



HAL
open science

On Temporal and Separation Logics

Stephane Demri

► **To cite this version:**

Stephane Demri. On Temporal and Separation Logics. 25th International Symposium on Temporal Representation and Reasoning, TIME 2018, Warsaw, Poland., Oct 2018, Varsovie, Poland. pp.1:1–1:4, 10.4230/LIPIcs.TIME.2018.1 . hal-02366656

HAL Id: hal-02366656

<https://hal.science/hal-02366656v1>

Submitted on 16 Nov 2019

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

1 On Temporal and Separation Logics

2 **Stéphane Demri**

3 LSV, CNRS, ENS Paris-Saclay, Université Paris-Saclay, France

4 demri@lsv.fr

5  <https://orcid.org/0000-0002-3493-2610>

6 — Abstract —

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

16 **2012 ACM Subject Classification** Theory of Computation, Logic, Modal and Temporal Logics,
17 Separation Logic

18 **Keywords and phrases** separation logics, temporal logics, expressive power

19 **Digital Object Identifier** 10.4230/LIPIcs.TIME.2018.1

20 **Category** invited paper

21 **1 Separation Logics**

22 Separation logic has been introduced as an extension of Hoare logic [24] to verify programs
23 with mutable data structures [28, 39, 41]. A major feature is to be able to reason locally
24 in a modular way, which can be performed thanks to the separating conjunction $*$ that
25 allows one to state properties in disjoint parts of the memory. The companion connective -*
26 corresponding to separating implication (a.k.a the magic wand) happens to be also helpful
27 for program verification. So, the study of separation logics is currently very active, with
28 works ranging from foundations to formal verification of programs. For instance, since the
29 evidence that the method is scalable [3, 46], many tools supporting separation logic as an
30 assertion language have been developed [3, 20, 46, 9, 10, 21]. Moreover, many variants
31 of separation logics have been considered, leading to many interesting problems related to
32 decidability/complexity of reasoning tasks, expressive power, relationships with other logical
33 formalisms, proof systems, etc. It is not reasonable to enumerate herein all the existing
34 variants and research directions. By way of example, decidability results about separation
35 logic with general inductive predicates can be found in [27, 7]: notably in [7], the satisfiability
36 problem for the symbolic heap fragment [2] with general inductively defined predicates is
37 shown decidable. Furthermore, as already advocated in [8, 43, 42, 26, 37], dealing with
38 the separating implication -* is a desirable feature for program verification and several
39 semi-automated or automated verification tools support it in some way, see e.g. [43, 42, 37],
40 going beyond separation logics built over the symbolic heap fragment. Nevertheless, the
41 combination of the magic wand -* and the list segment predicate ls (a simple inductive
42 predicate) may lead to undecidability [19]. First-order separation logics have been also been



© S. Demri;

licensed under Creative Commons License CC-BY

25th International Symposium on Temporal Representation and Reasoning (TIME 2018).

Editors: Natasha Alechina, Kjetil Nørsvåg and Wojciech Penczek; Article No. 1; pp. 1:1–1:4

Leibniz International Proceedings in Informatics



LIPICs Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

43 considered in [2, 6, 16]. So, the first part of the talk is dedicated to basics on separation
 44 logics.

45 **2 Relating Modal/Temporal Logics with Separation Logics.**

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

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

69 Similarly to the links between separation logics and (weak) second-order logics, ongoing
 70 investigations¹ relating separation logics with quantified temporal logics [31] shall be
 71 also evoked. So, apart from the analogies between temporal logics and separation logics
 72 and cross-fertilising results, we also motivate the introduction of formalisms that combine
 73 modal/temporal logics and separation logics, see e.g. [5, 33, 18], in order to reason about
 74 resources in a temporal framework.

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

77 **References**

- 78 **1** T. Antonopoulos and A. Dawar. Separating graph logic from MSO. In *FOSSACS'09*,
 79 volume 5504 of *Lecture Notes in Computer Science*, pages 63–77. Springer, 2009.
- 80 **2** J. Berdine, C. Calcagno, and P. O'Hearn. A decidable fragment of separation logic. In
 81 *FST&TCS'04*, volume 3328 of *Lecture Notes in Computer Science*, pages 97–109. Springer,
 82 2004.
- 83 **3** J. Berdine, C. Calcagno, and P. O'Hearn. Smallfoot: Modular automatic assertion checking
 84 with separation logic. In *FMC0'05*, volume 4111 of *Lecture Notes in Computer Science*,
 85 pages 115–137. Springer, 2005.

