J Autom Reasoning (2012) 48:43–105
DOI 10.1007/s10817-010-9194-x

Hybrid

A Definitional Two-Level Approach to Reasoning with Higher-Order Abstract Syntax

Amy Felty · Alberto Momigliano

Received: 19 September 2008 / Accepted: 19 July 2010 / Published online: 7 August 2010
© Springer Science+Business Media B.V. 2010

Abstract Combining higher-order abstract syntax and (co)-induction in a logical framework is well known to be problematic. We describe the theory and the practice of a tool called Hybrid, within Isabelle/HOL and Coq, which aims to address many of these difficulties. It allows object logics to be represented using higher-order abstract syntax, and reasoned about using tactical theorem proving and principles of (co)induction. Moreover, it is definitional, which guarantees consistency within a classical type theory. The idea is to have a de Bruijn representation of λ-terms providing a definitional layer that allows the user to represent object languages using higher-order abstract syntax, while offering tools for reasoning about them at the higher level. In this paper we describe how to use Hybrid in a multi-level reasoning fashion, similar in spirit to other systems such as *Twelf* and *Abella*. By explicitly referencing provability in a middle layer called a specification logic, we solve the problem of reasoning by (co)induction in the presence of non-stratifiable hypothetical judgments, which allow very elegant and succinct specifications of object logic inference rules. We first demonstrate the method on a simple example, formally proving type soundness (subject reduction) for a fragment of a pure functional language, using a minimal intuitionistic logic as the specification logic. We then prove an analogous result for a continuation-machine presentation of the operational

Felty was supported in part by the Natural Sciences and Engineering Research Council of Canada Discovery program. Momigliano was supported by EPSRC grant GR/M98555 and partially by the MRG project (IST-2001-33149), funded by the EC under the FET proactive initiative on Global Computing.

A. Felty (✉)
School of Information Technology and Engineering,
University of Ottawa, Ottawa, ON K1N 6N5, Canada
e-mail: afelty@site.uottawa.ca

A. Momigliano
Laboratory for the Foundations of Computer Science, School of Informatics,
University of Edinburgh, Edinburgh EH9 3JZ, Scotland
e-mail: amomigl1@inf.ed.ac.uk