Program Verification using Reachability Logic

Grigore Roşu[1], Andrei Ştefănescu[1], and Ştefan Ciobâcă[2]

[1] University of Illinois at Urbana-Champaign, USA
grosu@illinois.edu, stefane1@illinois.edu
[2] University "Alexandru Ioan Cuza" of Iaşi, Romania
stefan.ciobaca@info.uaic.ro

Abstract. Matching logic is a logic for reasoning about program configuration properties in a language-parametric manner. On top of matching logic we define reachability logic and equivalence logic. Reachability logic enables reasoning about the correctness of both deterministic programs (one-path reachability logic) and non-deterministic programs (all-path reachability logic). Equivalence logic enables reasoning about program equivalence. We introduce K, a semantics framework which has been used to define the operational semantics of real-world languages such as C, Java, and JavaScript. We show how the logics above are integrated in K. In particular, we show how the semantics of C, Java, and JavaScript yield automatic program verifiers for the respective languages. The verifiers can check the full functional correctness of challenging heap manipulation programs implementing the same data-structures in these languages (e.g. AVL trees). We also show how to reason about program equivalence using semantics defined in K.