Projet M1 : Spécialité SFPN

Titre du sujet. Sommes de carrés et certificats de positivité :
le cas ds polynômes univariés.
Encadrant. Mohab Safey El Din, Sorbonne Universités, UPMC Univ Paris 06, CNRS, INRIA Paris Center, LIP6, Equipe PolSys.
Nombre d'étudiants prévus : 2.

Problématique. Ce projet s'inscrit dans la problématique générale de certifier des résultats de calculs. Par exemple, pour certifier qu'un système d'équations

$$f_1 = \cdots = f_p = 0$$

n'a pas de solution, il suffit de renvoyer une suite $(q_1, \ldots, q_p)$ telle que

$$f_1 q_1 + \cdots + f_p q_p = 1.$$

Le calcul de certificats dans le contexte du calcul fiable et performant prend une importance de plus en plus grande du fait que de nombreux algorithmes de résolution sont aujourd'hui probabilistes et que la taille gigantesque des calculs que l'on peut dorénavant mener augmente la méfiance qu'on peut avoir quant à certains résultats fournis (notamment lorsqu'après plusieurs heures de calculs, on obtient une liste de solutions vide indiquant qu'il n'y a pas de solution au problème posé).

Dans ce contexte, un problème essentiel est de cerifier qu'un polynôme f ne change pas de signe sur les réels. Par exemple, il n'est pas rare que dans le domaine de la vérification de programmes, on soit amené à garantir qu'un système de contraintes (inégalités) n'ait pas de solution. Dans ces cas, la forme du certificat est plus délicate. On peut par exemple tenter tenter d'écrire f comme une somme de carrés de polynômes $(f_1, \ldots, f_s)$: ainsi l'identité $f = f_1^2 + \cdots + f_s^2$ garantit que f reste positif sur les réels. Une difficulté est que de tels certificats (sous forme de sommes de carrés) n'existent pas toujours, sauf dans le cas où f est un polynôme en *une* variable, qui se trouve être le cas d'étude pour ce projet qu'on tentera de rendre exacte.
Méthodologie et outils de mise en œuvre. On dispose de deux stratégies pour décomposer un polynôme univarié en sommes de carrés. La première s'appuie exclusivement sur du calcul algébrique : essentiellement, on retranche à f un polynôme g de degré 2 et tel que $f - g$ a des racines multiples facteur carré. Ainsi, en s'appuyant sur la décomposition (connue) des polynômes de degré 2, on obtient un algorithme récursif tel qu'à chaque appel récursif de l'algorithme, le degré de l'entrée baisse d'au moins 2. La seconde stratégie est de nature symbolique numérique. On peut retrancher à f une somme de carrés (par exemple la somme des puissances paires de la variable) de sorte ''a ce que ce nouveau polynôme n'a pas de racines réelles et est positif sur les réels. Puis on calcule une approximation numérique d'une décomposition en sommes de carrés
Travail attendu. Le travail attendu s'articule comme suit:

- étude de deux stratégies de résolution ;
- analyse de la complexité des deux algorithmes ;
- implantation des deux stratégies ;
- comparaisons expérimentales.