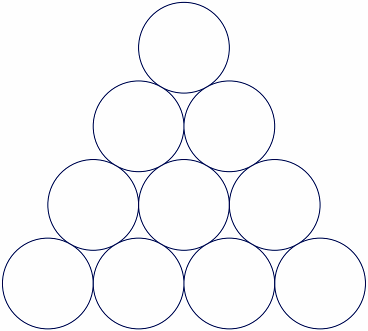
Lattice packings: an upper bound on the number of perfect lattices

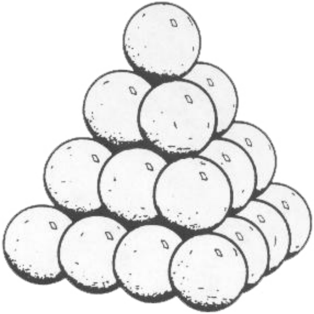
Wessel van Woerden, CWI, Amsterdam.

Centrum Wiskunde & Informatica

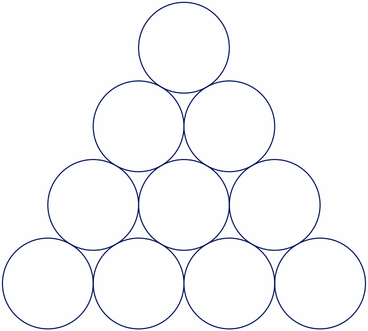
Sphere Packing Problem

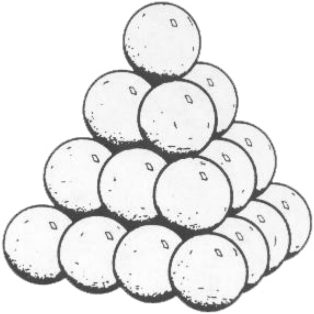
Sphere Packing Problem





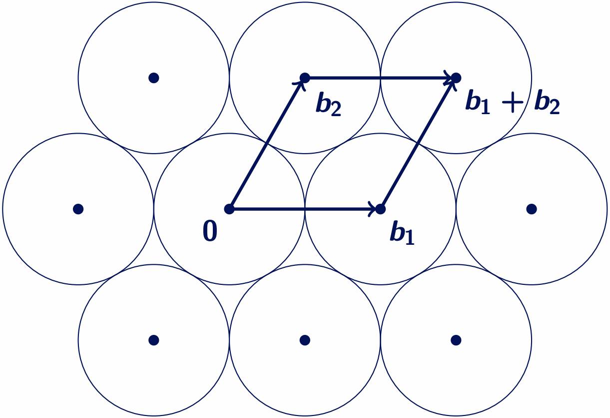
Sphere Packing Problem



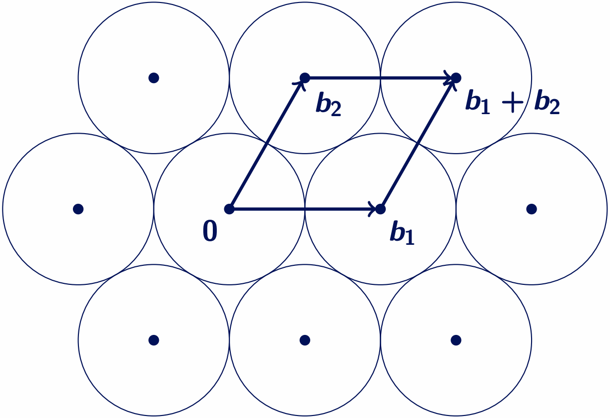


- Only solved in dimensions **2, 3, 8** and **24**...

Lattice Packing Problem



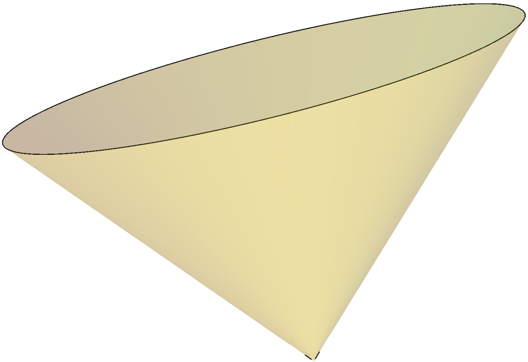
Lattice Packing Problem



- Solved in dimensions $\leq$ **8** and **24**.

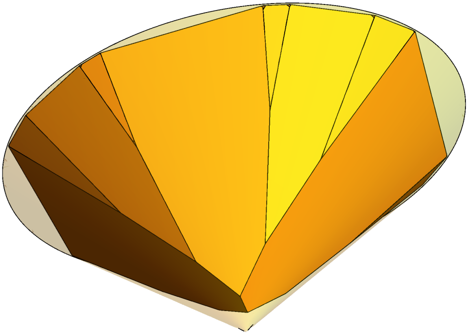
Solution space

- Cone of positive definite quadratic forms:



