Réduction de réseaux: Adaptations d'idées provenant du cas polynomial au cas entier.

Lucas Petit
Encadrant: Romain Lebreton

3 juillet 2025

Réseaux euclidiens

[1] où $\mathcal{B}(\mathbf{x}, \varepsilon)$ désigne la boule ouverte de rayon ε centrée en $\mathbf{x}$.

Réseaux euclidiens

Un **réseau euclidien** $\mathscr{L}$ est un sous-groupe discret additif de $\mathbb{R}^n$.

[1] où $\mathcal{B}(\mathbf{x}, \varepsilon)$ désigne la boule ouverte de rayon ε centrée en $\mathbf{x}$.

Réseaux euclidiens

Un **réseau euclidien** $\mathscr{L}$ est un sous-groupe discret additif de $\mathbb{R}^n$.

$\rightarrow$ **Sous-groupe additif:**

$$\mathbf{0} \in \mathscr{L}, \mathbf{x}+\mathbf{y} \in \mathscr{L}, \ -\mathbf{x} \in \mathscr{L} \text{ pour tout } \mathbf{x}, \mathbf{y} \in \mathscr{L}.$$

[1] où $\mathcal{B}(\mathbf{x}, \varepsilon)$ désigne la boule ouverte de rayon ε centrée en $\mathbf{x}$.

Réseaux euclidiens

Un **réseau euclidien** $\mathscr{L}$ est un sous-groupe discret additif de $\mathbb{R}^n$.

$\rightarrow$ **Sous-groupe additif:**

$$\mathbf{0} \in \mathscr{L}, \mathbf{x}+\mathbf{y} \in \mathscr{L}, -\mathbf{x} \in \mathscr{L} \text{ pour tout } \mathbf{x}, \mathbf{y} \in \mathscr{L}.$$

$\rightarrow$ **Discret:** Pour tout $\mathbf{x} \in \mathscr{L}$, il existe $\varepsilon > 0$ tel que

$$^{1}\mathcal{B}(\mathbf{x}, \varepsilon) \cap \mathscr{L} = \{\mathbf{x}\}$$

[1] où $\mathcal{B}(\mathbf{x}, \varepsilon)$ désigne la boule ouverte de rayon ε centrée en $\mathbf{x}$.

Réseaux euclidiens

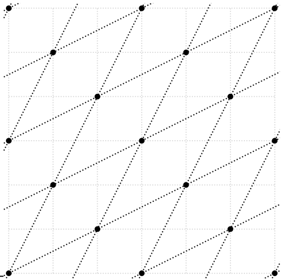
Un **réseau euclidien** $\mathscr{L}$ est un sous-groupe discret additif de $\mathbb{R}^n$.

→ **Sous-groupe additif:**

$$\mathbf{0} \in \mathscr{L}, \mathbf{x} + \mathbf{y} \in \mathscr{L}, \ -\mathbf{x} \in \mathscr{L} \text{ pour tout } \mathbf{x}, \mathbf{y} \in \mathscr{L}.$$

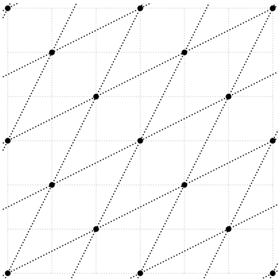
→ **Discret:** Pour tout $\mathbf{x} \in \mathscr{L}$, il existe $\varepsilon > 0$ tel que

$$^1\mathcal{B}(\mathbf{x}, \varepsilon) \cap \mathscr{L} = \{\mathbf{x}\}$$



[1] où $\mathcal{B}(\mathbf{x}, \varepsilon)$ désigne la boule ouverte de rayon ε centrée en $\mathbf{x}$.

Base d'un réseau euclidien

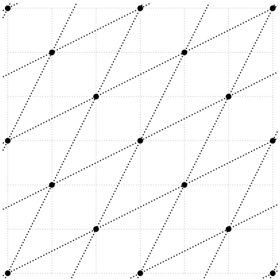


Base d'un réseau euclidien

Tout réseau $\mathscr{L} \subseteq \mathbb{R}^n$ admet une famille $\mathbb{Z}$-libre maximale $(\mathbf{b}_i)_{1\leq i \leq m}$, avec $m \leq n$ tel que:

$$\mathscr{L} = \bigoplus_{i=1}^{m} \mathbb{Z}\mathbf{b}_i = \{a_1\mathbf{b}_1 + \cdots + a_m\mathbf{b}_m \mid a_i \in \mathbb{Z}\}$$

Cette famille est appelée une **base** du réseau $\mathscr{L}$.

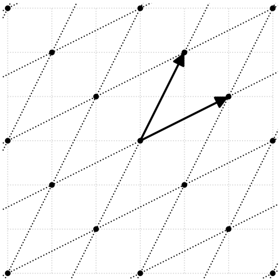


Base d'un réseau euclidien

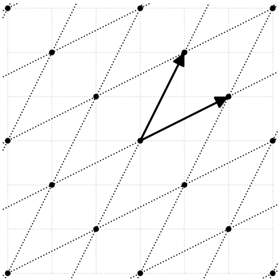
Tout réseau $\mathscr{L} \subseteq \mathbb{R}^n$ admet une famille $\mathbb{Z}$-libre maximale $(\mathbf{b}_i)_{1 \leq i \leq m}$, avec $m \leq n$ tel que:

$$\mathscr{L} = \bigoplus_{i=1}^{m} \mathbb{Z}\mathbf{b}_i = \{a_1\mathbf{b}_1 + \cdots + a_m\mathbf{b}_m \mid a_i \in \mathbb{Z}\}$$

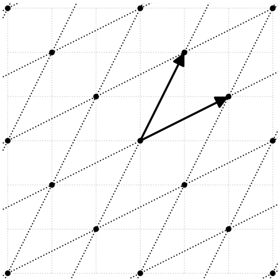
Cette famille est appelée une **base** du réseau $\mathscr{L}$.



