First-Order Interpolation in the Grey Area of Proofs

Laura Kovács

Abstract. Craig 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. 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. 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 implies that any interpolating proof system should deal with formulas of arbitrary quantifier complexity.

The results presented in this talk are based on joint work with Andrei Voronkov (University of Manchester, Vienna University of Technology and EasyChair).