Number of Voronoi-relevant vectors in lattices with respect to arbitrary norms

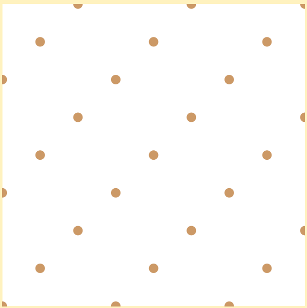
Kathlén Kohn

Faculty of Electrical Engineering, Computer Science and Mathematics
University of Paderborn

2015 – 07 – 15

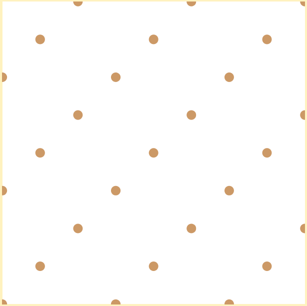
Section 1

Motivation



Definition (1)

An *n-dimensional lattice* is a discrete, additive subgroup of $\mathbb{R}^n$.



Definition (1)

An *n-dimensional lattice* is a discrete, additive subgroup of $\mathbb{R}^n$.

Definition (2)

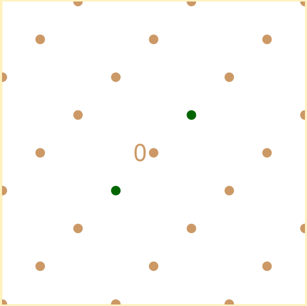
Let $b_1, \dots, b_m \in \mathbb{R}^n$ be linearly independent. Then

$$\mathcal{L}(b_1, \dots, b_m) := \left\{ \sum_{i=1}^{m} z_i b_i \;\middle|\; z_1, \dots, z_m \in \mathbb{Z} \right\}$$

is a *lattice* with *basis* $(b_1, \dots, b_m)$ of *rank* m and *dimension* n.

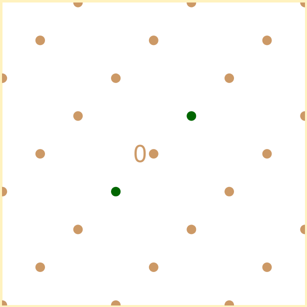
Shortest Vector Problem (SVP):

Given lattice basis $(b_1, \ldots, b_m)$, find shortest vector in $\mathcal{L}(b_1, \ldots, b_m) \backslash \{0\}$.



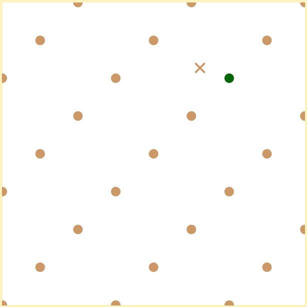
Shortest Vector Problem (SVP):

Given lattice basis $(b_1, \ldots, b_m)$, find shortest vector in $\mathcal{L}(b_1, \ldots, b_m) \backslash \{0\}$.



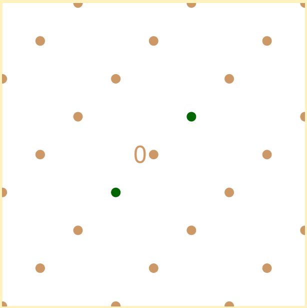
Closest Vector Problem (CVP):

Given lattice basis $(b_1, \ldots, b_m)$ and $x \in \mathbb{R}^n$, find closest vector to x in $\mathcal{L}(b_1, \ldots, b_m)$.



Shortest Vector Problem (SVP):

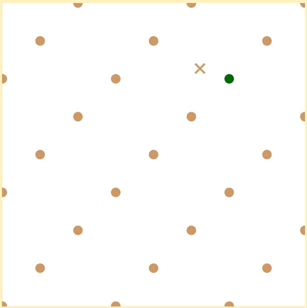
Given lattice basis $(b_1, \ldots, b_m)$, find shortest vector in $\mathcal{L}(b_1, \ldots, b_m) \backslash \{0\}$.



Decision variant NP-hard (under randomized reductions) [Ajtai]

Closest Vector Problem (CVP):

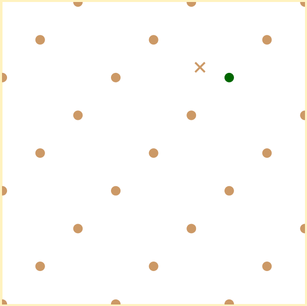
Given lattice basis $(b_1, \ldots, b_m)$ and $x \in \mathbb{R}^n$, find closest vector to x in $\mathcal{L}(b_1, \ldots, b_m)$.



Decision variant NP-complete [Micciancio, Goldwasser]

Algorithm by Micciancio and Voulgaris:

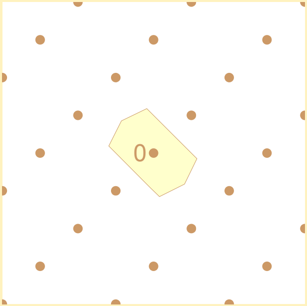
- solves both problems for Euclidean distance
- $2^{O(n)}$ time and space complexity
- core of algorithm:
  - solve CVP with additional input: Voronoi cell



Lattice problems

Algorithm by Micciancio and Voulgaris:

- solves both problems for Euclidean distance
- $2^{O(n)}$ time and space complexity
- core of algorithm:
  - solve CVP with additional input: Voronoi cell



Definition

The *Voronoi cell* of a lattice Λ w.r.t. a norm $\|\cdot\|$ is

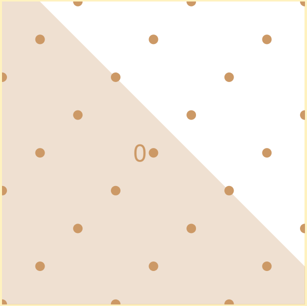
$$\mathcal{V}(\Lambda, \|\cdot\|) := \{x \in \operatorname{span}(\Lambda) \mid \forall v \in \Lambda : \|x\| \leq \|x - v\|\}.$$

Voronoi cell

Definition

The *Voronoi cell* of a lattice Λ w.r.t. a norm $\|\cdot\|$ is

$$\mathcal{V}(\Lambda, \|\cdot\|) := \{x \in \operatorname{span}(\Lambda) \mid \forall v \in \Lambda : \|x\| \leq \|x - v\|\}.$$



$$\mathcal{V}(\Lambda, \|\cdot\|) = \operatorname{span}(\Lambda) \cap \left(\bigcap_{v \in \Lambda} \mathcal{H}^{\leq}_{\|\cdot\|}(0, v) \right)$$

with

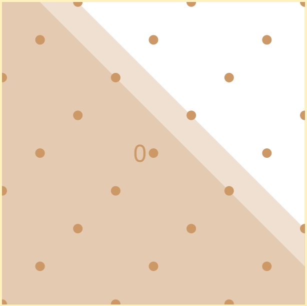
$$\mathcal{H}^{\leq}_{\|\cdot\|}(a, b) := \{x \in \mathbb{R}^n \mid \|x - a\| \leq \|x - b\|\}$$

Voronoi cell

Definition

The *Voronoi cell* of a lattice Λ w.r.t. a norm $\|\cdot\|$ is

$$\mathcal{V}(\Lambda, \|\cdot\|) := \{x \in \operatorname{span}(\Lambda) \mid \forall v \in \Lambda : \|x\| \leq \|x - v\|\}.$$



$$\mathcal{V}(\Lambda, \|\cdot\|) = \operatorname{span}(\Lambda) \cap \left(\bigcap_{v \in \Lambda} \mathcal{H}^{\leq}_{\|\cdot\|}(0, v) \right)$$

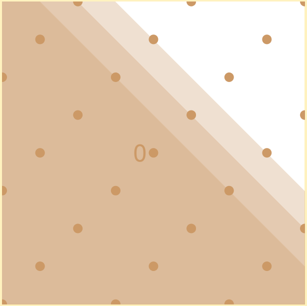
with

$$\mathcal{H}^{\leq}_{\|\cdot\|}(a, b) := \{x \in \mathbb{R}^n \mid \|x - a\| \leq \|x - b\|\}$$

Definition

The *Voronoi cell* of a lattice Λ w.r.t. a norm $\|\cdot\|$ is

$$\mathcal{V}(\Lambda, \|\cdot\|) := \{x \in \operatorname{span}(\Lambda) \mid \forall v \in \Lambda : \|x\| \leq \|x - v\|\}.$$



$$\mathcal{V}(\Lambda, \|\cdot\|) = \operatorname{span}(\Lambda) \cap \left(\bigcap_{v \in \Lambda} \mathcal{H}^{\leq}_{\|\cdot\|}(0, v) \right)$$

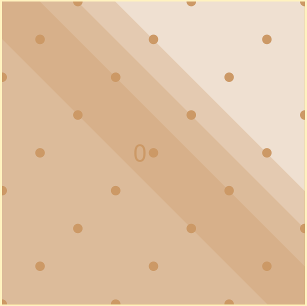
with

$$\mathcal{H}^{\leq}_{\|\cdot\|}(a, b) := \{x \in \mathbb{R}^n \mid \|x - a\| \leq \|x - b\|\}$$

Definition

The *Voronoi cell* of a lattice Λ w.r.t. a norm $\|\cdot\|$ is

$$\mathcal{V}(\Lambda, \|\cdot\|) := \{x \in \operatorname{span}(\Lambda) \mid \forall v \in \Lambda : \|x\| \le \|x - v\|\}\,.$$



$$\mathcal{V}(\Lambda, \|\cdot\|) = \operatorname{span}(\Lambda) \cap \left(\bigcap_{v \in \Lambda} \mathcal{H}^{\le}_{\|\cdot\|}(0, v)\right)$$

with

$$\mathcal{H}^{\le}_{\|\cdot\|}(a, b) := \{x \in \mathbb{R}^n \mid \|x - a\| \le \|x - b\|\}$$

Definition

The *Voronoi cell* of a lattice Λ w.r.t. a norm $\|\cdot\|$ is

$$\mathcal{V}(\Lambda, \|\cdot\|) := \{x \in \operatorname{span}(\Lambda) \mid \forall v \in \Lambda : \|x\| \leq \|x - v\|\}.$$

$$\mathcal{V}(\Lambda, \|\cdot\|) = \operatorname{span}(\Lambda) \cap \left(\bigcap_{v \in \Lambda} \mathcal{H}^{\leq}_{\|\cdot\|}(0, v) \right)$$

with

$$\mathcal{H}^{\leq}_{\|\cdot\|}(a, b) := \{x \in \mathbb{R}^n \mid \|x - a\| \leq \|x - b\|\}$$

Definition

The *Voronoi cell* of a lattice Λ w.r.t. a norm $\|\cdot\|$ is

$$\mathcal{V}(\Lambda, \|\cdot\|) := \{x \in \operatorname{span}(\Lambda) \mid \forall v \in \Lambda : \|x\| \le \|x - v\|\}.$$

$$\mathcal{V}(\Lambda, \|\cdot\|) = \operatorname{span}(\Lambda) \cap \left(\bigcap_{v \in \Lambda} \mathcal{H}^{\le}_{\|\cdot\|}(0, v) \right)$$

with

$$\mathcal{H}^{\le}_{\|\cdot\|}(a, b) := \{x \in \mathbb{R}^n \mid \|x - a\| \le \|x - b\|\}$$

