Démonstration automatique en Coq

Proposition de stage de Master

Valentin Blot <Valentin.Blot@lri.fr>
Chantal Keller <Chantal.Keller@lri.fr>

1 Cadre du stage

Le stage se déroulera au Laboratoire de Recherche en Informatique de l'Université Paris-Sud à Orsay (région parisienne), sous la direction de Valentin Blot et Chantal Keller.

Le stage peut être gratifié. Le stagiaire pourra continuer en thèse selon son souhait.

2 Contexte

SMTCoq [AFG+11, EKK+16, EMT+17] est un plugin pour l'assistant de preuves Coq développé en partenariat entre l'Université Paris-Sud, l'Université de l'Iowa (États-Unis) et l'Inria Sophia Antipolis Méditerranée.

Son but est de faire interagir Coq avec des prouveurs automatiques externes de satisfiabilité (prouveurs SAT et SMT), avec un double objectif :

- augmenter la confiance dans ces prouveurs automatiques, des programmes complexes qui peuvent contenir des bugs, en vérifiant les réponses qu'ils donnent ;
- augmenter l'automatisation de Coq en offrant la possibilité de faire appel à des prouveurs automatiques, sans compromettre sa cohérence.

SMTCoq permet ainsi de prouver automatiquement des buts Coq mélangeant raisonnement arithmétique avec des structures de données telles que vecteurs, tableaux, ... en intègrant différents prouveurs automatiques compétitifs tels que CVC4 [BCD+11] et veriT [BODF09].

Le cœur de SMTCoq est un vérificateur pour des certificats issus de prouveurs automatiques implanté et prouvé correct en Coq. Ce dernier permet de vérifier de manière très efficace et modulaire les résultats donnés par plusieurs prouveurs SAT et SMT. En amont de ce vérificateur, de nouvelles tactiques Coq permettent d'appeler des prouveurs automatiques sur des buts Coq et de vérifier les résultats obtenus.

Le but de ce stage est de renforcer l'expressivité de ces tactiques afin d'offrir aux utilisateurs de Coq une automatisation la plus grande possible.

3 Contribution attendue

Afin de se familiariser avec SMTCoq, le premier mois du stage se concentrera sur un ou plusieurs aspects pratiques :

- gérer les diverses représentations des entiers en Coq (unaires, binaires ; positifs, relatifs ; ...) ;
- gérer les diverses notions d'égalités en Coq et permettre à l'utilisateur d'en définir de nouvelles ;
- gérer les diverses représentation des propositions logiques (`bool` et `Prop`), notamment en utilisant l'approche de réflexion entre ces deux types proposée par SSReflect [GM08].

Le stage s'orientera ensuite vers des aspects mêlant théorie et pratique, en adaptant les techniques d'encodages de logiques expressives (logique d'ordre supérieure et théorie des types) vers les logiques utilisées par les prouveurs automatiques [BKPU16]. Cela débouchera sur des résultats théoriques sur les encodages entre systèmes logiques (nouveaux encodages, correction et complétude, ...) et une implantation pour SMTCoq.

4 Prérequis

Des connaissances basiques dans les assistants de preuve seront utiles. Il n'est pas nécessaire d'avoir des connaissances en démonstration automatique, SMTCoq ni SSReflect.

Références

[AFG+11] Michaël Armand, Germain Faure, Benjamin Grégoire, Chantal Keller, Laurent Théry, and Benjamin Werner. A Modular Integration of SAT/SMT Solvers to Coq through Proof Witnesses. In Jean-Pierre Jouannaud and Zhong Shao, editors, *CPP*, volume 7086 of *Lecture Notes in Computer Science*, pages 135–150. Springer, 2011.

[BCD+11] Clark Barrett, Christopher L. Conway, Morgan Deters, Liana Hadarean, Dejan Jovanovic, Tim King, Andrew Reynolds, and Cesare Tinelli. CVC4. In Ganesh Gopalakrishnan and Shaz Qadeer, editors, *Computer Aided Verification - 23rd International Conference, CAV 2011, Snowbird, UT, USA, July 14-20, 2011. Proceedings*, volume 6806 of *Lecture Notes in Computer Science*, pages 171–177. Springer, 2011.

[BKPU16] Jasmin Christian Blanchette, Cezary Kaliszyk, Lawrence C. Paulson, and Josef Urban. Hammering towards QED. *J. Formalized Reasoning*, 9(1) :101–148, 2016.

[BODF09] Thomas Bouton, Diego Caminha Barbosa De Oliveira, David Déharbe, and Pascal Fontaine. verit : An open, trustable and efficient smt-solver. In Renate A. Schmidt, editor, *Automated Deduction - CADE-22, 22nd International Conference on Automated Deduction, Montreal, Canada, August 2-7, 2009. Proceedings*, volume 5663 of *Lecture Notes in Computer Science*, pages 151–156. Springer, 2009.

[EKK+16] Burak Ekici, Guy Katz, Chantal Keller, Alain Mebsout, Andrew J. Reynolds, and Cesare Tinelli. Extending SMTCoq, a Certified Checker for SMT (Extended Abstract). In Jasmin Christian Blanchette and Cezary Kaliszyk, editors, *Proceedings First International Workshop on Hammers for Type Theories, HaTT@IJCAR 2016, Coimbra, Portugal, July 1, 2016.*, volume 210 of *EPTCS*, pages 21–29, 2016.

[EMT+17] Burak Ekici, Alain Mebsout, Cesare Tinelli, Chantal Keller, Guy Katz, Andrew Reynolds, and Clark W. Barrett. SMTCoq : A Plug-In for Integrating SMT Solvers into Coq. In Rupak Majumdar and Viktor Kuncak, editors, *Computer Aided Verification - 29th International Conference, CAV 2017, Heidelberg, Germany, July 24-28, 2017, Proceedings, Part II*, volume 10427 of *Lecture Notes in Computer Science*, pages 126–133. Springer, 2017.

[GM08] G. Gonthier and A. Mahboubi. A small scale reflection extension for the Coq system. *Rapport de recherche INRIA*, 2008.