Encadrant : Nicolas Stouls

Contact : nicolas.stouls@insa-lyon.fr

Titre : Encodage de propriétés dynamiques dans des assertions de logique du premier ordre

Contexte

Preuve de programme

La preuve de programmes est une méthode de vérification formelle consistant à établir, par la preuve, que toute exécution d'un programme respecte une propriété donnée. Par exemple, la chaine d'outils Frama-C/Jessie/Why[1] permet de générer des obligations de preuves[2] à partir d'un programme C contenant des propriétés sous la forme d'annotation (décrite avec le langage d'annotations ACSL). Classiquement, la preuve de programmes se limite aux propriétés invariantes. Cependant de récents travaux [TH02,Gro07,GS09] ont proposé différentes méthodes d'encodage de propriétés dynamiques sous la forme d'invariants. Bien que cette traduction soit nécessairement partielle, nous voulons proposer des heuristiques permettant de favoriser la faisabilité et l'automaticité des obligations de preuve générées. Ce stage s'insère dans la réalisation de l'outil Aoraï [GS09], qui est un greffon de la plateforme Frama-C.

Sujet

L'objectif de ce stage est dans un premier temps, d'étudier les différentes traductions proposées dans la littérature, avant de les comparer avec les choix effectués au sein de l'outil Aoraï. Ensuite, le candidat sera amené à proposer ses propres heuristiques et à les expérimenter manuellement sur différents exemples. Si ces tests sont concluants, alors il sera possible d'implanter ces propositions au sein de l'outil Aoraï avant la prochaine release de la plateforme Frama-C. Une réflexion pourra également être menée sur les extensions possibles du langage de spécification ACSL, pour y inclure des primitives comportementales.

Bibliographie

[Gro07] J. Groslambert. *Vérification de propriétés temporelles par génération d'annotations.* PhD thesis, Université de Franche-Comté, 2007.

[GS09] Julien Groslambert et Nicolas Stouls, *Vérification de propriétés LTL sur des programmes C par génération d'annotations*, in *AFADL'09*.

[TH02] K. Trentelman and M. Huisman. *Extending JML Specifications with Temporal Logic.* In AMAST'02, number 2422 in LNCS, pages 334–348.

1 http://www.frama-c.cea.fr/

2 Une obligation de preuve est une formule logique dont on cherche à établir la verracité.