Deux bases différentes du même réseau

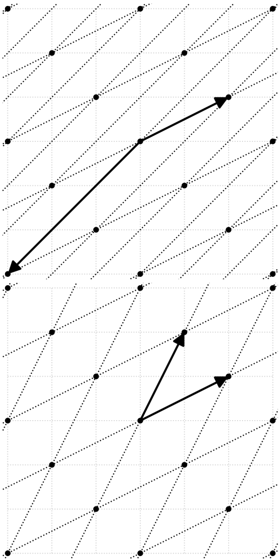


Deux bases différentes du même réseau



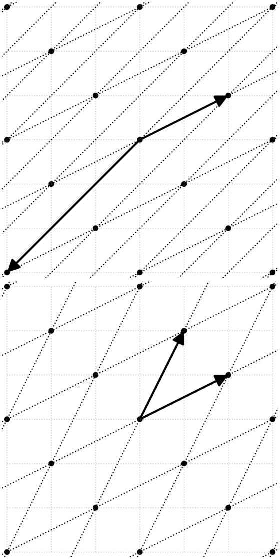
Vecteurs courts
"Orthogonaux"

Deux bases différentes du même réseau



Vecteurs courts
"Orthogonaux"

Deux bases différentes du même réseau



Vecteurs longs
Peu orthogonaux

Vecteurs courts
"Orthogonaux"

Réduction utopique et cryptographie

Réduction utopique et cryptographie

On appelle **minimums d'un réseau** $\mathscr{L}$:

$$\lambda_1(\mathscr{L}) = \min_{\substack{v \in \mathscr{L} \\ v \neq 0}} \|v\|, \quad \lambda_2(\mathscr{L}) = \cdots$$

On appelle **minimums d'un réseau** $\mathscr{L}$:

$$\lambda_1(\mathscr{L}) = \min_{\substack{v \in \mathscr{L} \\ v \neq 0}} \|v\|, \quad \lambda_2(\mathscr{L}) = \cdots$$

Shortest Independant Vector Problem ($_\gamma\mathrm{SIVP}$)
On veut une base $(\mathbf{b}_i)_{1 \leq i \leq n}$ de $\mathscr{L}$ tel que:

$$\|\mathbf{b}_1\| = \gamma(n) \cdot \lambda_1(\mathscr{L}), \quad \|\mathbf{b}_2\| = \gamma(n) \cdot \lambda_2(\mathscr{L}), \quad \ldots, \quad \|\mathbf{b}_n\| = \gamma(n) \cdot \lambda_n(\mathscr{L})$$

Réduction utopique et cryptographie

On appelle **minimums d'un réseau** $\mathscr{L}$:

$$\lambda_1(\mathscr{L}) = \min_{\substack{v \in \mathscr{L} \\ v \neq 0}} \|v\|, \quad \lambda_2(\mathscr{L}) = \cdots$$

Shortest Independant Vector Problem ($_\gamma\mathrm{SIVP}$)
On veut une base $(\mathbf{b}_i)_{1 \leq i \leq n}$ de $\mathscr{L}$ tel que:

$$\|\mathbf{b}_1\| = \gamma(n) \cdot \lambda_1(\mathscr{L}), \quad \|\mathbf{b}_2\| = \gamma(n) \cdot \lambda_2(\mathscr{L}), \quad \ldots, \quad \|\mathbf{b}_n\| = \gamma(n) \cdot \lambda_n(\mathscr{L})$$

$\gamma(n) = \mathcal{O}(1)$ $\qquad$ SIVP — **NP-difficile** (Ajtai, 1996)

Réduction utopique et cryptographie

On appelle **minimums d'un réseau** $\mathscr{L}$:

$$\lambda_1(\mathscr{L}) = \min_{\substack{v \in \mathscr{L} \\ v \neq 0}} \|v\|, \quad \lambda_2(\mathscr{L}) = \cdots$$

Shortest Independant Vector Problem ($_\gamma\mathrm{SIVP}$)
On veut une base $(\mathbf{b}_i)_{1 \leq i \leq n}$ de $\mathscr{L}$ tel que:

$$\|\mathbf{b}_1\| = \gamma(n) \cdot \lambda_1(\mathscr{L}), \quad \|\mathbf{b}_2\| = \gamma(n) \cdot \lambda_2(\mathscr{L}), \quad \ldots, \quad \|\mathbf{b}_n\| = \gamma(n) \cdot \lambda_n(\mathscr{L})$$

$\gamma(n) = \mathcal{O}(1)$ SIVP — **NP-difficile** (Ajtai, 1996)
$\gamma(n) = \mathrm{poly}(n)$ **Cryptographie** à base de réseaux (Conjecturé difficile)

Réduction utopique et cryptographie

On appelle **minimums d'un réseau** $\mathscr{L}$:

$$\lambda_1(\mathscr{L}) = \min_{\substack{v \in \mathscr{L} \\ v \neq 0}} \|v\|, \quad \lambda_2(\mathscr{L}) = \cdots$$

