Separation Logics: Semantics and Proofs (Extended Abstract)

Didier Galmiche

Université de Lorraine, CNRS, LORIA Vandoeuvre-lès-Nancy, F-54506, France

Abstract

In this talk we give an overview of works and results about so-called BI-based Separation Logics, with a main focus on semantics and proofs. We present some key ideas and works mainly developed in our research team in LORIA laboratory (Nancy, France) since more than twenty years. After a reminder about resource models and resource logics we start to present the BI logic (with intuitionistic additives), Boolean BI (BBI) logic (with classical additives), and also BI's Pointer logic, called now Separation Logic, that deals with memory cells. We summarize the main results about semantics and proofs in these logics with an emphasis on the notions of constraints and resource graphs on which the design of labelled proof systems is based. The next part is devoted to the presentation of various modal and epistemic BBI-based (or separation) logics that manage different kinds of modalities, again with a focus on semantics, expressiveness, and proofs. We complete this overview by mentioning recent works on proof translations between calculi in BI and their possible consequences on some completeness results. Then we conclude with some perspectives about separation logics from current studies of non-aggregative models of resource composition.

Keywords

Logics with Separation, Resources, Semantics, Labelled Calculi, Modal logics

CEUR-WS.org/Vol-3875/ARQNL2024_abstract1.pdf

1. Extended Abstract

In this talk we give an overview of researchs and results about so-called BI-based Separation Logics, with a main focus on semantics and proofs. We present some key ideas, works and results mainly developed in our research team in LORIA laboratory (Nancy, France) since more than twenty years. After a reminder about resource models and resource logics we start by giving the BI logic (with intuitionistic additives) [1], its bunched calculus (LBI) and its resource semantics that is complete only for BI without $\perp$ [2]. We also remind that BI logic, that focuses on resource separation and sharing, is different from Linear Logic [3], that focuses instead on resource comsumption. We also consider some variants of BI logic like Boolean BI (BBI) (with classical additives) [4] and BI's Pointer logic, also called Separation Logic (SL), that is based on BBI and deals with memory cells [5]. Separation Logic has provided key developments in formal reasoning about programs with the frame rule that allows a proof to be localized to the resources that a program component accesses andalso with the key notion of local reasoning [6, 7]. We do not consider here the impressive developments from SL in the last twenty years but we can mention the Concurrent Separation Logic [8], that allows modular reasoning about threads that share storage and other resources, the Incorrectness Separation Logic [9], with the goal of proving that compositional bug catchers find actual bugs and its concurrent extension to account for bug catching in concurrent programs [10]. In the rest of the talk Separation logics denote the (B)BI-based logics with separation and their extensions.

After this first part we introduce BI logic, its semantics and mainly on so-called resource tableaux, that are labelled tableaux with resource constraints of two kinds (assertions and requirements), and also define the key notion of resource graph [2]. The tableau calculus designed for BI logic is proved sound and complete w.r.t. the Grothendick topological semantics (GR models). To solve the question to have a semantics of BI based on partial monoids we propose different new semantics for BI logic, namely a relational semantics (RM models), a Kripke resource semantics (KR models) and a partially defined

ARQNL 2024: Automated Reasoning in Quantified Non-Classical Logics, 1 July 2024, Nancy, France

Didier.Galmiche@loria.fr (D. Galmiche)

© 2024 Copyright for this paper by its authors. Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0).

CEUR Workshop Proceedings ceur-ws.org ISSN 1613-0073

monoid semantics (PDM models) and show that the tableaux calculus is sound and complete w.r.t. these models. Moreover BI logic is sound and complete w.r.t these models except for KR models, that is still an open question [11].

From our notion of resource graph we also show that one can define a connection-based characterization of BI's validity with constraints without using prefixes like in other non-classical logics [12]. Moreover we study and define resource graphs for other logics and then provide a tableaux calculus for BI's Pointer logic (or SL) [13, 14], a new connection-based characterization of validity for Non Commutative Logic [15] and also such a connection-based characterization for Bi-intuitionistic logic (Bi-Int) with both implication and co-implication [16]. These works illustrate the interest to study semantics and then to define and use constraints and resource graphs for designing calculi for different resource logics.

We also mention works on semantics for Boolean BI (BBI) with the proposal of a Kripke relational semantics for BBI (a non-deterministic monoidal semantics) with faithful embeddings of S4 and of IL into BBI. It provides also a logical characterization of the observational power of BBI through an adequate definition of bisimulation [17]. From this study of BBI semantics one can propose a labelled tableau for BBI that is sound and also a sound and faithful embedding of BI into BBI [18]. In addition we propose a complete phase semantics for BBI and an embedding between phase semantics for ILL and Kripke semantics of BBI. By defining a fragment of ILL undecidable and complete for phase semantics one can prove the undecidability of BBI [19, 20]. Concerning the labelled tableaux for partial monoidal Boolean BI, it is important to note that the schema of its proof of strong completeness is original and it has been completely formalized in Coq [21].

