J Autom Reasoning (2012) 49:241–273
DOI 10.1007/s10817-011-9218-1

# A Two-Level Logic Approach to Reasoning About Computations

**Andrew Gacek · Dale Miller · Gopalan Nadathur**

Received: 1 February 2011 / Accepted: 2 February 2011 / Published online: 23 February 2011


**Abstract** Relational descriptions have been used in formalizing diverse computational notions, including, for example, operational semantics, typing, and acceptance by non-deterministic machines. We therefore propose a (restricted) logical theory over relations as a language for specifying such notions. Our *specification logic* is further characterized by an ability to explicitly treat binding in object languages. Once such a logic is fixed, a natural next question is how we might prove theorems about specifications written in it. We propose to use a second logic, called a *reasoning logic*, for this purpose. A satisfactory reasoning logic should be able to completely encode the specification logic. Associated with the specification logic are various notions of binding: for quantifiers within formulas, for eigenvariables within sequents, and for abstractions within terms. To provide a natural treatment of these aspects, the reasoning logic must encode binding structures as well as their associated notions of scope, free and bound variables, and capture-avoiding substitution. Further, to support arguments about provability, the reasoning logic should possess strong mechanisms for constructing proofs by induction and co-induction. We provide these capabilities here by using a logic called $\mathcal{G}$ which represents relations over $\lambda$-terms via definitions of atomic judgments, contains inference rules for induction and co-induction, and includes a special *generic* quantifier. We show how provability in the specification logic can be transparently encoded in $\mathcal{G}$. We also describe an interactive

A. Gacek · D. Miller (✉)
INRIA Saclay—Île-de-France & LIX/École Polytechnique, Palaiseau, France
e-mail: dale.miller@inria.fr

A. Gacek
e-mail: gacek@lix.polytechnique.fr

G. Nadathur
Department of Computer Science and Engineering, University of Minnesota,
4-192 EE/CS Building, 200 Union Street SE, Minneapolis, MN 55455, USA
e-mail: gopalan@cs.umn.edu