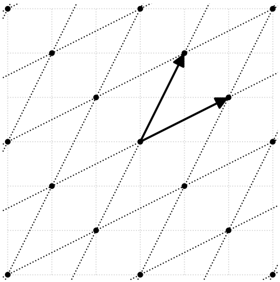
Shortest Independant Vector Problem ($_\gamma\mathrm{SIVP}$)
On veut une base $(\mathbf{b}_i)_{1 \leq i \leq n}$ de $\mathscr{L}$ tel que:

$$\|\mathbf{b}_1\| = \gamma(n) \cdot \lambda_1(\mathscr{L}), \quad \|\mathbf{b}_2\| = \gamma(n) \cdot \lambda_2(\mathscr{L}), \quad \ldots, \quad \|\mathbf{b}_n\| = \gamma(n) \cdot \lambda_n(\mathscr{L})$$

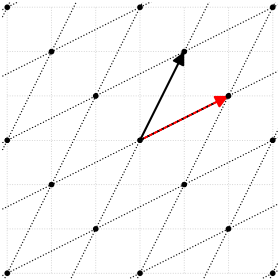
$\gamma(n) = \mathcal{O}(1)$ — SIVP — **NP-difficile** (Ajtai, 1996)
$\gamma(n) = \mathrm{poly}(n)$ — **Cryptographie** à base de réseaux (Conjecturé difficile)
$\gamma(n) = 2^{\mathcal{O}(n)}$ — **Temps polynomial** (Lenstra, Lenstra, Lovasz, 1982)

Orthogonalisation dans les $\mathbb{R}$ – espaces vectoriels

Orthogonalisation dans les $\mathbb{R}$ – espaces vectoriels

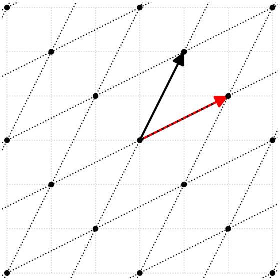


Orthogonalisation dans les $\mathbb{R}$ – espaces vectoriels



$\mathbb{R} \rightarrow$ procédé d'orthogonalisation de Gram–Schmidt.

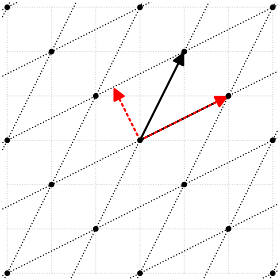
Orthogonalisation dans les $\mathbb{R}$ – espaces vectoriels



$b_1^* \leftarrow b_1$

$\mathbb{R} \rightarrow$ procédé d'orthogonalisation de Gram–Schmidt.

Orthogonalisation dans les $\mathbb{R}$ – espaces vectoriels

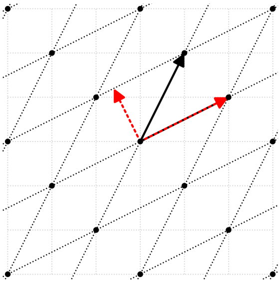


$$b_1^* \leftarrow b_1$$

$$b_2^* \leftarrow b_2 - \frac{\langle b_2, b_1^* \rangle}{\|b_1^*\|^2} b_1^*$$

$\mathbb{R} \rightarrow$ procédé d'orthogonalisation de Gram–Schmidt.

Orthogonalisation dans les $\mathbb{R}$ – espaces vectoriels

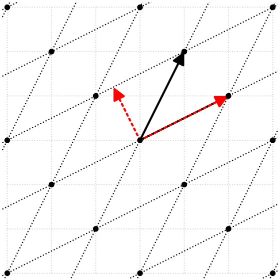


$b_1^* \leftarrow b_1$

$b_2^* \leftarrow b_2 - \frac{4}{5} b_1^*$

$\mathbb{R} \rightarrow$ procédé d'orthogonalisation de Gram–Schmidt.

Orthogonalisation dans les $\mathbb{R}$ – espaces vectoriels



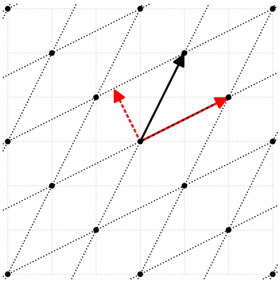
$b_1^* \leftarrow b_1$

$b_2^* \leftarrow b_2 - \frac{4}{5} b_1^*$

$\mathbb{R} \rightarrow$ procédé d'orthogonalisation de Gram–Schmidt.

$$\underbrace{\begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}}_{\mathcal{B}} = \underbrace{\begin{pmatrix} 1 & 0 \\ \frac{4}{5} & 1 \end{pmatrix}}_{U} \times \underbrace{\begin{pmatrix} 2 & 1 \\ \frac{-3}{5} & \frac{6}{5} \end{pmatrix}}_{\mathcal{B}^*}$$

Orthogonalisation dans les $\mathbb{R}$ – espaces vectoriels



$b_1^* \leftarrow b_1$

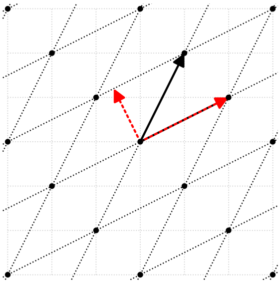
$b_2^* \leftarrow b_2 - \frac{4}{5} b_1^*$

$\mathbb{R} \rightarrow$ procédé d'orthogonalisation de Gram–Schmidt.

$$\underbrace{\begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}}_{\mathcal{B}} = \underbrace{\begin{pmatrix} 1 & 0 \\ \frac{4}{5} & 1 \end{pmatrix}}_{U} \times \underbrace{\begin{pmatrix} 2 & 1 \\ \frac{-3}{5} & \frac{6}{5} \end{pmatrix}}_{\mathcal{B}^*}$$

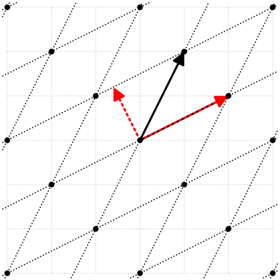
Les coefficients $\mu_{i,j}$ sont appelés coefficients de **Gram–Schmidt**.

