Software Verification "Across the Stack"

Alexander J. Summers

ETH Zürich
Zürich, Switzerland
alexander.summers@inf.ethz.ch

Abstract

Producing reliable programs has always been tough, and the complexity and variety of programming tasks just keeps on growing. Fortunately, the growth of computing power has also enabled substantial advances in automated reasoning, particularly the development of SMT solvers and automatic theorem provers. In turn, this has resulted in new research directions for program correctness, with the aim of producing tools which can verify complex properties of software automatically.

Developing useful verification techniques requires balancing a number of competing factors. We want to be as expressive as possible in the program properties we can support – if we can write it down, we'd like to be able to prove it. But to progress beyond pen-and-paper efforts, we also need to tailor our approaches such that they can be implemented or encoded by tools, ideally with both precise and efficient results. To make things harder still, if we hope to produce tools which everyday programmers can benefit from, we also need techniques that require manageable interaction from a user, and give understandable feedback.

In this talk, I'll describe some of the fun experiences I've had working on these kinds of problems, from the design of front-end program logics and reasoning techniques to the development of underlying implementation technology, and the tricky encoding challenges that show up in between.

1998 ACM Subject Classification F.3.1 Specifying and Verifying and Reasoning about Programs

Keywords and phrases software verification, program logic, automatic verifier, program correctness, SMT solvers

Digital Object Identifier 10.4230/LIPIcs.ECOOP.2015.3

Category Invited Talk

29th European Conference on Object-Oriented Programming (ECOOP'15).
Editor: John Tang Boyland; pp. 3–3
Leibniz International Proceedings in Informatics
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany