Available online at www.sciencedirect.com

ScienceDirect

Electronic Notes in Theoretical Computer Science 336 (2018) 101–118

Electronic Notes in Theoretical Computer Science

www.elsevier.com/locate/entcs

A Stone-type Duality Theorem for Separation Logic Via its Underlying Bunched Logics

Simon Docherty[1] and David Pym [2]

Department of Computer Science
University College London
London, United Kingdom

Abstract

Stone-type duality theorems, which relate algebraic and relational/topological models, are important tools in logic because — in addition to elegant abstraction — they strengthen soundness and completeness to a categorical equivalence, yielding a framework through which both algebraic and topological methods can be brought to bear on a logic. We give a systematic treatment of Stone-type duality theorems for the structures that interpret bunched logics, starting with the weakest systems, recovering the familiar Boolean BI, and concluding with Separation Logic. Our results encompass all the known existing algebraic approaches to Separation Logic and prove them sound with respect to the standard store-heap semantics. We additionally recover soundness and completeness theorems of the specific truth-functional models of these logics as presented in the literature. This approach synthesises a variety of techniques from modal, substructural and categorical logic and contextualises the 'resource semantics' interpretation underpinning Separation Logic amongst them. As a consequence, theory from those fields — as well as algebraic and topological methods — can be applied to both Separation Logic and the systems of bunched logics it is built upon. Conversely, the notion of *indexed resource frame* (generalizing the standard model of Separation Logic) and its associated completeness proof can easily be adapted to other non-classical predicate logics.

Keywords: Separation logic, bunched logic, substructural logic, program logic, categorical logic, algebraic logic, representation, Stone duality, complex systems, hyperdoctrine, relational semantics, topological semantics, completeness.

1 Introduction

Bunched logics, beginning with O'Hearn and Pym's **BI** [36], 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 [14,15,23]. Perhaps the most striking example is Separation Logic [38,41] (via BI Pointer Logic [31]), a specific theory of first-order Boolean BI with primitives for mutable data structures. Other examples include layered graph

[1] Email: simon.docherty.14@ucl.ac.uk
[2] Email: d.pym@ucl.ac.uk

https://doi.org/10.1016/j.entcs.2018.03.018

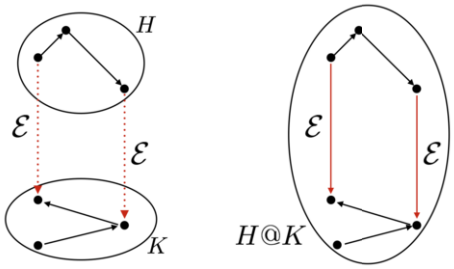

Fig. 1. A layered graph $H \,@_{\mathcal{E}}\, K$

logics [14,15,23], modal and epistemic systems [20,26], and Hennessy–Milner-style process logics that have applications in security [15] and systems modelling [16,2].

The weakest bunched systems are the so-called layered graph logics [14,23]. These logics have a multiplicative conjunction that is neither associative nor commutative, together with its associated implications, and additives that may be classical or intuitionistic. These systems can be used to describe the decomposition of directed graphs into layers (see Fig 1), with applications such as complex systems modelling (e.g., [14,23]) and issues in security concerning the relationship of policies and the systems to which they are intended to apply (e.g., [15,23]). Strengthening the multiplicative conjunction to be associative and commutative yields **BI**, for intuitionistic additives, and Boolean BI (**BBI**), for classical additives. Further extensions include additive and multiplicative modalities and, with the addition of parametrization of modalities on actions, Hennessy–Milner-syle process logics [16,2]. Yet further extensions include additive and multiplicative epistemic modalities [26], with applications in security modelling.

All of the applications of bunched logics to reasoning about computational and information-theoretic phenomena essentially rely on the interpretation of the truth-functional models of these systems known as *resource semantics*. Truth-functional models of bunched logics are, essentially, constructed from pre- or partially ordered partial monoids [29] which, in resource semantics, are interpreted as describing how resource-elements can be combined (monoid composition) and compared (order). The program logic known as *Separation Logic* [31,38,41] is a specific theory of first-order Boolean BI (**FOBBI**) based on the partial monoid of elements of the heap (with the order being simply equality). Separation Logic has found industrial-strength application to static analysis through Facebook's Infer tool (`fbinfer.com`).

Stone's representation theorem for Boolean algebras [39] establishes that every Boolean algebra is isomorphic to a field of sets. Specifically, every Boolean algebra $\mathbb{A}$ is isomorphic to the algebra of clopen subsets of its associated *Stone space* [32] $S(\mathbb{A})$. This result generalizes to a family of Stone-type duality theorems which establish equivalences between certain categories of topological spaces and categories of partially ordered sets. From the logical point of view, Stone-type dualities strengthen the semantic equivalence of truth-functional (such as **BI**'s resource semantics or Kripke's semantics for intuitionistic logic) and algebraic (such as BI algebras or Heyting algebras) models to a dual equivalence of categories. This is useful for