Simons workshop
Lattices Geometry, Algorithms and Hardness

Berkeley, February 21st 2020

A simplex-type Voronoi algorithm based on short vector computations of copositive quadratic forms

Achill Schürmann
(Universität Rostock)

based on work with Mathieu Dutour Sikirić and Frank Vallentin

Perfect Forms (for $Q \in \mathcal{S}^n_{>0}$ positive definite)

- $\min(Q) \;=\; \min\limits_{x \in \mathbb{Z}^n \setminus \{0\}} Q[x]$ is the arithmetical minimum

- Q perfect $\;\Leftrightarrow\;$ Q is uniquely determined by $\min(Q)$ and $\mathrm{Min}Q \;=\; \{\, x \in \mathbb{Z}^n \;:\; Q[x] = \min(Q) \,\}$

- $V(Q) = \mathrm{cone}\{xx^t \;:\; x \in \mathrm{Min}Q\}$ is Voronoi cone of Q

  (Voronoi cones are full dimensional if and only if Q is perfect!)

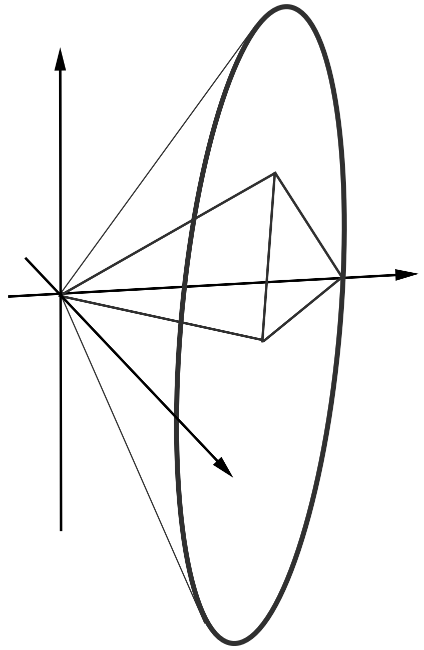
THM: Voronoi cones give a polyhedral tessellation of $\mathcal{S}^n_{>0}$ and there are only finitely many up to $\mathrm{GL}_n(\mathbb{Z})$-equivalence.

