ICERM Conference on
Computational Challenges in the Theory of Lattices

Providence, April 2018

Variations and Applications of Voronoi's algorithm

Achill Schürmann
(Universität Rostock)

(based on work with Mathieu Dutour Sikiric and Frank Vallentin)

PRELUDE
Voronoi's Algorithm
- classically -

Lattices and Quadratic Forms

Lattices and Quadratic Forms

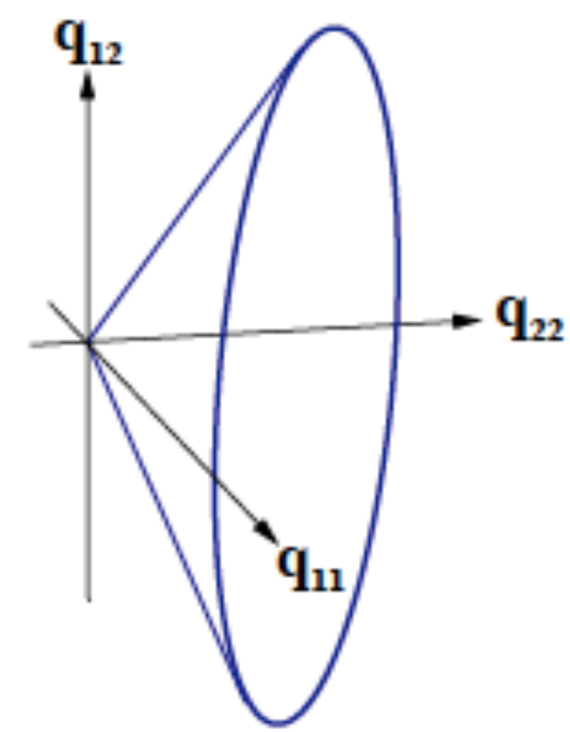
- Every lattice basis $A \in \mathsf{GL}_n(\mathbb{R})$ of a lattice $L = A\mathbb{Z}^n$ defines a positive definite symmetric (Gram) matrix $Q = A^t A$.

$$\mathcal{S}^n_{>0} := \{ \, Q \in \mathbb{R}^{n \times n} \; : \; Q \text{ symmetric and positive definite } \}$$

Lattices and Quadratic Forms

- Every lattice basis $A \in \mathrm{GL}_n(\mathbb{R})$ of a lattice $L = A\mathbb{Z}^n$ defines a positive definite symmetric (Gram) matrix $Q = A^t A$.

$$\mathcal{S}^n_{>0} \;:=\; \{\, Q \in \mathbb{R}^{n\times n} \;:\; Q \text{ symmetric and positive definite } \}$$



- $Q \in \mathcal{S}^n_{>0}$ defines a pos. def. quadratic form (PQF)

$$Q[x] \;=\; x^t Q x \;=\; \sum_{i=1}^{n} q_{ii} x_i^2 \;+\; 2 \sum_{i<j} q_{ij} x_i x_j$$

Different bases of a lattice yield integrally equivalent PQFs:

$$L = A\mathbb{Z}^n \quad \Leftrightarrow \quad L = (AU)\mathbb{Z}^n \text{ for } U \in \mathrm{GL}_n(\mathbb{Z})$$

$$A^t A = Q \sim Q' = U^t Q U = (AU)^t (AU)$$

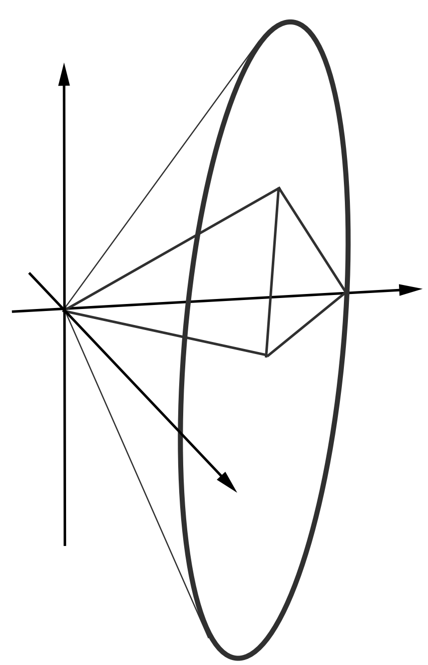
Reduction Theory

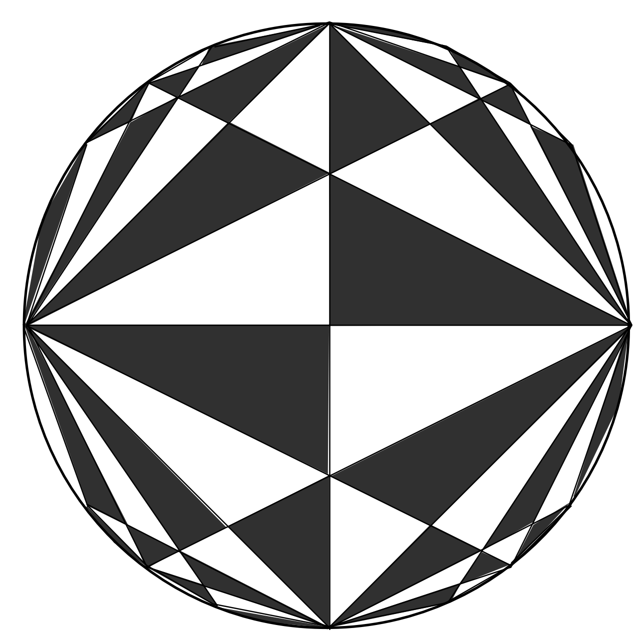
for positive definite quadratic forms

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

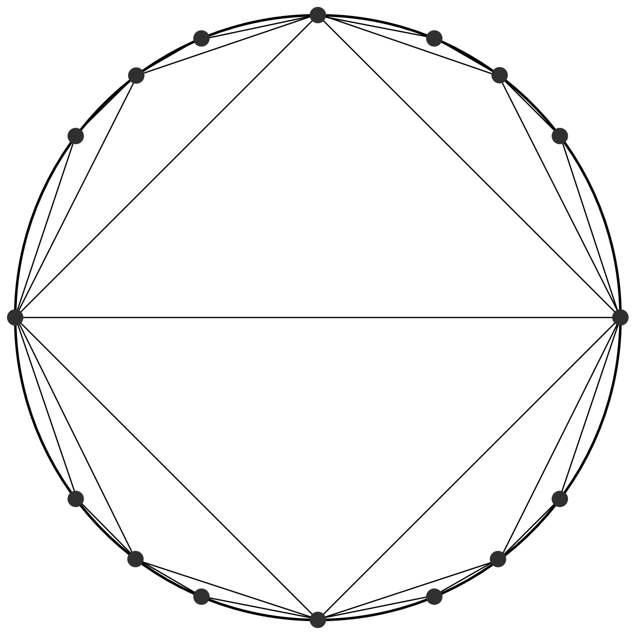
Task of a reduction theory is to provide a fundamental domain

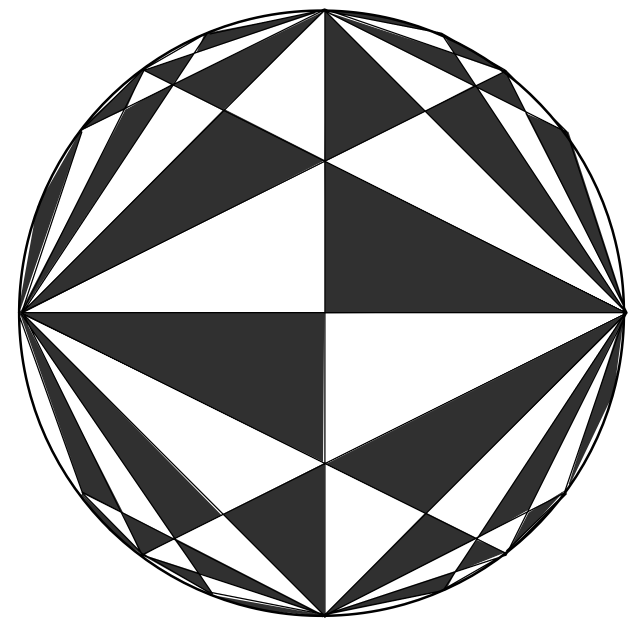
Classical reductions were obtained by Lagrange, Gauß, Korkin and Zolotareff, Minkowski and others… All the same for $n = 2$:





Voronoi's reduction idea

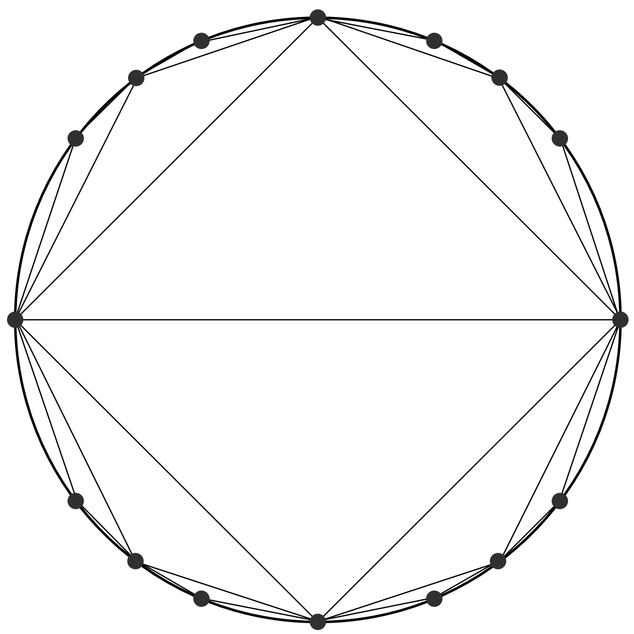


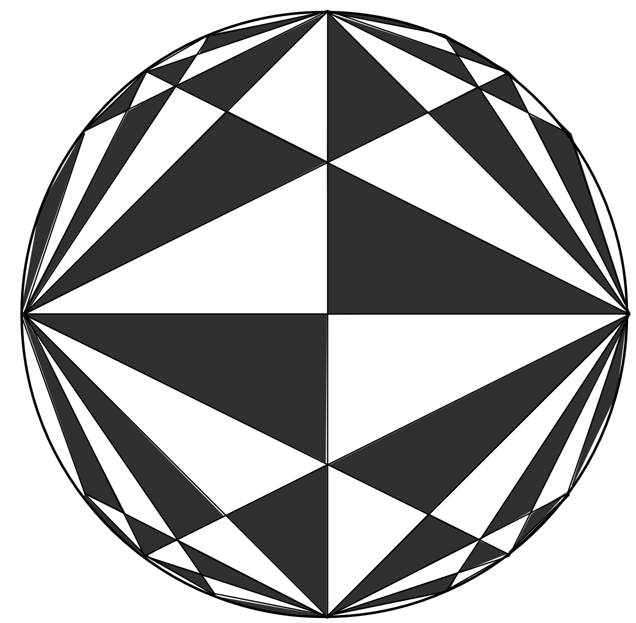


Georgy Voronoi
(1868 – 1908)

Observation: The fundamental domain can be obtained from polyhedral cones that are spanned by rank-1 forms only

Voronoi's reduction idea





Georgy Voronoi
(1868 – 1908)

Observation: The fundamental domain can be obtained from polyhedral cones that are spanned by rank-1 forms only

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

Perfect Forms

Perfect Forms

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

Perfect Forms

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

$Q \in \mathcal{S}^n_{>0}$ perfect $\Leftrightarrow$ Q is uniquely determined by $\min(Q)$ and

$$\mathrm{Min}Q \;=\; \{\, x \in \mathbb{Z}^n \;:\; Q[x] = \min(Q) \,\}$$

Perfect Forms

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

$Q \in \mathcal{S}^n_{>0}$ perfect $\;\Leftrightarrow\;$ Q is uniquely determined by $\min(Q)$ and

$$\mathrm{Min}Q \;=\; \{\, x \in \mathbb{Z}^n \;:\; Q[x] = \min(Q) \,\}$$

For $Q \in \mathcal{S}^n_{>0}$, its Voronoi cone is $\mathcal{V}(Q) = \mathrm{cone}\{xx^t \;:\; x \in \mathrm{Min}Q\}$

Perfect Forms

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

$Q \in \mathcal{S}^n_{>0}$ perfect $\;\Leftrightarrow\;$ Q is uniquely determined by $\min(Q)$ and

$$\mathrm{Min}Q \;=\; \{\, x \in \mathbb{Z}^n \;:\; Q[x] = \min(Q) \,\}$$

For $Q \in \mathcal{S}^n_{>0}$, its Voronoi cone is $\mathcal{V}(Q) = \mathrm{cone}\{xx^t \;:\; x \in \mathrm{Min}Q\}$

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.