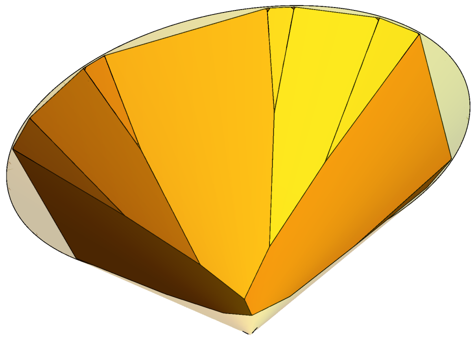
Ryshkov Polyhedron

- Spheres of radius at least **1**:



Ryshkov Polyhedron

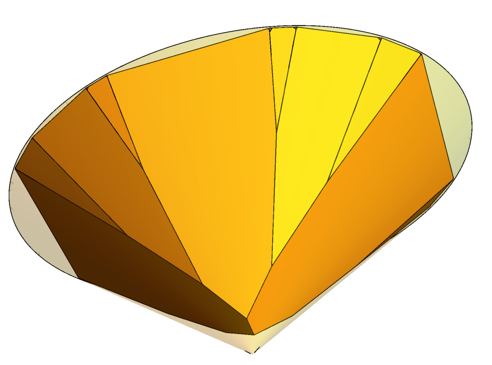
- Spheres of radius at least **1**:



- Concave minimization problem $\implies$ optima at vertices.

Ryshkov Polyhedron

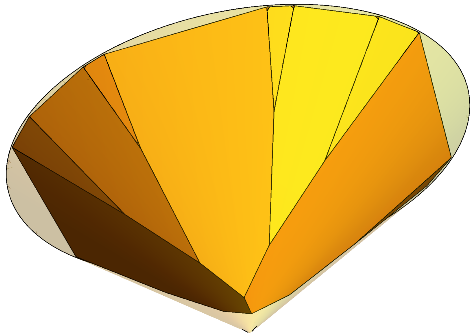
- Spheres of radius at least **1**:



- Concave minimization problem $\implies$ optima at vertices.
- Finite number of non-similar vertices.

Ryshkov Polyhedron

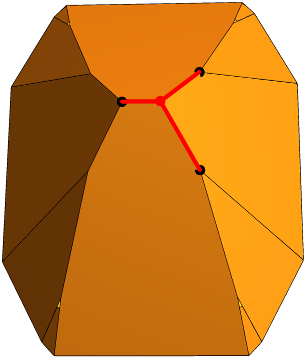
- Spheres of radius at least **1**:



- Concave minimization problem $\implies$ optima at vertices.
- Finite number of non-similar vertices. $\leftarrow$ **how many?**

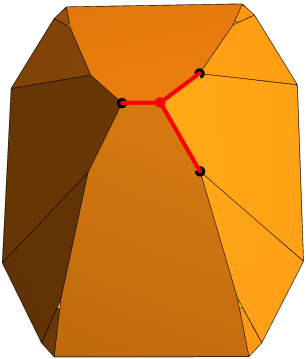
Voronoi's Algorithm

- How to solve the lattice packing problem in a fixed dimension:
  - Enumerate all non-similar vertices.



Voronoi's Algorithm

- How to solve the lattice packing problem in a fixed dimension:
  - Enumerate all non-similar vertices.
  - Pick the best one. □



Space of quadratic forms

- Let $\mathcal{S}^d \subset \mathbb{R}^{d \times d}$ be the space of real **symmetric** matrices.

Space of quadratic forms

- Let $\mathcal{S}^d \subset \mathbb{R}^{d \times d}$ be the space of real **symmetric** matrices.
- Dimension $n := \frac{1}{2}d(d+1)$.

Space of quadratic forms

- Let $\mathcal{S}^d \subset \mathbb{R}^{d \times d}$ be the space of real **symmetric** matrices.
- Dimension $n := \frac{1}{2}d(d+1)$.
- We define the following inner product on $\mathcal{S}^d$:

$$\langle A, B \rangle := \mathrm{Tr}(A^t B) = \sum_{i,j} A_{ij} B_{ij}$$

Space of quadratic forms

- Let $\mathcal{S}^d \subset \mathbb{R}^{d \times d}$ be the space of real **symmetric** matrices.
- Dimension $n := \frac{1}{2}d(d+1)$.
- We define the following inner product on $\mathcal{S}^d$:

$$\langle A, B \rangle := \mathrm{Tr}(A^t B) = \sum_{i,j} A_{ij} B_{ij}$$

- $Q \in \mathcal{S}^d$ defines a quadratic form by

$$Q[x] := x^t Q x = \langle Q, xx^t \rangle \quad \forall x \in \mathbb{R}^d$$

Space of quadratic forms

- Let $\mathcal{S}^d \subset \mathbb{R}^{d\times d}$ be the space of real **symmetric** matrices.
- Dimension $n := \frac{1}{2}d(d+1)$.
- We define the following inner product on $\mathcal{S}^d$:

$$\langle A, B\rangle := \mathrm{Tr}(A^t B) = \sum_{i,j} A_{ij}B_{ij}$$

- $Q \in \mathcal{S}^d$ defines a quadratic form by

$$Q[x] := x^t Q x = \langle Q, xx^t\rangle \;\; \forall x \in \mathbb{R}^d$$

- For a positive definite quadratic form (PQF) $Q \in \mathcal{S}^d_{>0}$:

$$\lambda(Q) := \min_{x\in\mathbb{Z}^d-\{0\}} Q[x]$$

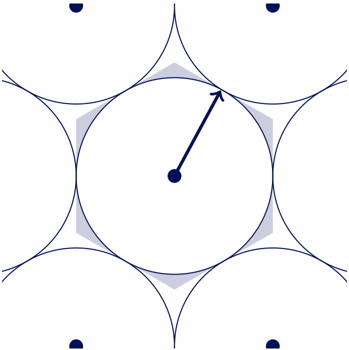
$$\mathrm{Min}\,(Q) := \{x \in \mathbb{Z}^d : Q[x] = \lambda(Q)\}$$

