Les deux réductions de Voronoi et leur application aux équations aux dérivées partielles

Jean-Marie Mirebeau

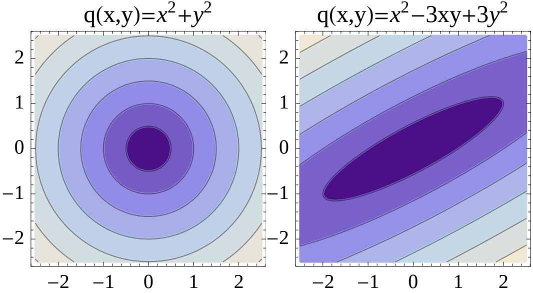
University Paris Sud, CNRS, University Paris-Saclay

May 4, 2017

Collège de France, cours de J.-D. Boissonnat

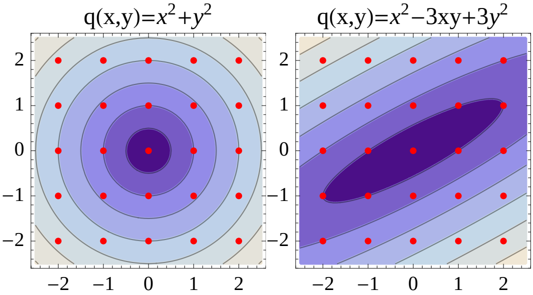
Réseaux et formes quadratiques

- Une forme quadratique est un polynôme homogène de degré 2, en d variables.
  On limite notre attention aux formes définies positives.



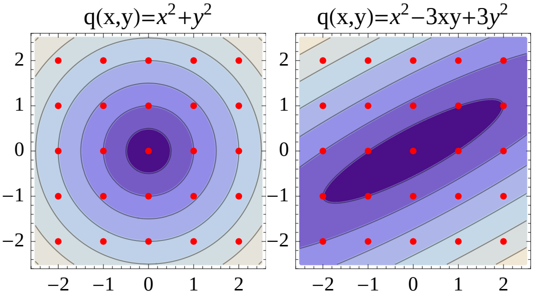
Réseaux et formes quadratiques

- Une forme quadratique est un polynôme homogène de degré 2, en d variables.
  On limite notre attention aux formes définies positives.
- Un réseau est un sous ensemble de $\mathbb{R}^d$, discret et stable par addition/soustraction. *On limite notre attention à $\mathbb{Z}^d$.*



Réseaux et formes quadratiques

- Une forme quadratique est un polynôme homogène de degré 2, en d variables.
  On limite notre attention aux formes définies positives.
- Un réseau est un sous ensemble de $\mathbb{R}^d$, discret et stable par addition/soustraction. *On limite notre attention à $\mathbb{Z}^d$.*



- Lagrange (1770), étudie $q(x) := x_1^2 + \cdots + x_4^2$ sur $\mathbb{Z}^4$
  "Tout entier positif est somme de quatre carrés".

La notation matricielle

- Une forme quadratique sur $\mathbb{R}^d$

$$q(x) = \sum_{1 \leq i,j \leq d} m_{ij} x_i x_j$$

s'écrit matriciellement

$$q(x) = \boldsymbol{x}^{\mathrm{T}} M \boldsymbol{x} \quad \text{où } M = \begin{pmatrix} m_{11} & \cdots & m_{1d} \\ \vdots & \ddots & \vdots \\ m_{d1} & \cdots & m_{dd} \end{pmatrix} \quad \text{et } \boldsymbol{x} = \begin{pmatrix} x_1 \\ \vdots \\ x_d \end{pmatrix}$$

La notation matricielle

- Une forme quadratique sur $\mathbb{R}^d$

$$q(x) = \sum_{1 \leq i,j \leq d} m_{ij} x_i x_j$$

s'écrit matriciellement

$$q(x) = \boldsymbol{x}^{\mathrm{T}} M \boldsymbol{x} \quad \text{où } M = \begin{pmatrix} m_{11} & \cdots & m_{1d} \\ \vdots & \ddots & \vdots \\ m_{d1} & \cdots & m_{dd} \end{pmatrix} \quad \text{et } \boldsymbol{x} = \begin{pmatrix} x_1 \\ \vdots \\ x_d \end{pmatrix}$$

- On note S_d^{++} l'ensemble des matrices symétriques qui définissent des formes quadratiques définies positives.

La notation matricielle

- Une forme quadratique sur $\mathbb{R}^d$

$$q(x) = \sum_{1 \leq i,j \leq d} m_{ij} x_i x_j$$

s'écrit matriciellement

$$q(x) = \boldsymbol{x}^{\mathrm{T}} M \boldsymbol{x} \quad \text{où } M = \begin{pmatrix} m_{11} & \cdots & m_{1d} \\ \vdots & \ddots & \vdots \\ m_{d1} & \cdots & m_{dd} \end{pmatrix} \quad \text{et } \boldsymbol{x} = \begin{pmatrix} x_1 \\ \vdots \\ x_d \end{pmatrix}$$

- On note S_d^{++} l'ensemble des matrices symétriques qui définissent des formes quadratiques définies positives.
- On pose $\|\boldsymbol{x}\|_M := \sqrt{\boldsymbol{x}^{\mathrm{T}} M \boldsymbol{x}}$.

$$q(x,y) = x^2 + y^2 \Leftrightarrow M = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$q(x,y) = x^2 - 3xy + 3y^2 \Leftrightarrow M = \begin{pmatrix} 1 & -3/2 \\ -3/2 & 3 \end{pmatrix}$$

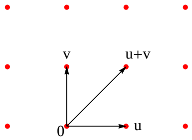
Les changements de coordonnées

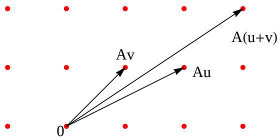
- Un changement de linéaire coordonnés dans $\mathbb{R}^d$ s'écrit

$$x'_i = \sum_{j=1}^{n} a_{ij} x_j,$$

pour tout $1 \leq i \leq d$. Matriciellement

$$x' = Ax, \text{ où } A = \begin{pmatrix} a_{11} & \cdots & a_{1d} \\ \vdots & \ddots & \vdots \\ a_{d1} & \cdots & a_{dd} \end{pmatrix} \text{ et } \boldsymbol{x} = \begin{pmatrix} x_1 \\ \vdots \\ x_d \end{pmatrix}$$





$$A = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}$$

Les changements de coordonnées

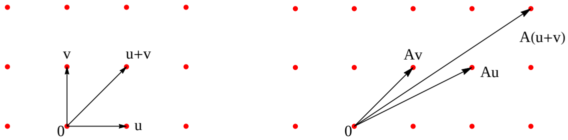
- Un changement de linéaire coordonnés dans $\mathbb{R}^d$ s'écrit

$$x_i' = \sum_{j=1}^{n} a_{ij} x_j,$$

pour tout $1 \leq i \leq d$. Matriciellement

$$x' = Ax, \text{ où } A \quad = \begin{pmatrix} a_{11} & \cdots & a_{1d} \\ \vdots & \ddots & \vdots \\ a_{d1} & \cdots & a_{dd} \end{pmatrix} \text{ et } \boldsymbol{x} \quad = \begin{pmatrix} x_1 \\ \vdots \\ x_d \end{pmatrix}$$

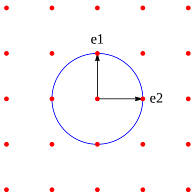
- On note $\mathrm{GL}_d(\mathbb{Z})$ l'ensemble des matrices qui induisent une bijection de $\mathbb{Z}^d$ dans lui-même.

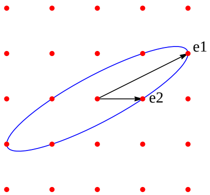


$$A = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}$$

La réduction de Minkowski.

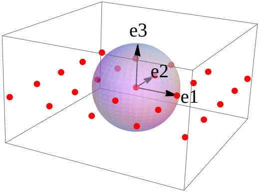
- Minkowski associe à $M \in \mathrm{S}_d^{++}$ la base $(\boldsymbol{e}_0, \cdots, \boldsymbol{e}_d)$ de $\mathbb{Z}^d$ telle que:
  - $(\|\boldsymbol{e}_1\|_M, \cdots, \|\boldsymbol{e}_d\|_M)$ est minimal, pour l'ordre lexicographique.
  - $\langle \boldsymbol{e}_i, \boldsymbol{e}_{i+1} \rangle_M \geq 0$ pour tout $i < d$.

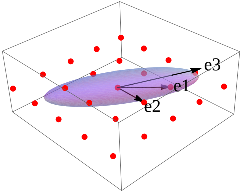




La réduction de Minkowski.

- Minkowski associe à $M \in \mathrm{S}_d^{++}$ la base $(\boldsymbol{e}_0, \cdots, \boldsymbol{e}_d)$ de $\mathbb{Z}^d$ telle que:
  - $(\|\boldsymbol{e}_1\|_M, \cdots, \|\boldsymbol{e}_d\|_M)$ est minimal, pour l'ordre lexicographique.
  - $\langle \boldsymbol{e}_i, \boldsymbol{e}_{i+1} \rangle_M \geq 0$ pour tout $i < d$.

