Available online at www.sciencedirect.com

ScienceDirect

Electronic Notes in Theoretical Computer Science 336 (2018) 57–78

Electronic Notes in Theoretical Computer Science

www.elsevier.com/locate/entcs

On Models of Higher-Order Separation Logic

Aleš Bizjak[1] Lars Birkedal[2]

Department of Computer Science, Aarhus University, Denmark

Abstract

We show how tools from categorical logic can be used to give a general account of models of higher-order separation logic with a sublogic of so-called persistent predicates satisfying the usual rules of higher-order logic. The models of separation logic are based on a notion of resource, a partial commutative monoid, and the persistent predicates can be defined using a modality. We classify well-behaved sublogics of persistent predicates in terms of interior operators on the partial commutative monoid of resources. We further show how the general constructions can be used to recover the model of Iris, a state-of-the-art higher-order separation logic with guarded recursive predicates.

Keywords: separation logic, model, modalities

1 Introduction

In recent years we have seen many models of variations of higher-order separation logic, e.g., [4,14,6,3,1,16,10,9,11]. Separation logic is a substructural logic and the models are all based on some notion of resource. Originally, resources were heap fragments, and predicates in the logic described sets of heaps. For instance, the points-to predicate $\ell \mapsto 3$ described those heaps that contain the value 3 at location ℓ. Later on, more elaborate notions of resources were used because they allow for stronger specifications and they can be used to keep track of data and relationships not explicitly given in the program code.

With these richer notions of resources it has often been noticed that it is very useful to be also able to single out and work with predicates that are "persistent". Persistent predicates are, in particular, duplicable (meaning $P \star P \Leftrightarrow P$), and they obey more standard (not substructural) logical rules. One way this has been achieved is via a modality $\Box$ (pronounced *always*) which is a necessity-like modality and obeys rules akin to those obeyed by the bang modality ! of linear logic. Such a

[1] Email: abizjak@cs.au.dk
[2] Email: birkedal@cs.au.dk

https://doi.org/10.1016/j.entcs.2018.03.016

modality also gives the ability to make propositions persistent inside the logic, which significantly increases its expressiveness, as demonstrated in previous work [9,11].

Examples of persistent predicates are simple facts like equality of values, and Hoare triples. Hoare triples are specifications of (parts of) programs. They describe the *knowledge* (in separation logic jargon) that a program requires certain resources (precondition) and ensures certain properties after execution (postcondition). As such this knowledge should be reusable many times, in the sense that during verification of a larger program, we can use the specification of the subparts as many times as the subparts appear. In sophisticated logics, in particular in concurrent separation logics such as Iris [10], there are many other persistent predicates, e.g., invariants, which describe the knowledge that a certain predicate holds for some shared memory. This knowledge should be shared between different parts of the program which operate on the shared memory, and hence invariants should be duplicable.

Thus in advanced separation logics it is useful to have a distinction between predicates which involve some form of *ownership*, such as $\ell \mapsto 3$, and persistent predicates, such as Hoare triples and invariants, which do not involve any exclusive ownership, but rather express *knowledge*, i.e., which can be freely duplicated. The $\Box$ modality can be used to take out the "persistent core" of a predicate inside the logic, i.e., $\Box P$ contains those resources *in* P which are duplicable. This ability can, e.g., be used for *defining* Hoare triples in Iris [10,9,11] and also for modelling intuitionistic types inside a separation logic [15,18,12].

In this paper we show how tools from categorical logic can be used to give a general account of models of higher-order separation logic with a sublogic of persistent predicates. We focus on the basic rules and basic connectives used in separation logic and do not consider the so-called specification logic, i.e., Hoare triples, and concepts such as invariants, and rules particular to specific separation logics. We aim to show how to model the basic parts of the logic in a general way, so that in future work the effort can be spent on modelling the parts particular to the logic at hand.

We make use of the standard notion of a complete Heyting algebra to model standard higher-order logic and the notion of a complete BI algebra [4] to model higher-order separation logic. We show how to construct such algebras based on a model of resources, formalized by a kind of partial commutative monoid, and different ways of singling out the idempotent (duplicable) monoid elements. We show that our abstract framework is general enough to encompass models which also include a modality for reasoning about guarded recursive predicates: by a simple change of the ambient category, from sets to the topos of trees, we recover the step-indexed notion of resource model used to model Iris [9], a state-of-the-art higher-order separation logic with guarded recursive predicates.

Overview

In Section 2 we recall the definition of BI hyperdoctrine and how models of resources can be used to construct BI hyperdoctrines. In the end of the section we

show that it is in general impossible to single out *exactly* the duplicable resources using a well-behaved modality.

In Sections 3 and 4 we study conditions under which one can obtain a logic of *persistent* predicates. We give two different constructions, one based on idempotent resources and one based on an interior operator on the resources. For the first construction, one obtains a sublogic closed under some of the logical connectives, but in general not all. In particular it can fail to be closed under universal quantification of the ambient logic. For the second construction, one obtains a sublogic closed under all the standard logical connectives of the ambient logic.

In Section 5 we show that any sublogic on duplicable predicates only, and closed under all the standard connectives must be of the form considered in Section 4. We further show that sublogics considered in Section 4 are all at most as expressive as the logic based on idempotent elements considered in Section 3, and we show necessary and sufficient conditions for this latter logic to be closed under universal quantification. These conditions are stated in terms of the structure of the idempotents of the resource monoid.

The approach using an interior operator is closely related to the core operator of Pottier [15], (though Pottier includes some additional requirements on his notion of core); and to the core operator used in Iris [9]. In Section 5 we thus show that the notion of the core arises naturally as soon as we desire a well-behaved modality in the logic.

The models described hitherto do not directly support guarded recursive predicates, as used in Iris [10,9] and other logics, e.g. Appel [1]. To support guarded recursive predicates, the types and terms of the Iris logic are modelled using a subcategory of the topos of trees [9]. The Iris model construction is based on a kind of step-indexed resource model, called a complete metric resource algebra (CMRA). The technical definition of a CMRA, recalled in Definition 6.5, perhaps looks a bit ad-hoc. In Section 6 we show that it is in fact canonical, because it can be understood as a partial commutative monoid, just in a different ambient category. Moreover, we also show that the model of Iris predicates [9] can be recovered by using the topos of trees as the ambient category in which the constructions from Sections 3 and 4 are carried out.

2 BI-algebras and BI-hyperdoctrines

In this section we begin by calling to mind the notion of a BI-hyperdoctrine, a category-theoretic definition of a model of higher-order separation logic [4]. For simplicity, we focus on so-called canonically presented BI-hyperdoctrines.

Recall that a hyperdoctrine [13] is a cartesian closed category $\mathbb{C}$ together with a *generic object* Ω and for each object $X \in \mathbb{C}$ a choice of a partial order on the hom set $\mathrm{Hom}_{\mathbb{C}}(X, \Omega)$ satisfying the following properties:

- $\mathrm{Hom}_{\mathbb{C}}(X, \Omega)$ is a complete Heyting algebra for all X.
- $\mathrm{Hom}_{\mathbb{C}}(f, \Omega) : \mathrm{Hom}_{\mathbb{C}}(X, \Omega) \to \mathrm{Hom}_{\mathbb{C}}(Y, \Omega)$ is a complete Heyting algebra homo-

morphism for all $f : Y \to X$ in $\mathbb{C}$.

- For any pair of objects $X, Y \in \mathbb{C}$ the function

$$\mathrm{Hom}_{\mathbb{C}}(\pi, \Omega) : \mathrm{Hom}_{\mathbb{C}}(X, \Omega) \to \mathrm{Hom}_{\mathbb{C}}(X \times Y, \Omega)$$

has left and right adjoints which additionally satisfy the Beck-Chevalley condition.

A complete BI-algebra [4] is a complete Heyting algebra which in addition has closed monoidal structure $(\star, \mathrel{-\!\!\star}, I)$. A *BI-hyperdoctrine* is a hyperdoctrine such that for each X the set $\mathrm{Hom}_{\mathbb{C}}(X, \Omega)$ is a complete BI-algebra and $\mathrm{Hom}_{\mathbb{C}}(f, \Omega)$ is a complete BI-algebra homomorphism.

To model logic using a hyperdoctrine we interpret types and terms of the logic as objects and morphisms of $\mathbb{C}$, whereas predicates are interpeted as elements of $\mathrm{Hom}_{\mathbb{C}}(X, \Omega)$, where X is the (denotation of the) domain of the predicate.

A canonical way to construct a hyperdoctrine is from an internal complete Heyting algebra H in $\mathbb{C}$ (this requires that $\mathbb{C}$ has sufficient structure to express what a complete Heyting algebra is). The Heyting algebra H is the generic object and the order on $\mathrm{Hom}_{\mathbb{C}}(X, H)$ is pointwise, as are all the complete Heyting algebra operations.

Similarly, a canonical way to construct a BI-hyperdoctrine is from an internal complete BI-algebra. Operations are again given pointwise.

It is well-known [4] how to model higher-order separation logic in BI-hyperdoctrines. Thus, in light of the above canonical constructions, in the remainder of this paper we focus on constructing and studying complete Heyting algebras and complete BI-algebras.

2.1 Construction of complete BI-algebras

A very general way to construct BI-algebras is from a partial commutative monoid $\mathcal{M}$ equipped with a preorder $\leq$ which interacts with the operation in a reasonable way, which we make precise below. The set of upwards-closed subsets of $\mathcal{M}$, written $\mathcal{P}^{\uparrow}(\mathcal{M})$, is a complete BI-algebra.

By varying the preorder on the monoid we can obtain models of different separation logics. In particular if the order is extension order (also called divisibility preorder) then we get a model of so-called *affine* separation logic, which enjoys the weakening rule $p \star q \vdash p$ for all propositions p, q. Recent logics such as iCAP [16], and various versions of Iris [10,9,11] have been such logics.

On the other hand if we take the discrete preorder, i.e., equality, we obtain a model which does not validate weakening. Such a logic allows for a more precise control over resources. For instance it allows one to express the property that the heap is empty, which is, e.g., used in the logics in some logics [1] to, for instance, guarantee that programs which are proved correct do not leak memory.

Most of the constructions below work for an arbitrary preorder and partial commutative monoid. In various statements we point out how additional assumptions on the preorder lead to validity of certain additional rules.

Definition 2.1 In this paper an *ordered partial commutative monoid* is a structure $(\mathcal{M}, \cdot, \mathcal{E}, \leq)$ such that $\cdot : M \times M \rightharpoonup M$ is a partial function and $\mathcal{E} \subseteq \mathcal{M}$ is the *set of units* satisfying the following axioms [3]

$$
\begin{aligned}
&m \cdot n \simeq n \cdot m \\
&(m \cdot n) \cdot k \simeq m \cdot (n \cdot k) \\
&\forall m \in \mathcal{M}, \exists e \in \mathcal{E}, m \cdot e \simeq m \\
&\forall m \in \mathcal{M}, e \in \mathcal{E}, m \cdot e \text{ defined} \Rightarrow m \cdot e \simeq m
\end{aligned}
$$

Finally $\leq$ is a preorder (a reflexive and transitive relation) on $\mathcal{M}$ satisfying monotonicity in the following sense: if $n' \leq n$ and $m' \leq m$, and if $n \cdot m$ is defined then so is $n' \cdot m'$ and $n' \cdot m' \leq n \cdot m$.

Canonical examples of orders satisfying monotonicity are extension, or divisibility, preorder, and the discrete order (equality). Recall that the extension order relates $m \leq n$ if there is a k, such that $m \cdot k \simeq n$, i.e., if n is divisible by m.

We write $m \cong n$ if $m \leq n$ and $n \leq m$. In particular when we write $m \cdot n \cong m' \cdot n'$ we also mean that both sides are defined.

Departing slightly from the usual terminology we call an element $s \in \mathcal{M}$ *idempotent* if $s \cdot s \cong s$. The motivation for this looser notion of idempotents is that if $n \cong m$ then n and m are completely exchangeable with regards to any logical operations, and thus there is no need to treat them differently in the model.

An example the reader should keep in mind is the partial monoid of finite partial functions $\mathbb{N} \rightharpoonup X$ to some set X where composition is only defined when the domains are disjoint and in that case is given by the union of the graphs of the respective functions. There is a single unit, the map with the empty domain.

Let $\mathcal{B} = \mathcal{P}^{\uparrow}(\mathcal{M})$ be the set of upwards-closed subsets of $\mathcal{M}$ with respect to the order $\leq$ and let $\mathcal{P}(\mathcal{M})$ be the power set of $\mathcal{M}$. Recall that any element $p \in \mathcal{B}$ is a union of *principal ideals* $\uparrow m = \{n \mid n \geq m\}$.

The following facts are well-known.

Fact 2.2 *The sets $\mathcal{B}$ and $\mathcal{P}(\mathcal{M})$ when ordered by subset inclusion are complete Heyting algebras. The operations on $\mathcal{B}$ are given as*

$$
\begin{aligned}
\top &= \mathcal{M} & \qquad \bot &= \emptyset \\
p \wedge q &= p \cap q & \qquad p \vee q &= p \cup q \\
\bigwedge_{i \in \mathcal{I}} p_i &= \bigcap_{i \in \mathcal{I}} p_i & \qquad \bigvee_{i \in \mathcal{I}} p_i &= \bigcup_{i \in \mathcal{I}} p_i \\
p \Rightarrow q &= \{m \mid \forall n \geq m, n \in p \Rightarrow n \in q\}
\end{aligned}
$$

[3] We use $\simeq$ for Kleene equality.

and the operations on $\mathcal{P}(\mathcal{M})$ *as*

$$\begin{aligned} \top &= \mathcal{M} & \bot &= \emptyset \\ p \wedge q &= p \cap q & p \vee q &= p \cup q \\ \bigwedge_{i \in \mathcal{I}} p_i &= \bigcap_{i \in \mathcal{I}} p_i & \bigvee_{i \in \mathcal{I}} p_i &= \bigcup_{i \in \mathcal{I}} p_i \\ p \Rightarrow q &= \{m \mid m \in p \Rightarrow m \in q\} \end{aligned}$$

Moreover there is an inclusion $\iota : \mathcal{B} \to \mathcal{P}(\mathcal{M})$ *which preserves both infima and suprema.*

Since ι preserves infima and suprema it has in particular a left adjoint, which is the closure operation $\mathrm{Cl}(\cdot) : \mathcal{P}(\mathcal{M}) \to \mathcal{B}$, which maps a subset p to the least upwards-closed subset containing p.

$$\mathrm{Cl}(p) = \{m \in \mathcal{M} \mid \exists n \in p, n \leq m\}$$

Lemma 2.3 *The closure operation preserves suprema but in general it* does not *preserve infima.*

The following is also well-known.

Fact 2.4 *The set* $\mathcal{P}(\mathcal{M})$ *is a complete BI-algebra for the following operations.*

$$\begin{aligned} I &= \mathcal{E} \\ p \star q &= \{k \mid \exists m \in p, n \in q, k = m \cdot n\} \\ p \mathrel{-\!\!\star} q &= \{n \mid \forall m \in p, m \cdot n \ \textit{defined} \Rightarrow m \cdot n \in q\} \end{aligned}$$

Proposition 2.5 *The set* $\mathcal{B}$ *is also a complete BI-algebra where the unit and multiplication are defined as follows*

$$\begin{aligned} I' &= Cl(I) \\ p \star' q &= Cl(p \star q) \end{aligned}$$

where the operations on the right-hand side are those defined in 2.4.

Proof It is easy to see $\mathrm{Cl}(p \star q) = \mathrm{Cl}(\mathrm{Cl}(p) \star \mathrm{Cl}(q))$ in $\mathcal{P}(\mathcal{M})$. Because for any $p \in \mathcal{B}$ we have $\mathrm{Cl}(p) = p$ we get for any $p \in \mathcal{B}$

$$I' \star' p = \mathrm{Cl}(\mathrm{Cl}(I) \star p) = \mathrm{Cl}(\mathrm{Cl}(I) \star \mathrm{Cl}(p)) = \mathrm{Cl}(I \star p) = \mathrm{Cl}(p) = p.$$

To show that $p \star' -$ has a right adjoint it suffices to check that it preserves suprema. This follows from the fact that $\star$ in $\mathcal{P}(\mathcal{M})$ does so and the fact that closure $\mathrm{Cl}(-)$ preserves suprema.

$$p \star' \bigvee_{i \in I} p_i = \mathrm{Cl}\left(p \star \bigvee_{i \in I} p_i\right) = \mathrm{Cl}\left(\bigvee_{i \in I} (p \star p_i)\right) = \bigvee_{i \in I} \mathrm{Cl}(p \star p_i) = \bigvee_{i \in I} (p \star' p_i)$$

□

These allow us to construct a model of basic logic of resources. Additional properties we might wish to model however depend on the interaction of $\leq$ and $\cdot$.

