

TP3 : Réseaux euclidiens

Résumé du TP

Bertrand Meyer

27 novembre 2019

Contexte

Les réseaux euclidiens

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.

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



Perspective historique de la notion de réseau

Géométrie des nombres (Minkowski ~ 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**)

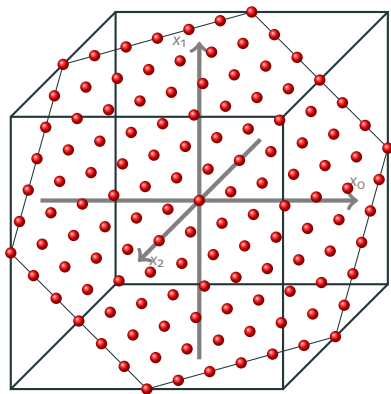
Problèmes **NP**-difficiles (XXIe s.)

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

Quelques exemples : le réseau hexagonal \mathbb{A}_2

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**

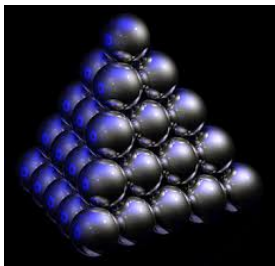


Quelques exemples : le réseau cubique face centré $\mathbb{A}_3 \simeq \mathbb{D}_3$

Définition

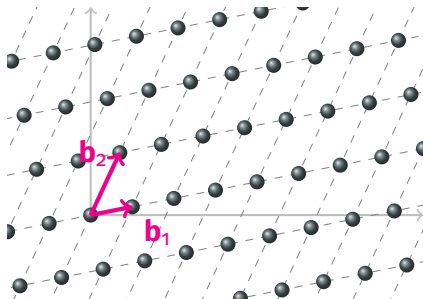
$$\mathbb{A}_3 = \{(x_0, x_1, x_2, x_3) \in \mathbb{Z}^4; x_0 + x_1 + x_2 + x_3 = 0\}$$

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



Attributs d'un réseau

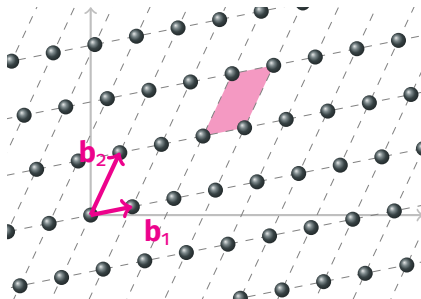
- Un réseau se décrit par une **base**



$$\mathbf{B} = [\mathbf{b}_1, \mathbf{b}_2, \dots, \mathbf{b}_m] \in \mathbb{R}^{n \times m}$$

Attributs d'un réseau

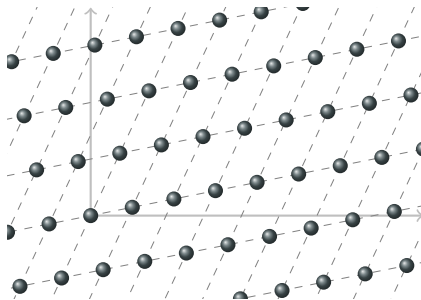
- Un réseau possède un **déterminant**



$$\det \mathcal{L} = \det(\mathbf{B}^\top \mathbf{B}) \quad \text{disc } \mathcal{L} = \sqrt{\det(\mathbf{B}^\top \mathbf{B})} = \text{Vol}(\mathcal{L})$$

Attributs d'un réseau

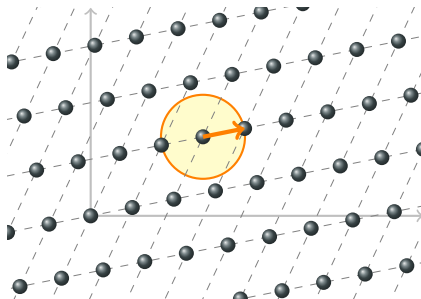
- On peut étudier ses **minima successifs**



Se notent λ_1 , λ_2 , etc.

Attributs d'un réseau

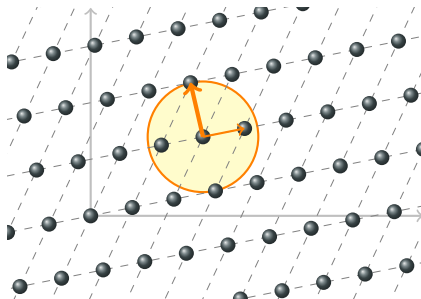
- On peut étudier ses **minima successifs**



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

Attributs d'un réseau

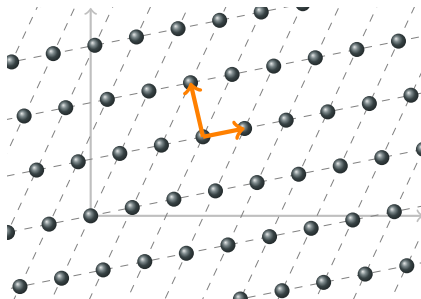
- On peut étudier ses **minima successifs**



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 → 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 $\dim. \leq 8$ et **24**.

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)



Théorème de Hales (1998)

Dimension **3** $\rightarrow \mathbb{D}_3$.

Questions classiques

Les réseaux comme expression de réponse à des questions classiques

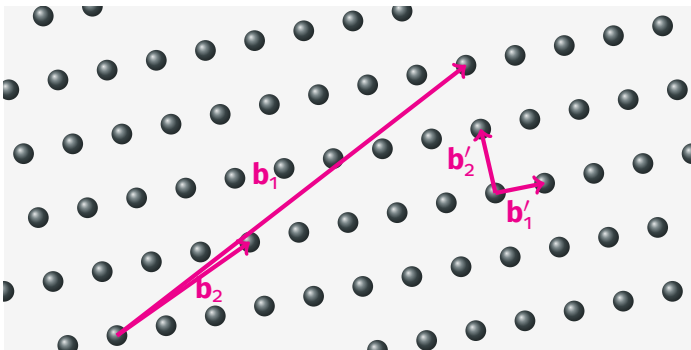
- Empilement structuré le plus dense
- Empilement non-structuré le plus dense
- **Nombre de contact** (kissing number)



Connu en dimension ≤ 4 , 8 et 24.

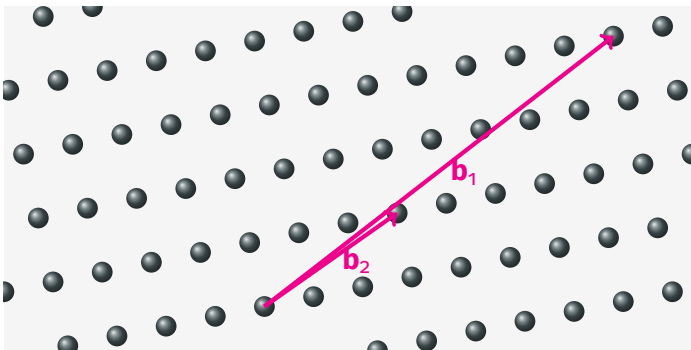
L'algorithme LLL

Toutes les bases ne se valent pas



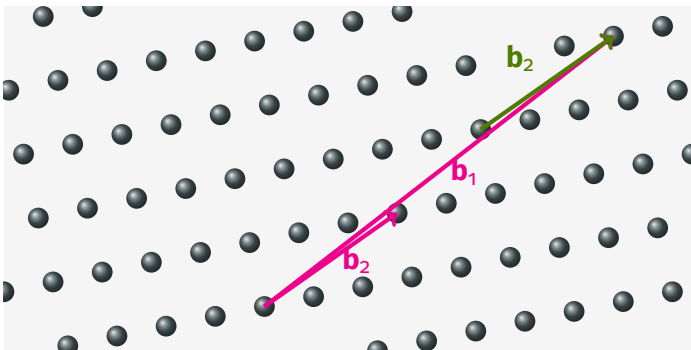
La base $(\mathbf{b}'_1, \mathbf{b}'_2)$ est plus adaptée car plus « orthonormée ».

Exemple visuel en rang 2



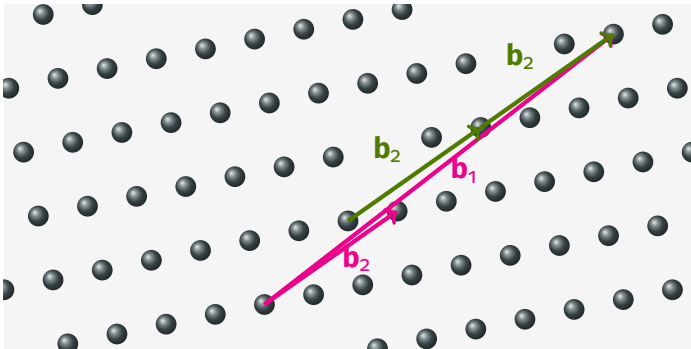
On peut toujours **racourcir** le **grand vecteur** d'une base en retranchant des multiples du petit vecteur.

Exemple visuel en rang 2



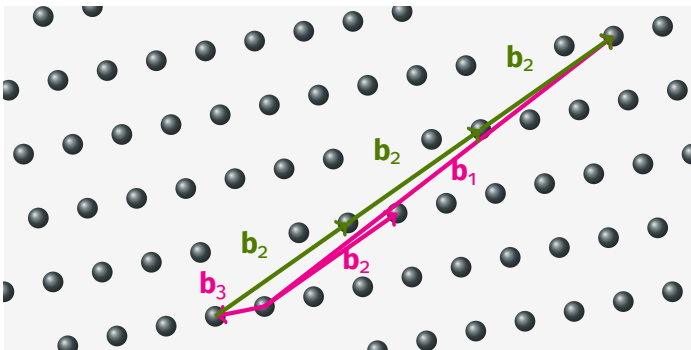
On peut toujours **racourcir** le **grand vecteur** d'une base en retranchant des multiples du petit vecteur.