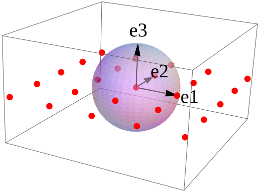


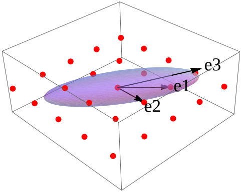


- $\boldsymbol{e}_1$ est le plus court vecteur non-nul de $\mathbb{Z}^d$ pour $\|\cdot\|_M$. Son calcul est NP-Complet en dimension arbitraire, (van Emde Boas, 1981)

La réduction de Minkowski.

- Minkowski associe à $M \in \mathrm{S}_d^{++}$ la base $(\boldsymbol{e}_0, \cdots, \boldsymbol{e}_d)$ de $\mathbb{Z}^d$ telle que:
  - $(\|\boldsymbol{e}_1\|_M, \cdots, \|\boldsymbol{e}_d\|_M)$ est minimal, pour l'ordre lexicographique.
  - $\langle \boldsymbol{e}_i, \boldsymbol{e}_{i+1} \rangle_M \geq 0$ pour tout $i < d$.





- $\boldsymbol{e}_1$ est le plus court vecteur non-nul de $\mathbb{Z}^d$ pour $\|\cdot\|_M$. Son calcul est NP-Complet en dimension arbitraire, (van Emde Boas, 1981)
- Cette base, dite M-réduite, est génériquement unique à un changement global de signe près.

Le domaine fondamental

- On note $\mathcal{M}_d^+$ l'ensemble des $M \in \mathrm{S}_d^{++}$ pour lesquelles la base canonique est réduite au sens de Minkowski.

Theorem (Minkowski,1905)

L'ensemble $\overline{\mathcal{M}_d^+}$ est un cône polyhédral. De plus, pour toute $M \in \mathrm{S}_d^{++}$, il existe $A \in \mathrm{GL}_d(\mathbb{Z})$ telle que $(A^{-1})^{\mathrm{T}} M A^{-1} \in \mathcal{M}_d^+$.

Le domaine fondamental

- On note $\mathcal{M}_d^+$ l'ensemble des $M \in \mathrm{S}_d^{++}$ pour lesquelles la base canonique est réduite au sens de Minkowski.

Theorem (Minkowski,1905)

L'ensemble $\overline{\mathcal{M}_d^+}$ est un cône polyhédral. De plus, pour toute $M \in \mathrm{S}_d^{++}$, il existe $A \in \mathrm{GL}_d(\mathbb{Z})$ telle que $(A^{-1})^{\mathrm{T}} M A^{-1} \in \mathcal{M}_d^+$.

- $A = A(M)$ est la matrice de colonnes la base M-réduite.

Le domaine fondamental

- On note $\mathcal{M}_d^+$ l'ensemble des $M \in \mathrm{S}_d^{++}$ pour lesquelles la base canonique est réduite au sens de Minkowski.

Theorem (Minkowski,1905)

L'ensemble $\overline{\mathcal{M}_d^+}$ est un cône polyhédral. De plus, pour toute $M \in \mathrm{S}_d^{++}$, il existe $A \in \mathrm{GL}_d(\mathbb{Z})$ telle que $(A^{-1})^{\mathrm{T}} M A^{-1} \in \mathcal{M}_d^+$.

- $A = A(M)$ est la matrice de colonnes la base M-réduite.
- Les inégalités linéaires minimales caractérisant $\mathcal{M}_d^+$ sont établies par Minkowski en dimension $d \leq 6$,

Le domaine fondamental

- On note $\mathcal{M}_d^+$ l'ensemble des $M \in \mathrm{S}_d^{++}$ pour lesquelles la base canonique est réduite au sens de Minkowski.

Theorem (Minkowski,1905)

L'ensemble $\overline{\mathcal{M}_d^+}$ est un cône polyhédral. De plus, pour toute $M \in \mathrm{S}_d^{++}$, il existe $A \in \mathrm{GL}_d(\mathbb{Z})$ telle que $(A^{-1})^{\mathrm{T}} M A^{-1} \in \mathcal{M}_d^+$.

- $A = A(M)$ est la matrice de colonnes la base M-réduite.
- Les inégalités linéaires minimales caractérisant $\mathcal{M}_d^+$ sont établies par Minkowski en dimension $d \leq 6$, puis étendues pour $d = 7$ (Tammela, 1977).

Le domaine fondamental

- On note $\mathcal{M}_d^+$ l'ensemble des $M \in \mathrm{S}_d^{++}$ pour lesquelles la base canonique est réduite au sens de Minkowski.

Theorem (Minkowski,1905)

L'ensemble $\overline{\mathcal{M}_d^+}$ est un cône polyhédral. De plus, pour toute $M \in \mathrm{S}_d^{++}$, il existe $A \in \mathrm{GL}_d(\mathbb{Z})$ telle que $(A^{-1})^{\mathrm{T}} M A^{-1} \in \mathcal{M}_d^+$.

- $A = A(M)$ est la matrice de colonnes la base M-réduite.
- Les inégalités linéaires minimales caractérisant $\mathcal{M}_d^+$ sont établies par Minkowski en dimension $d \leq 6$, puis étendues pour $d = 7$ (Tammela, 1977). Les rayons extrémaux du cône $\mathcal{M}_d^+$ sont connus pour $d \leq 5$. (Schurmann, 2009)

- Considérons $M \in \mathcal{M}_2^+$, $M = \begin{pmatrix} a & b \\ b & c \end{pmatrix}$. Alors

$$\begin{aligned} \|\boldsymbol{e}_1\|_M \leq \|\boldsymbol{e}_2\|_M \quad &\Rightarrow \quad 0 \leq a \leq c, \\ \geq \|\boldsymbol{e}_2\|_M \end{aligned}$$

- Considérons $M \in \mathcal{M}_2^+$, $M = \begin{pmatrix} a & b \\ b & c \end{pmatrix}$. Alors

$$\|\mathbf{e}_1\|_M \leq \|\mathbf{e}_2\|_M \quad \Rightarrow \quad 0 \leq a \leq c,$$

$$\forall k \in \mathbb{Z}, \|\mathbf{e}_2 + k\mathbf{e}_1\|_M \geq \|\mathbf{e}_2\|_M$$

- Considérons $M \in \mathcal{M}_2^+$, $M = \begin{pmatrix} a & b \\ b & c \end{pmatrix}$. Alors

$$\begin{aligned} \|\boldsymbol{e}_1\|_M \leq \|\boldsymbol{e}_2\|_M \quad &\Rightarrow \quad 0 \leq a \leq c, \\ \|\boldsymbol{e}_2 - \boldsymbol{e}_1\|_M \geq \|\boldsymbol{e}_2\|_M \quad &\Rightarrow \quad 2b \leq a, \end{aligned}$$

- Considérons $M \in \mathcal{M}_2^+$, $M = \begin{pmatrix} a & b \\ b & c \end{pmatrix}$. Alors

$$\begin{aligned} \|\boldsymbol{e}_1\|_M \leq \|\boldsymbol{e}_2\|_M \quad &\Rightarrow \quad 0 \leq a \leq c, \\ \|\boldsymbol{e}_2 - \boldsymbol{e}_1\|_M \geq \|\boldsymbol{e}_2\|_M \quad &\Rightarrow \quad 2b \leq a, \\ \langle \boldsymbol{e}_1, \boldsymbol{e}_2 \rangle_M \geq 0 \quad &\Rightarrow \quad b \geq 0. \end{aligned}$$

Les inégalités de droite caractérisent $\overline{\mathcal{M}_2^+}$.

- Considérons $M \in \mathcal{M}_2^+$, $M = \begin{pmatrix} a & b \\ b & c \end{pmatrix}$. Alors

$$\begin{aligned} \|\boldsymbol{e}_1\|_M \leq \|\boldsymbol{e}_2\|_M \quad &\Rightarrow \quad 0 \leq a \leq c, \\ \|\boldsymbol{e}_2 - \boldsymbol{e}_1\|_M \geq \|\boldsymbol{e}_2\|_M \quad &\Rightarrow \quad 2b \leq a, \\ \langle \boldsymbol{e}_1, \boldsymbol{e}_2 \rangle_M \geq 0 \quad &\Rightarrow \quad b \geq 0. \end{aligned}$$

  Les inégalités de droite caractérisent $\overline{\mathcal{M}_2^+}$.
- Question: quels entiers s'écrivent

$$149x^2 + 2 \times 44xy + 13y^2.$$

- Considérons $M \in \mathcal{M}_2^+$, $M = \begin{pmatrix} a & b \\ b & c \end{pmatrix}$. Alors

$$\begin{aligned} \|\boldsymbol{e}_1\|_M \leq \|\boldsymbol{e}_2\|_M &\quad\Rightarrow\quad 0 \leq a \leq c, \\ \|\boldsymbol{e}_2 - \boldsymbol{e}_1\|_M \geq \|\boldsymbol{e}_2\|_M &\quad\Rightarrow\quad 2b \leq a, \\ \langle \boldsymbol{e}_1, \boldsymbol{e}_2 \rangle_M \geq 0 &\quad\Rightarrow\quad b \geq 0. \end{aligned}$$

