Abstract: Automatic Verification of SMT Rewrites in Isabelle/HOL

Hanna Lachnitt¹, Mathias Fleury², Leni Aniva¹, Andrew Reynolds³, Haniel Barbosa⁴, Andres Noetzli⁵, Clark Barrett¹ and Cesare Tinelli³

¹Stanford University ²University of Freiburg ³The University of Iowa ⁴Universidade Federal de Minas Gerais ⁵Cubist, Inc.

Abstract

Satisfiability modulo theories (SMT) solvers are widely used to ensure the correctness of safety- and security- critical applications. Therefore, being able to trust a solver's results is crucial. One way to increase trust is to generate proof certificates, which record the reasoning steps the solver has done. These proof certificates can be given to a proof checker which determines whether the steps in the proof are correct. One key challenge with this approach is that it is difficult to efficiently and accurately produce proofs for reasoning steps involving term rewriting rules (of which there are many in modern SMT solvers). Previous work showed how a domain-specific language, RARE, can be used to capture rewriting rules for the purposes of proof production. However, the RARE rules were trusted—i.e., the correctness of the rules themselves was not checked by the proof checker. In this paper, we present IsaRARE, a tool that can automatically generate lemmas in the interactive theorem prover Isabelle/HOL corresponding to RARE rewrite rules. The correctness of the rules can then be verified by proving the lemmas. We evaluate our approach by verifying an extensive set of rewrite rules used by the cvc5 SMT solver.

SMT'23: 21st International Workshop on Satisfiability Modulo Theories, July 5–6, 2023, Rome, Italy lachnitt@stanford.edu (H. Lachnitt); fleury@cs.uni-freiburg.de (M. Fleury); leniv@stanford.edu (L. Aniva); andrew-reynolds@uiowa.edu (A. Reynolds); hbarbosa@dcc.ufmg.br (H. Barbosa); noetzli@cs.stanford.edu (A. Noetzli); barrett@cs.stanford.edu (C. Barrett); cesare-tinelli@uiowa.edu (C. Tinelli)

^{© 0 023} Copyright for this paper by its authors. Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0).

CEUR Workshop Proceedings (CEUR-WS.org)