Definition

The *Voronoi cell* of a lattice Λ w.r.t. a norm $\|\cdot\|$ is

$$\mathcal{V}(\Lambda, \|\cdot\|) := \{x \in \operatorname{span}(\Lambda) \mid \forall v \in \Lambda : \|x\| \leq \|x - v\|\}.$$

$$\mathcal{V}(\Lambda, \|\cdot\|) = \operatorname{span}(\Lambda) \cap \left(\bigcap_{v \in \Lambda} \mathcal{H}^{\leq}_{\|\cdot\|}(0, v) \right)$$

with

$$\mathcal{H}^{\leq}_{\|\cdot\|}(a, b) := \{x \in \mathbb{R}^n \mid \|x - a\| \leq \|x - b\|\}$$

Voronoi cell

Definition

The *Voronoi cell* of a lattice Λ w.r.t. a norm $\|\cdot\|$ is

$$\mathcal{V}(\Lambda, \|\cdot\|) := \{x \in \operatorname{span}(\Lambda) \mid \forall\, v \in \Lambda : \|x\| \le \|x - v\|\}\,.$$

$$\mathcal{V}(\Lambda, \|\cdot\|) = \operatorname{span}(\Lambda) \cap \left(\bigcap_{v \in \Lambda} \mathcal{H}^{\le}_{\|\cdot\|}(0, v) \right)$$

with

$$\mathcal{H}^{\le}_{\|\cdot\|}(a, b) := \{x \in \mathbb{R}^n \mid \|x - a\| \le \|x - b\|\}$$

Definition

The *Voronoi cell* of a lattice Λ w.r.t. a norm $\|\cdot\|$ is

$$\mathcal{V}(\Lambda, \|\cdot\|) := \{x \in \operatorname{span}(\Lambda) \mid \forall v \in \Lambda : \|x\| \leq \|x - v\|\}.$$

$$\mathcal{V}(\Lambda, \|\cdot\|) = \operatorname{span}(\Lambda) \cap \left(\bigcap_{v \in \Lambda} \mathcal{H}^{\leq}_{\|\cdot\|}(0, v) \right)$$

with

$$\mathcal{H}^{\leq}_{\|\cdot\|}(a, b) := \{x \in \mathbb{R}^n \mid \|x - a\| \leq \|x - b\|\}$$

Voronoi cell

Definition

The *Voronoi cell* of a lattice Λ w.r.t. a norm $\|\cdot\|$ is

$$\mathcal{V}(\Lambda, \|\cdot\|) := \{x \in \operatorname{span}(\Lambda) \mid \forall v \in \Lambda : \|x\| \le \|x - v\|\}.$$

$$\mathcal{V}(\Lambda, \|\cdot\|) = \operatorname{span}(\Lambda) \cap \left(\bigcap_{v \in \Lambda} \mathcal{H}^{\le}_{\|\cdot\|}(0, v) \right)$$

with

$$\mathcal{H}^{\le}_{\|\cdot\|}(a, b) := \{x \in \mathbb{R}^n \mid \|x - a\| \le \|x - b\|\}$$

Definition

The *Voronoi cell* of a lattice Λ w.r.t. a norm $\|\cdot\|$ is

$$\mathcal{V}(\Lambda, \|\cdot\|) := \{x \in \operatorname{span}(\Lambda) \mid \forall v \in \Lambda : \|x\| \leq \|x - v\|\}.$$

$$\mathcal{V}(\Lambda, \|\cdot\|) = \operatorname{span}(\Lambda) \cap \left(\bigcap_{v \in \Lambda} \mathcal{H}^{\leq}_{\|\cdot\|}(0, v) \right)$$

with

$$\mathcal{H}^{\leq}_{\|\cdot\|}(a, b) := \{x \in \mathbb{R}^n \mid \|x - a\| \leq \|x - b\|\}$$

Voronoi cell

Definition

The *Voronoi cell* of a lattice Λ w.r.t. a norm $\|\cdot\|$ is

$$\mathcal{V}(\Lambda, \|\cdot\|) := \{x \in \operatorname{span}(\Lambda) \mid \forall v \in \Lambda : \|x\| \leq \|x - v\|\}\,.$$

$$\mathcal{V}(\Lambda, \|\cdot\|) = \operatorname{span}(\Lambda) \cap \left(\bigcap_{v \in \Lambda} \mathcal{H}^{\leq}_{\|\cdot\|}(0, v) \right)$$

with

$$\mathcal{H}^{\leq}_{\|\cdot\|}(a, b) := \{x \in \mathbb{R}^n \mid \|x - a\| \leq \|x - b\|\}$$

Voronoi cell

Definition

The *Voronoi cell* of a lattice Λ w.r.t. a norm $\|\cdot\|$ is

$$\mathcal{V}(\Lambda, \|\cdot\|) := \{x \in \operatorname{span}(\Lambda) \mid \forall v \in \Lambda : \|x\| \leq \|x - v\|\}.$$

$$\mathcal{V}(\Lambda, \|\cdot\|) = \operatorname{span}(\Lambda) \cap \left(\bigcap_{v \in \Lambda} \mathcal{H}^{\leq}_{\|\cdot\|}(0, v) \right)$$

with

$$\mathcal{H}^{\leq}_{\|\cdot\|}(a, b) := \{x \in \mathbb{R}^n \mid \|x - a\| \leq \|x - b\|\}$$

Definition

The *Voronoi cell* of a lattice Λ w.r.t. a norm $\|\cdot\|$ is

$$\mathcal{V}(\Lambda, \|\cdot\|) := \{x \in \operatorname{span}(\Lambda) \mid \forall v \in \Lambda : \|x\| \leq \|x - v\|\}.$$

$$\mathcal{V}(\Lambda, \|\cdot\|) = \operatorname{span}(\Lambda) \cap \left(\bigcap_{v \in \Lambda} \mathcal{H}^{\leq}_{\|\cdot\|}(0, v) \right)$$

with

$$\mathcal{H}^{\leq}_{\|\cdot\|}(a, b) := \{x \in \mathbb{R}^n \mid \|x - a\| \leq \|x - b\|\}$$

Definition

The *Voronoi cell* of a lattice Λ w.r.t. a norm $\|\cdot\|$ is

$$\mathcal{V}(\Lambda, \|\cdot\|) := \{x \in \operatorname{span}(\Lambda) \mid \forall v \in \Lambda : \|x\| \leq \|x - v\|\} .$$

$$\mathcal{V}(\Lambda, \|\cdot\|) = \operatorname{span}(\Lambda) \cap \left(\bigcap_{v \in \Lambda} \mathcal{H}^{\leq}_{\|\cdot\|}(0, v) \right)$$

with

$$\mathcal{H}^{\leq}_{\|\cdot\|}(a, b) := \{x \in \mathbb{R}^n \mid \|x - a\| \leq \|x - b\|\}$$

Definition

The *Voronoi cell* of a lattice Λ w.r.t. a norm $\|\cdot\|$ is

$$\mathcal{V}(\Lambda, \|\cdot\|) := \{x \in \mathrm{span}(\Lambda) \mid \forall v \in \Lambda : \|x\| \leq \|x - v\|\}.$$

$$\mathcal{V}(\Lambda, \|\cdot\|) = \mathrm{span}(\Lambda) \cap \left(\bigcap_{v \in \Lambda} \mathcal{H}^{\leq}_{\|\cdot\|}(0, v) \right)$$

with

$$\mathcal{H}^{\leq}_{\|\cdot\|}(a, b) := \{x \in \mathbb{R}^n \mid \|x - a\| \leq \|x - b\|\}$$

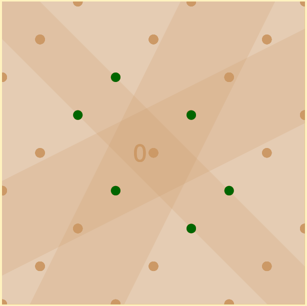
Voronoi-relevant vectors

$$\mathcal{V}(\Lambda, \|\cdot\|) = \operatorname{span}(\Lambda) \cap \left(\bigcap_{v \in \Lambda} \mathcal{H}^{\leq}_{\|\cdot\|}(0, v) \right)$$

with

$$\mathcal{H}^{\leq}_{\|\cdot\|}(a, b) := \{x \in \mathbb{R}^n \mid \|x - a\| \leq \|x - b\|\}$$

Voronoi-relevant vectors

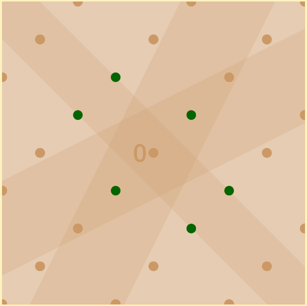


$$\mathcal{V}(\Lambda, \|\cdot\|) = \operatorname{span}(\Lambda) \cap \left(\bigcap_{v \in \Lambda} \mathcal{H}^{\leq}_{\|\cdot\|}(0, v) \right)$$

with

$$\mathcal{H}^{\leq}_{\|\cdot\|}(a, b) := \{ x \in \mathbb{R}^n \mid \|x - a\| \leq \|x - b\| \}$$

Voronoi-relevant vectors



$$\mathcal{V}(\Lambda, \|\cdot\|) = \mathrm{span}(\Lambda) \cap \left(\bigcap_{v \in \Lambda} \mathcal{H}^{\leq}_{\|\cdot\|}(0, v) \right)$$

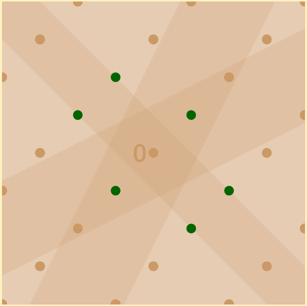
with

$$\mathcal{H}^{\leq}_{\|\cdot\|}(a, b) := \{x \in \mathbb{R}^n \mid \|x - a\| \leq \|x - b\|\}$$

Definition

$v \in \Lambda \setminus \{0\}$ is *Voronoi-relevant (VR)* w.r.t. $\|\cdot\|$ if

$$\exists x \in \mathrm{span}(\Lambda) : \|x\| = \|x - v\|,$$
$$\forall w \in \Lambda \setminus \{0, v\} : \|x\| < \|x - w\|.$$



$$\mathcal{V}(\Lambda, \|\cdot\|_2) = \mathrm{span}(\Lambda) \cap \left(\bigcap_{v \in \Lambda \mathrm{VR}} \mathcal{H}^{\leq}_{\|\cdot\|_2}(0, v) \right)$$

for Euclidean norm $\|\cdot\|_2$ [Agrell et al.]

