Proposition de Stage

Terminaison interactive de preuve de programme avionique

Lieu

Airbus, Toulouse

Personnes encadrant le stage

Encadrant principal
Jean Souyris
Airbus, Toulouse
Tél : 05.61.93.00.57
Email : `jean.souyris@airbus.com`
Fiche du stage accessible à l'URL
http://www.eads.com/eads/france/fr/travailler-pour-eads/postuler/rechercher-les-offres.html,
rechercher le stage numéro 10148055.

Enseignant du MPRI tuteur de ce stage
Claude Marché (Equipe ProVal)
http://www.lri.fr/proval
INRIA Saclay & Université Paris-Sud
Orsay, France Tél : 01 72 92 59 69
Email : `Claude.Marche@inria.fr`

Description du travail de stage

Frama-C (http://www.frama-c.com) est un environnement pour l'analyse statique de code source en langage C. Cet environnement permet d'établir la conformité du code vis-à-vis de spécifications formelles écrites en ACSL [2]. Cette validation s'effectue à l'aide d'outils de démonstration automatique, ou dans les cas les plus durs, avec l'assistant interactif de preuve Coq (http://coq.inria.fr/ [3]). La communication avec les outils de preuve externes passe par le système Why3 (http://why3.lri.fr [4]).

Cet environnement est utilisé expérimentalement à Airbus pour valider du code embarqué d'avionique. Dans un tel contexte, Il est souhaitable d'alléger autant que possible le travail de preuve interactive. C'est là l'objectif de ce stage.

Une description plus détaillée de ce stage est accessible depuis l'URL de contact donnée ci-dessus.

Les pistes envisagées pour traiter le sujet sont de 2 types. D'une part, on visera à définir une collection de tactiques Coq qui seraient plus ou moins spécialisées pour le domaine d'application considéré. D'autre part, on étudiera la possibilité d'appeler depuis Coq les autres prouveurs automatiques disponibles dans Why3. Les fondements de cette approche sont décrits dans [5, 1]

Prérequis souhaités

Connaissances de base en logique, théorie de la démonstration, en méthodes de spécification formelle de programmes. Connaissance pratique de l'environnment de preuve Coq.

Références

[1] Nicolas Ayache and Jean-Christophe Filliâtre. Combining the Coq proof assistant with first-order decision procedures. http://www.lri.fr/~filliatr/publis/coq-dp.ps.gz, March 2006.

[2] Patrick Baudin, Jean-Christophe Filliâtre, Claude Marché, Benjamin Monate, Yannick Moy, and Virgile Prevosto. *ACSL : ANSI/ISO C Specification Language, version 1.4*, 2009. http://frama-c.cea.fr/acsl.html.

[3] Yves Bertot and Pierre Castéran. *Interactive Theorem Proving and Program Development.* Springer-Verlag, 2004.

[4] François Bobot, Jean-Christophe Filliâtre, Claude Marché, and Andrei Paskevich. Why3 : Shepherd your herd of provers. In *Boogie 2011 : First International Workshop on Intermediate Verification Languages*, Wrocław, Poland, August 2011.

[5] Stéphane Lescuyer. *Formalisation et développement d'une tactique réflexive pour la démonstration automatique en Coq.* Thèse de doctorat, Université Paris-Sud, 2011.