Les bases locales dans LLL

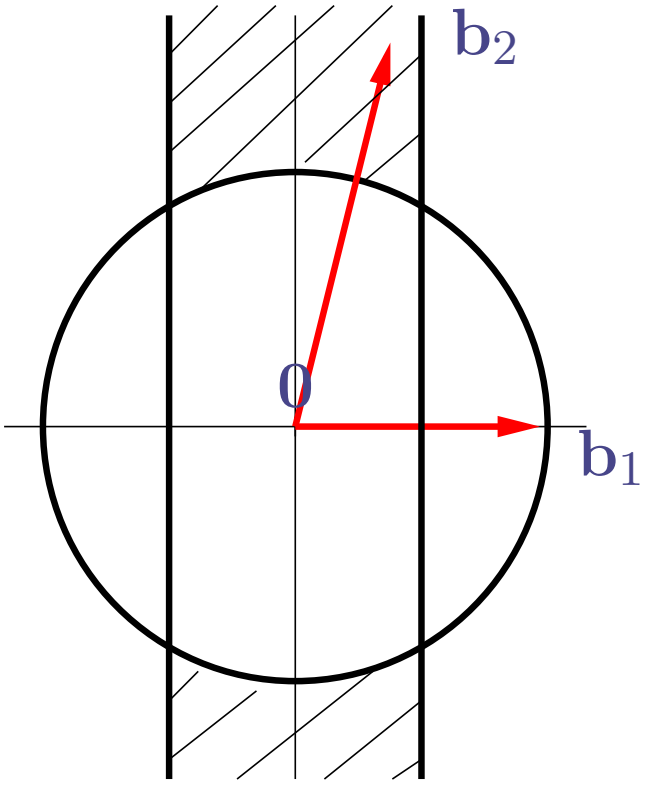
Damien STEHLÉ

Réduction LLL

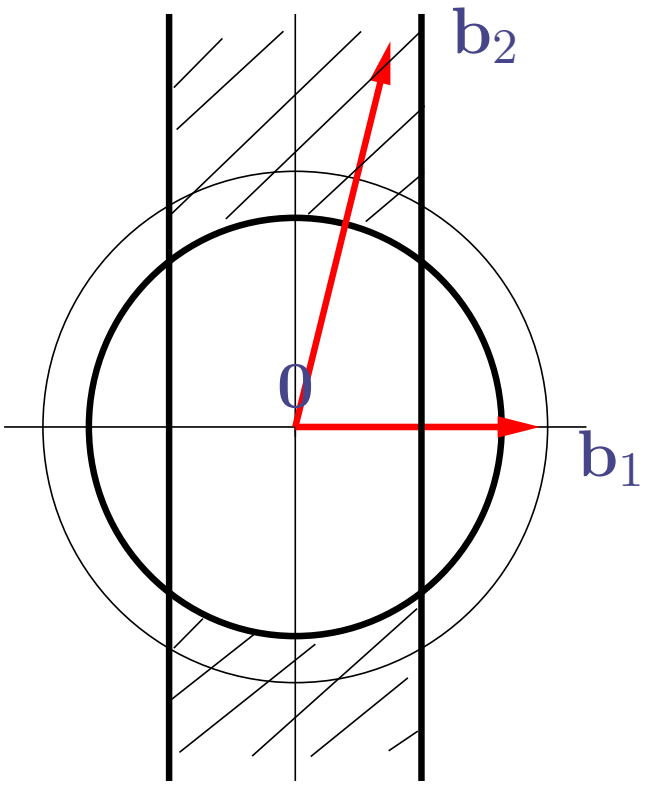
- Soit $\delta \in]1/4, 1]$.
- Une base est δ-LLL-réduite si:
  - $\forall i > j,\ |\mu_{i,j}| \leq 1/2$.
  - $\forall i,\ \delta \cdot \|\mathbf{b}_{i-1}^*\|^2 \leq \mu_{i,i-1}^2 \|\mathbf{b}_{i-1}^*\|^2 + \|\mathbf{b}_i^*\|^2$.
- On a alors :

$$(\delta - 1/4) \cdot \|\mathbf{b}_{i-1}^*\|^2 \leq \|\mathbf{b}_i^*\|^2.$$

Dans un LLL parfait : $\delta = 1$



δ-LLL avec $\delta < 1$



Autre réduction LLL

- Pour prendre en compte les erreurs de l'arithmétique flottante, on définit les bases (δ, η)-LLL-réduites par:
  - $\forall i > j,\ |\mu_{i,j}| \leq \eta$.
  - $\forall i,\ \delta \cdot \|\mathbf{b}_{i-1}^*\|^2 \leq \mu_{i,i-1}^2 \|\mathbf{b}_{i-1}^*\|^2 + \|\mathbf{b}_i^*\|^2$.
- On a alors :

$$\left(\delta - \eta^2\right) \cdot \|\mathbf{b}_{i-1}^*\|^2 \leq \|\mathbf{b}_i^*\|^2.$$

- Avec $\eta \in [1/2, 1[$ and $\delta \in]\sqrt{\eta}, 1]$.

(δ, η)-LLL avec $\delta < 1$ et $\eta > 1/2$