Perfect Forms

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

$Q \in \mathcal{S}^n_{>0}$ perfect $\;\Leftrightarrow\;$ Q is uniquely determined by $\min(Q)$ and

$$\mathrm{Min}Q \;=\; \{\, x \in \mathbb{Z}^n \;:\; Q[x] = \min(Q) \,\}$$

For $Q \in \mathcal{S}^n_{>0}$, its Voronoi cone is $\mathcal{V}(Q) = \mathrm{cone}\{xx^t \;:\; x \in \mathrm{Min}Q\}$

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

Ryshkov Polyhedron

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

Ryshkov Polyhedron

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

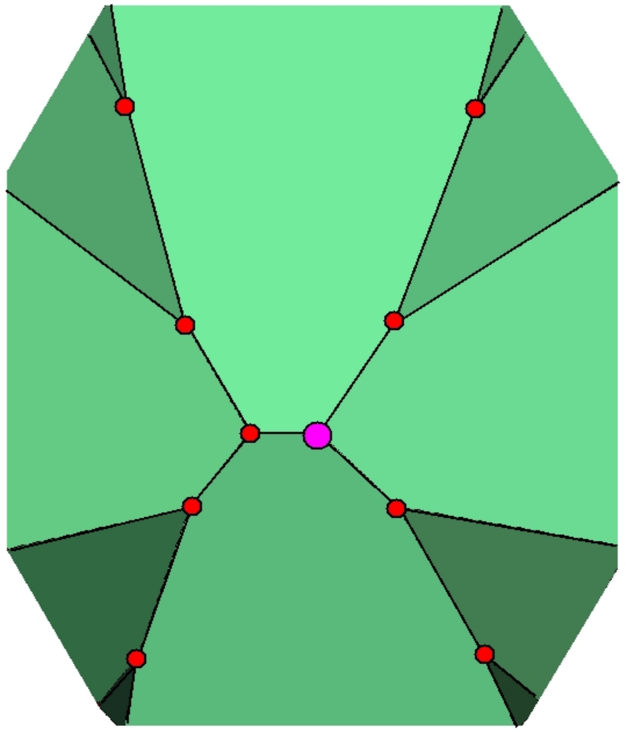
$$\mathcal{R} = \left\{ Q \in \mathcal{S}^n_{>0} \; : \; Q[x] \geq 1 \text{ for all } x \in \mathbb{Z}^n \setminus \{0\} \right\}$$

Ryshkov Polyhedron

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

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

- $\mathcal{R}$ is a locally finite polyhedron

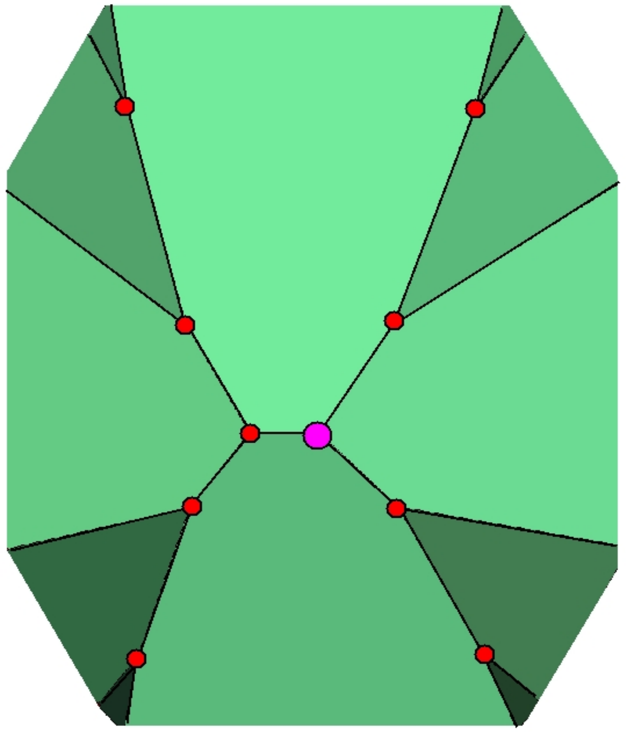


Ryshkov Polyhedron

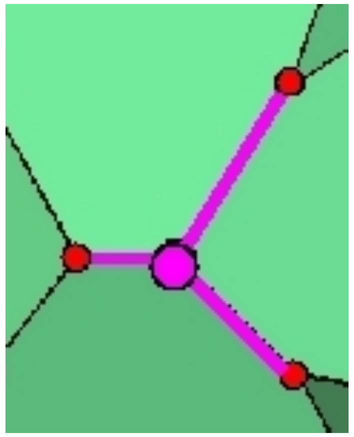
The set of all positive definite quadratic forms / matrices with arithmetical minimum at least 1 is called Ryshkov polyhedron

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

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



Voronoi's Algorithm



Start with a perfect form Q

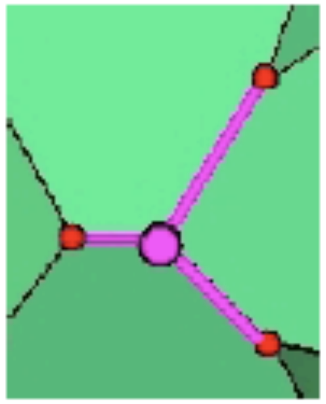
1. SVP: Compute $\operatorname{Min} Q$ and describing inequalities of the polyhedral cone

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

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

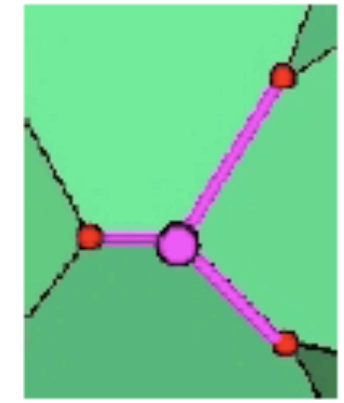
Computational Results

- **BOTTLENECK**: Computing vertices of polyhedra!
- **Martinet (2003)**: "The existence of E_8 [...] makes hopeless any attempt [...] in dimension 8."



Computational Results

- **BOTTLENECK**: Computing vertices of polyhedra!
- **Martinet (2003)**: “The existence of E_8 [...] makes hopeless any attempt [...] in dimension 8.”



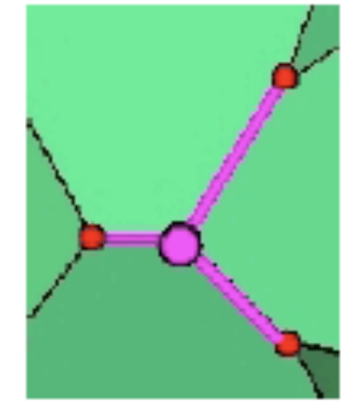
n	**# perfect forms**	**author(s)**
2	1	Lagrange, 1773
3	1	Gauß, 1840
4	2	Korkine & Zolotareff, 1877
5	3	Korkine & Zolotareff, 1877
6	7	Barnes, 1957
7	33	Jaquet-Chiffelle, 1991
8	10916	Dutour Sikirić, Sch. & Vallentin, 2007
9	> 500000	

Computer assisted proof with *Recursive Adj. Decomp. Method* (ADM) for vertex enumeration up to symmetries

(showing that the “E_8-polytope” has 25075566937584 vertices in 83092 orbits)

Computational Results

- **BOTTLENECK**: Computing vertices of polyhedra!
- **Martinet (2003)**: “The existence of E_8 [...] makes hopeless any attempt [...] in dimension 8.”



n	**# perfect forms**	**author(s)**
2	1	Lagrange, 1773
3	1	Gauß, 1840
4	2	Korkine & Zolotareff, 1877
5	3	Korkine & Zolotareff, 1877
6	7	Barnes, 1957
7	33	Jaquet-Chiffelle, 1991
8	10916	Dutour Sikirić, Sch. & Vallentin, 2007
9	$>$ 5000000	Wessel van Woerden, 2018 ?!

Computer assisted proof with *Recursive Adj. Decomp. Method* (ADM) for vertex enumeration up to symmetries

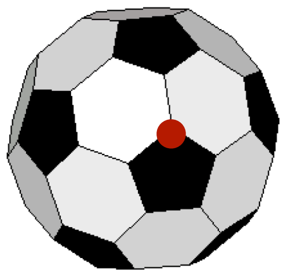
(showing that the “E_8-polytope” has 25075566937584 vertices in 83092 orbits)

Adjacency Decomposition Method

(for vertex enumeration)

Adjacency Decomposition Method

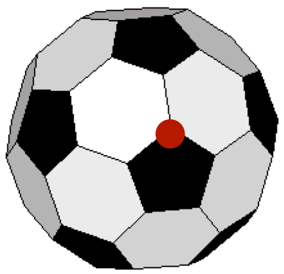
(for vertex enumeration)



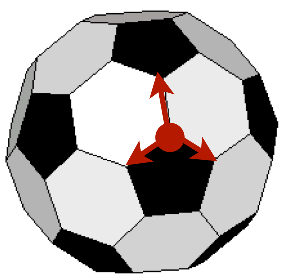
- Find initial orbit(s) / representing vertice(s)

Adjacency Decomposition Method

(for vertex enumeration)



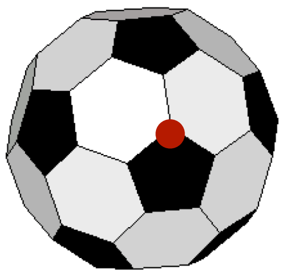
- Find initial orbit(s) / representing vertice(s)