Definition

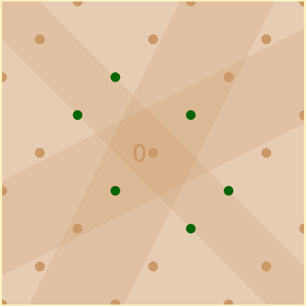
$v \in \Lambda \backslash \{0\}$ is *Voronoi-relevant (VR)* w.r.t. $\|\cdot\|$ if

$$\exists x \in \mathrm{span}(\Lambda) : \|x\| = \|x - v\|,$$
$$\forall w \in \Lambda \backslash \{0, v\} : \|x\| < \|x - w\|.$$

Voronoi-relevant vectors

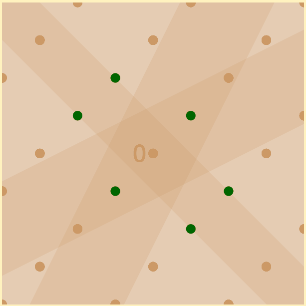
Algorithm by Micciancio and Voulgaris:

- solves SVP and CVP for Euclidean distance
- $2^{O(n)}$ time and space complexity
- core of algorithm:
  - solve CVP with additional input: Voronoi cell



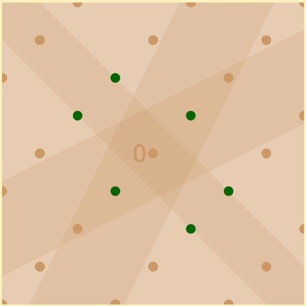
Algorithm by Micciancio and Voulgaris:

- solves SVP and CVP for Euclidean distance
- $2^{O(n)}$ time and space complexity
- core of algorithm:
    - solve CVP with additional input: **Voronoi-relevant vectors**



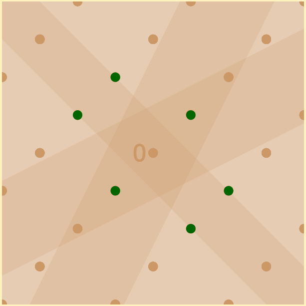
Algorithm by Micciancio and Voulgaris:

- solves SVP and CVP for Euclidean distance
- $2^{O(n)}$ time and space complexity
- core of algorithm:
  - solve CVP with additional input: **Voronoi-relevant vectors**



- at most $2(2^n - 1)$ Voronoi-relevant vectors in n-dimensional lattice w.r.t. Euclidean norm [Agrell et al.]
  - essential for above algorithm

Voronoi-relevant vectors

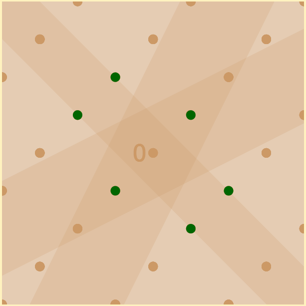


Algorithm by Micciancio and Voulgaris:

- solves SVP and CVP for Euclidean distance
- $2^{O(n)}$ time and space complexity
- core of algorithm:
  - solve CVP with additional input: **Voronoi-relevant vectors**
- at most $2(2^n - 1)$ Voronoi-relevant vectors in n-dimensional lattice w.r.t. Euclidean norm [Agrell et al.]
  - essential for above algorithm
  - proof uses parallelogram identity

Algorithm by Micciancio and Voulgaris:

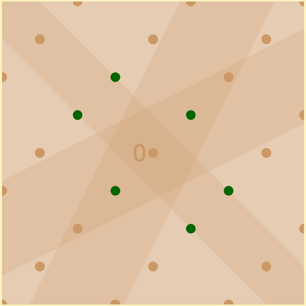
- solves SVP and CVP for Euclidean distance
- $2^{O(n)}$ time and space complexity
- core of algorithm:
  - solve CVP with additional input: **Voronoi-relevant vectors**



- at most $2(2^n - 1)$ Voronoi-relevant vectors in n-dimensional lattice w.r.t. Euclidean norm [Agrell et al.]
  - essential for above algorithm
  - proof uses parallelogram identity
  - open problem by Micciancio and Voulgaris: extend algorithm to p-norms

Algorithm by Micciancio and Voulgaris:

- solves SVP and CVP for Euclidean distance
- $2^{O(n)}$ time and space complexity
- core of algorithm:
  - solve CVP with additional input: **Voronoi-relevant vectors**



- at most $2(2^n - 1)$ Voronoi-relevant vectors in n-dimensional lattice w.r.t. Euclidean norm [Agrell et al.]
  - essential for above algorithm
  - proof uses parallelogram identity
  - open problem by Micciancio and Voulgaris: extend algorithm to p-norms

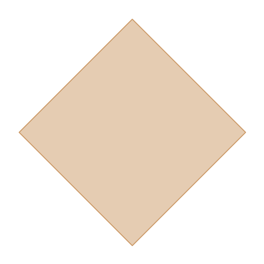
$\Longrightarrow$ **Upper bound for number of Voronoi-relevant vectors w.r.t. arbitrary p-norms?**

Section 2

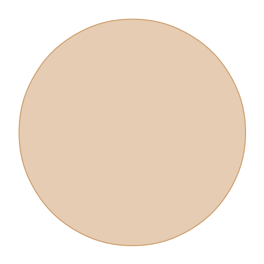
Strictly convex norms

Definition

A norm is strictly convex if its unit sphere does not contain a line segment.

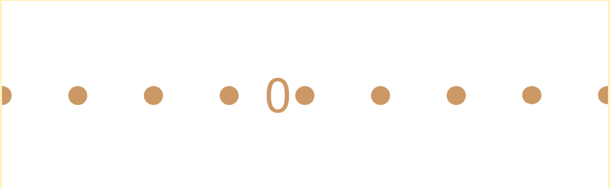


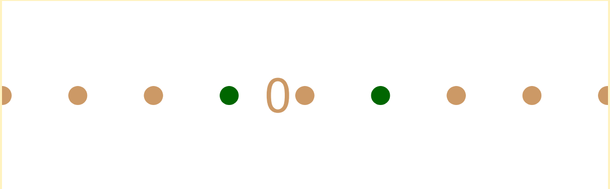
not strictly convex



strictly convex

Rank 1

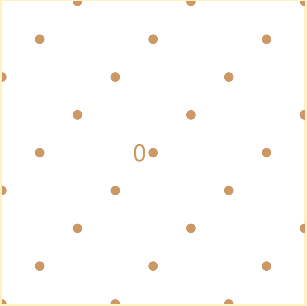




2 Voronoi-relevant vectors

Theorem (Blömer, K., Teusner)

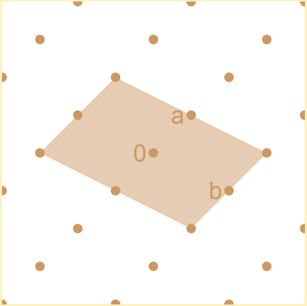
Every lattice Λ of rank 2 has exactly 4 or 6 Voronoi-relevant vectors w.r.t. every strictly convex norm.



Theorem (Blömer, K., Teusner)

Every lattice Λ of rank 2 has exactly 4 or 6 Voronoi-relevant vectors w.r.t. every strictly convex norm.

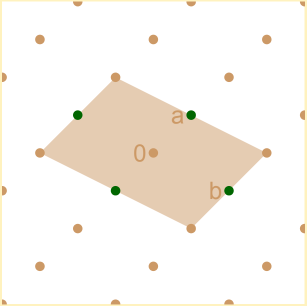
- Let $a, b \in \Lambda$ be shortest, linearly independent vectors



Theorem (Blömer, K., Teusner)

Every lattice Λ of rank 2 has exactly 4 or 6 Voronoi-relevant vectors w.r.t. every strictly convex norm.

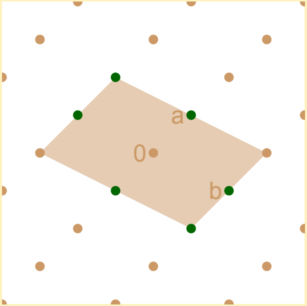
- Let $a, b \in \Lambda$ be shortest, linearly independent vectors
- $\pm a, \pm b$ are Voronoi-relevant



Theorem (Blömer, K., Teusner)

Every lattice Λ of rank 2 has exactly 4 or 6 Voronoi-relevant vectors w.r.t. every strictly convex norm.

- Let $a, b \in \Lambda$ be shortest, linearly independent vectors
- $\pm a, \pm b$ are Voronoi-relevant
- at most 2 of $\{\pm(a+b), \pm(a-b)\}$ are Voronoi-relevant



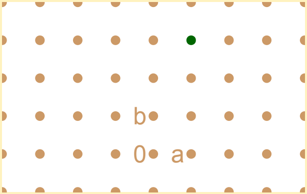
There is no upper bound for the number of Voronoi-relevant vectors

- **w.r.t. general strictly convex norms**
- **that depends only on the lattice dimension!**

There is no upper bound for the number of Voronoi-relevant vectors

- **w.r.t. general strictly convex norms**
- **that depends only on the lattice dimension!**

Q: Can $a + mb$ for $a, b \in \Lambda$ and large $m \in \mathbb{N}$ be Voronoi-relevant?

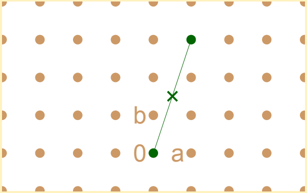


$m = 3$

There is no upper bound for the number of Voronoi-relevant vectors

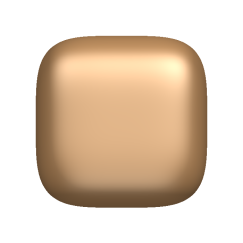
- **w.r.t. general strictly convex norms**
- **that depends only on the lattice dimension!**

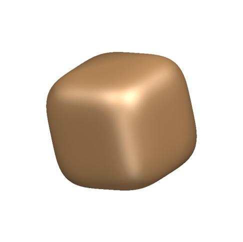
Q: Can $a + mb$ for $a, b \in \Lambda$ and large $m \in \mathbb{N}$ be Voronoi-relevant?



