First-Order Interpolation and Grey Areas of Proofs*

Laura Kovács

Vienna University of Technology, Vienna, Austria
laura.kovacs@tuwien.ac.at

Abstract

Interpolation is an important technique in computer aided verification and static analysis of programs. In particular, interpolants extracted from so-called local proofs are used in invariant generation and bounded model checking. An interpolant extracted from such a proof is a boolean combination of formulas occurring in the proof.

In this talk we first describe a technique of generating and optimizing interpolants based on transformations of what we call the "grey area" of local proofs. Local changes in proofs can change the extracted interpolant. Our method can describe properties of extracted interpolants obtained by such proof changes as a pseudo-boolean constraint. By optimizing solutions of this constraint we also improve the extracted interpolants. Unlike many other interpolation techniques, our technique is very general and applies to arbitrary theories. Our approach is implemented in the theorem prover Vampire and evaluated on a large number of benchmarks coming from first-order theorem proving and bounded model checking using logic with equality, uninterpreted functions and linear integer arithmetic. Our experiments demonstrate the power of the new techniques: for example, it is not unusual that our proof transformation gives more than a tenfold reduction in the size of interpolants.

While local proofs admit efficient interpolation algorithms, standard complete proof systems, such as superposition, for theories having the interpolation property are not necessarily complete for local proofs. In this talk we therefore also investigate interpolant extraction from non-local proofs in the superposition calculus and prove a number of general results about interpolant extraction and complexity of extracted interpolants. In particular, we prove that the number of quantifier alternations in first-order interpolants of formulas without quantifier alternations is unbounded. This result has far-reaching consequences for using local proofs as a foundation for interpolating proof systems - any such proof system should deal with formulas of arbitrary quantifier complexity.

1998 ACM Subject Classification F.3.1. Specifying and Verifying and Reasoning about Programs, F.4.1 Mathematical Logic, I.2.3 Deduction and Theorem Proving

Keywords and phrases Theorem proving, interpolation, proof transformations, constraint solving, program analysis

Digital Object Identifier 10.4230/LIPIcs.CSL.2017.3

Category Invited Talk

Acknowledgements. This talk is based on joint work with Andrei Voronkov (University of Manchester, Vienna University of Technology and EasyChair).

[*] This work was supported by the ERC Starting Grant 2014 SYMCAR 639270, the Wallenberg Academy Fellowship 2014 TheProSE, the Swedish VR grant GenPro D0497701 and the FWF projects S11403-N23 and S11409-N23. We also acknowledge support from the FWF project W1255-N23.

26th EACSL Annual Conference on Computer Science Logic (CSL 2017).
Editors: Valentin Goranko and Mads Dam; Article No. 3; pp. 3:1–3:1
Leibniz International Proceedings in Informatics
LIPICS Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany