Algorithmes de resolution pour certains systèmes d'equations Diophantiens

Responsables de stage :
Marius Bozga, CNRS (Marius.Bozga@imag.fr)
Radu Iosif, CNRS (Radu.Iosif@imag.fr)

Laboratoire d'accueil : VERIMAG (UMR 5104)
Centre Equation, 2 avenue de Vignate, 38610 GIERES
`http://www-verimag.imag.fr`

Durée du stage : 3 à 4 mois

1 Motivation et contexte

La vérification des algorithmes, programmes et systèmes informatiques a été déjà posée au début du 20ème siècle comme une problématique de recherche par Alan Turing (1912-1954), un des fondateurs de l'informatique. Cette problématique a depuis connu des avancées significatives. A titre d'exemple, les travaux de J. Sifakis, A. Emerson, E. Clarke et A. Pnueli sur la vérification algorithmique des programmes et les liens entre la vérification des programmes et les logiques temporelles ont été récompensées (en 1996 et 2007) avec le Prix Turing, équivalent du Prix Nobel pour l'informatique.

La vérification de logiciels embarqués est actuellement un des thèmes de recherche majeurs dans le domaine des technologies du logiciel. La complexité grandissante et le caractère souvent critique de ces systèmes rend nécessaire le développement de méthodes et d'outils de conception et de validation permettant de garantir leur sûreté de fonctionnement. Dans ce contexte, le laboratoire VERIMAG se concentre sur le développement des outils ainsi théoriques que pratiques pour la vérification automatique de systèmes embarqués.

2 Systèmes Diophantiens

Les systèmes Diophantiens sont des systèmes d'equations polynomiales aux coefficients entiers pour lequels l'on cherche des solutions entieres. Ce type de systèmes se retrouvent naturellement comme conditions de vérification pour les programmes qui manipulent des variables entières, des vecteurs, ou meme parfois des structures recursives.

Trouver un algorithme pour resoudre un système Diophantien arbitraire a été posé comme probleme par David Hilbert en 1900 (Le 10éme Probleme de Hilbert) et montré indecidable en 1976 par Yuri Matyiasevich. Depuis ce résultat negatif, la recherche dans ce domaine consiste á trouver des sous-classes de systémes pour lesquelles il existe une solution algorithmique. La classe decidable la plus repandue est la classe de *systémes lineaires*, pour laquelle il existe egalement des algorithmes trés efficaces (Simplex, Branch and Bound, Cutting Planes, etc.).

Une autre sous-classe, strictement plus expressive que la classe lineaire, appelle la classe D[1], se décrit comme des systémes lineaire, dont les coefficients sont des *polynomes dans une variable*. La decidabilité de cette classe a été prouve dans [1]. En outre, les systémes D[1] se retrouvent facilement en pratique, dans l'analyse de boucles de programme ettiquettés par des contraintes de differences parametrés.

3 But du stage

Lors de ce stage on étudiera dans un premier temps la complexité des algorithmes pour la resolution de systémes D[1]. On essayera de donner des bornes inferieure et superieure de complexité, et eventuellement, de trouver des classes de complexité pour ce probleme.

Dans un deuxieme temps, le stagiaire implementera un algorithme de resolution, de preference utilisant une plate-forme ouverte, comme par exemple, le solveur OpenSMT [2]. Il aura également la possibilité d'intégrer l'algorithme au sein de l'outil FLATA [3], un outil pour l'analyse de programmes entiers, développe a présent a VERIMAG.

Références

[1] M. Bozga, R. Iosif, Y. Lakhnech. Flat Parametric Counter Automata. Fundamenta Informaticae, Volume 91 (2), 275 - 303, IOS Press (2009)

[2] OpenSMT homepage : `http://verify.inf.usi.ch/opensmt`

[3] FLATA homepage : `http://www-verimag.imag.fr/FLATA.html`