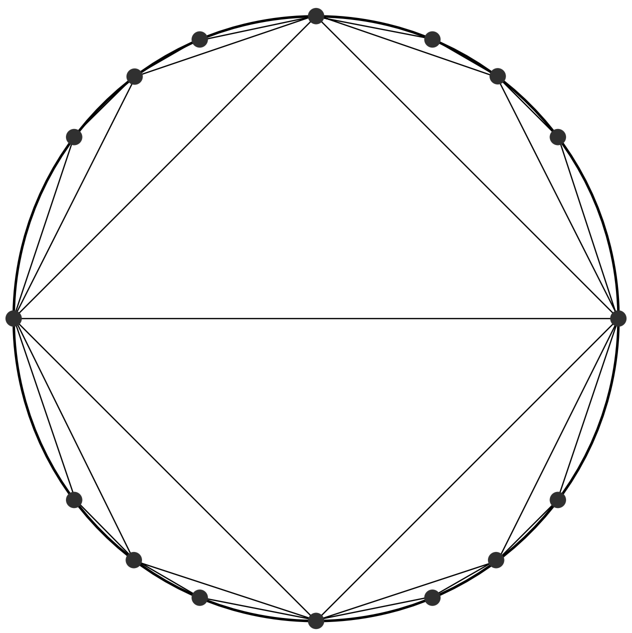
Voronoi's Reduction Theory

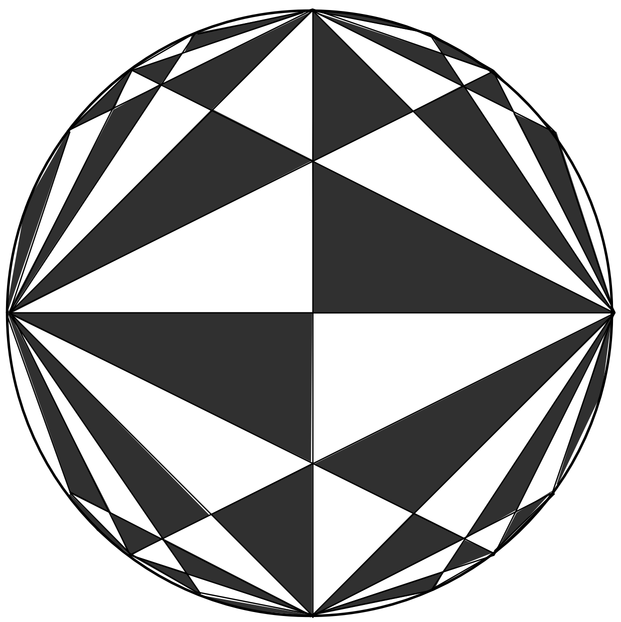
Georgy Voronoi
(1868 – 1908)

$\mathrm{GL}_n(\mathbb{Z})$ acts on $\mathcal{S}^n_{>0}$ by $Q \mapsto U^t Q U$

Task of a reduction theory is to provide a fundamental domain







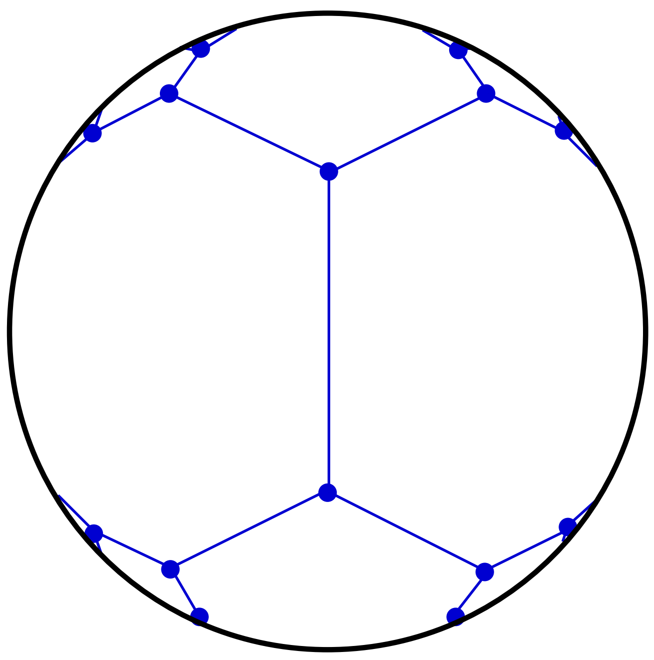
Voronoi's algorithm gives a recipe for the construction of a complete list of such polyhedral cones up to $\mathrm{GL}_n(\mathbb{Z})$-equivalence

Ryshkov Polyhedron

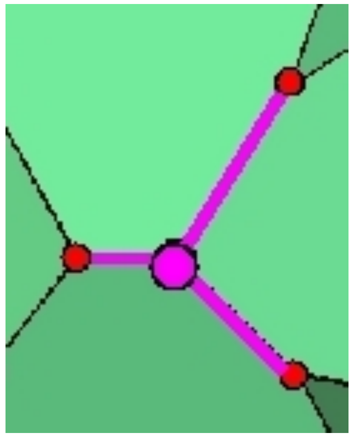
The set of all positive definite quadratic forms / matrices with arithmetical minimum at least 1 is called Ryshkov polyhedron

$$\mathcal{R} \;=\; \left\{\, Q \in \mathcal{S}^n_{>0} \;:\; Q[x] \geq 1 \text{ for all } x \in \mathbb{Z}^n \setminus \{0\} \,\right\}$$

- $\mathcal{R}$ is a locally finite polyhedron
- Vertices of $\mathcal{R}$ are perfect



Voronoi's Algorithm



Start with a perfect form Q

1. SVP: Compute $\operatorname{Min} Q$ and describing inequalities of the polyhedral cone

$$\mathcal{P}(Q) \;=\; \{\; Q' \in \mathcal{S}^n \;:\; Q'[x] \geq 1 \text{ for all } x \in \operatorname{Min} Q \;\}$$