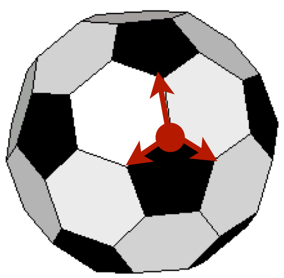
- For each new orbit representative
  - enumerate neighboring vertices

Adjacency Decomposition Method

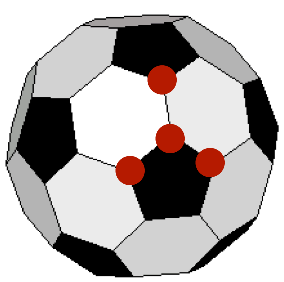
(for vertex enumeration)



- Find initial orbit(s) / representing vertice(s)



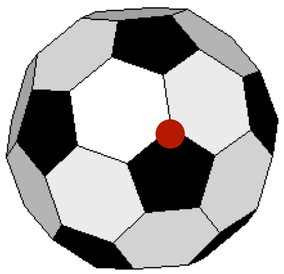
- For each new orbit representative
  - enumerate neighboring vertices



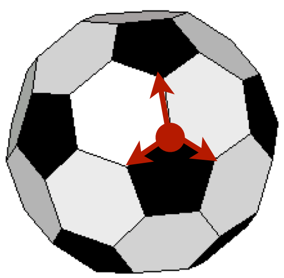
  - add as orbit representative if in a new orbit

Adjacency Decomposition Method

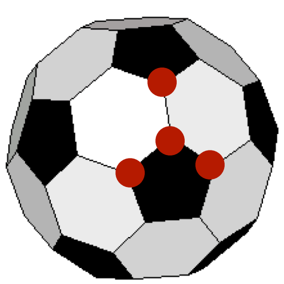
(for vertex enumeration)



- Find initial orbit(s) / representing vertice(s)



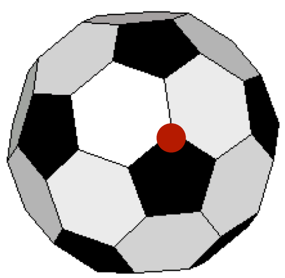
- For each new orbit representative
  - enumerate neighboring vertices (up to symmetry)
  - add as orbit representative if in a new orbit



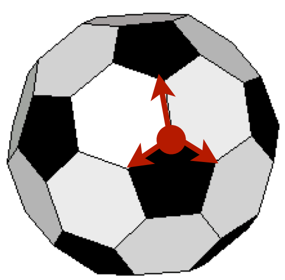
Representation conversion problem

Adjacency Decomposition Method

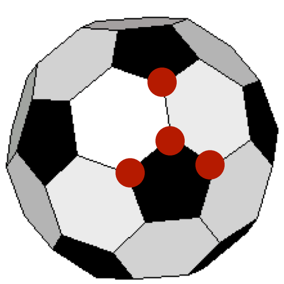
(for vertex enumeration)



- Find initial orbit(s) / representing vertice(s)



- For each new orbit representative
  - enumerate neighboring vertices (up to symmetry)
  - add as orbit representative if in a new orbit



Representation conversion problem

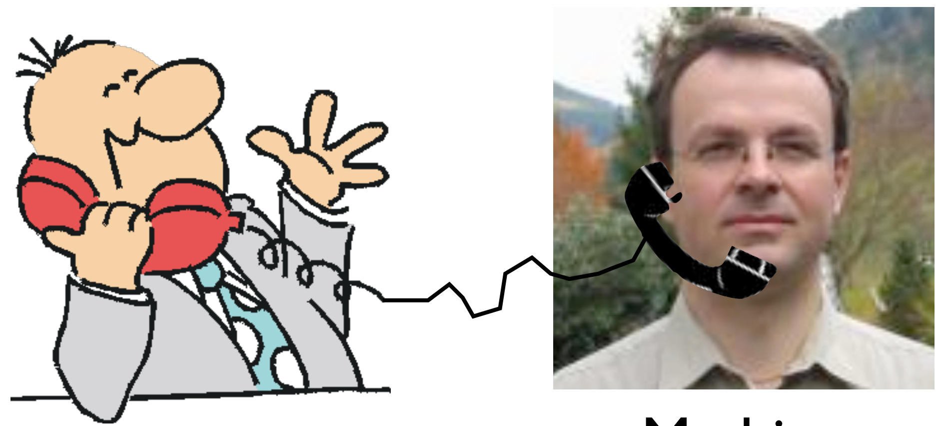
BOTTLENECK: Stabilizer and In-Orbit computations

=> Need of efficient data structures and algorithms for permutation groups: BSGS, (partition) backtracking

Representation Conversion
in practice

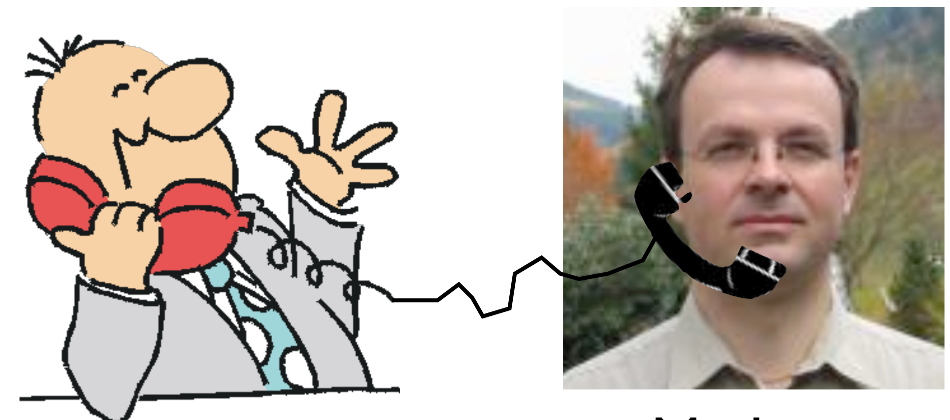
Representation Conversion
in practice

Best known Algorithm:



Mathieu

Representation Conversion
in practice



Mathieu

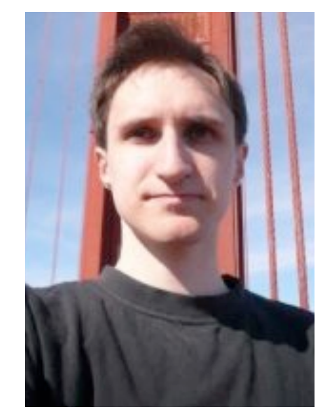
Best known Algorithm:

A C++-Tool SymPol

also available through polymake

- helps to compute linear automorphism groups
- converts polyhedral representations using

Recursive Decomposition Methods (Incidence/Adjacency)



Thomas Rehn
(Phd 2014)

http://www.geometrie.uni-rostock.de/software/

Applicaton: Lattice Sphere Packings

The lattice sphere packing problem can be phrased as:

Minimize $(\det Q)^{1/n}$ on

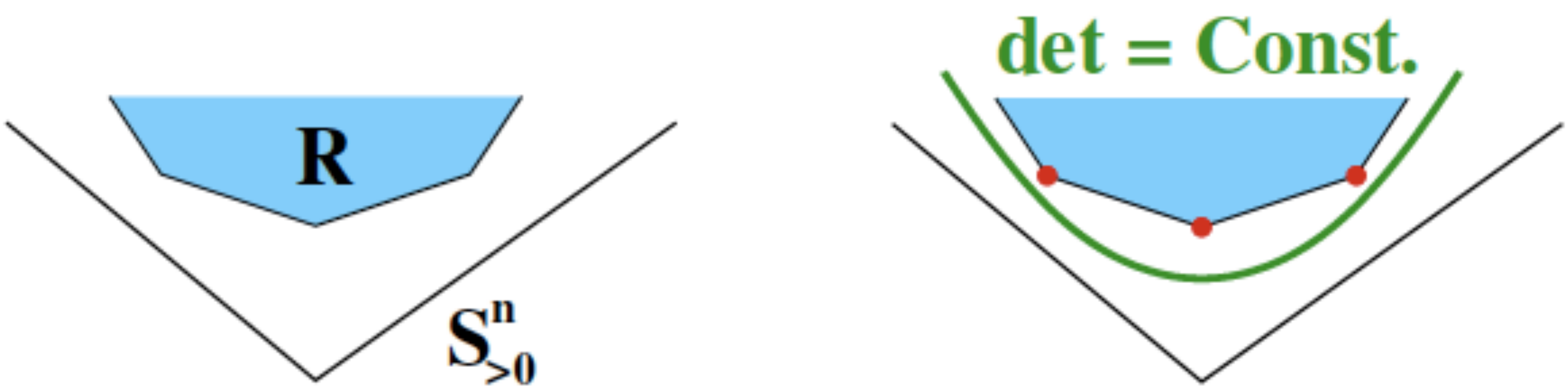
$$\mathcal{R} = \{ Q \in \mathcal{S}^n_{>0} : Q[x] \geq 1 \text{ for all } x \in \mathbb{Z}^n \setminus \{0\} \}$$

Applicaton: Lattice Sphere Packings

The lattice sphere packing problem can be phrased as:

Minimize $(\det Q)^{1/n}$ on

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



$\min_{Q \in \mathcal{R}} (\det Q)^{1/n}$ is attained at vertices of $\mathcal{R}$ (perfect forms)

Part II: Koecher's generalization and T-perfect forms

Koecher's generalization

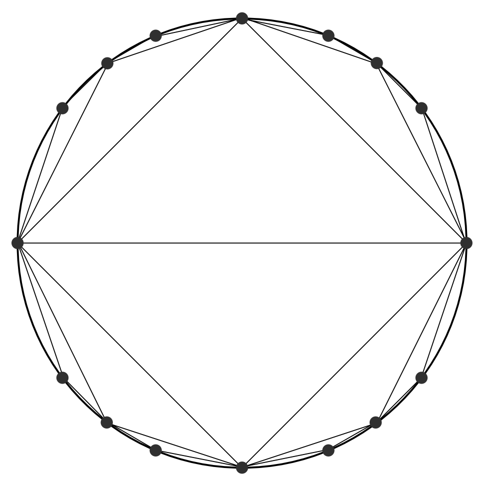
1960/61 Max Koecher generalized Voronoi's reduction theory and proofs to a setting with a self-dual cone C

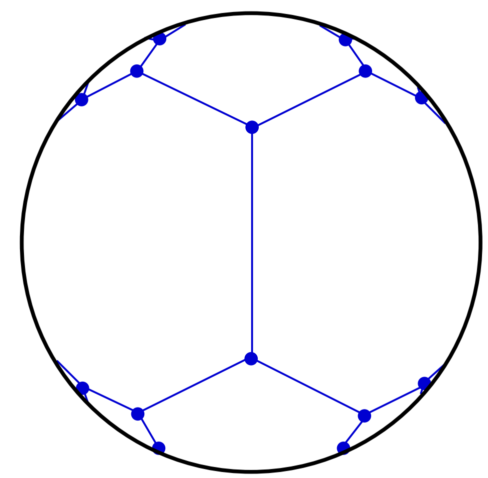
Max Koecher, 1924-1990

Koecher's generalization

Max Koecher, 1924-1990

1960/61 Max Koecher generalized Voronoi's reduction theory and proofs to a setting with a self-dual cone C



