Approximation

Par réduction de base (Algorithme LLL)

• LLL est un algorithme polynomial qui, étant donné une base B et un facteur $0.25 < \delta < 1$, retourne une nouvelle base \tilde{B} engendrant le même espace et dite δ -LLL réduite

Si
$$\tilde{B}$$
 est δ -LLL réduite, alors $\|\tilde{b}_1\| \leq \left(\frac{2}{\sqrt{4\delta-1}}\right)^{n-1} \lambda$

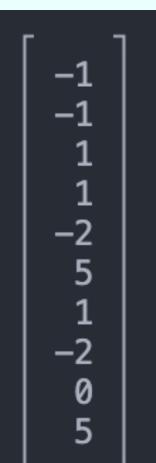
- Fonctionne par raffinements successifs de la base via l'algorithme de Gram-Schmidt
- En arrondissant les coefficients de projections aux entiers les plus près, pour obtenir une nouvelle base "presque orthogonale"
- Donne une base excellente pour l'énumération si on veut une solution exacte

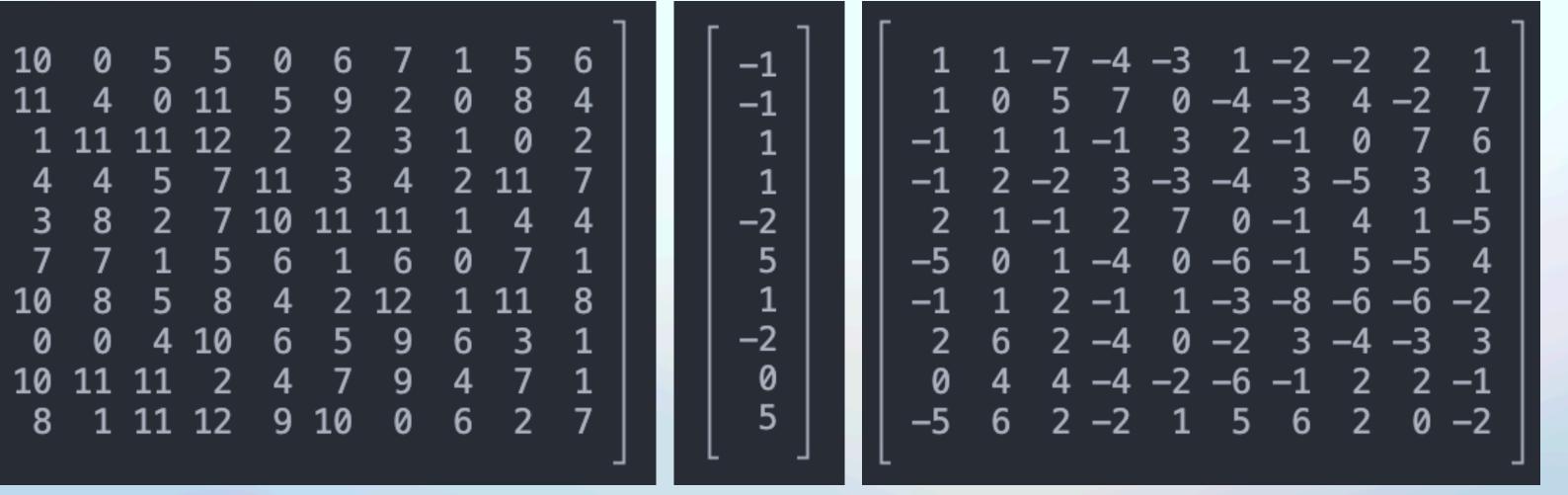
Benchmarks

Sur une matrice aléatoire de 10x10 de déterminant 11

- Coupe de moitié fonctionne comme attendu
- Coupe par mise à jour améliore agréablement
- L'approximation LLL améliore drastiquement

 \boldsymbol{B}





Exact SVP

Bench	Temps moyen
Naive	1.7942 s
Half	1.0757 s
Cut	620.28 ms
Half+Cut	371.21 ms
LLL	12.885 ms
All	7.8795 ms