IMPLANTATION DE TECHNIQUES D'ÉLAGAGE DANS LES ALGORITHMES D'ÉNUMÉRATION

G. HANROT

1. Lieu du stage

Le stage s'effectuera au sein de l'équipe Arénaire/Aric[1] du LIP (Laboratoire d'Informatique du Parallélisme), au sein de l'ENS Lyon.

2. Encadrement

L'encadrant principal sera Guillaume Hanrot[2], avec pour co-encadrants Xavier Pujol et Damien Stehlé.

3. Rémunération

Une rémunération est possible pour les stagiaires non-normaliens.

4. Description du sujet

Un réseau de $\mathbb{R}^n$ est une grille, ie. un ensemble de points régulièrement espacés dans l'espace de dimension n. De façon équivalente, on peut voir un réseau comme l'ensemble des combinaisons linéaires entières d'un ensemble fini de vecteurs linéairement indépendants de $\mathbb{R}^n$, appelé base du réseau.

Les réseaux sont une structure très générale qui intervient dans de nombreux champs des mathématiques et de l'informatique. Citons la cryptologie, la programmation linéaire entière, l'arithmétique, le calcul formel, etc.

La principale tâche algorithmique pour ces applciations est généralement de trouver un vecteur non nul le plus court du réseau, ou un vecteur le plus proche d'un point de $\mathbb{R}^n$ donné. Ces problèmes peuvent être prouvés (presque) NP-difficiles, mais des algorithmes efficaces permettent de les approcher (réduction des réseaux) ou de les résoudre exactement (énumération, cribles).

Le stage réalisera une étude et une implémentation de certains des algorithmes les plus récents du domaine. Le point de départ sera l'étude théorique et expérimentale, puis l'implémentation de la stratégie d'élaguage extrême ("extreme pruning") dans la bibliothèque FPLLL.

5. Références

N. Gama, P. Nguyen, O. Regev, Lattice Enumeration using Extreme Pruning, Proceedings of EUROCRYPT '10 –, H. Gilbert (Ed.), Lecture Notes in Computer Science, Springer-Verlag.

FPLLL library, `http://perso.ens-lyon.fr/xavier.pujol/fplll/`

[1] `http://www.ens-lyon.fr/LIP/Arenaire/`

[2] `http://perso.ens-lyon.fr/guillaume.hanrot`