In the next part we present some modal extensions of (B)BI-based logics with different kinds of modalities. A first one, called BI-Loc, considers a spatial modality for locations and resource trees and proposes a new logic for resource distribution [22]. A second one, called DBI, extends BBI logic with two modalities for expressing properties on states of process or on interacting systems. As the related semantics introduces states in addition to resources, one also introduces state constraints in addition to the resource constraints and then define a labelled tableaux calculus that is sound and complete w.r.t. the semantics [23]. A third one, called DMBI (Dynamic Modal BI), is an extension of DBI for introducing dynamics (resource transformations) with modalities à la Hennessy-Milner. Then new kinds of constraints (resources, actions, states) are considered in the tableaux calculus that is proved sound and complete w.r.t. the semantics [24]. A fourth one, called LSM, considers modalities, generalyzing S4 modalities. They are defined with two-dimensional worlds, one for S4 accessibility and one for resource parametrization. and allow us to express properties of models of distributed computing. A sound and complete labelled calculus is provided [25].
For these new modal separation logics we have mentioned modelling examples in order to illustrate their expressivity and also the related labelled calculi with their properties of soundness and completeness. We emphasize that the completeness proofs are based on the proof schema given in [21] for BBI logic, that is extended and adapted, in a non-trivial way, for these logics.

In this context we also consider works on separation logics with knowledge and then propose some epistemic extensions of BBI. One first, called ESL, considers epistemic modalities with a semantics for which the possible (epistemic) worlds are resources that can be composed and decomposed. The tableaux calculus for ESL is defined with resource constraints but also with agent constraints and it is proved sound and complete w.r.t. the semantics [26]. The addition of public announcements modalities to ESL has been also studied and results in a public announcement separation logic (PASL) [27].
Another epistemic extension of BBI, called ERL, deals with epistemic modalities that are parametrized on agents' local resources and allow us the modelling of some acces control problems. Let us note that it is a conservative extension of BBI and Epistemic Logic. Again the study of the semantics and the expressiveness has been completed by the design of a sound and complete labelled tableaux calculus [28].

We then continue this overview of BI and BBI modal and/or epistemic extensions, with a strong focus on semantics and proof theory, by mentioning two works that benefit from some of the previous results. A first work studies proof translations in BI logic between labelled and label-free calculi. The results and their proofs emphasize the difficulty to design a translation from a proof in a labelled calculus into a proof in a label-free calculus in BI logic, like in other logics. We expect that having a general schema for such a translation would help us to prove a still open question for BI logic, that is the completeness of the bunched calculus LBI w.r.t. KRM semantics [29].
A second work is about Separation Logic (SL) and inductive predicates. Proof systems for this logic are often dedicated to some fragments of SL (symbolic heaps) that cannot express some properties about pointers. They mainly allow either the full set of connectives, or the definition of arbitrary inductive predicates, but not both. Then we comment a cyclic labelled system for SL that allows both [30]. This work about cyclic proofs opens perspectives for some extensions of BI that will be developed in the future. .

We conclude with a current work on a temporal extension of BI, called LTBI (Linear Time Bunched Implication Logic) that is dedicated to resource evolution over time by combining BI separation connectives and LTL temporal connectives [31]. A new semantics is given and a labelled calculus is defined for LTBI and is proved sound but the completeness, proved for bounded timelines, is not trivial in the general case of unbounded timelines. We expect that the definition of a cyclic proof system for this logic would lead to the completeness result in this general setting. Finally we briefly present a current study of new non-aggregative models of resource composition, namely compositions that do not obey the principle that the whole is the sum of its parts. Our first objectives are to find algebraic properties characterizing such compositions and then to design resource logics for such non-aggregative compositions, if possible in the spirit of our previous works for BI, BBI and their extensions.

References

[1] P. W. O'Hearn, D. Pym, The Logic of Bunched Implications, Bulletin of Symbolic Logic 5 (1999) 215–244.

[2] D. Galmiche, D. Méry, Semantic Labelled Tableaux for propositional BI (without bottom), Journal of Logic and Computation 13 (2003) 707–753.

[3] J. Girard, Linear logic, Theoretical Computer Science 50 (1987) 1–102.

[4] D. J. Pym, The Semantics and Proof Theory of the Logic of Bunched Implications, volume 26, Applied Logic Series. Kluwer Academic Publishers, 2002.

[5] S. S. Ishtiaq, P. W. O'Hearn, BI as an Assertion Language for Mutable Data Structures, in: Proceedings of the 28th ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages, 2001, pp. 14—26.

[6] J. C. Reynolds, Separation Logic: A Logic for Shared Mutable Data Structures., 17th Annual IEEE Symposium on Logic in Computer Science (LICS'02) (2002) 55–74.

[7] P. W. O'Hearn, Separation Logic, Communications of ACM 62 (2019) 86–95.

[8] S. Brookes, P. W. O'Hearn, Concurrent Separation Logic, ACM SILOG News 3 (2016) 47–65.

