio, Acín '12)

  $\rightsquigarrow$ problem in dk noncommutative real variables.
- Quantum random access codes and nonlocal games.

  $\rightsquigarrow$ 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 $S_d \wr S_k = S_d^k \rtimes S_k$.

- 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.

- We compute several levels of the hierarchy.
  - Up to level 5.5 for $(d, k) = (6, 7)$.
  - Numerical SOS-certificates that no $d + 2$ MUBs exist in dimensions $d = 2, 3, 4, 5, 6, 7, 8$.

MUB-algebra

If $\{u_1^{(1)}, \ldots, u_d^{(1)}\}, \ldots, \{u_1^{(k)}, \ldots, u_d^{(k)}\}$ are k MUBs in $\mathbb{C}^d$, define

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

MUB-algebra

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. $X_{i,j} X_{\ell,j} = \delta_{i,\ell} X_{i,j}$ for all $i, \ell \in [d]$, $j \in [k]$.
   ↳ $X_{i,j} X_{\ell,j} = u_i^{(j)} (u_i^{(j)})^* u_\ell^{(j)} (u_\ell^{(j)})^* = \delta_{i,\ell} X_{i,j}$.

MUB-algebra

If $\{u_1^{(1)}, \dots, u_d^{(1)}\}, \dots, \{u_1^{(k)}, \dots, u_d^{(k)}\}$ 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. $X_{i,j}X_{\ell,j} = \delta_{i,\ell}X_{i,j}$ for all $i, \ell \in [d]$, $j \in [k]$.
   ↳ $X_{i,j}X_{\ell,j} = u_i^{(j)}(u_i^{(j)})^* u_\ell^{(j)}(u_\ell^{(j)})^* = \delta_{i,\ell}X_{i,j}$.
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 $i \in [d]$, $j \in [k]$, $U, V \in \mathbb{C}^{d \times d}$.

MUB-algebra

If $\{u_1^{(1)}, \dots, u_d^{(1)}\}, \dots, \{u_1^{(k)}, \dots, u_d^{(k)}\}$ 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. $X_{i,j}X_{\ell,j} = \delta_{i,\ell}X_{i,j}$ for all $i, \ell \in [d]$, $j \in [k]$.
   ↳ $X_{i,j}X_{\ell,j} = u_i^{(j)}(u_i^{(j)})^* u_\ell^{(j)}(u_\ell^{(j)})^* = \delta_{i,\ell}X_{i,j}$.
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 MUBs in dimension d $\iff$
$\exists$ C^*-algebra $\mathcal{A}$ with self-adjoint operators $X_{i,j} \in \mathcal{A}$ satisfying 1-4

MUB-algebra

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. $X_{i,j}X_{\ell,j} = \delta_{i,\ell}X_{i,j}$ for all $i, \ell \in [d]$, $j \in [k]$.
   ↳ $X_{i,j}X_{\ell,j} = u_i^{(j)}(u_i^{(j)})^* u_\ell^{(j)}(u_\ell^{(j)})^* = \delta_{i,\ell}X_{i,j}$.
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 MUBs in dimension d $\iff$
$\exists$ C^*-algebra $\mathcal{A}$ with self-adjoint operators $X_{i,j} \in \mathcal{A}$ satisfying 1-4
with linear $\tau : \mathcal{A} \to \mathbb{R}$ which is *positive* $\tau(a^*a) \geq 0$ and *tracial* $\tau(ab) = \tau(ba)$ for all $a, b \in \mathcal{A}$.

SDP formulation

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

SDP formulation

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

Level t bound

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

SDP formulation

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

Level t bound

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

Positivity condition gives SDP:

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

SDP formulation

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

Level t bound

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

Positivity condition gives SDP:

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

Certificates

$\mathrm{sdp}(d,k,t)$ infeasible $\Longrightarrow$ no k MUBs in $\mathbb{C}^d$.

