Réduction de réseaux en petite dimension

Damien STEHLÉ

Soutenance de DEA, 24 Juin 2002

Sommaire

- La réduction des réseaux
- L'algorithme de Dirichlet
- Complexité de l'algorithme de Dirichlet

Les réseaux Euclidiens

- Déf 1 : Réseau := Sous-groupe discret de $\mathbb{R}^n$.
- Exemple : $\mathbb{Z}^n$.
- Déf 2 : Réseau == $\{\sum_{i=1}^{d} x_i \mathbf{b}_i\}$.
- Base : $[\mathbf{b}_1, ..., \mathbf{b}_d]$, dimension : d.

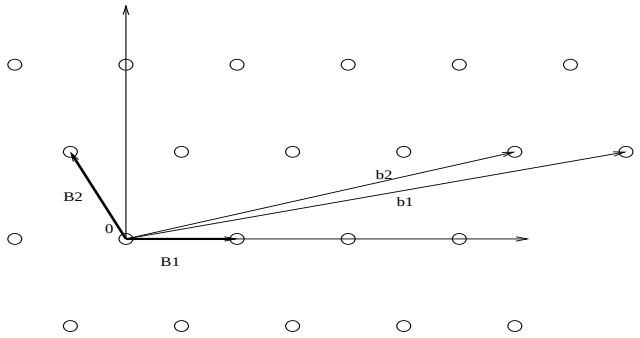

FIG. 1 – Bonne et mauvaise base

Minima d'un réseau

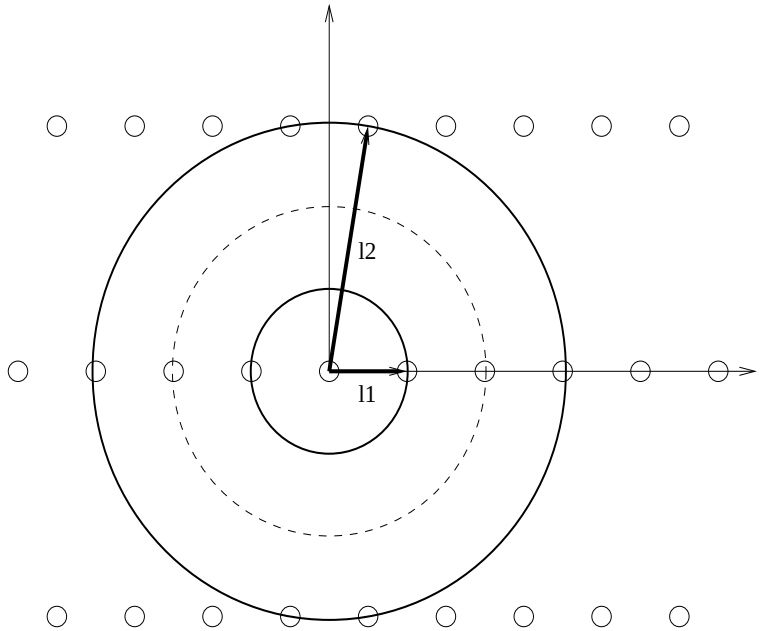

FIG. 2 – Minima successifs

Les problèmes algorithmiques

- SVP et CVP
- Bases “optimales” : Réductions de Minkowski, Hermite, etc.

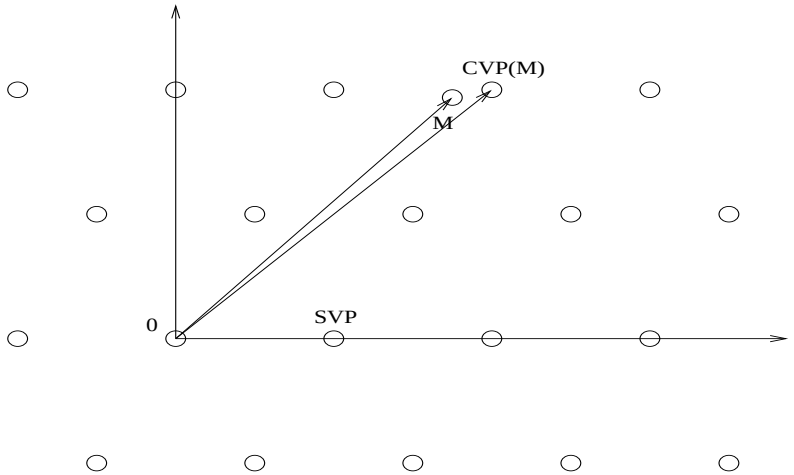

FIG. 3 – SVP et CVP

Réduction des réseaux et applications

- LLL (1982), Schnorr-BHKZ (1987), segment-LLL (2001).
- Programmation entière (1981),
  approximation diophantienne (1982),
  factorisation des polynômes de $\mathbb{Q}[X]$ (1982),
  petites racines de polynômes de $\mathbb{Z}_n[X]$ (1997).
- Attaques contre RSA à petits exposants (1985),
  attaques contre le sac-à-dos (1982).
- Cryptosystèmes Ajtai-Dwork (1997), GGH (1997), NTRU (1996).

