Putting order to the separation logic jungle

Qinxiang Cao*, Santiago Cuellar†, Andrew Appel ‡
Department of Computer Science, Princeton University
* qinxiang@princeton.edu, † scuellar@princeton.edu, ‡ appel@princeton.edu
* † Equal contribution joint first authors

Abstract—Research results from so-called “classical” separation logics are not easily ported to so-called “intuitionistic” separation logics, and vice versa. Basic questions like, “can Brookes’s soundness proof of CSL be extended to intuitionistic separation logics?” “Can the frame rule be proved independently of whether the programming language is garbage-collected?” “Can amortized resource analysis be ported from one separation logic to another?” should be straightforward. But they are not. Proofs done in a particular separation logic are difficult to generalize. We argue that this limitation is caused by incompatible semantics. For example, emp sometimes holds everywhere and sometimes only on units.

In this paper, we introduce a unifying semantics and build a framework that allows to reason parametrically over all separation logics. Many separation algebras in the literature are accompanied, explicitly or implicitly, by a preorder. Our key insight is to axiomatize the interaction between the join relation and the preorder. We prove every separation logic to be sound and complete with respect to this unifying semantics. Further, our framework enables us to generalize the soundness proofs for the frame rule and CSL. It also reveals a new world of meaningful intermediate separation logics between “intuitionistic” and “classical”.

I. INTRODUCTION

Separation logic, introduced at the turn of the millennium by Reynolds [30], has led to tremendous progress in modular verification in a multitude of applications: for reasoning about multiple languages, including those with C-like (malloc/free) or Java-like (garbage-collected) memory model; for reasoning about concurrency; for amortized resource analysis; or for reasoning about garbage-collected languages. Other works of concurrent separation logic proved by Brookes [7] does not naturally extend to garbage-collected languages. Other works that are hard to extend include the discussion of preciseness and the conjunction rule [24], [14], and recent advances in logics for concurrency [20].

The main difficulty in unifying the two worlds is that authors use different and sometimes incompatible semantics. For instance, one side enforces that emp holds only on units, while for the other side it is simply equal to True. In fact, even within each side there are several conflicting semantics.

Ideally, the semantics of the separating operators would be given by the intuitive definitions

\[ m \models \varphi \star \psi \iff \exists m_1, m_2 \text{ s.t. } (m_1, m_2, m) \]

\[ m_1 \models \varphi \text{ and } m_2 \models \psi \]  

\[ m \models \varphi \rightarrow \psi \iff \text{for any } m_1, m_2, \text{ if } (m, m_1, m_2) \]

\[ \text{then } m_1 \models \varphi \text{ implies } m_2 \models \psi \]  

where \( \oplus \) is a join operation on the underlying model, called a separation algebra [9]. Unfortunately, when the objects of interest are not just simple heaplets—when step-indexing [15] or topology [29] §3 or amortized analysis [4] is involved—authors have had to define more intricate semantics; the simple semantics is (apparently) unsound. We explain this in section V-D. Not only are these “messier” semantic definitions inconvenient, they cause nonportability of results.

In this paper we show that all of those semantics are in fact instances of a unifying flat semantics over the generalized ordered separation algebras. An ordered separation algebra is just a separation algebra together with a preorder \( \leq \).

Ordered separation algebras are not a new idea. In fact, the heap model defined by Reynolds in his first paper on separation logic [30] is ordered by heap extension. Similarly,
the monotonic state of Pilkiewicz and Potter \cite{27} and the amortized resource of Atkey \cite{4} are also ordered. Furthermore, Pym et al. \cite{29}, Galmiche et al. \cite{13} and Jensen \cite{18} have used ordered separation algebras explicitly as their semantic model. Despite this common trend, orders have been used to define different semantics, tailored to specific models, and no unification had yet been discovered.

**Contributions.** We argue that all models of separation logic are ordered separation algebras (section \cite{V-A}) and we show that all semantics in the literature, to the best of our knowledge, can be formulated as instances of our flat semantics (section \cite{V-F}). Our unification holds for the “classical” side, the “intuitionistic” side and all separation logics in between.

By this unifying semantics, we establish a correspondence between all different separation logics and classes of ordered separation algebras. We prove that any separation logic is sound and complete w.r.t. flat semantics in its corresponding class of models (section \cite{V-I}).

We generalize two theoretical applications of separation logics (section \cite{VIII}). We show that the frame rule (given frame property) and CSL are sound parametrically on different separation logic semantics.

All the definitions, propositions, lemmas and theorems in this paper have been formalized in Coq. We will often omit uninteresting proofs, but a curious reader can find them in our publicly available development.

**II. RELATED WORK**

Ishtiaq and O’Hearn \cite{17} showed a modal translation ($\triangleright^o$) that embeds separation logic without excluded middle \cite{30} into their logic with excluded middle. The translation preserves validity; i.e.

$$s, h \models^{30} P \iff s, h \models^{17} P^o .$$

The translation is enough to show the soundness of both logics with respect to their model, but not for other models. Of particular interest, they show the frame rule is sound w.r.t. operational semantics with the frame property. We extend the soundness of the frame rule, parametrically on different semantic models.

Brookes \cite{21}’s soundness proof of concurrent separation logic (CSL) is based on a classical separation logic. We extend his proof parametrically on all separation logics.

Brotherston and Villard \cite{8} prove the parametric completeness of classical separation logics. Our soundness and completeness proof generalizes their result to nonclassical logics.

Jensen \cite{18} has a thorough review of separation logics and separation algebras. The chapter is expositional, but he explicitly imposes an order on each separation algebra. Our presentation of separation logic semantics is closely related to his. In particular, his Propositions 3.6 and 3.7 correspond to our definitions \cite{27}1 and \cite{27}2, of which he writes:

The conditions of neither Proposition 3.6 nor Proposition 3.7 generalise the conditions of the other, so perhaps a unifying theorem is still waiting to be discovered.

Our theorem \cite{38} is exactly that theorem.

**III. TAXONOMY OF SEPARATION LOGIC**

In this section, we formally define the scope of separation logics based on their proof systems. In turn, this allows us to group the separation logics to provide parametric proofs of soundness and completeness in section \cite{VI}. This classification will hopefully dispel the unfortunate nomenclature (classical vs. intuitionistic) that has been prevalent.

**A. Defining separation logic**

In this paper, we take the syntax below to be the assertion language of separation logic.

**Definition 1** (Separation logic syntax). For a given set of atomic assertions $\Sigma$, we use $\mathcal{L}(\Sigma)$ to represent the smallest language with all following assertions:

$$\varphi ::= p(\in \Sigma) | \varphi_1 \land \varphi_2 | \varphi_1 \lor \varphi_2 | \varphi_1 \rightarrow \varphi_2 | \bot |$$

$$\varphi_1 * \varphi_2 | \varphi_1 \leftarrow \varphi_2$$

As usual, we use the following connectives as abbreviations:

$$\varphi_1 \leftrightarrow \varphi_2 \triangleq (\varphi_1 \rightarrow \varphi_2) \land (\varphi_2 \rightarrow \varphi_1)$$

$$\neg \varphi \triangleq \varphi \rightarrow \bot$$

$$\top \triangleq \bot \rightarrow \bot$$

Our assertion language does not explicitly include emp. In section \cite{V-F} we will consider languages with $\text{emp} \in \Sigma$ and discuss the semantics of $\text{emp}$ in detail. In the rest of the paper, we won’t explicitly specify whether $\text{emp} \in \Sigma$ if it can be implied from context.

Reynolds \cite{30} originally introduced separation logics with an explicit constructor for atomic heaplets, $\cdot \rightarrow \cdot$. Since separation logic is now often used to reason about nonheap resources, we omit such constructor but allow it in $\Sigma$. We will define separation logics based on a Hilbert-style proof system; that is a set of axioms and proof rules. Intuitionistic propositional logic is defined by the the rules IP in fig. \cite{1} EM, GD and WEM in fig. \cite{2} are optional axioms for propositional logic. A logic with EM is classical, while the weaker axioms GD and WEM give rise to intermediate logics. Many other similar axioms give rise to more intermediate logics; we omit them here for the sake of space.

The axioms and rules for separation logic (SL) are in fig. \cite{4} commutativity, associativity, adjoint property of the separating operators and monotonicity of separation over implication. The double line in $\text{ADJ}$ implies the derivation works both ways. The axioms $\ast E$, EXT and EMP in fig. \cite{4} are optional: $\ast E$ is the elimination rule of the separating conjunction; EXT enforces that every predicate can be extended in the separation sense of $\ast$; and EMP is the property that a logic has $\text{emp} \in \Sigma$ and $\text{emp}$ is the unit of the separating conjunction.

**Definition 2** (Separation logic). A proof system is a separation logic if it contains all axioms and rules in IP + SL.

Even with the minimum set of axioms and proof rules (IP + SL), many useful properties can be derived. For example,
The unfortunate misnomer not only hides the fact that there are separation logics without *E and without EM, but also that there are separation logics with an intermediate propositional logic, i.e., that is neither intuitionistic nor classical. Such logics have a weaker version of EM from fig. 2 such as the axiom WEM, which gives rise to a De Morgan Logic; or the axiom GD, which gives rise to a Gödel-Dummett logic.

Other nomenclatures have been proposed, such as Linear/Affine [21] (even though separation logic is not a linear logic [17, 31]) or BBI/Affine [18]. We use the proof system to classify separation logics in a precise way. There are three characteristics that define a separation logic:

1) The propositional logic: A separation logic restricted to its propositional connectives is a propositional logic determined by the optional axioms of figure 2. WEM induces a De Morgan logic [32]; GD induces a Gödel-Dummett logic [12]; EM induces classical logic; and without any of the axioms the logic is intuitionistic. Other intermediate axioms (weaker than EM) will give rise to a corresponding intermediate logic in the same way.

2) The separating elimination: A separation logic with *E is garbage-collected and one without it malloc/free. This nomenclature derives from the application: logics without *E were first used in languages with explicit memory deallocation while logics with *E are used with a garbage collector.

3) Empty or separating extension: we say a separation logic is with empty, with separating extension or without separating extension if it has EMP, EXT or none, respectively. Since EMP implies EXT, the three categories are sufficient. In most of this paper we will focus on logics with EMP, which are by far the most common.

Table 5 illustrates the classification for several examples.

C. Degenerate separation logic

Reynolds [30] and Ishiataq and O’Hearn [17] informally postulated that EM and *E are “incompatible”. It turns out that a classical garbage-collected separation logic with emp collapses to classical propositional logic. We formalize that result in the following theorem.