No k MUBs in $\mathbb{C}^d$ $\Longrightarrow$ $\exists\, t$ with $\mathrm{sdp}(d,k,t)$ infeasible.

Group-invariant problem

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

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

Group-invariant problem

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

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

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

Group-invariant problem

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

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

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

- $M(\sigma \cdot L) \succeq 0$
  $\hookrightarrow M(\sigma \cdot L)_{u,v} = \sigma \cdot L(u^* v) = L(\sigma(u^* v)) = L(\sigma(u^*)\sigma(v)) = M(L)_{\sigma \cdot u, \sigma \cdot v}$
- $\sigma \cdot L = 0$ on $\mathcal{I}_{\mathrm{MUB}}$
- $\sigma \cdot L$ is tracial.
  $\hookrightarrow \sigma \cdot L(ab) = L(\sigma(ab)) = L(\sigma(a)\sigma(b)) = L(\sigma(b)\sigma(a)) = \sigma \cdot L(ba).$

Group-invariant problem

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

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

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

- $M(\sigma \cdot L) \succeq 0$
  $\hookrightarrow$ $M(\sigma \cdot L)_{u,v} = \sigma \cdot L(u^* v) = L(\sigma(u^* v)) = L(\sigma(u^*)\sigma(v)) = M(L)_{\sigma \cdot u, \sigma \cdot v}$
- $\sigma \cdot L = 0$ on $\mathcal{I}_{\mathrm{MUB}}$
- $\sigma \cdot L$ is tracial.
  $\hookrightarrow$ $\sigma \cdot L(ab) = L(\sigma(ab)) = L(\sigma(a)\sigma(b)) = L(\sigma(b)\sigma(a)) = \sigma \cdot L(ba)$.

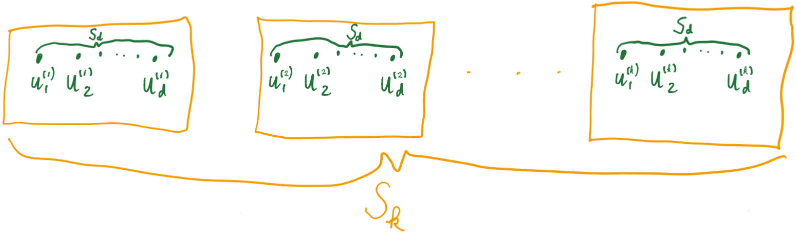
$$\Longrightarrow \quad L^G := \frac{1}{|G|} \sum_{\sigma \in G} \sigma \cdot L \text{ is feasible, and } G\text{-invariant.}$$

Assumption

Optimum L is G-invariant. $\rightsquigarrow$ significant reduction in number of variables

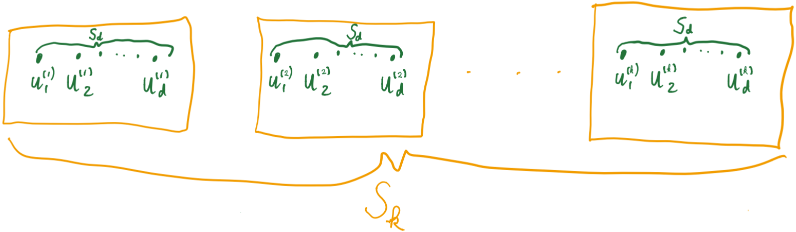
The symmetry of the problem

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

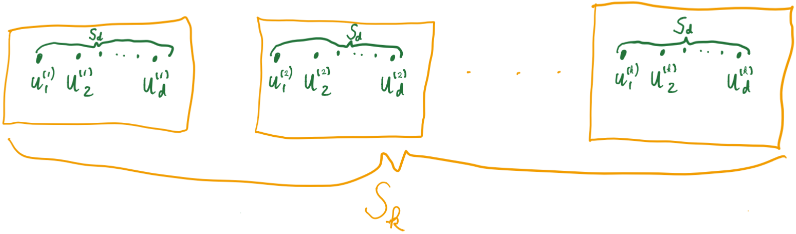


The group $G = S_d \wr S_k$ acts on the $X_{i,j} = u_i^{(j)}(u_i^{(j)})^*$ via:

$(\sigma_1, \dots, \sigma_k; \pi) \cdot X_{i,j} = X_{\sigma_{\pi(j)}(i), \pi(j)}, \qquad (i \in [d], j \in [k]),$ respecting $\mathcal{I}_{\mathrm{MUB}}$.

