Compositional Compiler Verification for a Multi-Language World*

Amal Ahmed

Northeastern University, Boston, USA
`amal@ccs.neu.edu`

Abstract

Verified compilers are typically proved correct under severe restrictions on what the compiler's output may be linked with, from no linking at all to linking only with code compiled from the same source language. Such assumptions contradict the reality of how we use these compilers since most software systems today are comprised of components written in different languages compiled by different compilers to a common target, as well as low-level libraries that may be handwritten in the target language.

The key challenge in verifying compilers for today's world of multi-language software is how to formally state a compiler correctness theorem that is compositional along two dimensions. First, the theorem must guarantee correct compilation of components while allowing compiled code to be composed (linked) with target-language components of arbitrary provenance, including those compiled from other languages. Second, the theorem must support verification of multi-pass compilers by composing correctness proofs for individual passes. In this talk, I will describe a methodology for verifying compositional compiler correctness for a higher-order typed language and discuss the challenges that lie ahead [1, 2]. I will argue that compositional compiler correctness is, in essence, a language interoperability problem: for viable solutions in the long term, high-level languages must be equipped with *principled foreign-function interfaces* that specify safe interoperability between high-level and low-level components, and between more precisely and less precisely typed code.

Category Invited Talk

References

1 Amal Ahmed. Verified compilers for a multi-language world. In *1st Summit on Advances in Programming Languages (SNAPL 2015)*, volume 32 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 15–31, 2015.
2 James T. Perconti and Amal Ahmed. Verifying an open compiler using multi-language semantics. In *Programming Languages and Systems - 23rd European Symposium on Programming, ESOP 2014*, pages 128–148, April 2014.

1st International Conference on Formal Structures for Computation and Deduction (FSCD 2016).
Editors: Delia Kesner and Brigitte Pientka; Article No. 1; pp. 1:1–1:1

Leibniz International Proceedings in Informatics
LIPIcs Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany