Automatic Theorem Proving in Coq

Master internship proposal

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

1 Context

SMTCoq [AFG+11, EMT+17, HR19] is a plugin for the Coq interactive theorem prover, developed in collaboration between Université Paris-Saclay, the University of Iowa (US), the University of Stanford (US) and Inria Sophia Antipolis Méditerranée.

Its goal is to make Coq interact with external, automatic theorem provers based on satisfiability (SAT and SMT), with a twofold objective:

- increase confidence in automatic provers, which are large programs that may be buggy, by checking the answers they give;
- increase Coq automation by offering the possibility to call automatic provers without compromising soundness.

SMTCoq thus allows users to automatically prove Coq goals mixing arithmetic reasoning and data structures such as vectors, arrays, ... by integrating various competitive automatic solvers such as CVC4 and veriT.

The heart of SMTCoq is a checker for *proof certificates* coming from automatic provers, implemented and proved correct inside Coq. This checker is able to check in a very efficient and modular way answers coming from different SAT and SMT solvers. On top of this checker, new Coq tactics allow users to call automatic solvers on Coq goals, automatically checking the answers.

The objective of the internship is to reinforce the expressivity of these tactics in such a way that Coq users can enjoy as much automation as possible.

2 Expected contribution

In order to get familiar with SMTCoq, the first month of internship will focus on one or multiple practical aspects:

- handle the various notions of equality in Coq, and allow the users to add new ones and link them with the SMT notion of equality;
- implement various algorithms to select the context to be sent to the automatic solvers, as proposed in the literature; ...

The internship will then focus on aspects mixing theory and practice: (1) propose a new method to encode the expressive logic of Coq into the less expressive logics of automatic provers and (2) establish its correctness. The originality of this new encoding will be to be fine grained, meaning that it will consist in small, simple encodings, each of them tackling one aspect of Coq's

logic. It allows one to make a modular proof of correctness, and offers a better composability of encodings and the possibility to incrementally add new ones on demand. Depending on the nature of the encodings, their correctness proofs will be performed directly (as a Coq proof) or by outputting certificates that will be checked *a posteriori*, following the SMTCoq general approach.

3 Environment

The internship will take place in the Inria team Deducteam of the research center Inria Saclay–Île-de-France. This team's research focuses on interoperability between proof systems. The intern will be a member of the Laboratoire Spécification et Vérification and the Laboratoire de Recherche en Informatique in Université Paris-Saclay, both located at Orsay since Spring 2020. The internship will be funded.

The internship is part of a collaboration with the Nomadic Labs company. The goal of this larger project is to improve Coq automation and apply it to blockchains verification [BCP+19]. The intern will be able to continue for a PhD thesis in this project.

4 Prerequisites

Basic knowledge in the Coq proof assistant can be useful. It is not necessary to have knowledge in automatic theorem proving nor SMTCoq.

References

[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*, 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`.