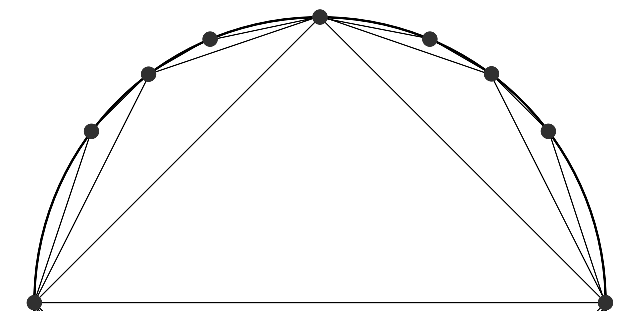
2. PolyRepConv: Enumerate extreme rays $R_1, \ldots, R_k$ of $\mathcal{P}(Q)$
3. SVPs: Determine contiguous perfect forms $Q_i = Q + \alpha R_i$, $i = 1, \ldots, k$
4. ISOMs: Test if Q_i is arithmetically equivalent to a known form
5. Repeat steps 1.–4. for new perfect forms

(graph traversal search on edge graph of Ryshkov polyhedron)

Generalization

… and application!

IDEA: Generalize Voronoi's theory to other convex cones and their duals (Opgenorth, 2001)



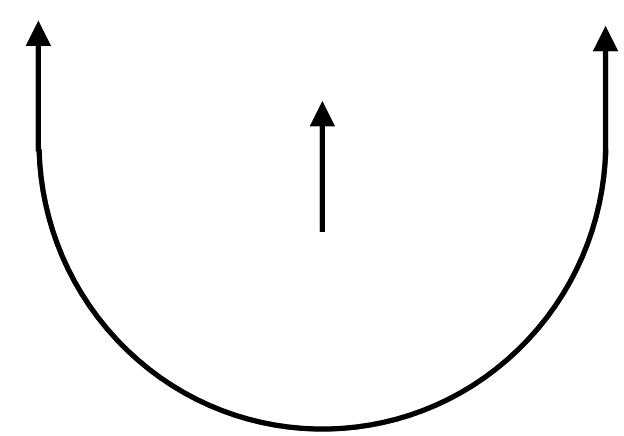
In particular to the completely positive cone

$$\mathcal{CP}_n = \mathrm{cone}\{xx^{\mathsf{T}} : x \in \mathbb{R}^n_{\geq 0}\}$$ and its dual, the copositive cone

$$\mathcal{COP}_n = (\mathcal{CP}_n)^* = \{B \in \mathcal{S}^n : \langle A, B\rangle \geq 0 \text{ for all } A \in \mathcal{CP}_n\}$$

$$= \{B \in \mathcal{S}^n : B[x] \geq 0 \text{ for all } x \in \mathbb{R}^n_{\geq 0}\}$$

$$\mathcal{CP}_n \quad \subset \quad \mathcal{S}^n_{>0} \quad \subset \quad \mathcal{COP}_n$$



$\langle A, B\rangle = \mathrm{Trace}(A \cdot B)$ denotes the standard inner product on $\mathcal{S}^n$

Application: Copositive Optimization

- Copositive optimization problems are convex conic problems

$$\min \langle C, Q \rangle \quad \text{such that } \langle Q, A_i \rangle = b_i, \; i = 1, \ldots, m$$

$$\text{and } Q \in \text{CONE}$$

$\text{CONE} = \mathbb{R}^n_{\geq 0}$

Linear Programming (LP)

$\text{CONE} = \mathcal{S}^n_{\geq 0}$

Semidefinite Programming (SDP)

$\text{CONE} = \mathcal{CP}_n$ or $\mathcal{COP}_n$

Copositive Programming (CP)

Task: Certify or disprove $Q \in \tilde{\mathcal{CP}}_n = \text{cone}\left\{ xx^\top : x \in \mathbb{Q}^n_{\geq 0} \right\}$

(due to duality theory we can give certificates for solutions of convex conic problems)

Copositive minimum (COP-SVP)

DEF: $\min_{\mathcal{COP}} Q = \min_{x \in \mathbb{Z}^n_{\geq 0} \setminus \{0\}} Q[x]$ is the copositive minimum

Difficult to compute!?

