TP3 : Réseaux euclidens

Résumé du TP

Bertrand Meyer

9 décembre

Contexte

Définition
Un réseau euclidien est un ensemble des vecteurs de la forme

$$\mathbb{Z}\mathbf{b}_1 \oplus \mathbb{Z}\mathbf{b}_2 \oplus \cdots \mathbb{Z}\mathbf{b}_n$$

où $(\mathbf{b}_i)_{1 \leq i \leq n}$ est une famille libre d'un espace euclidien.

$\rightarrow$ $\mathbb{Z}$-module libre + notion de produit scalaire

Perspective historique de la notion de réseau

Géométrie des nombres (Minkowski $\sim$ 1890)

- Résolution de problèmes diophantiens.

L'algorithme LLL (fin XXe s.)

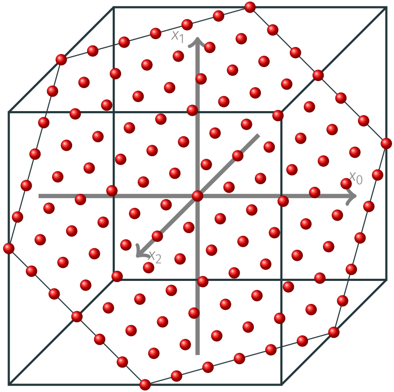
- Outil pour la factorisation dans $\mathbb{Z}[X]$ (cf **TP 5**)
- Outil pour la cryptanalyse (cf **TP 12**)

Problèmes **NP**-difficiles (XXIe s.)

- Construction de primitives cryptographiques (1996) (cf **TP 12**) dont NTRU (1998), LWE (2005)
- Incarnation du chiffrement homomorphe (2009)

Définition

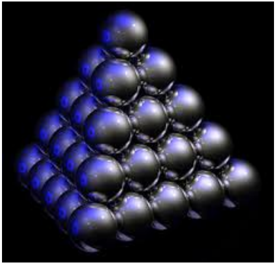
$$\mathbb{A}_2 = \{(x_0, x_1, x_2) \in \mathbb{Z}^3 ; x_0 + x_1 + x_2 = 0\}$$



Appelé aussi réseau hexagonal

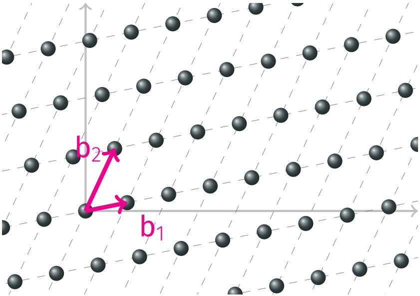
Définition

$$\mathbb{A}_3 = \{(x_0, x_1, x_2, x_3) \in \mathbb{Z}^4; x_0 + x_1 + x_2 + x_3 = 0\}$$
$$\simeq \mathbb{D}_3 = \{(x_1, x_2, x_3) \in \mathbb{Z}^3; x_1 + x_2 + x_3 \equiv 0 \mod 2\}$$



Attributs d'un réseau

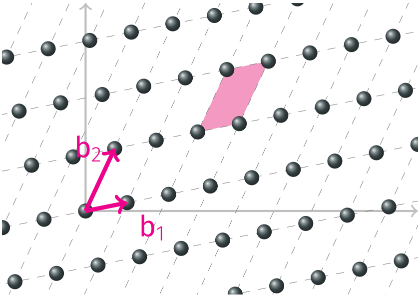
- Un réseau se décrit par une base



$$B = [b_1, b_2, \ldots, b_m] \in \mathbb{R}^{n \times m}$$

Attributs d'un réseau

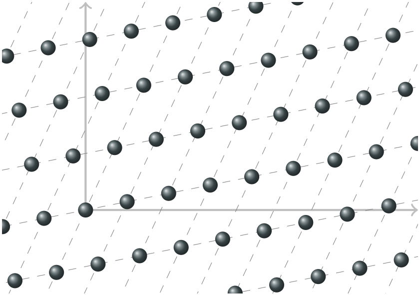
- Un réseau possède un déterminant



$$\det \mathcal{L} = \det(B^\top B) \qquad \operatorname{disc} \mathcal{L} = \sqrt{\det(B^\top B)} = \mathrm{Vol}(\mathcal{L})$$

Attributs d'un réseau

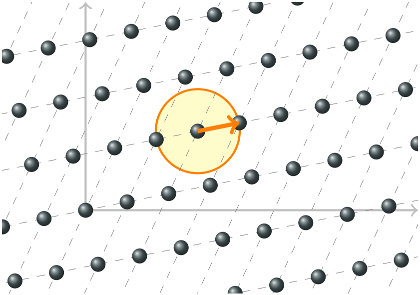
- On peut étudier ses minima successifs



Se notent λ_1, λ_2, etc.

