

Année 2009

Proposition de sujet de thèse

TITRE : PREUVES EN AVANT ET EN ARRIÈRE MODULO THÉORIES

LIEU : Projet ProVal, INRIA Saclay Île de France
Parc club Orsay Université, Zac des Vignes
4, rue Jacques Monod, Bâtiment N
91893 Orsay cedex

PERSONNES ENCADRANT LA THÈSE :
Sylvain Conchon et Evelyne Contejean
Tél : 01 72 92 59 {56, 96}
Email : {conchon, contejea}@lri.fr

CONTEXTE :

Le projet ProVal commun au LRI et à l'INRIA Saclay propose des méthodes et outils de développement logiciel faisant une large place à la preuve de programmes assistée par ordinateurs. Des applications logicielles critiques dans les domaines du transport, des transactions bancaires ou des télécommunications sont mises rapidement sur le marché. Pour garantir aux utilisateurs un comportement acceptable, il est nécessaire qu'une large part de vérification soit réalisée de manière mécanique. Nous développons des environnements qui à partir d'une description formelle du comportement attendu du programme, exprimée par le développeur dans un langage adapté à son problème, engendre des formules logiques (obligations de preuve) suffisantes pour garantir la correction du programme. Ces formules peuvent ensuite être traitées par des démonstrateurs adaptés.

OBJECTIFS SCIENTIFIQUES :

Les démonstrateurs automatiques actuels se divisent en deux catégories :

- ceux basés sur le mécanisme générique de la résolution permettent d'attaquer tous les problèmes finiment axiomatisables sous forme de clauses ;
- les prouveurs SMT (« satisfiabilité modulo théories ») quant à eux, sont construits à l'aide d'un solveur SAT et d'une combinaison de procédures de décision pour des théories prédéfinies.

Les mécanismes de recherche de ces démonstrateurs sont basés pour les premiers sur l'unification (preuve en arrière) et pour les seconds sur l'instanciation des lemmes par des termes déjà présents dans le système (preuve en avant). L'avantage de la première approche est qu'elle est générale et complète par réfutation, mais elle ne permet pas d'intégrer toutes les théories traitées par les prouveurs SMT (celles qui ne sont pas finiment axiomatisables), et de plus elle ne bénéficie pas des avancées des solveurs SAT en matière d'efficacité .

D'un point de vue théorique, l'objectif de cette thèse est de proposer un nouveau paradigme de recherche de preuve combinant les avantages de ces deux approches. À partir d'une architecture SMT, il s'agira d'intégrer des phases de génération de nouveaux lemmes. En particulier, il serait bon d'intégrer l'aspect modulo théories dans le mécanisme de résolution.

Le but pratique est de renforcer l'efficacité du prouveur SMT Alt-Ergo, développé dans l'équipe ProVal, en intégrant ce nouveau schéma de recherche de preuves.

COMPÉTENCES :

- démonstration automatique,
- connaissance du langage Ocaml.