THM: (Bundfuss and Dür, 2008)

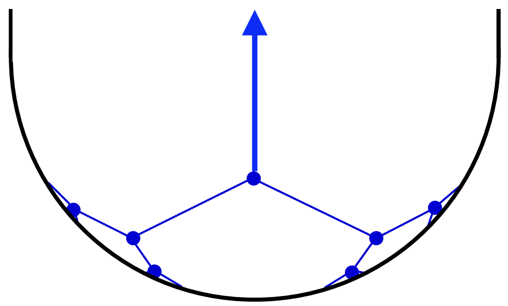
For $Q \in \operatorname{int} \mathcal{COP}_n$ we can construct a family of simplices Δ^k in the standard simplex $\Delta = \left\{ x \in \mathbb{R}^n_{\geq 0} : x_1 + \ldots x_n = 1 \right\}$ such that each Δ^k has vertices $v_1, \ldots v_n$ with $v_i^\top Q v_j > 0$

A first naive algorithm:

"Fincke-Pohst strategy" to compute $\min_{\mathcal{COP}} Q$ in each cone Δ^k

Generalized Ryshkov polyhedron

The set of all copositive quadratic forms / matrices with copositive minimum at least 1 is called **Ryshkov polyhedron**



$$\mathcal{R} \;=\; \left\{ Q \in \mathcal{COP}_n \;:\; Q[x] \geq 1 \text{ for all } x \in \mathbb{Z}^n_{\geq 0} \setminus \{0\} \right\}$$

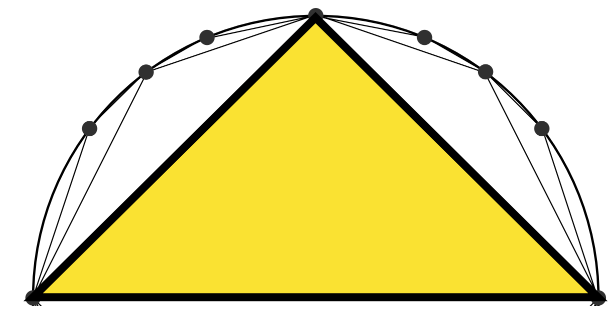
DEF: $Q \in \operatorname{int} \mathcal{COP}_n$ is called $\mathcal{COP}$-perfect if and only if

Q is uniquely determined by $\min_{\mathcal{COP}} Q$ and

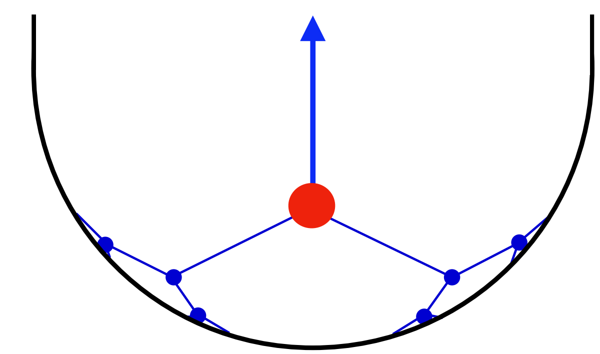
$$\mathrm{Min}_{\mathcal{COP}} Q \;=\; \left\{ x \in \mathbb{Z}^n_{\geq 0} \;:\; Q[x] = \min_{\mathcal{COP}} Q \right\}$$

- $\mathcal{R}$ is a locally finite polyhedron (with dead-ends / rays)
- Vertices of $\mathcal{R}$ are $\mathcal{COP}$-perfect

A copositive starting point



THM: $$\begin{pmatrix} 2 & -1 & 0 & \dots & 0 \\ -1 & 2 & \ddots & \ddots & \vdots \\ 0 & \ddots & \ddots & \ddots & 0 \\ \vdots & \ddots & \ddots & 2 & -1 \\ 0 & \dots & 0 & -1 & 2 \end{pmatrix}$$ is $\mathcal{COP}$-perfect



Proof. Matrix Q_{A_n} is positive definite since

$$Q_{\mathsf{A}_n}[x] = x_1^2 + \sum_{i=1}^{n-1} (x_i - x_{i+1})^2 + x_n^2 \quad \text{for } x \in \mathbb{R}.$$

In particular it lies in the interior of the copositive cone. Furthermore,

$$\min_{\mathcal{COP}} Q_{\mathsf{A}_n} = 2 \quad \text{with} \quad \operatorname{Min}_{\mathcal{COP}} Q_{\mathsf{A}_n} = \left\{ \sum_{i=j}^{k} e_j : 1 \le j \le k \le n \right\}$$

Voronoi-type simplex algorithm

Input: $A \in \mathcal{S}^n$

Obtain an initial $\mathcal{COP}$-perfect matrix B_P

1. $\texttt{if}$ $\langle B_P, A\rangle < 0$ $\texttt{then}$ $\texttt{output}$ $A \notin \mathcal{CP}_n$ (with witness B_P)
2. LP: $\texttt{if}$ $A \in \text{cone}\left\{xx^\top : x \in \text{Min}_{\mathcal{COP}} B_P\right\}$ $\texttt{then}$ $\texttt{output}$ $A \in \tilde{\mathcal{CP}}_n$
3. COP-SVP: Compute $\text{Min}_{\mathcal{COP}} B_P$ and the polyhedral cone

$$\mathcal{P}(B_P) \;=\; \{\, B \in \mathcal{S}^n \;:\; B[x] \geq 1 \text{ for all } x \in \text{Min}_{\mathcal{COP}} B_P \,\}$$

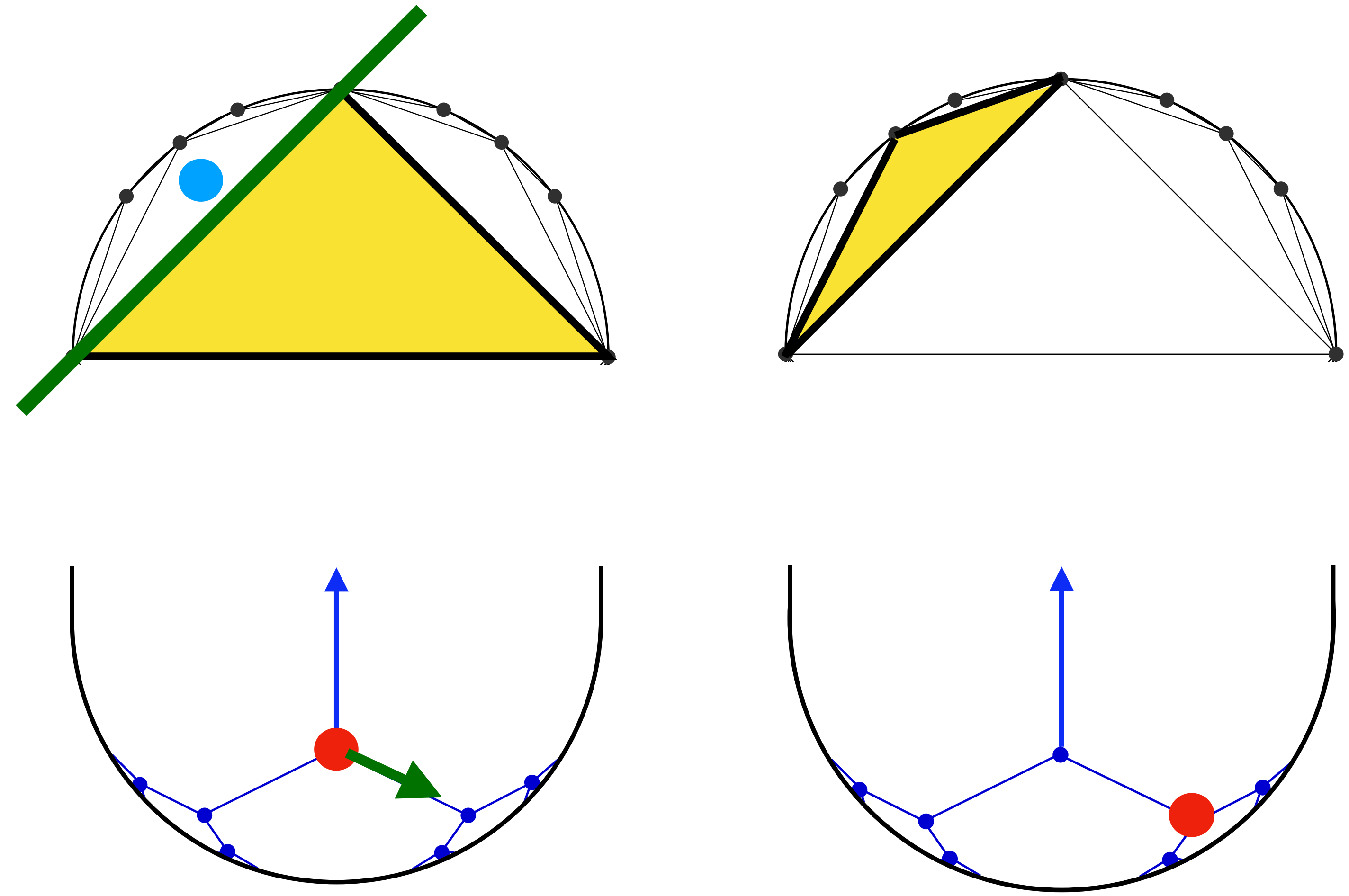
4. PolyRepConv: Determine a generator R of an extreme ray of $\mathcal{P}(B_P)$ with $\langle A, R\rangle < 0$. (flexible "pivot-rule")
5. SimplexDiv: $\texttt{if}$ $R \in \mathcal{COP}_n$ $\texttt{then}$ $\texttt{output}$ $A \notin \mathcal{CP}_n$ (with witness R)
6. COP-SVPs: Determine the contiguous $\mathcal{COP}$-perfect matrix