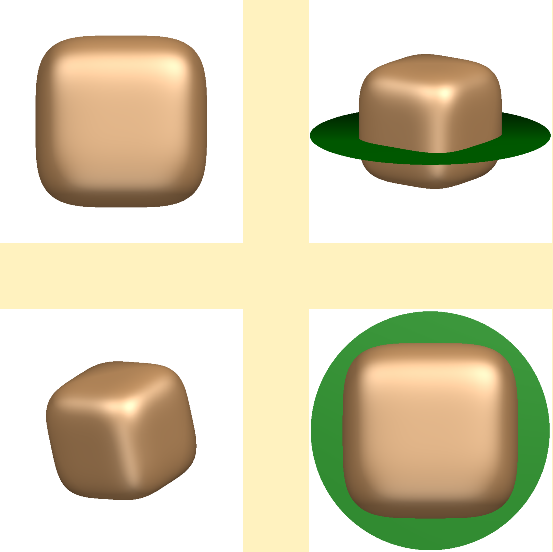
$m = 3$

3-norm

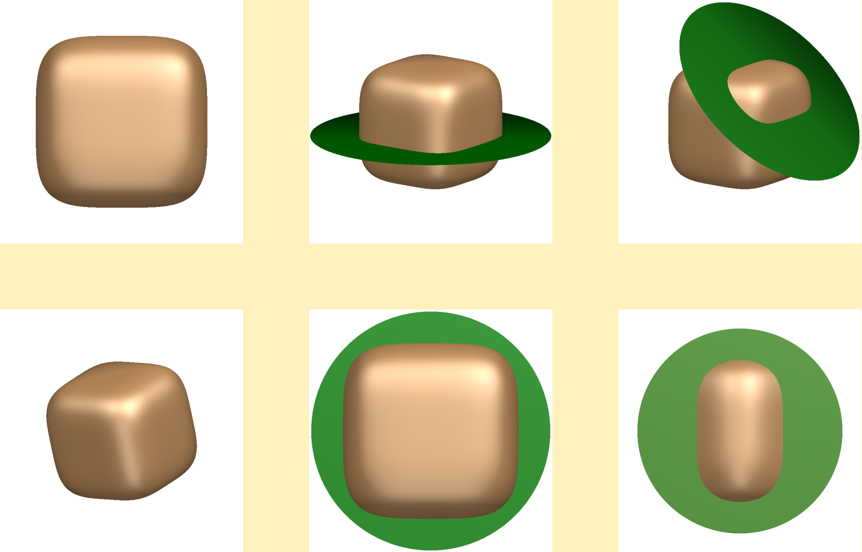




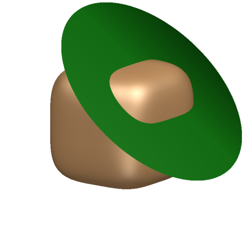
3-norm

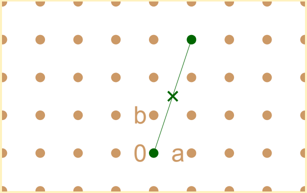


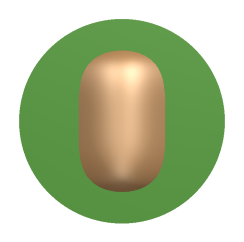
3-norm



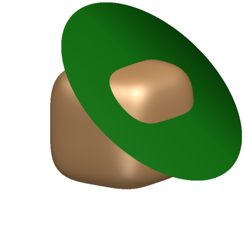
Rank 3

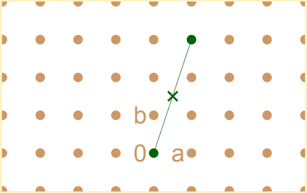




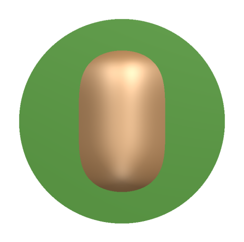


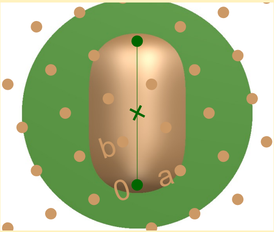
Rank 3

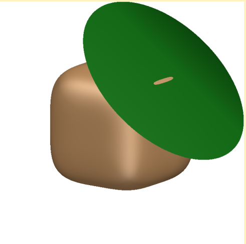


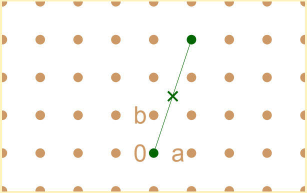


Rotate lattice s.t.

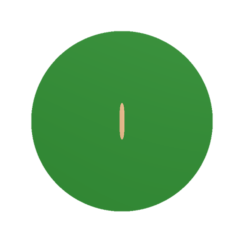


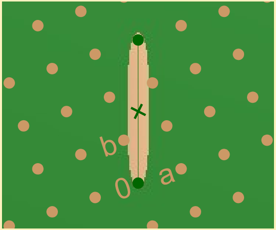




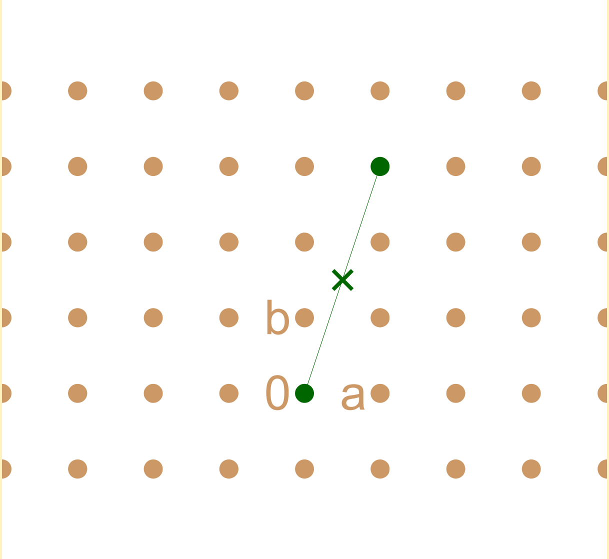


Rotate lattice s.t.

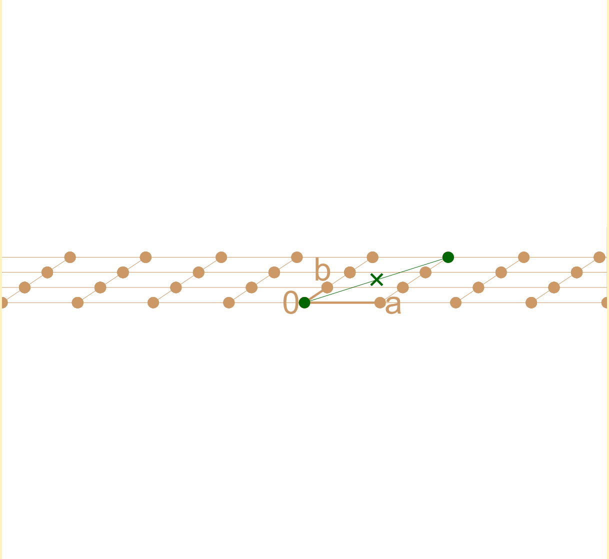




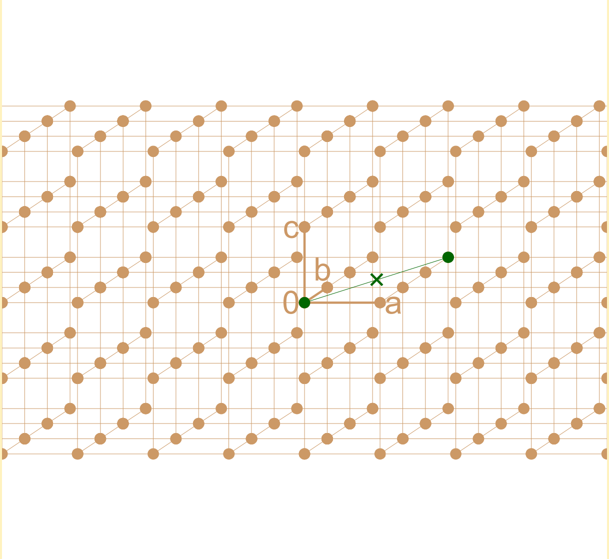
Modify standard lattice:



Modify standard lattice:



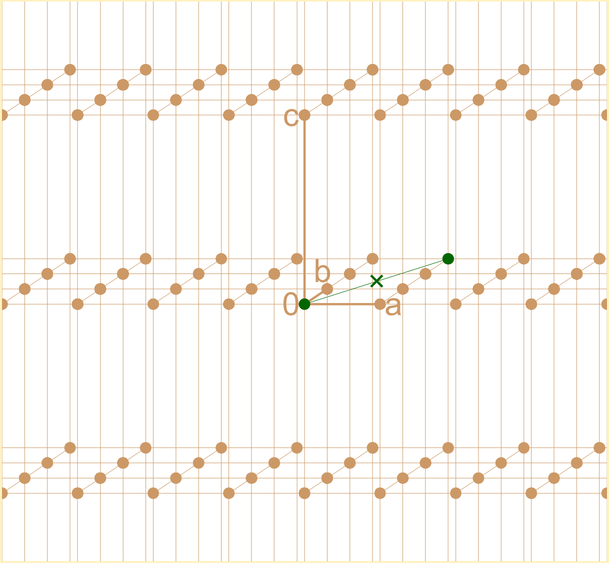
Modify standard lattice:



Rank 3

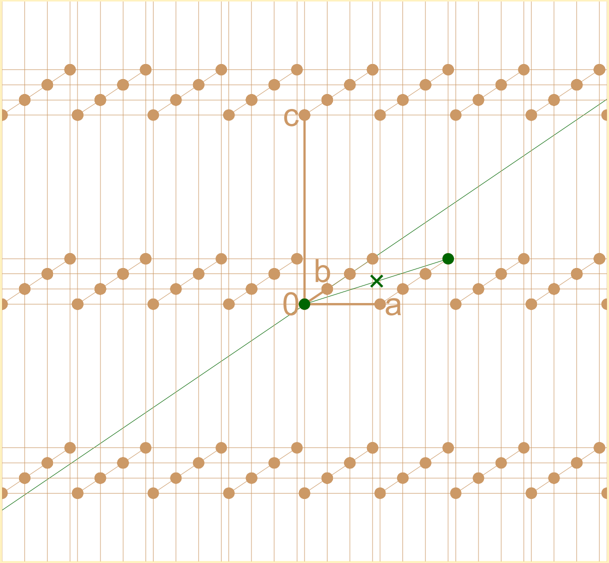
Modify standard lattice:

1. Stretch in c-direction by $5\sqrt{2}m^5$



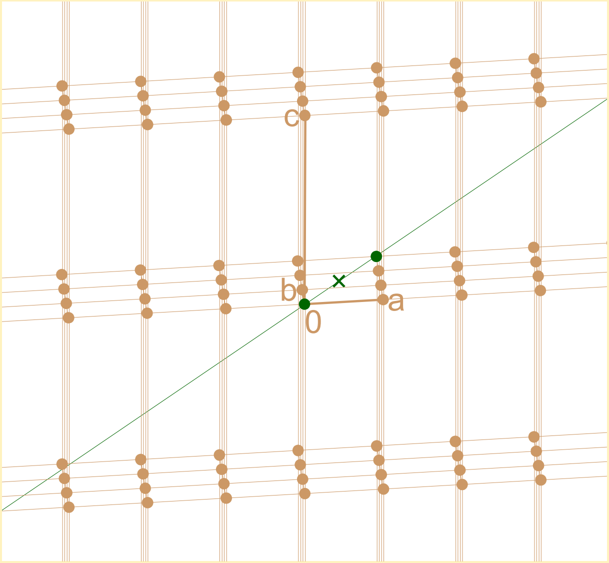
Modify standard lattice:

1. Stretch in c-direction by $5\sqrt{2}m^5$
2. Rotate around c-axis s.t. $a + mb$ lies on green axis



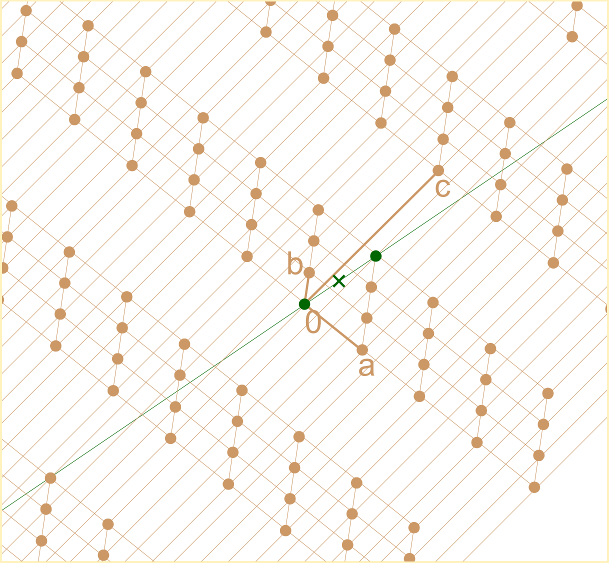
Modify standard lattice:

1. Stretch in c-direction by $5\sqrt{2}m^5$
2. Rotate around c-axis s.t. $a + mb$ lies on green axis



Modify standard lattice:

