On Temporal and Separation Logics
Stephane Demri

To cite this version:

HAL Id: hal-02366656
https://hal.science/hal-02366656
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.
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, Logic, Modal and Temporal Logics, 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 $\ast$ that allows one to state properties in disjoint parts of the memory. The companion connective $-\ast$ 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 developed [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 $\rightarrow$ 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 $\ast$ and the list segment predicate $\mathsf{ls}$ (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 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 Bartosz Bednarczyk’s internship at LSV (2018) is dedicated to related issues.


On Temporal and Separation Logics


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


