Research proposal: Decision procedures for separation logics

Location: Laboratoire Spécification et Vérification
Ecole Normale Supérieure Paris-Saclay

Advisor: Stéphane Demri (LSV, CNRS, ENS Paris-Saclay)
demri@lsv.fr

Separation logic. Separation logic has been introduced as an extension of Hoare logic [Hoa69] to verify programs with mutable data structures [IO01, Rey02]. A major feature is to be able to reason locally in a modular way, which can be performed thanks to the separating conjunction that allows to state properties in disjoint parts of the memory. Moreover, the adjunct implication asserts that whenever a fresh heap satisfies a property, its composition with the current heap satisfies another property. This is particularly useful when a piece of code mutates memory locally, and we want to state some property of the entire memory (such as the preservation of data structure invariants). The development of proof methods for separation logic (and its fragments and variants) is nowadays a very active area, see e.g. [GM10, BV14, DGLWM14]. There are also a lot of activities to develop verification methods with decision procedures for fragments of practical use, see e.g. [CHO+11]. Many decision procedures have been designed for fragments of separation logics or abstract variants, from analytic methods [GM10] to translation to theories handled by SMT solvers [PWZ13], passing via graph-based algorithms [HIOPT13]. The framework of satisfiability modulo theories (SMT) [BT] remains probably the most promising one to develop decision procedures dedicated to reasoning tasks for separation logics, see e.g [PWZ13]. See a survey on the logical aspects of separation logics in [DD15b] or the lecture notes [DD15a].

The objectives of the PhD thesis are to provide a complete map for the main decision problems for fragments or extensions of separation logics.

References