Exemple visuel en rang 2



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

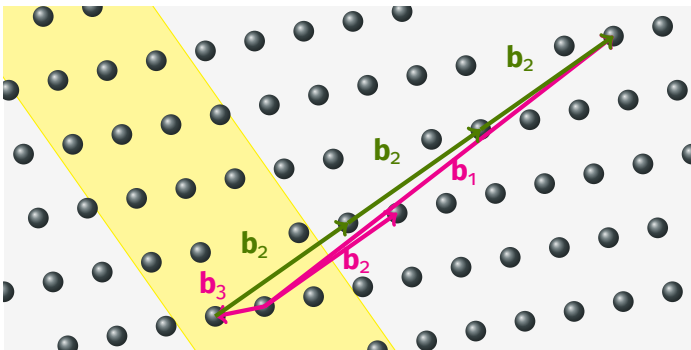
Exemple visuel en rang 2



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

$$\text{Base } (\mathbf{b}_1, \mathbf{b}_2) \rightarrow (\mathbf{b}_2, \mathbf{b}_3) \quad \mathbf{b}_1 = q_1 \mathbf{b}_2 + \mathbf{b}_3.$$

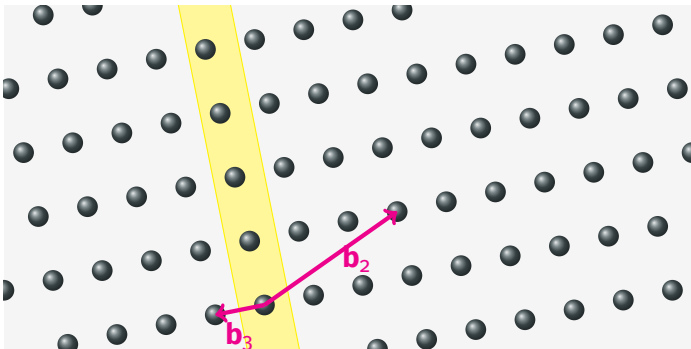
Exemple visuel en rang 2



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

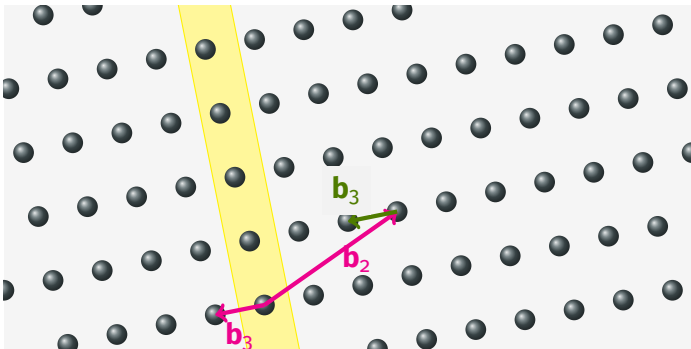
$$\text{Base } (\mathbf{b}_1, \mathbf{b}_2) \rightarrow (\mathbf{b}_2, \mathbf{b}_3) \quad \mathbf{b}_1 = q_1 \mathbf{b}_2 + \mathbf{b}_3.$$

Exemple visuel en rang 2 (suite)



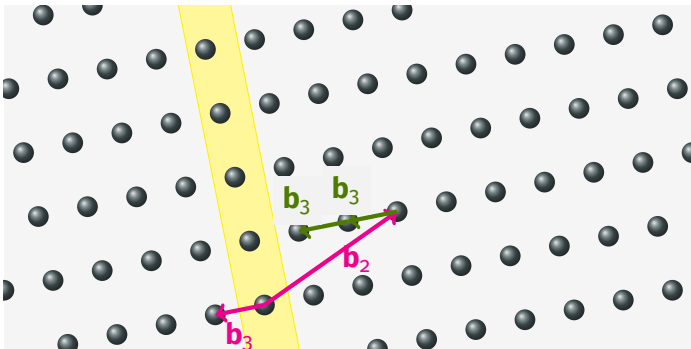
Et recommencer

Exemple visuel en rang 2 (suite)