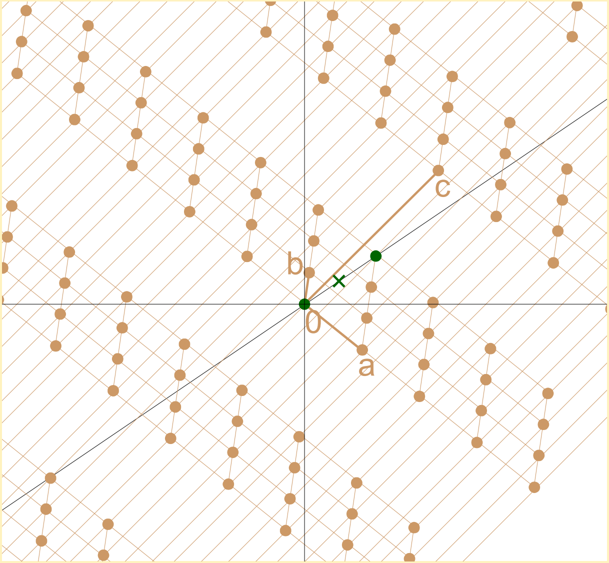
1. Stretch in c-direction by $5\sqrt{2}m^5$
2. Rotate around c-axis s.t. $a + mb$ lies on green axis
3. Rotate around green axis by 45°



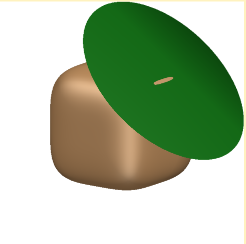
Modify standard lattice:

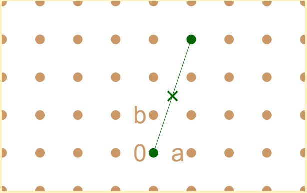
1. Stretch in c-direction by $5\sqrt{2}m^5$
2. Rotate around c-axis s.t. $a + mb$ lies on green axis
3. Rotate around green axis by 45°

$\Longrightarrow$ Lattice Λ_m

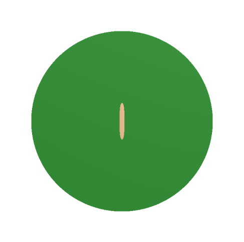


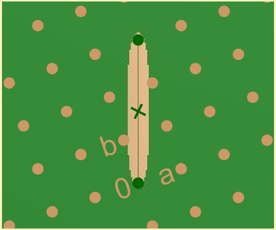
Rank 3



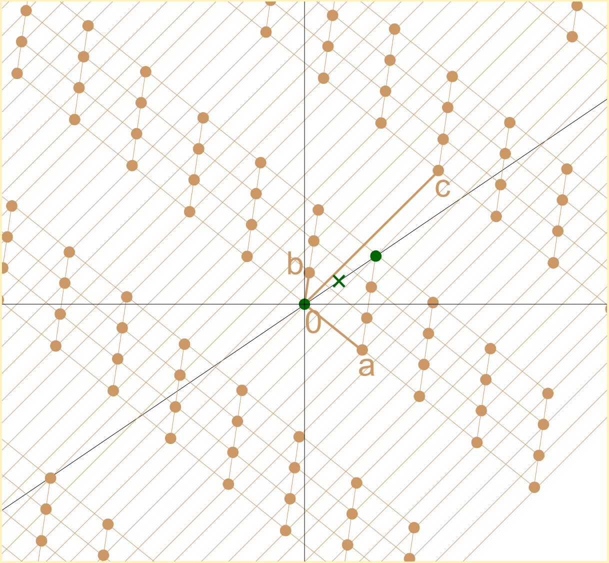


Rotate lattice s.t.





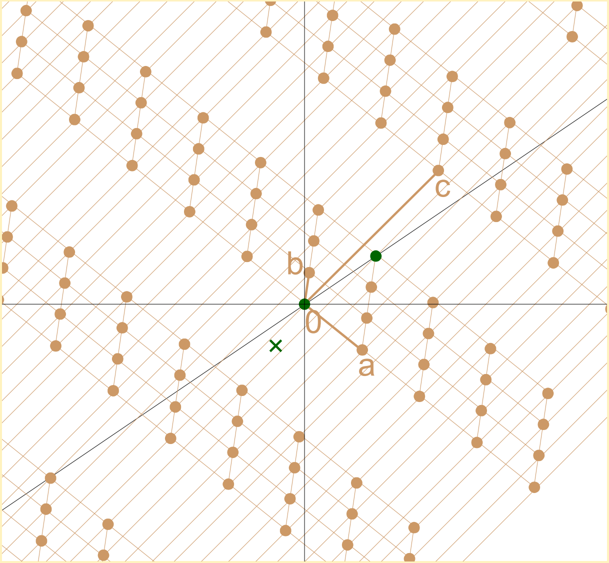
Λ_m:



Λ_m:

- Move x along c-direction

$\Longrightarrow a + mb$ Voronoi-rel. w.r.t. 3-norm



Λ_m:

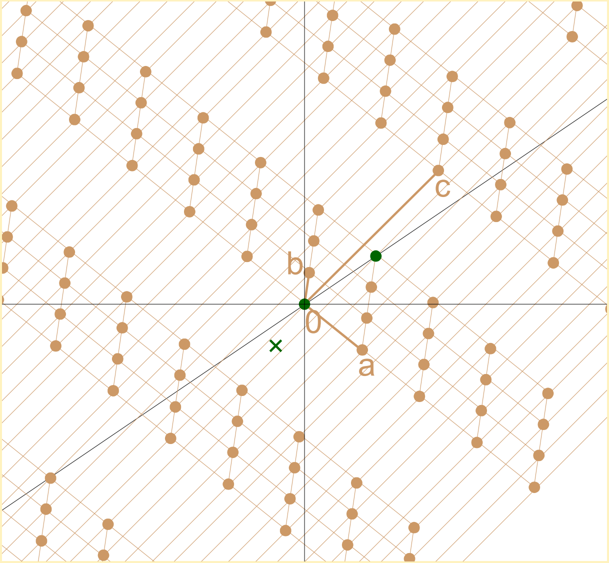
- Move x along c-direction

$\Longrightarrow$ $a + mb$ Voronoi-rel. w.r.t. 3-norm

- Analogous:

Theorem (K.)

For $2 \leq k \leq \sqrt{m}$, $a + kb$ is Voronoi-relevant in Λ_m w.r.t. 3-norm.



Corollary

Λ_m has $\Omega(\sqrt{m})$ Voronoi-relevant vectors w.r.t. 3-norm.

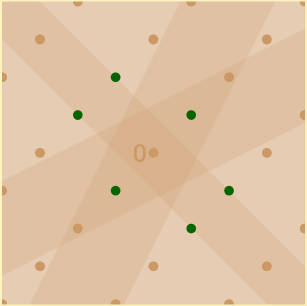
There is no upper bound for the number of Voronoi-relevant vectors

- **w.r.t. general strictly convex norms**
- **that depends only on the lattice dimension!**

Section 3

Non-strictly convex norms

Voronoi-relevant vectors



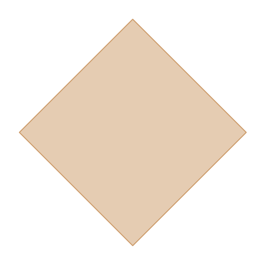
$$\mathcal{V}(\Lambda, \|\cdot\|_2) = \mathrm{span}(\Lambda) \cap \left(\bigcap_{v \in \Lambda \mathrm{VR}} \mathcal{H}^{\leq}_{\|\cdot\|_2}(0, v) \right)$$

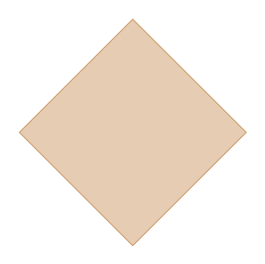
for Euclidean norm $\|\cdot\|_2$ [Agrell et al.]

Definition

$v \in \Lambda \setminus \{0\}$ is *Voronoi-relevant (VR)* w.r.t. $\|\cdot\|$ if

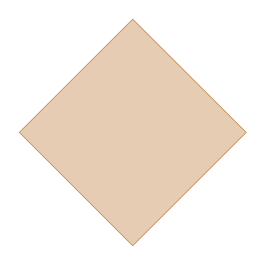
$$\exists x \in \mathrm{span}(\Lambda) : \|x\| = \|x - v\|,$$
$$\forall w \in \Lambda \setminus \{0, v\} : \|x\| < \|x - w\|.$$

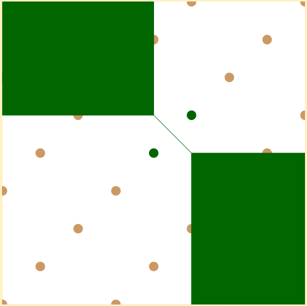




Definition

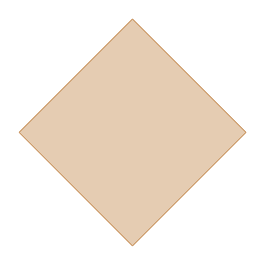
The *bisector* between $a, b \in \mathbb{R}^n$, $a \neq b$ is $\mathcal{H}^{=}_{\|\cdot\|}(a,b) := \{x \in \mathbb{R}^n \mid \|x-a\| = \|x-b\|\}$.





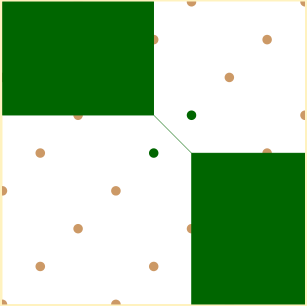
Definition

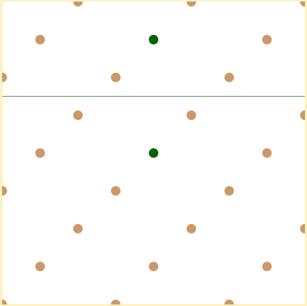
The *bisector* between $a, b \in \mathbb{R}^n$, $a \neq b$ is $\mathcal{H}^{=}_{\|\cdot\|}(a,b) := \{x \in \mathbb{R}^n \mid \|x-a\| = \|x-b\|\}$.

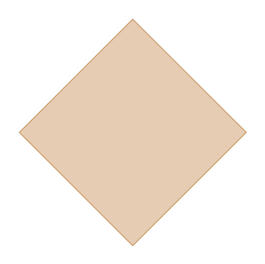


Definition

The *bisector* between $a, b \in \mathbb{R}^n$, $a \neq b$ is
$\mathcal{H}^{=}_{\|\cdot\|}(a,b) := \{x \in \mathbb{R}^n \mid \|x-a\| = \|x-b\|\}$.