Lemma 2.6 *The property $p \star q \subseteq p$ is equivalent to the following property. For any $m, n \in \mathcal{M}$ such that $m \cdot n$ is defined, we have $m \cdot n \geq m$.*

Proof That the second property implies the first is straightforward.

To see the converse we have by assumption $(\uparrow m) \star (\uparrow n) \subseteq \uparrow m$. Since by definition $m \cdot n \in (\uparrow m) \star (\uparrow n)$ we get $m \cdot n \in \uparrow m$ which by definition means that $m \cdot n \geq m$.□

The condition in the previous lemma is for instance satisfied by extension ordering on a monoid, but it is not satisfied by discrete ordering.

2.2 Duplicable Predicates

As we alluded to in the introduction the main property we wish to single out with the sublogic is that a predicate P is duplicable, i.e., that it satisfies $P \Leftrightarrow P \star P$. Thus let $\mathcal{F} \subseteq \mathcal{B}$ be the set of those P which satisfy $P \star P = P$. Notice that $\mathcal{F}$ is the set of fixed points for a monotone operator $P \mapsto P \star P$ on a complete lattice $\mathcal{B}$, hence is itself a complete lattice by Knaster-Tarski's fixed point theorem, although in general not a sublattice of $\mathcal{B}$. In order to have a modality on $\mathcal{B}$ that singles out exactly $\mathcal{F}$, the inclusion of $\mathcal{F}$ into $\mathcal{B}$ must have a right adjoint, which is equivalent to the property that $\mathcal{F}$ is closed under arbitrary unions.

Lemma 2.7 *Suppose the order $\leq$ on $\mathcal{M}$ is extension order. Then $\mathcal{F}$ is closed under arbitrary unions.*

Proof It suffices to show that if $P_i = P_i \star P_i$ for any collection $i \in \mathcal{I}$ then

$$\bigcup_{i \in \mathcal{I}} P_i \subseteq \left(\bigcup_{i \in \mathcal{I}} P_i \right) \star \left(\bigcup_{i \in \mathcal{I}} P_i \right).$$

But this is immediate, since for any $i \in \mathcal{I}$ we have

$$P_i = P_i \star P_i \subseteq \left(\bigcup_{i \in \mathcal{I}} P_i \right) \star \left(\bigcup_{i \in \mathcal{I}} P_i \right).$$

□

Thus in a large class of practical cases the inclusion of $\mathcal{F}$ to $\mathcal{B}$ has a right adjoint G. However we wish the modality arising from this adjunction to be well-behaved and thus we also wish that it preserve unions, since this is needed for the modality to commute with existential quantification in the logic. Therefore we are interested in situations where G preserve unions as well. However it does not do so in many practical cases as we demonstrate below.

Example 2.8 Let $\mathcal{M}$ be the non-negative rational numbers and $\leq$ the extension order, which coincides with the usual ordering on rationals. It is straightforward to compute that $\mathcal{F} = \{\emptyset, P_0, P_{>0}\}$ where $P_0 = \mathcal{M}$ and $P_{>0} = \{q \in \mathcal{M} \mid q > 0\}$. Moreover it is easy to see that the function

$$G(P) = \begin{cases} P & \text{if } P \in \mathcal{F} \\ \emptyset & \text{otherwise} \end{cases}$$

is the right adjoint to inclusion $\mathcal{F} \subseteq \mathcal{B}$. And G does not preserve unions, since $P_{>0} = \bigcup_{q>0} \{r \mid r \geq q\}$.

Note that essentially the same counterexample, mutatis mutandis, can be constructed using the partial commutative monoid of partial finite maps with fractional permissions, as used in some program logics. One particular thing we can learn from this example is that problems are caused by duplicable elements P which are approximated entirely by non-duplicable ones. Thus one possible solution presents itself. We restrict attention to those predicates P which are generated by duplicable principal ideals. We study the set of such predicates in the next section.

3 Persistent Predicates via Idempotent Resources

The definition of $\mathcal{C}$ below is motivated by the following two properties.

Lemma 3.1 *A principal ideal $\uparrow m$ is in $\mathcal{F}$ if and only if $m \cdot m \cong m$.*

Proof Suppose $m \cdot m \cong m$. We show two inclusions. First $\uparrow m \subseteq (\uparrow m) \star (\uparrow m)$. If $x \geq m$ then also $x \geq m \cdot m$ and so $x \in (\uparrow m) \star (\uparrow m)$ because $m \cdot m$ is.

Conversely if $x \in (\uparrow m) \star (\uparrow m)$ then are y, y_1, y_2 such that $x \geq y$, $y = y_1 \cdot y_2$ and $y_1, y_2 \geq m$. Then $y \geq m \cdot m$ and so $x \geq y \geq m \cdot m \cong m$, thus $x \in \uparrow m$.

Suppose now that $\uparrow m$ is duplicable. Since $m \in \uparrow m$ there are x_1, x_2 such that $m \geq x_1 \cdot x_2$ and $x_1, x_2 \geq m$. Thus $m \cdot m$ is defined and $m \geq m \cdot m$. Finally, $m \cdot m \in (\uparrow m) \star (\uparrow m)$ and so $m \cdot m \geq m$ because we have assume that $\uparrow m$ is duplicable. We thus have $m \cdot m \cong m$. □

Similar reasoning yields the following proposition.

Proposition 3.2 *If the order $\leq$ satisfies that for any two idempotents s_1, s_2, if $s_1 \cdot s_2$ is defined then either $s_1 \leq s_1 \cdot s_2$ or $s_2 \leq s_1 \cdot s_2$ then any union $\bigcup_{s \in X} \uparrow s$ for some set of idempotents X is duplicable.*

It is perhaps slightly unfortunate that the condition on idempotents is necessary, but the condition is satisfied by a large class of monoids of practical interest. In particular, the condition is satisfied when the order is the extension order.

Let $\mathcal{C}$ be those elements p of $\mathcal{B}$ which are generated by idempotents in the following sense.

$$\mathcal{C} = \{p \in \mathcal{B} \mid \forall m \in p, \exists s \in p, s \leq m \wedge s \cdot s \cong s\}$$

Let $\delta : \mathcal{C} \to \mathcal{B}$ be the inclusion.

We have the following simple lemma.

Lemma 3.3 *$\mathcal{C}$ and δ have the following properties.*

- *δ is monotone and also reflects the order, i.e., it is a full and faithful functor.*
- *$\mathcal{C}$ has suprema inherited from $\mathcal{B}$ and δ preserves them.*
- *δ has a right adjoint $\gamma : \mathcal{B} \to \mathcal{C}$ given by*

$$\gamma(q) = \{m \in \mathcal{M} \mid \exists s \in q, s \leq m \wedge s \cdot s \cong s\}.$$

  Moreover $\gamma \circ \delta = id$.
- *The right adjoint γ preserves suprema.*
- *γ has a right adjoint ξ, given by*

$$\xi(q) = \bigcup_{p \in \mathcal{B}, \gamma(p) \subseteq q} p.$$

  Further, ξ is full and faithful.

Proof Most of this is completely straightforward. For the last part, observe that we now have $\delta \dashv \gamma \dashv \xi$ and the result follows by [7, Lemma 1.3] and the fact that δ is full and faithful, i.e., it reflects and preserves the order. □

Lemma 3.4 *$\mathcal{C}$ has all infima. They are given as*

$$\bigwedge_{i \in \mathcal{I}} p_i = \gamma \left(\bigwedge_{i \in \mathcal{I}} \delta(p_i) \right).$$

Proof First recall that we have $\gamma \circ \delta = \mathrm{id}$. We are now ready to show that $\bigwedge_{i \in \mathcal{I}} p_i$ is the infimum of all p_i. Since $\bigwedge_{i \in \mathcal{I}} \delta(p_i)$ is the infimum in $\mathcal{B}$, we have $\bigwedge_{i \in \mathcal{I}} \delta(p_i) \subseteq \delta(p_i)$ for all $i \in \mathcal{I}$. Then by definition of the proposed infimum and monotonicity of γ, we have $\bigwedge_{i \in \mathcal{I}} p_i \subseteq \gamma(\delta(p_i)) = p_i$ for all $i \in \mathcal{I}$. This shows that we have a lower bound. Suppose now there is another lower bound b for all p_i. Then $\delta(b)$ is a lower bound for all $\delta(p_i)$ and so $\delta(b) \subseteq \bigwedge_{i \in \mathcal{I}} \delta(p_i)$, since this is the infimum in $\mathcal{B}$. Using γ again we get $b = \gamma(\delta(b)) \subseteq \bigwedge_{i \in \mathcal{I}} \delta(p_i)$, concluding the proof. □

We can see from this construction that in general the inclusion δ will not preserve infima. In Section 5 we establish a necessary and sufficient condition for infima to be constructed by intersections using the structure of the idempotents of $\mathcal{M}$.

