On Temporal and Separation Logics

Stéphane Demri
LSV, CNRS, ENS Paris-Saclay, Université Paris-Saclay, France
demri@lsv.fr
https://orcid.org/0000-0002-3493-2610

Abstract

There exist many success stories about the introduction of logics designed for the formal verification of computer systems. Obviously, the introduction of temporal logics to computer science has been a major step in the development of model-checking techniques. More recently, separation logics extend Hoare logic for reasoning about programs with dynamic data structures, leading to many contributions on theory, tools and applications. In this talk, we illustrate how several features of separation logics, for instance the key concept of separation, are related to similar notions in temporal logics. We provide formal correspondences (when possible) and present an overview of related works from the literature. This is also the opportunity to present bridges between well-known temporal logics and more recent separation logics.

2012 ACM Subject Classification Theory of computation → Modal and temporal logics, Theory of computation → Separation logic

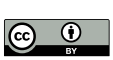
Keywords and phrases separation logics, temporal logics, expressive power

Digital Object Identifier 10.4230/LIPIcs.TIME.2018.1

Category Invited Paper

1 Separation Logics

Separation logic has been introduced as an extension of Hoare logic [24] to verify programs with mutable data structures [28, 39, 41]. 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 one to state properties in disjoint parts of the memory. The companion connective $-\!\!*$ corresponding to separating implication (a.k.a the magic wand) happens to be also helpful for program verification. So, the study of separation logics is currently very active, with works ranging from foundations to formal verification of programs. For instance, since the evidence that the method is scalable [3, 46], many tools supporting separation logic as an assertion language have been developped [3, 20, 46, 9, 10, 21]. Moreover, many variants of separation logics have been considered, leading to many interesting problems related to decidability/complexity of reasoning tasks, expressive power, relationships with other logical formalisms, proof systems, etc. It is not reasonable to enumerate herein all the existing variants and research directions. By way of example, decidability results about separation logic with general inductive predicates can be found in [27, 7]: notably in [7], the satisfiability problem for the symbolic heap fragment [2] with general inductively defined predicates is shown decidable. Furthermore, as already advocated in [8, 43, 42, 26, 37], dealing with the separating implication $-\!\!*$ is a desirable feature for program verification and several semi-automated or automated verification tools support it in some way, see e.g. [43, 42, 37], going beyond separation logics built over the symbolic heap fragment. Nevertheless, the combination of the magic wand $-\!\!*$ and the list segment predicate `ls` (a simple inductive



predicate) may lead to undecidability [19]. First-order separation logics have been also been considered in [2, 6, 16]. So, the first part of the talk is dedicated to basics on separation logics.

2 Relating Modal/Temporal Logics with Separation Logics

As the first versions of separation logic can be understood as a concretisation of the logic of bunched implication BI [38, 28, 40], it is not surprising that separation logics can be related to other logics, see also [15]. For instance, the concept of separation can be found in interval temporal logics (see e.g. [44, 45, 25, 35]), in graph logics (see e.g. [14, 1]), or in other formalisms [23, 22, 4]. Besides, as for temporal logics, the relationships between separation logic, and first-order or second-order logics have been the source of many characterizations and works. This is particularly true since the separating connectives are second-order in nature, see e.g. [32, 29, 11, 6, 17]. Moreover, separation logics can be shown to have close relationships with hybrid modal logics (see e.g. [8, 18]), with relevance logics (see e.g. [13, 12]) or with logics equipped with associative binary modalities (see e.g. [30, 4]).

In this talk, we illustrate how several features of separation logics are related to similar notions in temporal logics. We provide formal correspondences (when possible) and present an overview of related works from the literature. It is worth noting that temporal logics and separation logics can be related in many ways. At the semantical level, memory states from separation logics can be understand as tree-like models or as linear structures, see e.g. [16, 18] leading to explicit relationships with temporal logics on similar structures. Nevertheless, the correspondence is not always immediate. At the level of the operators, separation is a key concept that has been already introduced in interval temporal logic PITL [36]. Relationships between interval temporal logics and separation logics can be formally stated, see e.g. [16, 18, 34] and we shall show how complexity results about separation logics can be concluded. Typically, the TOWER-hardness of the satisfiability problem for first-order separation logics restricted to the separation conjunction and to two individual variables with one record field, can be established by reduction the satisfiability problem for PITL [16].