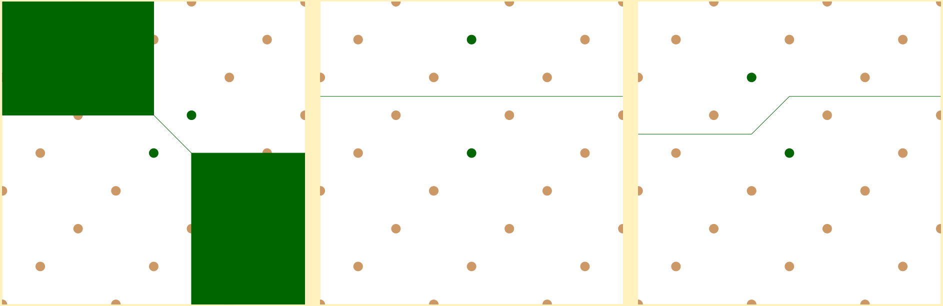


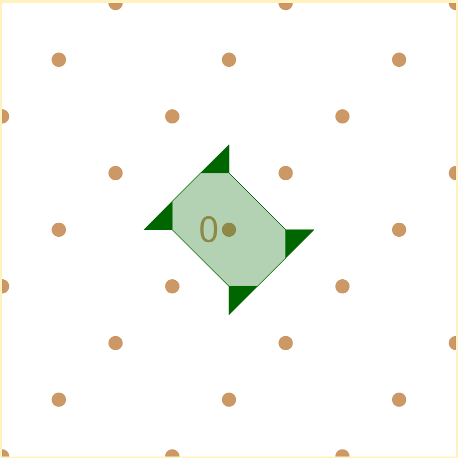


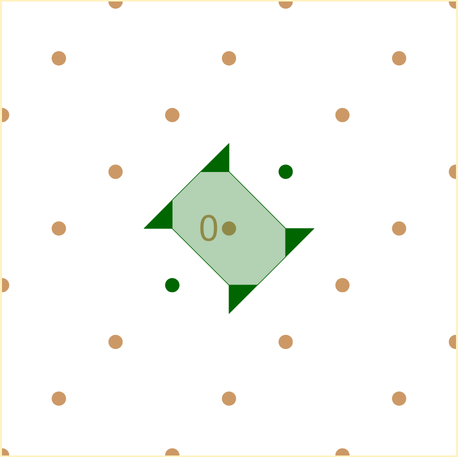


Definition

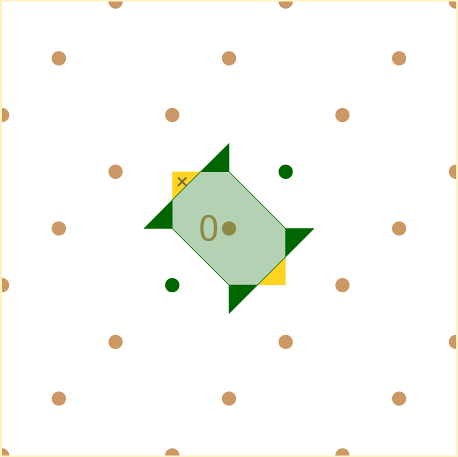
The *bisector* between $a, b \in \mathbb{R}^n$, $a \neq b$ is $\mathcal{H}^{=}_{\|\cdot\|}(a,b) := \{x \in \mathbb{R}^n \mid \|x-a\| = \|x-b\|\}$.



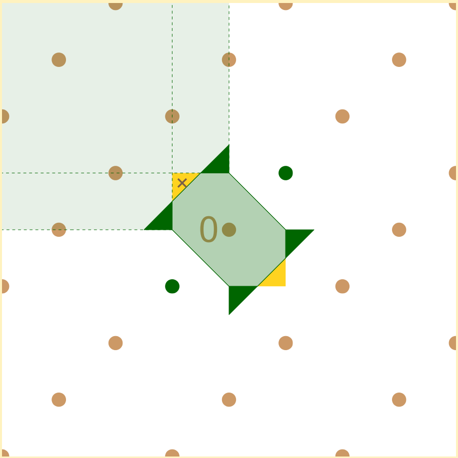

0



- 2 Voronoi-relevant vectors



- 2 Voronoi-relevant vectors
- x not in Voronoi-cell



- 2 Voronoi-relevant vectors
- x not in Voronoi-cell, BUT:
- x closer to 0 than to Voronoi-relevant vectors

Definition

$v \in \Lambda \setminus \{0\}$ is *Voronoi-relevant (VR)* w.r.t. $\|\cdot\|$ if

$$\exists x \in \mathrm{span}(\Lambda) : \|x\| = \|x - v\|,$$
$$\forall w \in \Lambda \setminus \{0, v\} : \|x\| < \|x - w\|.$$

Definition

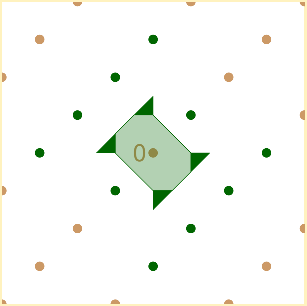
$v \in \Lambda \backslash \{0\}$ is *generalized Voronoi-relevant (GVR)* w.r.t. $\|\cdot\|$ if

$$\exists x \in \mathrm{span}(\Lambda) : \|x\| = \|x - v\|,$$
$$\forall w \in \Lambda : \|x\| \leq \|x - w\|.$$

Definition

$v \in \Lambda \backslash \{0\}$ is *generalized Voronoi-relevant (GVR)* w.r.t. $\|\cdot\|$ if

$$\exists x \in \text{span}(\Lambda) : \|x\| = \|x - v\|,$$
$$\forall w \in \Lambda : \|x\| \leq \|x - w\|.$$



Theorem (K.)

For every lattice Λ *and every norm* $\|\cdot\|$,

$$\mathcal{V}(\Lambda, \|\cdot\|) = \operatorname{span}(\Lambda) \cap \left(\bigcap_{v \in \Lambda GVR} \mathcal{H}^{\leq}_{\|\cdot\|}(0, v) \right).$$

Theorem (K.)

For every lattice Λ and every norm $\|\cdot\|$,

$$\mathcal{V}(\Lambda, \|\cdot\|) = \mathrm{span}(\Lambda) \cap \left(\bigcap_{v \in \Lambda GVR} \mathcal{H}^{\leq}_{\|\cdot\|}(0, v) \right).$$

Conjecture

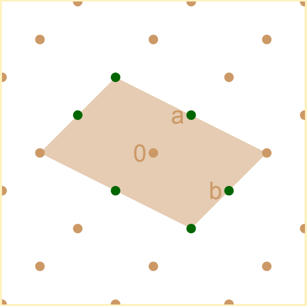
For every lattice Λ and every strictly convex norm $\|\cdot\|$,

$$\mathcal{V}(\Lambda, \|\cdot\|) = \mathrm{span}(\Lambda) \cap \left(\bigcap_{v \in \Lambda VR} \mathcal{H}^{\leq}_{\|\cdot\|}(0, v) \right).$$

Theorem (Blömer, K., Teusner)

Every lattice Λ of rank 2 has exactly 4 or 6 Voronoi-relevant vectors w.r.t. every strictly convex norm.

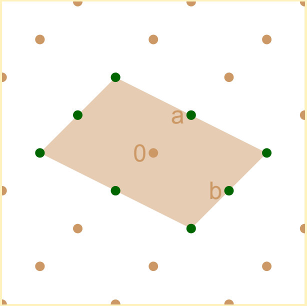
- Let $a, b \in \Lambda$ be shortest, linearly independent vectors
- $\pm a, \pm b$ are Voronoi-relevant
- at most 2 of $\{\pm(a+b), \pm(a-b)\}$ are Voronoi-relevant



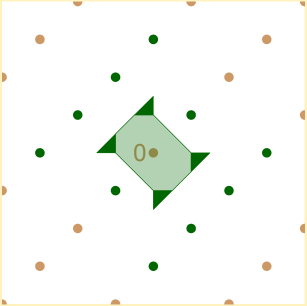
Theorem (Blömer, K., Teusner)

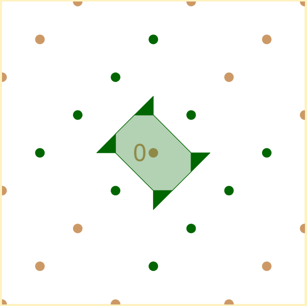
Every lattice Λ of rank 2 has at most 8 generalized Voronoi-relevant vectors w.r.t. every strictly convex norm.

- Let $a, b \in \Lambda$ be shortest, linearly independent vectors
- $\pm a, \pm b$ are Voronoi-relevant
- at most $\pm(a+b), \pm(a-b)$ are generalized Voronoi-relevant



Rank 2





$m = 3$

Theorem (K.)
$\mathcal{L}\left(\begin{pmatrix}1\\1\end{pmatrix},\begin{pmatrix}0\\m\end{pmatrix}\right)$ *has at least* $2m$ *generalized Voronoi-relevant vectors w.r.t. 1-norm.*

General upper bound

Proposition (K.)

Every n-dimensional lattice Λ has at most $\left(1 + 4\frac{\mu(\Lambda,\|\cdot\|)}{\lambda_1(\Lambda,\|\cdot\|)}\right)^n$ generalized Voronoi-relevant vectors w.r.t. every norm.

Definition

The *covering radius* of Λ w.r.t. $\|\cdot\|$ is

$$\mu(\Lambda, \|\cdot\|) := \inf\{d \in \mathbb{R}_{\geq 0} \mid \forall x \in \operatorname{span}(\Lambda)\, \exists v \in \Lambda : \|x - v\| \leq d\}.$$

The *first successive minimum* of Λ w.r.t. $\|\cdot\|$ is

$$\lambda_1(\Lambda, \|\cdot\|) := \inf\{\|v\| \mid v \in \Lambda, v \neq 0\}.$$

Section 4

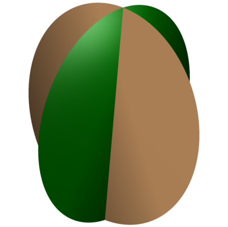
Bisectors

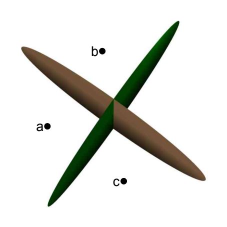
Theorem (Horváth)

For every strictly convex norm, every bisector is homeomorphic to a hyperplane.

Theorem (Ma)

For every strictly convex and smooth norm and every $a, b, c \in \mathbb{R}^3$ non-collinear, $\mathcal{H}^{=}_{\|\cdot\|}(a,b) \cap \mathcal{H}^{=}_{\|\cdot\|}(a,c)$ is homeomorphic to a line.

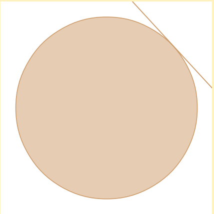


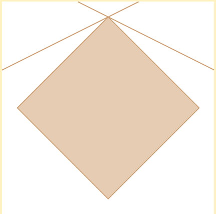


Definition

Let $S \subseteq \mathbb{R}^n$ and $s \in \partial S$. A hyperplane $H \in \mathbb{R}^n$ is a supporting hyperplane of S at s if

- $s \in H$ and
- S is contained in one of the 2 closed halfspaces bounded by H.

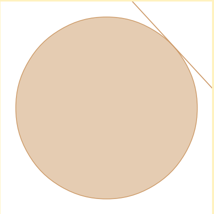


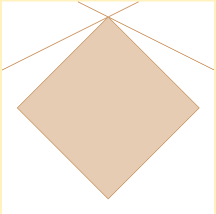


Definition

Let $S \subseteq \mathbb{R}^n$ and $s \in \partial S$. A hyperplane $H \in \mathbb{R}^n$ is a supporting hyperplane of S at s if

- $s \in H$ and
- S is contained in one of the 2 closed halfspaces bounded by H.

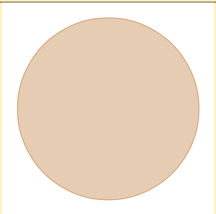
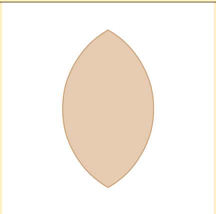
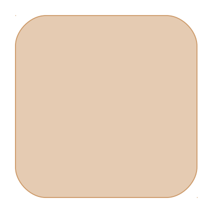
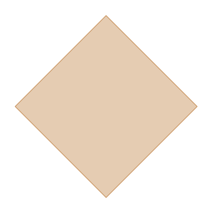




Definition

A norm is smooth if each point on its unit sphere has a unique supporting hyperplane.