Proposition 3.5 *$\mathcal{C}$ is a complete Heyting algebra.*

Proof It follows from Lemma 3.4 that $\mathcal{C}$ has all infima. By the previous Lemma γ preserves infima, i.e., all limits. Since ξ is full and faithful with a left adjoint that preserves finite limits, $\mathcal{C}$ is (equivalent to) an exponential ideal of $\mathcal{B}$ [8, A4.3.1], which implies that $\mathcal{C}$ is cartesian closed, i.e., a Heyting algebra. □

Since we have the adjunction $\delta \dashv \gamma$ with δ full and faithful we can characterize the subset $\mathcal{C}$ of $\mathcal{B}$ using a modality $\blacksquare = \delta \circ \gamma$ on $\mathcal{B}$. That is, $\mathcal{C}$ is the set of fixed points of $\blacksquare$. Or if we view $\blacksquare$ as a comonad (i.e., interior operator) then $\mathcal{C}$ is the set of coalgebras of $\blacksquare$.

Proposition 3.6 *The $\blacksquare$ operator satisfies the following properties.*

- $\blacksquare$ *is idempotent.*
- *For all $p \in \mathcal{B}$, $\blacksquare(p) \subseteq p$.*
- $\blacksquare$ *preserves all suprema, but not infima in general.*

However as stated above in general neither δ nor $\blacksquare$ preserve infima. Thus $\mathcal{C}$ is in particular not a Heyting subalgebra of $\mathcal{B}$ [8, A4.3.1].

However in some cases it will be. In the case when the ordering on the monoid is extension ordering it is possible to show that δ and so $\blacksquare$ preserves *finite* infima. Indeed we only need to show that $p \wedge q$ is the intersection of p and q for any $p, q \in \mathcal{C}$.

Suppose $r \in p \cap q$. Then there exists an $s \in p$ such that $s \cdot s \cong s$ and $s \leq r$ and similarly there exists a $t \in q$ such that $t \cdot t \cong t$ and $t \leq r$. In particular, this means that $r = r' \cdot t$ and $r = r'' \cdot s$, by definition of the extension ordering. Then

$$s \cdot t \leq s \cdot r = s \cdot r'' \cdot s = r'' \cdot s = r$$

and since $s, t \leq s \cdot t$ we have $s \cdot t \in p \cap q$ and since $s \cdot t$ is clearly idempotent we have shown that $p \cap q \in \mathcal{C}$.

It is clear that δ preserves $\top$ and so since δ is just inclusion and (finite) infima in $\mathcal{B}$ are given by interesections, δ clearly preserves them, and so also $\blacksquare$.

This then also implies by [8, A4.3.1] that $\mathcal{C}$ is a Heyting subalgebra of $\mathcal{B}$, however it is not a complete Heyting subalgebra, that is, infinite infima are in general not given by intersections.

In the case when ordering on the monoid is discrete on the other hand it is easy to see that δ and $\blacksquare$ preserve all infima. Indeed, in such a case $\blacksquare(p)$ is the set of idempotents in p.

In general the reason $\blacksquare$ does not preserve infima is that given a collection of idempotents $s_i \leq m$ for some element m such that $s_i \in p_i$ there is no canonical choice of an idempotent $s \in \bigcap_{i \in \mathcal{I}} p_i$ such that $s \leq m$. In fact, in Section 5 we show that infima are given by intersections if and only if the set $\mathcal{I}(m) = \{s \leq m \mid s \cdot s \cong s\}$ has a greatest element. In the following section we show that given such a choice of idempotents we have that $\mathcal{C}$ is a complete Heyting subalgebra of $\mathcal{B}$ and that the $\blacksquare$ is a complete Heyting algebra morphism. Before that we discuss one of the reasons for introducing $\mathcal{C}$ and $\blacksquare$.

3.1 Idempotents and separating conjunction

One of the reasons for introducing $\blacksquare$ is that it allows us to express more properties of propositions, in particular in how $\star$ and $\wedge$ interact.

Lemma 3.7

- *If the order* $\leq$ *satisfies that for any* idempotent s *and any element* $x \in \mathcal{M}$ *such that* $x \geq s$*, the composition* $x \cdot s$ *is defined then*

$$\blacksquare(p) \wedge q \subseteq \blacksquare(p) \star q$$

- *If the order* $\leq$ *satisfies the property that for any element* x *and any* idempotent s *such that* $x \cdot s$ *is defined, then* $x \cdot s \geq s$*, then the following property holds.*

$$\blacksquare(p) \star q \subseteq \blacksquare(p) \wedge q.$$

The first condition is satisfied by extension order as well as the discrete order. The second condition is satisfied by the extension order, but not necessarily by the discrete order.

4 Persistent Predicates via an Interior Operator

In this section we show that an interior operator on $\mathcal{M}$, interior with respect to the preorder $\leq$, lifts to an interior modality on $\mathcal{B}$ which preserves suprema and infima and moreover that the set of its fixed points is a complete Heyting subalgebra of $\mathcal{B}$. By assuming additional properties relating f and the monoid operation we recover rules governing the interaction of $\star$ and $\wedge$ as in the previous section.

Let $f : \mathcal{M} \to \mathcal{M}$ be an interior operator on $\mathcal{M}$ with respect to the order $\leq$. Explicitly, this means that f is a monotone function that additionally satisfies $f(m) \leq m$ and $f(m) \leq f(f(m))$ for all $m \in \mathcal{M}$.

Note that together, the above properties imply that for all $m \in \mathcal{M}$, $f(m) \approx f(f(m))$, i.e. $f(f(m)) \leq f(m)$ and $f(f(m)) \geq f(m)$.

The function f lifts to a function f^{-1} on $\mathcal{B}$ by taking preimages. Let

$$\mathcal{L}_f = \{p \in \mathcal{B} \mid p = f^{-1}[p]\}$$

be the set of fixed points of f^{-1} and let $\Delta : \mathcal{L}_f \to \mathcal{B}$ be the inclusion. Equivalently $\mathcal{L}_f$ could be defined as $\mathcal{L}_f = \{p \in \mathcal{B} \mid p \subseteq f^{-1}[p]\}$ since $f(m) \leq m$ for all $m \in \mathcal{M}$.

Lemma 4.1 *If we consider* $\mathcal{L}_f$ *and* $\mathcal{B}$*, partially ordered by inclusion then*

- Δ *preserves and reflects the order, i.e., is a full and faithful functor.*
- $\mathcal{L}_f$ *is closed under arbitrary suprema and infima in* $\mathcal{B}$*.*
- Δ *preserves infima and suprema.*
- Δ *has a right adjoint* $\Gamma : \mathcal{B} \to \mathcal{L}_f$ *given by*

$$\Gamma(q) = f^{-1}[q]$$

Further, Γ *preserves all infima and suprema.*

Proof The fact that $\mathcal{L}_f$ has infima and suprema given by intersection follows directly from the fact that the preimage function preserves intersections and unions. The first and third items are immediate.

For the last item we proceed as follows. To show that Γ is the right adjoint to Δ we have to show that it actually maps to $\mathcal{L}_f$ and that $\Delta(p) \subseteq q \iff p \subseteq \Gamma(q)$ for $p \in \mathcal{L}_f$ and $q \in \mathcal{B}$.

To see that it maps to $\mathcal{L}_f$ is not difficult, using the fact that f is monotone and idempotent up to isomorphism: Suppose $q \in \mathcal{B}$. Since f is monotone $f^{-1}[q]$ is also upwards closed, whenever q is. Since q is upwards closed we have that $f(f(m)) \in q$ if and only if $f(m) \in q$ and so $f^{-1}\left[f^{-1}[q]\right] = f^{-1}[q]$.