  Les inégalités de droite caractérisent $\overline{\mathcal{M}_2^+}$.
- Question: quels entiers s'écrivent

$$149x^2 + 2 \times 44xy + 13y^2.$$

  Réponse: par changement de coordonnées dans $\mathbb{Z}^2$, ces nombres s'écrivent $ax^2 + 2bxy + cy^2$, où a, b, c satisfont aux conditions précédentes et

$$ac - b^2 = 1 = 149 * 13 - 44^2.$$

- Considérons $M \in \mathcal{M}_2^+$, $M = \begin{pmatrix} a & b \\ b & c \end{pmatrix}$. Alors

$$\begin{aligned} \|\mathbf{e}_1\|_M \leq \|\mathbf{e}_2\|_M &\quad\Rightarrow\quad 0 \leq a \leq c, \\ \|\mathbf{e}_2 - \mathbf{e}_1\|_M \geq \|\mathbf{e}_2\|_M &\quad\Rightarrow\quad 2b \leq a, \\ \langle \mathbf{e}_1, \mathbf{e}_2 \rangle_M \geq 0 &\quad\Rightarrow\quad b \geq 0. \end{aligned}$$

  Les inégalités de droite caractérisent $\overline{\mathcal{M}_2^+}$.
- Question: quels entiers s'écrivent

$$149x^2 + 2 \times 44xy + 13y^2.$$

  Réponse: par changement de coordonnées dans $\mathbb{Z}^2$, ces nombres s'écrivent $ax^2 + 2bxy + cy^2$, où a, b, c satisfont aux conditions précédentes et

$$ac - b^2 = 1 = 149 * 13 - 44^2.$$

  Ainsi $a = c = 1$, $b = 0$, et ces nombres sont les sommes de deux carrés

$$x^2 + y^2.$$

Table 1

Δ	positive reduced forms			
1	$\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}$			
2	$\begin{pmatrix}1 & 0\\ 0 & 2\end{pmatrix}$			
3	$\begin{pmatrix}1 & 0\\ 0 & 3\end{pmatrix}$	$\begin{pmatrix}2 & 1\\ 1 & 2\end{pmatrix}$		
4	$\begin{pmatrix}1 & 0\\ 0 & 4\end{pmatrix}$	$\begin{pmatrix}2 & 0\\ 0 & 2\end{pmatrix}$		
5	$\begin{pmatrix}1 & 0\\ 0 & 5\end{pmatrix}$	$\begin{pmatrix}2 & 1\\ 1 & 3\end{pmatrix}$		
6	$\begin{pmatrix}1 & 0\\ 0 & 6\end{pmatrix}$	$\begin{pmatrix}2 & 0\\ 0 & 3\end{pmatrix}$		
7	$\begin{pmatrix}1 & 0\\ 0 & 7\end{pmatrix}$	$\begin{pmatrix}2 & 1\\ 1 & 4\end{pmatrix}$		
8	$\begin{pmatrix}1 & 0\\ 0 & 8\end{pmatrix}$	$\begin{pmatrix}2 & 0\\ 0 & 4\end{pmatrix}$	$\begin{pmatrix}3 & 1\\ 1 & 3\end{pmatrix}$	
9	$\begin{pmatrix}1 & 0\\ 0 & 9\end{pmatrix}$	$\begin{pmatrix}2 & 1\\ 1 & 5\end{pmatrix}$	$\begin{pmatrix}3 & 0\\ 0 & 3\end{pmatrix}$	
10	$\begin{pmatrix}1 & 0\\ 0 & 10\end{pmatrix}$	$\begin{pmatrix}2 & 0\\ 0 & 5\end{pmatrix}$		
11	$\begin{pmatrix}1 & 0\\ 0 & 11\end{pmatrix}$	$\begin{pmatrix}2 & 1\\ 1 & 6\end{pmatrix}$	$\begin{pmatrix}3 & 1\\ 1 & 4\end{pmatrix}$	$\begin{pmatrix}3 & -1\\ -1 & 4\end{pmatrix}$
12	$\begin{pmatrix}1 & 0\\ 0 & 12\end{pmatrix}$	$\begin{pmatrix}2 & 0\\ 0 & 6\end{pmatrix}$	$\begin{pmatrix}3 & 0\\ 0 & 4\end{pmatrix}$	$\begin{pmatrix}4 & 2\\ 2 & 4\end{pmatrix}$

Figure: Formes quadratiques positives à coefficients entiers, appartenant au domaine fondamental $\mathcal{M}_2^+$, classées par déterminant. (Lagrange, 1775)

Algorithme d'Euclide de calcul du pgcd

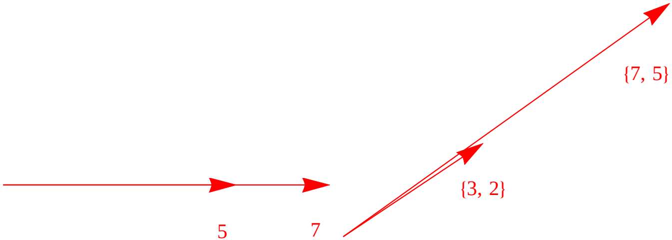
Input: $a, b \in \mathbb{Z}$

While $ab \neq 0$ **do**

Réordonner de sorte que $|a| \leq |b|$

Soustraire à b le plus proche multiple de a.

$$b \leftarrow b - \mathrm{Round}(b/a)a.$$



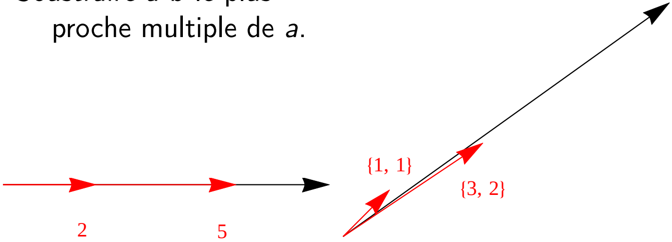
Algorithme d'Euclide de calcul du pgcd

Input: $a, b \in \mathbb{Z}$
While $ab \neq 0$ **do**
Réordonner de sorte que $|a| \leq |b|$
Soustraire à b le plus proche multiple de a.

$$b \leftarrow b - \text{Round}\left(\frac{\langle a, b\rangle}{\|a\|^2}\right) a.$$

Algorithme de Lagrange de calcul d'une base réduite

Input: $a, b \in \mathbb{R}^2$, $\|a\| \geq \|b\|$
Until $\|a\|\|b\|$ stabilizes **do**
Réordonner de sorte que $\|a\| \leq \|b\|$
Soustraire à b le plus
proche multiple de a.



Algorithme d'Euclide de calcul du pgcd

Input: $a, b \in \mathbb{Z}$

While $ab \neq 0$ **do**

Réordonner de sorte que $|a| \leq |b|$

Soustraire à b le plus proche multiple de a.

$$b \leftarrow b - \mathrm{Round}\left(\frac{\langle a, b\rangle}{\|a\|^2}\right) a.$$

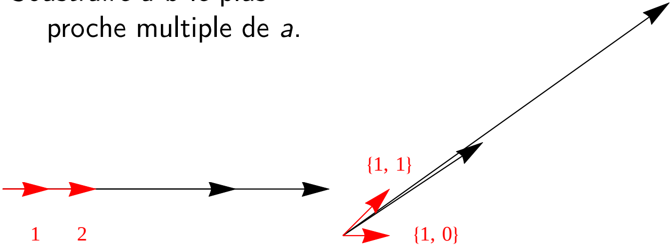
Algorithme de Lagrange de calcul d'une base réduite

Input: $a, b \in \mathbb{R}^2$, $\|a\| \geq \|b\|$

Until $\|a\|\|b\|$ stabilizes **do**

Réordonner de sorte que $\|a\| \leq \|b\|$

Soustraire à b le plus proche multiple de a.



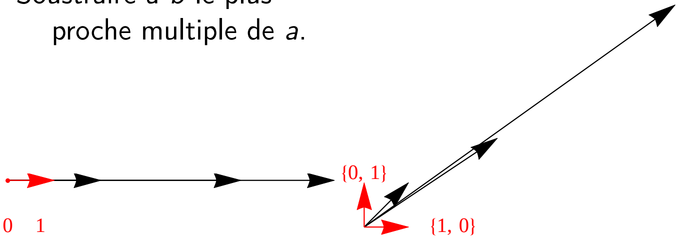
Algorithme d'Euclide de calcul du pgcd

Input: $a, b \in \mathbb{Z}$
While $ab \neq 0$ **do**
Réordonner de sorte que $|a| \leq |b|$
Soustraire à b le plus proche multiple de a.

$$b \leftarrow b - \mathrm{Round}\left(\frac{\langle a, b\rangle}{\|a\|^2}\right) a.$$

Algorithme de Lagrange de calcul d'une base réduite

Input: $a, b \in \mathbb{R}^2$, $\|a\| \geq \|b\|$
Until $\|a\|\|b\|$ stabilizes **do**
Réordonner de sorte que $\|a\| \leq \|b\|$
Soustraire à b le plus
proche multiple de a.