Hermite Constant

- Lattice $\boldsymbol{L} = \boldsymbol{B}\mathbb{Z}^{\boldsymbol{d}} \implies$ PQF $\boldsymbol{Q} = \boldsymbol{B^t B} \in \boldsymbol{S}^{\boldsymbol{d}}_{>\mathbf{0}}$.

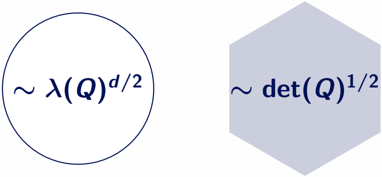
Hermite Constant

- Lattice $\boldsymbol{L} = \boldsymbol{B}\mathbb{Z}^{\boldsymbol{d}} \implies$ PQF $\boldsymbol{Q} = \boldsymbol{B}^{\boldsymbol{t}}\boldsymbol{B} \in \boldsymbol{S}^{\boldsymbol{d}}_{>\mathbf{0}}$.



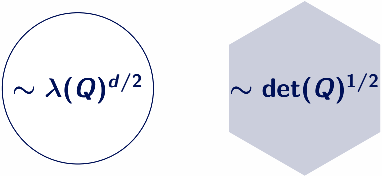
Hermite Constant

- Lattice $\boldsymbol{L} = \boldsymbol{B}\mathbb{Z}^{\boldsymbol{d}} \implies$ PQF $\boldsymbol{Q} = \boldsymbol{B}^{\boldsymbol{t}}\boldsymbol{B} \in \boldsymbol{S}^{\boldsymbol{d}}_{>\mathbf{0}}$.



Hermite Constant

- Lattice $L = B\mathbb{Z}^d \implies$ PQF $Q = B^t B \in S^d_{>0}$.

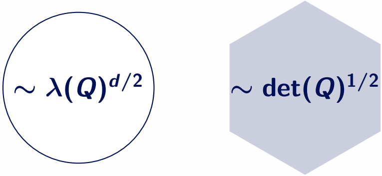


- Hermite invariant:

$$\gamma(Q) = \frac{\lambda(Q)}{(\det Q)^{1/d}} \sim \text{density}(L)^{2/d}$$

Hermite Constant

- Lattice $L = B\mathbb{Z}^d \implies$ PQF $Q = B^t B \in S^d_{>0}$.



- Hermite invariant:

$$\gamma(Q) = \frac{\lambda(Q)}{(\det Q)^{1/d}} \sim \text{density}(L)^{2/d}$$

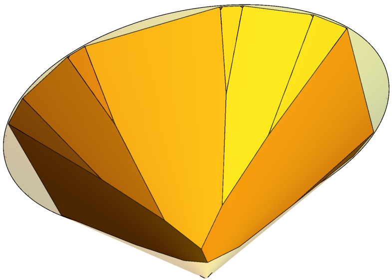
- Lattice packing problem $\Leftrightarrow$ determine Hermite's constant:

$$\mathcal{H}_d := \sup_{Q \in \mathcal{S}^d_{>0}} \gamma(Q)$$

Ryshkov Polyhedra

- For $\lambda > 0$ we define the Ryshkov Polyhedron

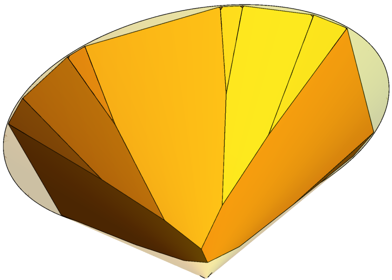
$$\mathcal{P}_\lambda = \{Q \in \mathcal{S}^d_{>0} : \lambda(Q) \geq \lambda\}$$



Ryshkov Polyhedra

- For $\lambda > 0$ we define the Ryshkov Polyhedron

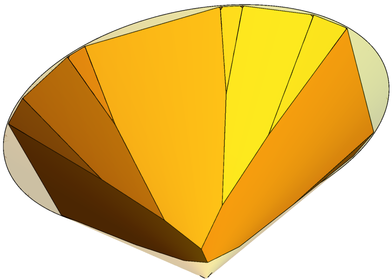
$$\mathcal{P}_\lambda = \bigcap_{x \in \mathbb{Z}^d \setminus \{0\}} \{Q \in \mathcal{S}^d : \langle Q, xx^t \rangle \geq \lambda\} \subset \mathcal{S}^d_{>0}$$



Ryshkov Polyhedra

- For $\lambda > 0$ we define the Ryshkov Polyhedron

$$\mathcal{P}_\lambda = \bigcap_{x \in \mathbb{Z}^d \setminus \{0\}} \{Q \in \mathcal{S}^d : \langle Q, xx^t \rangle \geq \lambda\} \subset \mathcal{S}^d_{>0}$$



- Facets correspond to $x \in \mathbb{Z}^d \setminus \{0\}$.