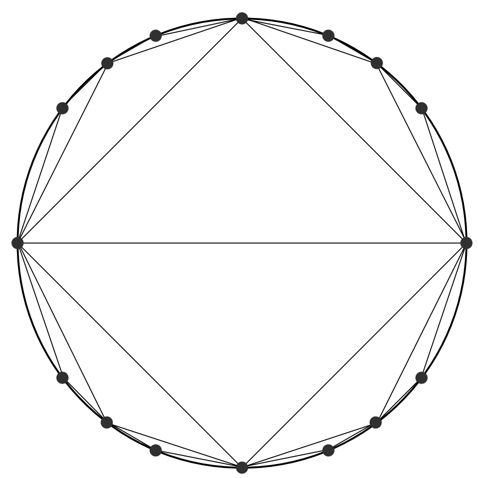


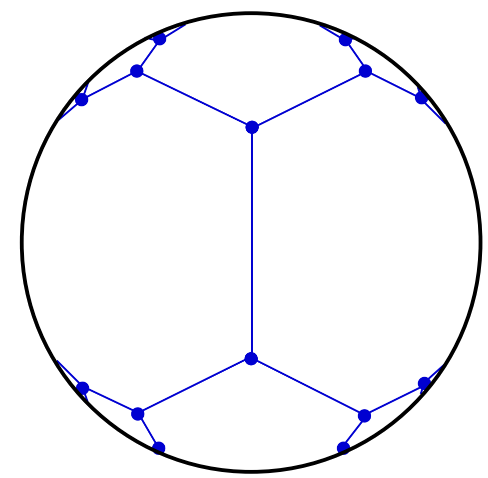
Under certain conditions, he shows that
C is covered by a tessellation of polyhedral Voronoi cones and "approximated from inside" by a Ryshkov polyhedron

Koecher's generalization

Max Koecher, 1924-1990

1960/61 Max Koecher generalized Voronoi's reduction theory and proofs to a setting with a self-dual cone C



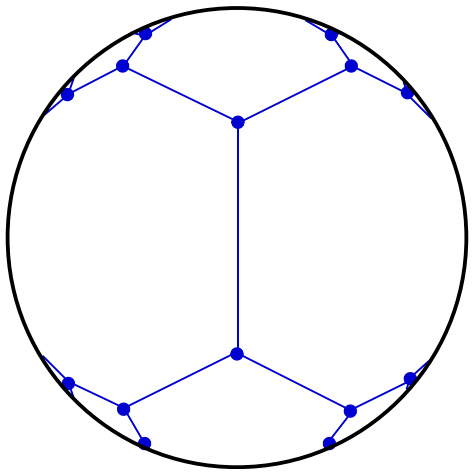


Under certain conditions, he shows that C is covered by a tessellation of polyhedral Voronoi cones and "approximated from inside" by a Ryshkov polyhedron

Can in particular be applied to obtain reduction domains for the action of $\mathrm{GL}_n(\mathcal{O}_K)$ on suitable quadratic spaces

Applications in Math

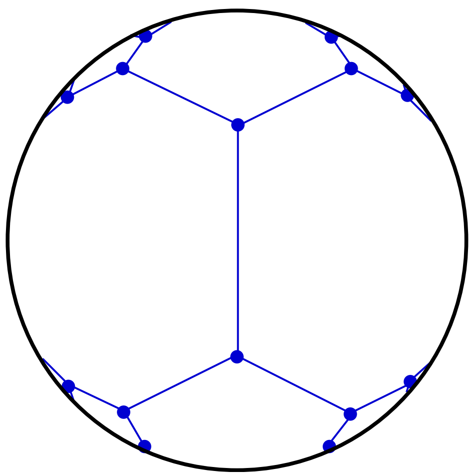
Ryshkov Polyhedron



$\mathrm{GL}_n(\mathcal{O}_K)$ symmetric

Applications in Math

Ryshkov Polyhedron



$\mathrm{GL}_n(\mathcal{O}_K)$ symmetric

Representation Conversion

Vertices / Perfect Forms:

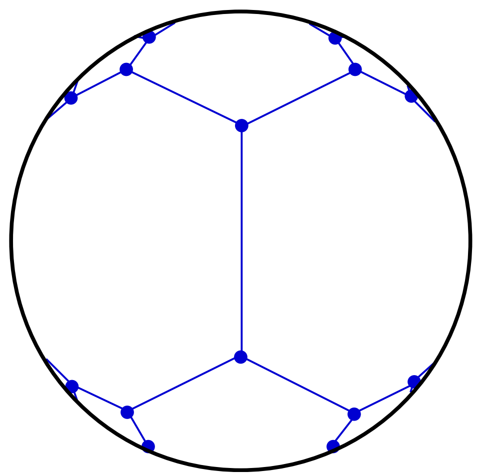
- Reduction theory
- Hermite constant

Polyhedral complex:

- Cohomology of $\mathrm{GL}_n(\mathcal{O}_K)$
- Hecke operators
- Compactifications of moduli spaces of Abelian varieties

Applications in Math

Ryshkov Polyhedron



$\mathrm{GL}_n(\mathcal{O}_K)$ symmetric

Representation Conversion

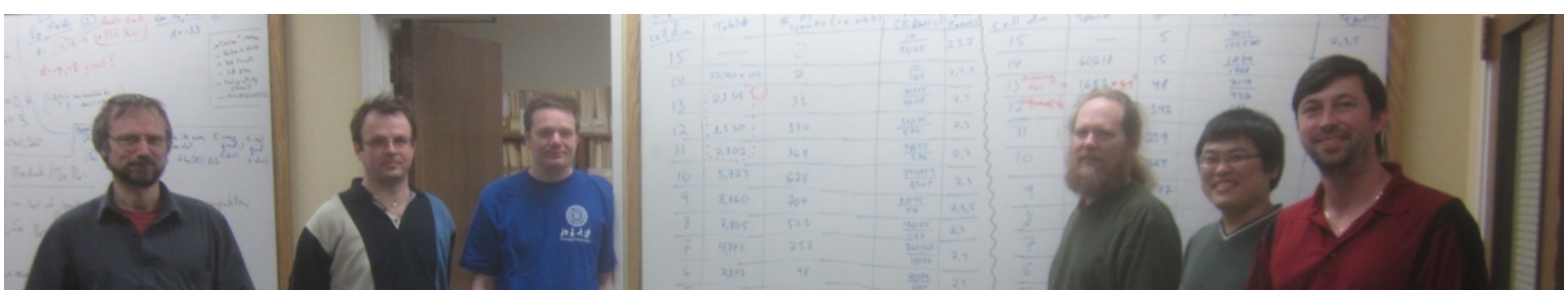
Vertices / Perfect Forms:

- Reduction theory
- Hermite constant

Polyhedral complex:

- Cohomology of $\mathrm{GL}_n(\mathcal{O}_K)$
- Hecke operators
- Compactifications of moduli spaces of Abelian varieties

See Mathieu's talk after the coffee break!



AIM Square group 2012: Gangl, Dutour Sikirić, Schürmann, Gunnells, Yasaki, Hanke

Embedding Koecher's theory

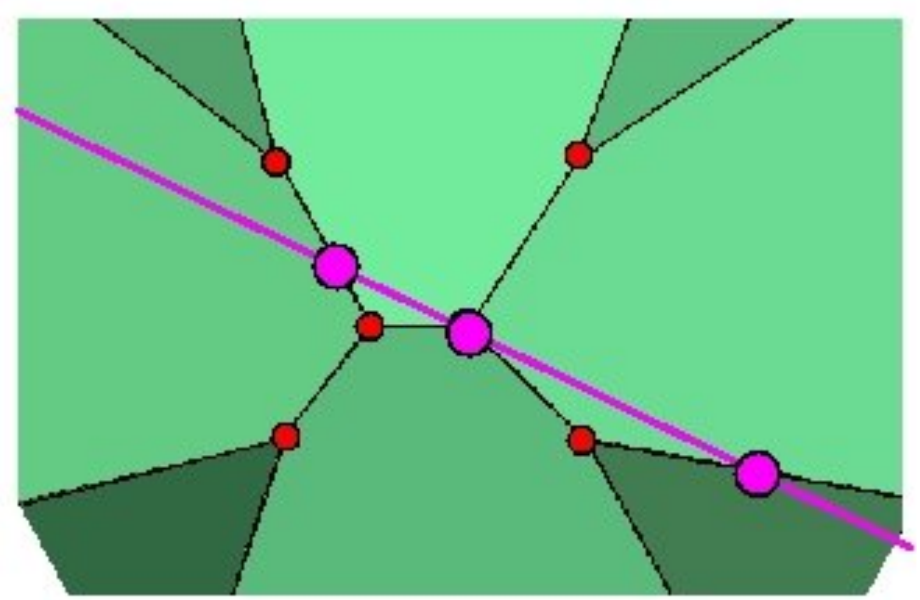
For practical computations: Koecher's theory can be embedded into a linear subspace T in some higher dimensional space of symmetric matrices

Embedding Koecher's theory

For practical computations: Koecher's theory can be embedded into a linear subspace *T* in some higher dimensional space of symmetric matrices

IDEA (Bergé, Martinet, Sigrist, 1992):

Intersect Ryshkov polyhedron $\mathcal{R}$ with a linear subspace $T \subset \mathcal{S}^n$

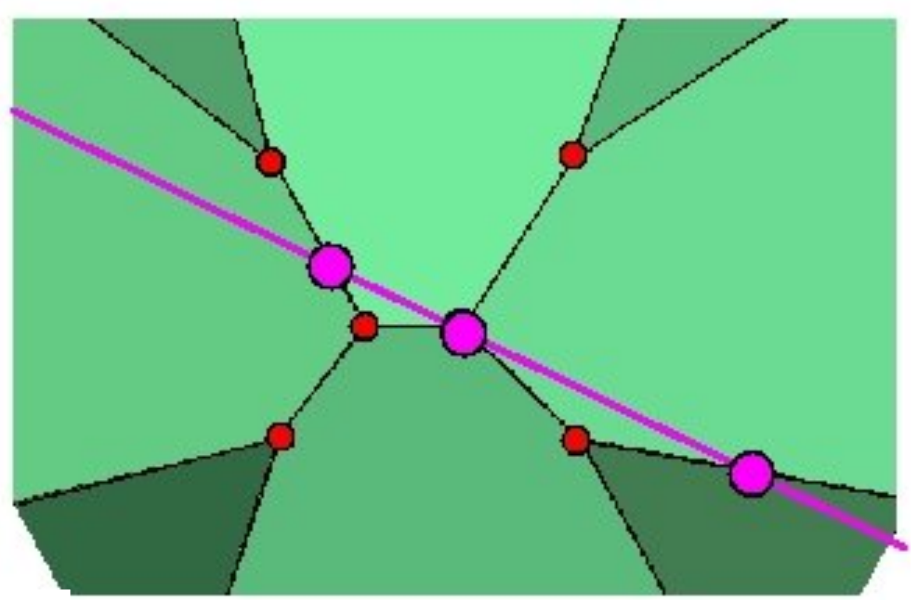


Embedding Koecher's theory

For practical computations: Koecher's theory can be embedded into a linear subspace *T* in some higher dimensional space of symmetric matrices

IDEA (Bergé, Martinet, Sigrist, 1992):