Now we show $\Delta(p) \subseteq q \iff p \subseteq \Gamma(q)$.

$\Rightarrow$ Suppose $\Delta(p) \subseteq q$. Then $f^{-1}[p] \subseteq f^{-1}[q] = \Gamma(q)$ and since $p \in \mathcal{L}_f$, $p \subseteq f^{-1}[p]$, thus $p \subseteq \Gamma(q)$.

$\Leftarrow$ Suppose $p \subseteq \Gamma(q) = f^{-1}[q]$. Then $f[p] \subseteq f\left[f^{-1}[q]\right] \subseteq q$. Since q is upwards closed and using the fact that $f(m) \leq m$, this together implies $\Delta(p) = p \subseteq q$.

Since infima and suprema are given by unions and intersections respectively it is immediate that Γ preserves them. □

Lemma 4.2 *Δ has a left adjoint $\Xi : \mathcal{B} \to \mathcal{L}_f$ given by*

$$\Xi(p) = \bigcap \{q \in \mathcal{L}_f \mid p \subseteq q\}$$

Proof This is an immediate consequence of Lemma 4.1 and [2, Corollary 9.32]. □

Lemma 4.3 *Γ has a right adjoint ∇, given by*

$$\nabla(q) = \bigcup \{p \in \mathcal{B} \mid \Gamma(p) \subseteq q\}$$

Further, ∇ is full and faithful.

Proof That Γ has a right adjoint given as above follows from the Lemma 4.1 and [2, Corollary 9.32].

For the second part, observe that we now have $\Delta \dashv \Gamma \dashv \nabla$ and the result follows by [7, Lemma 1.3] and the fact that Δ is full and faithful. □

Proposition 4.4 *$\mathcal{L}_f$ is a complete Heyting* subalgebra *of $\mathcal{B}$.*

Proof By the above lemmas $\mathcal{L}_f$ has all infima and suprema. Since Γ is a right adjoint it preserves infima. Since ∇ is full and faithful with a left adjoint that preserves finite infima, $\mathcal{L}_f$ is (equivalent to) an exponential ideal of $\mathcal{B}$ [8, A4.3.1], which implies that $\mathcal{L}_f$ is cartesian closed, i.e., a Heyting algebra. □

We have shown that we have a sequence of adjunctions

$$\Xi \dashv \Delta \dashv \Gamma \dashv \nabla,$$

where Δ and ∇ are full and faithful. Further, it does not seem that Ξ preserves infima or that ∇ preserves suprema so we cannot extend this sequence of adjunctions further.

Define $\Box_f : \mathcal{B} \to \mathcal{B}$ as the interior operator arising from the adjunction $\Delta \dashv \Gamma$, explicitly

$$\Box_f(p) = \{m \in \mathcal{M} \mid f(m) \in p\} = f^{-1}[p].$$

When f is clear from the context we will write simply $\Box$ for $\Box_f$.

Lemma 4.5 *The $\Box$ operator satisfies the following properties.*

- *$\Box$ preserves all infima and suprema.*
- *$\Box(p) \subseteq p$ for all $p \in \mathcal{B}$.*
- *$\Box$ is idempotent.*

These follow immediately from properties of Δ and Γ stated above.

4.1 Separating conjunction and the $\Box$ operator

Lemma 4.6 *If the function f satisfies that for any m, $f(m) \cdot m \cong m$ then*

$$\Box(p) \wedge q \subseteq \Box(p) \star q.$$

Corollary 4.7 *If $\leq$ satisfies the conditions of Lemma 2.6 and f satisfies the condition in Lemma 4.6 then $\Box(p) \star q = \Box(p) \wedge q$ and $\Box(p) = \Box(p) \star p$.*

To summarise we have the following theorem.

Theorem 4.8 *Let $(\mathcal{M}, \cdot, \mathcal{E}, \leq)$ be an ordered partial commutative monoid and $f : \mathcal{M} \to \mathcal{M}$ an interior operator with respect to $\leq$. Then $\mathcal{B}$ is a complete BI-algebra for operations defined above. The subset $\mathcal{L}_f$ of $\mathcal{B}$ consisting of fixed points of $\Box$ is a* complete Heyting subalgebra *of $\mathcal{B}$.*

Moreover.

- *If f satisfies $f(m) \cdot m \simeq m$ for all m then $\Box(p) \wedge q \subseteq \Box(p) \star q$.*
- *If the order $\leq$ satisfies $m \leq m \cdot n$ whenever $m \cdot n$ is defined then $p \star q \subseteq p \wedge q$.*

Thus, starting with an ordered partial commutative monoid we construct a complete BI-algebra. Using this complete BI-algebra we construct a BI-hyperdoctrine which is a model of higher-order separation logic, together with a $\Box$ modality which singles out the sublogic of persistent predicates which enjoy special properties with respect to separating conjunction, as explained in the above theorem.

5 The Interior Operator is Necessary

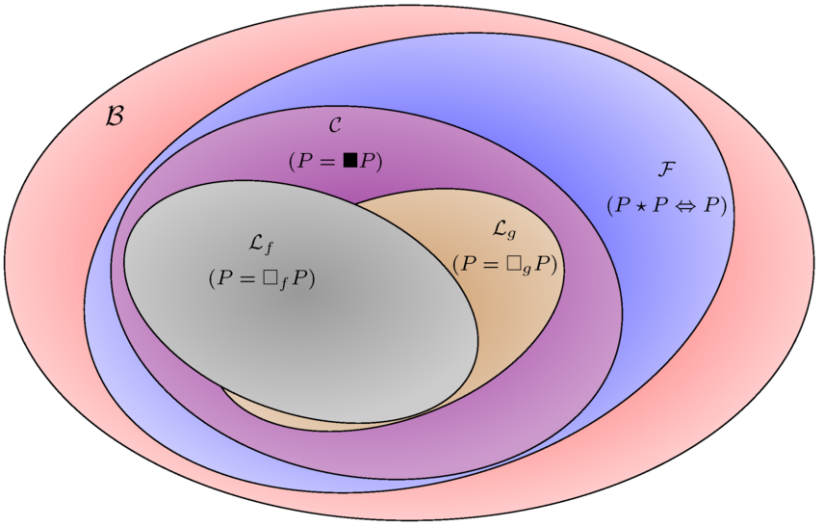
In this section we show that any complete sublattice $\mathcal{L}$ of $\mathcal{B}$ for which the right adjoint G to the inclusion also preserves unions, is of the form $\mathcal{L}_f$ for an interior operator f. Moreover, if $\mathcal{L} \subseteq \mathcal{F}$ then it must also be a subset of $\mathcal{C}$, and we establish necessary and sufficient conditions for when $\mathcal{L}_f = \mathcal{C}$ for some f. The characterisation uses the structure of the idempotents of $\mathcal{M}$.

Thus we can state a form of completeness of the class of models. If we wish a well-behaved modality on $\mathcal{B}$ then it must be of the form considered in Section 4 for

some function f. Further, if we wish that all predicates in $\mathcal{L}_f$ are duplicable then f must map into idempotents. Hence we show in particular that the notion of a core, as considered in Iris, is necessary as soon as we decide that we wish a well-behaved modality $\Box$ in the logic. [4]

Note that when we say $\mathcal{L}$ is a complete sublattice of $\mathcal{B}$ we in particular mean that infima and suprema on $\mathcal{L}$ are inherited from $\mathcal{B}$, i.e., they are intersections and unions, respectively.

In brief, if the monoid $\mathcal{M}$ satisfies the assumptions of Proposition 3.2, e.g., if it is extension order, then the complete sublattices $\mathcal{L}$ of $\mathcal{B}$, which are included in $\mathcal{F}$, can be depicted as follows.



Theorem 5.1 *Suppose $\mathcal{L}$ is a complete sublattice of $\mathcal{B}$. Let $G : \mathcal{B} \to \mathcal{L}$ be the right adjoint to the inclusion $\mathcal{L} \subseteq \mathcal{B}$. Then there exists an interior operator on $\mathcal{M}$ such that $G = f^{-1}$.*

Proof Since G is the right adjoint to inclusion and $\mathcal{L}$ and $\mathcal{B}$ are posets we have for any $p \in \mathcal{B}$ that $p \in \mathcal{L}$ if and only if $G(p) = p$.