Ryshkov Polyhedra

- For $\lambda > 0$ we define the Ryshkov Polyhedron

$$\mathcal{P}_\lambda = \{Q \in \mathcal{S}^d_{>0} : \lambda(Q) \geq \lambda\}$$

- We have

$$\mathcal{H}_d = \frac{\lambda}{\inf\limits_{Q \in \mathcal{P}_\lambda} \det(Q)^{1/d}}$$

Ryshkov Polyhedra

- For $\lambda > 0$ we define the Ryshkov Polyhedron

$$\mathcal{P}_\lambda = \{Q \in \mathcal{S}^d_{>0} : \lambda(Q) \geq \lambda\}$$

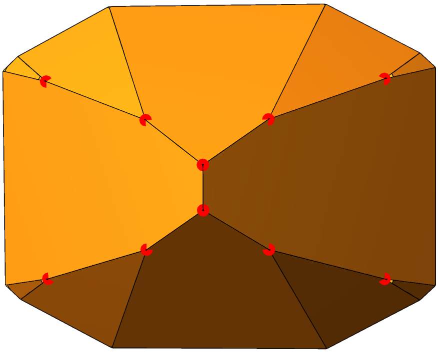
- We have

$$\mathcal{H}_d = \frac{\lambda}{\inf\limits_{Q \in \mathcal{P}_\lambda} \det(Q)^{1/d}}$$

- Minkowski: $\det(Q)^{1/d}$ is (strictly) concave on $\mathcal{S}^d_{>0}$
  $\implies$ Local optima at vertices of $\mathcal{P}_\lambda$.

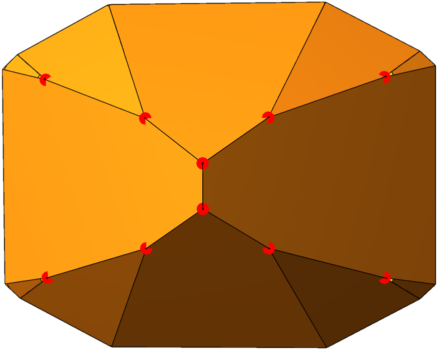
Perfect forms

- $\boldsymbol{Q}$ is perfect $\Leftrightarrow$ $\boldsymbol{Q}$ is a vertex of $\mathcal{P}_{\lambda(\boldsymbol{Q})}$.



Perfect forms

- Q is perfect $\Leftrightarrow$ Q is a vertex of $\mathcal{P}_{\lambda(Q)}$.
- Note that $|\text{Min } Q| \geq 2n = d(d+1)$



Similarity

- $\boldsymbol{B}$ and $\boldsymbol{BU}$ generate the same lattice for $\boldsymbol{U} \in \mathrm{GL}_{\boldsymbol{d}}(\mathbb{Z})$.

Similarity

- $\boldsymbol{B}$ and $\boldsymbol{BU}$ generate the same lattice for $\boldsymbol{U} \in \mathrm{GL}_{\boldsymbol{d}}(\mathbb{Z})$.
- **Arithmetically equivalence:** $\exists \boldsymbol{U}$ s.t. $\boldsymbol{Q}' = \boldsymbol{U}^t \boldsymbol{Q} \boldsymbol{U}$.

Similarity

- $\boldsymbol{B}$ and $\boldsymbol{BU}$ generate the same lattice for $\boldsymbol{U} \in \mathrm{GL}_{\boldsymbol{d}}(\mathbb{Z})$.
- **Arithmetically equivalence:** $\exists \boldsymbol{U}$ s.t. $\boldsymbol{Q}' = \boldsymbol{U}^t \boldsymbol{Q} \boldsymbol{U}$.
- Note that $\lambda_1(\boldsymbol{U}^t \boldsymbol{Q} \boldsymbol{U}) = \lambda_1(\boldsymbol{Q})$ and $\det(\boldsymbol{U}^t \boldsymbol{Q} \boldsymbol{U}) = \det(\boldsymbol{Q})$.

Similarity

- B and BU generate the same lattice for $U \in \mathrm{GL}_d(\mathbb{Z})$.
- **Arithmetically equivalence:** $\exists U$ s.t. $Q' = U^t Q U$.
- Note that $\lambda_1(U^t Q U) = \lambda_1(Q)$ and $\det(U^t Q U) = \det(Q)$.
- **Similarity:** Arithmetical equivalence up to scaling.

Perfect Forms: how many?

