J Autom Reasoning (2011) 47:369–398
DOI 10.1007/s10817-011-9234-1

Monotonicity Inference for Higher-Order Formulas

Jasmin Christian Blanchette · Alexander Krauss

Received: 30 May 2011 / Accepted: 3 July 2011 / Published online: 13 August 2011

Abstract Formulas are often monotonic in the sense that satisfiability for a given domain of discourse entails satisfiability for all larger domains. Monotonicity is undecidable in general, but we devised three calculi that infer it in many cases for higher-order logic. The third calculus has been implemented in Isabelle's model finder Nitpick, where it is used both to prune the search space and to soundly interpret infinite types with finite sets, leading to dramatic speed and precision improvements.

Keywords Higher-order logic · Model finding · Isabelle/HOL

1 Introduction

Formulas occurring in logical specifications often exhibit monotonicity in the sense that if the formula is satisfiable when the types are interpreted with sets of given (positive) cardinalities, it is still satisfiable when these sets become larger. Consider the following formulas, in which superscripts indicate types and $\simeq$ denotes equality:

1. $\exists x^\alpha\ y.\ x \not\simeq y$
2. $f\ x^\alpha \simeq x \wedge f\ y \not\simeq y$
3. $(\forall x^\alpha.\ f\ x \simeq x) \wedge f\ y \not\simeq y$
4. $\{y^\alpha\} \simeq \{z\}$
5. $\exists x^\alpha\ y.\ x \not\simeq y \wedge \forall z.\ z \simeq x \vee z \simeq y$
6. $\forall x^\alpha\ y.\ x \simeq y$

Research partially supported by the Deutsche Forschungsgemeinschaft (grants Ni 491/11-1 and Ni 491/11-2).

J. C. Blanchette (✉) · A. Krauss
Institut für Informatik, Technische Universität München, Munich, Germany
e-mail: blanchette@in.tum.de

A. Krauss
e-mail: krauss@in.tum.de