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

- 86 4 J. Boudou. Decidable logics with associative binary modalities. In *CSL'17*, volume 82 of
87 *LIPICs*, pages 1–15. Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik, 2017.
- 88 5 R. Brochenin, S. Demri, and E. Lozes. Reasoning about sequences of memory states. *Annals*
89 *of Pure and Applied Logic*, 161(3):305–323, 2009.
- 90 6 R. Brochenin, S. Demri, and E. Lozes. On the almighty wand. *Information and Computa-*
91 *tion*, 211:106–137, 2012.
- 92 7 J. Brotherston, C. Fuhs, N. Gorogiannis, and J. Navarro Perez. A decision procedure for
93 satisfiability in separation logic with inductive predicates. In *CSL-LICS'14*, 2014.
- 94 8 J. Brotherston and J. Villard. Parametric completeness for separation theories. In *POPL'14*,
95 pages 453–464. ACM, 2014.
- 96 9 C. Calcagno and D. Distefano. Infer: An automatic program verifier for memory safety
97 of C programs. In *NASA Formal Methods*, volume 6617 of *Lecture Notes in Computer*
98 *Science*, pages 459–465. Springer, 2011.
- 99 10 C. Calcagno, D. Distefano, P.W. O'Hearn, and H. Yang. Compositional shape analysis by
100 means of bi-abduction. *Journal of the ACM*, 58(6):26:1–26:66, 2011.
- 101 11 C. Calcagno, Ph. Gardner, and M. Hague. From separation logic to first-order logic. In
102 *FOSSACS'05*, volume 3441 of *Lecture Notes in Computer Science*, pages 395–409. Springer,
103 2005.
- 104 12 J. Spring D. Pym and P. O'Hearn. Why separation logic works. Manuscript, 2017.
- 105 13 M. Dams. *Relevance logic and concurrent composition*. PhD thesis, University of Edinburgh,
106 1989.
- 107 14 A. Dawar, Ph. Gardner, and G. Ghelli. Expressiveness and complexity of graph logic.
108 *Information and Computation*, 205(3):263–310, 2007.
- 109 15 S. Demri and M. Deters. Separation logics and modalities: A survey. *Journal of Applied*
110 *Non-Classical Logics*, 25(1):50–99, 2015.
- 111 16 S. Demri and M. Deters. Two-variable separation logic and its inner circle. *ACM Transac-*
112 *tions on Computational Logics*, 2(16), 2015.
- 113 17 S. Demri and M. Deters. Expressive completeness of separation logic with two variables and
114 no separating conjunction. *ACM Transactions on Computational Logics*, 17(2):12, 2016.
- 115 18 S. Demri and R. Fervari. On the complexity of modal separation logics. In *AiML'18*, 2018.
116 to appear.
- 117 19 S. Demri, E. Lozes, and A. Mansutti. The effects of adding reachability predicates in
118 propositional separation logic. In *FOSSACS'18*, volume 10803 of *Lecture Notes in Computer*
119 *Science*, pages 476–493. Springer, 2018.
- 120 20 D. Distefano, P. O'Hearn, and H. Yang. A local shape analysis based on separation logic.
121 In *TACAS'06*, volume 3920 of *Lecture Notes in Computer Science*, pages 287–302. Springer,
122 2006.
- 123 21 C. Haase, S. Ishtiaq, J. Ouaknine, and M. Parkinson. SeLogger: A tool for graph-based
124 reasoning in separation logic. In *CAV'13*, volume 8044 of *Lecture Notes in Computer*
125 *Science*, pages 790–795. Springer, 2013.
- 126 22 L. Hella, K. Luosto, K. Sano, and J. Virtema. The expressive power of modal dependence
127 logic. In *AIML'14*, pages 294–312. College Publications, 2014.
- 128 23 A. Herzig. A simple separation logic. In *WoLLIC'13*, volume 8071 of *Lecture Notes in*
129 *Computer Science*, pages 168–178. Springer, 2013.
- 130 24 C.A.R. Hoare. An axiomatic basis for computer programming. *Communications of the*
131 *ACM*, 12(10):576–580, 1969.
- 132 25 I. Hodkinson, A. Montanari, and G. Sciavicco. Non-finite axiomatizability and undecidability
133 of interval temporal logics with C, D, and T. In *CSL'08*, volume 5213 of *Lecture Notes*
134 *in Computer Science*, pages 308–322. Springer, 2008.

