Research Internship – Master M2 (2016/2017)

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

Title : Decision procedures for separation logics

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 [HIOP13]. 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].

Objectives of the research internship

The main objectives of the internship consist in determining new decidable fragments of first-order separation logics, possibly with a complexity characterisation.

(1) To become familiar with tractable [resp. decidable] fragments of separation logic and with existing logical theories for deciding separation logic. See e.g. [DD15b, DD15a].

(2) To design maximal decidable fragments for the modal logic for heaps presented in [DD15b, Section 3.4.2].

(3) Based on (2), design new fragments of separation logics with inductive predicates such as reachability.

This research internship may be pursued as a PhD thesis, whose subject may vary according to the candidate's research interests.

Related courses at MPRI:

For your information, the following MPRI courses are related to this research internship. Students from other master programmes are welcomed to apply too.

- Course 2.5.1 *Automated Deduction*
- Course 2.9.1 *Mathematical foundations of the theory of infinite transition systems*
- Course 2.9.2 *Algorithmic verification of programs*
- Course 2.36.1 *Proofs of programs*

References

[BT] C. Barrett and C. Tinelli. Satisfiability Modulo Theories.

[BV14] J. Brotherston and J. Villard. Parametric completeness for separation theories. In *POPL'14*, pages 453–464. ACM, 2014.

[CHO+11] B. Cook, C. Haase, J. Ouaknine, M. Parkinson, and J. Worrell. Tractable reasoning in a fragment of separation logic. In *CONCUR'11*, volume 6901 of *Lecture Notes in Computer Science*, pages 235–249. Springer, 2011.

[DD14] S. Demri and M. Deters. Expressive completeness of separation logic with two variables and no separating conjunction. In *LICS'14*, page 37. ACM, 2014.

[DD15a] S. Demri and M. Deters. Logical investigations on separation logics. Lecture Notes, European Summer School on Logic, Language and Information (ESSLLI'15), August 2015.

[DD15b] S. Demri and M. Deters. Separation logics and modalities: A survey. *Journal of Applied Non-Classical Logics*, 25(1):50–99, 2015.

[DGLWM14] S. Demri, D. Galmiche, D. Larchey-Wendling, and D. Mery. Separation logic with one quantified variable. In *CSR'14*, volume 8476 of *Lecture Notes in Computer Science*, pages 125–138. Springer, 2014.

[GM10] D. Galmiche and D. Méry. Tableaux and resource graphs for separation logic. *Journal of Logic and Computation*, 20(1):189–231, 2010.

[HIOP13] C. Haase, S. Ishtiaq, J. Ouaknine, and M. Parkinson. Seloger: A Tool for Graph-Based Reasoning in Separation Logic. In *CAV'13*, volume 8044 of *Lecture Notes in Computer Science*, pages 790–795. Springer, 2013.

[Hoa69] C.A.R. Hoare. An axiomatic basis for computer programming. *Communications of the ACM*, 12(10):576–580, 1969.

[IO01] S. Ishtiaq and P. O'Hearn. BI as an assertion language for mutable data structures. In *POPL'01*, pages 14–26. ACM, 2001.

[PWZ13] R. Piskac, Th. Wies, and D. Zufferey. Automating separation logic using SMT. In *CAV'13*, volume 8044 of *Lecture Notes in Computer Science*, pages 773–789. Springer, 2013.

[Rey02] J.C. Reynolds. Separation logic: a logic for shared mutable data structures. In *LICS'02*, pages 55–74. IEEE, 2002.