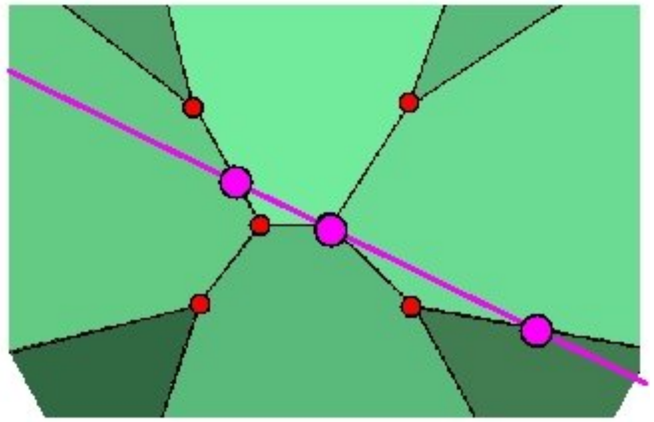
Intersect Ryshkov polyhedron $\mathcal{R}$ with a linear subspace $T \subset \mathcal{S}^n$



DEF: $Q \in T \cap \mathcal{S}^n_{>0}$ is T-perfect if it is a vertex of $\mathcal{R} \cap T$

Voronoi's Algorithm

for a linear subspace *T*



SVPs: Obtain a T-perfect form Q

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

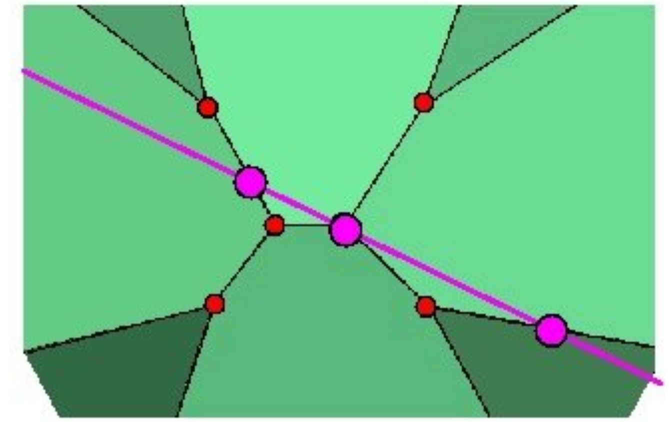
$$\mathcal{P}(Q) \;=\; \{\; Q' \in T \;\;:\;\; Q'[x] \geq 1 \text{ for all } x \in \operatorname{Min} Q \;\}$$

2. PolyRepConv: Enumerate extreme rays $R_1, \ldots, R_k$ of $\mathcal{P}(Q)$
3. For the indefinite R_i, $i = 1, \ldots, k$

   SVPs: Determine contiguous perfect forms $Q_i = Q + \alpha R_i$
4. T-ISOMs: Test if Q_i is T-equivalent to a known form
5. Repeat steps 1.–4. for new perfect forms

Voronoi's Algorithm

for a linear subspace *T*



SVPs: Obtain a T-perfect form Q

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

$$\mathcal{P}(Q) \;=\; \{\; Q' \in T \;:\; Q'[x] \geq 1 \text{ for all } x \in \mathrm{Min}\, Q \;\}$$

2. PolyRepConv: Enumerate extreme rays $R_1, \ldots, R_k$ of $\mathcal{P}(Q)$
3. For the indefinite R_i, $i = 1, \ldots, k$

   SVPs: Determine contiguous perfect forms $Q_i = Q + \alpha R_i$
4. T-ISOMs: Test if Q_i is T-equivalent to a known form
5. Repeat steps 1.–4. for new perfect forms

Possible existence of "Dead-Ends" (for PQFs *R*)

G-invariant theory

$Q, Q' \in T \cap \mathcal{S}^n_{>0}$ are called T-equivalent, if $\exists U \in \mathrm{GL}_n(\mathbb{Z})$ with

$$Q' = U^t Q U \quad \text{and} \quad T = U^t T U$$

For a finite group $G \subset \mathrm{GL}_n(\mathbb{Z})$ the space of invariant forms

$$T_G \quad := \quad \{ \, Q \in \mathcal{S}^n \ : \ G \subset \operatorname{Aut} Q \, \}$$

is a linear subspace of $\mathcal{S}^n$; $\qquad T_G \cap \mathcal{S}^n_{>0}$ is called Bravais space

THM (Jaquet-Chiffelle, 1995):

$$\{ \, T_G\text{-perfect } Q \ : \ \lambda(Q) = 1 \, \} \ / \sim_{T_G} \quad \text{finite}$$

Applicaton: Lattice Sphere Packings

with prescribed symmetry

n	2	4	6	8	10	12
# $\mathcal{E}$-perfect	1	1	2	5	1628	?
maximum δ	$0.9069\ldots$	$0.6168\ldots$	$0.3729\ldots$	$0.2536\ldots$	$0.0360\ldots$	

Perfect Eisenstein forms

n	2	4	6	8	10	12
# $\mathcal{G}$-perfect	1	1	1	2	≥ 8192	?
maximum δ	$0.7853\ldots$	$0.6168\ldots$	$0.3229\ldots$	$0.2536\ldots$		

Perfect Gaussian forms

n	4	8	12	16
# $\mathcal{Q}$-perfect	1	1	8	?
maximum δ	$0.6168\ldots$	$0.2536\ldots$	$0.03125\ldots$	

Perfect Quaternion forms

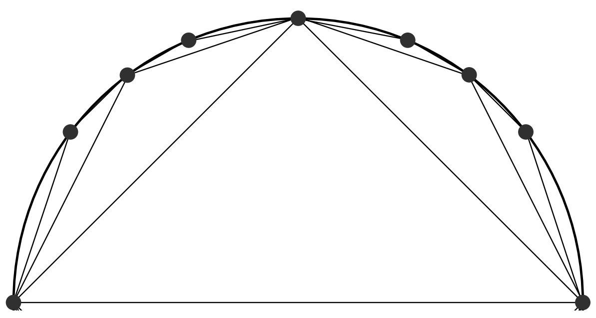
PART III:
A new Generalization

Further Generalization? … and application!

IDEA: Generalize Voronoi's theory to
other convex cones and their duals

Further Generalization? … and application!

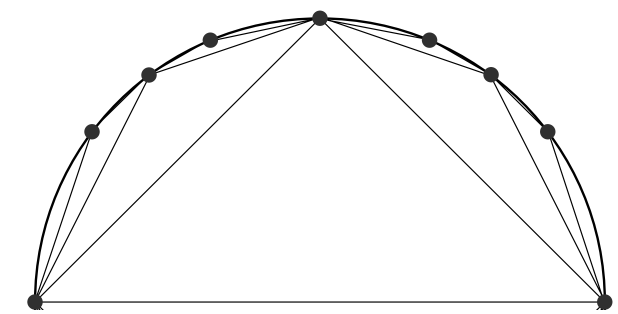
IDEA: Generalize Voronoi's theory to
other convex cones and their duals



In particular to the completely positive cone

Further Generalization? … and application!

IDEA: Generalize Voronoi's theory to
other convex cones and their duals



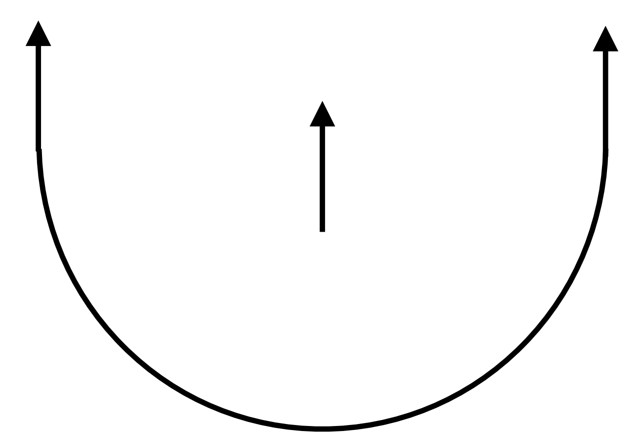
In particular to the completely positive cone

$$\mathcal{CP}_n = \mathrm{cone}\{xx^{\mathsf{T}} : x \in \mathbb{R}^n_{\geq 0}\}$$ 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

Application: Copositive Optimization

- Copositive optimization problems are convex conic problems

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

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

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)

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)

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)

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

Copositive Programming (CP)

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

Semidefinite Programming (SDP)

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)

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

Copositive Programming (CP)

NP-hard (2000)

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

Semidefinite Programming (SDP)

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)

NP-hard (2000)

Such problems have a duality theory and allow certificates for solutions!

cp-factorizations and certificates

DEF: A finite set $X \subset \mathbb{R}^n_{\geq 0}$ is called a certificate for $Q \in \mathcal{S}^n$ being completely positive, if it gives a cp-factorization $Q = \sum_{x \in X} x x^\top$

cp-factorizations and certificates

DEF: A finite set $X \subset \mathbb{R}^n_{\geq 0}$ is called a certificate for $Q \in \mathcal{S}^n$ being completely positive, if it gives a cp-factorization $Q = \sum_{x \in X} x x^\top$

PROBLEM: How to find a cp-factorization for a given Q ?

cp-factorizations and certificates

DEF: A finite set $X \subset \mathbb{R}^n_{\geq 0}$ is called a certificate for $Q \in \mathcal{S}^n$ being completely positive, if it gives a cp-factorization $Q = \sum_{x \in X} x x^\top$

PROBLEM: How to find a cp-factorization for a given Q ?

Known approaches so far:

- Anstreicher, Burer and Dickinson (in Dickinson's thesis 2013) give an algorithm only for matrices in interior based on ellipsoid method
- Numerical heuristics have been proposed by Jarre, Schmallowsky (2009), Nie (2014), Sponsel and Dür (2014), Groetzner and Dür (preprint 2018)

cp-factorizations and certificates

DEF: A finite set $X \subset \mathbb{R}^n_{\geq 0}$ is called a certificate for $Q \in \mathcal{S}^n$ being completely positive, if it gives a cp-factorization $Q = \sum_{x \in X} x x^\top$

PROBLEM: How to find a cp-factorization for a given Q ?

Known approaches so far:

- Anstreicher, Burer and Dickinson (in Dickinson's thesis 2013) give an algorithm only for matrices in interior based on ellipsoid method
- Numerical heuristics have been proposed by Jarre, Schmallowsky (2009), Nie (2014), Sponsel and Dür (2014), Groetzner and Dür (preprint 2018)

Non of these approaches is exact and latter do not even guarantee to find solutions!

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

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!