Similarly to the links between separation logics are (weak) second-order logics, ongoing investigations[1] relating separation logics with quantified temporal logics [31] shall be also evoked. So, apart from the analogies between temporal logics and separation logics and cross-fertilising results, we also motivate the introduction of formalisms that combine modal/temporal logics and separation logics, see e.g. [5, 33, 18], in order to reason about resources in a temporal framework.

So, the talk is the opportunity to present bridges between well-known temporal logics and more recent separation logics.

References

1 T. Antonopoulos and A. Dawar. Separating graph logic from MSO. In *FOSSACS'09*, volume 5504 of *Lecture Notes in Computer Science*, pages 63–77. Springer, 2009.

2 J. Berdine, C. Calcagno, and P. O'Hearn. A decidable fragment of separation logic. In *FST&TCS'04*, volume 3328 of *Lecture Notes in Computer Science*, pages 97–109. Springer, 2004.

[1] Bartosz Bednarczyk's internship at LSV (2018) is dedicated to related issues.

3 J. Berdine, C. Calcagno, and P. O'Hearn. Smallfoot: Modular automatic assertion checking with separation logic. In *FMCO'05*, volume 4111 of *Lecture Notes in Computer Science*, pages 115–137. Springer, 2005.

4 J. Boudou. Decidable logics with associative binary modalities. In *CSL'17*, volume 82 of *LIPIcs*, pages 1–15. Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik, 2017.

5 R. Brochenin, S. Demri, and E. Lozes. Reasoning about sequences of memory states. *Annals of Pure and Applied Logic*, 161(3):305–323, 2009.

6 R. Brochenin, S. Demri, and E. Lozes. On the almighty wand. *Information and Computation*, 211:106–137, 2012.

7 J. Brotherston, C. Fuhs, N. Gorogiannis, and J. Navarro Perez. A decision procedure for satisfiability in separation logic with inductive predicates. In *CSL-LICS'14*, 2014.

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

9 C. Calcagno and D. Distefano. Infer: An automatic program verifier for memory safety of C programs. In *NASA Formal Methods*, volume 6617 of *Lecture Notes in Computer Science*, pages 459–465. Springer, 2011.

10 C. Calcagno, D. Distefano, P.W. O'Hearn, and H. Yang. Compositional shape analysis by means of bi-abduction. *Journal of the ACM*, 58(6):26:1–26:66, 2011.

11 C. Calcagno, Ph. Gardner, and M. Hague. From separation logic to first-order logic. In *FOSSACS'05*, volume 3441 of *Lecture Notes in Computer Science*, pages 395–409. Springer, 2005.

12 J. Spring D. Pym and P. O'Hearn. Why separation logic works. Manuscript, 2017.

13 M. Dams. *Relevance logic and concurrent composition*. PhD thesis, University of Edinburgh, 1989.

14 A. Dawar, Ph. Gardner, and G. Ghelli. Expressiveness and complexity of graph logic. *Information and Computation*, 205(3):263–310, 2007.

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

16 S. Demri and M. Deters. Two-variable separation logic and its inner circle. *ACM Transactions on Computational Logics*, 2(16), 2015.

17 S. Demri and M. Deters. Expressive completeness of separation logic with two variables and no separating conjunction. *ACM Transactions on Computational Logics*, 17(2):12, 2016.

18 S. Demri and R. Fervari. On the complexity of modal separation logics. In *AiML'18*, 2018. to appear.

19 S. Demri, E. Lozes, and A. Mansutti. The effects of adding reachability predicates in propositional separation logic. In *FOSSACS'18*, volume 10803 of *Lecture Notes in Computer Science*, pages 476–493. Springer, 2018.

20 D. Distefano, P. O'Hearn, and H. Yang. A local shape analysis based on separation logic. In *TACAS'06*, volume 3920 of *Lecture Notes in Computer Science*, pages 287–302. Springer, 2006.

21 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.

22 L. Hella, K. Luosto, K. Sano, and J. Virtema. The expressive power of modal dependence logic. In *AIML'14*, pages 294–312. College Publications, 2014.

23 A. Herzig. A simple separation logic. In *WoLLIC'13*, volume 8071 of *Lecture Notes in Computer Science*, pages 168–178. Springer, 2013.

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

25 I. Hodkinson, A. Montanari, and G. Sciavicco. Non-finite axiomatizability and undecidability of interval temporal logics with C, D, and T. In *CSL'08*, volume 5213 of *Lecture Notes in Computer Science*, pages 308–322. Springer, 2008.

26 Z. Hou, R. Goré, and A. Tiu. Automated theorem proving for assertions in separation logic with all connectives. In *CADE'15*, volume 9195 of *Lecture Notes in Computer Science*, pages 501–516. Springer, 2015.

27 R. Iosif, A. Rogalewicz, and J. Simacek. The tree width of separation logic with recursive definitions. In *CADE'13*, volume 7898 of *Lecture Notes in Computer Science*, pages 21–38. Springer, 2013.

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

29 V. Kuncak and M. Rinard. On spatial conjunction as second-order logic. Technical Report MIT–CSAIL–TR–2004–067, MIT CSAIL, October 2004.

30 A. Kurucz, I. Németi, I. Sain, and A. Simon. Decidable and undecidable logics with a binary modality. *Journal of Logic, Language, and Information*, 4:191–206, 1995.

31 F. Laroussinie and N. Markey. Quantified CTL: Expressiveness and complexity. *Logical Methods in Computer Science*, 10(4:17), 2014.

32 E. Lozes. *Expressivité des Logiques Spatiales*. Phd thesis, ENS Lyon, 2004.

33 Xu Lu, Cong Tian, and Zhenhua Duan. Temporalising separation logic for planning with search control knowledge. In *IJCAI'17*, pages 1167–1173, 2017.

34 A. Mansutti. Extending propositional separation logic for robustness properties, July 2018. Manuscript.

35 D. Della Monica, V. Goranko, A. Montanari, and G. Sciavicco. Interval temporal logics: a journey. *Bulletin of the EATCS*, 105:73–99, 2011.

36 B. Moszkowski. Reasoning about digital circuits. Technical Report STAN-CS-83-970, Dept. of Computer Science, Stanford University, Stanford, CA, 1983.

37 P. Müller, M. Schwerhoff, and A.J. Summers. Viper: A verification infrastructure for permission-based reasoning. In *VMCAI'16*, volume 9583 of *Lecture Notes in Computer Science*, pages 41–62. Springer, 2016.

38 P. O'Hearn and D. Pym. The logic of bunched implications. *Bulletin of Symbolic Logic*, 5(2):215–244, 1999.

39 P.W. O'Hearn, J.C. Reynolds, and H. Yang. Local reasoning about programs that alter data structures. In *CSL'01*, volume 2142 of *Lecture Notes in Computer Science*, pages 1–19. Springer, 2001.

40 D. Pym. *The Semantics and Proof Theory of the Logic of Bunched Implications*, volume 26 of *Applied Logic*. Kluwer Academic Publishers, 2002.

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

42 M. Schwerhoff and A. Summers. Lightweight support for magic wands in an automatic verifier. In *ECOOP'15*, pages 999–1023. Leibniz-Zentrum für Informatik, LIPICS, 2015.

43 A. Thakur, J. Breck, and T. Reps. Satisfiability modulo abstraction for separation logic with linked lists. In *SPIN'14*, pages 58–67. ACM, 2014.

44 Y. Venema. Expressiveness and completeness of an interval tense logic. *NDJFL*, 31(4):529–547, 1990.

45 Y. Venema. A modal logic for chopping intervals. *Journal of Logic and Computation*, 1(4):453–476, 1991.

46 H. Yang, O. Lee, J. Berdine, C. Calcagno, B. Cook, D. Distefano, and P. O'Hearn. Scalable shape analysis for systems code. In *CAV'08*, volume 5123 of *Lecture Notes in Computer Science*, pages 385–398. Springer, 2008.