TECHNISCHE
UNIVERSITÄT
DARMSTADT

Machine Proving the Soundness of Averroes

Research Assistant

April 2015

Ali and Lhoták [2] present and evaluate Averroes, a tool that generates a placeholder library that over-approximates the possible behaviour of an original library. Any existing whole-program call graph construction framework can use the placeholder library as a replacement for the actual libraries to efficiently construct a sound and precise application call graph. Ali [1] provides a formal paper-and-pencil proof for the soundness of Averroes. The proof is based on Featherweight Java [4], a core calculus for the Java language.

The main goal of the correctness proof is to show that if in the application code of the FJ program, method m calls m', then there is a trace for the transformed Averroes program in which m also calls m'. However, the trace of the Averroes program cannot contain code from the library methods of the FJ program because the Averroes program does not contain the bodies of those methods. Therefore, Averroes replaces the unanalyzed library code with the special expression `LIB` that simulates the side effects the original library code would have on the application code.

The main task of this project is to prove the soundness of Averroes using Twelf [5], a language used to specify, implement, and prove properties of deductive systems such as programming languages and logics. Alternatively, you could use Coq [3], a formal proof management system.

Ideal candidates have experience with static analysis, in particular for Java. Prior knowledge of formal proofs, programming language theory, and using Twelf/Coq is helpful but not necessary.

Interested? Please contact Karim Ali at karim.ali@cased.de

References

[1] Karim Ali. "The Separate Compilation Assumption". PhD thesis. University of Waterloo, 2014.

[2] Karim Ali and Ondrej Lhoták. "Averroes: Whole-Program Analysis without the Whole Program". In: *ECOOP*. 2013, pp. 378–400.

[3] The Coq Proof Assistant. `https://coq.inria.fr`. Apr. 2015.

[4] Atsushi Igarashi, Benjamin C. Pierce, and Philip Wadler. "Featherweight Java: a minimal core calculus for Java and GJ". In: *TOPLAS* 23.3 (2001), pp. 396–450.

[5] The Twelf Project. `http://twelf.org/wiki/Main_Page`. Apr. 2015.