Sujet de stage de Master 2

Multiplication de matrices à coefficients polynomiaux de degrès déséquilibrés

Informations

Lieu: Université Montpellier 2, laboratoire LIRMM

Équipe d'accueil: ARITH - www.lirmm.fr/arith

Encadrant: Pascal Giorgi - pascal.giorgi@lirmm.fr

Durée: 6 mois

Contexte

La multiplication de matrices est l'une des opérations d'algèbre linéaire les plus étudiés depuis plus de 40 ans. En effet, cette opération est centrale au niveau algorithmique puisque pratiquement tous les problèmes d'algèbre linéaire se réduisent au produit de matrices. Un des résultats les plus connu pour ce problème est celui de Strassen [4] qui a proposé en 1969 le premier algorithme permettant de multiplier 2 matrices de dimension n en moins de n^3 opérations. En effet, l'algorithme de Strassen permet de multiplier $A, B \in \mathbb{K}^{n\times n}$ avec $O(n^{\log_2 7}) = O(n^{2.8})$ opérations dans $\mathbb{K}$. Depuis les travaux de Strassen, plusieurs autres algorithmes ont été proposés afin d'améliorer la complexité théorique de cette opération. Le record actuel est détenue par Coppersmith et Winograd [2] qui ont montré qu'il existait un algorithme permettant de calculer un produit matriciel en $O(n^{2.38})$ opérations dans $\mathbb{K}$. De manière générale, on considère que le problème du produit matriciel en dimension n à une complexité algébrique de $O(n^\omega)$, ou ω correspond à l'exposant de l'algorithme utilisé ($\omega = 2.38$ étant le plus petit exposant connu).

Dans le cas des matrices de $\mathbb{F}_p[x]^{n\times n}$, on peut étendre la complexité du problème pour prendre en compte les coût liés à l'arithmétique sous-jacente, ici les calculs dans $\mathbb{F}_p[x]$. Soit $p, q \in \mathbb{F}_p[x]$ deux polynômes de degrés inférieur à d, on sait que l'on peut calculer $p+q$ en $O(d)$ opérations dans $\mathbb{F}_p$ et $p\times q$ en $O(d \log d)$ opérations dans $\mathbb{F}_p$ [3]. Il est assez facile de montrer que si l'on considère les matrices $A, B \in \mathbb{F}_p[x]^{n\times n}$ telles que $\max_{i,j} \deg(A_{i,j}) \leq d$ et $\max_{i,j} \deg(B_{i,j}) \leq d$, on peut calculer le produit $A \times B$ en $O(n^\omega d \log d)$ opérations dans $\mathbb{F}_p$ [1]. Cette évaluation de complexité est alors très fine quand tous les coefficients des matrices A et B ont effectivement un degrés égal à d. Maintenant si l'on considère le cas où uniquement quelques coefficients de A et B ont un degrés égal à d et que le reste ont des degrés $\ll d$, il est facile de se convaincre que cette complexité n'est pas du tout fine, au moins dans le cas $\omega = 3$.

Objectif et Programme de travail

L'objectif de se stage est d'étudier le problème de la multiplication de matrices polynomiale lorsque les degrés des coefficients sont fortement déséquilibrés. En particulier, nous souhaitons dégager une analyse de complexité non plus en fonction de la dimension des matrices et du degrés maximum des coefficients, mais plutôt en fonction de la quantité d'information contenue dans les matrices. Par exemple, dans le cas des matrices de dimension n ayant des coefficients de degrés identiques d, la quantité d'information dans les matrices est de $n^2 d$ éléments de $\mathbb{F}_p$ et la complexité de la multiplication est de $O(n^\omega d \log d)$ opérations dans $\mathbb{F}_p$. Est-il possible d'obtenir la même complexité pour des matrices ayant la même quantité d'information mais avec des degrès de coefficients déséquilibrés.

Le travail pourra s'organiser selon plusieurs tâches:

- étude bibliographique,
- étude du cas du produit de matrice classique ($\omega = 3$),
- étude du case du produit de matrice rapide de Strassen ($\omega = 2.8$),
- proposition d'algorithmes de multiplication de matrices améliorant le cas des degrés déséquilibrés,
- implantation et validation logicielle des concepts.

References

[1] D. G. Cantor and E. Kaltofen. On fast multiplication of polynomials over arbitrary algebras. *Acta Informatica*, 28(7):693–701, 1991.

[2] D. Coppersmith and S. Winograd. Matrix multiplication via arithmetic progressions. *Journal of Symbolic Computation*, 9(3):251–280, 1990.

[3] J. v. Gathen and J. Gerhard. *Modern Computer Algebra*. Cambridge University Press, New York, NY, USA, 1999.

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