Attributs d'un réseau

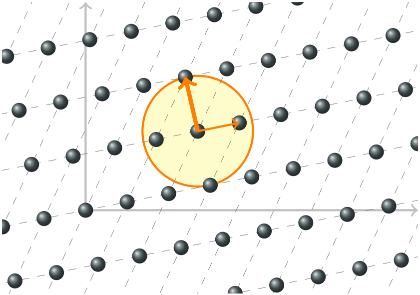
- On peut étudier ses minima successifs



$\lambda_1 =$ longueur du plus court vecteur non nul

Attributs d'un réseau

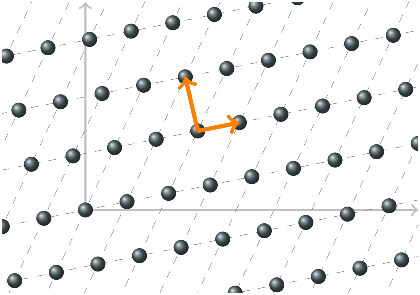
- On peut étudier ses minima successifs



λ_2 : il existe 2 vecteurs lin. indép. $\leq \lambda_2$

Attributs d'un réseau

- On peut étudier ses minima successifs



NP-difficile à calculer $\rightarrow$ pas de réduction viable.

Questions classiques

Les réseaux comme expression de réponse à des questions classiques

- Empilement structuré le plus dense
- Empilement non-structuré le plus dense
- Nombre de contact (kissing number)

$$\gamma(\mathcal{L}) = \frac{\lambda_1(\mathcal{L})}{\sqrt[n]{\det \mathcal{L}}}$$

$\min \gamma(\mathcal{L})$ connu en dim. ≤ 8 et 24.

Les réseaux comme expression de réponse à des questions classiques

- Empilement structuré le plus dense
- Empilement non-structuré le plus dense
- Nombre de contact (kissing number)

Théorème de Hales (1998)
Dimension 3 $\rightarrow \mathbb{D}_3$.

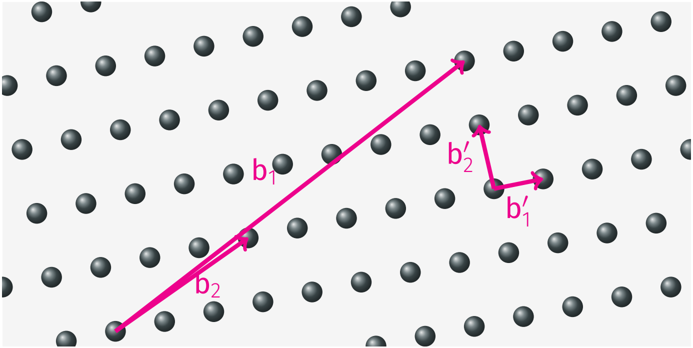
Les réseaux comme expression de réponse à des questions classiques

- Empilement structuré le plus dense
- Empilement non-structuré le plus dense
- Nombre de contact (kissing number)

Connu en dimension ≤ 4, 8 et 24.

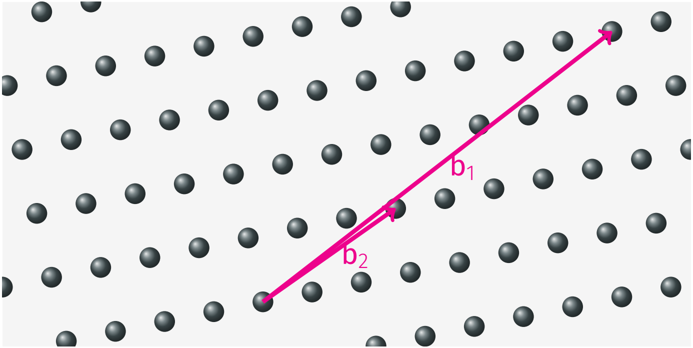
L'algorithme LLL

Toutes les bases ne se valent pas



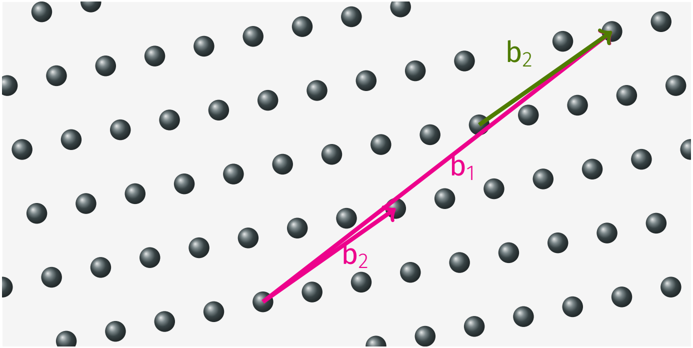
La base (b'_1, b'_2) est plus adaptée car plus « orthonormée ».