**Theorem 3.** In a separation logic Γ which has EM, *E and EXT, the separating connectives collapse to the propositional ones, i.e. for any φ and ψ:

\[ \Gamma \vdash \varphi \rightarrow \varphi \land \psi \]
\[ \Gamma \vdash (\varphi \rightarrow \psi) \leftrightarrow (\varphi \rightarrow \psi) \]

**Proof.** We first show that \( \Gamma \vdash \varphi \rightarrow \varphi \land \psi \) holds for any \( \varphi \):

\[ \Gamma \vdash \varphi \rightarrow \varphi \land \psi \]
\[ \Gamma \vdash \varphi \rightarrow \varphi \land \psi \]

\[ \Gamma \vdash \varphi \land \psi \rightarrow \varphi \lor \psi \]
\[ \Gamma \vdash \varphi \land \psi \rightarrow \varphi \lor \psi \]

\[ \Gamma \vdash \varphi \lor \psi \rightarrow \varphi \land \psi \]
\[ \Gamma \vdash \varphi \lor \psi \rightarrow \varphi \land \psi \]

\[ \Gamma \vdash \varphi \land \psi \rightarrow \varphi \lor \psi \]
\[ \Gamma \vdash \varphi \land \psi \rightarrow \varphi \lor \psi \]

\[ \Gamma \vdash \varphi \lor \psi \rightarrow \varphi \land \psi \]
\[ \Gamma \vdash \varphi \lor \psi \rightarrow \varphi \land \psi \]

\[ \Gamma \vdash \varphi \rightarrow \varphi \land \psi \rightarrow \varphi \lor \psi \]
\[ \Gamma \vdash \varphi \rightarrow \varphi \land \psi \rightarrow \varphi \lor \psi \]

\[ \Gamma \vdash \varphi \land \psi \rightarrow \varphi \lor \psi \rightarrow \varphi \land \psi \]
\[ \Gamma \vdash \varphi \land \psi \rightarrow \varphi \lor \psi \rightarrow \varphi \land \psi \]

\[ \Gamma \vdash \varphi \lor \psi \rightarrow \varphi \land \psi \rightarrow \varphi \lor \psi \]
\[ \Gamma \vdash \varphi \lor \psi \rightarrow \varphi \land \psi \rightarrow \varphi \lor \psi \]

\[ \Gamma \vdash \varphi \land \psi \rightarrow \varphi \lor \psi \rightarrow \varphi \land \psi \]
\[ \Gamma \vdash \varphi \land \psi \rightarrow \varphi \lor \psi \rightarrow \varphi \land \psi \]
Then we can prove $\vdash \varphi \land \psi \rightarrow \varphi \ast \psi$ as follows.
\[
\begin{align*}
\vdash \varphi \land \psi & \rightarrow (\varphi \land \psi) \ast (\varphi \land \psi) \\
\vdash (\varphi \land \psi) \ast (\varphi \land \psi) & \rightarrow \varphi \ast \psi.
\end{align*}
\]
The converse, $\vdash \varphi \ast \psi \rightarrow \varphi \land \psi$, follows directly from *E. Finally, $\vdash (\varphi \rightarrow \psi) \leftrightarrow (\varphi \rightarrow \psi)$ follows from the above and the adjoint property.

**Corollary 4.** In a separation logic with EM, *E and EMP, the separating connectives collapse to the propositional ones.

### IV. Background

#### A. Separation Algebra

The semantics of all separation logics are built on structures (e.g., heaps, histories, amortized resources) that share common properties such as associativity and commutativity.

**Definition 5** (Commutativity). Given a set $M$, the join relation $\oplus \subseteq M \times M \times M$ is commutative iff for all $m_1$, $m_2$, and $m$,

\[\oplus(m_1, m_2, m) \implies \oplus(m_2, m_1, m).\]

**Definition 6** (Associativity). Given a set $M$, the join relation $\oplus \subseteq M \times M \times M$ is associative iff for all $m_x$, $m_y$, $m_z$, $m_{xy}$ and $m_{xyz}$,

\[\text{if } \oplus(m_x, m_y, m_{xy}) \text{ and } \oplus(m_x, m_y, m_{xyz}) \text{ then there exists } m_{xyz} \text{ such that }\]

\[\oplus(m_x, m_{yz}, m) \text{ and } \oplus(m_z, m_{yz}, m)\]

Calcagno, O’Hearn and Yang \[9\] first called such structures $(M, \oplus)$ *separation algebras* and proposed them to be also cancellative, functional\[\dagger\] and with a unit. Since then, the definition has been revisited several times \[11,14,19,23\]. We follow Brotherston and Villard \[8\] in that the $\oplus$ relation is neither functional nor cancellative. We depart from them in that we require no units, so we only require a separation algebra to be commutative and associative.

Using the algebras, Calcagno, O’Hearn and Yang define the semantics of separation logic as in definition \[7\]. This is the most widely used and intuitive definition. Foreshadowing the stronger definition \[22\], we will call them weak semantics.

**Definition 7** (Weak Semantics).

\[m \vDash \varphi \ast \psi \triangleq \text{exists } m_1 m_2 \text{ s.t. } \oplus(m_1, m_2, m)\]

and $m_1 \vDash \varphi$ and $m_2 \vDash \psi \quad (7.1)$

\[m \vDash \varphi \rightarrow \psi \triangleq \text{for any } m_1 m_2, \text{ if } \oplus(m_1, m_2, m) \text{ then } m_1 \vDash \varphi \text{ implies } m_2 \vDash \psi \quad (7.2)\]

$\dagger\oplus(a, b, c)$ and $\oplus(a, b, c')$ implies $c = c'$.

#### B. Kripke semantics for intuitionistic logic

The Kripke semantics \[22\] for propositional language is defined on Kripke models.

**Definition 8** (Kripke model). For an intuitionistic logic with atomic proposition set $\Sigma$, a Kripke model is a tuple $(M, \leq, J)$ in which

1) $\leq$ is a preorder on $M$

2) $J \in M \rightarrow P(\Sigma)$ is an interpretations of atomic propositions and is monotonic, i.e., for any $m, n \in M$, if $m \leq n$ then $J(m) \subseteq J(n)$.

We also call such tuple $(M, \leq)$ a Kripke structure.

**Definition 9** (Kripke Semantics). Given a Kripke model $(M, \leq, J)$, the satisfaction relation $(\cdot \vDash_{(M, \leq, J)} \cdot)$ is defined as follows (when the Kripke model is unambiguous from the context, we will omit it for conciseness)

\[m \vDash p \triangleq p \in J(m)\]

\[m \vDash \bot \triangleq \text{never}\]

\[m \vDash \varphi \land \psi \triangleq m \vDash \varphi \text{ and } m \vDash \psi\]

\[m \vDash \varphi \lor \psi \triangleq m \vDash \varphi \text{ or } m \vDash \psi\]

\[m \vDash \varphi \rightarrow \psi \triangleq \text{for any } m_0, \text{ if } m \leq m_0 \text{ then } m_0 \vDash \varphi \text{ implies } m_0 \vDash \psi\]

Intuitionistic logic is sound and complete w.r.t. this semantics \[22\]. Moreover, since the identity relation is a trivial preorder, classical logic is sound and complete w.r.t. Kripke semantics in all models with a discrete order.

#### V. Model and Semantics

In this section, we introduce a framework to define flat semantics on ordered separation algebras which unifies all different semantics of separation logic (we know of) in the literature.

We introduce ordered separation algebras, define properties that they and their elements may have (increasing, unital, residual, upwards-closed, downwards-closed). We show examples from the literature of algebras with and without these properties. We show ways of constructing downwards-closed upwards-closed algebras. We demonstrate examples from the literature of different semantics of separation logic and we show that they are all equivalent to instances of flat semantics.

#### A. Ordered separation algebras

Using a Kripke semantics is a motivation to impose an order over separation algebras and in fact this is a very common practice (implicitly or explicitly). For example, the heap model defined by Reynolds in his first paper of separation logic \[30\] is ordered by heap extension\[\dagger\] and the resources of a monotonically increasing counter \[27\] \[19\] are ordered by the order of natural numbers.

More interesting examples are those that impose an execution order. For instance, states that are step indexed \[2\] will be ordered by the index, which decreases with execution. In

\[\dagger\text{Heap extension is actually the reverse order for the semantics.}\]
the same vein, Pottier \cite{Pottier2011} has an active execution order\footnote{Pottier also adds a passive execution order which constitutes what he calls a monotonic separation algebra. The idea is similar but goes in a different direction, aiming for a type system and not a separation logic.} for elements of his algebra. The separation algebra by Jung et al. \cite{Jung2001} is ordered both by heap extension and step index.

Since the identity relation is also a preorder, it is not overly restrictive to require separation algebras to be ordered—any separation algebra is trivially ordered by the discrete order. With that in mind we define ordered separation algebra as a more expressive way to view separation algebras.

**Definition 10** (Ordered separation algebra). An ordered separation algebra is a tuple \((M, \leq, +)\), where \(M\) is the carrier set, \(\leq\) is a preorder on \(M\) and \(\oplus \subseteq M \times M \times M\) is a three-place relation that is commutative and associative.

If the order is irrelevant or can be inferred by context we will simply call it a separation algebra. Also, we call a tuple \((M, \leq, \oplus, J)\) an extended Kripke model if \((M, \leq, \oplus)\) is an ordered separation algebra and \((M, \leq, J)\) is a Kripke model.

The most obvious example of ordered separation algebras are heaps, which are most commonly discrete or ordered by heap extension (see tables \ref{table:discrete} and \ref{table:ordered} for details).

**Example 11** (Heaps). For a set of addresses \(\text{adr}\) and a nonempty set of values \(V\), a heap is a partial function \(H_V : \text{adr} \rightarrow V\) with join defined by

\[
\oplus_{H_V} \triangleq \{(h_1, h_2, h) \mid h_1 \uplus h_2 = h\}
\]

Where \(\uplus\) is the disjoint union of maps.

\[1\] Discrete heaps are used for reasoning about malloc/free languages. Their order is the diagonal relation:

\[\Delta_2 \triangleq \{(h, h) \mid h \in H_V\}\]

\[2\] Monotonic heaps are used for garbage-collected languages. Their order is monotonic on the domain:

\[\sqsubseteq_{H_V} \triangleq \{(h_1, h_2) \mid \text{dom } h_1 \subseteq \text{dom } h_2 \text{ and } \forall x \in \text{dom } h_2, h_1 x = h_2 x\}\]

This order is often referred to as heap extension.

Many other resources are ordered separation algebras, such as ordered monoids, which are used for amortized resource analysis \cite{Dockins2012}. We show two examples on the natural numbers and positive rationals:

**Example 12** (Ordered monoids). Let \(+_N\) and \(\leq_N\) be the usual sum and order of \(\mathbb{N}\) and \(+_\mathbb{Q}\) and \(\geq_\mathbb{Q}\) the usual sum and downwards-order for \(\mathbb{Q}\). The following ordered monoids are ordered separation algebras

\[1\] Inverted sum \(\mathbb{Q}^+\): \((\mathbb{Q}^+, \geq_\mathbb{Q}, +)\). We remove the 0 to emphasize that units are unimportant.

\[2\] Sum \(\mathbb{N}\): \((\mathbb{N}, \leq_N, +)\).

**B. Increasing elements and algebras**

Definition \ref{def:increasing} imposes almost no constraints on \(\leq\) other than being a preorder. Particularly, there is no relation between \(\oplus\) and \(\leq\). We do this in order to be as general as possible and we will revisit this goal in section \ref{section:increasing}. However, it is worth spelling out an intuitive and important connection between the two relations. In some separation algebras (like ex.\ref{ex:product}), joining two heaps always results in a larger heap. We capture this property in the following definitions.

**Definition 13** (Increasing element). For a separation algebra \((M, \leq, \oplus)\), an increasing element \(e \in M\) is one such that for all \(m, n \in M\), if \(\oplus(e, m, n)\) then \(m \leq n\).

**Definition 14** (Increasing separation algebra). A separation algebra is increasing if all its elements are increasing.

The relevance of increasing elements will be made clear throughout the paper; it is used for the semantics of emp (section \ref{section:increasing}) and it is key for defining separation logics for garbage-collected languages (thm \ref{thm:increasing}).

**C. The algebra of ordered separation algebras**

We follow Dockins et al. \cite{Dockins2012} to show that the definition of ordered separation algebra is compositional. We will rely on this composition to construct future examples (ex.\ref{ex:product}) prop. \ref{prop:composition}. More operations on ordered separation algebras, such as the option algebra and the ordered-disjointed sum, can be found in our Coq development.

**Lemma 15** (Sum, product and exponential OSA). For two ordered separation algebras \((M_1, \leq_1, \oplus_1)\) and \((M_2, \leq_2, \oplus_2)\) and a set \(S\), the following are ordered separation algebras:

- The sum algebra: \((M_1 \uplus M_2, \leq_1 \uplus \leq_2, \oplus_1 \uplus \oplus_2), \text{ where } \uplus \text{ is the disjoint union.}\)
- The product algebra: \((M_1 \times M_2, \leq_1 \times \leq_2, \oplus_1 \times \oplus_2)\)
- The exponential algebra: \((S \rightarrow M, \leq_{S\rightarrow M}, \oplus_{S\rightarrow M}), \text{ defined by }\)

\[
\begin{align*}
& f \leq_{S\rightarrow M} g \triangleq \forall x \in S. f x \leq g x \\
& \oplus_{S\rightarrow M}(f, g, h) \triangleq \forall x \in S. \oplus(f x, g x, h x)
\end{align*}
\]

**Lemma 16** (Increasing compositions). Moreover, if the original algebras are increasing then so is their sum, product and exponential algebras.

We will later build examples \ref{ex:product}, \ref{ex:sum} and \ref{ex:exp} as products.

**D. Extending Kripke semantics**

It is a fundamental property of Kripke semantics that the denotations of all assertions is monotonic, not just those of atomic assertions. More precisely.

\[
\text{If } n \leq m \text{ then } n \models \varphi \text{ implies } m \models \varphi
\] (1)

The property is critical in proving soundness of intuitionistic logic and any of its extensions (e.g. intuitionistic first order logic or intuitionistic modal logic).

Therefore, in extending Kripke semantics with separating connectives, property (1) must be preserved. To do so, if separating conjunction is defined as in \ref{def:increasing}, then the separation algebra must be upwards-closed:
Definition 17 (Upwards-closed separation algebra). An ordered separation algebra \((M, \leq, \oplus)\) is upwards-closed if the join relation is upwards-closed with respect to the order. In other words, for all \(m_1, m_2, m\) and \(n\):

If \(\oplus (m_1, m_2, m)\) and \(m \leq n\),
then there exist \(n_1\) and \(n_2\) s.t.
\(\oplus (n_1, n_2, n)\) and \(m_1 \leq n_1\) and \(m_2 \leq n_2\).

Similarly, if separating implication is defined as in (7.2),
then we must require our separation algebra to be downwards-closed:

Definition 18 (Downwards-closed separation algebra). An ordered separation algebra \((M, \leq, \oplus)\) is downwards-closed if the join relation is downwards-closed with respect to the order. In other words, for all \(m_1, m_2, m, n_1\) and \(n_2\):

If \(\oplus (m_1, m_2, m)\), \(n_1 \leq m_1\) and \(n_2 \leq m_2\)
then there exists \(n\) s.t. \(\oplus (n_1, n_2, n)\) and \(n \leq m\).

The two definitions are justified by theorem 19. Lemma 20 shows that both properties are satisfied by algebras with trivial order and lemma 21 shows that both properties are preserved by the compositions in lemma 15.

Theorem 19 (Weak semantics monotonicity). For any assertions \(\varphi\) and \(\psi\) with monotonic denotation,

1) in a upwards-closed separation algebras the weak denotation of \(\varphi \land \psi\) is monotonic.
2) For downwards-closed separation algebras the weak denotation of \(\varphi \land \psi\) is monotonic.

Lemma 20. A separation algebra with a discrete order is upwards-closed and downwards-closed.

Lemma 21. If the original algebras are upwards- or downwards-closed then so is the sum, product and exponential algebras.

Unfortunately, many separation algebras don’t satisfy requirements 17 and 18. For instance, the following example describes a heap where short is two bytes long. It is motivated by the treatment of multibyte locks in VST 11 pp. 366-7.

Example 22 (Typed Heaps). Let a typed heap be \(\mathcal{H}_T : \mathbb{N} \rightarrow \{\text{char}, \text{short}_1, \text{short}_2\}\), such that \(H(n) = \text{short}_1\) iff \(H(n+1) = \text{short}_2\). Define \(\oplus\) as the typical heap addition (i.e. disjoint union map union) and define the order as follows

\[ H_1 \sqsubseteq_{\mathcal{H}_T} H_2 \triangleq \text{for all } n \in \text{dom } H_1, n \in \text{dom } H_2 \text{ and } H_1(n) = H_2(n) \text{ or } H_1(n) = \text{char} \]

Then \((\mathcal{H}_T, \sqsubseteq_{\mathcal{H}_T}, \oplus)\) is an ordered separation algebra which is downwards-closed but not upwards-closed.

In order to keep separation algebras as inclusive as possible, it is desirable to avoid requirements 17 and 18. With that goal, stronger semantics of \(\ast\) and \(\rightarrow\) have been proposed 18 to be monotonic by design. Theorem 24 justifies the choice.

Definition 23 (Strong semantics).

\[ m \models \varphi \land \psi \triangleq \exists m_0, m_1, m_2 \text{ s.t.} \]
\[ m_0 \leq m, \ominus (m_1, m_2, m_0) \text{ and} \]
\[ m_1 \models \varphi \text{ and } m_2 \models \psi \]

\[ m \models \varphi \land \psi \triangleq \text{for any } m_0, m_1, m_2 \]
\[ \text{if } m \leq m_0, \ominus (m_0, m_1, m_2) \]
\[ \text{then } m_1 \models \varphi \text{ implies } m_2 \models \psi \]

Theorem 24 (Strong semantics monotonicity). For any assertions \(\varphi\) and \(\psi\), if their denotations are both monotonic, then

1) strong semantics of separating conjunction (23.1) ensures the denotation of \(\varphi \land \psi\) to be monotonic
2) strong semantics of separating implication (23.2) ensures the denotation of \(\varphi \land \psi\) to be monotonic.

Alas, it is not possible to use both strong semantics 23.1 and 23.2. As we show with the following lemma, separation logic is unsound w.r.t such strong semantics in very general separation algebras.

Example 25. Consider the following separation algebra, where \(\cdot\) represents string concatenation:

- Let \(M\) be all strings composed of \(a, b, c\) and \(+\).
- Let \(\oplus (s_1, s_2, s_3) \mapsto s_1 \cdot s_2 = s_3\).
- Let \(\leq \triangleq \{\{(bc, b + c)\} \cup \{(s, s)\} | s \in M\}\).

Lemma 26. Separation logic is unsound w.r.t. the semantics of \(\ast\) and \(\rightarrow\) defined by (23.1) and (23.2).

Proof. Define an extended Kripke model \((M, \leq, \oplus, \text{id})\), where \(M, \leq, \oplus\) are defined as in 23.5 and the interpretation \text{id} is the identity. Then, under the any semantics with (23.1) and (23.2), \(ab + c \models a \ast (b + c)\) but \(ab + c \not\models (a \ast b) + c\). Thus \(*\text{ASSOC}\) is unsound with respect to this algebra.

Consequently, one must accept at least one restriction (i.e. upwards-closed or downwards-closed) over separation algebras. We summarize all viable separation logic semantics below and we will consider their soundness in section VI.

Definition 27 (Separation Logic semantics). Over the propositional connectives (i.e. \(\land, \lor, \rightarrow, \bot\)), the semantics of separation logic is defined by definition 9. The semantics of the separating connectives is then defined as follows

1) In upwards semantics \((\models \land, \cdot)\), the conjunction is weak and implication strong (i.e. 7.1 and 7.2);
2) In downwards semantics \((\models \lor, \cdot)\) the conjunction is strong and implication weak (i.e. 23.1 and 23.2).
3) In flat semantics \((\models \land, \lor)\), both definitions are weak (i.e. 7.1 and 7.2).

Lemma 28. If a separation algebra is upwards-closed, the weak semantics of \(\ast\) on it is equivalent to the strong semantics. If a separation algebra is downwards-closed, the weak semantics of \(\rightarrow\) on it is equivalent to the strong semantics.

Corollary 29. For separation algebras with discrete order, upwards semantics, downwards semantics and flat semantics are equivalent.
A flat semantics is by far the most common and intuitive; it is used whenever the algebra is discrete, as suggested by corollary \[29\] and was used in Reynolds’s original logic \[30\]. The upwards semantics is also fairly common, since it maintains the familiar semantics of \(*\) which is commonly associated with separation logic; it is used by \[11\]. The downwards semantics appears in \[13, 29\].

To the best of our knowledge, all semantics are covered by \[27\] although in some cases it is not immediately obvious \[4, 5, 6\]. The following example is one such case.

**Example 30** (Step-indexed heap). Consider a heap (unordered) separation algebra \((\mathcal{H}, \oplus_{\mathcal{H}})\), the following is a semantics of separation logic defined on \(\mathbb{N} \times \mathcal{H}\):

\[
(i, h) \models \varphi \iff \exists h_1, h_2 \text{ s.t. } \oplus_{\mathcal{H}} (h_1, h_2, h)
\]

and \((i, h_1) \models \varphi\) and \((i, h_2) \models \varphi\).

\[
(i, h) \models \varphi \lor \psi \iff \text{for any } i \geq j \text{ and any } h_1, h_2
\]

if \(\ominus (h_1, h_2)\)

then \((j, h_1) \models \varphi\) implies \((j, h_2) \models \psi\).

Such models \[21, 5, 6\] are used to define mixvariant recursive predicates \[3\] inside the heap.

In fact, this semantics on step indexed heap is just a upwards semantics on a product algebra, as formalized in proposition \[32\]. It seems like a hybrid semantics: upwards for the indices (in an inverted order) and flat for the heap. But since the monotonic heap is upwards-closed, by lemma \[28\] such hybrid semantics is equivalent to a upwards semantics.

**Example 31** (Index algebra). The index algebra is denoted by \((\mathbb{N}, \geq_{\mathbb{N}}, \Delta_{\mathbb{N}})\) where \(\geq_{\mathbb{N}}\) is the downwards-order of natural numbers and the join is the diagonal relation \(\Delta_{\mathbb{N}} \triangleq \{(n, n, n) \mid n \in \mathbb{N}\}\).