Number of perfect forms

- The exact set of perfect forms is known up to dimension **8**.
- For $d \geq 6$ Voronoi's Algorithm was used.

d	# non-similar Perfect forms
2	1 (Lagrange, 1773)
3	1 (Gauss, 1840)
4	2 (Korkine & Zolotarev, 1877)
5	3 (Korkine & Zolotarev, 1877)
6	7 (Barnes, 1957)
7	33 (Jaquet, 1993)
8	10916 (DSV, 2005)
9	$\geq$ 500.000 (DSV, 2005)
	$\geq$ 23.000.000 (vW, 2018)

An improved upper bound

- $p_d :=$ number of non-similar d-dimensional perfect forms.

An improved upper bound

- $p_d :=$ number of non-similar d-dimensional perfect forms.
- Known bounds for p_d.

$$p_d < e^{O(d^4 \log(d))} \qquad \text{(C. Soulé, 1998)}$$

$$e^{\Omega(d)} < p_d < e^{O(d^3 \log(d))} \qquad \text{(R. Bacher, 2017)}$$

An improved upper bound

- $p_d :=$ number of non-similar d-dimensional perfect forms.
- Known bounds for p_d.

$$p_d < e^{O(d^4 \log(d))} \qquad \text{(C. Soulé, 1998)}$$

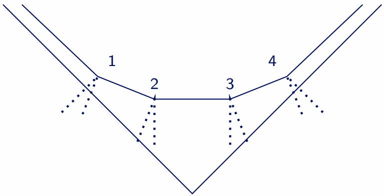
$$e^{\Omega(d)} < p_d < e^{O(d^3 \log(d))} \qquad \text{(R. Bacher, 2017)}$$

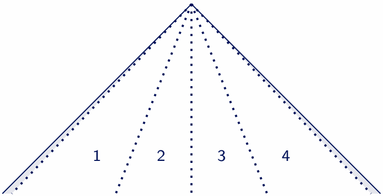
Theorem (This talk)

$$p_d < e^{O(d^2 \log(d))}$$

Outer Normal Cones

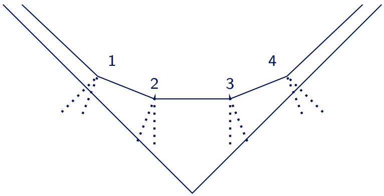
polyhedron inside cone $\Longrightarrow$ subdivision of cone

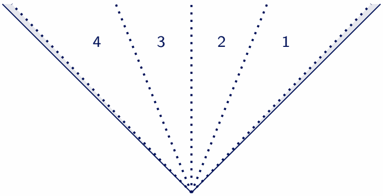




Inner Normal Cones

polyhedron inside cone $\Longrightarrow$ subdivision of cone





Subdivision for $d = 2$

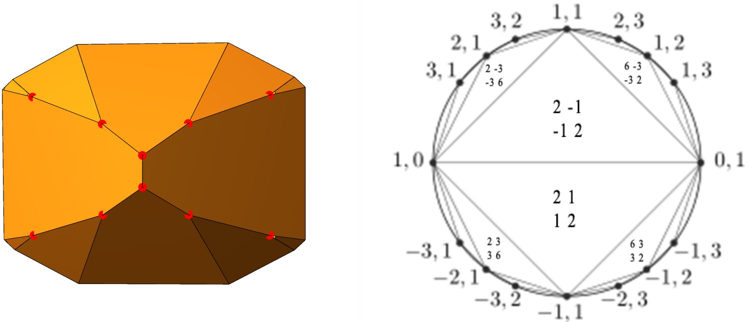


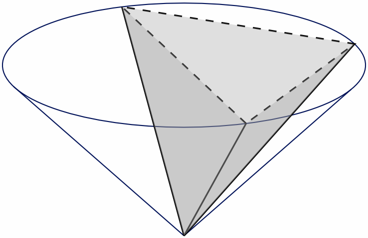
Figure: Subdivision by normal cones of Ryshkov Polyhedron.

Voronoi Domain

Definition

For a PQF $Q \in \mathcal{S}^d_{>0}$ its Voronoi Domain $\mathcal{V}(Q)$ is

$$\mathcal{V}(Q) := \text{cone}(\{xx^t : x \in \text{Min}\, Q\}) \subset \mathcal{S}^d_{\geq 0}.$$



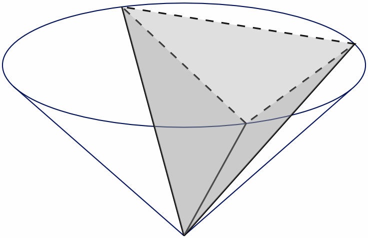
Voronoi Domain

Definition

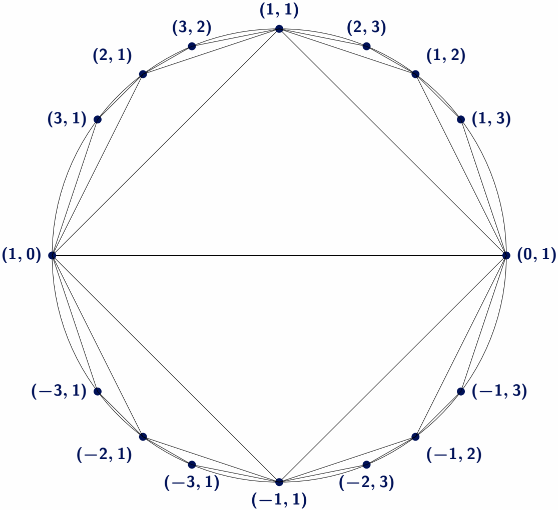
For a PQF $Q \in \mathcal{S}^d_{>0}$ its Voronoi Domain $\mathcal{V}(Q)$ is

$$\mathcal{V}(Q) := \operatorname{cone}(\{xx^t : x \in \operatorname{Min} Q\}) \subset \mathcal{S}^d_{\geq 0}.$$