Exemple visuel en rang 2



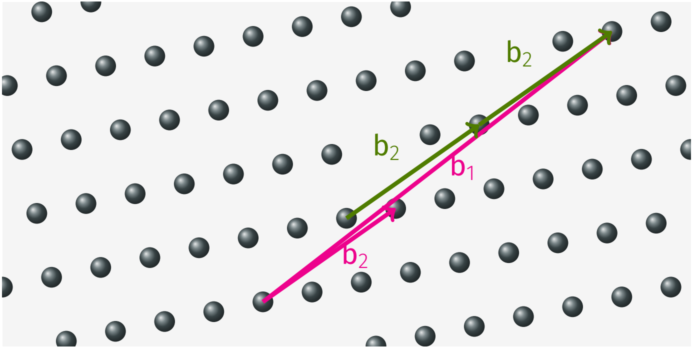
On peut toujours racourcir le grand vecteur d'une base en retranchant des multiples du petit vecteur.

Exemple visuel en rang 2



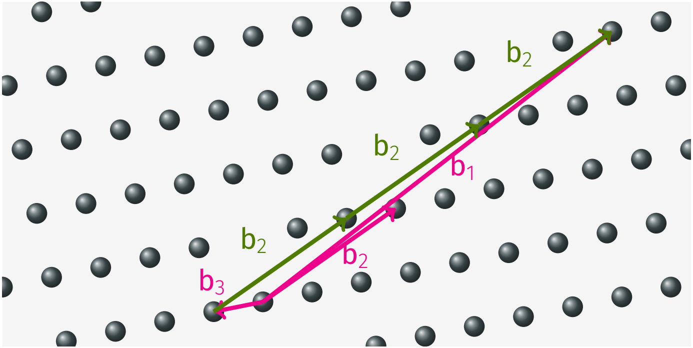
On peut toujours racourcir le grand vecteur d'une base en retranchant des multiples du petit vecteur.

Exemple visuel en rang 2



On peut toujours racourcir le grand vecteur d'une base en retranchant des multiples du petit vecteur.

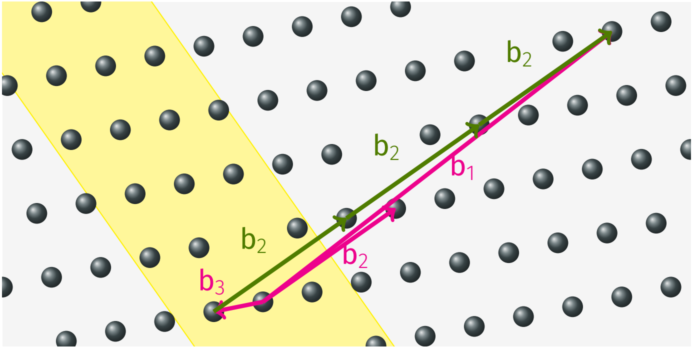
Exemple visuel en rang 2



On peut toujours racourcir le grand vecteur d'une base en retranchant des multiples du petit vecteur.

Base $(\mathbf{b}_1, \mathbf{b}_2) \to (\mathbf{b}_2, \mathbf{b}_3)$ $\qquad \mathbf{b}_1 = q_1 \mathbf{b}_2 + \mathbf{b}_3.$

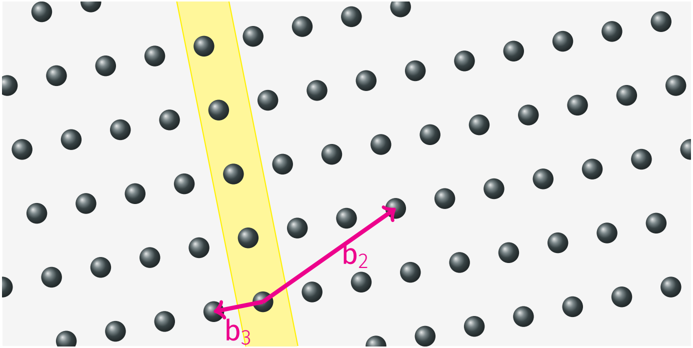
Exemple visuel en rang 2



On peut toujours racourcir le grand vecteur d'une base en retranchant des multiples du petit vecteur.