Let us look at $\mathcal{L}$ as a topology on $\mathcal{M}$. Since it is by assumption closed under arbitrary intersections (it is an Alexandrov topology) points have least neighbourhoods. For $m \in \mathcal{M}$ let $\mathcal{N}(m) \in \mathcal{L}$ be the least neighbourhood of m. Then there exist some $X \subseteq \mathcal{M}$ such that

$$\mathcal{N}(m) = \bigcup_{x \in X} \uparrow x.$$

[4] Note that some of the proofs in this section, in particular those which construct functions f, use choice, and are thus not constructive. For some monoids $\mathcal{M}$ and orders $\leq$ the use of choice can be avoided, but we do not study such conditions.

For instance take $X = \mathcal{N}(m)$. Hence

$$\mathcal{N}(m) = G(\mathcal{N}(m)) = \bigcup_{x \in X} G(\uparrow x)$$

and so there exists $x \in X$ such that $m \in G(\uparrow x)$. But then $G(\uparrow x)$ is clearly a neighbourhood of m, and so $\mathcal{N}(m) = G(\uparrow x)$.

We now claim $G(\uparrow x) = \uparrow x$, for which it suffices to show $\uparrow x \subseteq G(\uparrow x)$. We have

$$\uparrow x \subseteq \bigcup_{x \in X} \uparrow x = \mathcal{N}(m) = G(\uparrow x).$$

Thus $\mathcal{N}(m) = \uparrow x$. Moreover it is clear that this x is unique up to $\cong$. Let $f : \mathcal{M} \to \mathcal{M}$ be a function which picks for each m an element $f(m)$ such that $\mathcal{N}(m) = \uparrow f(m)$. It is immediate that f is an interior operator.

Finally, let $p \in \mathcal{B}$. Then $p \in \mathcal{L}$ if and only if $\bigcup_{m \in p} \mathcal{N}(m) = p$, and so

$$G(p) = \bigcup \{\mathcal{N}(m) \mid \mathcal{N}(m) \subseteq p\}$$

by the adjoint functor theorem for posets and the fact that $\mathcal{N}(m)$ generate $\mathcal{L}$.

Hence $m \in G(p)$ if there exists n, such that $m \in \mathcal{N}(n)$ and $\mathcal{N}(n) \subseteq p$. But then $\mathcal{N}(n)$ is a neighbourhood of m and so $\mathcal{N}(m) \subseteq \mathcal{N}(n)$ and thus we conclude $m \in G(p)$ if and only if $\mathcal{N}(m) \subseteq p$, or in other words, if and only if $f(m) \in p$. □

5.1 Relationship between the two modalities

A natural question is how $\mathcal{C}$ and $\mathcal{L}_f$, and ■ and □ are related.

Proposition 5.2 *The set $\mathcal{L}_f$ is a subset of $\mathcal{C}$ if and only if $f(m) \cdot f(m) \cong f(m)$ for all m.*

Proof For the first part suppose first that $\mathcal{L}_f \subseteq \mathcal{C}$ and let $m \in \mathcal{M}$. Since we always have $\uparrow f(m) \in \mathcal{L}_f$ from the fact that f is monotone and idempotent, we have $\uparrow f(m) \in \mathcal{C}$, hence there exists an element $s \cong f(m)$ such that $s \cdot s \cong s$. Hence $f(m) \cdot f(m) \cong f(m)$.

Conversely suppose $f(m) \cdot f(m) \cong f(m)$ for all m and let $p \in \mathcal{L}_f$. Then clearly for any $m \in p$ there is an idempotent $f(m) \in p$ below m, thus $p \in \mathcal{C}$. □

Proposition 5.3 *If the order $\leq$ satisfies that for any two idempotents s_1, s_2, if $s_1 \cdot s_2$ is defined then either $s_1 \leq s_1 \cdot s_2$ or $s_2 \leq s_1 \cdot s_2$, then the set $\mathcal{L}_f$ is a subset of $\mathcal{F}$ (duplicable predicates) if and only if $f(m) \cdot f(m) \cong f(m)$ for all m. Thus $\mathcal{L}_f \subseteq \mathcal{F}$ if and only if $\mathcal{L}_f \subseteq \mathcal{C}$.*

Proof Suppose $f(m) \cdot f(m) \cong f(m)$ for all m. Then by Proposition 5.2 $\mathcal{L}_f \subseteq \mathcal{C}$ and so, using Proposition 3.2, we have $\mathcal{L}_f \subseteq \mathcal{F}$ as claimed.

Suppose now that $\mathcal{L}_f \subseteq \mathcal{F}$. Since f is idempotent we have $\uparrow f(m) \in \mathcal{L}_f$ for all m. Hence by Lemma 3.1 $f(m)$ is idempotent for each m. □

Lemma 5.4 *The property $\Box(p) \subseteq \blacksquare(p)$ is equivalent to $f(m) \cdot f(m) \cong f(m)$ for all m.*

Proof For the right to left direction assume $f(m) \cdot f(m) \cong f(m)$ for all m. Let $p \in \mathcal{B}$. If $m \in \Box(p)$ then $f(m) \in p$ and thus $m \in \blacksquare(p)$, since $f(m)$ is an idempotent.

Suppose now that $\Box(p) \subseteq \blacksquare(p)$ for all p. In particular $\Box(\uparrow f(m)) \subseteq \blacksquare(\uparrow f(m)) \subseteq \uparrow f(m)$. Notice that $\uparrow f(m) = \Box(\uparrow f(m))$. Thus $\blacksquare(\uparrow f(m)) = \uparrow f(m)$, which means in particular (because $f(m) \in \uparrow f(m)$) that there exists an idempotent $s \in \uparrow f(m)$ with $f(m) \leq s$. Hence $f(m) \cong s$, and thus $f(m) \cdot f(m) \cong s \cdot s \cong s \cong f(m)$. □

Proposition 5.5 *The lattices $\mathcal{L}_f$ and $\mathcal{C}$ coincide if and only if f is a retraction to the set of idempotents, i.e., if $f(m) \cdot f(m) \cong f(m)$ for all m and $f(s) \cong s$ for all idempotents s.*

Proof Suppose first that f is a retraction to the set of idempotents. Then we know from the previous lemma that $\Box(p) \subseteq \blacksquare(p)$, so it suffices to show the converse inclusion. If $m \in \blacksquare(p)$ then there is an idempotent $s \in p$ below m. But $f(s) \cong s$, so $f(m) \geq f(s) \geq s$, hence $m \in \Box(p)$.

Suppose that $\mathcal{L}_f$ and $\mathcal{C}$ coincide. Let s be an idempotent. Then $\uparrow s \in \mathcal{C}$ and so $\uparrow s \in \mathcal{L}_f$, but this means $f(s) \in \uparrow s$, thus $f(s) \geq s$, and since we always assume $f(s) \leq s$ we have $f(s) \cong s$. □

Finally we characterise exactly when such a retraction exists.

Proposition 5.6 *Let $\mathcal{I}(m)$ be the set of idempotents below m. There exists a retraction f in the sense of Proposition 5.5 if and only if $\mathcal{I}(m)$ has a greatest element for each m.*

Proof Suppose a retraction f exists. We claim $f(m) \in \mathcal{I}(m)$ is the greatest element of $\mathcal{I}(m)$. This is immediate, since if $s \in \mathcal{I}(m)$ then $s \cong f(s) \leq f(m)$ by monotonicity of f and the assumption that it is a retraction.

Suppose now that each $\mathcal{I}(m)$ has a greatest element. Let f be a function which for $m \in \mathcal{M}$ picks one of the greatest elements $f(m) \in \mathcal{I}(m)$. It is clearly monotone, idempotent, and satisfies $f(m) \leq m$, i.e., it is an interior operator. Moreover it clearly maps into idempotents and if s is an idempotent then s is the greatest element of $\mathcal{I}(s)$, and so $f(s) \cong s$. □

We now summarise the lemmas and propositions above in the useful case of monoids with extension order.

