Utilisation de prouveurs automatiques en Coq

Proposition de stage de Master

Chantal KELLER <Chantal.Keller@lri.fr>

November, 9th 2016

1 Cadre du stage

Le stage se déroulera au Laboratoire de Recherche en Informatique de l'Université Paris-Sud, sous la direction de Chantal KELLER.

2 Contexte

SMTCoq [AFG+11] est un plugin pour l'assistant de preuves Coq offrant une interaction avec des prouveurs automatiques externes de satisfiabilité (prouveurs SAT et SMT). Le but de cette interaction est double :

— 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.

Ainsi, le cœur de SMTCoq est un vérificateur pour des certificats SAT et SMT implanté et prouvé correct en Coq. Ce dernier permet de vérifier très efficacement les résultats donnés par plusieurs prouveurs SAT et SMT de manière modulaire [AFG+11, EKK+16], remplissant parfaitement son premier objectif.

En amont de ce vérificateur, de nouvelles tactiques Coq permettent d'appeler des prouveurs SAT et SMT sur des buts Coq et de vérifier le résultat obtenu, afin de remplir le deuxième objectif. Cependant, ces tactiques sont aujourd'hui peu performantes pour diverses raisons :

— elles forcent le but à être sous une certaine forme ne correspondant pas forcément aux habitudes des utilisateurs ;

— elles offrent peu d'expressivité car ne gèrent que les buts directement exprimés dans les logiques utilisées par les prouveurs automatiques.

Le but de ce stage est d'améliorer ces deux aspects afin d'offrir aux utilisateurs de Coq des tactiques automatiques strictement plus puissantes que les tactiques existantes, comme par exemple des tactiques permettant de résoudre des buts faisant intervenir à la fois égalité et arithmétique.

3 Contribution attendue

Le stage comporte des aspects théoriques et d'implantation.

Afin de se familiariser avec SMTCoq, la première partie du stage visera à l'amélioration du premier aspect, avec les possibilités suivantes :

— 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 stagiaire pourra ensuite s'orienter vers le deuxième aspect, 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 donnera lieu à des résultats théoriques sur les encodages entre systèmes logiques (nouveaux encodages, correction et complétude, ...) et à une implantation pour SMTCoq.

4 Prérequis

Des connaissances en Coq sont attendues, ainsi que des notions en théorie de la démonstration. Il n'est pas nécessaire de connaître la 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.

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

[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.

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