The symmetry of the problem

Suppose $\{u_1^{(1)}, \dots, u_d^{(1)}\}, \dots, \{u_1^{(k)}, \dots, u_d^{(k)}\}$ 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:

$$(\sigma_1, \dots, \sigma_k; \pi) \cdot X_{i,j} = X_{\sigma_{\pi(j)}(i), \pi(j)}, \qquad (i \in [d], j \in [k]),$$ respecting $\mathcal{I}_{\text{MUB}}$.

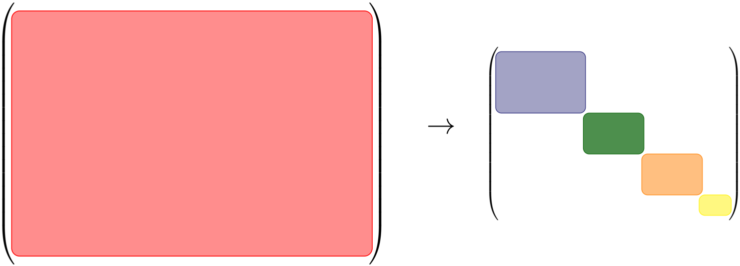
Example of G-invariant L

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

$$L(x_{1,1}x_{1,1}) = L(x_{1,1}) = 1,$$
$$L(x_{1,1}x_{1,2}) = L(x_{1,1}x_{1,2}x_{1,1}) = 1/d,$$
$$L(x_{1,1}x_{2,1}) = 0.$$

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.

Block-diagonalization

Artin-Wedderburn

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

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

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

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

Block-diagonalization

Artin-Wedderburn

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

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

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

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

Applications in

- Coding theory (Schrijver '05)
- Other areas of combinatorics (survey De Klerk, '10)
- Polynomial optimization

(Gatermann, Parrilo '04, Riener, Theobald, Andrén, Lasserre '13)

Group invariance and Artin-Wedderburn

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 $i = i'$.

Group invariance and Artin-Wedderburn

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

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

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

Group invariance and Artin-Wedderburn

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

$$\begin{aligned} \Phi \,:\, \left(\mathbb{C}^{Z\times Z}\right)^G &\to \bigoplus_{i=1}^{k} \mathbb{C}^{m_i \times m_i}, \\ A &\mapsto \bigoplus_{i=1}^{k} \left(\langle u_{i,j'}, A u_{i,j}\rangle\right)_{j,j' \in [m_i]} \end{aligned}$$

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: $\mathrm{sdp}(d,k,t) = \inf\{0 : \exists\, L \in \mathbb{R}\langle \mathbf{x} \rangle_{2t}^{*}$ s.t. L is tracial, G-invariant,

$L = 0$ on $\mathcal{I}_{\mathrm{MUB},2t}$, $L(I) = d$,

$M_t(L) := (L(u^* v))_{u,v \in \langle \mathbf{x} \rangle_{=t}} \succeq 0\}$.