Theorem 5.7 *Let $\mathcal{M}$ be a partial commutative monoid and $\leq$ the extension order on $\mathcal{M}$. Then*

- $\mathcal{C} \subseteq \mathcal{F}$
- *Any modality $\Box$ on $\mathcal{B}$ that preserves unions and intersections and such that $\Box P$ is duplicable for any P is of the form $\Box_f$ for some interior operator f mapping into idempotents. Moreover the set $\mathcal{L}$ of fixed points of $\Box$ is a subset of $\mathcal{C}$.*

- *The lattice $\mathcal{C}$ is of the form $\mathcal{L}_f$ for some (necessarily unique up to $\cong$) f if and only if for each element $m \in \mathcal{M}$ the set of idempotents below m has a greatest element. Moreover, this is the case if and only if $\mathcal{C}$ is closed under arbitrary intersections. Finally, in such case the modalities $\Box$ and $\blacksquare$ coincide.*

Interior operators f mapping into idempotents correspond to the *core* operation of Iris. What we have shown is that the choice made in Iris is necessary if we wish to have a well-behaved sublogic of persistent predicates, all of which are duplicable. Moreover, we have shown conditions under which a largest such sublogic exists. This is exactly when the set of idempotents below m has a greatest element for any m. For many of the monoids considered in practice, and in Iris, there will in fact be a unique idempotent below every element m, and thus there will automatically be the greatest one.

6 Changing the Ambient Logic

In this section we show how some previous results found in the literature are instances of the above constructions. In particular by working in an ambient logic of the topos of trees [5] we recover the notion of complete metric resource algebra [9], from the notion of a resource algebra, thus showing in particular that the notion of a complete metric resource algebra and the model derived from it are natural and canonical.

A resource algebra is a notion of resources used in the model of the Iris program logic, which is a very general program logic which can be used for reasoning about fine grained concurrent algorithms, but also as a metalanguage for constructing models of programming languages via logical relations. Iris simplifies these by abstracting handling of resources, such as heaps, and invariants.

Definition 6.1 [[9,11]] A (unital) resource algebra is a structure $(\mathcal{M}, \cdot, \varepsilon, |\cdot|, \mathcal{V})$ such that $(\mathcal{M}, \cdot, \varepsilon)$ is a commutative monoid, $|\cdot| : \mathcal{M} \to \mathcal{M}$ called the *core* is a monotone function with respect to the extension order of $\mathcal{M}$, and $\mathcal{V} \subseteq \mathcal{M}$ is a subset of so-called *valid elements* which is downwards closed with respect to the extension order and contains the unit. Additionally the core is assumed to be an interior operator (with respect to the extension order of $\mathcal{M}$) which maps into idempotents of $\mathcal{M}$.

Remark 6.2 There is also a notion of a non-unital resource algebra [9]. These are used as intermediate steps in the construction of a unital resource algebras which is used in the construction of the model. Since we are interested in the model we only focus on unital resource algebras in connection with ordered partial commutative monoids.

A (unital) resource algebra gives rise to a complete BI-algebra by taking upwards closed subsets of *valid elements* with respect to the extension order:

$$\mathcal{P}^{\uparrow}(\mathcal{V}) = \{p \subseteq \mathcal{V} \mid \forall m \in p, \forall n \in \mathcal{V}, n \geq m \Rightarrow n \in p\}\,.$$

Remark 6.3 In the actual model of Iris one instead takes upwards closed subsets of $\mathcal{M}$ but only upwards closed with respect to the valid elements, quotiented by the relation equating two subsets if they agree on the valid elements. This is clearly order-isomorphic to $\mathcal{P}^{\uparrow}(\mathcal{V})$ defined above so we choose to work with the above presentation since it is simpler for our purposes.

The notion of a (unital) resource algebra is subsumed by the notion of a partial commutative monoid with regards to models as explained in the following proposition.

Proposition 6.4 *For any unital resource algebra $(\mathcal{M}, \cdot, \varepsilon, |\cdot|, \mathcal{V})$ there exists an ordered partial commutative monoid $(\mathcal{M}', \cdot, \mathcal{E}, \leq)$ such that the complete BI-algebras $\mathcal{P}^{\uparrow}(\mathcal{V})$ and $\mathcal{B}$ (as defined in Section 2) are isomorphic.*

Moreover the core $|\cdot|$ gives rise to an interior operation $f : \mathcal{M}' \to \mathcal{M}'$ satisfying assumptions of Theorem 4.8.

Proof Given a unital resource algebra as in the statement of the proposition define $\mathcal{M}'$ to be the set of valid elements $\mathcal{V}$. Let $\mathcal{E} = \{\varepsilon\}$ and let $\leq$ be the extension order. Finally we define the partial multiplication $\cdot$ on $\mathcal{M}'$ as a function $\cdot : \mathcal{M}' \times \mathcal{M}' \to \mathbb{S}(\mathcal{M}')$ into the set of subsingletons,[5] using the fact that the set of subsingletons is the partial map classifier [8, A2.4]. Define for $m, n \in \mathcal{M}'$ the element $m \cdot n \in \mathbb{S}(\mathcal{M}')$ as

$$m \cdot n = \{m \cdot n \mid m \cdot n \in \mathcal{V}\}$$

It is clear that with these definitions we have the equivalence of $\mathcal{P}^{\uparrow}(\mathcal{V})$ and $\mathcal{B}$ as defined above.[6]

The assumptions on the core in a unital resource algebra ensure that it restricts to a function $\mathcal{V} \to \mathcal{V}$, and by assumption the core is an interior operator which also satisfies assumptions of Theorem 4.8. □

6.1 Resource algebras in the topos of trees

The equivalence and constructions described above are valid in any topos. Hence we can read the definitions in particular in the topos of trees $\mathcal{S}$ [5], the presheaf category over the first infinite ordinal ω. Recall that objects of this category are families of sets and restriction functions

$$X_1 \xleftarrow{r_1} X_2 \xleftarrow{r_2} X_3 \xleftarrow{r_3} \cdots$$

The full subcategory of $\mathcal{S}$ on those objects whose restrictions are surjective (such objects are called *total*) is equivalent to the category of complete ordered families of

[5] Classically $\mathbb{S}(\mathcal{M}') = 1 + \mathcal{M}'$, of course, however we do not wish do use classical reasoning principles because we will later apply this result in the topos of trees, whose logic is not classical.

[6] Note that the correct definition of "$m \cdot n$ defined" is that the subsingleton $m \cdot n$ is *inhabited*.

equivalences (COFE) [5] whose objects are sets $\mathcal{X}$ together with a family of equivalence relations $=_n$ indexed by natural numbers n and satisfying suitable closure and completeness conditions. A morphism between such objects is a function which respects the equivalence relations (the non-expansive functions) in the sense that for any $n \in \mathbb{N}$ we have

$$x =_n y \Rightarrow f(x) =_n f(y).$$

Let $\mathfrak{U}$ be the category of COFEs.

Indeed, given an object X in the topos of trees the COFE $\mathcal{X}$ corresponding to it is defined as

$$\mathcal{X} = \{\{x_n\}_{n\in\mathbb{N}} \mid x_n \in X_n \wedge r_n(x_{n+1}) = x_n\}$$

which is the set of global sections of X. The equivalence relations are defined as $\{x_i\}_{i\in\mathbb{N}} =_n \{y_i\}_{i\in\mathbb{N}}$ whenever $x_n = y_n$.

With this presentation a subobject A of a total object X can be described as a family of subset $\mathcal{A}_n \subseteq \mathcal{X}$ such that $\mathcal{A}_{n+1} \subseteq \mathcal{A}_n$ for all n and additionally satisfying for any $x, y \in X$ such that $x =_n y$ then $x \in \mathcal{A}_n \Leftrightarrow y \in \mathcal{A}_n$.

Similarly, a monoid in $\mathcal{S}$ whose carrier is total can be presented as an ordinary monoid $\mathcal{M}$ equipped with a family of equivalence relations $=_n$ making $\mathcal{M}$ a COFE, such that the operation $\cdot$ is non-expansive.

With these equivalent we have the following proposition relating resource algebras and CMRAs. To state it we recall the definition of a complete metric resource algebra [9].

Definition 6.5 [CMRA] A (unital) complete metric resource algebra [9] is a tuple

$$(\mathcal{M}, \{\mathcal{V}_n\}_{n\in\mathbb{N}}, |\cdot|, \cdot, \varepsilon)$$

such that $\mathcal{M}$ is a COFE, $(\mathcal{M}, |\cdot|, \varepsilon)$ is a commutative monoid, the functions $|\cdot|$ and the multiplication $\cdot$ are non-expansive and the structure satisfies the following additional axioms.

$$\begin{aligned}
&\forall n, a, b, a =_n b \Rightarrow a \in \mathcal{V}_n \Leftrightarrow b \in \mathcal{V}_n\\
&\forall m, n, m \geq n \Rightarrow \mathcal{V}_m \subseteq \mathcal{V}_n\\
&\forall a, |a| \cdot a = a\\
&\forall a, ||a|| = |a|\\
&\forall a, b, a \leq b \Rightarrow |a| \leq |b|\\
&\forall n, a, b, a \cdot b \in \mathcal{V}_n \Rightarrow a \in \mathcal{V}_n\\
&\forall n, \varepsilon \in \mathcal{V}_n
\end{aligned}$$

where the order $\leq$ is extension order.

