Sujet de thèse CIFRE

Calculs en virgule flottante sur les polyèdres convexes

(cette thèse peut être précédée d'un stage de master 2 dans la même thématique)

Encadrants (recherche) David Monniaux (david.monniaux@univ-grenoble-alpes.fr), Michaël Périn (michael.perin@univ-grenoble-alpes.fr)

Encadrant (industrie) Olivier Bouissou (olivier.bouissou@mathworks.com)

Résumé

Un polyèdre convexe dans est l'ensemble des solutions d'un système d'équations et d'inégalités linéaires à n inconnues réelles. Dans certaines application on s'intéresse à $n = 3$ mais pour celles qui nous intéressent, concernant la conception et la vérification de logiciels et de systèmes hybrides, n est quelconque et on doit donc veiller à croissance de la complexité des algorithmes en fonction de n.

La plupart des bibliothèques permettant de calculer sur les polyèdres convexes utilisent des calculs exacts en entiers ou rationnels en précision arbitraire. Ces calculs sont coûteux, même si des implantations astucieuses permettent de limiter au nécessaire le recours aux entiers multiprécision. Il est donc tentant de recourir à des calculs en virgule flottante, bien plus rapides. Toutefois, les algorithmes géométriques supposent en général des calculs exacts. **L'objet de la thèse est donc de concevoir une algorithmique robuste en virgule flottante sur les polyèdres convexes, utilisable pour la conception et la vérification de logiciels et de systèmes hybrides.** En particulier, nous nous intéresserons à :

- évaluer l'utilisation de calculs à virgule flottante pour optimiser la programmation linéaire paramétrique ;
- fournir des invariants relationnels précis pour les programmes utilisant fortement des calculs numériques ;
- mesurer l'efficacité des méthodes développées sur des problèmes de grande dimension.

Détails

L'*interprétation abstraite* (IA) est une théorie permettant de calculer automatiquement des invariants corrects et précis sur les variables d'un programme. Pour cela, un interpréteur abstrait utilise une version abstraite de l'algorithme du point fixe de Kleene et des représentations efficaces d'ensembles d'états du programme, appartenant à un *domaine abstrait*. S'agissant de propriétés numériques sur les variables du programme, ces ensembles sont le plus souvent convexes.

Il existe un grand nombre d'outils utilisant l'interprétation abstraite pour vérifier des propriétés de sûreté de programmes embarqués. Le premier outil industriel utilisant l'IA est Polyspace [1], commercialisé par MathWorks depuis 2007. Les outils Polyspace utilisent un ensemble de domaines abstraits pour garantir l'absence de nombreux bugs trouvés dans les logiciels embarqués, comme :

- bugs arithmétiques (dépassement de capacité, division par zéro…)
- bugs mémoire (*buffer overflow*, accès hors des bornes d'un tableau…)
- bugs liés au multitâche (*data-race*, mauvaise utilisation de ressources…)
- bugs liés à la sécurité (fuite d'information, utilisation de données teintées…)

Une des plus grandes difficultés pour le développement d'un analyseur précis et efficace est la génération d'invariants numériques relationnels entre les variables à virgule flottante d'un programme. Une technique classique consiste à utiliser des domaines abstraits relationnels conçus pour gérer des variables entières (par exemple le domaine des polyèdres convexes) et à adapter les opérateurs pour les variables à virgule flottante. Cela conduit généralement soit à des pertes de précision importantes pour modéliser correctement les arrondis, soit à des pertes de performance, dues à la manipulation de très grands nombres rationnels.

Des travaux récents [1] ont montré la possibilité de concevoir des algorithmes efficaces pour les polyèdres convexes sans utiliser la représentation en générateurs. Ces travaux reposent uniquement sur une représentation par contraintes et ouvrent la voie à l'utilisation poussée d'algorithmes en virgule flottante pour optimiser les calculs.

Le but de cette proposition de thèse est de développer de nouveaux algorithmes, reposant uniquement sur des calculs en virgule flottante, pour accélérer les domaines polyédriques. En particulier, il conviendra d'étudier des extensions de la *programmation linéaire paramétrique* pour garantir la correction des résultats dans un cadre où les calculs sont toujours approximatifs.

Les nombreuses applications de ces techniques (génération d'invariants relationnels pour des programmes numériques, amélioration de solveur SMT, synthèse de contrôleurs, …) permettront de mesurer leur intérêt industriel.

Détails pratiques

- Durée : 3 ans
- Localisation : Meudon (MathWorks) et Grenoble (Verimag)
- Salaire brut : 23 484€ annuel

Références

[1] Alexis Fouilhé, David Monniaux, and Michaël Périn. Efficient generation of correctness certificates for the abstract domain of polyhedra. In *Static analysis (SAS)*, 2013.

1. `https://www.mathworks.com/products/polyspace.html`