**Proposition 32.** The semantics defined in ex.30 is equivalent to upwards semantics on the product algebra of \((\mathbb{N}, \geq_{\mathbb{N}}, \Delta_{\mathbb{N}})\) (ex.31) and \((\mathcal{H}, \ominus_{\mathcal{H}}, \oplus_{\mathcal{H}})\) (ex.17).

**E. Semantic equivalence**

In this subsection, we show that flat semantics, upwards semantics and downwards semantics are all equivalent to instances of each other.

First, flat semantics are direct instances of upwards semantics and downwards semantics.

**Theorem 33.** Given an extended Kripke model \(\mathcal{M} = (M, \preceq, \ominus, J)\) with downwards closed and upwards closed separation algebra, for any \(\varphi\) and \(m\),

\[
m \models_{\mathcal{M}} \varphi \iff m \models_{\mathcal{M}} \varphi
\]

\[
m \models_{\mathcal{M}} \varphi \iff m \models_{\mathcal{M}} \varphi
\]

**Proof.** Obvious by lemma \[28\].

Second, we define two separation algebra transformations:

**Definition 34** (Upwards closure and downwards closure). Given a separation algebra \((M, \preceq, \ominus)\), its upwards closure is the triple \((M, \preceq, \oplus)\) where \(\ominus \oplus (m_1, m_2, m)\) iff there is \(m' \leq m\) such that \(m' \preceq m\).

**Example 35** (Index closure). The downwards closure of index algebra (ex.31) is the minimum algebra \((\mathbb{N}, \leq_{\mathbb{N}}, \ominus_{\text{min}, \mathbb{N}})\) with

\[
\ominus_{\text{min}} \triangleq \{(x, y, z) \mid z \leq_{\mathbb{N}} x \text{ and } z \leq_{\mathbb{N}} y\}.
\]

**Lemma 36.** Given an ordered separation algebra \((M, \preceq, \ominus)\):

If \((M, \preceq, \ominus)\) is upwards closed, \((M, \preceq, \ominus)\) is a downwards closed and upwards closed ordered separation algebra. If \((M, \preceq, \ominus)\) is downwards closed, \((M, \preceq, \ominus)\) is a downwards closed and upwards closed ordered separation algebra.

At this point, you might think that any ordered separation algebra can be made downwards- and upwards-closed by taking both of its closures. Unfortunately, such a two-sided closure might not be an ordered separation algebra at all!

**Proposition 37.** Let \((M, \preceq, \ominus^\oplus)\) be the upwards closure of the downwards closure of example 35. Then \((M, \preceq, \ominus^\oplus)\) is not associative.

Fortunately, as we will soon learn in section V-C, it is possible to find a closure for some algebras that are neither downwards nor upwards closed (see ex.39). When the algebra is upwards- or downwards-closed (as ex.31) the closure is upwards- and downwards-closed (as ex.35). Then, we can use the flat semantics on closures, which happens to be equivalent with a stronger semantics over algebra before the closure.

**Theorem 38.** Given an extended Kripke model \(\mathcal{M} = (M, \preceq, \ominus, J)\)

1) if it is downwards closed, then the flat semantics on \(\mathcal{M}^\oplus\) is equivalent to the downwards semantics on \(\mathcal{M}\), i.e. for any \(\varphi\) and \(m\), \(m \models_{\mathcal{M}^\oplus} \varphi\) iff \(m \models_{\mathcal{M}} \varphi\)

2) if it is upwards closed, then the flat semantics on \(\mathcal{M}^\ominus\) is equivalent to the upwards semantics on \(\mathcal{M}\), i.e. for any \(\varphi\) and \(m\), \(m \models_{\mathcal{M}^\ominus} \varphi\) iff \(m \models_{\mathcal{M}} \varphi\)

In summary, flat semantics is a direct instance of upwards semantics and downwards semantics (thm.33). Upwards semantics and downwards semantics are instances of flat semantics via the downwards and upwards closures (thm.38).

As far as we know, the idea of closure and the semantic preservation is completely novel. However, we consider Atkey’s separation logic for amortized resource analysis \[4\] a precursor worth mentioning, as explained in the next example.

**Example 39** (Resource-bounds). We present two examples of resource-bound algebra as use cases for closures.

**Atkey** \[4\] proposed the resource-bound algebras to be the product of the discrete heap (ex.17) and a consumable (what we call amortized) resource, which is an ordered monoid (such as ex.12). Since ordered monoid are not
necessarily upwards-closed and Akey wanted to use a
flat semantics, he uses the product of a discrete heap and
the closure of a resource as his model.

Now consider an amortized resource analysis with a step-
indexed heap (prop[32]). The step-indexed heap is not
downwards-closed and the amortized resources are not
necessarily upwards-closed, so the product is neither. We
can’t use any of the semantics in def[27] and the closure
in def[24] might not be an ordered separation algebra!
Fortunately, we can separately take the closures of the
step-indexed heap and of the amortize resource, and then
take their product, obtaining the following upwards- and
downwards-closed algebra:

\[(R \times \mathbb{N} \times H, \leq_{R \times \mathbb{N} \times H}, \oplus_{R} \Delta_{2}^{\mathbb{N}} \times \oplus_{H})\]

F. Semantics of emp

Garbage-collect separation logic and malloc/free separation
logic disagree on the semantics of emp. In a malloc/free
separation logic,

\[m \models \text{emp} \iff m \text{ is a unit} \quad \text{(Emp}_1\text{)}\]

and for a garbage-collected separation logic, emp just means
True, i.e.

\[m \models \text{emp} \iff \text{always} \quad \text{(Emp}_2\text{)}\]

How would you define the semantics of emp for the product
of the min. algebra (ex[35]) and the discrete heap (ex[11.1])?
The product has no units, so (Emp1) wouldn’t work, but
(Emp2) seems wrong too.

Intuitively, the only elements that should satisfy emp are
those that have an empty heap. This are exactly the increasing
elements! We propose, then, the following generalization of
the semantics of emp:

Definition 40 (Semantics of emp). For a separation algebra
\((M; \leq, \oplus)\) and \(m \in M\),

\[m \models \text{emp} \iff m \text{ is increasing} \]

Definition 40 will not be sound if the set of increasing
elements is not monotonic. To solve that, just like we did
in section V.D we can define a stronger semantics to ensure
soundness. This stronger semantics is an instance of definition
40 via the downwards closure, just like in theorem 38 Never-
theless, we know of no practical application of such semantics,
we omit the discussion here. In what follows we just assume
that the increasing set is monotonic.

Lemma 41. If the algebra is downwards-closed, the increas-
ing set is monotonic.

For increasing algebras (ex[11.2]) all elements are increasing,
so the semantics of emp is equivalent to (Emp2). For algebras
with discrete order (ex[11.1]), as stated in the lemma below,
only units are increasing, so the semantics of emp is equivalent
to (Emp1).

Lemma 42. In a separation algebra with discrete order, an
element is increasing iff it is a unit.

Finally, we define a unital separation algebra as one in
which each element has a “increasing part”. For example, the
separation algebra in example 43 is unital.

Example 43 (Discrete step-indexed). The discrete step-
indexed algebra \((\mathbb{N} \times H, \geq_{\mathbb{N}} \Delta_{2}, \Delta_{1} \times \oplus_{H})\) is the product
of indices \(\mathbb{N}\) (ex[7]) and the discrete heap (ex[17]).

Definition 44 (Residue). In a separation algebra \((M; \leq, \oplus)\),
we say \(m\) is a residue of \(n\) if there exists \(n’\) such that
\(\oplus(m, n’, n)\) and \(n \leq n’\).

Definition 45 (Unital separation algebras). A separation
algebra is unital if all elements have an increasing residue.
For antisymmetric orders this is equivalent to: all elements
have a identity element.

Most interesting ordered separation algebras are unital, but
not all (see fig[5]). Some that are not, like example 12.1
at least satisfy the following weaker property.

Definition 46 (Residual separation algebras). A separation
algebra is residual if every element has a residue.

The lemmas bellow shows that the two properties are equiva-
 lent for increasing algebras but, in general, being residual is
weaker than being unital. There are certainly algebras which
are not residual (e.g. with an unjoinable error state), but the
“interesting” part of any algebra is always the residual subset.
All the examples on this paper are residual.

Lemma 47. A unital separation algebra is residual.

Lemma 48. An increasing separation algebras is unital iff it
is residual.

The compositions in lemma 15 preserve both definitions.

Lemma 49. If the original algebras are unital or residual,
then so is the sum, product and exponential algebras.

Lemma 50 (Increasing set compositions). For down-
wards-closed algebras: the increasing set of the sum algebra is the
sum of the increasing sets of each algebra; The increasing
set of the product algebra is the product of increasing sets of
each algebra; The increasing set of the exponential algebra
are those functions that uniquely map to increasing elements.

VI. PARAMETRIC SOUNDNESS AND COMPLETENESS

Different propositional logics are sound and complete with
respect to their corresponding class of Kripke models. Intu-
itionistic logic is sound and complete w.r.t. Kripke semantics
in all models [22]; Classical logic is sound and complete w.r.t.
Kripke semantics in the Kripke models with a discrete
order; and Gödel-Dummett or De Morgan logic are sound and
complete w.r.t. Kripke models with nonbranching or always-
joining orders (def[51], respectively.

Definition 51. An order \(\leq\) is nonbranching iff for any \(m, n\)
and \(n’\), with \(m \leq n\) and \(m \leq n’\) then \(n \leq n’\) or \(n’ \leq n\).

An order \(\leq\) always joins iff for any \(m, n\) and \(n’\), if \(m \leq n\)
and \(m \leq n’\) then exists \(n''\) s.t. \(n \leq n''\) and \(n'' \leq n’\).

In this section, we determine corresponding classes of
extended Kripke models for each separation logic, as defined
in section III based on the framework for separation algebras developed in section V. We then proceed to prove soundness and completeness for each separation logic w.r.t. the flat semantics in it’s corresponding class of models. According to the equivalence theorem proved in section V, separation logics are then also proven sound and complete w.r.t. upwards semantics and downwards semantics.

**Definition 52** (Corresponding class of extended Kripke models). Given a separation logic $\Gamma$, its corresponding class of extended Kripke models is the set of models which (1) are upwards-closed (2) are downwards-closed (3) satisfies the canonical properties of all optional axioms in $\Gamma$, as listed in the following table.

