

Problème du plus court vecteur

Optimisation combinatoire sur les réseaux

Plan de l'exposé

- **Définition**

- Réseau d'espace vectoriel Euclidien
- Problème du plus court vecteur
- Algorithme d'énumération naïf

- **Optimisation**

- Coupure de l'espace en deux
- Coupure par mise à jour des bornes (B&B)
- Traitement par lots
- Approximation par réduction de base (**LLL**)

- **Benchmarks**

- Réseau arbitraire
- Petite instance difficile
- Grande instance difficile

- **Ressources**

- Code
- Références