

Abstract: Challenges and Solutions for Higher-Order SMT Proofs

Chad E. Brown¹, Mikoláš Janota¹ and Cezary Kaliszyk²

¹Czech Technical University in Prague, Czech Institute of Informatics, Robotics and Cybernetics, Prague, Czech Republic

²University of Innsbruck, Innsbruck, Austria

Abstract

An interesting goal is for SMT solvers to produce independently checkable proofs. SMT languages already have expressive power that goes beyond first-order languages, and further extensions would give even more expressive power by allowing quantification over function types. Indeed, such extensions are considered in the current proposal for the new standard SMT3. Given the expressive power of SMT and its extensions, careful thought must be given to the intended semantics and an appropriate notion of proof. We propose higher-order set theory as an appropriate interpretation of SMT (and extensions) and obtain an adequate notion of SMT proofs via proof terms in higher-order set theory. To demonstrate the strength of this approach, we give a number of abstract examples that would be difficult to handle by other notions of proof. To demonstrate the practicality of the approach, we describe a family of integer difference logic examples. We give proof terms for each of these examples and check the correctness of the proofs using two proof checkers: the proof checker distributed with the Proofgold system and an alternative checker we have implemented that does not rely on access to the Proofgold block chain.

Keywords

Satisfiability Modulo Theories, Bit-Vector Reasoning, Local Search


SMT 2022: Satisfiability Modulo Theories, August 11–12, 2022, Haifa, Israel

✉ Mikolas.Janota@cvut.cz (M. Janota); cezary.kaliszyk@uibk.ac.at (C. Kaliszyk)

🆔 0000-0003-3487-784X (M. Janota); 0000-0002-8273-6059 (C. Kaliszyk)



© 2022 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)