
Decision Procedures for Separation Logic

Alessio Mansutti*¹

¹Ecole Normale Supérieure Paris-Saclay – CNRS : UMR8643 – France

Résumé

Separation logic [1] is a well-known assertion logic providing a scalable solution for Hoare-style verification of imperative, heap-manipulating programs. To achieve scalability, separation logic relies in two spatial connectives to represent memory regions: the separating conjunction (\star) and the separating implication (\multimap).

To achieve automation, the underlying Hoare-style proof system requires these tools to check for the classical decision problems of satisfiability and entailment. Hence, the development of proof methods for separation logic (and its fragments and variants) is nowadays a very active area.

By showing a result similar to the Gaifman's Theorem of first-order logic, we were able to design [2] an extension of propositional separation logic that is still PSPACE-complete and subsumes various other extensions and fragments of separation logic that were known to be PSPACE-complete.

Moreover, again relying on our "Gaifman's Theorem", we developed [3] the first Hilbert-style axiomatisation of separation logic (and similar logics [4]).

J.C. Reynolds. Separation logic: a logic for shared mutable data structures. In LICS'02

A. Mansutti. Extending propositional separation logic for robustness properties. In FSTTCS'18

S. Demri, É. Lozes, and A. Mansutti. Internal calculi for Separation Logics (submitted).

S. Demri, R. Fervari, and A. Mansutti. Axiomatising logics with separating conjunction and modalities. In JELIA'19

*Intervenant