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 $v_i^\top Q v_j > 0$

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 $v_i^\top Q v_j > 0$

Computation in practice:

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

Generalized Ryshkov polyhedron

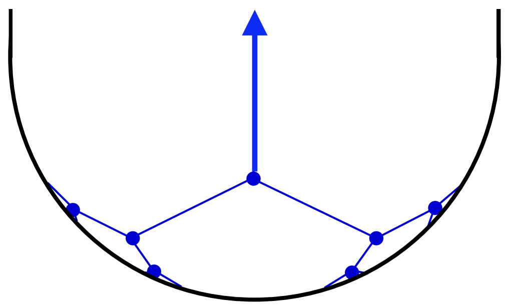
Generalized Ryshkov polyhedron

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

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

Generalized Ryshkov polyhedron

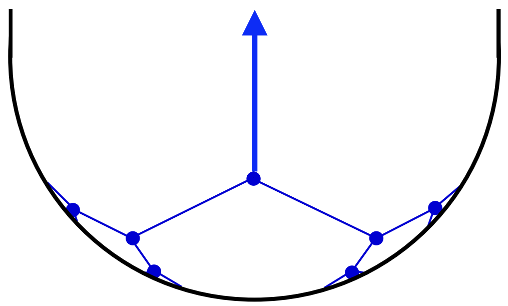
The set of all copositive quadratic forms / matrices with copositive minimum at least 1 is called
Ryshkov polyhedron



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

Generalized Ryshkov polyhedron

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



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

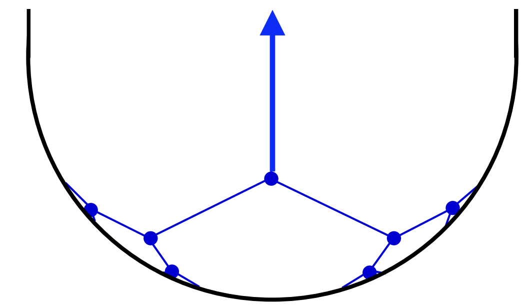
DEF: $Q \in \operatorname{int}\mathcal{COP}_n$ is called $\mathcal{COP}$-perfect if and only if

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

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

Generalized Ryshkov polyhedron

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



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

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

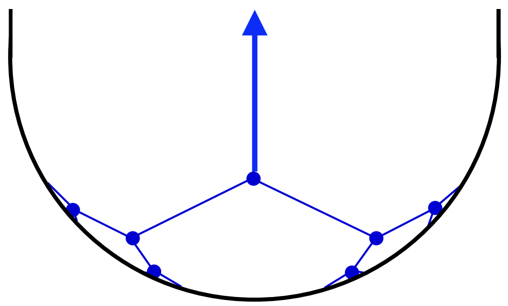
Q is uniquely determined by $\min_{\mathcal{COP}} Q$ and

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

- $\mathcal{R}$ is a locally finite polyhedron (with dead-ends / rays)

Generalized Ryshkov polyhedron

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



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

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

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

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

Voronoi-type simplex algorithm

Input: $A \in \mathcal{S}^n_{>0}$

Voronoi-type simplex algorithm

Input: $A \in \mathcal{S}^n_{>0}$

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

Voronoi-type simplex algorithm

Input: $A \in \mathcal{S}^n_{>0}$

COP-SVPs: 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 $\langle A, R\rangle < 0$.
5. LPs: $\texttt{if}$ $R \in \mathcal{COP}_n$ $\texttt{then}$ $\texttt{output}$ $A \notin \mathcal{CP}_n$ (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.

Voronoi-type simplex algorithm

Input: $A \in \mathcal{S}^n_{>0}$

$\tilde{\mathcal{CP}}_n = \text{cone}\left\{xx^\top : x \in \mathbb{Q}^n\right\}$

COP-SVPs: 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 $\langle A, R\rangle < 0$.
5. LPs: $\texttt{if}$ $R \in \mathcal{COP}_n$ $\texttt{then}$ $\texttt{output}$ $A \notin \mathcal{CP}_n$ (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.

Voronoi-type simplex algorithm

Input: $A \in \mathcal{S}^n_{>0}$ $\qquad$ $\tilde{\mathcal{CP}}_n = \text{cone}\left\{xx^\top : x \in \mathbb{Q}^n\right\}$

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

1. `if` $\langle B_P, A\rangle < 0$ `then` `output` $A \notin \mathcal{CP}_n$ (with witness B_P)
2. LP: `if` $A \in \text{cone}\left\{xx^\top : x \in \text{Min}_{\mathcal{COP}} B_P\right\}$ `then` `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 $\langle A, R\rangle < 0$. $\qquad$ (flexible "pivot-rule")
5. LPs: `if` $R \in \mathcal{COP}_n$ `then` `output` $A \notin \mathcal{CP}_n$ (with witness R)
6. COP-SVPs: Determine the contiguous $\mathcal{COP}$-perfect matrix

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

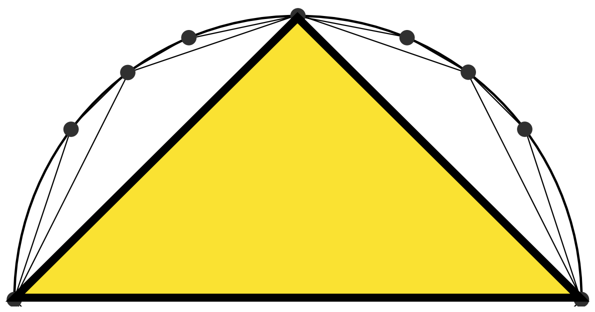
7. Set $B_P := B_N$ and `goto` 1.

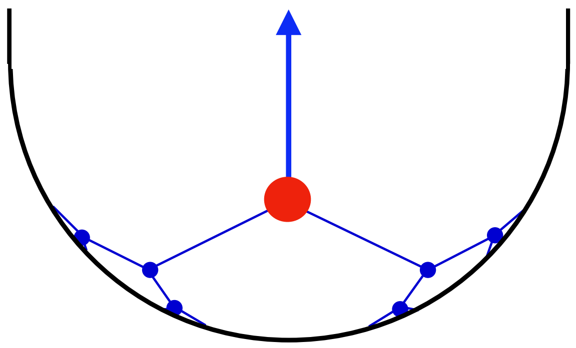
A copositive starting point

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

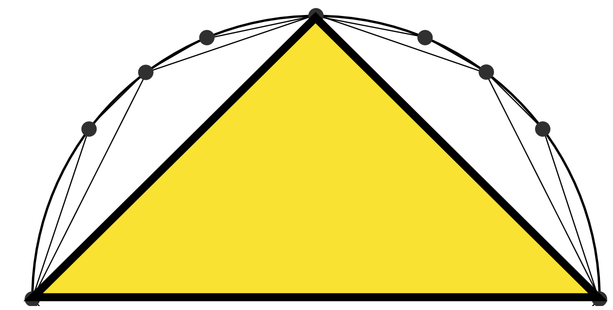
A copositive starting point

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

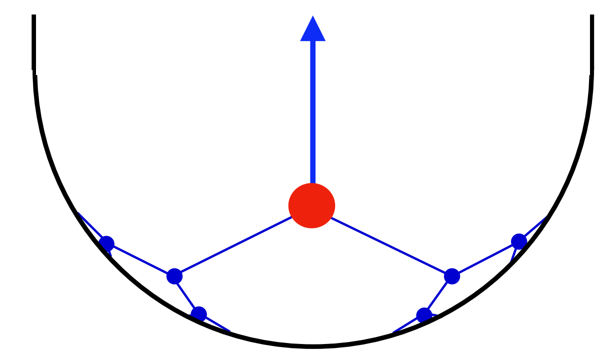




A copositive starting point



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

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

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

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

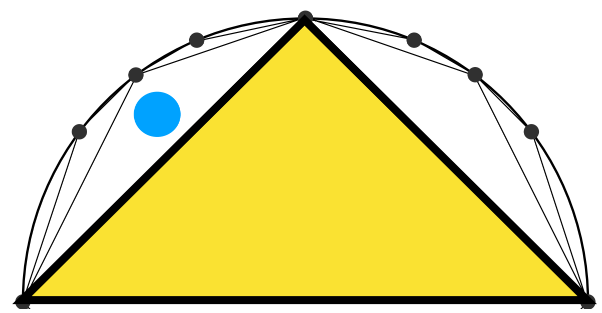
Interior cases

(algorithm terminates)

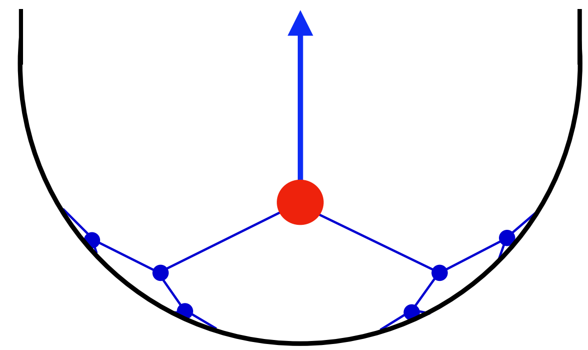
EX: $$A = \begin{pmatrix} 6 & 3 \\ 3 & 2 \end{pmatrix}$$

Interior cases

(algorithm terminates)

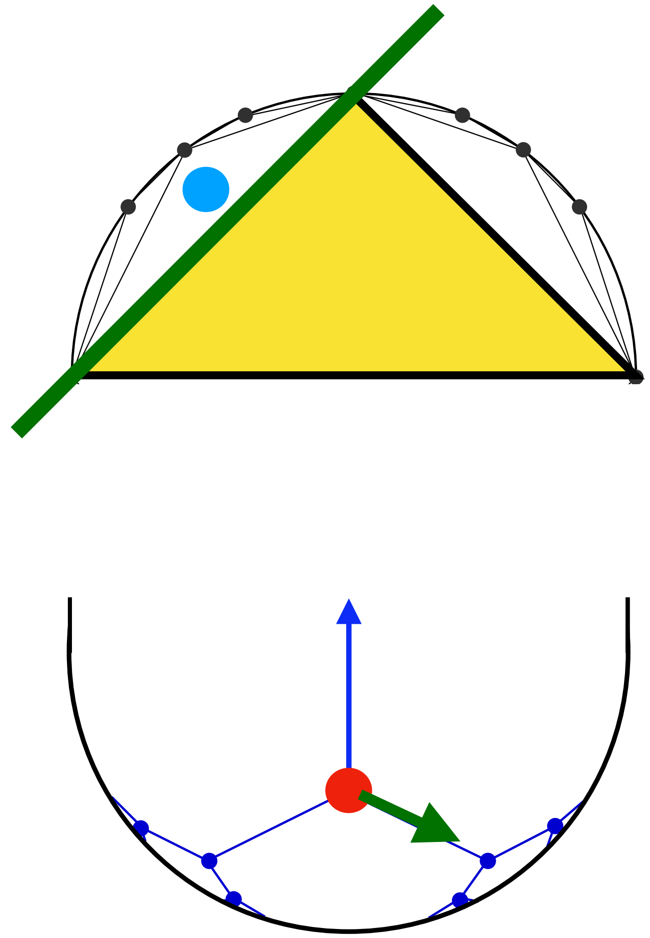


EX: $A = \begin{pmatrix} 6 & 3 \\ 3 & 2 \end{pmatrix}$



Interior cases

(algorithm terminates)

