

Compilation de programmes SCADE avec garantie de la précision numérique

Mots clés : Sémantique, Analyse Statique, Interprétation Abstraite, transformation de codes

Lieu : Laboratoire ELIAUS, Université de Perpignan Via Domitia

Equipe d'accueil : Equipe de recherche DALI

Directeur de stage : Matthieu Martel (matthieu.martel@univ-perp.fr)

SCADE est un langage largement utilisé pour le développement de systèmes embarqués critiques synchrones tels que les systèmes de commande de vol numérique d'un avion. D'abord utilisé pour la spécification, la simulation et la vérification de propriétés de sûreté de haut niveau, ce langage permet aussi de produire un code final via un processus de compilation. Il est alors légitime que l'utilisateur souhaite que les propriétés prouvées sur le modèle soient garanties pour le code objet. Actuellement, le principal obstacle à cela est que la sémantique de SCADE spécifie que les calculs sont effectués en nombres réels. Or le programme final utilise des nombres flottants dont l'arithmétique est très différente de celle des réels, notamment à cause des erreurs d'arrondi. Le but de ce projet est d'utiliser des techniques de transformation d'expressions tenant compte de la précision des calculs pour garantir la préservation des propriétés numériques lors de la compilation de SCADE. Les preuves de correction reposent sur une interprétation abstraite des différentes traces d'exécution obtenues.

L'optimisation de la précision des calculs en nombres flottants est difficilement réalisable manuellement car l'arithmétique utilisée est particulièrement non-intuitive (par exemple les opérations sont non-associatives, non-inversibles, etc.). Pour contourner cette difficulté, une nouvelle sorte de transformation de programmes permettant d'améliorer automatiquement la précision de calculs en nombres flottants a récemment été proposée. Elle consiste à autoriser des ré-écritures de formules, normalement fausses dans les nombres flottants (parenthésage, factorisation, modification de constantes) de façon à générer automatiquement une nouvelle formule, mathématiquement égale à la première et plus précise en ce qui concerne son évaluation par un ordinateur. Cette technique permet aussi de garantir des bornes d'erreurs sur les résultats produits par le code objet.

L'objectif de ce stage est d'adapter les résultats actuels, qui portent sur la transformation d'expressions arithmétiques, à la transformation de programmes écrits dans un noyau de langage SCADE. On s'intéressera notamment aux calculs effectués à travers plusieurs variables dépendantes et éventuellement dans des boucles. D'un point de vue théorique, il sera nécessaire de concevoir une nouvelle analyse statique permettant d'approcher finement les erreurs pouvant survenir dans des ensembles de traces d'exécution de programmes SCADE. Selon l'avancement, un prototype pourra être développé et il sera possible d'étudier l'impact de la nouvelle méthode sur des extraits de codes issus d'applications industrielles (logiciels d'avionique ou autres systèmes embarqués critiques).

Ce stage est susceptible de déboucher sur une thèse portant sur la conception et l'implémentation d'un compilateur pour SCADE utilisable industriellement, en relation avec des entreprises majeures du domaine (dans l'aéronautique notamment). Possibilité de rémunération.