Base réduite vis-a-vis de $M \in \mathrm{S}_2^{++}$

Initialization: $\boldsymbol{e}_1 = (1,0)$, $\boldsymbol{e}_2 = (0,1)$

Until $\|\boldsymbol{e}_1\|_M \, \|\boldsymbol{e}_2\|_M$ stabilizes **do**

Réordonner de sorte que $\|\boldsymbol{e}_1\|_M \leq \|\boldsymbol{e}_2\|_M$

Soustraire à $\boldsymbol{e}_2$ le plus proche multiple de $\boldsymbol{e}_1$.

$$\boldsymbol{e}_2 \leftarrow \boldsymbol{e}_2 - \mathrm{Round}\left(\frac{\langle \boldsymbol{e}_1, \boldsymbol{e}_2 \rangle_M}{\|\boldsymbol{e}_1\|_M^2}\right) \boldsymbol{e}_1.$$

Base réduite vis-a-vis de $M \in \mathrm{S}_2^{++}$

Initialization: $\boldsymbol{e}_1 = (1,0)$, $\boldsymbol{e}_2 = (0,1)$
Until $\|\boldsymbol{e}_1\|_M \|\boldsymbol{e}_2\|_M$ stabilizes **do**

Réordonner de sorte que $\|\boldsymbol{e}_1\|_M \leq \|\boldsymbol{e}_2\|_M$
Soustraire à $\boldsymbol{e}_2$ le plus proche multiple de $\boldsymbol{e}_1$.

$$\boldsymbol{e}_2 \leftarrow \boldsymbol{e}_2 - \mathrm{Round}\left(\frac{\langle \boldsymbol{e}_1, \boldsymbol{e}_2\rangle_M}{\|\boldsymbol{e}_1\|_M^2}\right)\boldsymbol{e}_1.$$

Vitesse de convergence

le produit $\|\boldsymbol{e}_1\|_M \|\boldsymbol{e}_2\|_M$ décroit d'un facteur $\sqrt{3}$ à chaque itération. (Sauf la peut-être la première et la dernière.)

Base réduite vis-a-vis de $M \in \mathrm{S}_2^{++}$

Initialization: $\boldsymbol{e}_1 = (1,0)$, $\boldsymbol{e}_2 = (0,1)$

Until $\|\boldsymbol{e}_1\|_M \|\boldsymbol{e}_2\|_M$ stabilizes **do**

Réordonner de sorte que $\|\boldsymbol{e}_1\|_M \leq \|\boldsymbol{e}_2\|_M$

Soustraire à $\boldsymbol{e}_2$ le plus proche multiple de $\boldsymbol{e}_1$.

$$\boldsymbol{e}_2 \leftarrow \boldsymbol{e}_2 - \mathrm{Round}\left(\frac{\langle \boldsymbol{e}_1, \boldsymbol{e}_2\rangle_M}{\|\boldsymbol{e}_1\|_M^2}\right)\boldsymbol{e}_1.$$

Vitesse de convergence

le produit $\|\boldsymbol{e}_1\|_M \|\boldsymbol{e}_2\|_M$ décroit d'un facteur $\sqrt{3}$ à chaque itération. (Sauf la peut-être la première et la dernière.)

Généralisation à $M \in \mathrm{S}_d^{++}$, en dimension $d > 2$

Heuristique: initialiser $(\boldsymbol{e}_1, \cdots, \boldsymbol{e}_d)$ puis, itérativement

Ré-ordonner par normes croissantes $\|\boldsymbol{e}_1\|_M \leq \cdots \leq \|\boldsymbol{e}_d\|_M$.

Soustraire à chaque $\boldsymbol{e}_i$, $2 \leq j \leq d$, la plus proche combinaison linéaire entière des $\{\boldsymbol{e}_j;\, j < i\}$.

Résultats: $d = 3$ (Semaev, 2001), $d = 4$ (Nguyen, Stelhé, 2004)

L'algorithme de Lenstra-Lenstra-Lovasz, 1982

Heuristique: initialiser $(\boldsymbol{e}_1, \cdots, \boldsymbol{e}_d)$ puis, itérativement

Ré-ordonner par normes croissantes.
Soustraire à $\boldsymbol{e}_i$ le plus proche multiple de $\boldsymbol{e}_{i-1}$, $2 \leq i \leq d$.

- Critère de terminaison souple $\Rightarrow$ complexité polynomiale.
- Ne calcule pas la base réduite de Minkowski, mais une "bonne base" ayant des garanties d'orthogonalité.
- Utilisé pour déterminer le plus petits élément d'un réseau, ou le plus proche élément d'un point donné.
- Factorisation (de polynômes, d'entiers), attaques cryptographiques.

RSA-768 =
1230186684530117755130494958384962720 7728535695953347921973224521517264005
0726365751874520219978646938995647494 2774063845925192557326303453731548268
5079170261221429134616704292143116022 2124047927473779408066535141959745985
6902143413 =
3347807169895689878604416984821269081 7704794983713768568912431388982883793
8780022876147116525317430877378144679994 89 × 3674604366679959042824463379962795263
2279158164343087642676032283815739666 5112792333734171433968102700927987363089 17

Le problème du sac à dos

Etant donnés $a_1, \cdots, a_n \in \mathbb{N}$, et $a \in \mathbb{N}$, trouver:

$$\varepsilon_1, \cdots, \varepsilon_n \in \{0,1\}, \text{ tels que } a_1\varepsilon_1 + \cdots + a_n\varepsilon_n = a.$$

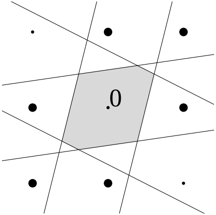
- NP-Complet en général.
- Instances utilisées en cryptographie par Merkle, Hellman, 1978. (Seule alternative au RSA à l'époque.)
- On peut appliquer l'Algorithme LLL pour trouver:

$$\varepsilon_1, \cdots, \varepsilon_n \in \mathbb{Z} \text{ tels que } (a_1\varepsilon_1 + \cdots + a_n\varepsilon_n, \varepsilon_1, \cdots, \varepsilon_n)$$
$$\text{est proche de } (a, 1/2, \cdots, 1/2).$$

La solution est “souvent” la même que celle du problème original, ce qui met en défaut le code cryptographique.

Seconde réduction de Voronoi de $M \in \mathbb{S}_d^{++}$

C'est la triangulation de Delaunay $\mathcal{T}_M$ de $\mathbb{Z}^d$ vis-à-vis de $\|\cdot\|_M$.



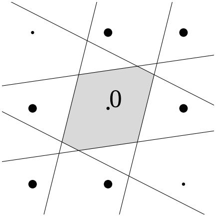
Dimension	1	2	3	4	5
# Triangulations inéquivalentes	1	1	1	3	222

Seconde réduction de Voronoi de $M \in \mathrm{S}_d^{++}$

C'est la triangulation de Delaunay $\mathcal{T}_M$ de $\mathbb{Z}^d$ vis-à-vis de $\| \cdot \|_M$.
$\boldsymbol{e}_1, \cdots, \boldsymbol{e}_k \in \mathbb{Z}^d$ sont les sommets d'une facette ssi

$$\mathrm{Vor}_M(\boldsymbol{e}_1) \cap \cdots \cap \mathrm{Vor}_M(\boldsymbol{e}_k) \neq \emptyset,$$

où $\mathrm{Vor}_M(\boldsymbol{e}) := \{\boldsymbol{p} \in \mathbb{R}^d;\ \forall \boldsymbol{e}' \in \mathbb{Z}^d,\ \|\boldsymbol{p} - \boldsymbol{e}\|_M \leq \|\boldsymbol{p} - \boldsymbol{e}'\|_M\}$.



Dimension	1	2	3	4	5
# Triangulations inéquivalentes	1	1	1	3	222

Qu'est ce qu'une réduction ?

- Une réduction, de l'ensemble S_d^{++} sous l'action de $\mathrm{GL}_d(\mathbb{Z})$, est un procédé permettant d'écrire chaque $M \in \mathrm{S}_d^{++}$

$$M = A \cdot N, \qquad \text{où } A \cdot N := (A^{-1})^{\mathrm{T}} N (A^{-1}).$$

Ici $A \in \mathrm{GL}_d(\mathbb{Z})$, et N est (génériquement) unique et appartient à un domaine fondamental.

Qu'est ce qu'une réduction ?

- Une réduction, de l'ensemble S_d^{++} sous l'action de $\mathrm{GL}_d(\mathbb{Z})$, est un procédé permettant d'écrire chaque $M \in \mathrm{S}_d^{++}$

$$M = A \cdot N, \qquad \text{où } A \cdot N := (A^{-1})^{\mathrm{T}} N (A^{-1}).$$

Ici $A \in \mathrm{GL}_d(\mathbb{Z})$, et N est (génériquement) unique et appartient à un domaine fondamental.

- En pratique, on construit une application $\rho : \mathrm{S}_d^{++} \to X$, compatible avec l'action de $\mathrm{GL}_d(\mathbb{Z})$

$$\rho(A \cdot M) = A \cdot \rho(M).$$

Puis on hérite une réduction sur S_d^{++} de celle associée à X.

Qu'est ce qu'une réduction ?

