Démonstration automatique en Coq

Proposition de stage de Master

Valentin Blot <valentin.blot@inria.fr>
Gilles Dowek <gilles.dowek@ens-paris-saclay.fr>
Chantal Keller <Chantal.Keller@lri.fr>

1 Contexte

SMTCoq [AFG+11, EMT+17, HR19] est un plugin pour l'assistant de preuves Coq développé en partenariat entre l'Université Paris-Saclay, l'Université de l'Iowa (États-Unis), l'Université de Stanford (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 et veriT.

Le cœur de SMTCoq est un vérificateur pour des *certificats de preuve* 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.

2 Contribution attendue

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

— gérer les diverses notions d'égalités en Coq et permettre à l'utilisateur d'en définir de nouvelles, en lien avec la notion d'égalité connue des prouveurs SMT ;
— implanter différents algorithmes de sélection du contexte à envoyer aux prouveurs automatiques proposés dans la littérature ;
— ...

Le stage s'orientera ensuite vers des aspects mêlant théorie et pratique, pour proposer une nouvelle technique d'encodage de la logique expressive de Coq vers les logiques moins expressives utilisées par les prouveurs automatiques, et prouver sa correction. L'originalité de cet encodage sera d'être "à petits pas", c'est-à-dire qu'il sera découpé en plusieurs encodages simples et portant chacun sur un aspect de la logique de Coq. Cela permet une preuve de la correction plus modulaire, une meilleure composabilité des encodages et l'ajout incrémental de nouveaux encodages

au besoin. Selon les cas, la preuve de correction sera faite directement (par une preuve Coq) ou par la génération de certificats ensuite vérifiés, suivant l'approche générale de SMTCoq.

3 Cadre du stage

Le stage se déroulera au sein de l'équipe Inria Deducteam du centre Inria Saclay–Île-de-France, dont les travaux portent sur l'interopérabilité entre systèmes de preuves. Le stagiaire sera membre du Laboratoire Spécification et Vérification et du Laboratoire de Recherche en Informatique au sein de l'Université Paris-Saclay, tous deux situés à Orsay à partir du printemps 2020. Le stage sera gratifié.

Ce stage fait partie d'un projet en collaboration avec l'entreprise Nomadic Labs, portant sur l'automatisation en Coq et son application à la certification de blockchains [BCP+19]. Dans ce cadre, le stage pourra déboucher sur une thèse portant sur ces thématiques.

4 Prérequis

Des connaissances basiques dans l'assistant de preuve Coq seront utiles. Il n'est pas nécessaire d'avoir des connaissances en démonstration automatique ni SMTCoq.

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, *Certified Programs and Proofs - First International Conference, CPP 2011, Kenting, Taiwan, December 7-9, 2011. Proceedings*, volume 7086 of *Lecture Notes in Computer Science*, pages 135–150. Springer, 2011. Available at `http://hal.inria.fr/docs/00/63/91/30/PDF/cpp11.pdf`.

[BCP+19] Bruno Bernardo, Raphaël Cauderlier, Basile Pesin, Zhenlei Hu, and Julien Tesson. Mi-Cho-Coq, a framework for certifying Tezos Smart Contracts. In *10th Coq Workshop*, 2019.

[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. Available at `https://hal.archives-ouvertes.fr/hal-01669345/document`.

[HR19] Gila Hanna and David A. Reid, editors. *Proof Technology in Mathematics Research and Teaching*, chapter SMTCoq : Mixing automatic and interactive proof technologies. LNCS, 2019. Available at `https://www.lri.fr/~keller/Documents-recherche/Publications/proof-Technology-in-Mathematics-Research-and-Teaching_smtcoq.pdf`.