$$B_N := B_P + \lambda R \text{ with } \lambda > 0 \text{ and } \min_{\mathcal{COP}} B_N = 1$$

7. Set $B_P := B_N$ and $\texttt{goto}$ 1.

Interior cases

(algorithm terminates)



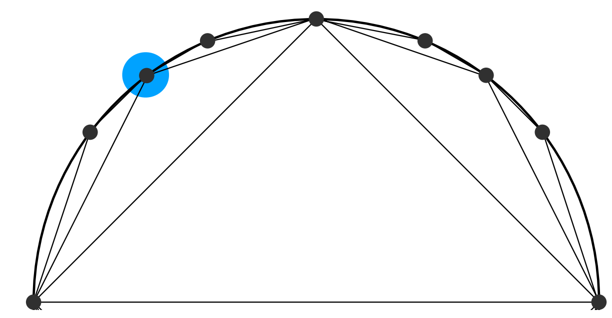
EX: $A = \begin{pmatrix} 6 & 3 \\ 3 & 2 \end{pmatrix}$

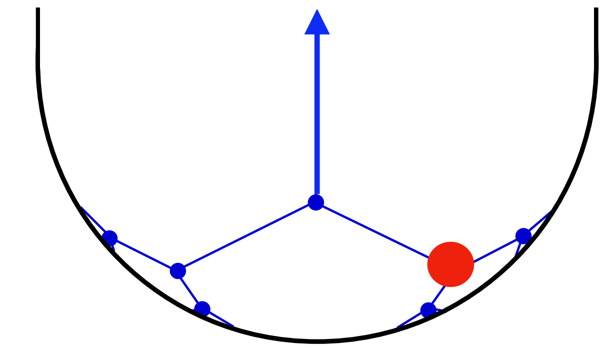
Starting with Q_{A_2} one iteration of the algorithm finds the $\mathcal{COP}$-perfect matrix $B_P = \begin{pmatrix} 1 & -3/2 \\ -3/2 & 3 \end{pmatrix}$ and

$$A = \begin{pmatrix} 1 \\ 0 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix}^\top + \begin{pmatrix} 1 \\ 1 \end{pmatrix}\begin{pmatrix} 1 \\ 1 \end{pmatrix}^\top + \begin{pmatrix} 2 \\ 1 \end{pmatrix}\begin{pmatrix} 2 \\ 1 \end{pmatrix}^\top$$

Boundary cases from $\mathcal{C}\tilde{\mathcal{P}}_n$

(algorithm terminates with a suitable pivot-rule)





EX: $$\begin{pmatrix} 8 & 5 & 1 & 1 & 5 \\ 5 & 8 & 5 & 1 & 1 \\ 1 & 5 & 8 & 5 & 1 \\ 1 & 1 & 5 & 8 & 5 \\ 5 & 1 & 1 & 5 & 8 \end{pmatrix}$$ from Groetzner, Dür (2018)

