PhD Proposal
Verification of relational properties on C programs

Keywords: Formal methods, Program specification and verification

Context

Complex software is nowadays pervasive, including in critical domains where a malfunction might have severe consequences (energy, transportation, health care, defense, ...). It is thus crucial to provide strong safety and security guarantees on such code. This in turn requires powerful tools, capable of expressing and verifying a very broad range of properties about programs.

At CEA LIST institute (`http://www-list.cea.fr/`), located in the south of Paris, the Software Safety and Security lab (LSL) is developing such tools, including in particular the Frama-C framework (`http://frama-c.com`), dedicated to the analysis of C programs. Frama-C proposes among other things a deductive verification plug-in based on Hoare logic, that can prove that C functions are correct with respect to a formal specification written in the ACSL language. The main ingredient of ACSL is the notion of function contract, in which one can specify the pre-condition indicating what input the function expects, and the post-condition, indicating the intended behavior of the function. Similarly, the LOGIMAS team at École Centrale de Paris (`http://centralesupelec.fr`) performs research on formal methods for analyzing and verifying systems.

Objectives

Not all properties of interest can be easily described as function contracts. For instance, one can be interested in a property related to the execution of several functions, or in comparing the results of various calls to the same function. Function contracts and existing deductive verification techniques are not well adapted to this context. The topic of this thesis will be to propose new verification techniques for such relational properties.

Starting from existing case studies, a first step will be to characterize precisely the class of properties that have to be handled. Then, extensions to existing deductive verification techniques will be devised in order to accomodate for such properties. Possible solutions include the generation of new functions simulating the calls involved, together with a contract indicating the expected properties, or the generation of several contracts related through a set of model variables. Such extension will then be implemented on top of the existing Frama-C plugin. Similarly, the ACSL language will be extended to let users specify such properties. Finally, the proposed method will be validated on the case studies.

Applying

Profile

- Master in Computer Science,
- Specialization in Formal Methods and/or Programming Languages
- Experience in *OCaml* development
- Some knowledge of C would be appreciated

Schedule Position is available immediately and will remain opened until it is filled or before the end of 2016 at the latest. The grant will last 3 years.

Location CEA LIST, Nano-Innov, on the Université Paris-Saclay campus, France (see on OpenStreetMap)

Contact Nikolai Kosmatov (nikolay.kosmatov@cea.fr), Virgile Prevosto (virgile.prevosto@cea.fr), and Pascale Le Gall (pascale.legall@ecp.fr)