- Une réduction, de l'ensemble S_d^{++} sous l'action de $\mathrm{GL}_d(\mathbb{Z})$, est un procédé permettant d'écrire chaque $M \in \mathrm{S}_d^{++}$

$$M = A \cdot N, \qquad \text{où } A \cdot N := (A^{-1})^{\mathrm{T}} N (A^{-1}).$$

Ici $A \in \mathrm{GL}_d(\mathbb{Z})$, et N est (génériquement) unique et appartient à un domaine fondamental.

- En pratique, on construit une application $\rho : \mathrm{S}_d^{++} \to X$, compatible avec l'action de $\mathrm{GL}_d(\mathbb{Z})$

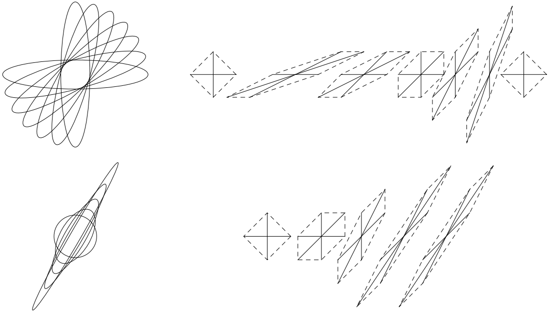
$$\rho(A \cdot M) = A \cdot \rho(M).$$

Puis on hérite une réduction sur S_d^{++} de celle associée à X.
- Minkowski: X est l'ensemble des bases de $\mathbb{Z}^d$.
- Voronoi 2: X est un ensemble de triangulations.
- Voronoi 1: X est un sous-ensemble discret de S_d^{++}.

Proposition (Une propriété géométrique de $\mathcal{T}_M$, $M \in \mathrm{S}_d^{++}$)

Soient $\boldsymbol{e}_0, \boldsymbol{e}_1, \boldsymbol{e}_2$ les sommets d'un triangle de $\mathcal{T}_M$. Alors

$$\langle \boldsymbol{e}_2 - \boldsymbol{e}_0, \boldsymbol{e}_2 - \boldsymbol{e}_1 \rangle_M \geq 0.$$



Proposition (Une propriété géométrique de $\mathcal{T}_M$, $M \in \mathrm{S}_d^{++}$)

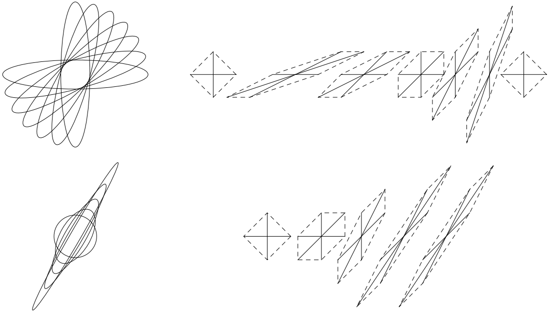
Soient $\boldsymbol{e}_0, \boldsymbol{e}_1, \boldsymbol{e}_2$ les sommets d'un triangle de $\mathcal{T}_M$. Alors

$$\langle \boldsymbol{e}_2 - \boldsymbol{e}_0, \boldsymbol{e}_2 - \boldsymbol{e}_1 \rangle_M \geq 0.$$

Preuve: Soit $\boldsymbol{p} \in \mathrm{Vor}_M(\boldsymbol{e}_0) \cap \mathrm{Vor}_M(\boldsymbol{e}_1) \cap \mathrm{Vor}_M(\boldsymbol{e}_2)$. Alors

$$\|\boldsymbol{p} - \boldsymbol{e}_0\|_M^2 - \|\boldsymbol{p} - \boldsymbol{e}_1\|_M^2 - \|\boldsymbol{p} - \boldsymbol{e}_2\|_M^2 + \|\boldsymbol{p} - (\boldsymbol{e}_1 + \boldsymbol{e}_2 - \boldsymbol{e}_0)\|_M^2$$

est positif, par déf. de Vor_M, et égal à $\langle \boldsymbol{e}_2 - \boldsymbol{e}_0, \boldsymbol{e}_2 - \boldsymbol{e}_1 \rangle_M$.



Proposition (Une propriété géométrique de $\mathcal{T}_M$, $M \in \mathrm{S}_d^{++}$)

Soient $\boldsymbol{e}_0, \boldsymbol{e}_1, \boldsymbol{e}_2$ les sommets d'un triangle de $\mathcal{T}_M$. Alors

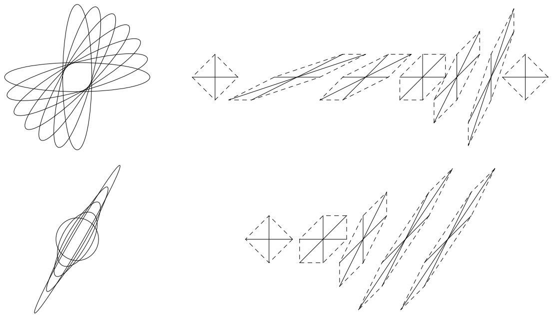
$$\langle \boldsymbol{e}_2 - \boldsymbol{e}_0, \boldsymbol{e}_2 - \boldsymbol{e}_1 \rangle_M \geq 0.$$

Preuve: Soit $\boldsymbol{p} \in \mathrm{Vor}_M(\boldsymbol{e}_0) \cap \mathrm{Vor}_M(\boldsymbol{e}_1) \cap \mathrm{Vor}_M(\boldsymbol{e}_2)$. Alors

$$\|\boldsymbol{p} - \boldsymbol{e}_0\|_M^2 - \|\boldsymbol{p} - \boldsymbol{e}_1\|_M^2 - \|\boldsymbol{p} - \boldsymbol{e}_2\|_M^2 + \|\boldsymbol{p} - (\boldsymbol{e}_1 + \boldsymbol{e}_2 - \boldsymbol{e}_0)\|_M^2$$

est positif, par déf. de Vor_M, et égal à $\langle \boldsymbol{e}_2 - \boldsymbol{e}_0, \boldsymbol{e}_2 - \boldsymbol{e}_1 \rangle_M$.

- Utilise la stabilité additive de $\mathbb{Z}^d$.



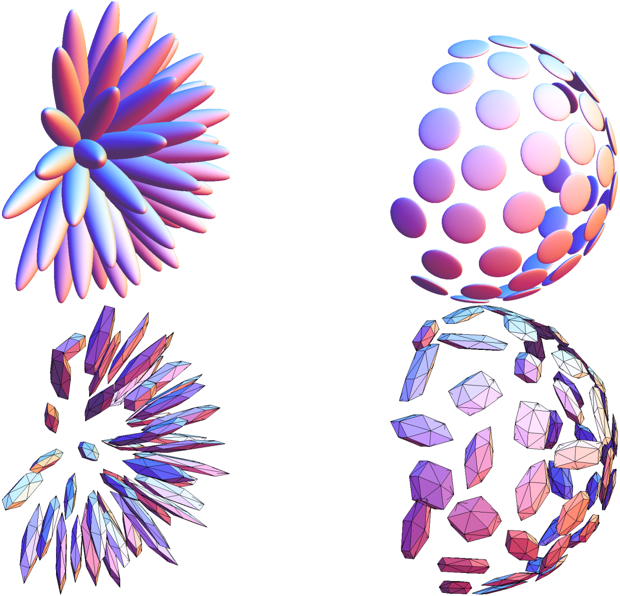


Figure: Boule unité de M, et voisinage de l'origine dans $\mathcal{T}_M$.

L'algorithme de Dijkstra

- Soit $X \subseteq \mathbb{R}^d$ un ensemble fini, $\partial X \subseteq X$.
- Soit pour tout $\boldsymbol{x} \in X \setminus \partial X$, $V(\boldsymbol{x}) \subseteq X$ un ensemble de voisins. Soit $V[\boldsymbol{x}] := \{\boldsymbol{y} \in X;\, \boldsymbol{x} \in V(\boldsymbol{y})\}$.
- Objectif: trouver $u : X \to \mathbb{R}$, nulle sur ∂X, satisfaisant

$$\forall \boldsymbol{x} \in X \setminus \partial X,\ u(\boldsymbol{x}) = \Lambda u(\boldsymbol{x}) := \min_{\boldsymbol{y} \in V(\boldsymbol{x})} \|\boldsymbol{x} - \boldsymbol{y}\| + u(\boldsymbol{y}).$$

Initialiser $u : X \to \mathbb{R}$ to 0 on ∂X, $+\infty$ elsewhere.
accepté : $X \to \{true, false\}$ to $false$.
Tant que il reste un point non accepté
Trouver le point non-accepté $\boldsymbol{x} \in X$ minimisant u.
Marquer $\boldsymbol{x}$ comme accepté.
Pout tout $\boldsymbol{y} \in V[\boldsymbol{x}]$, $u(\boldsymbol{y}) \leftarrow \Lambda u(\boldsymbol{y})$.

Programmation dynamique/Fast-Marching.

- Dijkstra calcule le point fixe de l'opérateur Λ, qui est la distance à ∂X sur le graphe (X, V).
- La programmation dynamique/Fast-Marching appliquent Dijkstra à un opérateur Λ et voisinage V modifiés.

