The TLA$^+$ Proof System: Building a Heterogeneous Verification Platform[⋆]

Kaustuv Chaudhuri[1], Damien Doligez[2], Leslie Lamport[3], and Stephan Merz[4]

[1] INRIA Saclay, France
[2] INRIA Rocquencourt, France
[3] Microsoft Research Silicon Valley, USA
[4] INRIA Nancy, France

Model checking has proved to be an efficient technique for finding subtle bugs in concurrent and distributed algorithms and systems. However, it is usually limited to the analysis of small instances of such systems, due to the problem of state space explosion. When model checking finds no more errors, one can attempt to verify the correctness of a model using theorem proving, which also requires efficient tool support.

TLAPS, the TLA$^+$ proof system, is a platform for the development and mechanical verification of TLA$^+$ proofs. Proofs are written in TLA$^+$, which contains a hierarchical proof language based on elementary mathematics [1]. It has been designed independently of any specific verification tool or strategy. TLAPS consists of a front-end, called the proof manager, and of a collection of back-end verifiers that include theorem provers, SMT solvers, and decision procedures. The proof manager interprets TLA$^+$ proofs and generates the corresponding proof obligations that must be verified, The current release [2] handles almost all the non-temporal part of TLA$^+$, which suffices for proving standard safety properties, but not liveness properties. The proof manager supports hierarchical and non-linear proof construction and verification so that the skeleton of an incomplete proof can be verified independently of the lower-level subproofs.

In this talk we discuss the design of the TLA$^+$ proof language and of the proof system. The different back-end verifiers used by TLAPS have complementary strengths and weaknesses, and having a heterogeneous set of proof techniques makes for a stronger overall verification system. However, it is important to ensure the overall correctness of the resulting proof. We approach this problem by making back-end verifiers proof-producing and certifying these proofs within the kernel of the interactive proof assistant Isabelle, for which we developed an encoding of the TLA$^+$ logic.

References

1. Chaudhuri, K., Doligez, D., Lamport, L., Merz, S.: A TLA$^+$ proof system. In: Sutcliffe, G., Rudnicki, P., Schmidt, R., Konev, B., Schulz, S. (eds.) Proc. of the LPAR Workshop Knowledge Exchange: Automated Provers and Proof Assistants (KEAPPA 2008). CEUR Workshop Proceedings, vol. 418, pp. 17–37 (2008)
2. Chaudhuri, K., Doligez, D., Lamport, L., Merz, S.: Verifying safety properties with the TLA$^+$ proof system. In: Giesl, J., Hähnle, R. (eds.) Intl. Joint Conf. Automated Reasoning (IJCAR 2010). LNCS. Springer, Heidelberg (to appear, 2010), `http://msr-inria.inria.fr/~doligez/tlaps/`

[⋆] This work is supported by the Joint Centre of Microsoft Research and INRIA in Saclay, France.

A. Cavalcanti et al. (Eds.): ICTAC 2010, LNCS 6255, p. 44, 2010.