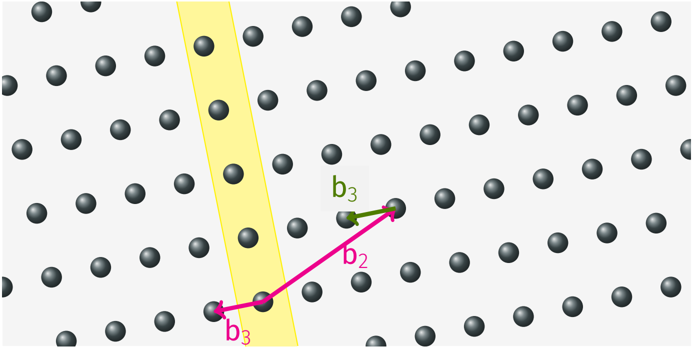
Base $(\mathbf{b}_1, \mathbf{b}_2) \to (\mathbf{b}_2, \mathbf{b}_3)$ $\qquad \mathbf{b}_1 = q_1\mathbf{b}_2 + \mathbf{b}_3.$

Exemple visuel en rang 2 (suite)



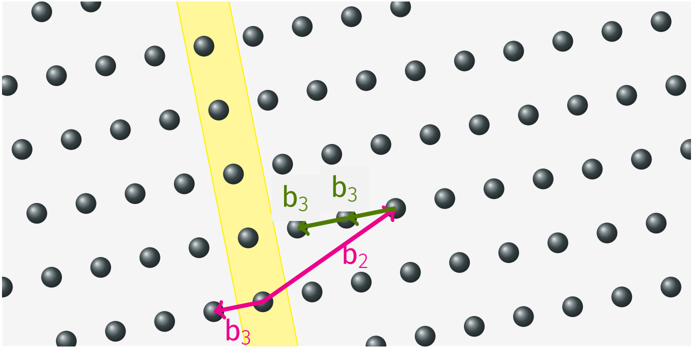
Et recommencer

Exemple visuel en rang 2 (suite)



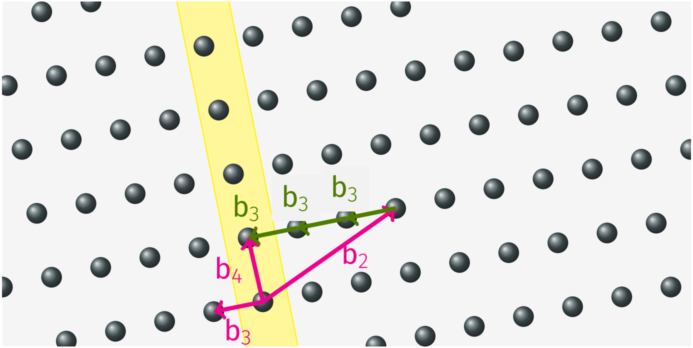
Et recommencer

Exemple visuel en rang 2 (suite)



Et recommencer

Exemple visuel en rang 2 (suite)



Et recommencer

Base $(\mathbf{b}_2, \mathbf{b}_3) \to (\mathbf{b}_3, \mathbf{b}_4)$ $\qquad \mathbf{b}_2 = q_2\mathbf{b}_3 + \mathbf{b}_4.$

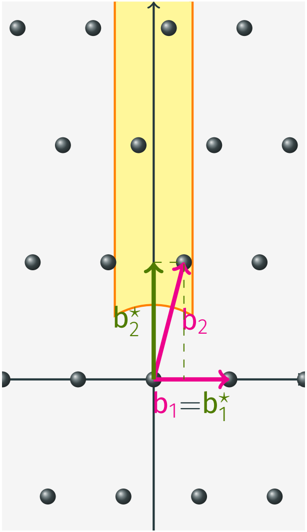
$$\vdots$$

Base $(\mathbf{b}_r, \mathbf{b}_{r+1}) \to (\mathbf{b}_{r+1}, \mathbf{b}_{r+2})$ $\qquad \mathbf{b}_r = q_r\mathbf{b}_{r+1} + \mathbf{b}_{r+2}.$

Définition
Soit $(\mathbf{b}_1^\star, \mathbf{b}_2^\star)$ la base de Gram-Schmidt de $\mathbf{b}_1, \mathbf{b}_2$.
Une base $(\mathbf{b}_1, \mathbf{b}_2)$ est réduite si

1. $\|\mathbf{b}_1\| \leq \|\mathbf{b}_2\|$
2. $\mathbf{b}_2 = \mathbf{b}_2^\star + \mu \mathbf{b}_1^\star$ avec $|\mu| \leq \frac{1}{2}$.

