Stone Duality for Separation Logic

Part 2: A Duality Theorem for Separation Logic

Simon Docherty

University College London

Thursday 8th June 2017

S Docherty and D Pym. A Stone-Type Duality Theorem for Separation Logic via Its Underlying Bunched Logics. MFPS 2017

Outline

What is Separation Logic?

Outline

What is Separation Logic?

Stone Duality for Star

Outline

What is Separation Logic?

Stone Duality for Star

Structure for Quantification

Outline

What is Separation Logic?

Stone Duality for Star

Structure for Quantification

Stone Duality for Separation Logic

What is Separation Logic?

A Logic for Shared Mutable Data Structures

- Separation logic is a tool used in static analysis of programs that access and mutate data structures[1][2]
- Two components:
  1. An **assertion language** for describing memory states.
  2. A Hoare-style logic of triples $\{\varphi\}C\{\psi\}$
- φ, ψ are formulas of the assertion language, C is a program
- "If C executes from state satisfying precondition φ then it will end in a state satisfying postcondition ψ."

[1] J. Reynolds. Separation Logic: A Logic for Shared Mutable Data Structures, LICS 2002

[2] S. Ishtiaq and P. O'Hearn. BI as an Assertion Language for Mutable Data Structures, POPL 2001

Syntax of the Assertion Language

$$e \mapsto e' \mid \top \mid \bot \mid \neg\varphi \mid \varphi \wedge \varphi \mid \varphi \vee \varphi \mid \varphi \to \varphi \mid \varphi * \varphi \mid \varphi \mathrel{-\!\!*} \varphi \mid \mathrm{Emp} \mid \exists x \varphi \mid \forall x \varphi$$

- Terms e, e' built from variables, integers and arithmetic functions + and −.
- $\bot, \top, \neg, \wedge, \vee, \to \exists, \forall$ as in first-order logic.
- $\mapsto$ is the **points-to predicate** for reasoning about pointers.
- $*, \mathrel{-\!\!*}, \mathrm{Emp}$ are for reasoning about **separation** (more on this soon).

Stores and Heaps

- The **store** s is a partial function mapping variables to values (eg: stack-allocated memory).
- s acts as a valuation on variables occuring in terms, giving an evaluation of all terms e, $[e]s$.

Stores and Heaps

- The **store** s is a partial function mapping variables to values (eg: stack-allocated memory).
- s acts as a valuation on variables occuring in terms, giving an evaluation of all terms e, $[e]s$.
- The **heap** h is a partial function from addresses to values (eg: dynamically-allocated memory)
- Two heaps h, h' are disjoint ($h\#h'$) if their domains are disjoint.
- If $h\#h'$ then $h \cdot h'$ gives the disjoint union of h and h'.
- The empty heap [] is the empty function.

Store-Heap Semantics of Separation Logic

- $s, h \vDash e \mapsto e'$ iff $dom(h) = \{[e]s\}$ and $h([e]s) = [e']s$.

Store-Heap Semantics of Separation Logic

- $s, h \vDash e \mapsto e'$ iff $dom(h) = \{[e]s\}$ and $h([e]s) = [e']s$.
- $s, h \vDash \varphi * \psi$ iff h can be separated into disjoint h', h'' s.t. $h' \vDash \varphi$ and $h'' \vDash \psi$.

Store-Heap Semantics of Separation Logic

- $s, h \vDash e \mapsto e'$ iff $dom(h) = \{[e]s\}$ and $h([e]s) = [e']s$.
- $s, h \vDash \varphi * \psi$ iff h can be separated into disjoint h', h'' s.t. $h' \vDash \varphi$ and $h'' \vDash \psi$.
- $s, h \vDash \varphi \mathrel{-\!\!*} \psi$ iff for every h' satisfying φ disjoint from h, $s, h \cdot h' \vDash \psi$.