Smooth norms

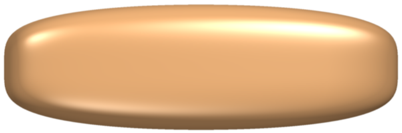
	smooth	not smooth
strictly convex		
not strictly convex		

Conjecture

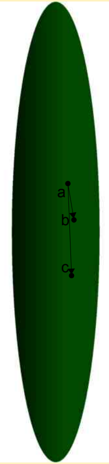
For every strictly convex and smooth norm and every $a, b, c \in \mathbb{R}^n$ *non-collinear,* $\mathcal{H}^{=}_{\|\cdot\|}(a, b) \cap \mathcal{H}^{=}_{\|\cdot\|}(a, c)$ *is homeomorphic to* $\mathbb{R}^{n-2}$*.*

Conjecture

For every strictly convex and smooth norm and every $a, b, c \in \mathbb{R}^n$ *non-collinear,* $\mathcal{H}^{=}_{\|\cdot\|}(a, b) \cap \mathcal{H}^{=}_{\|\cdot\|}(a, c)$ *is homeomorphic to* $\mathbb{R}^{n-2}$.

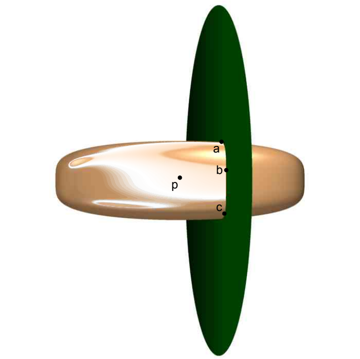


unit ball
$\mathcal{B}_{\|\cdot\|,1}(0) := \{x \in \mathbb{R}^n \mid \|x\| < 1\}$

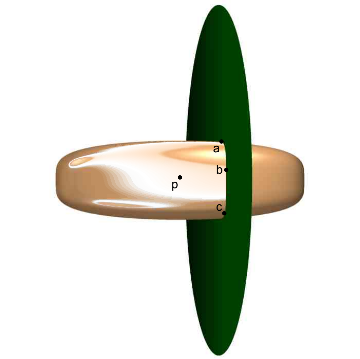


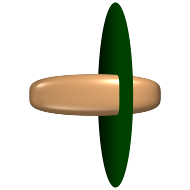
plane H
spanned by a, b, c

Intersection of bisectors



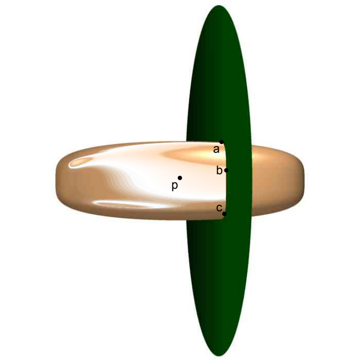
Intersection of bisectors

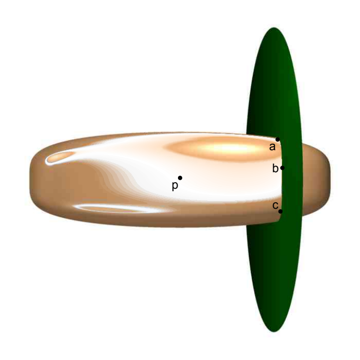




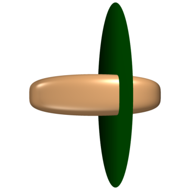
unit ball

Intersection of bisectors

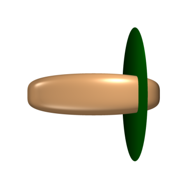




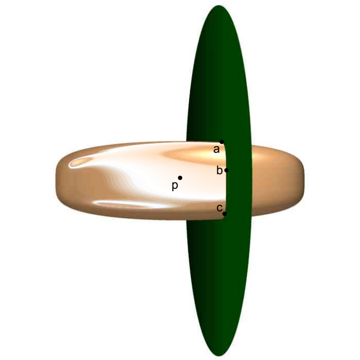
unit ball

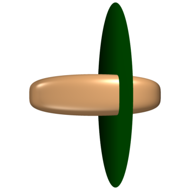


unit ball



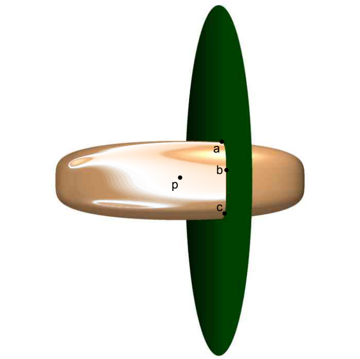
Intersection of bisectors





unit ball

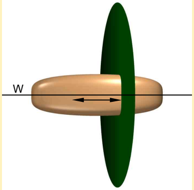
Intersection of bisectors



$W := (H - a)^{\perp}$ orthogonal complement

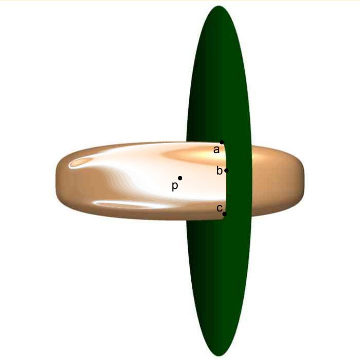
$\Longrightarrow \dim(W) = n - 2$

$\Longrightarrow \mathrm{proj}_W : \mathbb{R}^n = (H - a) \oplus W \to W$



unit ball

Intersection of bisectors

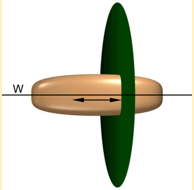


$W := (H - a)^{\perp}$ orthogonal complement

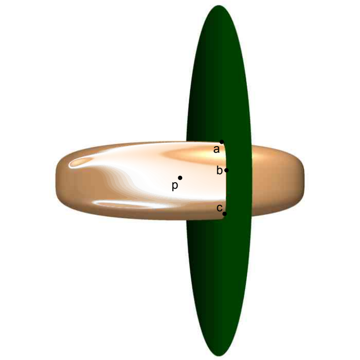
$\Longrightarrow \dim(W) = n - 2$

$\Longrightarrow \mathrm{proj}_W : \mathbb{R}^n = (H - a) \oplus W \to W$

$$p \mapsto \frac{a-p}{\|a-p\|}$$



unit ball

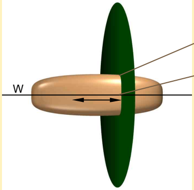


$W := (H - a)^{\perp}$ orthogonal complement

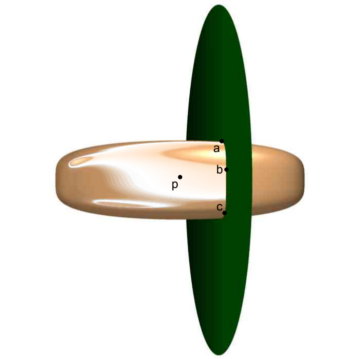
$\Longrightarrow \dim(W) = n - 2$

$\Longrightarrow \text{proj}_W : \mathbb{R}^n = (H - a) \oplus W \to W$

$$p \mapsto \frac{a-p}{\|a-p\|} \mapsto \text{proj}_W\left(\frac{a-p}{\|a-p\|}\right)$$



unit ball



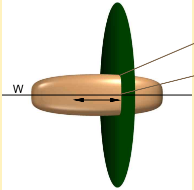
$W := (H - a)^{\perp}$ orthogonal complement

$\Longrightarrow \dim(W) = n - 2$

$\Longrightarrow \mathrm{proj}_W : \mathbb{R}^n = (H - a) \oplus W \to W$

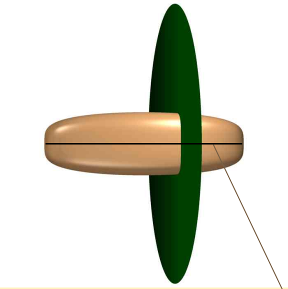
$$\varphi : \mathcal{H}^{=}_{\|\cdot\|}(a, b) \cap \mathcal{H}^{=}_{\|\cdot\|}(a, c) \to W$$

$$p \mapsto \frac{a-p}{\|a-p\|} \mapsto \mathrm{proj}_W\left(\frac{a-p}{\|a-p\|}\right)$$



unit ball

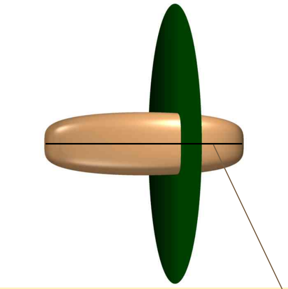
Intersection of bisectors



$$\varphi : \mathcal{H}^{=}_{\|\cdot\|}(a,b) \cap \mathcal{H}^{=}_{\|\cdot\|}(a,c) \longrightarrow \mathrm{proj}_W\left(\mathcal{B}_{\|\cdot\|,1}(0)\right),$$

$$x \longmapsto \mathrm{proj}_W\left(\frac{a-p}{\|a-p\|}\right)$$

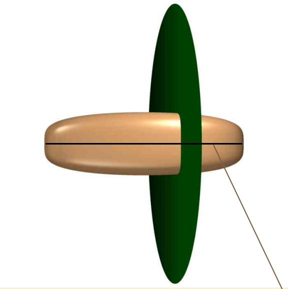
Intersection of bisectors



$$\varphi : \mathcal{H}^{=}_{\|\cdot\|}(a,b) \cap \mathcal{H}^{=}_{\|\cdot\|}(a,c) \longrightarrow \mathrm{proj}_W\left(\mathcal{B}_{\|\cdot\|,1}(0)\right),$$
$$x \longmapsto \mathrm{proj}_W\left(\frac{a-p}{\|a-p\|}\right)$$

$\Longrightarrow \varphi$ continuous bijection

Intersection of bisectors



$$\varphi : \mathcal{H}^{=}_{\|\cdot\|}(a,b) \cap \mathcal{H}^{=}_{\|\cdot\|}(a,c) \longrightarrow \mathrm{proj}_W \left(\mathcal{B}_{\|\cdot\|,1}(0)\right),$$

$$x \longmapsto \mathrm{proj}_W \left(\frac{a-p}{\|a-p\|}\right)$$

$\Longrightarrow$ φ continuous bijection

Conjecture

φ^{-1} *continuous*

- $\mathrm{proj}_W\left(\mathcal{B}_{\|\cdot\|,1}(0)\right)$ is open unit ball of some norm on W

Intersection of bisectors

- $\mathrm{proj}_W\left(\mathcal{B}_{\|\cdot\|,1}(0)\right)$ is open unit ball of some norm on W
- For every norm F on subspace $V \subseteq \mathbb{R}^n$, $\mathcal{B}_{F,1}(0)$ is homeomorphic to V

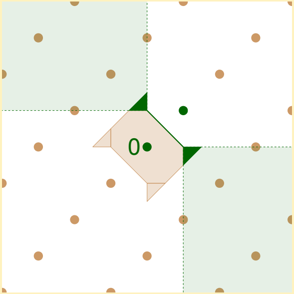
- $\text{proj}_W\left(\mathcal{B}_{\|\cdot\|,1}(0)\right)$ is open unit ball of some norm on W
- For every norm F on subspace $V \subseteq \mathbb{R}^n$, $\mathcal{B}_{F,1}(0)$ is homeomorphic to V