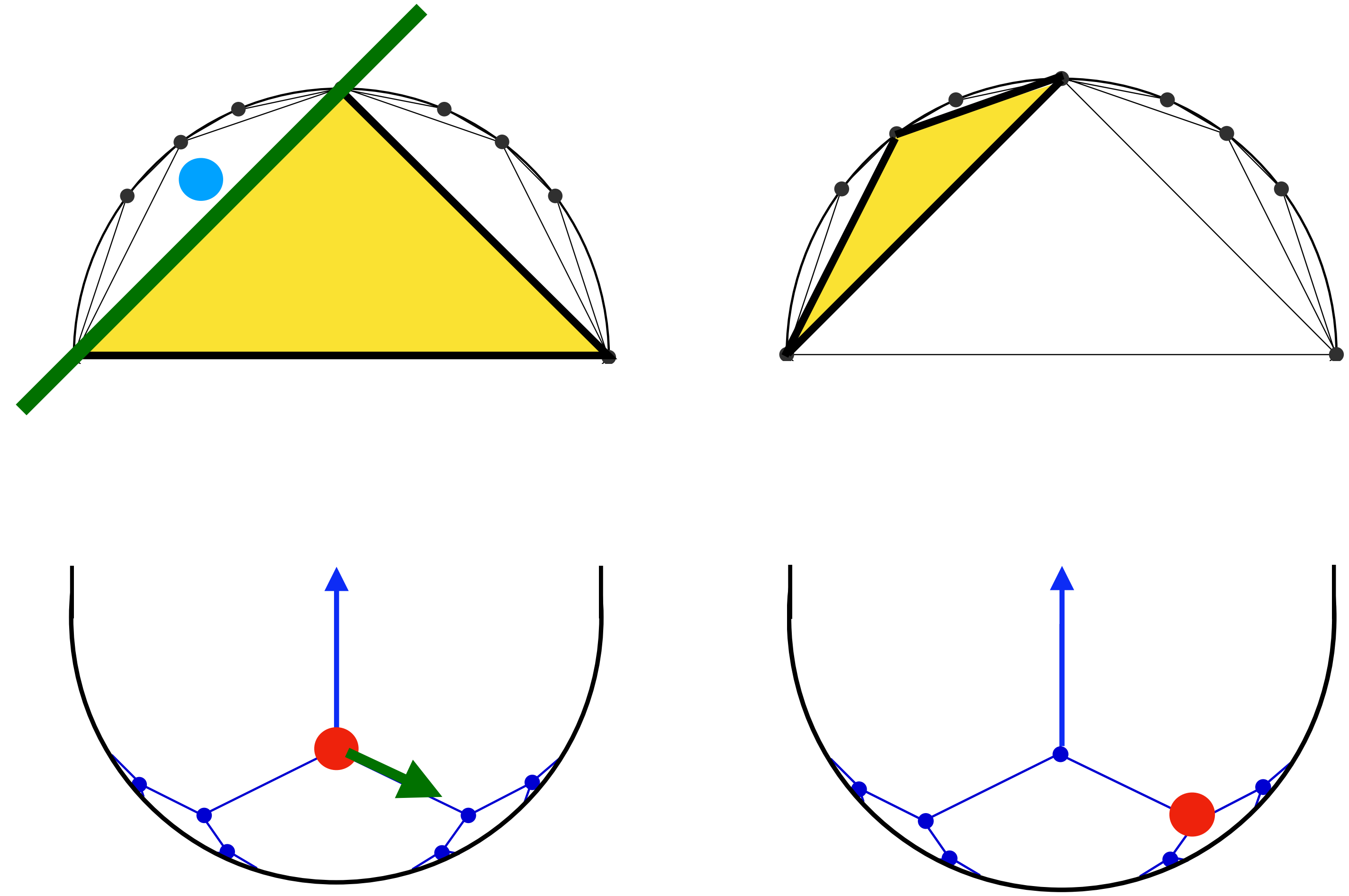


EX: $A = \begin{pmatrix} 6 & 3 \\ 3 & 2 \end{pmatrix}$

Interior cases

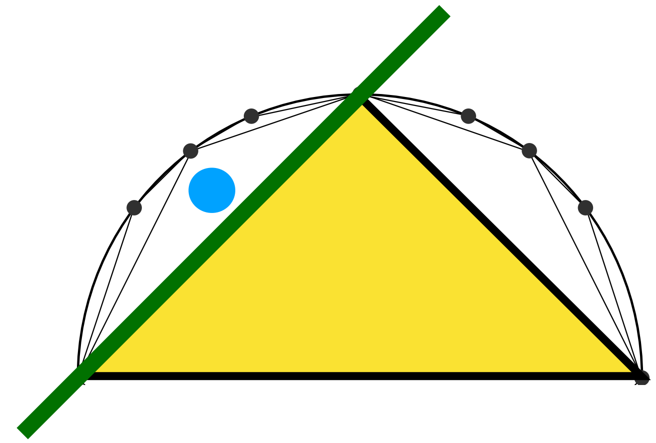
(algorithm terminates)

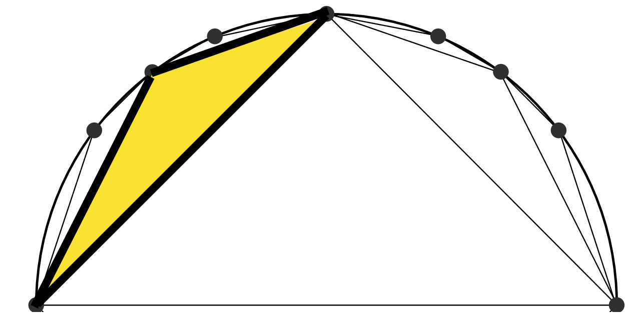
EX: $A = \begin{pmatrix} 6 & 3 \\ 3 & 2 \end{pmatrix}$



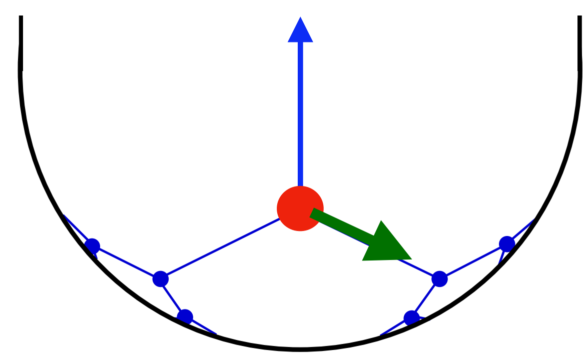
Interior cases

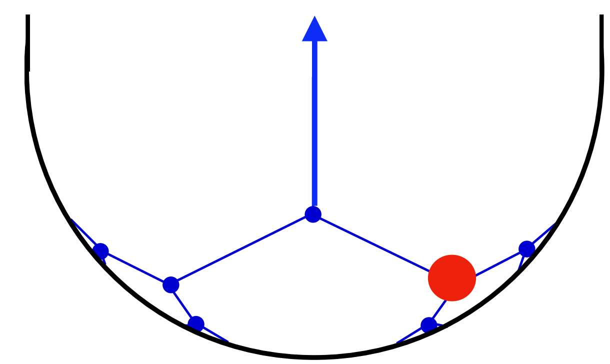
(algorithm terminates)





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



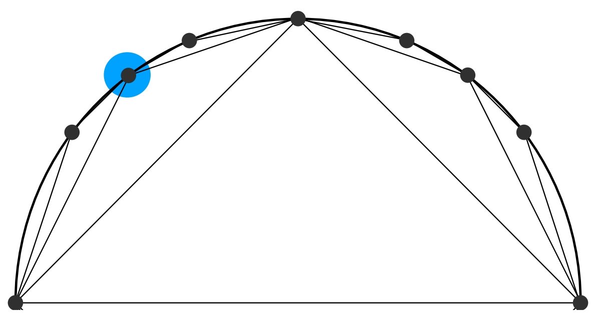


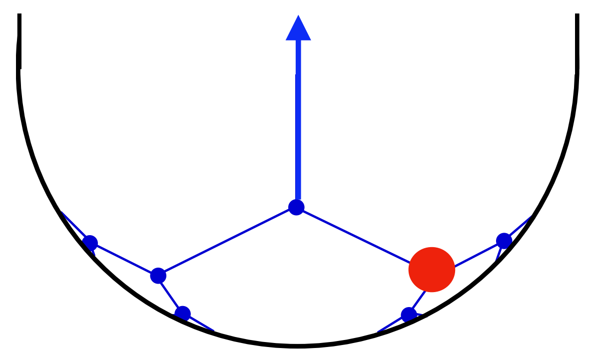
Starting with Q_{A_2} one iteration of the algorithm finds the $\mathcal{COP}$-perfect matrix $B_P = \begin{pmatrix} 1 & -3/2 \\ -3/2 & 3 \end{pmatrix}$ and

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

Boundary cases from $\tilde{\mathcal{CP}}_n$

(algorithm terminates with a suitable pivot-rule)





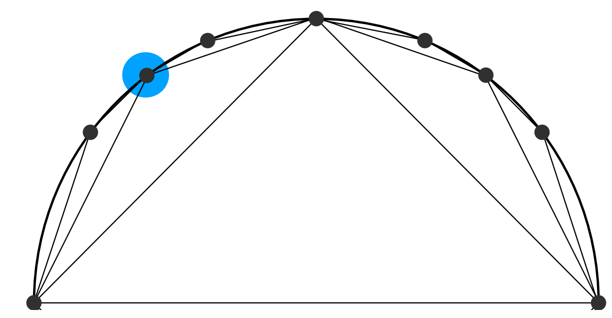
EX: $\begin{pmatrix} 8 & 5 & 1 & 1 & 5 \\ 5 & 8 & 5 & 1 & 1 \\ 1 & 5 & 8 & 5 & 1 \\ 1 & 1 & 5 & 8 & 5 \\ 5 & 1 & 1 & 5 & 8 \end{pmatrix}$

from Groetzner, Dür (2018)

not solved by their algorithms

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

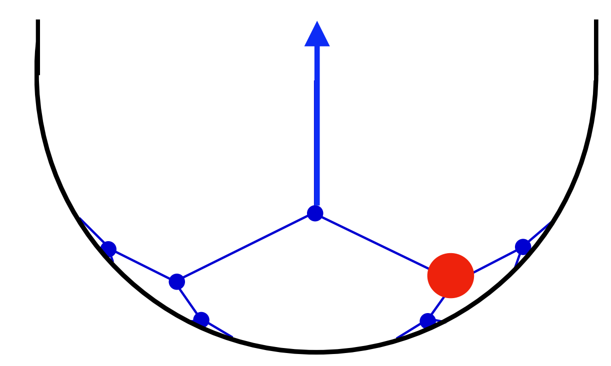
(algorithm terminates with a suitable pivot-rule)



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)

not solved by their algorithms



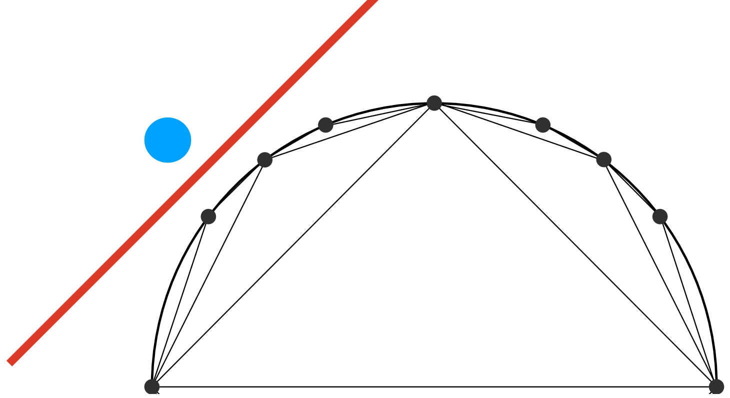
Starting with Q_{A_5}, our algorithm finds a cp-factorization after 5 iterations