Store-Heap Semantics of Separation Logic

- $s, h \vDash e \mapsto e'$ iff $dom(h) = \{[e]s\}$ and $h([e]s) = [e']s$.
- $s, h \vDash \varphi * \psi$ iff h can be separated into disjoint h', h'' s.t. $h' \vDash \varphi$ and $h'' \vDash \psi$.
- $s, h \vDash \varphi \mathrel{-\!\!*} \psi$ iff for every h' satisfying φ disjoint from h, $s, h \cdot h' \vDash \psi$.
- $s, h \vDash \mathrm{Emp}$ iff h is the empty heap [].

Store-Heap Semantics of Separation Logic

- $s, h \vDash e \mapsto e'$ iff $dom(h) = \{[e]s\}$ and $h([e]s) = [e']s$.
- $s, h \vDash \varphi * \psi$ iff h can be separated into disjoint h', h'' s.t. $h' \vDash \varphi$ and $h'' \vDash \psi$.
- $s, h \vDash \varphi \mathrel{-\!\!*} \psi$ iff for every h' satisfying φ disjoint from h, $s, h \cdot h' \vDash \psi$.
- $s, h \vDash \mathrm{Emp}$ iff h is the empty heap [].
- $s, h \vDash \exists x \varphi$ iff there exists a such that $s[x \rightharpoonup a], h \vDash \varphi$.

How Does It Work?

- Proof rules for deriving new triples $\{\varphi\}C\{\psi\}$.
- Crucial: the frame rule

$$\frac{\{\phi\}\, C\, \{\psi\}}{\{\phi * \chi\}\, C\, \{\psi * \chi\}},$$

  where C does not modify any variable in χ.
- Local reasoning about a smaller specification carries through to bigger specification.
- Further proof theoretic techniques allow automation and scalability[3].

[3] C. Calcagno, D. Distefano, P. O'Hearn, and H. Yang. Compositional Shape Analysis by Means of Bi-abduction. Journal of the ACM, 58(6), 2011

Roadmap for the Duality Theorem

SL extends propositional logic in two ways: separating connectives and quantifiers/predicates.

1. Prove duality theorem for the propositional basis of SL, **BBI**.

Roadmap for the Duality Theorem

SL extends propositional logic in two ways: separating connectives and quantifiers/predicates.

1. Prove duality theorem for the propositional basis of SL, **BBI**.
2. Extend algebraic and topological models of **BBI** with structure for interpreting quantifiers, yielding **predicate BBI**.

Roadmap for the Duality Theorem

SL extends propositional logic in two ways: separating connectives and quantifiers/predicates.

1. Prove duality theorem for the propositional basis of SL, **BBI**.
2. Extend algebraic and topological models of **BBI** with structure for interpreting quantifiers, yielding **predicate BBI**.
3. Show the SL model is an instance of the topological model of predicate **BBI**.

Roadmap for the Duality Theorem

SL extends propositional logic in two ways: separating connectives and quantifiers/predicates.

1. Prove duality theorem for the propositional basis of SL, **BBI**.
2. Extend algebraic and topological models of **BBI** with structure for interpreting quantifiers, yielding **predicate BBI**.
3. Show the SL model is an instance of the topological model of predicate **BBI**.
4. Extend **BBI** duality to predicate **BBI**.

Stone Duality for Star

Boolean Bunched Logic: Syntax

BBI is a **bunched logic**[4] freely combining propositional logic and multiplicative intuitionistic linear logic.

$$\varphi ::= \mathrm{p} \mid \top \mid \bot \mid \neg\varphi \mid \varphi \wedge \varphi \mid \varphi \vee \varphi \mid \varphi \to \varphi \mid \varphi * \varphi \mid \mathrel{-\!\!*} \mid \mathrm{I}$$

The connectives $*, \mathrm{I}$ and $\mathrel{-\!\!*}$ are governed by:

$$\frac{\xi \vdash \phi \quad \eta \vdash \psi}{\xi * \eta \vdash \phi * \psi} \qquad \frac{\eta * \phi \vdash \psi}{\eta \vdash \phi \mathrel{-\!\!*} \psi}$$

$$\frac{\xi \vdash \phi \mathrel{-\!\!*} \psi \quad \eta \vdash \phi}{\xi * \eta \vdash \psi} \qquad \phi * (\psi * \xi) \dashv\vdash (\phi * \psi) * \xi$$

$$\phi * \psi \vdash \psi * \phi \qquad \phi * \mathrm{I} \dashv\vdash \phi$$

[4] P. O'Hearn and D. Pym. The Logic of Bunched Implications. Bulletin of Symbolic Logic, 5(2), 1999

Boolean Bunched Logic: Semantics

A **resource frame** is a structure $(X, \circ, E)$ such that

- $\circ : X^2 \to \mathcal{P}(X)$ is an associative & commutative operation,
- $E \subseteq X$ satisfies $\{r\} \circ E = \{r\}$ for all $r \in X$ (using obvious extension of $\circ$ to an operation on sets).

Boolean Bunched Logic: Semantics

A **resource frame** is a structure $(X, \circ, E)$ such that

- $\circ : X^2 \to \mathcal{P}(X)$ is an associative & commutative operation,
- $E \subseteq X$ satisfies $\{r\} \circ E = \{r\}$ for all $r \in X$ (using obvious extension of $\circ$ to an operation on sets).

Let $\mathcal{V} : \mathrm{Prop} \to \mathcal{P}(X)$ be a valuation on a resource frame.

Boolean Bunched Logic: Semantics

A **resource frame** is a structure $(X, \circ, E)$ such that

- $\circ : X^2 \to \mathcal{P}(X)$ is an associative & commutative operation,
- $E \subseteq X$ satisfies $\{r\} \circ E = \{r\}$ for all $r \in X$ (using obvious extension of $\circ$ to an operation on sets).

Let $\mathcal{V} : \mathrm{Prop} \to \mathcal{P}(X)$ be a valuation on a resource frame.

- $x \vDash_{\mathcal{V}} \mathrm{p}$ iff $x \in \mathcal{V}(\mathrm{p})$.
- $x \vDash_{\mathcal{V}} \varphi * \psi$ iff $\exists y, z$ s.t. $x \in y \circ z$ and $y \vDash \varphi$ and $z \vDash \psi$.
- $x \vDash_{\mathcal{V}} \varphi \mathrel{-\!\!*} \psi$ iff $\forall y, z$ s.t. $y \vDash \varphi$ and $z \in x \circ y$, $z \vDash \psi$.
- $x \vDash_{\mathcal{V}} \mathrm{I}$ iff $x \in E$.

Boolean Bunched Logic: Semantics

A **resource frame** is a structure $(X, \circ, E)$ such that

- $\circ : X^2 \to \mathcal{P}(X)$ is an associative & commutative operation,
- $E \subseteq X$ satisfies $\{r\} \circ E = \{r\}$ for all $r \in X$ (using obvious extension of $\circ$ to an operation on sets).

Let $\mathcal{V} : \mathrm{Prop} \to \mathcal{P}(X)$ be a valuation on a resource frame.

- $x \vDash_{\mathcal{V}} \mathrm{p}$ iff $x \in \mathcal{V}(\mathrm{p})$.
- $x \vDash_{\mathcal{V}} \varphi * \psi$ iff $\exists y, z$ s.t. $x \in y \circ z$ and $y \vDash \varphi$ and $z \vDash \psi$.
- $x \vDash_{\mathcal{V}} \varphi \mathrel{-\!\!*} \psi$ iff $\forall y, z$ s.t. $y \vDash \varphi$ and $z \in x \circ y$, $z \vDash \psi$.
- $x \vDash_{\mathcal{V}} \mathrm{I}$ iff $x \in E$.

