Problème du plus court vecteur dans les réseaux
Projet de session du cours INF889B

Félix Larose-Gervais

Décembre 2023

Contents

1 Introduction

Cet article porte sur le problème du plus cours vecteur dans les réseaux (souvent nommé SVP, de l'anglais Shortest Vector Problem), sujet de mon projet de session lors du cours INF889B (Algorithmes d'optimisation combinatoire). On y explore la manière d'énumérer l'espace de solutions, puis comment accélérer la recherche via diverses techniques d'optimisation.

1.1 Motivation

Le sujet est d'intérêt puisque sa difficulté supposée forme la base de plusieurs crypto-systèmes émergents. En effet, la sécurité de plusieurs crypto-systèmes modernes tels que RSA et Diffie-Hellman reposent sur l'hypothèse que la factorisation entière et le logarithme discret sont des problèmes difficiles. Cependant, l'algorithme quantique de Shor vient mettre en péril cette supposition. Or, il est cru que les problèmes sur les réseaux euclidiens comme le SVP sont difficiles même pour un ordinateur quantique. Les systèmes basés sur ce problème sont aussi les seuls connus à ce jours pour être totalement homomorphes, une propriété désirable pour permettre la délégation de calcul respectant la vie privée.

1.2 Définitions

1.2.1 Réseaux euclidiens

Un réseau d'un espace vectoriel euclidien est un sous-groupe discret de l'espace.

Soient $n \in \mathbb{N}$ et $B \in GL_n(\mathbb{R})$ appelée une base, on définit le réseau $\mathcal{L}$ ainsi:

$$\mathcal{L}(B) = \{Bx \mid x \in \mathbb{Z}^n\} \subset \mathbb{R}^n$$

C'est-à-dire l'ensemble des points atteignables par une combinaison linéaire entière des colonnes de la base. On note que le réseau dépend de la base, en effet, plusieurs bases peuvent engendrer le même réseau.

1.2.2 Problème du vecteur le plus court

Étant donné un réseau $\mathcal{L}$, notons la longueur de son plus petit vecteur non nul:

$$\lambda(\mathcal{L}) = \min_{v \in \mathcal{L} \setminus \{0\}} \|v\|$$

où $\|v\|$ dénote ici la norme euclidienne, avec $v = (v_1, \ldots, v_n)$:

$$\|v\| = \sqrt{v_1^2 + \cdots + v_n^2}$$

Le problème consiste à trouver un tel v non nul minimisant la norme étant donné un réseau de base B. Ce problème est connu pour être NP-Difficile.

1.3 Méthode naïve

A priori, il suffit d'énumérer les points du réseau, et choisir celui minimisant la norme. Cependant, il en existe un nombre infini. Pour pouvoir compléter l'énumération, il faut borner les coefficients de la combinaison linéaire entière, tout en garantissant qu'un vecteur de longueur λ se trouve dans l'espace de recherche.

Une telle borne est présentée par U. Dieter dans son article 'How to calculate shortest vectors in a lattice' [1].

Il suffit de calculer la base du réseau dual de $\mathcal{L}$ c'est-à-dire $D = B^{-T}$, puis, étant donné une borne supérieure w sur λ (prenons la norme du plus petit vecteur de la base B), on peut borner nos coefficients entiers comme suit:

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

avec $x_i \in \mathbb{Z}$ les coefficients entiers à énumérer et $d_i \in \mathbb{R}^n$ les colonnes de D. Pour chaque dimension, on a donc $(2\|d_i\|w + 1)$ entiers à énumérer, c'est-à-dire un nombre $O(2^n)$ de points à énumérer au total.

2 Optimisation combinatoire

2.1 Symmétrie

2.2 Séparation et évaluation

2.3 Traitement par lots

2.4 Approximation

3 Algorithme LLL

3.1 Orthogonalisation de Gram-Schmidt

3.2 Procédure principale

3.3 Complexité

4 Benchmark

5 Conclusion

References

[1] U. Dieter. How to calculate shortest vectors in a lattice. *Mathematics of Computation*, 29(131):827–833, 1975.