

Développements ϕ -adiques en parallèle

- Équipe : CFHP cfhp.univ-lille.fr. Directeur François Boulier.
- Encadrants : Pierre Fortin, pierre.fortin@univ-lille.fr et Adrien Poteaux, adrien.poteaux@univ-lille.fr.
- Laboratoire : CRIStAL, Lille (France). Directeur Olivier Colot, cristal.univ-lille.fr.

Mots clés : calcul formel, calcul haute performance, parallélisme.

1 Objectif

L'objectif de ce stage sera de travailler sur le déploiement HPC d'un algorithme de développement ϕ -adique d'un polynôme $F \in \mathbb{A}[x]$. Cet algorithme est une étape nécessaire pour le déploiement HPC d'un algorithme de résolution de singularités de courbes algébriques (possibilité de continuation en thèse).

Le problème mathématique est relativement simple : étant donné $F, \phi \in \mathbb{A}[x]$ deux polynômes, il s'agit de calculer les coefficients $a_i \in \mathbb{A}[x]$ du développement

$$F = \sum_{i=0}^n a_i \phi^i, \text{ avec } \deg(a_i) < \deg(\phi).$$

L'idée de l'algorithme est très simple : on effectue la division euclidienne de $F = q\phi^{n/2} + r$, puis on applique récursivement cette stratégie sur les polynômes q et r .

Ces appels récursifs indépendants offrent un niveau de parallélisme que nous souhaitons exploiter pour accélérer ces calculs sur des serveurs dotés de processeurs multi-cœurs. Nous visons pour cela à exploiter le parallélisme de tâches (tel qu'offert par exemple dans le standard OpenMP). Ce parallélisme de tâches est en effet bien adapté à de tels algorithmes récursifs, et il nous permettra de nous appuyer sur un équilibrage de charge dynamique entre les tâches (voir par exemple [2]) bien adapté à ces calculs. Nous pourrons aussi étudier l'existence de parallélisme au niveau des opérations élémentaires, et chercher à l'exploiter (à nouveau via le parallélisme de tâches). Enfin, au sein de chaque cœur de calcul on pourra chercher à exploiter les instructions vectorielles (AVX et AVX-512) qui peuvent offrir un gain en performance supplémentaire très important.

Ce stage est donc prioritairement consacré aux aspects HPC de l'algorithme de développement ϕ -adique d'un polynôme (en particulier, la compréhension du contexte évoqué ci-dessous n'est pas nécessaire à l'accomplissement du stage).

2 Contexte

Un tel développement ϕ -adique est une étape nécessaire des algorithmes développés dans [3], qui permettent d'étudier efficacement les singularités d'une courbe algébrique plane. L'étude de singularités (parfois décrites comme des « points infiniment proches ») de variétés algébriques et analytiques est un domaine de recherche ancien (l'étude de singularités de certaines courbes apparaît dans les problèmes étudiés pas les géomètres grecs) et actif. C'est d'ailleurs devenu une discipline à part entière depuis les années 1960, à partir des travaux d'Hironaka, Zariski etc.

Les applications sont multiples : calcul du genre d'une courbe via la formule d'Hurwitz, de bases intégrales d'un corps de fonction [4], d'une base pour l'espace de Riemann-Roch $\mathcal{L}(D)$ associé à un diviseur D (via l'algorithme de Dedekind-Weber's [1]), etc.

Compétences souhaitées : un goût pour les mathématiques (en particulier l'algèbre) et l'informatique (algorithmique et programmation ; des bases en calcul haute performance sont bienvenues mais non nécessaires).

Références

- [1] D. Duval. Diverses questions relatives au calcul formel avec des nombres algébriques, 1987. Thèse d'État.
- [2] C. Gueunet, P. Fortin, J. Jomier, and J. Tierny. Task-based augmented contour trees with fibonacci heaps. *IEEE Trans. on Parallel and Distributed Systems*, 30(8) :1889–1905, 2019.
- [3] A. Poteaux and M. Weimann. A quasi-linear irreducibility test in $\mathbb{K}[[x]][y]$, 2019.
- [4] M. van Hoeij. An Algorithm for Computing an Integral Basis in an Algebraic Function Field. *Journal of Symbolic Computation*, 18 :353–363, 1994.