<table>
<thead>
<tr>
<th>Optional axiom</th>
<th>Canonical property</th>
</tr>
</thead>
<tbody>
<tr>
<td>$EM \in \Gamma$</td>
<td>Discrete order</td>
</tr>
<tr>
<td>$GD \in \Gamma$</td>
<td>Nonbranching order</td>
</tr>
<tr>
<td>$WEM \in \Gamma$</td>
<td>Always-joining order</td>
</tr>
<tr>
<td>$*E \in \Gamma$</td>
<td>Increasing</td>
</tr>
<tr>
<td>$EMP \in \Gamma$</td>
<td>Unital and $J(emp)$ is the increasing set</td>
</tr>
<tr>
<td>$EXT \in \Gamma$</td>
<td>Residual</td>
</tr>
</tbody>
</table>

We use the standard notation $\Phi \vdash \psi$ to represent the existence of finite elements $\varphi_1, \varphi_2, ..., \varphi_n \in \Phi$ such that

$$\vdash \left( \bigwedge_{i=1}^{n} \varphi_i \right) \rightarrow \psi$$

Also, $\Phi \models_U \psi$ means that for any model $m \in U$ if every assertion in $\Phi$ is satisfied on $m$ then $\psi$ is satisfied on $m$.

**Definition 53** (Soundness and completeness). A proof theory $\Gamma$ is sound w.r.t. a semantics $\models$ in a class of models $U$ iff for any $\varphi$, $\models^\Gamma \varphi$ implies $\models_U \varphi$.

A proof theory $\Gamma$ is weakly complete w.r.t. a semantics $\models$ in a class of models $U$ iff for any $\varphi$, $\models_U \varphi$ implies $\models^\Gamma \varphi$.

A proof theory $\Gamma$ is strongly complete w.r.t. a semantics $\models$ in $U$ iff for any $\Phi$ and $\varphi$, $\Phi \models_U \varphi$ implies $\Phi \models^\Gamma \varphi$.

Strong completeness clearly implies weak completeness. In the rest of the section we present the soundness and strong completeness of separation logics stated as follows:

**Theorem 54** (Parametric soundness and completeness). A separation logic $\Gamma$ is sound and strongly complete w.r.t. the flat semantics in $\Gamma$’s corresponding class of models.

A. Soundness

It is trivial to show that every single proof rule is sound in corresponding class of extended Kripke models. Thus soundness can be proved by induction on proofs.

B. Strong Completeness

We use Henkin-style proofs to prove strong completeness of separation logics w.r.t. flat semantics. In other words, we show that for any $\Phi$ and $\varphi$, $\Phi \not\vdash^\Gamma \varphi$ implies $\Phi \not\vdash_U \varphi$ by following these steps:

1) Construct a canonical model $\mathcal{M}^c = (M^c, \leq^c, \oplus^c, J^c)$ where $M^c \subseteq \mathcal{L}(\Sigma)$

2) Show that $M^c \in U$

3) Show that for any $\Psi$ and $\psi, \psi \in \Psi$ iff $\Psi \models_{\mathcal{M}} \psi$

4) Show that if $\Phi \not\vdash^\Gamma \varphi$, then there is an $\Psi \in M^c$ s.t. $\Phi \subseteq \Psi$ but $\varphi \not\in \Psi$

This proof strategy is an extension of Kripke’s famous proof of strong completeness of intuitionistic logic [22]. We always assume $\Sigma$ is countable and thus so is $\mathcal{L}(\Sigma)$.

**Definition 55** (DDCS). Given $\Sigma$, we call a set of formulas $\Phi \subseteq \mathcal{L}(\Sigma)$ a deriveable closed, disjunction-witnessed, consistent set (DDCS) of proof theory $\Gamma$ if

1) it is deriveable closed, i.e. for any $\phi$, if $\Phi \vdash^\Gamma \phi$ then $\phi \in \Phi$.

2) it is disjunction witnessed, i.e. for any $\phi$ and $\psi$, if $\phi \lor \psi \in \Phi$ then $\phi \in \Phi$ or $\psi \in \Phi$.

3) it is consistent, i.e. $\Phi \not\vdash^\Gamma \bot$

To define canonical models, we lift separating conjunction to sets of assertions (not only DDCSs but any sets), as follows:

$$\Phi \ast \Psi = \{ \phi \ast \psi \mid \Phi \vdash^\Gamma \phi \text{ and } \Psi \not\vdash^\Gamma \psi \}$$

**Definition 56** (Canonical model). Given a separation logic $\Gamma$ of $\mathcal{L}(\Sigma)$, we call $M^c = (M^c, \leq^c, \oplus^c, J^c)$ the canonical model of $\Gamma$ where

1) $M^c$ is the set of DDCSs of $\Gamma$

2) for any $\Phi, \Psi \in M^c$, $\Phi \leq^c \Psi$ iff $\Phi \subseteq \Psi$

3) for any $\Phi_1, \Phi_2, \Phi \in M^c$, $\oplus^c(\Phi_1, \Phi_2, \Phi)$ iff $\Phi_1 \ast \Phi_2 \subseteq \Phi$

4) for any $p \in \Sigma$ and $\Phi \in M^c$, $\Phi \in J^c(p)$ iff $p \in \Phi$

This definition of canonical model is actually well defined, in other words, $\leq^c$ is a preorder, $\oplus^c$ is commutative and associative and $J^c$ is monotonic. Also, it is upwards closed and downwards closed.

**Lemma 57**. Given a separation logic $\Gamma$ of $\mathcal{L}(\Sigma)$, its canonical model $(M^c, \leq^c, \oplus^c, J^c)$ is an extended Kripke model, which is upwards-closed and downwards-closed at the same time.

Because a canonical model has a upwards- and downwards-closed ordered separation algebra we can define the flat semantics on it. The most important property of canonical models, formalized by the truth lemma below, is that assertions in a DDCS are exactly the ones satisfied on the same DDCS w.r.t. flat semantics.

**Lemma 58** (Truth lemma). Given a separation logic $\Gamma$ of $\mathcal{L}(\Sigma)$, for any $\Phi \in M^c$ and $\varphi \in \mathcal{L}(\Sigma)$,

$$\Phi \models_{\mathcal{M}} \varphi \iff \varphi \in \Phi$$

Moreover, a canonical model is an element of the corresponding class of extended Kripke models.

**Lemma 59**. Given a separation logic $\Gamma$, its canonical model $\mathcal{M}$ satisfies the canonical properties of all optional axioms in $\Gamma$.

Now we can prove separation logics complete. A more detailed proof is in the appendix.

**Proof**. We prove the contrapositive of strong completeness. Supposing $\Gamma \not\vdash^\Gamma \varphi$, we know (from existence lemma I in the appendix) that there exists a DDCS $\Psi$ s.t. $\Phi \subseteq \Psi$ and $\Psi \not\vdash^\Gamma \varphi$. By the truth lemma, we know that $\Psi \models_{\mathcal{M}} \Phi$ and $\Psi \models_{\mathcal{M}} \varphi$. By lemma 59 we know that the canonical model of $\Gamma$ is indeed in the corresponding class of extended Kripke models.

□
VII. Classiﬁcation of Logics and Algebras

In section III we presented a convenient way to classify separation logics and, similarly, the framework developed in section VII allows us to classify ordered separation algebras according to their properties. To illustrate the classiﬁcations, we categorize the examples presented in this paper. In ﬁgure 5 we classify the algebras and, in ﬁgure 6 we describe logics whose corresponding class of models contains the closure of each algebra (deﬁnition 52). Each logic is sound w.r.t. that closure according to theorem 54.

The algebras of indices N and it’s closure, minimum on N, share a column in ﬁgure 6 since their closure is the same (i.e. min. N). There is no direct closure over the step-indexed resource-bounds algebra (ex. 39.2), so we omit it in ﬁgure 6. However, as explained in example 39.2, we can separately take closures of each component; the result is in the corresponding class of a Gödel-Dummett, malloc/free logic with empty.

Although algebras are often upwards-closed, Typed-heap is not; Resource-bounds (before closure) are up.-closed if and only if the amortized resource is. Step-indexed algebras are not downwards-closed because heaps only join heaps with the same index.

Ordered separation algebras are increasing when the increasing set is exactly the carrier set. For discrete heaps, only the empty heap H₀ is increasing. For resource-bounds, the increasing set depends on R_{inc}, the increasing set of the amortized resource. The sum algebra on N⁺ has no increasing elements and is not unital.

We don’t show an examples of De Morgan for the sake of brevity, but there are practical examples. For instance, a monotonic heap, indexed by the algebra of sets (S, ⊆, ∪), which is ordered by set inclusion and joined by disjoint union, can be used for amortized resource analysis with distinguishable, unique resources.

Highlighting that propositional logics and separation elimination are two independent classiﬁcations, we show all combinations of three intermediate logics (i.e. Intuitionistic, Gödel-Dummett, Classical) and all separation eliminations (garbage-collected and malloc/free), with two exceptions. First, a classical, garbage-collected logic must have no EMP or EXT (by thm. 5); such logics are possible, but we know of no interesting example. Second, intuitionistic and malloc/free exist and can be practical. For instance, the sum of a monotonic heap and a discrete heap is not increasing, always-meet nor nonbranching; it could be used to reason about a memories which are only partially garbage-collected.

VIII. Applications of The Unifying Semantics

In the past 15 years, separation logic has been proﬁc tool for modular program veriﬁcation. However, until now, most research was only applicable to one speciﬁc semantic model. For example, Ishtiaq and O’Hearn [17] showed that the frame rule is sound as long as the operational semantics has the frame property, but their conclusion was only demonstrated for unordered separation algebras (in our framework, separation algebra with discrete order). So, their work does not directly beneﬁt separation-logic-based veriﬁcation tools such as VST [11] and Iris [20], since their semantics are based on step-indexed models. Similarly, the soundness of CSL [7] was only established on unordered separation algebra.

We have already shown one example of how to generalize results about separation logic. The soundness proof of IP + SL, in section VII, holds for all semantics of separation logic (because they are instances of the ﬂat semantics). In this sections, we will further shows that the two soundness results mentioned above—frame rule and CSL— can be generalized to any ordered separation algebra with ﬂat semantics, and thus for all separation logics.

A. Frame rule

The frame rule is a fundamental property for modular reasoning in separation logic.

$$\{P\} c \{Q\} \Rightarrow \{P + R\} c \{Q + R\} \quad \text{(FRAME)}$$

Ishtiaq and O’Hearn [17] showed that the frame rule is sound with their “classical” separation logic, as long as the operational semantics has, what the called, the frame property. Here, we generalize the deﬁnition of frame property for all ordered separation algebras, and show that the soundness of frame rule still holds.

Definition 60 (Small-step semantics). A small-step semantics of a programming language is a tuple (M, cmd, ⇒) in which M represents program states, cmd represents program commands and ⇒ is a binary relation between (M × cmd) and (M × cmd + {Err, NT}). Here, Err and NT means error state and nonterminating state respectively.

We write ⇒* to mean the transitive reﬂexive closure of ⇒.

Definition 61 (Accessibility from small-step semantics). Given a small-step semantics (M, cmd, ⇒), we deﬁne accessibility as a binary relation between M and M + {Err, NT}:

1. if (m, c) ⇒* Err
2. if (m, c) ⇒* NT
3. if there exist inﬁnite sequences {m_k} and {c_k} (for k ∈ N) such that (m, c) ⇒ (m_0, c_0) and (m_k, c_k) ⇒ (m_{k+1}, c_{k+1}).