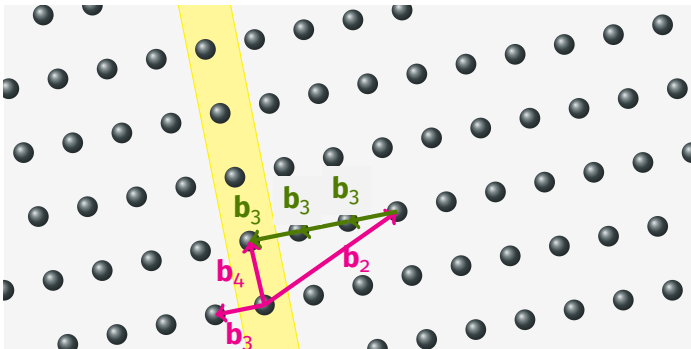
Et recommencer

Exemple visuel en rang 2 (suite)



Et recommencer

Exemple visuel en rang 2 (suite)



Et recommencer

$$\text{Base } (\mathbf{b}_2, \mathbf{b}_3) \rightarrow (\mathbf{b}_3, \mathbf{b}_4) \quad \mathbf{b}_2 = q_2 \mathbf{b}_3 + \mathbf{b}_4.$$

\vdots

$$\text{Base } (\mathbf{b}_r, \mathbf{b}_{r+1}) \rightarrow (\mathbf{b}_{r+1}, \mathbf{b}_{r+2}) \quad \mathbf{b}_r = q_r \mathbf{b}_{r+1} + \mathbf{b}_{r+2}.$$

Réduction en rang 2

Définition

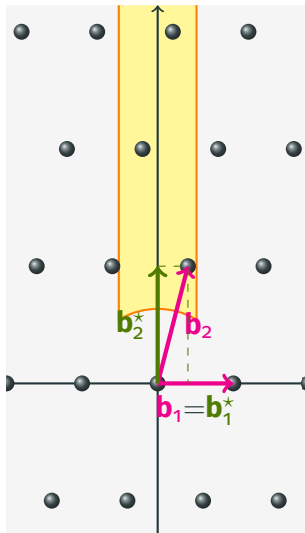
Soit $(\mathbf{b}_1^*, \mathbf{b}_2^*)$ la base de Gram-Schmidt de $\mathbf{b}_1, \mathbf{b}_2$.

Une base $(\mathbf{b}_1, \mathbf{b}_2)$ est **réduite** si

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

Théorème

La base réduite atteint les minima successifs.



Réduction en rang 2

Définition

Soit $(\mathbf{b}_1^*, \mathbf{b}_2^*)$ la base de Gram-Schmidt de $\mathbf{b}_1, \mathbf{b}_2$.

Une base $(\mathbf{b}_1, \mathbf{b}_2)$ est **réduite** si

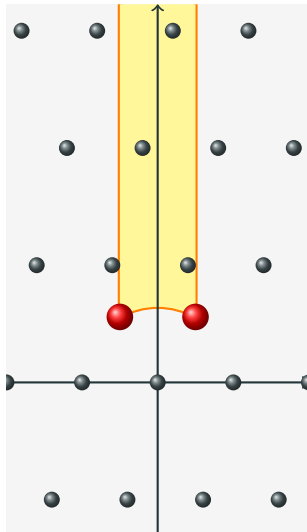
1. $\|\mathbf{b}_1\| \leq \|\mathbf{b}_2\|$
2. $\mathbf{b}_2 = \mathbf{b}_2^* + \mu \mathbf{b}_1^*$ avec $|\mu| \leq \frac{1}{2}$.

Théorème

La base réduite atteint les minima successifs.

Observation pour la suite :

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



Les bases LLL réduites

Définition

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

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

1. pour tout $i < j$, $|\mu_{j,i}| \leq \frac{1}{2}$
2. pour tout i , $\|\mathbf{b}_i^*\|^2 \leq 2\|\mathbf{b}_{i+1}^*\|^2$

L'algorithme LLL (Esquisse)

Algorithme

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

Théorème

Cette procédure s'arrête en temps polynomial.

Preuve : La quantité $\prod_{i \leq n} |\det(\langle \mathbf{b}_1, \dots, \mathbf{b}_i \rangle)| \in \mathbb{N}$ décroît 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.

→ résolution en temps polynomial d'un problème **NP**-difficile.

Théorème

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

→ algorithme d'approximation.

Application : retrouver une relation entre réels

Connus : $n_1, n_2, \dots, n_r \in \mathbb{R}$ approchés.

Inconnus : $\alpha_1, \alpha_2, \dots, \alpha_r \in \mathbb{Z}$ tels que

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

Pour M grand, on pose

$$\mathbf{B} = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \dots & 0 & 1 \\ [Mn_1] & [Mn_2] & \dots & [Mn_r] \end{pmatrix} \quad \mathbf{v} = \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_r \\ \simeq 0 \end{pmatrix}$$

Fait : $\mathbf{v} \in \langle \mathbf{B} \rangle$ avec $\|\mathbf{v}\|$ petit.

Heuristique : LLL **retrouve** \mathbf{v} en tant que court vecteur de $\langle \mathbf{B} \rangle$.