

Approximation

Par réduction de base (Algorithme LLL)

- LLL est un algorithme polynomial qui, étant donné une base \mathbf{B} et un facteur $0.25 < \delta < 1$, retourne une nouvelle base $\tilde{\mathbf{B}}$ engendrant le même espace et dite δ -LLL réduite
- Si $\tilde{\mathbf{B}}$ est δ -LLL réduite, alors $\|\tilde{\mathbf{b}}_1\| \leq \left(\frac{2}{\sqrt{4\delta - 1}} \right)^{n-1} \lambda$
- 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

B λ \tilde{B}

10	0	5	5	0	6	7	1	5	6
11	4	0	11	5	9	2	0	8	4
1	11	11	12	2	2	3	1	0	2
4	4	5	7	11	3	4	2	11	7
3	8	2	7	10	11	11	1	4	4
7	7	1	5	6	1	6	0	7	1
10	8	5	8	4	2	12	1	11	8
0	0	4	10	6	5	9	6	3	1
10	11	11	2	4	7	9	4	7	1
8	1	11	12	9	10	0	6	2	7

-1
-1
1
1
-2
5
1
-2
0
5

1	1	-7	-4	-3	1	-2	-2	2	1
1	0	5	7	0	-4	-3	4	-2	7
-1	1	1	-1	3	2	-1	0	7	6
-1	2	-2	3	-3	-4	3	-5	3	1
2	1	-1	2	7	0	-1	4	1	-5
-5	0	1	-4	0	-6	-1	5	-5	4
-1	1	2	-1	1	-3	-8	-6	-6	-2
2	6	2	-4	0	-2	3	-4	-3	3
0	4	4	-4	-2	-6	-1	2	2	-1
-5	6	2	-2	1	5	6	2	0	-2

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