Proposition de stage Master 2 recherche

Extraction de contre-exemples

Mots-clés : méthodes formelles, vérification déductive, programmes C

Cadre

Le CEA LIST est un centre de recherche technologique sur les systèmes à logiciel prépondérant qui mène ses recherches en partenariat avec les grands acteurs industriels du nucléaire, de l'automobile, de l'aéronautique, de la défense et du médical pour étudier et développer des solutions innovantes adaptées à leurs besoins. Au sein du CEA LIST, le Laboratoire de Sûreté des Logiciels (LSL), localisé à Saclay (Essonne, 91), développe des outils d'aide à la validation et à la vérification de logiciels et de systèmes matériels/logiciels, tout particulièrement dans le domaine des systèmes embarqués critiques.

Frama-C (`http://frama-c.com`) est une plate-forme logicielle facilitant le développement en *OCaml* d'outils d'analyses de programmes C. Le stage se déroulera au sein de l'équipe de R&D développant Frama-C.

Objectifs

Le greffon Value Analysis de Frama-C, basé sur l'interprétation abstraite, vise entre autres à vérifier l'absence d'erreur à l'exécution du code sous analyse. Quand il détecte une erreur potentielle, il émet un avertissement, et génère une annotation ACSL (ANSI/ISO C Specification Language) dont la vérification permettrait de s'assurer qu'on est en présence d'une fausse alarme. On peut alors essayer d'utiliser le greffon WP sur cette annotation. WP va générer une obligation de preuve correspondant à l'annotation par remontée de plus faible pré-condition, avant de l'envoyer à un prouveur automatique, comme alt-ergo, Simplify ou Z3. Dans le cas où on est en présence d'une vraie alarme, certains de ces prouveurs sont susceptibles de renvoyer un *modèle*, c'est à dire une instantiation des variables de l'obligation de preuve aboutissant à la négation de la formule. Ce modèle est cependant exprimé au niveau logique, et ne reflète donc qu'indirectement les variables du programme C mises en jeu.

Un prototype de greffon Frama-C se propose de faire remonter les informations des prouveurs au niveau du C afin de fournir à l'utilisateur un test directement exploitable menant au problème détecté par l'analyse de valeur. Ce greffon est cependant assez limité, et le but du stage sera de l'étendre significativement dans différentes directions, comme par exemple :

- prise en compte de nouveaux prouveurs/meilleure prise en compte des modèles générés
- Utilisation des résultats de Value Analysis pour faciliter le passage des boucles (nombre de tours, invariants de boucle)

Candidatures

Profil des candidats

- Bonnes connaissances en *OCaml*
- Capacité de travail en équipe
- Une connaissance du C serait un plus.

Conditions : stage indemnisé, aide au logement possible, transports CEA en Île-de-France.

Contact : Virgile Prevosto (virgile.prevosto@cea.fr)

Les délais administratifs au CEA étant de 2 à 3 mois minimum, nous vous recommandons de prendre contact au plus tôt.