Orthogonalisation dans les $\mathbb{Z}$ – espaces vectoriels



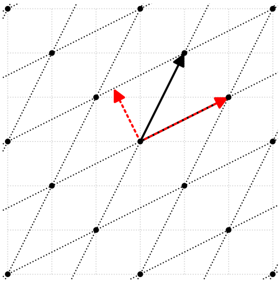
$$\underbrace{\begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}}_{\mathcal{B}} = \underbrace{\begin{pmatrix} 1 & 0 \\ \frac{4}{5} & 1 \end{pmatrix}}_{U} \times \underbrace{\begin{pmatrix} 2 & 1 \\ \frac{-3}{5} & \frac{6}{5} \end{pmatrix}}_{\mathcal{B}^*}$$

Orthogonalisation dans les $\mathbb{Z}$ – espaces vectoriels



Problème: $\mathcal{B}^*$ pas une base de $\mathscr{L}(\mathcal{B})$.

$$\underbrace{\begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}}_{\mathcal{B}} = \underbrace{\begin{pmatrix} 1 & 0 \\ \frac{4}{5} & 1 \end{pmatrix}}_{U} \times \underbrace{\begin{pmatrix} 2 & 1 \\ \frac{-3}{5} & \frac{6}{5} \end{pmatrix}}_{\mathcal{B}^*}$$

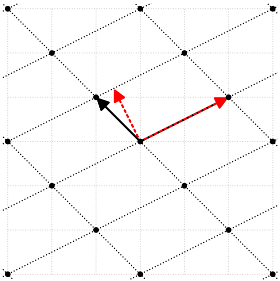


Problème: $\mathcal{B}^*$ pas une base de $\mathscr{L}(\mathcal{B})$.

$\mathbb{Z} \to$ Gram–Schmidt discret.

$$\underbrace{\begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}}_{\mathcal{B}} = \underbrace{\begin{pmatrix} 1 & 0 \\ \frac{4}{5} & 1 \end{pmatrix}}_{U} \times \underbrace{\begin{pmatrix} 2 & 1 \\ \frac{-3}{5} & \frac{6}{5} \end{pmatrix}}_{\mathcal{B}^*}$$

Orthogonalisation dans les $\mathbb{Z}$ – espaces vectoriels

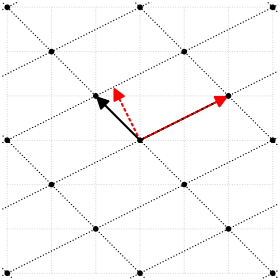


Problème: $\mathcal{B}^*$ pas une base de $\mathscr{L}(\mathcal{B})$.

$\mathbb{Z} \rightarrow$ Gram–Schmidt discret.

$$\underbrace{\begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}}_{\mathcal{B}} = \underbrace{\begin{pmatrix} 1 & 0 \\ \frac{4}{5} & 1 \end{pmatrix}}_{U} \times \underbrace{\begin{pmatrix} 2 & 1 \\ \frac{-3}{5} & \frac{6}{5} \end{pmatrix}}_{\mathcal{B}^*}$$

Orthogonalisation dans les $\mathbb{Z}$ – espaces vectoriels

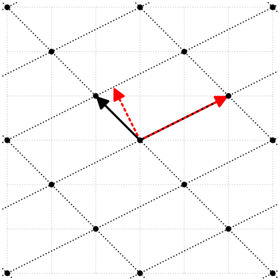


Problème: $\mathcal{B}^*$ pas une base de $\mathscr{L}(\mathcal{B})$.

$\mathbb{Z} \rightarrow$ Gram–Schmidt discret.

$$\underbrace{\begin{pmatrix} 2 & 1 \\ -1 & 1 \end{pmatrix}}_{\mathcal{B}} = \underbrace{\begin{pmatrix} 1 & 0 \\ \frac{1}{5} & 1 \end{pmatrix}}_{U} \times \underbrace{\begin{pmatrix} 2 & 1 \\ \frac{-3}{5} & \frac{6}{5} \end{pmatrix}}_{\mathcal{B}^*}$$

Orthogonalisation dans les $\mathbb{Z}$ – espaces vectoriels



Problème: $\mathcal{B}^*$ pas une base de $\mathscr{L}(\mathcal{B})$.

$\mathbb{Z} \rightarrow$ Gram–Schmidt discret.

$$\underbrace{\begin{pmatrix} 2 & 1 \\ -1 & 1 \end{pmatrix}}_{\mathcal{B}} = \underbrace{\begin{pmatrix} 1 & 0 \\ \frac{1}{5} & 1 \end{pmatrix}}_{U} \times \underbrace{\begin{pmatrix} 2 & 1 \\ \frac{-3}{5} & \frac{6}{5} \end{pmatrix}}_{\mathcal{B}^*}$$

$\mathcal{B}$ est dite **size-réduite** si:

$$\max_{1 \leq j < i \leq n} |\mu_{i,j}| \leq \frac{1}{2}$$

Définition: condition de Lovász

Définition: condition de Lovász

Gram–Schmidt projette, réduit la taille des vecteurs.