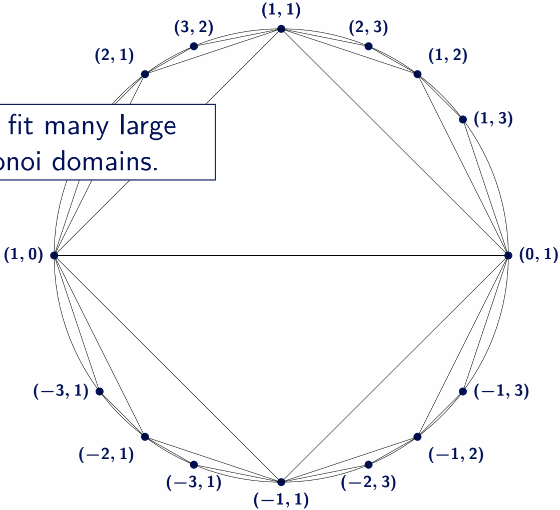
- Q is perfect $\Leftrightarrow$ $\mathcal{V}(Q)$ is full dimensional.



Proof strategy

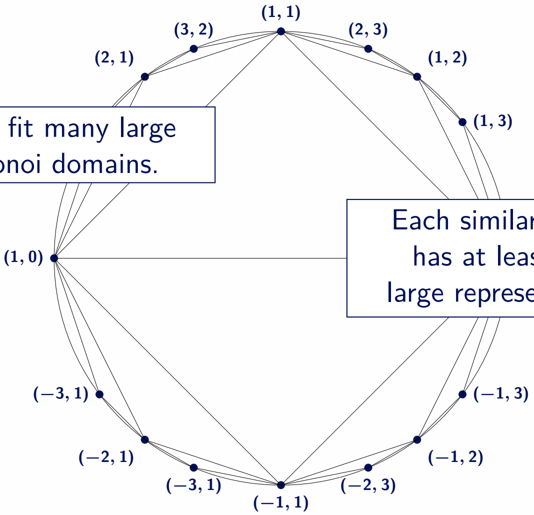


Proof strategy



Can't fit many large Voronoi domains.

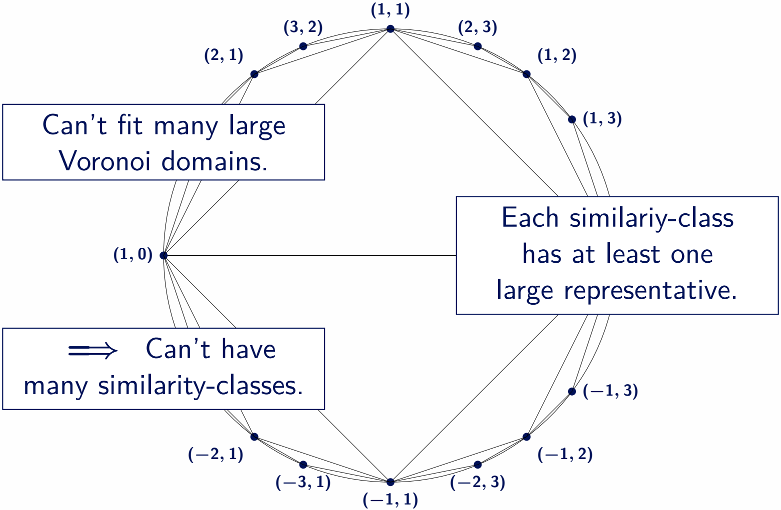
Proof strategy



Can't fit many large Voronoi domains.

Each similariy-class has at least one large representative.

Proof strategy



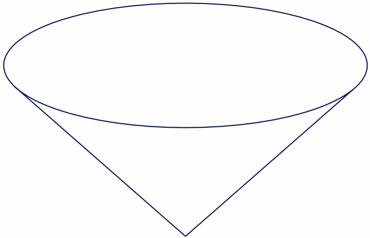
Can't fit many large Voronoi domains.

Each similariy-class has at least one large representative.

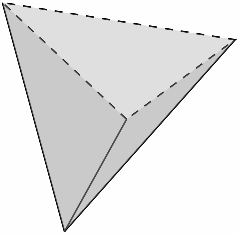
$\implies$ Can't have many similarity-classes.