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

Symmetry reduction

Recall: $\mathrm{sdp}(d,k,t) = \inf\{0 : \exists\, L \in \mathbb{R}\langle \mathbf{x}\rangle_{2t}^{*}$ s.t. L is tracial, G-invariant,

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

$$M_t(L) := (L(u^*v))_{u,v\in\langle \boldsymbol{x}\rangle_{=t}} \succeq 0\}.$$

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: $\mathbb{C}^Z = \bigoplus_{(P,\mathbf{Q})} V_{P,\boldsymbol{Q}}$, where

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

Symmetry reduction

Recall: $\mathrm{sdp}(d,k,t) = \inf\{0 : \exists\, L \in \mathbb{R}\langle \mathbf{x}\rangle_{2t}^{*}$ s.t. L is tracial, G-invariant,

$$L = 0 \text{ on } \mathcal{I}_{\mathrm{MUB},2t},\ L(I) = d,$$
$$M_t(L) := (L(u^* v))_{u,v\in\langle \boldsymbol{x}\rangle_{=t}} \succeq 0\}.$$

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: $\mathbb{C}^Z = \bigoplus_{(P,\mathbf{Q})} V_{P,\boldsymbol{Q}}$, where

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

Example of $(P, \boldsymbol{Q})$ for $t = 4$:

$P = \big\{\{1,3,4\},\{2\}\big\}$, $\boldsymbol{Q} = \big\{Q_1, Q_2\big\}$ with $Q_1 = \big\{\{1,3\},\{4\}\big\}$, $Q_2 = \{2\}$

$$V_{P,\mathbf{Q}} := \text{span of monomials with indices } \ (i,j)\,(a,\ell)\,(i,j)\,(b,j)$$

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 $\langle \mathbf{x} \rangle_{=\mathbf{t}} \xleftrightarrow{1:1} P = \{P_1, \ldots, P_r\}$ 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 $\langle \mathbf{x} \rangle_{=\mathbf{t}} \xleftrightarrow{1:1} P = \{P_1, \ldots, P_r\}$ set partition of $[t]$ in $\leq k$ parts.

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

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

Example: $x_3 x_7 x_3 x_7 x_4 \longleftrightarrow \begin{array}{l} \hline \cdots\cdots\cdots \\ \hline 3 \\ \hline 7 \\ \hline 4 \\ \hline \end{array}$

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 $\langle \mathbf{x} \rangle_{=\mathbf{t}} \xleftrightarrow{1:1} P = \{P_1, \ldots, P_r\}$ set partition of $[t]$ in $\leq k$ parts.

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

$$\begin{array}{l} \hline \cdots\cdots\cdots \\ \hline w_1 \\ \hline w_2 \\ \hline \vdots \\ \hline w_r \\ \hline \end{array} . \qquad \text{Example:} \quad x_3 x_7 x_3 x_7 x_4 \longleftrightarrow \begin{array}{l} \hline \cdots\cdots\cdots \\ \hline 3 \\ \hline 7 \\ \hline 4 \\ \hline \end{array}$$

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 $V_{P,\boldsymbol{Q}}$ with $S_d \wr S_k$-action

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

As before: if $w(j) \in [k]$ assigned to P_j $\longrightarrow$ $w = \begin{array}{l} \hline \cdots\cdots\cdots \\ \hline w(1) \\ \hline \vdots \\ \hline w(r) \\ \hline \end{array}$

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

Decomposing $V_{P,\boldsymbol{Q}}$ with $S_d \wr S_k$-action

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

As before: if $w(j) \in [k]$ assigned to P_j $\longrightarrow$ $$w = \begin{array}{l} \hline \cdots\cdots\cdots \\ \hline w(1) \\ \hline \vdots \\ \hline w(r) \\ \hline \end{array}$$

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

$S_d \wr S_k$-action is $(\sigma_1, \ldots, \sigma_k; \tau) \cdot \left(\left(\bigotimes_{i \in [r]} v_i \right) \otimes w \right) = \left(\bigotimes_{i \in [r]} \sigma_{\tau w(i)} v_i \right) \otimes \tau w$

Decomposing $V_{P,\boldsymbol{Q}}$ 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:

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

Decomposing $V_{P,\boldsymbol{Q}}$ 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 $V_{P,\boldsymbol{Q}}$ by separately decomposing each permutation module for S_d or S_k.

