Specification and Proof of Programs with Frama-C

SAC 2013 Tutorial Abstract

Nikolai Kosmatov, Virgile Prevosto, and Julien Signoles

CEA, LIST, Software Safety Laboratory, PC 174, 91191 Gif-sur-Yvette France
firstname.lastname@cea.fr
Phone: + 33 1 69 08 71 83, Fax: + 33 1 69 08 83 95

1 Abstract

Despite the spectacular progress made by the developers of formal verification tools, their usage remains basically reserved for the most critical software. More and more engineers and researchers today are interested in such tools in order to integrate them into their everyday work. This half-day tutorial proposes a practical introduction during which the participants will write C program specifications, observe the proof results, analyze proof failures and fix them. Participants will be taught how to write a specification for a C program, in the form of function contracts, and easily prove it with an automatic tool in FRAMA-C[1], a freely available software verification toolset. Those who will have FRAMA-C and JESSIE installed (recommended, e.g. from ready-to-install packages `frama-c, why, alt-ergo` under Linux) will also run automatic proof of programs on their computer. Program specifications will be written in the specification language ACSL[2] similar to other specification languages like JML that some participants may know. ACSL syntax is intentionally close to C and can be easily learned on-the-fly.

The tutorial is aimed mainly at software engineering students and professionals who will learn more about the state of the art in automated software verification and how it could help them in their career in software development or validation. Using freely available tools FRAMA-C and JESSIE will allow them to quickly install and try the tools. Software engineering lecturers will also be interested in how a tool such as FRAMA-C can help in teaching software verification.

The only necessary background is some familiarity with the C language.

2 About the Presenters

The presenters are researchers at CEA LIST. Nikolai Kosmatov obtained Ph.D. degree in Mathematics at Saint-Petersburg State University in 2000 and a M.Sc. in Computer Science in Besançon in 2003. His research interests focus on software verification and test generation. He developed the `PathCrawler-online.com` web service. Nikolai has taught various courses in Mathematics and Computer Science at Saint-Petersburg State University, the University of Orléans, the University of Besançon, the University

[1] Cuoq, P., Kirchner, F., Kosmatov, N., Prevosto, V., Signoles, J., Yakobowski, B.: Frama-C: A software analysis perspective. In: SEFM 2012. URL: `http://frama-c.com/`

[2] `http://frama-c.com/acsl.html`

Pierre and Marie Curie in Paris, the RWTH Aachen University in Germany etc. He gave several theoretical courses and exercise sessions on proof of programs in 2009-2012.

Julien Signoles got his PhD from University of Paris 11 in 2006. His research focused on extensions of the ML language, software security, runtime assertion checking and various applications of static analysis. One of the main developers of FRAMA-C, he gave several university and training courses on FRAMA-C, on the existing FRAMA-C analyzers and development of new plugins. In particular, he taught proof of programs in 2010-2012. He participates in many national and international projects related to FRAMA-C.

Virgile Prevosto is a researcher at CEA LIST. He got a PhD in Computer Science from University of Paris 6 in 2003. His research interests include mainly formal methods and static analysis of programs. He is one of the developers of FRAMA-C, and was among the organizers of FRAMA-C training sessions in 2009 (Saclay, France) and 2010 (Berlin, Germany, as part of the Device-Soft project). He also presented FRAMA-C at the Coq Summer School in Beijing in 2009 and during the Static Analysis course he's giving at ENSIIE Évry since 2009/2010.