Définition: condition de Lovász

Gram–Schmidt projette, réduit la taille des vecteurs.

Utopie pour Gram–Schmidt discret:

$$\|\mathbf{b}_i^*\|^2 \leq \|\mathbf{b}_{i+1}^*\|^2$$

$\rightarrow$ trop difficile, on relache la contrainte

Définition: condition de Lovász

Gram–Schmidt projette, réduit la taille des vecteurs.

Utopie pour Gram–Schmidt discret:

$$\|\mathbf{b}_i^*\|^2 \leq \|\mathbf{b}_{i+1}^*\|^2$$

$\rightarrow$ trop difficile, on relache la contrainte

Condition de Lovàsz (2–quasi croissance) :

$$\|\mathbf{b}_i^*\|^2 \leq 2\|\mathbf{b}_{i+1}^*\|^2$$

Définition: condition de Lovász

Gram–Schmidt projette, réduit la taille des vecteurs.

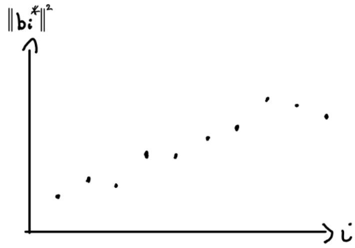
Utopie pour Gram–Schmidt discret:

$$\|\mathbf{b}_i^*\|^2 \leq \|\mathbf{b}_{i+1}^*\|^2$$

$\rightarrow$ trop difficile, on relache la contrainte

Condition de Lovàsz (2–quasi croissance) :

$$\|\mathbf{b}_i^*\|^2 \leq 2\|\mathbf{b}_{i+1}^*\|^2$$



Définition: condition de Lovász

Gram–Schmidt projette, réduit la taille des vecteurs.

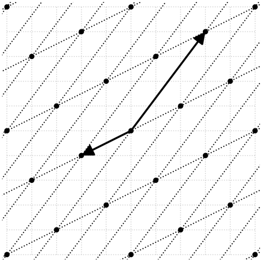
Utopie pour Gram–Schmidt discret:

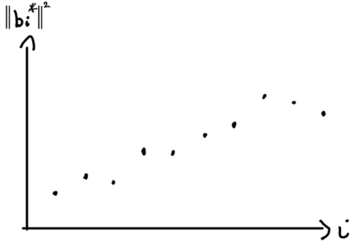
$$\|\mathbf{b}_i^*\|^2 \leq \|\mathbf{b}_{i+1}^*\|^2$$

$\rightarrow$ trop difficile, on relache la contrainte

Condition de Lovàsz (2–quasi croissance) :

$$\|\mathbf{b}_i^*\|^2 \leq 2\|\mathbf{b}_{i+1}^*\|^2$$





Définition: condition de Lovász

Gram–Schmidt projette, réduit la taille des vecteurs.

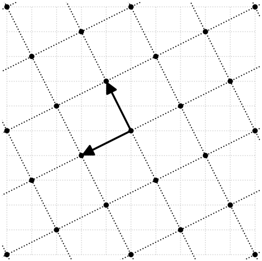
Utopie pour Gram–Schmidt discret:

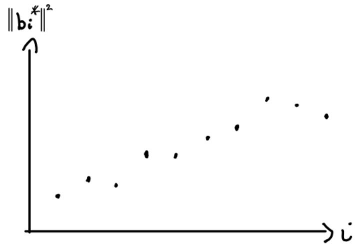
$$\|\mathbf{b}_i^*\|^2 \leq \|\mathbf{b}_{i+1}^*\|^2$$

$\rightarrow$ trop difficile, on relache la contrainte

Condition de Lovàsz (2–quasi croissance) :

$$\|\mathbf{b}_i^*\|^2 \leq 2\|\mathbf{b}_{i+1}^*\|^2$$





Algorithme LLL(Lenstra, Lenstra, Lovàsz, 1982)

Algorithme LLL(Lenstra, Lenstra, Lovàsz, 1982)

Définition: $\mathcal{B} = (\mathbf{b_i})_{1 \leq i \leq n}$ est dite LLL–**réduite** si :

- $\mathcal{B}$ est **size-réduite**.
- $\mathcal{B}$ satisfait la **condition de Lovász**.

Algorithme LLL(Lenstra, Lenstra, Lovàsz, 1982)

Définition: $\mathcal{B} = (\mathbf{b_i})_{1 \leq i \leq n}$ est dite LLL–**réduite** si :

- $\mathcal{B}$ est **size-réduite**.
- $\mathcal{B}$ satisfait la **condition de Lovász**.

Algorithme 0 : *LLL (vulgarisé)*

Entrée : Une base $\mathcal{B} = (\mathbf{b_i})_{1 \leq i \leq n}$ de $\mathscr{L}$.
Sortie : Une base de $\mathscr{L}$ LLL-réduite.

```
Tant que B n'est pas LLL–réduite faire
    size-réduire(B)
    Lovász(B)
Retourner B
```

Algorithme LLL(Lenstra, Lenstra, Lovàsz, 1982)

Définition: $\mathcal{B} = (\mathbf{b_i})_{1 \leq i \leq n}$ est dite LLL**–réduite** si :

- $\mathcal{B}$ est **size-réduite**.
- $\mathcal{B}$ satisfait la **condition de Lovász**.

Algorithme 0 : *LLL (vulgarisé)*

Entrée : Une base $\mathcal{B} = (\mathbf{b_i})_{1 \leq i \leq n}$ de $\mathscr{L}$.
Sortie : Une base de $\mathscr{L}$ LLL-réduite.

```
Tant que B n'est pas LLL–réduite faire
    size-réduire(B)
    Lovász(B)
Retourner B
```

Théorème: LLL utilise $\widetilde{\mathcal{O}}\left(n^5 \log^2\left(\max_{1 \leq i \leq n} \|\mathbf{b}_i\|\right)\right)$ opérations binaires.

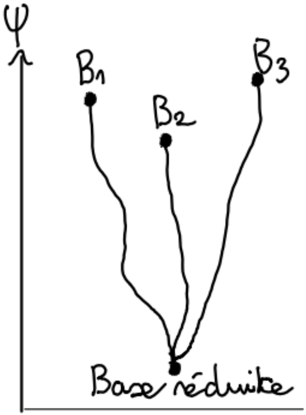
Appropriation du domaine

- Théorie des réseaux euclidiens
- Implémentation efficace de LLL et Gram-Schmidt (SageMath)
- Groupe de travail(interne): cryptographie à base de réseaux
- Analyse et explication vulgarisée de LLL (en anglais)

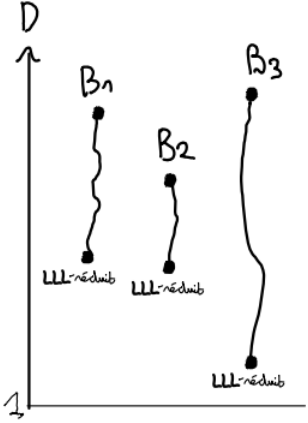
Piste de recherche: qualité de réduction

Piste de recherche: qualité de réduction

Réseaux polynomiaux

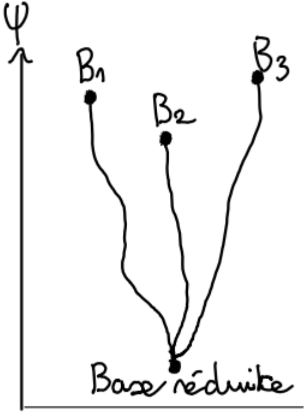


Réseaux euclidiens



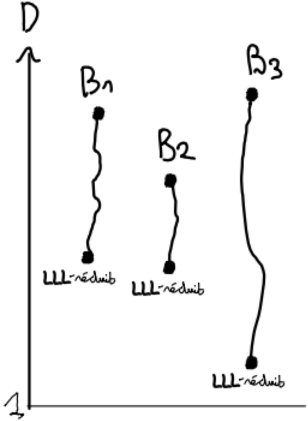
Piste de recherche: qualité de réduction

Réseaux polynomiaux



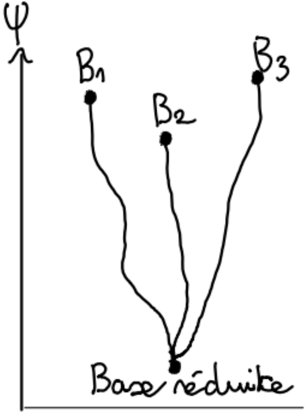
→ unicité de la réduction.

Réseaux euclidiens



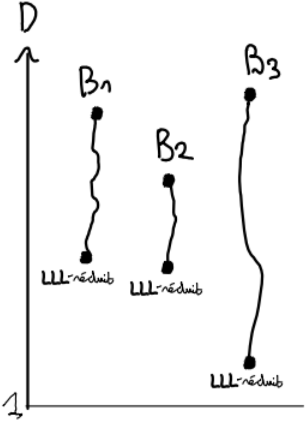
Piste de recherche: qualité de réduction

Réseaux polynomiaux



→ unicité de la réduction.

Réseaux euclidiens

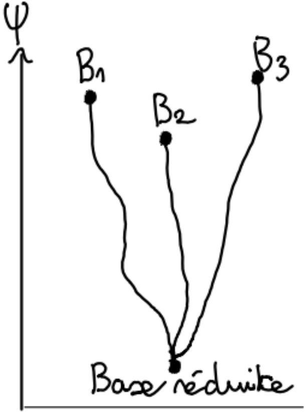


→ pas d'unicité sur la LLL-réduction.

→ utilisé pour terminaison de LLL.

Piste de recherche: qualité de réduction

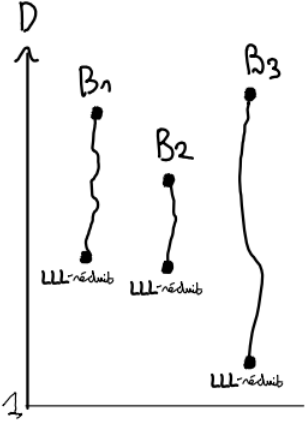
Réseaux polynomiaux



→ unicité de la réduction.

Piste: The lower the D, the better?

Réseaux euclidiens



→ pas d'unicité sur la LLL-réduction.

→ utilisé pour terminaison de LLL.

Réseau défini par une relation

Réseau défini par une relation

Soit $F \in M_n(\mathbb{Z})$, un degré de précision $\sigma \in \mathbb{N}$, et $p \in \mathbb{N}$. On définit :

$$F_{p^\sigma} := \{v \in \mathbb{Z}^n \mid vF = 0 \mod p^\sigma\}$$

Réseau défini par une relation

Soit $F \in M_n(\mathbb{Z})$, un degré de précision $\sigma \in \mathbb{N}$, et $p \in \mathbb{N}$. On définit :

$$F_{p^\sigma} := \{v \in \mathbb{Z}^n \mid vF = 0 \mod p^\sigma\}$$

$\rightarrow$ réseau euclidien, fondamentale en cryptographie

Réseau défini par une relation

Soit $F \in M_n(\mathbb{Z})$, un degré de précision $\sigma \in \mathbb{N}$, et $p \in \mathbb{N}$. On définit :

$$F_{p^\sigma} \coloneqq \{v \in \mathbb{Z}^n \mid vF = 0 \mod p^\sigma\}$$

$\rightarrow$ réseau euclidien, fondamentale en cryptographie

Analogue polynomial : classe **P**, réduction exacte, approche diviser-pour-régner

Réseau défini par une relation

Soit $F \in M_n(\mathbb{Z})$, un degré de précision $\sigma \in \mathbb{N}$, et $p \in \mathbb{N}$. On définit :

$$F_{p^\sigma} := \{v \in \mathbb{Z}^n \mid vF = 0 \mod p^\sigma\}$$

$\rightarrow$ réseau euclidien, fondamentale en cryptographie

Analogue polynomial : classe **P**, réduction exacte, approche diviser-pour-régner

$\rightarrow$ LLL utilise $\widetilde{\mathcal{O}}\left(n^5\sigma^2 \log^2 p\right)$ opérations binaires.

Réseau défini par une relation

Soit $F \in M_n(\mathbb{Z})$, un degré de précision $\sigma \in \mathbb{N}$, et $p \in \mathbb{N}$. On définit :

$$F_{p^\sigma} \coloneqq \{v \in \mathbb{Z}^n \mid vF = 0 \mod p^\sigma\}$$

$\rightarrow$ réseau euclidien, fondamentale en cryptographie

Analogue polynomial : classe **P**, réduction exacte, approche diviser-pour-régner

$\rightarrow$ LLL utilise $\widetilde{\mathcal{O}}\left(n^5\sigma^2 \log^2 p\right)$ opérations binaires.

Problème : comment calculer une base LLL-réduite de ce réseau ?

Extraire une base de F_{p^σ}

Extraire une base de F_{p^σ}

$\rightarrow$ on s'inspire du monde polynomial.

Extraire une base de F_{p^σ}

$\rightarrow$ on s'inspire du monde polynomial.
Soit $F \in M_n(\mathbb{Z})$ de rang r. On peut écrire

Extraire une base de F_{p^σ}

$\rightarrow$ on s'inspire du monde polynomial.
Soit $F \in M_n(\mathbb{Z})$ de rang r. On peut écrire

$$\begin{pmatrix} L_r & 0 \\ G & I_{m-r} \end{pmatrix} PF = \begin{pmatrix} E' \\ 0 \end{pmatrix} \mod p$$

L_r : triangulaire inférieure, P : permutation, E' : échelonnée en ligne.
$\rightarrow$ généralisation de la décomposition PLU

Extraire une base de F_{p^σ}

$\rightarrow$ on s'inspire du monde polynomial.

Soit $F \in M_n(\mathbb{Z})$ de rang r. On peut écrire

$$\begin{pmatrix} L_r & 0 \\ G & I_{m-r} \end{pmatrix} PF = \begin{pmatrix} E' \\ 0 \end{pmatrix} \mod p$$

L_r : triangulaire inférieure, P : permutation, E' : échelonnée en ligne.

$\rightarrow$ généralisation de la décomposition PLU

$$\begin{pmatrix} L_r & 0 \\ G & I_{m-r} \end{pmatrix} PF = \begin{pmatrix} E' \\ 0 \end{pmatrix} \mod p$$

Extraire une base de F_{p^σ}

$\rightarrow$ on s'inspire du monde polynomial.
Soit $F \in M_n(\mathbb{Z})$ de rang r. On peut écrire

$$\begin{pmatrix} L_r & 0 \\ G & I_{m-r} \end{pmatrix} PF = \begin{pmatrix} E' \\ 0 \end{pmatrix} \mod p$$

L_r : triangulaire inférieure, P : permutation, E' : échelonnée en ligne.
$\rightarrow$ généralisation de la décomposition PLU

$$\begin{pmatrix} p \cdot L_r & 0 \\ G & I_{m-r} \end{pmatrix} PF = \begin{pmatrix} p \cdot E' \\ 0 \end{pmatrix} \mod p$$

Extraire une base de F_{p^σ}

$\rightarrow$ on s'inspire du monde polynomial.

Soit $F \in M_n(\mathbb{Z})$ de rang r. On peut écrire

$$\begin{pmatrix} L_r & 0 \\ G & I_{m-r} \end{pmatrix} PF = \begin{pmatrix} E' \\ 0 \end{pmatrix} \mod p$$

L_r : triangulaire inférieure, P : permutation, E' : échelonnée en ligne.

$\rightarrow$ généralisation de la décomposition PLU

$$\begin{pmatrix} p \cdot L_r & 0 \\ G & I_{m-r} \end{pmatrix} PF = \begin{pmatrix} 0 \\ 0 \end{pmatrix} \mod p$$

Extraire une base de F_{p^σ}

$\rightarrow$ on s'inspire du monde polynomial.
Soit $F \in M_n(\mathbb{Z})$ de rang r. On peut écrire

$$\begin{pmatrix} L_r & 0 \\ G & I_{m-r} \end{pmatrix} PF = \begin{pmatrix} E' \\ 0 \end{pmatrix} \mod p$$

L_r : triangulaire inférieure, P : permutation, E' : échelonnée en ligne.
$\rightarrow$ généralisation de la décomposition PLU

$$\begin{pmatrix} p \cdot I_r & 0 \\ G & I_{m-r} \end{pmatrix} PF = \begin{pmatrix} 0 \\ 0 \end{pmatrix} \mod p$$

Extraire une base de F_{p^σ}

$\rightarrow$ on s'inspire du monde polynomial.

