

Une application concrète pour la spécification ou la certification formelle

Marc Daumas

Titre du stage : Une application concrète pour la spécification ou la certification formelle en arithmétique à virgule flottante ou en micro-électronique au format RTL

Mots-clés : Méthodes formelles, Coq, PVS, Arithmétique d'intervalles, Certification, EAL-7, Virgule flottante, Algorithme numérique, Contrôleur, Traitement du signal, Circuit, VHDL.

Durée : Février – début juillet 2006

Encadrant : Marc Daumas

Fonction : Chargé de recherche au CNRS, habilité à diriger des recherches

Cette proposition de stage est conditionnée à la mutation au LIRMM de l'encadrant. Une demande est actuellement en cours d'examen par le Comité National et le Département MIPPU du CNRS.

Laboratoire : La localisation du stage, ou la répartition de la présence entre les deux sites, dépendra du choix de l'application et des contraintes personnelles de l'étudiant.

- Laboratoire d'Informatique, de Robotique et de Micro-électronique de Montpellier (LIRMM) — UMR 5506 CNRS — 161, rue Ada — 34392 Montpellier Cedex 5.
- Laboratoire de Physique Appliquée et d'Automatique (LP2A) — EA 3679 MENESR — 52, avenue Paul Alduy — 66860 Perpignan Cedex.

Téléphone : +33 (0)4 68 66 21 25

Télécopie : +33 (0)4 68 66 22 87

Mél : Marc.Daumas@ENS-Lyon.Fr.

Domaine du stage

Ce stage se trouve à l'interface entre l'utilisation des méthodes formelles et selon l'application choisie soit l'algorithmique numérique et l'arithmétique de ordinateurs soit la micro-électronique et l'architecture des processeurs. Le stagiaire bénéficiera du rapprochement scientifique en cours de discussion sur l'ensemble de ces thématiques entre le LIRMM et le LP2A.

Description détaillée du travail

Le stage consistera à spécifier ou à certifier une application concrète en utilisant un outil de preuve formelle, directement ou indirectement. Une connaissance des outils Coq ou PVS sera appréciée mais le travail pourra aussi être entièrement réalisé dans le cadre de l'arithmétique d'intervalles classique grâce à l'outil Gappa développé actuellement dans la thèse de Melquiond. L'application concrète sera soit un algorithme numérique récemment mis au point au LP2A soit un contrôleur très simple (mais efficace) codé au niveau RTL et actuellement commercialisé par une jeune pousse (start-up) de Montpellier.

Pour la spécification du contrôleur, il faudra la concevoir avec un outil formel comme Coq ou PVS. Le circuit est décrit au niveau des transferts de registres. Il est relativement simple ce qui permet d'envisager une spécification complète ainsi qu'une preuve de correction de certaines parties du circuit.

Le stage consistera dans un premier temps à faire une étude bibliographique des projets antérieurs, spécialement en Coq, PVS et ACL2. L'étudiant proposera ensuite une méthode et implantera sa spécification. Il devrait lui rester du temps pour montrer la correction de certaines parties du circuit en regard de sa spécification. Le choix des parties à valider sera réalisé par l'étudiant avec un objectif de modularité et d'impact.

Pour la certification d'un algorithme numérique, nous nous intéresserons aux travaux récents de Graillat, Langlois et Louvet du LP2A sur l'évaluation de Horner compensée. L'étudiant commencera par modéliser ce problème avec l'outil Gappa. La suite de son travail consistera soit à proposer et à

certifier des algorithmes du même type avec Gappa soit à proposer des développements plus spécifiques avec l'outil Coq ou PVS.

Commentaires

Industriellement, la certification d'un code ou d'une architecture est particulièrement rentable. Un article paru récemment dans la revue IEEE Spectrum présente la compagnie Praxis, en Angleterre, qui développe du logiciel validé. Un de leurs projets, donné en exemple, n'a eu que 4 erreurs pour 100 000 lignes de code après un an de fonctionnement. Soit 0,04 erreurs pour 1 000 lignes de code. On est bien loin de 2-10 erreurs pour 1 000 lignes communément admises dans les projets logiciels. Praxis facture la ligne de code 50% plus cher, mais le test peut représenter entre 30 et 90% du temps de développement. Réduire le temps de test peut donc permettre des économies énormes. Enfin, l'auteur estime que l'absence d'erreur a réduit les coûts de maintenance de 20 à 25%.

<http://www.spectrum.ieee.org/sep05/1454>

Pour ce qui est du matériel, les deux seuls projets à avoir atteint le niveau EAL-7 soit le plus haut niveau de confiance dans les critères communs pour l'évaluation des produits et systèmes des technologies de l'information ont mis en oeuvre des méthodes formelles.

<http://www.rockwellcollins.com/news/page6237.html>

<http://newsroom.slb.com/press/newsroom/index.cfm?PRID=16261>

Comme indiqué dans ce qui précède, la connaissance d'un outil de preuve formelle tel que Coq ou PVS n'est pas nécessaire pour réussir ce stage. Un soutien financier ou une rémunération au mérite seront envisagés au vu des compétences de l'étudiant et des retombées industrielles attendues de l'application choisie.

Il n'est pas exclu que certaines nationalités classées comme sensibles par le Ministère de la Défense ne puissent pas travailler sur toutes les applications mentionnées dans ce sujet. Ces deux derniers points seront envisagés au cas par cas avec les candidats avant le début du stage.