Definition 62 (Frame property). An accessibility relation (⇒) is said to verify the frame property w.r.t. an ordered separation algebra (M, ≤, ⊕) if for all m, m', n, n' ∈ M and any command c,

1. if ⊕(m, m', n) and n ⇒ Err, then m ⇒ Err
2. if ⊕(m, m', n) and n ⇒ NT, then m ⇒ NT
3. if ⊕(m, m', n), n ⇒ n' and executing c terminates normally from m, then there exists m'' such that m ⇒ m', ⊕(m'', m', n') and m'' ≤ m'.
existence of a greater \( m'_i \) satisfying the join relation. For step-indexed semantics, \( \oplus (m', m'_j, n') \) is too strong! Instead, step-indexed semantics like VST [1] Iris [20], and Charge! satisfy the frame property defined by definition 62. We can specialize theorem 65 to any step-indexed semantics.

**Definition 64** (Step-indexed semantics). Suppose \((M, \text{cmd}, \rightsquigarrow)\) is a small-step semantics, its step-indexed semantics is the small-step semantics \((N \times M, \text{cmd}, \rightsquigarrow_1)\) in which

1) \((k + 1, m, c) \rightsquigarrow_1 (k, m', c') \) iff \((m, c) \rightsquigarrow (m', c')\);
2) \((0, m, c) \rightsquigarrow_1 \textbf{NT} \) for any \( m \) and \( c \)

**Theorem 65.** If the accessibility relation defined by \((M, \text{cmd}, \rightsquigarrow)\) always has frame property w.r.t. \((M, \leq, \oplus)\), then the accessibility relation defined by its step-indexed semantics \((N \times M, \text{cmd}, \rightsquigarrow_1)\) always has frame property w.r.t. \((N, \geq_N, =) \times (M, \leq, \oplus)\)

**B. Hoare rules for concurrent primitives**

Concurrent separation logic is an extension of separation logic to reason about concurrent programs. Brookes [2] proved CSL to be sound for unordered heap models; in particular, he required cancellativity of the algebra. But separation logics with ghost resources [20] don’t have cancellative algebras: the ghosts don’t naturally cancel. Is CSL with ghost resources sound? As we show, the soundness of CSL can be generalized to any models of ordered separation algebra, even without cancellativity.

Before we present the Hoare rule, we must introduce first the concept of preciseness. In a separation algebra with discrete order (e.g. in discrete heaps, where Brookes introduced the concept) an assertion \( \phi \) is precise when inside any piece of memory \( m \) there is at most one submemory \( m_1 \) which satisfies \( \phi \). The following generalization of preciseness just requires that all pieces of memory that satisfy \( \phi \) inside \( m \) are bounded by some \( m^*_1 \).

**Definition 66** (Preciseness). Given an upwards closed and downwards closed separation algebra \((M, \leq, \oplus)\), an assertion \( \phi \) is precise w.r.t. flat semantics if for any \( m_1, m_2 \) and \( m \), if \( \oplus (m_1, m_2, m) \) and \( m_1 \models \phi \) then there exists \( m^*_1 \) and \( m^*_2 \), such that

1) \( \oplus (m^*_1, m^*_2, m) \) and \( m^*_1 \models \phi \)
2) for any \( m^*_1 \) and \( m^*_2 \), if \( \oplus (m^*_1, m^*_2, m) \) and \( m^*_1 \models \phi \) then \( m^*_2 \leq m^*_1 \)

We are now ready to state our generalized theorem for the soundness of CSL.

**Theorem 67** (Soundness of CSL). If all resource invariants are precise w.r.t. flat semantics, then Hoare rules in CSL are sound w.r.t. flat semantics of separation logic. The following are the Hoare rules of concurrent primitives:

1) If \( I \models \phi \) \( c_1 \{ \psi_1 \} \) and \( I \models \phi \) \( c_2 \{ \psi_2 \} \), then \( I \models \)
\{\phi_1 \land \phi_2\} C_1 || C_2 \{\psi_1 \land \psi_2\}

2) If \( I \vdash \{ \phi \} c \{ \psi \}, \) then \( I ; r : I_r \vdash \{ \phi \} \) with \( r \) do \( c \{ \psi \}\)

The proof follows along the same lines as Brookes’ proof. We formalize it in Coq and omit it here.

IX. FUTURE WORK

We are particularly excited to use the present work as a starting point to find a unifying framework of Hoare separation logic. There are many incompatible definitions for the semantics for Hoare triples \([20, 11, 17]\) which make their different results incompatible. We believe the present work is the first step towards resolving this incompatibility, but there are many issues yet to be solved. For instance, the two examples in section \(\text{VIII}\) have first order Hoare logics, but Hoare logics for programs with function calls are high ordered. Unifying such Hoare logics is more challenging. It will also be particularly challenging to unify the operational semantics for verifying concurrent programs. We believe this is the way to solve Parkinson’s challenge for the next 700 separation logics.

Our hope is that the present work will be a fertile ground for generalizing many known results, as we did in \(\text{VIII}\) Of particular interest to us is whether preciseness is required in a Hoare logic with the conjunction rule \([24, 14]\). A related conundrum is whether a separation algebra must be cancellative in order to have the conjunction rule. Both questions have been answered for classical, malloc/free logics, but are open in general.

X. CONCLUSION

We have clarified the terminology “classical vs. intuitionistic” and “malloc/free vs. garbage-collected” separation logic. They are two independent taxonomies.

We present flat semantics on upwards-closed and downwards-closed ordered separation algebra as a unification for all different semantics of separation logics. All separation logics are proved sound and complete w.r.t. corresponding model classes. This unification is powerful enough to generalize related concepts like frame property and preciseness and to generalize theoretical applications of separation logic like the soundness of frame rule (given frame property) and the soundness of CSL.

All the definitions, propositions, lemmas and theorems in this paper have been formalized in Coq in:

https://github.com/QinxiangCao/UnifySL

REFERENCES


APPENDIX

A. Proof of Semantic Equivalence

Here, we recall the definition of downwards closure and upwards closure.

Definition 34 (Upwards closure and downwards closure). Given a separation algebra \( (M, \leq, \oplus) \), its upwards closure is the triple \( (M, \leq, \oplus^\uparrow) \) where \( \oplus^\uparrow(m_1, m_2, m) \) iff there is \( m' \) such that \( m' \leq m \) and \( \oplus(m_1, m_2, m') \).

Given a separation algebra \( (M, \leq, \oplus) \), its downwards closure is the triple \( (M, \leq, \oplus^\downarrow) \) where \( \oplus^\downarrow(m_1, m_2, m) \) iff there are \( m'_1 \) and \( m'_2 \) such that \( m_1 \leq m'_1 \), \( m_2 \leq m'_2 \) and \( \oplus(m'_1, m'_2, m) \).

We first prove that both upwards closures of downwards-closed algebra and downwards closures of upwards-closed algebra are upwards-closed and downwards-closed at the same time. We then prove that the flat semantics on the closures are equivalent with downwards (resp. upwards) semantics in the original algebra.

Lemma 36. Given an ordered separation algebra \( (M, \leq, \oplus) \): If \( (M, \leq, \oplus) \) is downwards closed, \( (M, \leq, \oplus^\uparrow) \) is an upwards closed and downwards closed ordered separation algebra. If \( (M, \leq, \oplus) \) is upwards closed, \( (M, \leq, \oplus^\downarrow) \) is an upwards closed and downwards closed ordered separation algebra.

Proof. 1) If \( (M, \leq, \oplus) \) is downwards-closed, \( (M, \leq, \oplus^\uparrow) \) is downwards-closed: Obvious because \( \leq \) is transitive.

2) If \( (M, \leq, \oplus) \) is upwards-closed, \( (M, \leq, \oplus^\downarrow) \) is upwards-closed: Suppose \( m_1, m_2, m \) and \( n \) satisfy \( \oplus^\downarrow(m_1, m_2, m) \) and \( m \leq n \). According to the definition of \( \oplus^\downarrow \), there exist \( m'_1 \) and \( m'_2 \) s.t.

\[
\begin{align*}
m_1 & \leq m'_1 \\
m_2 & \leq m'_2 \\
\oplus(m'_1, m'_2, m) & \leq n
\end{align*}
\]

Since \( (M, \leq, \oplus) \) is upwards-closed, there must exist \( n_1 \) and \( n_2 \) s.t.

\[
\begin{align*}
m'_1 & \leq n_1 \\
m'_2 & \leq n_2 \\
\oplus(m'_1, m'_2, n) & \leq n
\end{align*}
\]

So we know that \( m_1 \leq n_1, m_2 \leq n_2 \) and \( \oplus^\downarrow(n_1, n_2, n) \).

In other words, \( (M, \leq, \oplus^\downarrow) \) is upwards-closed.

3) If \( (M, \leq, \oplus) \) is downwards-closed, \( (M, \leq, \oplus^\uparrow) \) is upwards-closed: Obvious because \( \leq \) is transitive.

4) If \( (M, \leq, \oplus) \) is downwards-closed, \( (M, \leq, \oplus^\downarrow) \) is downwards-closed: Suppose \( m_1, m_2, m, n_1 \) and \( n_2 \) satisfy\( \oplus^\downarrow(m_1, m_2, m) \), \( n_1 \leq m_1 \) and \( n_2 \leq m_2 \). According to the definition of \( \oplus^\downarrow \), there exist \( m' \) s.t.

\[
m' \leq m \\
\oplus(m_1, m_2, m')
\]

Since \( (M, \leq, \oplus) \) is downwards-closed, there exist \( n \) s.t.

\[
n \leq m' \\
\oplus(n_1, n_2, n)
\]

So we know that \( n \leq m \) and \( \oplus^\downarrow(n_1, n_2, n) \). In other words, \( (M, \leq, \oplus^\downarrow) \) is downwards-closed.

\[\square\]

Theorem 38. Given an extended Kripke model \( M = (M, \leq, \oplus, J) \)

1) if it is downwards closed, then the flat semantics on \( M^\uparrow \) is equivalent to the downwards semantics on \( M \), i.e. for any \( \varphi \) and \( m \), \( m \models^\uparrow \varphi \) iff \( m \models^\downarrow \varphi \)

2) if it is upwards closed, then the flat semantics on \( M^\downarrow \) is equivalent to the upwards semantics on \( M \), i.e. for any \( \varphi \) and \( m \), \( m \models^\downarrow \varphi \) iff \( m \models^\uparrow \varphi \)

Proof. We prove it by induction on the syntax of assertions. The only interesting cases are the following:

1) If \( (M, \leq, \oplus) \) is downwards-closed and for any \( m \):

\[
\begin{align*}
m & \models^\uparrow \varphi \iff m \models^\downarrow \varphi \\
m & \models^\uparrow \psi \iff m \models^\downarrow \psi
\end{align*}
\]

then for any \( m \):

\[
\begin{align*}
m & \models^\uparrow \varphi \land \psi \iff m \models^\downarrow \varphi \land \psi
\end{align*}
\]

Obvious by IH and the definition of \( \oplus^\uparrow \), flat semantics, downwards semantics.