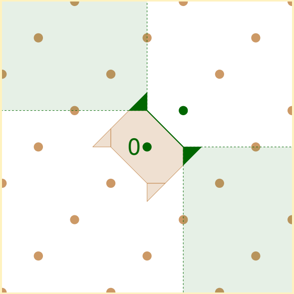
$\Longrightarrow$ $\text{proj}_W\left(\mathcal{B}_{\|\cdot\|,1}(0)\right)$ homeomorphic to W

Definition

$\mathcal{F} \subseteq \mathcal{V}(\Lambda, \|\cdot\|)$ facet if

1. $\exists v \in \Lambda \backslash \{0\} : \mathcal{F} \subseteq \mathcal{H}^{=}_{\|\cdot\|}(0, v)$
2. $\mathcal{F}$ at least $(m-1)$-dimensional for $m := \operatorname{rank}(\Lambda)$
3. $\mathcal{F}$ is "maximal"

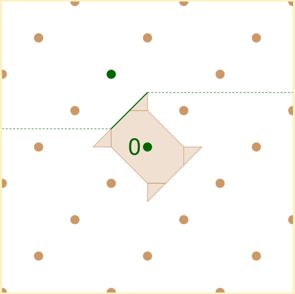




Definition

$\mathcal{F} \subseteq \mathcal{V}(\Lambda, \|\cdot\|)$ facet if

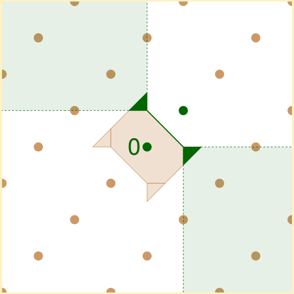
1. $\exists v \in \Lambda \setminus \{0\} : \mathcal{F} \subseteq \mathcal{H}^{=}_{\|\cdot\|}(0, v)$
2. $\mathcal{F}$ at least $(m-1)$-dimensional for $m := \operatorname{rank}(\Lambda)$
3. $\mathcal{F}$ is "maximal"

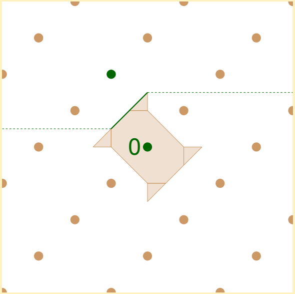


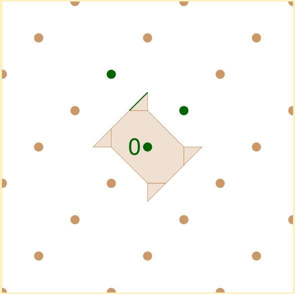
Definition

$\mathcal{F} \subseteq \mathcal{V}(\Lambda, \|\cdot\|)$ facet if

1. $\exists v \in \Lambda \setminus \{0\} : \mathcal{F} \subseteq \mathcal{H}^{=}_{\|\cdot\|}(0, v)$
2. $\mathcal{F}$ at least $(m-1)$-dimensional for $m := \mathrm{rank}(\Lambda)$
3. $\mathcal{F}$ is "maximal"



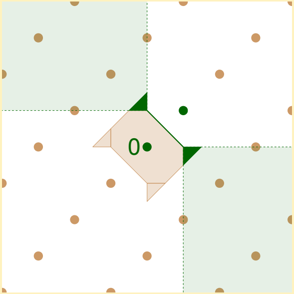


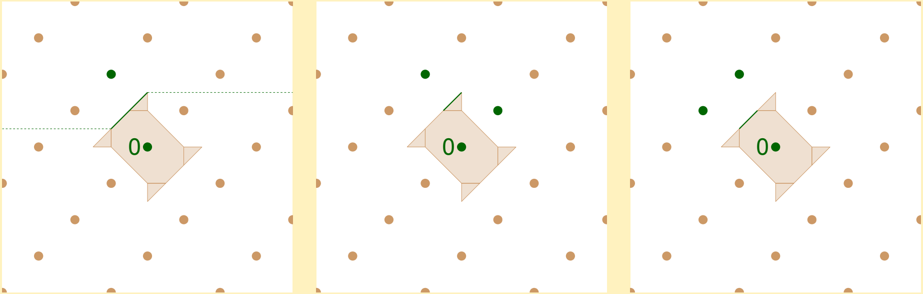


Definition

$\mathcal{F} \subseteq \mathcal{V}(\Lambda, \|\cdot\|)$ facet if

1. $\exists v \in \Lambda \setminus \{0\} : \mathcal{F} \subseteq \mathcal{H}^{=}_{\|\cdot\|}(0, v)$
2. $\mathcal{F}$ at least $(m-1)$-dimensional for $m := \text{rank}(\Lambda)$
3. $\mathcal{F}$ is "maximal"





Facets

- v Voronoi-relevant $\Rightarrow \mathcal{V}(\Lambda, \|\cdot\|) \cap \mathcal{H}^{=}_{\|\cdot\|}(0, v)$ facet

Facets

- v Voronoi-relevant $\Rightarrow \mathcal{V}(\Lambda, \|\cdot\|) \cap \mathcal{H}^{=}_{\|\cdot\|}(0, v)$ facet
- Λ 2-dimensional, strictly convex norm
  - every facet has above form

Facets

- v Voronoi-relevant $\Rightarrow \mathcal{V}(\Lambda, \|\cdot\|) \cap \mathcal{H}^{=}_{\|\cdot\|}(0, v)$ facet
- Λ 2-dimensional, strictly convex norm
  - every facet has above form
    $\Longrightarrow$ bijection between Voronoi-relevant vectors and facets

Facets

- v Voronoi-relevant $\Rightarrow \mathcal{V}(\Lambda, \|\cdot\|) \cap \mathcal{H}^{=}_{\|\cdot\|}(0, v)$ facet
- Λ 2-dimensional, strictly convex norm
  - every facet has above form
    $\Longrightarrow$ bijection between Voronoi-relevant vectors and facets
  - every facet is connected

- v Voronoi-relevant $\Rightarrow \mathcal{V}(\Lambda, \|\cdot\|) \cap \mathcal{H}^{=}_{\|\cdot\|}(0, v)$ facet
- Λ 2-dimensional, strictly convex norm
  - every facet has above form
    $\Longrightarrow$ bijection between Voronoi-relevant vectors and facets
  - every facet is connected
- general dimension, strictly convex and smooth norm

Conjecture

For every strictly convex and smooth norm and every $a, b, c \in \mathbb{R}^n$ non-collinear, $\mathcal{H}^{=}_{\|\cdot\|}(a, b) \cap \mathcal{H}^{=}_{\|\cdot\|}(a, c)$ is homeomorphic to $\mathbb{R}^{n-2}$.

Facets

- v Voronoi-relevant $\Rightarrow \mathcal{V}(\Lambda, \|\cdot\|) \cap \mathcal{H}^{=}_{\|\cdot\|}(0, v)$ facet
- Λ 2-dimensional, strictly convex norm
  - every facet has above form
    $\Longrightarrow$ bijection between Voronoi-relevant vectors and facets
  - every facet is connected
- general dimension, strictly convex and smooth norm
  - **If conjecture below is true:** every facet has above form
    $\Longrightarrow$ bijection between Voronoi-relevant vectors and facets

Conjecture

For every strictly convex and smooth norm and every $a, b, c \in \mathbb{R}^n$ non-collinear, $\mathcal{H}^{=}_{\|\cdot\|}(a, b) \cap \mathcal{H}^{=}_{\|\cdot\|}(a, c)$ is homeomorphic to $\mathbb{R}^{n-2}$.

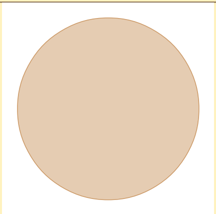
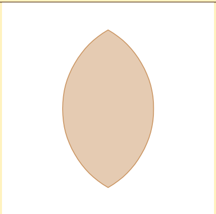
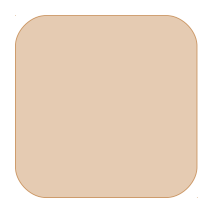
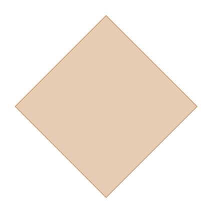
- v Voronoi-relevant $\Rightarrow \mathcal{V}(\Lambda, \|\cdot\|) \cap \mathcal{H}^{=}_{\|\cdot\|}(0, v)$ facet
- Λ 2-dimensional, strictly convex norm
  - every facet has above form
    $\Longrightarrow$ bijection between Voronoi-relevant vectors and facets
  - every facet is connected
- general dimension, strictly convex and smooth norm
  - **If conjecture below is true:** every facet has above form
    $\Longrightarrow$ bijection between Voronoi-relevant vectors and facets
  - facets probably not necessarily connected
    $\forall p \in \mathbb{N}, p \geq 3\ \exists a, b, c, d \in \mathbb{R}^3$: Voronoi diagram of a, b, c, d w.r.t. p-norm has unconnected facet

Conjecture

For every strictly convex and smooth norm and every $a, b, c \in \mathbb{R}^n$ non-collinear, $\mathcal{H}^{=}_{\|\cdot\|}(a, b) \cap \mathcal{H}^{=}_{\|\cdot\|}(a, c)$ is homeomorphic to $\mathbb{R}^{n-2}$.

Thank you!

Smooth norms

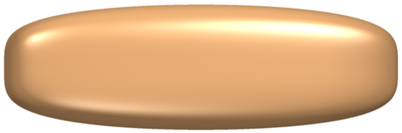
	smooth	not smooth
strictly convex		
not strictly convex		

Conjecture

For every strictly convex and smooth norm and every $a, b, c \in \mathbb{R}^n$ *non-collinear,* $\mathcal{H}^{=}_{\|\cdot\|}(a, b) \cap \mathcal{H}^{=}_{\|\cdot\|}(a, c)$ *is homeomorphic to* $\mathbb{R}^{n-2}$*.*

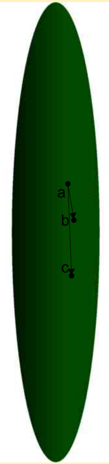
Conjecture

For every strictly convex and smooth norm and every $a, b, c \in \mathbb{R}^n$ *non-collinear,* $\mathcal{H}^{=}_{\|\cdot\|}(a,b) \cap \mathcal{H}^{=}_{\|\cdot\|}(a,c)$ *is homeomorphic to* $\mathbb{R}^{n-2}$*.*



unit ball

$\mathcal{B}_{\|\cdot\|,1}(0) := \{x \in \mathbb{R}^n \mid \|x\| < 1\}$

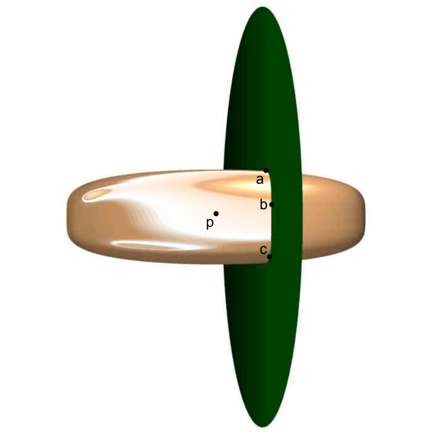


plane H

spanned by a, b, c

Conjecture

For every strictly convex and smooth norm and every $a, b, c \in \mathbb{R}^n$ non-collinear, $\mathcal{H}^{=}_{\|\cdot\|}(a,b) \cap \mathcal{H}^{=}_{\|\cdot\|}(a,c)$ is homeomorphic to $\mathbb{R}^{n-2}$.



Thank you!