Projet M1 : Spécialité SFPN

Titre du sujet. Résolution de systèmes polynomiaux bivariés : Algorithmes et implantation haute-performance

Encadrant. Mohab Safey El Din, Sorbonne Universités, UPMC Univ Paris 06, CNRS, INRIA Paris Center, LIP6, Equipe PolSys.

Nombre d'étudiants prévus : 2.

Problématique. Le systèmes polynomiaux apparaissent dans de nombreux domaines de l'informatique et des sciences de l'ingénieur. Citons pour l'informatique, entre autres exemples, la cryptographie (cryptanalyse algébrique des systèmes de chiffrement), la géométrie algorithmique (visualisation de scènes 3-D et étude des diagrammes de Voronoi) ou encore la vérification de programmes (problèmes d'atteignabilité).

Dans ces contextes applicatifs, la qualité des résultats calculés par l'algorithme de résolution est souvent essentielle. On privilégie donc l'usage de techniques de calcul algébrique (calcul formel) qui permettent de calculer une représentation *exacte* de *toutes* les solutions (globalement). La qualité du résultat obtenu a un coût et celui-ci est dans le meilleur des cas polynomial en la taille de la sortie, qui elle-même se trouve être exponentiel en le nombre de variables dans les pires cas. Ainsi, un effort particulier doit être entrepris pour obtenir les implantations les plus fines afin d'atteindre des niveaux d'efficacité les plus élevés possibles.

Dans ce contexte, une classe de problèmes intéressante est la classe des systèmes polynomiaux bivariés. Ceux-ci sont particulièrement importants car ils apparaissent dans de nombreuses applications et des algorithmes spécifiques peuvent (et doivent) être déployés afin d'obtenir des implantations performantes.

Méthodologie et outils de mise en œuvre. La technique qu'on étudiera pour la résolution des systèmes bivariés s'appuie sur le calcul de la suite des sous-résultants associée au couple de polynômes que l'on cherche à résoudre. La méthodologie que l'on mettra en œuvre relève des techniques d'évaluation interpolation qui permettent de scinder le calcul de la suite des sous-résultants en des calculs similaires à effectuer dans plusieurs corps premiers. Pour ces derniers calculs, on pourra s'appuyer sur des bibliothèques de calcul particulièrement efficaces (NTL et/ou FLINT). Aussi, se posera naturellement la question de paralléliser nos calculs afin de tirer le plus grand profit possible des architectures multi-cœurs.

Travail attendu. Le travail attendu s'articule comme suit:

- étude de deux stratégies relevant des techniques d'évaluation interpolation ;
- analyse de la complexité binaire et du grossissement des données intermédiaires selon les diverses stratégies ;
- implantation des deux stratégies en s'appuyant sur les bibliothèques FLINT et NTL ;
- production d'un code séquentiel efficace ;
- production de codes parallélisés ;
- comparaisons expérimentales.