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

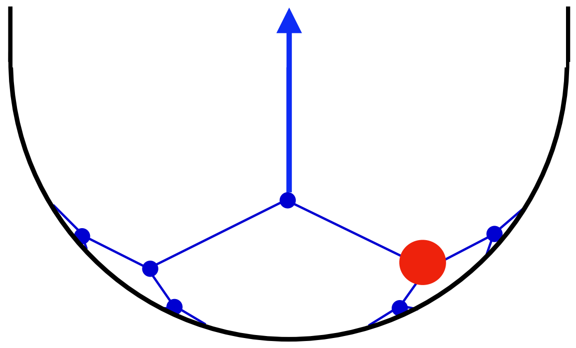
giving a certificate for the matrix to be completely positive

Exterior cases

(algorithm conjectured to terminate)

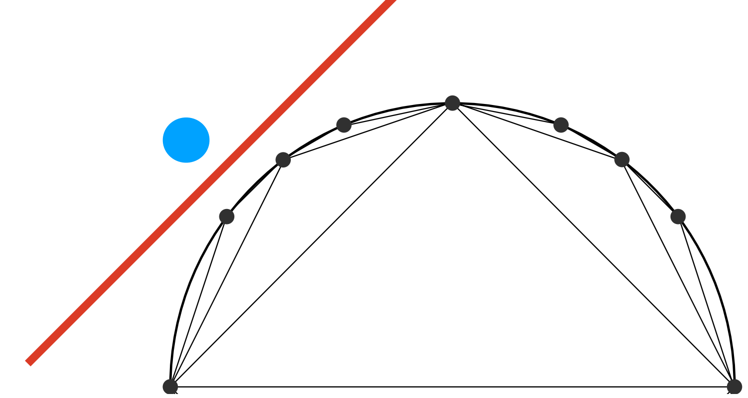


EX: $$\begin{pmatrix} 1 & 1 & 0 & 0 & 1 \\ 1 & 2 & 1 & 0 & 0 \\ 0 & 1 & 2 & 1 & 0 \\ 0 & 0 & 1 & 2 & 1 \\ 1 & 0 & 0 & 1 & 6 \end{pmatrix}$$ from Nie (2014)

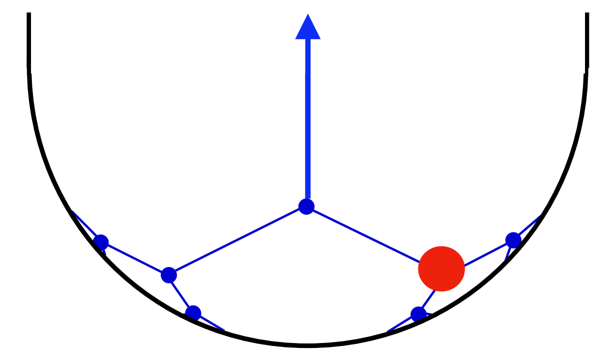


Exterior cases

(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)



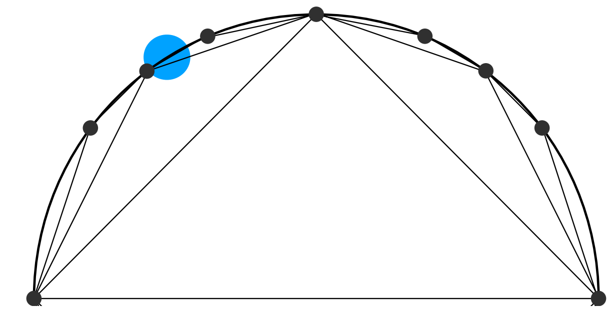
Starting with Q_{A_5}, after 18 iterations our algorithm finds the $\mathcal{COP}$-perfect

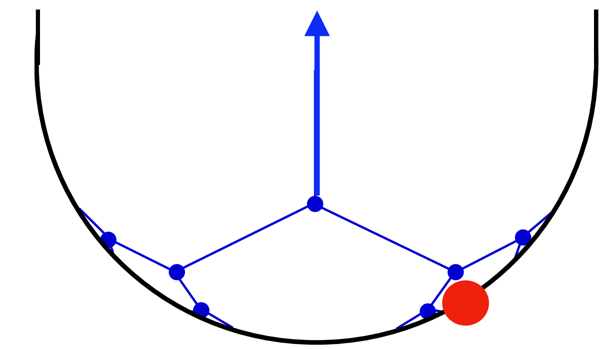
$$\begin{pmatrix} 363/5 & -2126/35 & 2879/70 & 608/21 & -4519/210 \\ -2126/35 & 1787/35 & -347/10 & 1025/42 & 253/14 \\ 2879/70 & -347/10 & 829/35 & -1748/105 & 371/30 \\ 608/21 & 1025/42 & -1748/105 & 1237/105 & -601/70 \\ -4519/210 & 253/14 & 371/30 & -601/70 & 671/105 \end{pmatrix}$$

giving a certificate for the matrix not to be completely positive

Irrational boundary cases

(algorithm is known not to terminate)

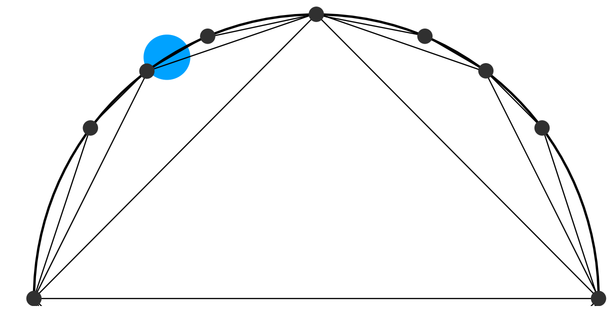




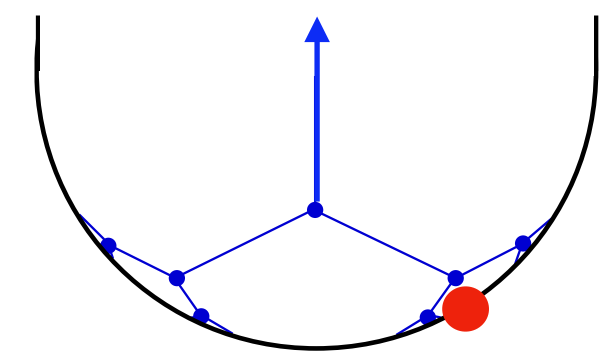
EX: $A = \begin{pmatrix} \sqrt{2} \\ 1 \end{pmatrix} \begin{pmatrix} \sqrt{2} \\ 1 \end{pmatrix}^{\top} = \begin{pmatrix} 2 & \sqrt{2} \\ \sqrt{2} & 1 \end{pmatrix}$

Irrational boundary cases

(algorithm is known not to terminate)



EX: $A = \begin{pmatrix} \sqrt{2} \\ 1 \end{pmatrix} \begin{pmatrix} \sqrt{2} \\ 1 \end{pmatrix}^{\top} = \begin{pmatrix} 2 & \sqrt{2} \\ \sqrt{2} & 1 \end{pmatrix}$



The $\mathcal{COP}$-perfect matrix after ten iterations of the algorithm is

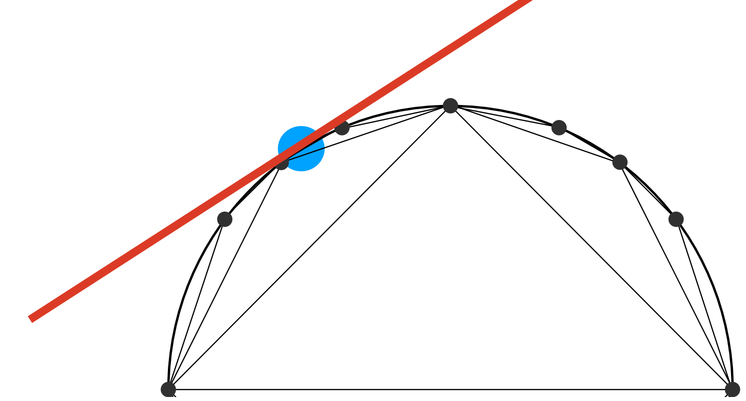
$$B_P^{(10)} = \begin{pmatrix} 4756 & -6726 \\ -6726 & 9512 \end{pmatrix}.$$

It can be shown that the matrices $B_P^{(i)}$ converge to a multiple of

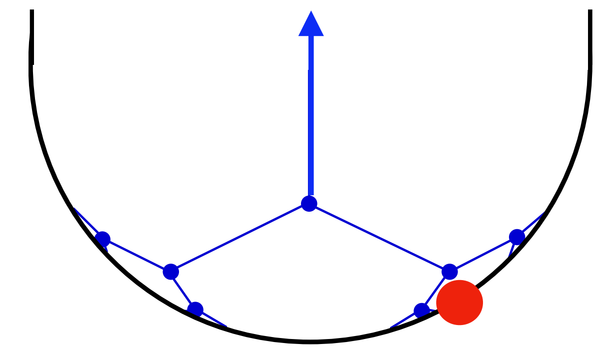
$$B = \begin{pmatrix} 1 & -\sqrt{2} \\ -\sqrt{2} & 2 \end{pmatrix} \text{ satisfying } \langle A, B \rangle = 0 \text{ and } \langle X, B \rangle \geq 0 \text{ for all } X \in \mathcal{CP}_2.$$

Irrational boundary cases

(algorithm is known not to terminate)



EX: $A = \begin{pmatrix} \sqrt{2} \\ 1 \end{pmatrix} \begin{pmatrix} \sqrt{2} \\ 1 \end{pmatrix}^{\top} = \begin{pmatrix} 2 & \sqrt{2} \\ \sqrt{2} & 1 \end{pmatrix}$



The $\mathcal{COP}$-perfect matrix after ten iterations of the algorithm is

$$B_P^{(10)} = \begin{pmatrix} 4756 & -6726 \\ -6726 & 9512 \end{pmatrix}.$$

It can be shown that the matrices $B_P^{(i)}$ converge to a multiple of

$$B = \begin{pmatrix} 1 & -\sqrt{2} \\ -\sqrt{2} & 2 \end{pmatrix} \text{ satisfying } \langle A, B \rangle = 0 \text{ and } \langle X, B \rangle \geq 0 \text{ for all } X \in \mathcal{CP}_2.$$

References

- Mathieu Dutour Sikirić, Achill Schürmann and Frank Vallentin, Classification of eight dimensional perfect forms, *Electron. Res. Announc. Amer. Math. Soc.*, 13 (2007).
- Achill Schürmann, Enumerating Perfect Forms, *AMS Contemporary Mathematics*, 437 (2009), 359–378.
- Achill Schürmann, *Computational Geometry of Positive Definite Quadratic Forms,* University Lecture Series, AMS, Providence, RI, 2009.
- Achill Schürmann, Exploiting Symmetries in Polyhedral Computations, *Fields Institute Communications,* 69 (2013), 265–278.
- 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 cp-factorization, Preprint, April 2018.