Théorème
La base réduite atteint les minima successifs.



Réduction en rang 2

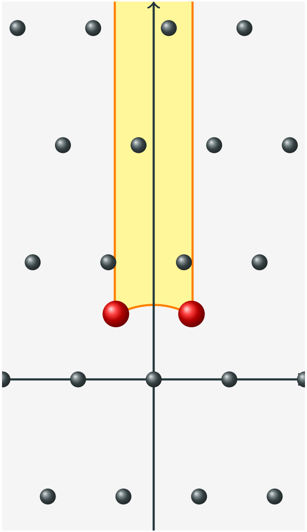
Définition
Soit $(\mathbf{b}_1^\star, \mathbf{b}_2^\star)$ la base de Gram-Schmidt de $\mathbf{b}_1, \mathbf{b}_2$.
Une base $(\mathbf{b}_1, \mathbf{b}_2)$ est réduite si

1. $\|\mathbf{b}_1\| \leq \|\mathbf{b}_2\|$
2. $\mathbf{b}_2 = \mathbf{b}_2^\star + \mu \mathbf{b}_1^\star$ avec $|\mu| \leq \frac{1}{2}$.

Théorème
La base réduite atteint les minima successifs.

Observation pour la suite :

$$\frac{3}{4}\|\mathbf{b}_1^\star\|^2 \leq \|\mathbf{b}_2^\star\|^2$$



Définition
Soit $\mathbf{B} = [\mathbf{b}_1, \ldots, \mathbf{b}_n]$ une base et $\mathbf{B}^\star = [\mathbf{b}_1^\star, \ldots, \mathbf{b}_n^\star]$ sa base de Gram-Schmidt. On note la matrice de passage $\mathbf{B} = \mathbf{B}^\star \mu$.

La base $\mathbf{B}$ est LLL -réduite si

1. pour tout $i < j$, $|\mu_{j,i}| \leq \dfrac{1}{2}$
2. pour tout i, $\left\|\mathbf{b}_i^\star\right\|^2 \leq 2\|\mathbf{b}_{i+1}^\star\|^2$

L'algorithme LLL (Esquisse)

Algorithme

1. Par des transvections $\mathbf{b}_i \leftarrow \mathbf{b}_i - \lfloor \mu_{j,i} \rceil \mathbf{b}_j$, satisfaire la condition 1 (attention à l'ordre des indices).
2. Si $\left\| \mathbf{b}^\star_{i_0} \right\|^2 \leq 2 \left\| \mathbf{b}^\star_{i_0+1} \right\|^2$, échanger $\mathbf{b}_{i_0}$ et $\mathbf{b}_{i_0+1}$ et recommencer.

Théorème

Cette procédure s'arrête en temps polynomial.

Preuve : La quantité $\prod_{i \leq n} |\det(\langle \mathbf{b}_1, \ldots, \mathbf{b}_i \rangle)| \in \mathbb{N}$ décroit d'un facteur multiplicatif à chaque itération.

Propriétés : LLL comme solveur SVP

La réduction LLL est un compromis « temps polynomial vs base avec de bonnes propriétés ».

En petite dimension, le premier vecteur d'une base LLL réduite est souvent un plus court vecteur du réseau.
$\rightarrow$ résolution en temps polynômial d'un problème **NP**-difficile.

Théorème

$$\|\mathbf{b}_1\| \leq 2^{(n-1)/2}\lambda_1.$$

$\rightarrow$ algorithme d'approximation.

Application : retrouver une relation entre réels

Connus : $n_1, n_2, \ldots, n_r \in \mathbb{R}$ approchés.
Inconnus : $\alpha_1, \alpha_2, \ldots, \alpha_r \in \mathbb{Z}$ tels que

$$\alpha_1 n_1 + \cdots + \alpha_r n_r = 0$$

Pour M grand, on pose

$$\mathbf{B} = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & 1 \\ \lfloor M n_1 \rceil & \lfloor M n_2 \rceil & \cdots & \lfloor M n_r \rceil \end{pmatrix} \qquad \mathbf{v} = \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_r \\ \simeq 0 \end{pmatrix}$$

Fait : $\mathbf{v} \in \langle \mathbf{B} \rangle$ avec $\|\mathbf{v}\|$ petit.
Heuristique : LLL retrouve $\mathbf{v}$ en tant que court vecteur de $\langle \mathbf{B} \rangle$.