# Sujet de stage de L3

## Résolution efficace de systèmes d'équations linéaires à coefficients entiers ou polynomiaux: étude et implantation

## INFORMATIONS

Lieu : Université Montpellier, laboratoire LIRMM

Équipe d'accueil : ECO - www.lirmm.fr/eco

Encadrants : Pascal Giorgi, Romain Lebreton (giorgi@lirmm.fr,lebreton@lirmm.fr)

## SUJET

Ce sujet se place dans le domaine de l'algèbre effective où l'on s'intéresse à faire des calculs d'algèbre à l'aide d'un ordinateur de manière efficace. Ce type de calcul exact est aujourd'hui fondamental pour de nombreuses applications (e.g. théorie des graphes, cryptologie, théorie des nombres).

L'une des premières questions de l'algèbre effective a été de savoir si l'on peut multiplier deux nombres entiers plus rapidement qu'avec l'algorithme de l'école primaire. Dans les années 60, Kolmogorov était convaincu que cela était impossible, et s'est amusé à poser le problème à ses étudiants. À son grand étonnement, un étudiant nommé Karatsuba trouva un contre-exemple et une méthode améliorant asymptotiquement la méthode de l'école primaire [1].

Dans le même ordre d'idée, un des problèmes majeur du domaine est l'étude de la complexité du produit de matrices. Ce n'est qu'en 1969 que Strassen [3] a démontré qu'on pouvait effectuer un produit de matrices plus rapidement que la méthode standard. La complexité du produit de matrices reste un problème fortement étudié aujourd'hui, notamment car de nombreux problèmes d'algèbre linéaire se réduisent au produit matriciel.

Ce sujet de stage est au croisement de ces deux problématiques : nos objets d'étude sont les matrices à coefficients entiers (ou polynomiaux). Dans ce contexte, ce n'est qu'en 2002 qu'une technique, appelée "High Order Lifting", a permis de réaliser des améliorations de complexité pour de nombreux problèmes en algèbre linéaire exacte en les ramenant à du produit de matrices entières [2]. Malgré l'avancée phénoménale apportée par cette méthode, il n'existe toujours pas d'implantation efficace de cette dernière.

Le but de ce stage est de proposer une première implantation de cette technique permettant de mettre en avant les gains de complexité asymptotique et les différents points bloquants. La démarche du travail demandé sera d'étudier dans un premier temps les travaux fondateurs du "High Order Lifting" [2] et de l'exposer à l'équipe d'accueil. Dans un deuxième temps, l'étudiant implantera l'algorithme dans un logiciel haut niveau (fournissant de nombreuses briques de base) comme SageMath.

Au delà du stage, ce travail est lié à des questions ouvertes de recherche, et pourra se poursuivre par exemple sur la nécessité de "High Order Lifting" dans les calculs efficaces de forme normale de matrices ou dans la réduction de réseaux Euclidien particuliers.

## Références

[1] A. Karatsuba and Y. Ofman. Multiplication of multidigit numbers on automata. *Doklady Akademii Nauk SSSR*, 145(2) :293–294, 1962.

[2] A. Storjohann. High-Order Lifting. In *International Symposium on Symbolic and Algebraic Computation, Lille, France*, pages 246–254. ACM Press, July 2002.

[3] V. Strassen. Gaussian elimination is not optimal. *Numerische Mathematik*, 13 :354–356, 1969.