Proposition de stage Master 2 recherche

Vérification de propriétés temporelles

Mots-clés : vérification de programmes, propriétés temporelles

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. 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

Un des greffons de Frama-C, Aoraï, s'intéresse à la vérification de propriétés sur les séquences d'appels de fonctions qu'un programme peut effectuer, données sous forme d'automate. Le stage consiste à proposer de nouveaux formalismes de description de ces propriétés. Frama-C utilise un langage de spécification ACSL permettant de préciser le contrat (pré- et post-condition) de chaque fonction d'un programme C. Le greffon Aoraï vise à établir des propriétés plus globales, décrivant à l'aide d'un automate, les séquences d'appels de fonctions qui sont autorisées lors d'une exécution. Pour cela, Aoraï traduit cet automate en un contrat ACSL pour chaque fonction du programme, qui peut être par la suite prouvé par les greffons d'analyse de Frama-C, tel que Value et WP. Aoraï s'appuie en outre sur l'outil `ltl2ba` pour permettre de décrire les séquences d'appels à l'aide d'une formule de logique temporelle (LTL). Le but du stage est d'étendre cette possibilité en développant un outil permettant de traduire des formules LTL directement dans le langage. Ce travail pourra également être l'occasion d'apporter des extensions au langage d'automate reconnu par Aoraï afin de faciliter l'écriture de certains scénarios d'appels de fonctions.

Candidatures

Profil des candidats

- Bonnes connaissances en *OCaml*
- Intérêt pour l'analyse automatique de programmes réels
- 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) - Sébastien Bardin (sebastien.bardin@cea.fr)

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