Decomposing $V_{P,\boldsymbol{Q}}$ 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 $V_{P,\boldsymbol{Q}}$ 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 $S^{\underline{\lambda}}$.

Decomposing $V_{P,\boldsymbol{Q}}$ 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 $V_{P,\boldsymbol{Q}}$ 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 $S^{\underline{\lambda}}$.
- Link to literature: $V_{P,\boldsymbol{Q}} \cong M^{\underline{\gamma}}$, for known 'permutation' module $M^{\underline{\gamma}}$.
  - Multiplicities of $S^{\underline{\lambda}}$ in $M^{\underline{\gamma}}$ 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.

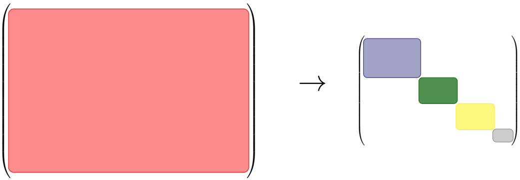
Computational results – full hierarchy

- $\sum m_i^2$ 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:

d	k	t	$(dk)^{\lfloor t \rfloor}$	#vars	#linear constraints	block sizes		result
						sum	max	
2	4	4.5	4096	7	8	472	85	**infeasible**
3	5	4.5	50625	7	2	1259	142	**infeasible**
4	6	5	7962624	43	2	6374	389	**infeasible**
5	7	5	52521875	43	2	6732	389	**infeasible**
6	8	5	254803968	43	2	6820	389	**infeasible**
7	9	5	992436543	43	2	6830	389	**infeasible**
8	10	5	3276800000	43	2	6831	389	**infeasible**
6	4	5.5	7962624	54	3	8049	577	feasible
6	7	4.5	3111696	7	0	1627	146	feasible
6	7	5	130691232	43	2	6749	389	feasible
6	7	5.5	130691232	75	3	18538	1107	feasible

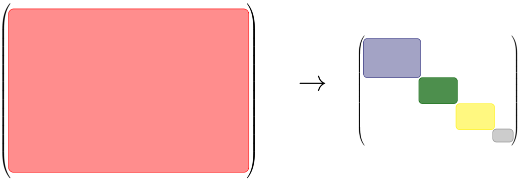
Future work

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



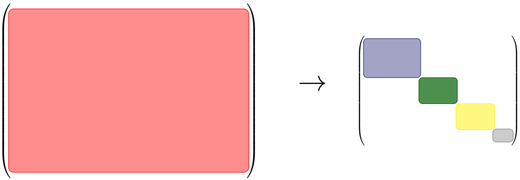
Future work

- 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.



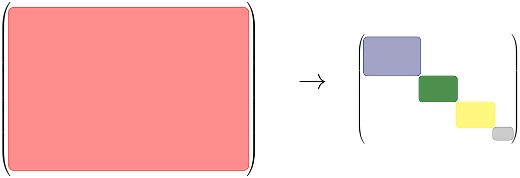
Future work

- 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 $t = 5$?



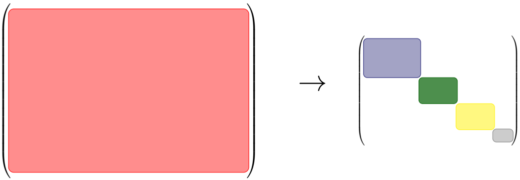
Future work

- 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)



Computational results – S_k-part

- 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.

d	k	t	$k^{\lfloor t \rfloor}$	#vars	#linear constraints	block sizes sum	block sizes max	result
2	4	4.5	256	5	0	48	24	**infeasible**
3	5	4.5	625	5	0	95	32	**infeasible**
4	6	5	7776	17	2	364	70	**infeasible**
5	7	6.5	117649	467	74	3288	640	**infeasible**
6	4	7.5	16384	20	5	586	293	feasible
6	7	6.5	117649	467	74	3288	640	feasible