Programmation dynamique/Fast-Marching.

- Dijkstra calcule le point fixe de l'opérateur Λ, qui est la distance à ∂X sur le graphe (X, V).
- La programmation dynamique/Fast-Marching appliquent Dijkstra à un opérateur Λ et voisinage V modifiés.

Propriétés requises de l'opérateur Λ

- Monotonie: $\forall u, v : X \to \mathbb{R}$
$$u \leq v \Rightarrow \Lambda u \leq \Lambda v.$$
- Causalité: $\forall u, v : X \to \mathbb{R}$
$$u^{<\lambda} = v^{<\lambda} \Rightarrow (\Lambda u)^{\leq \lambda} = (\Lambda v)^{\leq \lambda},$$
où l'on a noté
$$u^{<\lambda}(x) = \begin{cases} u(x) \text{ si } u(x) < \lambda, \\ +\infty \text{ sinon.} \end{cases}$$

Schéma semi-Lagrangien pour une distance Riemannienne

- Soit $\Omega \subseteq \mathbb{R}^d$ un domaine, échantillonné par X, et $M : \Omega \to \mathrm{S}_d^{++}$ une métrique Riemannienne.
- Soit $V(\boldsymbol{x})$ un polytope ayant ses sommets dans X, et $\mathrm{I}_{V(\boldsymbol{x})}$ l'interpolation linéaire. Posons

$$\Lambda u(\boldsymbol{x}) := \min_{\boldsymbol{y} \in V(\boldsymbol{x})} \|\boldsymbol{x} - \boldsymbol{y}\|_{M(\boldsymbol{x})} + \mathrm{I}_{V(\boldsymbol{x})}\, u(\boldsymbol{y}).$$

Schéma semi-Lagrangien pour une distance Riemannienne

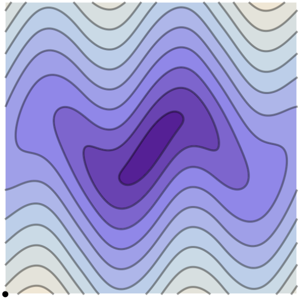
- Soit $\Omega \subseteq \mathbb{R}^d$ un domaine, échantillonné par X, et $M : \Omega \to \mathrm{S}_d^{++}$ une métrique Riemannienne.
- Soit $V(\boldsymbol{x})$ un polytope ayant ses sommets dans X, et $\mathrm{I}_{V(\boldsymbol{x})}$ l'interpolation linéaire. Posons

$$\Lambda u(\boldsymbol{x}) := \min_{\boldsymbol{y} \in V(\boldsymbol{x})} \|\boldsymbol{x} - \boldsymbol{y}\|_{M(\boldsymbol{x})} + \mathrm{I}_{V(\boldsymbol{x})}\, u(\boldsymbol{y}).$$

Propriétés de l'opérateur Λ

- Monotonie: découle de celle de l'interpolation linéaire.
- (Sethian, 2003) Causalité équivalente à: pour tout $\boldsymbol{x} \in X$, pour tous sommets $\boldsymbol{y}, \boldsymbol{z}$ d'une facette commune de $V(\boldsymbol{x})$

$$\langle \boldsymbol{z} - \boldsymbol{x}, \boldsymbol{y} - \boldsymbol{x} \rangle_{M(x)} \geq 0.$$



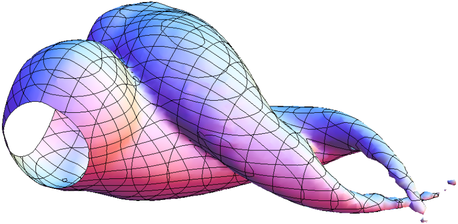
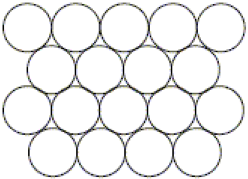
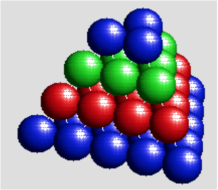


Figure: Ensembles de niveaux de distances Riemanniennes.

Formes quadratiques parfaites

- Voronoi introduit l'ensemble de formes quadratiques

$$K := \{Q \in \mathrm{S}_d^{++};\ \forall \boldsymbol{e} \in \mathbb{Z}^d,\ \|\boldsymbol{e}\|_Q \geq 1\}$$

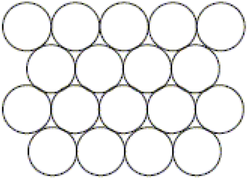
Formes quadratiques parfaites

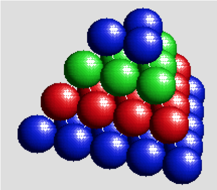
- Voronoi introduit l'ensemble de formes quadratiques

$$K := \{Q \in \mathrm{S}_d^{++};\ \forall \boldsymbol{e} \in \mathbb{Z}^d,\ \ \|\boldsymbol{e}\|_Q \geq 1\}$$

- K est un polytope convexe, en vertu de

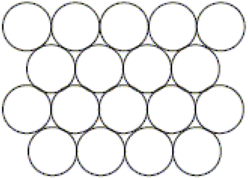
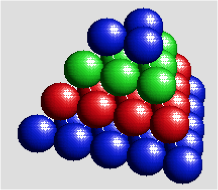
$$\|\boldsymbol{e}\|_Q^2 = \boldsymbol{e}^{\mathrm{T}} Q \boldsymbol{e} = \mathrm{Tr}(Q\, \boldsymbol{e}\boldsymbol{e}^{\mathrm{T}}).$$





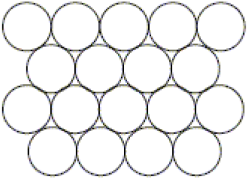
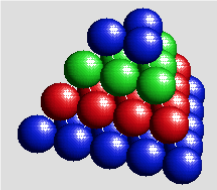
Formes quadratiques parfaites

- Voronoi introduit l'ensemble de formes quadratiques
$$K := \{Q \in \mathrm{S}_d^{++};\ \forall \boldsymbol{e} \in \mathbb{Z}^d,\ \ \|\boldsymbol{e}\|_Q \geq 1\}$$
- K est un polytope convexe, en vertu de
$$\|\boldsymbol{e}\|_Q^2 = \boldsymbol{e}^{\mathrm{T}} Q \boldsymbol{e} = \mathrm{Tr}(Q\, \boldsymbol{e}\boldsymbol{e}^{\mathrm{T}}).$$
- Les sommets de K sont appelés <u>formes parfaites</u>, et sont liés aux arrangements compacts de sphères.

Formes quadratiques parfaites

- Voronoi introduit l'ensemble de formes quadratiques
$$K := \{Q \in \mathrm{S}_d^{++};\ \forall \boldsymbol{e} \in \mathbb{Z}^d,\ \ \|\boldsymbol{e}\|_Q \geq 1\}$$
- K est un polytope convexe, en vertu de
$$\|\boldsymbol{e}\|_Q^2 = \boldsymbol{e}^{\mathrm{T}} Q \boldsymbol{e} = \mathrm{Tr}(Q\, \boldsymbol{e}\boldsymbol{e}^{\mathrm{T}}).$$
- Les sommets de K sont appelés formes parfaites, et sont liés aux arrangements compacts de sphères.
- Pour tout $Q \in K$, les ellipsoides disjoints
$$(\boldsymbol{e} + \mathcal{E}_Q)_{\boldsymbol{e} \in \mathbb{Z}^d} \qquad \text{où } \mathcal{E}_Q := \{\boldsymbol{p} \in \mathbb{R}^d;\ \|\boldsymbol{p}\|_Q \leq 1/2\},$$
occupent une portion $c_d (\det Q)^{-\frac{1}{2}}$ de l'espace.

Première réduction de Voronoi, de $M \in \mathrm{S}_d^{++}$

C'est la forme parfaite

$$\operatorname*{argmin}_{Q \in K} \mathrm{Tr}(QM).$$

Theorem (Voronoi, 1905)

En toute dimension d, ce problème d'optimisation linéaire est faisable (i.e. admet un ensemble compact de solutions). De plus il n'existe qu'un nombre fini de formes parfaites inéquivalentes.

Dimension	1	2	3	4	5	6	7	8	9
# Formes parfaites	1	1	1	2	3	7	33	10916	>500 000

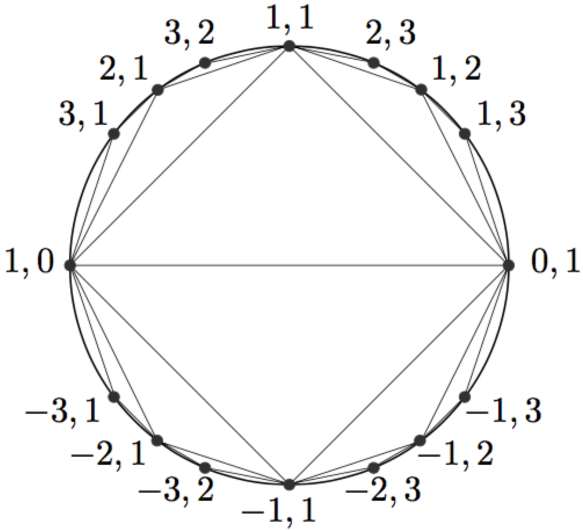


Figure: Partition du disque de Poincaré, $D \approxeq \{M \in S_2^{++}; \det M = 1\}$ induite par la première réduction de Voronoi. (Schurmann)

Relations de Kuhn et Tucker

- La première réduction est associée au programme linéaire

$$\min\{\langle\langle M, Q\rangle\rangle;\ \forall \boldsymbol{e} \in \mathbb{Z}^d,\ \langle\langle \boldsymbol{e} \otimes \boldsymbol{e}, Q\rangle\rangle \geq 1\}.$$

où $\langle\langle D, M\rangle\rangle := \mathrm{Tr}(DM)$, et $\boldsymbol{e} \otimes \boldsymbol{e} := \boldsymbol{e}\boldsymbol{e}^{\mathrm{T}}$.