Volumetric argument

- Find a complete set of representatives P_d such that:



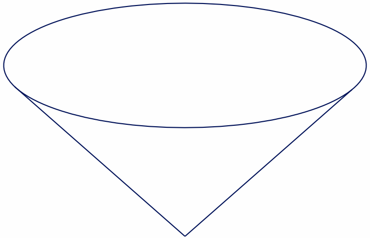
$\text{Vol}\left(\mathcal{S}^d_{\geq 0}\right) \leq u_d$



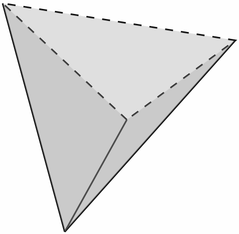
$\text{Vol}\left(\mathcal{V}(Q)\right) \geq \ell_d$
$\forall Q \in P_d$

Volumetric argument

- Find a complete set of representatives $\boldsymbol{P_d}$ such that:



$\text{Vol}\left(\mathcal{S}^d_{\geq 0}\right) \leq \boldsymbol{u_d}$

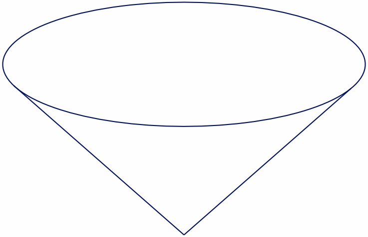


$\text{Vol}\,(\mathcal{V}(\boldsymbol{Q})) \geq \boldsymbol{\ell_d}$
$\forall \boldsymbol{Q} \in \boldsymbol{P_d}$

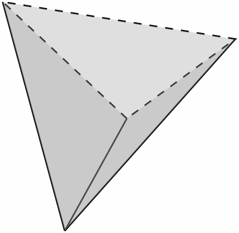
- Then $\boldsymbol{p_d} = |\boldsymbol{P_d}| \leq \frac{\boldsymbol{u_d}}{\boldsymbol{\ell_d}}$.

Volumetric argument

- Find a complete set of representatives $\boldsymbol{P_d}$ such that:



$$\text{Vol}\left(\mathcal{S}^d_{\geq 0}\right) \leq u_d = o(1)$$

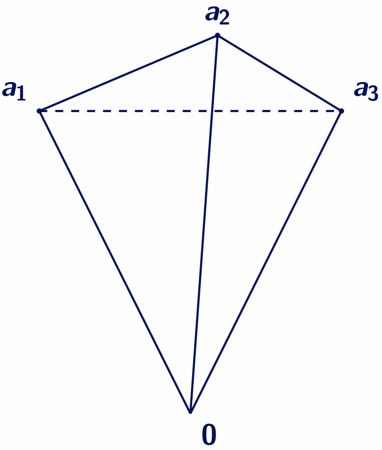


$$\text{Vol}\left(\mathcal{V}(Q)\right) \geq \ell_d \quad \forall Q \in P_d$$

- Then $p_d = |P_d| \leq \frac{u_d}{\ell_d}$.
- To quantify the volume we restrict to the half space

$$T_d := \{Q \in \mathcal{S}^d : \text{Tr}(Q) = \langle Q, I_d \rangle \leq 1\}.$$

Volume simplex



n-dimensional simplex:

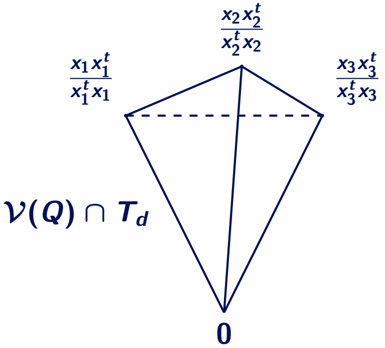
Volume $= \frac{1}{n!} \cdot \left|\det(\langle a_i, a_j \rangle)_{i,j}\right|^{1/2}$

Volume Voronoi domain

- $\mathrm{Tr}(\boldsymbol{x}\boldsymbol{x}^t) = \boldsymbol{x}^t\boldsymbol{x}$.

Volume Voronoi domain

- $\mathrm{Tr}(xx^t) = x^t x$.
- Can look at subcone: w.l.o.g. Min $Q = \{\pm x_1, \ldots, \pm x_n\}$.



Lower bound

We get

$$\mathrm{Vol}(\mathcal{V}(Q) \cap T_d) = \frac{1}{n!} \cdot \left| \det \left(\left\langle \frac{x_i x_i^t}{x_i^t x_i}, \frac{x_j x_j^t}{x_j^t x_j} \right\rangle \right)_{i,j \in [n]} \right|^{1/2}$$

Lower bound

We get

$$\mathrm{Vol}(\mathcal{V}(Q) \cap T_d) = \frac{1}{n!} \cdot \left| \det \left(\left\langle \frac{x_i x_i^t}{x_i^t x_i}, \frac{x_j x_j^t}{x_j^t x_j} \right\rangle \right)_{i,j \in [n]} \right|^{1/2}$$

$$= \frac{1}{n!} \cdot \left(\prod_{i=1}^{n} \frac{1}{x_i^t x_i} \right) \cdot \left| \det \left(\left\langle x_i x_i^t, x_j x_j^t \right\rangle \right)_{i,j \in [n]} \right|^{1/2}$$

