An Epistemic Resource Logic based on Boolean BI*

Didier Galmiche

LORIA - Université de Lorraine,
France

Abstract

The concept of resource is important in many fields including, among others, computer science, economics, and security. For example, in operating systems, processes access system resources such as memory, files, processor time, and bandwidth, with correct resource usage being essential for the robust function of the system. In recent years, the concept of resource has been studied and analysed in computer science through the Bunched Logic BI [10] and its variants, such as Boolean BI (BBI) [11] and applications, such as Separation Logic [11,14]. The *resource semantics* — that is, the interpretation of BI's semantics in terms of resources — that underpins these logics is mainly concerned with sharing and separation, corresponding to additive, such as $\wedge$, and multiplicative connectives, such as $*$, respectively. These logics are the logical kernels of the separating, or separation, logics, with resources being interpreted in various ways, such as memory regions, [11,14] or elements of other particular monoids of resources.

The logic BI of bunched implications [9,10,13] freely combines intuitionistic propositional additives with intuitionistic propositional multiplicatives. In Boolean BI (BBI) [11], the additives are classical. The key feature of BI as a modelling tool is its control of the representation and handling of resources provided by the resource semantics and the associated proof systems. BI's basic propositional connectives are the additives (disjunction, conjunction, and implication) that be handled either classically or intuitionistically and the multiplicatives with the multiplicative conjunction, $*$, that divides the resource between its propositional components, using a partial commutative monoidal operation, $\circ$. Then the monoid specifies a *separation* of the resources between the components of the conjunction.
BI's sequent proof systems employ *bunches*, with two context-building operations: one for the additives (characterized by $\wedge$, which admits weakening and contraction) and one for the multiplicatives (characterized by $*$, which admits neither weakening nor contraction). The soundness and completeness of BI for the semantics given above is established in [13] and via labelled tableaux in [9], and the completeness of BBI for the partial monoid semantics described above is established in [12].

Modal extensions of BI, such as MBI [1], DBI and DMBI [4] and LSM [6], have been proposed to introduce dynamics into resource semantics. In recent work, the idea of

* It is a joint work with Pierre Kimmel (Université de Lorraine, LORIA, France) and David Pym (University College London, UK). It is built on early ideas presented in [8].

introducing agents, together with their knowledge, into the resource semantics has led to an Epistemic Separation Logic, called ESL, in which epistemic possible worlds are considered as resources [5]. This logic corresponds to an extension of Boolean BI with a knowledge modality, K_a, such that $K_a\phi$ means that the agent a knows that ϕ holds.
Some previous works on epistemic logics consider the concept of resource [2]. Here we aim to explore more deeply the idea of epistemic reasoning [7] in the context of resource semantics, and its associated logic, by taking the basic epistemic modality K_a and parametrizing it with a resource s, with the associated introduction of relations not only between resources, according to an agent, but also between composition of resources in different ways. The parametrizing resource may be thought of as being associated with, or local to, the agent. This approach leads to the definition of three new modalities $\mathbf{L}^s_a$, $\mathbf{M}^s_a$, and $\mathbf{N}^s_a$ and, consequently, to a new logic in which, as a leading example, we can obtain an account of access to resources and its control, whether they be pieces of knowledge, locations, or other entities.

In this talk we present this epistemic resource logic ERL, based on Boolean BI, in which the epistemic modalities are parametrized on agents' local resources. The new modalities can be seen as generalizations of the usual epistemic modalities. The logic combines Boolean BI's resource semantics with epistemic agency.
We illustrate the use of ERL and its sublogic ERL*, by discussing some examples about access control using resource tokens. We explain how to use the logic to model and reason about the relationship between a security policy (in the context of access control) and the system to which it is applied (cf. Schneier's Gate problem [15]). Other examples about joint access, semaphores, and modelling with layers, can illustrate the applicability of ERL in these perspectives. We also give a labelled tableaux calculus and establish soundness and completeness with respect to the resource semantics.
Further work will be devoted to perspectives of the logic and its variants, to local reasoning, to connections with other approaches to modelling the relationship between policy and implementation in system management [16], and to approaches involving logics for layered graphs [1,3].

References

1. G. Anderson and D. Pym. A calculus and logic of bunched resources and processes. *Theoretical Computer Science*, 614:63–96, 2016.
2. A. Baltag, B. Coecke and M. Sadrzadeh. Epistemic Actions as Resources *Journal of Logic and Computation*, 17(3):555-585, 2006.
3. M. Collinson, K. McDonald, and D. Pym. Layered graph logic as an assertion language for access control policy models. *Journal of Logic and Computation*, 27(1):41–80, 2017. doi:10.1093/logcom/exv020.
4. J-R. Courtault and D. Galmiche. A Modal Separation Logic for Resource Dynamics. *Journal of Logic and Computation*, 46 pages, 2015. doi:10.1093/logcom/exv031.
5. J-R. Courtault, H. van Ditmarsch, and D. Galmiche. An epistemic separation logic. In *22nd International Workshop on Logic, Language, Information, and Computation, WoLLIC 2015, Bloomington, USA, July 2015*. LNCS 9160:156–173, 2015.
6. J.-R. Courtault, D. Galmiche, and D. Pym. A logic of separating modalities. *Theoretical Computer Science* 637, 30–58, 2016. doi: 10.1016/j.tcs.2016.04.040.

7. H. van Ditmarsch, J.Y. Halpern, W. van der Hoek, and B. Kooi (editors). *Handbook of Epistemic Logic*. College Publications, 2015.
8. D. Galmiche, P. Kimmel, and D. Pym. A Substructural Epistemic Resource Logic. *Proc. ICLA 2017*. LNCS 10119:106–122, 2017
9. D. Galmiche, D. Méry, and D. Pym. The semantics of BI and Resource Tableaux. *Math. Struct. Comp. Sci.* 15(6):1033–1088, 2005.
10. P. O'Hearn and D. Pym. The logic of Bunched Implications. *Bulletin of Symbolic Logic* 5(2):215-244, 1999.
11. S. Ishtiaq and P. O'Hearn. BI as an assertion language for mutable data structures. In *28th ACM Symposium on Principles of Programming Languages (POPL)*, London, 2001, 14–26.
12. D. Larchey-Wendling. The formal strong completeness of partial monoidal Boolean BI. *Journal of Logic and Computation* 26(2), 605–640, 2014. doi: 10.1093/logcom/exu031
13. D. Pym, P. O'Hearn, and H. Yang. Possible worlds and resources: the semantics of BI. *Theoretical Computer Science* 315(1): 257–305. Erratum: p. 22, l. 22 (preprint), p. 285, l. -12 (TCS): ', for some P' , $Q \equiv P;P'$' should be '$P \vdash Q$'.
14. J. Reynolds. Separation logic: A logic for shared mutable data structures. In *IEEE Symposium on Logic in Computer Science, LICS 2002*, 55–74, Copenhagen, Denmark, July 2002.
15. B. Schneier. The weakest link (`https://www.schneier.com/blog/archives/2005/02/the_weakest_lin.html`). Schneier on Security (`https://www.schneier.com`), 2005.
16. B. Toninho and L. Caires. A spatial-epistemic logic for reasoning about security protocols. In *8th Int. Workshop on Security Issues in Concurrency, SecCo 2010*, 2010.