Relations de Kuhn et Tucker

- La première réduction est associée au programme linéaire

$$\min\{\langle\langle M, Q\rangle\rangle;\ \forall \boldsymbol{e} \in \mathbb{Z}^d,\ \langle\langle \boldsymbol{e} \otimes \boldsymbol{e}, Q\rangle\rangle \geq 1\}.$$

  où $\langle\langle D, M\rangle\rangle := \mathrm{Tr}(DM)$, et $\boldsymbol{e} \otimes \boldsymbol{e} := \boldsymbol{e}\boldsymbol{e}^{\mathrm{T}}$.

- Il existe donc une famille finie $(\lambda_i, \boldsymbol{e}_i)_{i \in \mathbb{I}}$, avec $\lambda_i \geq 0$, $\boldsymbol{e}_i \in \mathbb{Z}^d$, et $\#(I) \leq d(d+1)/2$, tels que

$$M = \sum_{i \in I} \lambda_i \boldsymbol{e}_i \otimes \boldsymbol{e}_i.$$

Relations de Kuhn et Tucker

- La première réduction est associée au programme linéaire

$$\min\{\langle\langle M, Q\rangle\rangle;\ \forall \boldsymbol{e} \in \mathbb{Z}^d,\ \langle\langle \boldsymbol{e}\otimes \boldsymbol{e}, Q\rangle\rangle \geq 1\}.$$

  où $\langle\langle D, M\rangle\rangle := \mathrm{Tr}(DM)$, et $\boldsymbol{e}\otimes\boldsymbol{e} := \boldsymbol{e}\boldsymbol{e}^{\mathrm{T}}$.
- Il existe donc une famille finie $(\lambda_i, \boldsymbol{e}_i)_{i\in\mathbb{I}}$, avec $\lambda_i \geq 0$, $\boldsymbol{e}_i \in \mathbb{Z}^d$, et $\#(I) \leq d(d+1)/2$, tels que

$$M = \sum_{i\in I} \lambda_i \boldsymbol{e}_i \otimes \boldsymbol{e}_i.$$

- Cette décomposition s'apparente à la décomposition en vecteur propres/valeurs propres, mais
  (i) le nombre de termes est $d(d+1)/2$ et non d.
  (ii) les offsets $\boldsymbol{e}_i$ sont à coordonnées entières.

Application à la diffusion anisotrope

- L'équation de diffusion anisotrope, avec tenseurs constants, s'écrit

$$\partial_t u(t,x) = \mathrm{div}(D(x)\nabla u(t,x))$$

- Elle s'interprète comme le flot gradient L^2 de l'énergie elliptique

$$\int \|\nabla u(\boldsymbol{x})\|^2_{D(\boldsymbol{x})} \mathrm{d}\boldsymbol{x}$$

- La décomposition $D = \sum_{i \in I} \lambda_i \boldsymbol{e}_i \otimes \boldsymbol{e}_i$ donne l'approximation au premier ordre

$$\|\nabla u(x)\|^2_D \approx \sum_{i \in I} \lambda_i \frac{u(\boldsymbol{x}+\boldsymbol{e}_i) - u(\boldsymbol{x}))^2 + (u(\boldsymbol{x}-\boldsymbol{e}_i) - u(\boldsymbol{x}))^2}{2}$$

Diffusion anisotrope: $\partial_t u = \mathrm{div}(D(u)\nabla u)$.

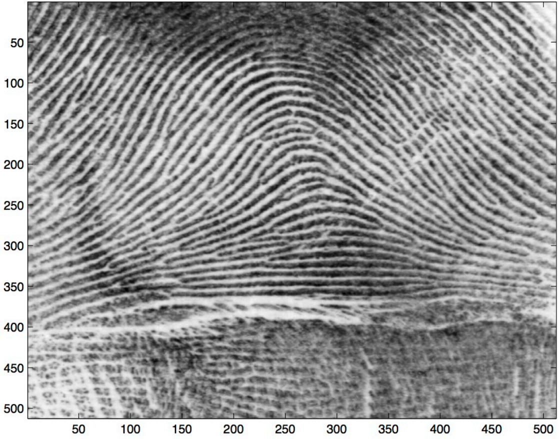


Figure: Effet de la diffusion par les tenseurs non-linéaires de Weickert

Diffusion anisotrope: $\partial_t u = \operatorname{div}(D(u)\nabla u)$.

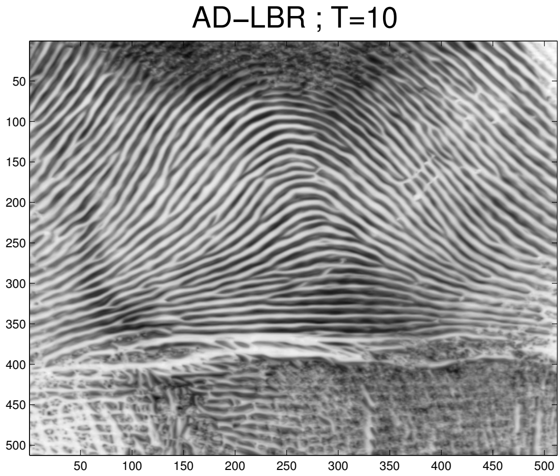


Figure: Effet de la diffusion par les tenseurs non-linéaires de Weickert

Diffusion anisotrope: $\partial_t u = \mathrm{div}(D(u)\nabla u)$.

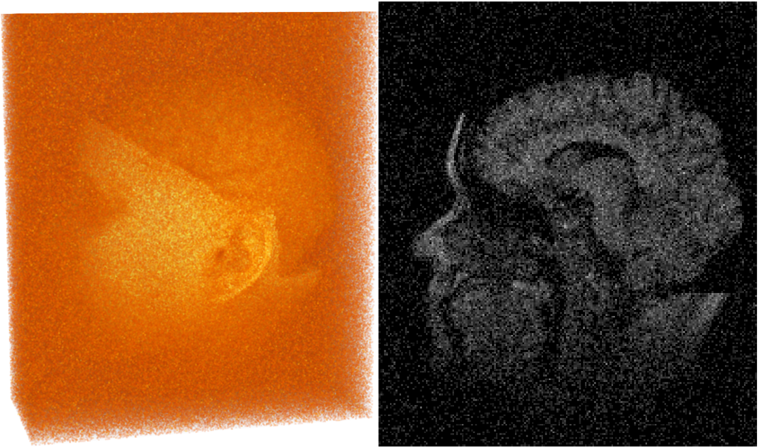


Figure: Effet de la diffusion par les tenseurs non-linéaires de Weickert

Diffusion anisotrope: $\partial_t u = \mathrm{div}(D(u)\nabla u)$.

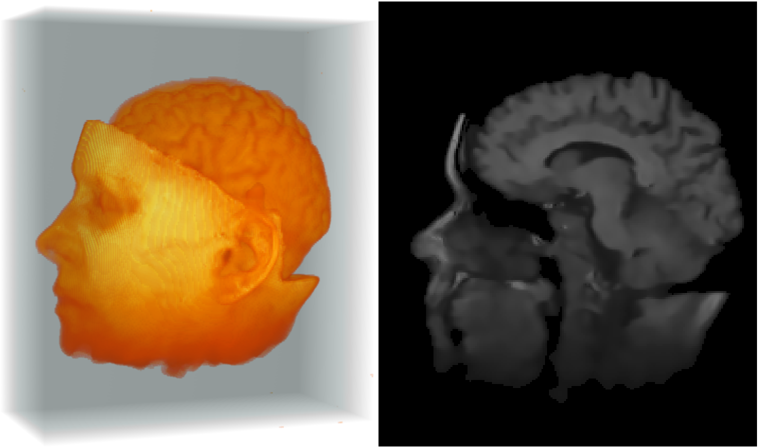


Figure: Effet de la diffusion par les tenseurs non-linéaires de Weickert

L'équation eikonale

C'est une EDP du premier ordre, de la forme

$$\mathcal{H}(\boldsymbol{x}, \nabla u(\boldsymbol{x})) = 1/2,$$

sur un domaine Ω, avec e.g. $u = 0$ sur $\partial\Omega$.

- Aussi appelée equation du Hamilton-Jacobi-Bellman statique du premier ordre.
- Caractérise les fonctions distances, et plus généralement des temps d'arrivée de fronts.