2) If \( (M, \leq, \oplus) \) is downwards-closed and for any \( m \):

\[
\begin{align*}
m & \models^\uparrow \varphi \iff m \models^\downarrow \varphi \\
m & \models^\uparrow \psi \iff m \models^\downarrow \psi
\end{align*}
\]

then for any \( m \):

\[
\begin{align*}
m & \models^\uparrow \varphi \lor \psi \iff m \models^\downarrow \varphi \lor \psi
\end{align*}
\]

Left to right is obvious because \( \oplus^\uparrow \supset \oplus \). We only prove the other direction here. Suppose \( m \models^\downarrow \varphi \land \psi \) (left side), \( \oplus^\uparrow(m_1, m_2, m) \) and \( m \models^\downarrow \varphi \) (the assumption of right side). Then by the definition of \( \oplus^\uparrow \), we know there exists \( n_2 \), s.t.

\[
n_2 \leq m_2 \\
\oplus(m_1, m_2, n_2)
\]

And by IH, we know that

\[
m_1 \models^\downarrow \varphi
\]

From the fact that \( m \models^\downarrow \varphi \land \psi \), we know

\[
n_2 \models^\downarrow \psi
\]

Since the denotation of all assertions are monotonic, \( m_2 \models^\downarrow \psi \), i.e. by IH: \( m_2 \models^\uparrow \psi \)

3) If \( (M, \leq, \oplus) \) is downwards-closed and for any \( m \):

\[
\begin{align*}
m & \models^\uparrow \varphi \iff m \models^\downarrow \varphi \\
m & \models^\uparrow \psi \iff m \models^\downarrow \psi
\end{align*}
\]

then for any \( m \):

\[
\begin{align*}
m & \models^\uparrow \varphi \land \psi \iff m \models^\downarrow \varphi \land \psi
\end{align*}
\]
Right to left is obvious, because $\varphi \subseteq \varphi'$. We only prove the other direction here. Suppose $m \models_{\mathcal{M}^+} \varphi$, then there exist $m_1$ and $m_2$ s.t.

$$\varphi \subseteq \varphi' \Rightarrow (m_1, m_2, m)$$

By the definition of $\varphi'$, there exist $n_1$ and $n_2$ s.t.

$$m_1 \subseteq n_1$$
$$m_2 \subseteq n_2$$
$$\varphi \subseteq (n_1, n_2, m)$$

By the monotonicity of $\varphi$ and $\psi$'s denotation and IH, we know that

$$n_1 \models_{\mathcal{M}} \varphi$$
$$n_2 \models_{\mathcal{M}} \psi$$

So, $m \models_{\mathcal{M}} \varphi * \psi$.

4) If $(\mathcal{M}, \leq, \oplus)$ is upwards-closed and for any $m$:

$$m \models_{\mathcal{M}} \varphi \text{ iff } m \models_{\mathcal{M}} \varphi$$

then for any $m$:

$$m \models_{\mathcal{M}} \varphi * \psi \text{ iff } m \models_{\mathcal{M}} \varphi \rightarrow \psi$$

Obvious by IH and the definition of $\oplus'$, flat semantics, upwards semantics.

\[\square\]

B. Proof of Completeness

Here, we always assume $\Sigma$ is countable and thus so is $L(\Sigma)$. We recall the definition of DDCS and canonical model.

Definition [DDCS]. Given $\Sigma$, we call a set of formulas $\Phi \subseteq L(\Sigma)$ a derivable closed, disjunction-witnessed, consistent set (DDCS) of proof theory $\Gamma$ if

1) it is derivable closed, i.e. for any $\phi$, if $\Phi \vdash \Gamma \phi$ then $\phi \in \Phi$  
2) it is disjunction witnessed, i.e. for any $\phi$ and $\psi$, if $\phi \lor \psi \in \Phi$ then $\phi \in \Phi$ or $\psi \in \Phi$  
3) it is consistent, i.e. $\Phi \not\vdash \bot$

Definition 68. We lift separating conjunction to sets of assertions (not only DDCSs but any sets), as follows:

$$\Phi * \Psi \equiv \{ \phi * \psi \mid \Phi \vdash \Gamma \phi \text{ and } \Psi \vdash \Gamma \psi \}$$

Definition [Canonical model]. Given a separation logic $\Gamma$ of $L(\Sigma)$, we call $\mathcal{M}^c = (M^c, \leq^c, \oplus^c, J^c)$ the canonical model of $\Gamma$ where

1) $M^c$ is the set of DDCSs of $\Gamma$  
2) for any $\Phi, \Psi \in M^c$, $\Phi \leq^c \Psi$ iff $\Phi \subseteq \Psi$  
3) for any $\Phi_1, \Phi_2, \Phi \in M^c$, $\oplus^c(\Phi_1, \Phi_2, \Phi)$ iff $\Phi_1 * \Phi_2 \subseteq \Phi$  
4) for any $p \in \Sigma$ and $\Phi \in M^c$, $\Phi \in J^c(p)$ iff $p \in \Phi$

It is an important fact that for any DDCS $\Phi$ of $\Gamma$ and assertion $\varphi$, $\Phi \vdash \Gamma \varphi$ is equivalent with $\varphi \in \Phi$. We will use these two concept interchangeably in the following proofs.

Here, we first prove a lemma about the lifted separating conjunction between sets of assertions.

Lemma 69. For any $\Phi, \Psi$ and $\theta$, if $\Phi * \Psi \vdash \Gamma \chi$ then there exist $\varphi_1, \varphi_2, ..., \varphi_n \in \Phi \text{ and } \psi_1, \psi_2, ..., \psi_m \in \Psi$, s.t.

$$\vdash (\bigwedge_{i=1}^{n} \varphi_i * \bigwedge_{i=1}^{m} \psi_i) \rightarrow \chi$$

Proof. By the definition of “derivable”, we know there exist $\chi_1, \chi_2, ..., \chi_k, \chi_1', \chi_2', ..., \chi_k'$ such that

$$\vdash (\bigwedge_{j=1}^{k} \varphi_{i,j}) \rightarrow \chi$$

$$\vdash (\bigwedge_{j=1}^{k} \psi_{i,j}) \rightarrow \chi'$$

$$\vdash (\bigwedge_{i=1}^{n} \varphi_i, \bigwedge_{i=1}^{m} \psi_i) \rightarrow \chi$$

By the fact the following assertion is a tautology in any $\Sigma$, we know that

$$(\varphi \land \varphi') \land (\psi \land \psi') \rightarrow (\varphi \land \psi) \land (\varphi' \land \psi')$$

we know that

$$\vdash (\bigwedge_{i=1}^{n} \chi_i) \land (\bigwedge_{i=1}^{m} \chi_i') \rightarrow \chi$$

So, by *MONO, we know

$$\vdash (\bigwedge_{i=1}^{n} \varphi_{i,j}) * (\bigwedge_{i=1}^{m} \psi_{i,j}) \rightarrow \chi$$

One important property of DDCS’s is that we can extend consistent set of assertions into DDCS’s. Specifically, we prove the following existence lemma.

Lemma 70 (Existence lemma I). Given a separation logic $\Gamma$, a set of assertions $\Phi$ and an assertion $\phi$, if $\Phi \vdash \Gamma \phi$, then there exists $\Phi'$, which is a DDCS of $\Gamma$, s.t. $\Phi \subseteq \Phi'$ and $\Phi' \vdash \Gamma \phi$.

Proof. See [22].

Lemma 71 (Existence lemma II). Given a separation logic $\Gamma$, of $L(\Sigma)$, and sets of assertions $\Phi_1, \Phi_2$ and $\Phi$ among which $\Phi$ is a DDCS of $\Gamma$, if $\Phi_1 \times \Phi_2 \subseteq \Phi$, then

1) there is a DDCS $\Phi'_1$, s.t. $\Phi_1 \subseteq \Phi'_1$ and $\Phi'_1 \times \Phi_2 \subseteq \Phi$.  
2) there is a DDCS $\Phi'_2$, s.t. $\Phi_2 \subseteq \Phi'_2$ and $\Phi_1 \times \Phi'_2 \subseteq \Phi$.

Proof. We only prove the first half here. The second half follows in the same way.
Because $\mathcal{L}(\Sigma)$ is countable, we can enumerate all asserts as $\psi_1, \psi_2, \ldots$. Then we construct the following sets of assertions and let $\Phi_1' = \bigcup_{k \in \mathbb{N}} \Psi_k$:

$$
\Psi_0 = \Phi_1,
\Psi_{k+1} = \{ \Psi_k \cup \{ \psi_{k+1} \} \} \text{ if } (\Psi_k \cup \{ \psi_{k+1} \}) \uparrow \Phi_2 \subseteq \Phi \text{ if } (\Psi_k \cup \{ \psi_{k+1} \}) \uparrow \Phi_2 \subseteq \Phi
$$

Obviously, $\Phi_1 \subseteq \Phi_1'$ and $\Phi_1' \cup \Phi_2 \subseteq \Phi$, so we only need to show that $\Phi_1'$ is actually a DDCS.

First, we prove that $\Phi_1'$ is derivable closed by contradiction. Suppose $\Phi_1' \uparrow \Gamma \psi_k$ and $\psi_k \notin \Phi_1'$. Then $\psi_k \notin \Psi_k$, which means there exists $\varphi_1$ and $\varphi_2$ s.t.

$$
\Psi_{k-1} \cup \{ \psi_k \} \uparrow \Gamma \varphi_1
$$

and

$$
\Phi_2 \uparrow \Gamma \varphi_2
$$

$$
\varphi_1 \uparrow \varphi_2 \notin \Phi
$$

(2)

At the same time, we know that $\Phi_1' \uparrow \Gamma \varphi_1$ because $\Psi_k \subseteq \Phi_1'$ and $\Phi_1' \uparrow \Gamma \psi_k$. Since we know $\Phi_1' \cup \Phi_2 \subseteq \Phi$, we can conclude that $\varphi_1 \uparrow \varphi_2 \notin \Phi$, which contradicts $\Phi_1'$.

Second, $\Phi_1'$ is disjunction-witnessed. We prove it by contradiction, mostly in the same way as above. Suppose $\psi_k \uparrow \forall \psi_k' \in \Phi_1'$, $\psi_k \notin \Phi_1'$ and $\psi_k' \notin \Phi_1'$. Then $\psi_k \notin \Psi_k$ and $\psi_k' \notin \Psi_k'$, which means there exists $\varphi_1$, $\varphi_2$, $\varphi_1'$ and $\varphi_2'$ s.t.

$$
\Psi_{k-1} \cup \{ \psi_k \} \uparrow \Gamma \varphi_1
$$

$$
\Psi_{k'} \uparrow \Gamma \varphi_1'
$$

$$
\Phi_2 \uparrow \Gamma \varphi_2
$$

$$
\Phi_2 \uparrow \Gamma \varphi_2'
$$

$$
\varphi_1 \uparrow \varphi_2 \notin \Phi
$$

$$
\varphi_1' \uparrow \varphi_2' \notin \Phi
$$

(3)(4)(5)(6)

From deduction theorem and (3) [4], we know:

$$
\Phi_1' \uparrow \Gamma \psi_k \rightarrow \varphi_1
$$

$$
\Phi_1' \uparrow \Gamma \psi_k \rightarrow \varphi_1'
$$

Then, by $\Phi_1' \supseteq \Psi_{k-1}$ and $\Phi_1' \supseteq \Psi_{k'}$, we know

$$
\Phi_1' \uparrow \Gamma \psi_k \vee \psi_k' \rightarrow \varphi_1 \vee \varphi_1'
$$

Moreover, since $\psi_k \vee \psi_k' \in \Phi_1'$ is assumed, $\Phi_1' \uparrow \Gamma \varphi_1 \vee \varphi_1'$. At the same time, $\Phi_2 \uparrow \Gamma \varphi_2 \vee \varphi_2'$ and $\Phi_1' \cup \Phi_2 \subseteq \Phi$ is already known, so

$$
\Phi \uparrow (\varphi_1 \vee \varphi_1') \uparrow (\varphi_2 \vee \varphi_2')
$$

Notice that the following assertion is a tautology in any separation logic,

$$
(\varphi_1 \vee \varphi_1') \uparrow (\varphi_2 \vee \varphi_2') \rightarrow (\varphi_1 \uparrow \varphi_2 \vee \varphi_1' \uparrow \varphi_2')
$$

Thus, we know the following fact because $\Phi$ is a DDCS:

$$
\varphi_1 \vee \varphi_1' \in \Phi \text{ or } \varphi_2 \vee \varphi_2' \notin \Phi
$$

which contradicts with (5) and (6)!

Third, $\Phi_1'$ is consistent. This follows the facts that $\Phi$ is consistent, $\Phi_1' \cup \Phi_2 \subseteq \Phi$ and $\uparrow \Gamma \bot \uparrow \bot$.

Now we can prove that a canonical model is actually well defined, i.e. we will show that $\leq^c$ is a preorder, $\oplus^c$ is commutative and associative and $J^c$ is monotonic. Also, it is upwards closed and downwards closed.

**Lemma** [57] *Given a separation logic $\Gamma$ of $\mathcal{L}(\Sigma)$, its canonical model $(M^c, \leq^c, \oplus^c, J^c)$ is an extended Kripke model, which is upwards closed and downwards closed at the same time.*

**Proof.** 1) $\leq^c$ is a preorder because set inclusion is preordered.

2) $\oplus^c$ is commutative: suppose $\Phi_1$, $\Phi_2$ and $\Phi_3$ are DDCS’s and $\Phi_1 \oplus^c \Phi_2 \lambda^c \Phi_3$. By definition, for any $\varphi_1$ and $\varphi_2$, if $\Phi_1 \uparrow \Gamma \varphi_1$ and $\Phi_2 \uparrow \Gamma \varphi_2$ then $\Phi \uparrow \Gamma \varphi_1 \varphi_2$. Since $\Gamma$ is a separation logic,

$$
\Phi_2 \uparrow \Gamma \varphi_2 \rightarrow \varphi_2 \varphi_2
$$

and thus $\oplus^c(\Phi_2, \Phi_3)$. 3) $\oplus^c$ is associative: suppose $\Phi_1, \Phi_2, \Phi_3, \Phi_4$ and $\Phi_{xyz}$ are DDCS’s such that $\oplus^c(\Phi_1, \Phi_2, \Phi_3)$ and $\oplus^c(\Phi_3, \Phi_4, \Phi_{xyz})$. First we show that

$$
\Phi_{x} \uparrow (\Phi_{y} \uparrow \Phi_{z}) \subseteq \Phi_{xyz}.
$$

Given $\varphi_x \in \Phi_x$, $\varphi_y \in \Phi_y$ and $\varphi_z \in \Phi_z$, we know that $\varphi_x \varphi_y \in \Phi_{xyz}$. Thus,

$$
(\varphi_x \varphi_y) \rightarrow \varphi_z \in \Phi_{xyz} \rightarrow \uparrow \Gamma (\varphi_x \varphi_y) \varphi_z
$$

From the fact that $\Gamma$ is a separation logic, it follows that $\Phi_{xyz} \uparrow \varphi_z \rightarrow (\varphi_x \varphi_y)$. Second, by existence lemma II(2), we know there exists a DDCS $\Phi_{xyz}$ such that $\Phi_1 \varphi_2 \subseteq \Phi_{xyz}$ and $\Phi_2 \varphi_3 \subseteq \Phi_{xyz}$, which implies that $\oplus^c$ is associative by definition.

4) $J^c$ is monotonic by definition. 5) Upwards-closed: trivial because $\Phi_1 \varphi_2 \supseteq \Phi$ and $\Phi \varphi' \supseteq \Phi_1 \varphi_2$. 6) Downwards-closed: trivial because $\Phi_1 \varphi_2 \subseteq \Phi$, $\Phi_1 \varphi_2 \subseteq \Phi_1 \varphi_2 \subseteq \Phi$. Because a canonical model has a upwards-closed and downwards-closed separation algebra we can define the flat semantics on it. The most important property of canonical models, formalized by the truth lemma below, is that assertions in a DDCS are the assertions that are exactly the ones satisfied on the same DDCS w.r.t. flat semantics.

**Lemma** [58] (Truth lemma). *Given a separation logic $\Gamma$ of $\mathcal{L}(\Sigma)$, for any $\Phi \in M^c$ and $\varphi \in \mathcal{L}(\Sigma)$,

$$
\Phi \vdash \varphi \text{ iff } \varphi \in \Phi
$$

**Proof.** We proceed by induction on the syntax of $\varphi$. The cases when $\varphi$ is an atomic assertion, a conjunction, a disjunction or an implication, are covered in the proof of intuitionistic logic completeness [22]. Here, we show the induction step for separating conjunction and separating disjunction. Specifically, given the induction hypothesis: for any DDCS $\Phi$,

$$
\Phi \vdash \varphi_1 \text{ iff } \varphi_1 \in \Phi
$$

$$
\Phi \vdash \varphi_2 \text{ iff } \varphi_2 \in \Phi
$$

we are going to show that for any DDCS $\Phi$,

$$
\Phi \vdash \varphi_1 \varphi_2 \text{ iff } \varphi_1 \varphi_2 \in \Phi
$$

(C*)
Lemma 59. Given a separation logic $\Gamma$, its canonical model $\mathcal{M}_\Gamma$ satisfies the canonical properties of all optional axioms in $\Gamma$.

Proof. It is well known results that

1) $\mathcal{M}_\Gamma$ has an identity relation as its preorder if $\text{EM} \in \Gamma$

2) $\mathcal{M}_\Gamma$ has a non-branching relation as its preorder if $\text{GD} \in \Gamma$

3) $\mathcal{M}_\Gamma$ has an always-join relation as its preorder if $\text{WEM} \in \Gamma$

Besides,

4) $\mathcal{M}_\Gamma$ is increasing separation algebra if $\ast\text{E} \in \Gamma$. Suppose $\Phi_1, \Phi_2$ and $\Phi$ are DDCSs and $\ast\text{E}(\Phi_1, \Phi_2, \Phi)$. Then for any $\varphi_1 \in \Phi_1$, we know $\varphi_1 \ast T \in \Phi$ (because $T \in \Phi_2$). Since $\ast\text{E} \in \Gamma$, $\Phi \ast \varphi_1$, i.e. $\varphi_1 \in \Phi$. So, $\Phi_1 \subseteq \Phi$.

5) $J^\ast\text{E}(\text{emp})$ is the increasing set if $\text{EMP} \in \Gamma$. Left to right: suppose $\Phi \in J^\ast\text{E}(\text{emp})$. Then $\text{emp} \in \Phi$ by definition. So, if $\Phi \ast \Psi \subseteq \Psi'$, then $\{\text{emp}\} \ast \Psi \subseteq \Psi'$. This tells $\Psi \subseteq \Psi'$.

As $\Psi$ and $\Psi'$ is arbitrarily chosen, $\Phi$ is increasing.

Right to left: suppose $\Phi$ is increasing. Then we first show that $\Phi \ast \{\text{emp}\} \ast \text{emp}$. If not, then we know from existence lemma I that there exists a DDCS $\Phi_1$ s.t.

$$\Phi \ast \{\text{emp}\} \ast \text{emp} \subseteq \Phi_1$$

Then, from existence lemma II(2), we know there exists a DDCS $\Phi_1$ s.t.

$$\Phi \ast \Phi_1 \ast \text{emp} \subseteq \Phi_1$$

Since $\Phi$ is increasing, $\text{emp} \in \Phi_1 \subseteq \Phi_2$. It contradicts with (7).

Now that $\Phi \ast \{\text{emp}\} \ast \text{emp}$, we know from lemma 69 that there exists $\varphi$ s.t.

$$\Phi \ast \varphi \ast \text{emp} \ast \text{emp} \ast \text{emp}$$

By the adjoint property, we know: $\ast\text{E} \varphi \ast \text{emp} \rightarrow (\text{emp} \ast \text{emp})$, so

$$\Phi \ast\text{E} \varphi \rightarrow (\text{emp} \ast \text{emp})$$

Consequently,

$$\Phi \ast\text{E} \varphi \ast \text{emp} \ast \text{emp} \ast \text{emp}$$

So, $\Phi \ast\text{E} \varphi \ast \text{emp} \rightarrow (\text{emp} \ast \text{emp})^\ast \text{emp}$

6) $\mathcal{M}_\Gamma$ is unital separation algebra if $\text{EMP} \in \Gamma$. Assume $\Phi$ is a DDCS. Because $\text{EMP} \in \Gamma$, we know that

$$\{\text{emp}\} \ast \Phi \subseteq \Phi$$

By existence lemma II, we know there is a DDCS $\Psi$ such that $\text{emp} \in \Psi$ and $\Psi \ast \Phi \subseteq \Phi$. So, $\Psi$ is $\Phi$’s increasing residual.

7) $\mathcal{M}_\Gamma$ is residual separation algebra if $\text{EXT} \in \Gamma$. Suppose $\Phi$ is a DDCS. Because $\text{EXT} \in \Gamma$, we know that for any $\varphi \in \Phi$,

$$\Phi \ast \varphi \ast T$$

i.e., $\varphi \ast \text{E} \in \Phi$, so $\Phi \ast \{\text{E}\} \subseteq \Phi$. By existence lemma II(2), there is a DDCS $\Psi$ s.t. $\Phi \ast \Psi \subseteq \Phi$. This shows $\Psi$ is $\Phi$’s residue.

Now we can prove separation logics complete.

Proof. We will prove the contrapositive of strong completeness. Suppose $\Gamma \varphi \text{E} \varphi$, we know from existence lemma I that there exists a DDCS $\Psi$ such that $\varphi \subseteq \Psi$ and $\Psi \varphi$. By truth lemma, we know that $\Psi \supseteq \Phi \ast \Psi \ast \{\text{E}\} \subseteq \Phi$. By lemma 59 we know that the canonical model of $\Gamma$ is indeed in the corresponding class of extended Kripke models.