Leveraging Automatic Deduction for Verification

Topics

Computer Science, Logic, Automatic and Interactive Theorem Proving, Satisfiability Modulo Theories, Higher-Order Logic, Induction, Verification

Institution

Inria, Loria, Université de Lorraine (in cooperation with VU Amsterdam)

Location

Nancy, France (in close cooperation with Amsterdam, The Netherlands)

Team/Project

VeriDis

Supervision

Stephan Merz, Stephan.Merz@loria.fr
Pascal Fontaine, Pascal.Fontaine@loria.fr
Jasmin Blanchette, Jasmin.Blanchette@inria.fr

Background

This PhD subject is proposed in the context of Jasmin Blanchette's ERC Starting Grant Matryoshka,[1] an ambitious five-year project that aims at making automatic provers more useful for interactive verification by reducing the gap between the automatic and interactive worlds.

The TLA$^+$ Proof System (TLAPS)[2] is a platform for mechanically checking proofs for system specifications written in the TLA$^+$ language [4], based on Zermelo-Fraenkel set theory and the Temporal Logic of Actions (TLA), a variant of linear-time temporal logic. TLA$^+$ is a general-purpose formal specification language that is particularly well-known for describing concurrent and distributed algorithms and systems. It has seen significant use in academia and industry, including Amazon [6], Intel, Microsoft and many others.

In previous work [7, 5], we have already defined an overall strategy for encoding TLA$^+$'s set theory into first-order logic. Our encoding has been implemented within TLAPS for translating TLA$^+$ proof obligations to the input languages of Satisfiability Modulo Theories (SMT) solvers [1, 2] and first-order provers [8], and we have demonstrated a reduction of proof effort, measured as the number of user interactions, by one or two orders of magnitude for obligations that mix elementary set theory, basic integer arithmetic, and first-order logic.

The overall ambition of the present thesis is to build upon this success and significantly improve the scope of automation within TLAPS, by building upon, and contributing to, the advances in Satisfiability Modulo Theories solvers within the scope of the Matryoshka project. This includes support for important data structures, such as sequences, that are outside the scope of the current SMT encoding. It also aims at leveraging the work within Matryoshka on lifting the reasoning capabilities of SMT solvers towards higher-order logic, including support for inductive reasoning and complex set-theoretic expressions such as set comprehension.

[1] http://matryoshka.gforge.inria.fr/
[2] https://tla.msr-inria.inria.fr/tlaps/

Objectives

Building on [7, 5], this thesis will design new techniques of automatic proof and make them available within TLAPS in order to further increase automation for deductive verification. We envisage the following possible directions:

- design decision procedures that support important data structures of TLA$^+$ such as finite sequences. Their theoretical properties (soundness, completeness, and complexity) will be analyzed, and they will be implemented as a prototype;
- exploit new capabilities of SMT solvers for higher-order reasoning, in particular for supporting proofs by inductive reasoning and for set comprehensions;
- use proofs and models to improve confidence and guidance in verification platforms;
- develop effective and complete techniques for iterative refinement of the translation into the solver language, in particular concerning the expansion of operator definitions;
- analyze the specification and proof obligations in order to provide hints for proof search in SMT, notably for instantiation: we aim at providing syntactic criteria and characterizing decidable fragments.

The results of the thesis will be of primary interest to users of TLA$^+$, but they can also be relevant for related set-based specification formalisms such as Event-B, and the associated verification platforms, such as Rodin, cf. [3]. The subject can and will be adjusted according to the interests of the PhD candidate, in particular for choosing which of the above directions will be pursued first.

Requirements

We are looking for excellent candidates with a strong interest for logic, decision procedures, proofs and verification. Some acquaintance with either automated, interactive theorem proving, or deductive verification platforms is a plus. Knowledge of French is not required. The student will work in an international environment, in collaboration with several PhD students and experienced scientists.

How to apply

Send the following documents to stephan.merz@loria.fr in a single ZIP file:

- your up-to-date CV,
- an accompanying letter explaining your motivation and background for carrying out this project,
- your degree certificates and transcripts for your Bachelor and Master degrees (or the last five years if not applicable),
- your Master thesis (or equivalent) if it is already completed or a description of the work in progress otherwise,
- publications if any (it is not expected that you have already published).

In addition, at least one letter of reference written by the person who supervises your Master thesis (or research project or internship) must be provided. At most two other recommendation letters may be sent. These letters should be sent directly to stephan.merz@loria.fr.

Benefits

- Monthly net salary of approximately 1600 euros, medical insurance included.
- Possibility of free French courses.
- Help with finding accommodation and administrative procedures, such as obtaining a visa.
- Subsidized lunch at the Inria restaurant.

References

[1] C. Barrett, R. Sebastiani, S. A. Seshia, and C. Tinelli. Satisfiability modulo theories. In A. Biere, M. J. H. Heule, H. van Maaren, and T. Walsh, editors, *Handbook of Satisfiability*, volume 185 of *Frontiers in Artificial Intelligence and Applications*, chapter 26, pages 825–885. IOS Press, Feb. 2009.

[2] T. Bouton, D. C. B. de Oliveira, D. Déharbe, and P. Fontaine. veriT: an open, trustable and efficient SMT-solver. In R. Schmidt, editor, *Proc. Conference on Automated Deduction (CADE)*, volume 5663 of *Lecture Notes in Computer Science*, pages 151–156, Montreal, Canada, 2009. Springer.

[3] D. Déharbe, P. Fontaine, Y. Guyot, and L. Voisin. SMT solvers for Rodin. In J. Derrick, J. A. Fitzgerald, S. Gnesi, S. Khurshid, M. Leuschel, S. Reeves, and E. Riccobene, editors, *ABZ*, volume 7316 of *Lecture Notes in Computer Science*, pages 194–207. Springer, 2012.

[4] L. Lamport. *Specifying Systems, The TLA$^+$ Language and Tools for Hardware and Software Engineers*. Addison-Wesley, Boston, Mass., 2002.

[5] S. Merz and H. Vanzetto. Encoding TLA$^+$ into unsorted and many-sorted first-order logic. *Science of Computer Programming*, 2017. To appear.

[6] C. Newcombe, T. Rath, F. Zhang, B. Munteanu, M. Brooker, and M. Deardeuff. How Amazon web services uses formal methods. *CACM*, 58(4):66–73, 2015.

[7] H. Vanzetto. *Proof automation and type synthesis for set theory in the context of TLA$^+$. (Automatisation de preuves et synthèse de types pour la théorie des ensembles dans le contexte de TLA$^+$).* PhD thesis, University of Lorraine, Nancy, France, 2014.

[8] C. Weidenbach, D. Dimova, A. Fietzke, M. Suda, and P. Wischnewski. Spass version 3.5. In R. Schmidt, editor, *22nd International Conference on Automated Deduction (CADE-22)*, volume 5663 of *Lecture Notes in Computer Science*, pages 140–145, Montreal, Canada, 2009. Springer.