Exemples

- $\|\nabla u(x)\| = 1$ pour la distance Euclidienne à $\partial\Omega$.
- $\|\nabla u(x)\|_{M(x)^{-1}} = 1$ pour la distance Riemannienne.
- Pour la distance associée au Lagrangien $\mathcal{L}$

$$\mathcal{H}(\boldsymbol{x}, \hat{\boldsymbol{p}}) = \sup_{\dot{\boldsymbol{p}}} \langle \hat{\boldsymbol{p}}, \dot{\boldsymbol{p}} \rangle - \mathcal{L}(\boldsymbol{x}, \dot{\boldsymbol{p}}).$$

Discrétisation de l'équation eikonale

Cherchée sous la forme suivante, où X échantillonne Ω,

$$H(\boldsymbol{x}, (u(\boldsymbol{x}) - u(\boldsymbol{y}))_{y \in X}) = 1/2.$$

- Monotone si H est croissante en les $u(\boldsymbol{x}) - u(\boldsymbol{y})$, $y \in X$.
- Causale si H ne dépend que des parties positives, $(u(\boldsymbol{x}) - u(\boldsymbol{y}))_+$, où $a_+ := \max\{a, 0\}$.
- Si ces deux conditions sont remplies, le système est résoluble en une passe par la programmation dynamique.

Le cas Riemannien

Etant donné $D = \sum_{i \in I} \lambda_i \boldsymbol{e}_i \otimes \boldsymbol{e}_i$, on a au premier ordre

$$\|\nabla u(\boldsymbol{x})\|_D^2 \approx \sum_{i \in I} \lambda_i \max\{0, u(\boldsymbol{x}) - u(x - \boldsymbol{e}_i), u(\boldsymbol{x}) - u(\boldsymbol{x} + \boldsymbol{e}_i)\}^2.$$

Cette discrétisation est monotone et causale.

Pénalisation de la courbure d'un chemin

- On recherche des chemins minimaux pour des coûts

$$\int_0^L \alpha(\gamma(s))\, \mathcal{C}(\kappa(s))\, ds,$$

où $\gamma : [0, L] \to \mathbb{R}^2$ est paramétré à vitesse unité, et $\kappa : [0, L] \to \mathbb{R}$ est sa courbure.

- L'implémentation requiert un relèvement dans l'espace $\mathbb{M} := \mathbb{R}^2 \times \mathbb{S}^1$, dont les points sont notés $\boldsymbol{p} = (\boldsymbol{x}, \boldsymbol{n})$.
- Le chemin γ se relève en $\eta = (\gamma, \gamma')$, d'énergie

$$\int_0^L \mathcal{F}(\gamma(t), \gamma'(t))dt$$

où

$$\mathcal{F}((\boldsymbol{x}, \boldsymbol{n}), (\dot{\boldsymbol{x}}, \dot{\boldsymbol{n}})) = \begin{cases} \alpha(\boldsymbol{x})\mathcal{C}(|\dot{\boldsymbol{n}}|/|\dot{\boldsymbol{x}}|)|\dot{\boldsymbol{x}}| & \text{si } \dot{\boldsymbol{x}} = \|\dot{\boldsymbol{x}}\|\boldsymbol{n} \\ +\infty & \text{sinon.} \end{cases}$$

- Ceci correspond au Lagrangien $\mathcal{L} = \frac{1}{2}\mathcal{F}^2$.

Hamiltoniens de ces modèles

Let $\boldsymbol{p} = (\boldsymbol{x}, \boldsymbol{n}) \in \mathbb{M}$, and $\hat{\boldsymbol{p}} = (\hat{\boldsymbol{x}}, \hat{\boldsymbol{n}}) \in T^*_{\boldsymbol{p}}\mathbb{M}$.

- Reeds-Shepp sans marche arrière $\mathcal{C}(\kappa) = \sqrt{1+\kappa^2}$

$$2\mathfrak{H}_1(\boldsymbol{p}, \hat{\boldsymbol{p}}) = \langle \boldsymbol{n}, \hat{\boldsymbol{x}} \rangle_+^2 + \|\hat{\boldsymbol{n}}\|^2$$

Hamiltoniens de ces modèles

Let $\boldsymbol{p} = (\boldsymbol{x}, \boldsymbol{n}) \in \mathbb{M}$, and $\hat{\boldsymbol{p}} = (\hat{\boldsymbol{x}}, \hat{\boldsymbol{n}}) \in T^*_{\boldsymbol{p}}\mathbb{M}$.

- Reeds-Shepp sans marche arrière $\mathcal{C}(\kappa) = \sqrt{1+\kappa^2}$

$$2\mathfrak{H}_1(\boldsymbol{p}, \hat{\boldsymbol{p}}) = \langle \boldsymbol{n}, \hat{\boldsymbol{x}} \rangle_+^2 + \|\hat{\boldsymbol{n}}\|^2$$

- Dubins $\mathcal{C}(\kappa) = 1$ si $|\kappa| \leq 1$, $\mathcal{C}(\kappa) = \infty$ sinon.

$$2\mathfrak{H}_\infty(\boldsymbol{p}, \hat{\boldsymbol{p}}) = \max\{\langle (\boldsymbol{n}, 1), \hat{\boldsymbol{p}} \rangle_+^2,\ \langle (\boldsymbol{n}, -1), \hat{\boldsymbol{p}} \rangle_+^2\}.$$

Hamiltoniens de ces modèles

Let $\boldsymbol{p} = (\boldsymbol{x}, \boldsymbol{n}) \in \mathbb{M}$, and $\hat{\boldsymbol{p}} = (\hat{\boldsymbol{x}}, \hat{\boldsymbol{n}}) \in T^*_{\boldsymbol{p}}\mathbb{M}$.

- Reeds-Shepp sans marche arrière $\mathcal{C}(\kappa) = \sqrt{1+\kappa^2}$

$$2\mathfrak{H}_1(\boldsymbol{p}, \hat{\boldsymbol{p}}) = \langle \boldsymbol{n}, \hat{\boldsymbol{x}} \rangle_+^2 + \|\hat{\boldsymbol{n}}\|^2$$

- Dubins $\mathcal{C}(\kappa) = 1$ si $|\kappa| \leq 1$, $\mathcal{C}(\kappa) = \infty$ sinon.

$$2\mathfrak{H}_\infty(\boldsymbol{p}, \hat{\boldsymbol{p}}) = \max\{\langle (\boldsymbol{n}, 1), \hat{\boldsymbol{p}} \rangle_+^2,\ \langle (\boldsymbol{n}, -1), \hat{\boldsymbol{p}} \rangle_+^2\}.$$

- Euler-Elastica $\mathcal{C}(\kappa) = 1 + \kappa^2$

$$2\mathfrak{H}_2(\hat{\boldsymbol{p}}) = \frac{1}{4}\left(\langle \boldsymbol{n}, \hat{x} \rangle + \sqrt{\langle \boldsymbol{n}, \hat{x} \rangle^2 + \|\hat{n}\|^2}\right)^2$$
$$= \frac{1}{3}\int_{-\pi/2}^{\pi/2} \langle (\boldsymbol{n} \cos\varphi, \sin\varphi), \hat{x} \rangle_+^2 \cos\varphi \, d\varphi$$

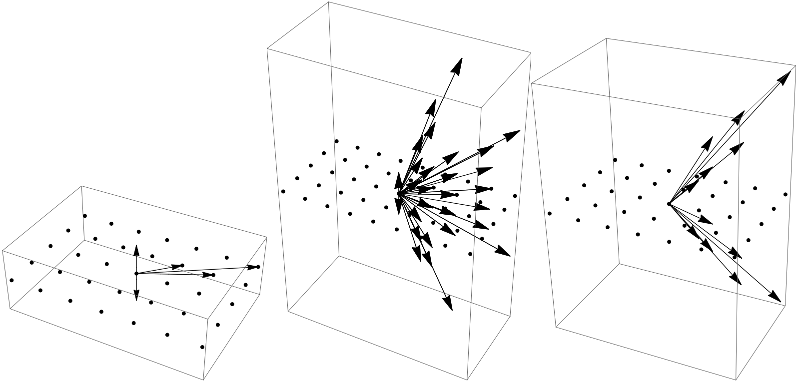
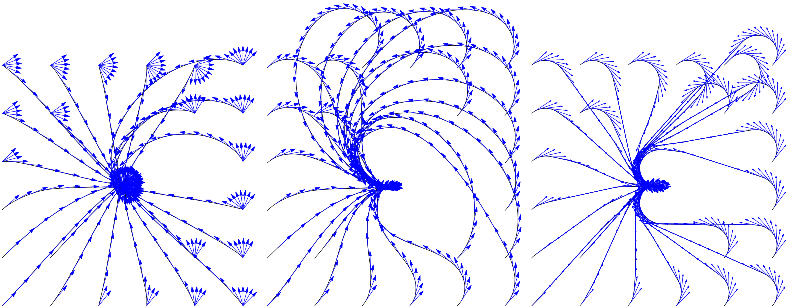


Figure: Stencils de discrétisation utilisés pour les modèles de Reeds-Shepp, Elastica, et Dubins.

Merci pour votre attention



Reeds-Shepp Elastica Dubins