[9] P. W. O'Hearn, Incorrectness logic, in: Proc. ACM on Programming Languages 4, POPL, Article 10, 2019, pp. 1–32.

[10] A. Raad, J. Berdine, D. Dreyer, P. W. O'Hearn, Concurrent Incorrectness Separation Logic, in: Proc. ACM on Programming Languages 6, POPL, Article 34, 2022, pp. 1–29.

[11] D. Galmiche, D. Méry, D. Pym, The semantics of BI and Resource Tableaux, Mathematical Structures in Computer Science 15 (2005) 1033–1088.

[12] D. Galmiche, D. Méry, Connection-based proof search in propositional BI logic, in: 18th Int. Conference on Automated Deduction, CADE-18, LNAI 2392, 2002, pp. 111–128. Copenhagen, Danemark.

[13] D. Galmiche, D. Méry, Characterizing provability in BI's pointer logic through resource graphs, in: Int. Conference on Logic for Programming, Artificial Intelligence, and Reasoning, LPAR 2005, LNAI 3835, Montego Bay, Jamaica, 2005, pp. 459–473.

[14] D. Galmiche, D. Méry, Tableaux and Resource Graphs for Separation Logic, Journal of Logic and Computation 20 (2010) 189–231.

[15] D. Galmiche, J. Notin, Connection-based Proof Construction in Non-commutative Logic, in: 10th Int. Conference on Logic for Programming, Artificial Intelligence, and Reasoning, LPAR'03, LNCS 2850, 2003, pp. 422–436. Almaty, Kazakhstan.

[16] D. Galmiche, D. Mery, A Connection-based Characterization of Bi-intuitionistic Validity, Journal of Automated Reasoning 51 (2013) 3–26.

[17] D. Galmiche, D. Larchey-Wendling, Expressivity properties of Boolean BI through Relational Models, in: 26th Conference on Foundations of Software Technology and Theoretical Computer Science, FSTTCS 2006, LNCS 4337, 2006, pp. 358–369. Kolkata, India.

[18] D. Larchey-Wendling, D. Galmiche, Exploring the Relation between Intuitionistic BI and Boolean BI: An unexpected Embedding, Mathematical Structures in Computer Science 19 (2009) 435–500.

[19] D. Larchey-Wendling, D. Galmiche, The Undecidability of Boolean BI through Phase Semantics, in: 25th Annual IEEE Symposium on Logic in Computer Science, LICS 2010, Edinburgh, UK, 2010, pp. 147–156.

[20] D. Larchey-Wendling, D. Galmiche, Nondeterministic Phase Semantics and the Undecidability of Boolean BI, ACM Transactions on Computational Logic 14 (2013) 6.

[21] D. Larchey-Wendling, The Formal Strong Completeness of Partial Monoidal Boolean BI, Journal of Logic and Computation 26 (2014) 605–640.

[22] N. Biri, D. Galmiche, Models and Separation Logics for Resource Trees, Journal of Logic and Computation 17 (2007) 687–726.

[23] J. Courtault, D. Galmiche, A Modal BI Logic for Dynamic Resource Properties, in: Logical Foundations of Computer Science, LFCS 2013, LNCS 7734, 2013, pp. 134–148. San Diego, CA.

[24] J.-R. Courtault, D. Galmiche, A Modal Separation Logic for Resource Dynamics., Journal of Logic and Computation 28 (2018) 733–778.

[25] J.-R. Courtault, D. Galmiche, D. Pym, A Logic of Separating Modalities, Theoretical Computer Science 637 (2016) 30–58.

[26] J.-R. Courtault, H. van Ditmarsch, D. Galmiche, An Epistemic Separation Logic, in: 22nd Int. Workshop on Logic, Language, Information, and Computation, WoLLIC 2015, LNCS 9160, Bloomington, IN, United States, 2015, pp. 156–173.

[27] J.-R. Courtault, H. van Ditmarsch, D. Galmiche, A Public Announcement Separation Logic, Mathematical Structures in Computer Science 29 (2019) 828–871.

[28] D. Galmiche, P. Kimmel, D. Pym, A Substructural Epistemic Resource Logic: Theory and Modelling Applications, Journal of Logic and Computation 29 (2019) 1251–1287.

[29] D. Galmiche, M. Marti, D. Méry, Relating Labelled and Label-Free Bunched Calculi in BI Logic, in: 28th Int. Conference on Automated Reasoning with Analytic tableaux and Related Methods, Tableaux 2019, LNAI 11714, 2019, pp. 130–146. London, UK.

[30] D. Galmiche, D. Mery, Labelled Cyclic Proofs for Separation Logic, Journal of Logic and Computation 31 (2021) 892–922.

[31] D. Galmiche, D. Méry, Labelled Tableaux for Linear Time Bunched Implication Logic, in: 8th International Conference on Formal Structures for Computation and Deduction, FSCD 2023, LIPIcs, Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagsthul, Roma, Italy, 2023, p. 27:1–27:17.