La réduction au sens de Minkowski

- $[\mathbf{b}_1, ..., \mathbf{b}_d]$ Minkowski-réduite ssi, chaque $\mathbf{b}_i$ est de norme minimale parmi ceux tels que $[\mathbf{b}_1, ..., \mathbf{b}_i]$ puisse être complétée en une base.
- Base réduite au sens de Minkowski $\Longrightarrow$ 4 premiers minima.

$$\begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 1 & 0 \\ 0 & 0 & -1 & 1 \\ 0 & 0 & 0 & -1 \end{bmatrix}$$

Les réseaux de petite dimension

- Dimension 2 : Gauss (19^e s.).
- Dimension 3 : Vallée (1986), Semaev (2001).
- Intérêt : meilleure compréhension, réduction par bloc, etc.

L'algorithme de Gauss

Entrée : $\mathbf{u}, \mathbf{v}$ linéairement indépendants avec $||\mathbf{u}|| \leq ||\mathbf{v}||$.
Sortie : Une base qui atteint les deux premiers minima du réseau engendré par $[\mathbf{u}, \mathbf{v}]$.

1. $q := \lfloor \frac{\langle \mathbf{u}, \mathbf{v} \rangle}{||\mathbf{u}||^2} \rceil$
2. $\mathbf{w} := \mathbf{v} - q\mathbf{u}$
3. Si $||\mathbf{w}|| \geq ||\mathbf{u}||$, renvoyer $\mathbf{u}, \mathbf{w}$.
4. Sinon, renvoyer Gauss$(\mathbf{w}, \mathbf{u})$.

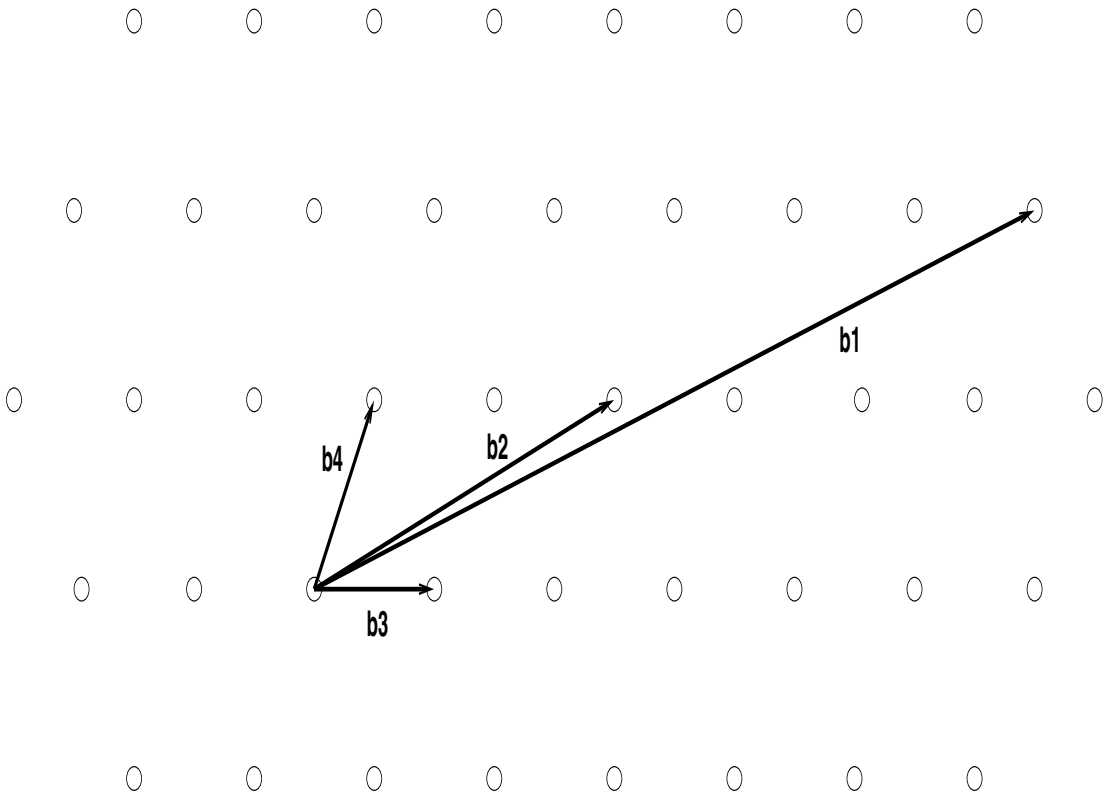

FIG. 4 – Algorithme de Gauss

L'algorithme de Dirichlet

Entrée : Une base $[\mathbf{b}_1, ..., \mathbf{b}_d]$, avec $||\mathbf{b}_1|| \leq ||\mathbf{b}_2|| \leq ... \leq ||\mathbf{b}_d||$

1. $[\mathbf{b}_1, ..., \mathbf{b}_{d-1}] := DIRICHLET_{d-1}[\mathbf{b}_1, ..., \mathbf{b}_{d-1}]$.
2. $\mathbf{a} := \mathbf{b}_d + x_1\mathbf{b}_1 + ... + x_{d-1}\mathbf{b}_{d-1}$ de norme minimale.
3. Si $||\mathbf{a}|| \geq ||\mathbf{b}_{d-1}||$, renvoyer $[\mathbf{b}_1, ..., \mathbf{b}_{d-1}, \mathbf{a}]$.
4. Sinon, $\mathbf{b}_d := \mathbf{a}$, réordonner les vecteurs et retourner en 1.