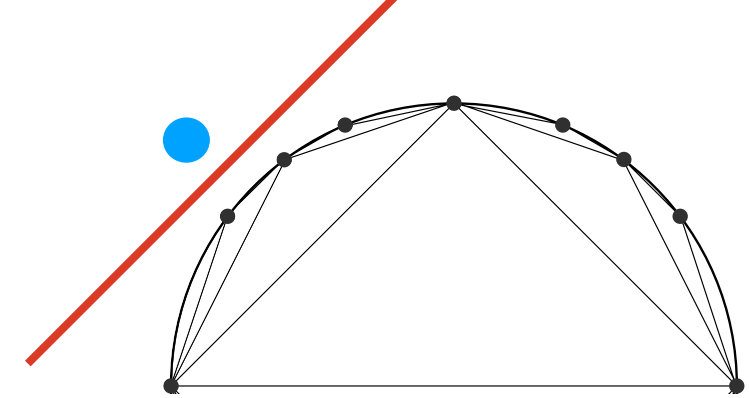
Starting with Q_{A_5}, our algorithm finds a cp-factorization after 5 iterations

$$\begin{aligned} v_1 &= (0,0,0,1,1) & v_6 &= (1,0,0,0,1) \\ v_2 &= (0,0,1,1,0) & v_7 &= (1,0,0,1,2) \\ v_3 &= (0,0,1,2,1) & v_8 &= (1,1,0,0,0) \\ v_4 &= (0,1,1,0,0) & v_9 &= (1,2,1,0,0) \\ v_5 &= (0,1,2,1,0) & v_{10} &= (2,1,0,0,1) \end{aligned}$$

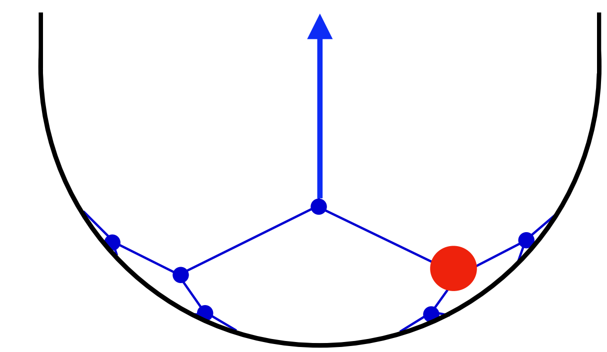
giving a certificate for the matrix to be completely positive

Exterior cases

(algorithm conjectured to terminate)



EX: $\begin{pmatrix} 1 & 1 & 0 & 0 & 1 \\ 1 & 2 & 1 & 0 & 0 \\ 0 & 1 & 2 & 1 & 0 \\ 0 & 0 & 1 & 2 & 1 \\ 1 & 0 & 0 & 1 & 6 \end{pmatrix}$ from Nie (2014)



Starting with Q_{A_5}, after 18 iterations our algorithm finds the $\mathcal{COP}$-perfect

$$\begin{pmatrix} 363/5 & -2126/35 & 2879/70 & 608/21 & -4519/210 \\ -2126/35 & 1787/35 & -347/10 & 1025/42 & 253/14 \\ 2879/70 & -347/10 & 829/35 & -1748/105 & 371/30 \\ 608/21 & 1025/42 & -1748/105 & 1237/105 & -601/70 \\ -4519/210 & 253/14 & 371/30 & -601/70 & 671/105 \end{pmatrix}$$

giving a certificate for the matrix not to be completely positive

Open Questions / TODOs

- Find suitable / good pivot rules for boundary cases
- Prove termination of algorithm for exterior cases
- Improve computations in practice
- … in particular: find a better algorithm to compute

$\min_{\mathcal{COP}}$ and the set of its representatives $\mathrm{Min}_{\mathcal{COP}}$

(COP-SVPs)

References

- Achill Schürmann, *Computational Geometry of Positive Definite Quadratic Forms,* University Lecture Series, AMS, Providence, RI, 2009.

- Mathieu Dutour Sikirić, Achill Schürmann and Frank Vallentin, Rational factorizations of completely positive matrices, *Linear Algebra and its Applications*, 523 (2017), 46–51.

- Mathieu Dutour Sikirić, Achill Schürmann and Frank Vallentin, A simplex algorithm for rational cp-factorization, Math. Prog. A, 2020, online first

THANKS !