Automation in the Coq proof assistant, and its application to blockchains verification

Two-years post-doc proposal

Valentin Blot <valentin.blot@inria.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 this project is to reinforce the expressivity of these tactics, and study the use of automation in the context of the certification of the Tezos blockchain, in collaboration with the Nomadic Labs company.

2 Research topic

The postdoc will work on the following topics:

- increase SMTCoq's tactics expressivity in general: incrementally encode higher-order aspects of Coq into first-order logic, using a fine-grained and modular approach
- apply it to the certification of the Tezos blockchain:
  - in collaboration with Nomadic Labs, study this domain of proofs, identify classes of problems and collect examples and benchmarks;
  - study encodings of these classes of problems into first-order logic, implement them and evaluate them on the collected benchmarks

  - propose a surface language for these classes of problems that would be more accessible to non Coq experts

- generalize this surface language to other classes of problems.

3 Environment

The postdoc 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 postdoc 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.

4 Prerequisites

The postdoc should have a background in the area of blockchains.

He or she should have knowledge in formal methods (it is not required to be a Coq expert) and in functional programming.

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`.

[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`.