Remark 6.6 A unital CMRA in [9] must satisfy the following axiom

$$\forall n, a, b_1, b_2, a \in \mathcal{V}_n \wedge a =_n b_1 \cdot b_2 \Rightarrow \exists c_1, c_2, a = c_1 \cdot c_2 \wedge c_1 =_n b_1 \wedge c_2 =_n b_2.$$

This is needed to validate certain interactions between the later modality $\triangleright$ and separating conjunction, but is not essential for any of the basic rules and connectives we are considering, hence we omit it in the rest of the paper.

Proposition 6.7 *A unital complete metric resource algebra (CMRA) [9,11] is simply a unital resource algebra $(\mathcal{M}, \cdot, \varepsilon, |\cdot|, \mathcal{V})$ in the topos of trees which additionally satisfies that the carrier $\mathcal{M}$ is a total object.*

The proof of this proposition is straightforward, using the equivalences described at the beginning of this section.

The above proposition, together with Proposition 6.4, shows that the notion of a complete metric resource algebra is just a presentation of a partial commutative monoid in the topos of trees.

To claim that Proposition 6.7 together with Proposition 6.4 imply that the model of (a large part of) Iris can be recovered from the general constructions of the preceding sections we must explain in what way carrying out constructions in the internal logic of the topos of trees gives the same result as the externally constructed model. The precise statement is the following theorem.

Theorem 6.8 *Let $p : \mathcal{E} \to \mathcal{S}$ be the $\mathcal{S}$-based hyperdoctrine presented as a fibration and derived from an RA $\mathcal{M}$ internal to the topos of trees. Let $\iota : \mathfrak{U} \to \mathcal{S}$ be the inclusion of the category of COFEs to the topos of trees and suppose that $\mathcal{M}$ is in the image of ι of a CMRA $\mathcal{M}'$. There is a pullback situation*

$$\begin{array}{ccc} \mathfrak{U} \times_{\mathcal{S}} \mathcal{E} & \longrightarrow & \mathcal{E} \\ \downarrow{\scriptstyle p_I} & \lrcorner & \downarrow{\scriptstyle p} \\ \mathfrak{U} & \xrightarrow{\iota} & \mathcal{S} \end{array}$$

such that p_I is the hyperdoctrine derived from the CMRA $\mathcal{M}'$ which is used to model the Iris program logic.

Thus all the operations defined for the model of Iris derived from a complete metric resource algebra are determined from the same general principles as in the case without step-indexing. They are but a particular presentation of the general construction carried out in the topos of trees.

6.2 Adding guarded recursion

Since the topos of trees is a model of guarded recursive terms [5] all predicates in $\mathcal{S}$ come equipped with a Löb induction principle. Since predicates in the logic such as Iris are modelled as particular predicates of $\mathcal{S}$ we have that in addition to the constructs considered above, we can also model the later modality and its properties, in particular Löb induction. This modality is essential in a higher-order separation logics such as Iris and iCAP to be able to deal with so-called

impredicative invariants, which are in turn needed for verifying intricate concurrent algorithms and data structures.

7 Conclusion and Future Work

We have shown how a modicum of categorical logic can be used to give a general account of models of higher-order separation logic with a sublogic of persistent predicates. In particular, we have shown that changing the ambient category provides a systematic way to obtain models supporting guarded recursive predicates, as used, e.g., in the model of Iris, a state-of-the-art higher-order separation logic with guarded recursive predicates. In the future, we are interested in employing this systematic approach to investigate variations of models which combine linear and separation logic together with guarded recursive predicates. Such combinations of linearity and separation are useful for tracking resource usage more precisely, as, e.g., demonstrated in recent work by Tassarotti et. al. [17].

Acknowledgement

This research was supported in part by the ModuRes Sapere Aude Advanced Grant from The Danish Council for Independent Research for the Natural Sciences (FNU).

References

[1] Andrew W. Appel. *Program Logics - for Certified Compilers*. Cambridge University Press, 2014.

[2] S. Awodey. *Category Theory*. Oxford Logic Guides. OUP Oxford, 2010.

[3] Jesper Bengtson, Jonas Braband Jensen, Filip Sieczkowski, and Lars Birkedal. Verifying object-oriented programs with higher-order separation logic in coq. In *Interactive Theorem Proving - Second International Conference, ITP 2011, Berg en Dal, The Netherlands, August 22-25, 2011. Proceedings*, pages 22–38, 2011.

[4] Bodil Biering, Lars Birkedal, and Noah Torp-Smith. Bi-hyperdoctrines, higher-order separation logic, and abstraction. *ACM Transactions on Programming Languages and Systems (TOPLAS)*, 29(5):24, 2007.

[5] Lars Birkedal, Rasmus Ejlers Møgelberg, Jan Schwinghammer, and Kristian Støvring. First steps in synthetic guarded domain theory: step-indexing in the topos of trees. *Logical Methods in Computer Science*, 8(4), 2012.

[6] Adam Chlipala. The bedrock structured programming system: combining generative metaprogramming and hoare logic in an extensible program verifier. In *ACM SIGPLAN International Conference on Functional Programming, ICFP'13, Boston, MA, USA - September 25 - 27, 2013*, pages 391–402, 2013.

[7] Roy Dyckhoff and W Tholen. Exponentiable morphisms, partial products and pullback complements. *Journal of Pure and Applied Algebra*, 49:103–116, Nov 1987.

[8] Peter T. Johnstone. *Sketches of an Elephant: A Topos Theory Compendiumm vol. 1 (Oxford Logic Guides, 43)*. Oxford University Press, USA, November 2002.

[9] Ralf Jung, Robbert Krebbers, Lars Birkedal, and Derek Dreyer. Higher-order ghost state. In *Proceedings of the 21st ACM SIGPLAN International Conference on Functional Programming*, ICFP 2016, pages 256–269, New York, NY, USA, 2016. ACM.

[10] Ralf Jung, David Swasey, Filip Sieczkowski, Kasper Svendsen, Aaron Turon, Lars Birkedal, and Derek Dreyer. Iris: Monoids and invariants as an orthogonal basis for concurrent reasoning. In *Proceedings of the 42Nd Annual ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages*, POPL '15, pages 637–650, New York, NY, USA, 2015. ACM.

[11] Robbert Krebbers, Ralf Jung, Aleš Bizjak, Jacques-Henri Jourdan, Derek Dreyer, and Lars Birkedal. The essence of higher-order concurrent separation logic. In *ESOP*, 2017.

[12] Robbert Krebbers, Amin Timany, and Lars Birkedal. Interactive proofs in higher-order concurrent separation logic. In *Proceedings of the 44th ACM SIGPLAN Symposium on Principles of Programming Languages*, POPL 2017, pages 205–217, New York, NY, USA, 2017. ACM.

[13] F.W. Lawvere. Adjointness in foundations. *Dialectica*, 23:281–296, 1969.

[14] Zhaozhong Ni and Zhong Shao. Certified assembly programming with embedded code pointers. In *Proceedings of the 33rd ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages, POPL 2006, Charleston, South Carolina, USA, January 11-13, 2006*, pages 320–333, 2006.

[15] François Pottier. Syntactic soundness proof of a type-and-capability system with hidden state. *Journal of Functional Programming*, 23(1):38–144, January 2013.

[16] Kasper Svendsen and Lars Birkedal. Impredicative concurrent abstract predicates. In *ESOP*, pages 149–168, 2014.

[17] Joseph Tassarotti, Ralf Jung, and Robert Harper. A higher-order logic for concurrent termination-preserving refinement. In *Proceedings of ESOP*, 2017.

[18] Aaron Turon, Derek Dreyer, and Lars Birkedal. Unifying refinement and hoare-style reasoning in a logic for higher-order concurrency. In *Proceedings of the 18th ACM SIGPLAN International Conference on Functional Programming*, ICFP '13, pages 377–390, New York, NY, USA, 2013. ACM.