Soit $F \in M_n(\mathbb{Z})$ de rang r. On peut écrire

$$\begin{pmatrix} L_r & 0 \\ G & I_{m-r} \end{pmatrix} PF = \begin{pmatrix} E' \\ 0 \end{pmatrix} \mod p$$

L_r : triangulaire inférieure, P : permutation, E' : échelonnée en ligne.

$\rightarrow$ généralisation de la décomposition PLU

$$\begin{pmatrix} p \cdot I_r & 0 \\ G & I_{m-r} \end{pmatrix} PF = \begin{pmatrix} 0 \\ 0 \end{pmatrix} \mod p$$

Piste: Choix de P.

$\rightarrow$ qui minimise D ?

$\rightarrow$ qui contrôle de la taille des entiers

Calcul de la décomposition : démarche scientifique

$\rightarrow$ Conception, implémentation, correction (`SageMath`)

$\rightarrow$ Valide sur $\mathbb{Z}_p$, p premier.

$\rightarrow$ Complexité binaire de manipulation d'entiers dans $\mathbb{Z}_p$: $\tilde{\mathcal{O}}(\log p)$

$\rightarrow$ Complexité binaire du calcul du noyau dans $M_n(\mathbb{Z}_p)$: $\tilde{\mathcal{O}}(n^3 \log p)$

Une étape de diviser-pour-régner

Une étape de diviser-pour-régner

Base réduite de $F \ mod \ x^{\sigma_1+\sigma_2}$?

$$\begin{tikzcd}
 & V_2 \cdot V_1 & \\
V_2 \arrow[ur] & & V_1 \arrow[ul]
\end{tikzcd}$$

Base réduite de $F \ mod \ x^{\sigma_2}$

Base réduite de $F \ mod \ x^{\sigma_1}$

Une étape de diviser-pour-régner

Base réduite de $F\ mod\ x^{\sigma_1+\sigma_2}$?

$$\begin{tikzcd}
 & V_2 \cdot V_1 & \\
V_2 \arrow[ur] & & V_1 \arrow[ul]
\end{tikzcd}$$

Base réduite décalée de $F\ mod\ x^{\sigma_2}$

Base réduite de $F\ mod\ x^{\sigma_1}$

Une étape de diviser-pour-régner

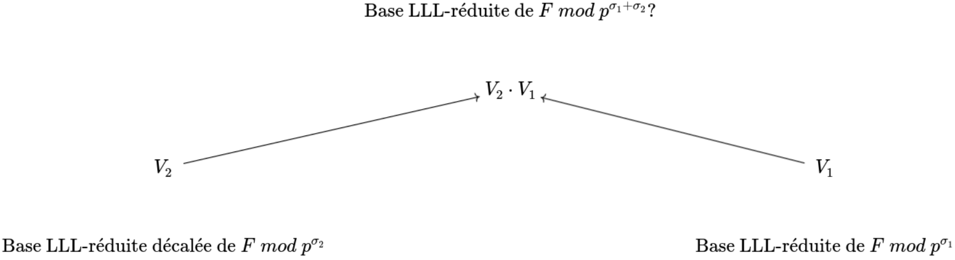
Base LLL-réduite de $F\ mod\ p^{\sigma_1+\sigma_2}$?

$$
\begin{tikzcd}
V_2 \arrow[r] & V_2 \cdot V_1 & V_1 \arrow[l]
\end{tikzcd}
$$

Base LLL-réduite décalée de $F\ mod\ p^{\sigma_2}$

Base LLL-réduite de $F\ mod\ p^{\sigma_1}$

Une étape de diviser-pour-régner



Pour quel décalage ?

Piste 1 : ShiftLLL(B, S^*) qui calcule B tel que BS^* est LLL-réduite

- **Théorème** : ShiftLLL est correct
- **Problème** : complexité pas plus intéressante

Piste 2 (prometteuse) : appliquer LLL sur V_2 avec une norme perturbée.

Conclusion et perspectives

Conclusion et perspectives

Limite du stage de recherche

$\rightarrow$ Pistes non encore testées expérimentalement ou théoriquement.

Conclusion et perspectives

Limite du stage de recherche

→ Pistes non encore testées expérimentalement ou théoriquement.

Pistes à explorer

→ Notion de décalage à mieux comprendre et exploiter.

→ Estimer plus précisément D.

→ Gagner de la complexité sur la taille des entiers ?

→ Réduire le nombre d'étapes de LLL final ?

Conclusion et perspectives

Limite du stage de recherche

→ Pistes non encore testées expérimentalement ou théoriquement.

Pistes à explorer

→ Notion de décalage à mieux comprendre et exploiter.

→ Estimer plus précisément D.

→ Gagner de la complexité sur la taille des entiers ?

→ Réduire le nombre d'étapes de LLL final ?

Questions ouvertes

Conjecture : $V_2 V_1$ est *size-réduit*.

$V_2 V_1$ est 4-quasi croissante ?

Décalage de norme prometteur.

Merci pour votre attention!

Questions?