

Benchmarks

Sur une matrice difficile 10x10 de déterminant 28561

- Deux premiers temps estimés à partir d’une seule itération
- Coupe par mise à jour améliore beaucoup
- L’approximation LLL améliore drastiquement

B
$$\begin{bmatrix} 13 & 0 & 0 & 0 & 4 & -2 & -5 & -5 & -5 & -2 \\ 0 & 13 & 0 & 0 & 1 & 6 & 2 & 0 & 3 & 4 \\ 0 & 0 & 13 & 0 & -3 & -5 & -2 & 6 & 5 & 0 \\ 0 & 0 & 0 & 13 & -3 & -2 & -3 & 6 & -1 & -4 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$




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

\tilde{B}
$$\begin{bmatrix} 0 & 0 & 0 & -1 & 1 & 0 & 3 & 1 & 0 & 1 \\ -1 & 0 & 2 & 0 & -1 & 1 & 0 & 1 & 1 & 1 \\ -1 & 1 & 1 & -2 & -1 & 0 & -1 & -2 & -2 & 0 \\ 0 & 1 & 1 & 0 & 1 & 2 & -1 & -2 & -2 & -1 \\ 0 & -1 & 2 & -1 & -1 & 1 & 0 & 1 & -1 & -2 \\ -1 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & -2 \\ -1 & -3 & 0 & 0 & 2 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 & 1 & 2 & -2 & 0 & 0 \\ 1 & 0 & 0 & -1 & 0 & -1 & 0 & 0 & 1 & 2 \\ 1 & 0 & 0 & 1 & -1 & -2 & 0 & 0 & 0 & -1 \end{bmatrix}$$

Exact SVP

Bench	Temps moyen
Naive	~ 16 m
Half	~ 8 m
Cut	3.1994 s
Half+Cut	1.8768 s
LLL	35.651 ms
All	21.415 ms

Code & Resources

- Mon projet (https://github.com/filedesless/classes/tree/main/INF889B/svp
 - SVP exact par énumération + coupures
 - Orthogonalization de base Gram-Schmidt & réduction de base LLL
- nalgebra (https://nalgebra.org/
 - Librairie d'algèbre linéaire
- SAGEMATH (https://www.sagemath.org/
 - Framework de math
 - Prototype, visualisation, génération de donnée de test et benchmark
- fpIII (c++): <https://github.com/fpIII/fpIII>
 - Algorithmes sur les réseaux (dont LLL) utilisé par sage