La réduction au sens de Dirichlet

- Déf : $||\mathbf{b}_1|| \leq ... \leq ||\mathbf{b}_d||$ et $(\forall i \in [1,d])(\forall x_1,...,x_{i-1} \in \mathbb{Z})$
  $(||x_1\mathbf{b}_1 + ... + x_{i-1}\mathbf{b}_{i-1} + \mathbf{b}_i|| \geq ||\mathbf{b}_i||)$
- Équivalence avec réduction de Minkowski ?

$d \leq 4$: OUI $\qquad$ $d \geq 5$: NON.

$$\begin{bmatrix} 2 & 0 & 0 & 0 & 1 \\ 0 & 2 & 0 & 0 & 1 \\ 0 & 0 & 2 & 0 & 1 \\ 0 & 0 & 0 & 2+\epsilon & 1+\frac{\epsilon}{2} \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

Cellule de Voronoï

Déf : Ensemble des points dont le CVP est 0.

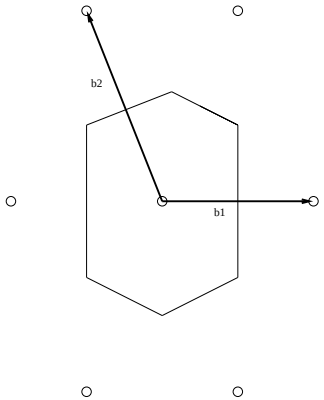

FIG. 5 – Cellule de Voronoï en dimension 2.

$\Longrightarrow$ Interprétation géométrique de l'algorithme de Dirichlet.

Complexité et nombre d'étapes

- Étape 2 : $O(\log ||\mathbf{b}_d||.[1+r])$ avec
  $r = \max\left(\left|\frac{\langle \mathbf{b}_1, \mathbf{b}_d \rangle}{||\mathbf{b}_1||^2}\right|, ..., \left|\frac{\langle \mathbf{b}_{d-1}, \mathbf{b}_d \rangle}{||\mathbf{b}_{d-1}||^2}\right|\right)$.
- Décroissance d'un facteur constant du produit des longueurs

  $\Downarrow$

  Linéarité du nombre d'itérations de boucle

  $\Downarrow$

  Quadraticité de l'algorithme.

Quadraticité de l'algorithme de Gauss

- Soit $[\mathbf{b}_1, \mathbf{b}_2]$ qui apparaît au cours de l'algorithme

  Écrivons $\mathbf{a} = \mathbf{b}_2 + x_1\mathbf{b}_1$.
- $x_1 = 0$? EXCLU

  $|x_1| = 1$? EXCLU

  $|x_1| \geq 2$ et $||\mathbf{a}|| \leq ||\mathbf{b}_1|| \implies ||\mathbf{b}_2||^2 \geq 2||\mathbf{b}_1||^2 + ||\mathbf{a}||^2$.

Quadraticité de l'algorithme de Semaev

- En dimension 2, les coordonnées possibles des Voronoïs ne font intervenir que des 1 (Tamella).
- Soit $[\mathbf{b}_1, \mathbf{b}_2]$ réduite.

  Écrivons $\mathbf{a} = \mathbf{b}_3 + x_2\mathbf{b}_2 + x_1\mathbf{b}_1$.

  Supposons $\mathbf{b}_2$ créé à l'itération précédente.
- $x_2 = 0$? EXCLU : $[\mathbf{b}_1, \mathbf{b}_3]$ réduite

  $|x_2| = 1$? EXCLU : par choix de $\mathbf{b}_2$

  $|x_2| \geq 2 \implies x_2\mathbf{b}_2 + x_1\mathbf{b}_1$ n'est pas un Voronoï !

Quadraticité en dimension 4

- En dimension 3, les coordonnées possibles des Voronoïs ne font intervenir que des 1 (Tamella).

  Le raisonnement reste valide.
- En dimension 5, ce n'est plus vrai.

  D'autre part, la base renvoyée n'est pas optimale.

Conclusion

- En dimension 3, une preuve plus naturelle car plus géométrique.
- Gain d'une dimension ($3 \to 4$).
- "Impossibilité" en dimension 5.

Questions ouvertes

- Borne explicite de la complexité en dimension 4.
- Réduction en dimension 5 et supérieure.
- Cas des autres normes.