Proposition de stage de master

Génération automatique de code à partir de spécifications formelles

Mots-clés : génération de code, spécification formelle.

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.

L'un des nos outils, nommé *Frama-C* (`http://frama-c.com`) et développé en *OCaml*, est une plateforme logicielle facilitant le développement d'analyses de programmes C. Le stage se déroulera au sein de l'équipe de R&D développant *Frama-C*.

Objectifs

Frama-C permet d'annoter formellement un programme C grâce au langage *ACSL* (`http://frama-c.com/acsl`) afin de spécifier le comportement attendu de ce programme. Cette plateforme propose aussi différentes techniques d'analyses pour vérifier que le programme satisfait bien sa spécification *ACSL*.

Lorsqu'un programme n'est que partiellement défini car le code de certaines fonctions (généralement issues de bibliothèques externes) n'est pas connu, il est toujours possible de le vérifier statiquement (*i.e.* sans l'exécuter) en spécifiant en *ACSL* le comportement attendu de ces fonctions.

Néanmoins, reposer uniquement sur ces spécifications en l'absence de code est problématique pour effectuer des vérifications dynamiques (*i.e.* avec exécution du programme sous analyse). Une solution est alors de fournir une implémentation alternative respectant la spécification *ACSL* de chaque fonction manquante, mais ce procédé peut vite devenir fastidieux.

Le but du stage est de développer un nouveau module *Frama-C* permettant de générer automatiquement un code correct des fonctions inconnues à partir de leurs spécifications en *ACSL*. Par exemple, lorsque la spécification indique que la fonction doit retourner 0, il suffit de générer `return 0;`. La génération – est-il besoin de le préciser ? – est cependant loin d'être toujours aussi simple et il conviendra d'identifier le schéma de génération pour le sous-ensemble le plus large possible du langage *ACSL*. Les travaux pourront s'appuyer sur les recherches récentes dans le domaine de la synthèse de fonctions, comme [1].

[1] V. Kuncak, M. Mayer, R. Piskac, P. Suter. Complete Functional Synthesis. Proceedings of the 2010 Programming Language Design and Implementation (PLDI'10). 2010.

Candidatures

Maîtriser les langages *OCaml* et *C* est nécessaire pour ce stage. Posséder des notions en compilation et en spécification formelle est un plus, mais n'est pas indispensable.

Contact : Julien Signoles (*julien.signoles*@cea.fr)

Les délais administratifs au CEA étant de 2 à 3 mois minimum, merci de prendre contact le plus tôt possible.