Lower bound

We get

$$\mathrm{Vol}(\mathcal{V}(Q) \cap T_d) = \frac{1}{n!} \cdot \left| \det \left(\left\langle \frac{x_i x_i^t}{x_i^t x_i}, \frac{x_j x_j^t}{x_j^t x_j} \right\rangle \right)_{i,j \in [n]} \right|^{1/2}$$

$$= \frac{1}{n!} \cdot \left(\prod_{i=1}^{n} \frac{1}{x_i^t x_i} \right) \cdot \left| \det \left(\left\langle x_i x_i^t, x_j x_j^t \right\rangle \right)_{i,j \in [n]} \right|^{1/2}$$

$$\geq \frac{1}{n!} \cdot \left(\prod_{i=1}^{n} \frac{1}{x_i^t x_i} \right) \leftarrow \text{ Uses integrality of the } x_i$$

Lower bound

We get

$$\begin{aligned}
\mathrm{Vol}(\mathcal{V}(Q) \cap T_d) &= \frac{1}{n!} \cdot \left| \det \left(\left\langle \frac{x_i x_i^t}{x_i^t x_i}, \frac{x_j x_j^t}{x_j^t x_j} \right\rangle \right)_{i,j \in [n]} \right|^{1/2} \\
&= \frac{1}{n!} \cdot \left(\prod_{i=1}^{n} \frac{1}{x_i^t x_i} \right) \cdot \left| \det \left(\left\langle x_i x_i^t, x_j x_j^t \right\rangle \right)_{i,j \in [n]} \right|^{1/2} \\
&\geq \frac{1}{n!} \cdot \left(\prod_{i=1}^{n} \frac{1}{x_i^t x_i} \right) \leftarrow \text{ Uses integrality of the } x_i \\
&\geq \ell_d ?
\end{aligned}$$

We need to upper bound all $x_i^t x_i$.

Short minimal vectors

Lemma

Let PQF $\boldsymbol{Q} \in \mathcal{S}^{\boldsymbol{d}}_{>\mathbf{0}}$. *Then there exists a* $\boldsymbol{Q}'$ *arithmetically equivalent to* $\boldsymbol{Q}$ *such that*

$$\boldsymbol{x}^{\boldsymbol{t}}\boldsymbol{x} = \boldsymbol{O}(\boldsymbol{d}^{\mathbf{4}}) \ \forall \boldsymbol{x} \in Min\, \boldsymbol{Q}'$$

Short minimal vectors

Lemma

Let PQF $\boldsymbol{Q} \in \mathcal{S}^{\boldsymbol{d}}_{>\boldsymbol{0}}$. *Then there exists a* $\boldsymbol{Q}'$ *arithmetically equivalent to* $\boldsymbol{Q}$ *such that*

$$\boldsymbol{x}^t\boldsymbol{x} = O(\boldsymbol{d}^4)\ \forall \boldsymbol{x} \in Min\,\boldsymbol{Q}'$$

- Proof: transference and dual lattice reduction.

Short minimal vectors

Lemma

Let PQF $\boldsymbol{Q} \in \mathcal{S}^d_{>0}$. Then there exists a $\boldsymbol{Q}'$ arithmetically equivalent to $\boldsymbol{Q}$ such that

$$x^t x = O(d^4) \ \forall x \in Min\, \boldsymbol{Q}'$$

- Proof: transference and dual lattice reduction.

$$\begin{aligned}\mathrm{Vol}(\mathcal{V}(Q) \cap T_d) &\geq \frac{1}{n!} \cdot \left(\prod_{i=1}^{n} \frac{1}{x_i^t x_i}\right) \\ &\geq \frac{1}{n!} \cdot \left(\frac{1}{O\left(d^4\right)}\right)^n =: \ell_d\end{aligned}$$

Conclusion

Remind that $n = \frac{1}{2}d(d+1)$. To conclude:

$$\begin{aligned} p_d = |P_d| &\leq \frac{u_d}{\ell_d} \\ &= o(1) \cdot n! \cdot O(d^4)^n \end{aligned}$$

Conclusion

Remind that $n = \frac{1}{2}d(d+1)$. To conclude:

$$\begin{aligned} p_d = |P_d| &\leq \frac{u_d}{\ell_d} \\ &= o(1) \cdot n! \cdot O(d^4)^n \\ &= e^{O(d^2 \log(d))} \quad \square \end{aligned}$$

Conclusion

Remind that $n = \frac{1}{2}d(d+1)$. To conclude:

$$\begin{aligned} p_d = |P_d| &\leq \frac{u_d}{\ell_d} \\ &= o(1) \cdot n! \cdot O(d^4)^n \\ &= e^{O(d^2 \log(d))} \quad \square \end{aligned}$$

Thank you!

Citations

- C. Soulé, Perfect forms and the Vandiver conjecture, Journal fur die Reine und Angewandte Mathematik 517 (1999) 209–222.
- R. Bacher, On the number of perfect lattices, Journal de Théorie des Nombres de Bordeaux 30 (3) (2018) 917–945.
- J. Martinet, Perfect Lattices in Euclidean Spaces, Grundlehren der mathematischen Wissenschaften, Springer Berlin Heidelberg, 2002.
- A. Schurmann, Computational Geometry of Positive Definite Quadratic Forms : Polyhedral Reduction Theories, Algorithms, and Applications, American Mathematical Society, 2009.