Master's Thesis Subject

Temporal Properties Verification

Keywords : program verification, temporal properties

Context

CEA LIST is a French technological research institute with a focus on smart and complex systems. Its research programs are conducted in coordination with major industrial actors from nuclear, automotive, aeronautics, defense and medical sector, in order to design and develop innovating solutions tailored to their needs. Within CEA LIST, the Software Security Laboratory, based in Palaiseau (in the Paris area), develops tools for the verification and validation of software and mixed hardware/software systems. Frama-C (`http://frama-c.com`) is a software platform written in *OCaml*, dedicated to the analysis of C programs. The thesis will take place in the R&D team who is developing Frama-C.

Objectives

Aoraï is a Frama-C plugin aiming at the verification of properties on the sequences of functions calls that a program is allowed to perform during an execution. Such properties are given as an automaton. The main objective of the thesis will be to propose new formalisms for describing these properties.

More precisely, Frama-C itself uses the ACSL specification language that allows to give each function of a C program the contract (pre- and post-conditions) that it is supposed to meet. Aoraï's automata allows to specify more global properties. For that, Aoraï translates the automaton into ACSL contracts, that can then be verified by the analysis plug-ins of Frama-C, such as Value and WP. As of now, it is also possible to use an LTL formula as input for Aoraï, which uses for that the output of the `ltl2ba` tool. This approach has some limitations, however, and one of the goal of the thesis will be to develop a tool that would be more tightly coupled to Aoraï, and that would be able to take into account some common LTL extensions. In addition, this work should also allows to propose extensions to Aoraï's automaton language itself, in order to facilitate the description of some call sequences. Other directions might also be relevant, such as letting Aoraï handle new classes of properties (in particular liveness properties).

Applying

Skills

- Good knowledge of *OCaml*
- Interest for static analysis of real-world programs
- Ability to work within a team
- Some knowledge of C programming

Conditions : paid internship ; housing stipend possible (under conditions) ; access to CEA's shuttle service for commuting.

Contact : Virgile Prevosto (virgile.prevosto@cea.fr) - Sébastien Bardin (sebastien.bardin@cea.fr)

The instruction of the administrative paperwork can take up to 2 or 3 months, you are thus encouraged to apply as soon as possible.