Réseaux Euclidiens

Recherche du vecteur le plus court: énumération

- Soit $D = B^{-T} = d_1, \ldots, d_n \in \mathbb{R}^n$ la base du réseaux dual de $L(B)$

D est telle que $b_i d_j = \delta_{i,j}$ (1 si $i = j$ et 0 sinon)

- Soit $w = \min_{b_i \in B} \|b_i\|$ la norme du plus petit vecteur de la base

- On peut borner les coefficients du plus court vecteur $v = \sum_{i=1}^{n} x_i b_i$ par

$$|x_i| \leq \|d_i\| w$$

Réseaux Euclidiens

Algorithme de Lenstra–Lenstra–Lovász

- Soit $B = b_1, \ldots, b_n \in \mathbb{R}^n$ la base d'un réseau $L(B)$ et $0.25 < \delta < 1$
- [Lenstra, 1982] $B*$ une base δ-LLL réduite de $L(B)$ est telle que

$$\|b_1^*\| \leq \frac{2}{\sqrt{4\delta - 1}}^{n-1} \lambda$$

- Résout SVP_γ pour γ exponentiel en temps polynomial