- 135 **26** Z. Hou, R. Goré, and A. Tiu. Automated theorem proving for assertions in separation logic
136 with all connectives. In *CADE'15*, volume 9195 of *Lecture Notes in Computer Science*,
137 pages 501–516. Springer, 2015.
- 138 **27** R. Iosif, A. Rogalewicz, and J. Simacek. The tree width of separation logic with recursive
139 definitions. In *CADE'13*, volume 7898 of *Lecture Notes in Computer Science*, pages 21–38.
140 Springer, 2013.
- 141 **28** S. Ishtiaq and P. O'Hearn. BI as an assertion language for mutable data structures. In
142 *POPL'01*, pages 14–26. ACM, 2001.
- 143 **29** V. Kuncak and M. Rinard. On spatial conjunction as second-order logic. Technical Report
144 MIT-CSAIL-TR-2004-067, MIT CSAIL, October 2004.
- 145 **30** A. Kurucz, I. Németi, I. Sain, and A. Simon. Decidable and undecidable logics with a
146 binary modality. *Journal of Logic, Language, and Information*, 4:191–206, 1995.
- 147 **31** F. Laroussinie and N. Markey. Quantified CTL: Expressiveness and complexity. *Logical
148 Methods in Computer Science*, 10(4:17), 2014.
- 149 **32** E. Lozes. *Expressivité des Logiques Spatiales*. Phd thesis, ENS Lyon, 2004.
- 150 **33** Xu Lu, Cong Tian, and Zhenhua Duan. Temporalising separation logic for planning with
151 search control knowledge. In *IJCAI'17*, pages 1167–1173, 2017.
- 152 **34** A. Mansutti. Extending propositional separation logic for robustness properties, July 2018.
153 Manuscript.
- 154 **35** D. Della Monica, V. Goranko, A. Montanari, and G. Sciavicco. Interval temporal logics: a
155 journey. *Bulletin of the EATCS*, 105:73–99, 2011.
- 156 **36** B. Moszkowski. Reasoning about digital circuits. Technical Report STAN-CS-83-970, Dept.
157 of Computer Science, Stanford University, Stanford, CA, 1983.
- 158 **37** P. Müller, M. Schwerhoff, and A.J. Summers. Viper: A verification infrastructure for
159 permission-based reasoning. In *VMCAI'16*, volume 9583 of *Lecture Notes in Computer
160 Science*, pages 41–62. Springer, 2016.
- 161 **38** P. O'Hearn and D. Pym. The logic of bunched implications. *Bulletin of Symbolic Logic*,
162 5(2):215–244, 1999.
- 163 **39** P.W. O'Hearn, J.C. Reynolds, and H. Yang. Local reasoning about programs that alter
164 data structures. In *CSL'01*, volume 2142 of *Lecture Notes in Computer Science*, pages 1–19.
165 Springer, 2001.
- 166 **40** D. Pym. *The Semantics and Proof Theory of the Logic of Bunched Implications*, volume 26
167 of *Applied Logic*. Kluwer Academic Publishers, 2002.
- 168 **41** J.C. Reynolds. Separation logic: a logic for shared mutable data structures. In *LICS'02*,
169 pages 55–74. IEEE, 2002.
- 170 **42** M. Schwerhoff and A. Summers. Lightweight support for magic wands in an automatic
171 verifier. In *ECOOP'15*, pages 999–1023. Leibniz-Zentrum für Informatik, LIPICS, 2015.
- 172 **43** A. Thakur, J. Breck, and T. Reps. Satisfiability modulo abstraction for separation logic
173 with linked lists. In *SPIN'14*, pages 58–67. ACM, 2014.
- 174 **44** Y. Venema. Expressiveness and completeness of an interval tense logic. *NDJFL*, 31(4):529–
175 547, 1990.
- 176 **45** Y. Venema. A modal logic for chopping intervals. *Journal of Logic and Computation*,
177 1(4):453–476, 1991.
- 178 **46** H. Yang, O. Lee, J. Berdine, C. Calcagno, B. Cook, D. Distefano, and P. O'Hearn. Scalable
179 shape analysis for systems code. In *CAV'08*, volume 5123 of *Lecture Notes in Computer
180 Science*, pages 385–398. Springer, 2008.