Resource Reasoning in Duality-theoretic Form: Stone-type Dualities for Bunched and Separation Logics

Simon Docherty and David Pym

University College London, London, United Kingdom
simon.docherty@ucl.ac.uk and d.pym@ucl.ac.uk

Bunched logics, beginning with O'Hearn and Pym's **BI** [9, 10], have proved to be exceptionally useful tools in modelling and reasoning about computational and information-theoretic phenomena such as resources, the structure of complex systems, and access control. Perhaps the most striking example is Separation Logic [11] a specific theory of predicate **BI** with primitives for mutable data structures. Separation Logic has heralded a paradigm shift in deployable program correctness proving, key examples of which being the static analysis tool Infer (www.fbinfer.com) — now part of the code review production line at Facebook, with millions of lines of code automatically checked for memory bugs to date — and the Coq-implemented Concurrent Separation Logic framework Iris, which has been used to give machine-checked safety proofs for the systems programming language Rust [8].

Bunched logics provide an alternative to the resource-sensitive reasoning facilitated by linear logic. In linear logic, the structural rules of weakening and contraction are dropped, leading to a splitting of conjunction and disjunction into *additive* and *multiplicative* forms. These structural rules are reintroduced in a controlled manner via the *exponentials* ! and ?. This leads to an operational *number-of-uses* interpretation of formulae: a formula φ is a resource that may be used once; however, $!\varphi$ denotes a duplicable resource φ that can be used as many times as one needs. In bunched logics, the control of structural rules is implemented very differently: in bunched sequent calculi, contexts are tree-shaped structures — *bunches* — built from *two* context formers to which different structural rules apply: one in which all apply, and another in which weakening and contraction (and possibly more) are dropped. Such systems can safely be seen as the free combination of intuitionistic propositional logic with multiplicative fragments of linear logics. The upshot of this is the existence (in contrast with linear logic) of a simple Kripke semantics of abstract resource: formulae have a declarative *separation* interpretation, describing properties a resource may satisfy, and, in particular, the manner in which resources must be (de)composed into components in order to meet a specification.

In the characteristic case of **BI**, Kripke resource models are given by ordered partial commutative monoids, in which worlds are seen to be resources that can be compared via an order $\leq$ and, when compatible, composed by a partial composition $\circ$. For example, in the standard model of Separation Logic the resources are heaps (chunks of dynamically allocated computer memory) which can be compared (when one heap contains another) and, when compatible (when the memory addresses assigned by each heap are disjoint), composed by disjoint union. The Kripke semantics then extends that for intuitionistic logic with clauses for the multiplicative connectives. In particular, the multiplicative conjunction, $*$, is interpreted as follows:

$$x \vDash \varphi * \psi \text{ iff there exists resources } y, z \text{ such that } y \circ z \leq x \text{ and } y \vDash \varphi \text{ and } z \vDash \psi,$$

to be read as "the resource x is sufficient for $\varphi * \psi$ iff part of x can be split into separate resources, y and z, with y sufficient for φ and z sufficient for ψ". Further multiplicative connectives—corresponding to implications, negation, disjunction, verum and falsum—are similarly given a straightforward Kripke semantics via operations on resources.

Resource semantics has been hugely influential; in particular, in its instantiations in Separation Logic and its descendents, with a huge body of literature and automated reasoning

tools successfully applying the idea to a range of computational phenomena. In contrast, the alternative *algebraic* view on bunched logics — as Heyting algebras extended with additional residuated monoidal operations — has seen little attention, with recent work by Galatos & Jipsen [5] and Litak & Jipsen [7] rare exceptions. This is quite an usual situation for a family of systems closely related to intuitionistic, modal and substructural logics.

In this talk, we give a systematic account of resource semantics via a family of Stone-type duality theorems between categories of bunched logic algebras and categories of ordered topological spaces. This framework encompasses the full range of systems: from the weakest bunched logics to those involving multiplicative variants of all of the standard propositional connectives, as well as those featuring (separating) modalities. By considering the category theoretic structures of bunched logic hyperdoctrines and indexed topological spaces, the duality theorems are extended to the predicate case, thus additionally capturing Separation Logic. As corollaries we retrieve soundness and completeness for the standard Kripke semantics found in the literature as well as new results for logics that previously lacked a semantic formulation.

To do so, we synthesise a variety of related work from modal [6], relevant [12], substructural [1] and categorical logic [2]. Much of the theory these areas enjoy is produced by way of algebraic and topological techniques. We argue that by recontextualizing the resource semantics of bunched logics in this way, similar theory can be given for both Separation Logic and its underlying systems. As examples, we prove a range of metatheory, including: decidability of weak bunched logics, the failure of interpolation, and a Goldblatt-Thomason-style characterisation of the definable classes of resource models. Further, we indicate a range of future directions building on our framework, including the *natural duality* generalisation of our results, extensions with semantics of program execution, and the development of Sahlqvist-style correspondence theory for bunched logics. This talk is based on material from the first author's PhD thesis [3], some of which will appear in a forthcoming journal article [4].

References

[1] K. Bimbó and J.M. Dunn. *Generalized Galois Logics. Relational Semantics of Nonclassical Logical Calculi.* CSLI Publications, 2008.

[2] D. Coumans. Duality for first-order logic. http://www.math.ru.nl/~coumans/talkAC.pdf.

[3] S. Docherty. Bunched logics: a uniform approach. PhD thesis, University College London, 2019.

[4] S. Docherty and D. Pym. Stone-type dualities for separation logics. *Log. Meth. Comp. Sci.*, to appear.

[5] N. Galatos and P. Jipsen. Distributive residuated frames and generalized bunched implication algebras. *Algebr. Univ.*, 78(3): 303–336, 2017.

[6] R. Goldblatt. Varieties of complex algebras. *Ann. Pure Appl. Logic*, 44(3):173-242, 1989.

[7] P. Jipsen and T. Litak. An algebraic glimpse at bunched implications and separation logic. In *Hiroakira Ono on Residuated Lattices and Substructural Logics*, arXiv:1709.07063v2, to appear.

[8] R. Jung, J.-H. Jourdan, R. Krebbers and D. Dreyer. RustBelt: Securing the foundations of the Rust programming language. *POPL 2018*, Article 66, 2018.

[9] P. O'Hearn and D. Pym. The logic of bunched implications. *Bull. Symb. Log.*, 5(2):215–244, 1999.

[10] D. Pym. Resource semantics: logic as a modelling technology. *ACM SIGLOG News*, April 2019, Vol. 6, No. 2, 5–41.

[11] J. Reynolds. Separation logic: a logic for shared mutable data structures. In *LICS 2002*, 55–74, 2002.

[12] Alasdair Urquhart. Duality for algebras of relevant logics. *Studia Logica*, 56(1/2): pp. 263–276, 1996.