Note: The structure $\mathcal{H} = (\mathrm{Heaps}, \cdot, \{[]\})$ is a resource frame.

Resource Algebras

A **resource algebra** $\mathbb{A}$ is an algebra $(A, \wedge, \vee, \bot, \top, *, \mathrel{-\!\!*}, I)$ such that

- $(A, \wedge, \vee, \bot, \top)$ is a Boolean algebra,
- $(A, *, I)$ is a commutative monoid,
- For all $a, b, c \in A$: $a * b \leq c$ iff $a \leq b \mathrel{-\!\!*} c$.

Resource algebras are to **BBI** what Boolean algebras are to classical propositional logic.

Representation Theorem for Resource Algebras

Theorem

Every resource algebra $\mathbb{A}$ is isomorphic to a resource algebra of sets.

Proof Sketch.

- We know $h(a) = \{F \in Uf(\mathbb{A}) \mid a \in F\}$ embeds into power-set algebra on set of ultrafilters.

Representation Theorem for Resource Algebras

Theorem

Every resource algebra $\mathbb{A}$ is isomorphic to a resource algebra of sets.

Proof Sketch.

- We know $h(a) = \{F \in Uf(\mathbb{A}) \mid a \in F\}$ embeds into power-set algebra on set of ultrafilters.
- $\circ_{Uf} : Uf(\mathbb{A})^2 \to \mathcal{P}(Uf(\mathbb{A}))$ given by $F \circ_{Uf} F' = \{F'' \mid \forall a \in F, \forall b \in F' : a * b \in F''\}$

Representation Theorem for Resource Algebras

Theorem

Every resource algebra $\mathbb{A}$ is isomorphic to a resource algebra of sets.

Proof Sketch.

- We know $h(a) = \{F \in Uf(\mathbb{A}) \mid a \in F\}$ embeds into power-set algebra on set of ultrafilters.
- $\circ_{Uf} : Uf(\mathbb{A})^2 \to \mathcal{P}(Uf(\mathbb{A}))$ given by $F \circ_{Uf} F' = \{F'' \mid \forall a \in F, \forall b \in F' : a * b \in F''\}$
- Define $E_{Uf} = \{F \in Uf(\mathbb{A}) \mid \mathrm{I} \in F\}$.

Representation Theorem for Resource Algebras

Theorem

Every resource algebra $\mathbb{A}$ is isomorphic to a resource algebra of sets.

Proof Sketch.

- We know $h(a) = \{F \in Uf(\mathbb{A}) \mid a \in F\}$ embeds into power-set algebra on set of ultrafilters.
- $\circ_{Uf} : Uf(\mathbb{A})^2 \to \mathcal{P}(Uf(\mathbb{A}))$ given by $F \circ_{Uf} F' = \{F'' \mid \forall a \in F, \forall b \in F' : a * b \in F''\}$
- Define $E_{Uf} = \{F \in Uf(\mathbb{A}) \mid \mathrm{I} \in F\}$.
- $(Uf(\mathbb{A}), \circ_{Uf}, E_{Uf})$ is a resource frame and generates a power set algebra that $\mathbb{A}$ embeds into with h.

□

Strengthening to a Duality

A **resource space** is a structure $(X, \mathcal{O}, \circ, E)$ such that

- $(X, \mathcal{O})$ is a Stone space.
- $(X, \circ, E)$ is a resource frame.
- Clopen sets are closed under $\circ$ and its adjoint
- E is a clopen set.
- If $z \notin x \circ y$ then there exists clopen O_1 and O_2 such that $x \in O_1$ and $y \in O_2$ but $z \notin O_1 \circ O_2$.

Theorem

The categories of resource algebras and resource spaces are dually equivalent.

Structure for Quantification

An Algebraic Model of Predicate BBI: Structures

A **resource hyperdoctrine**[5] is a functor $\mathbb{P} : \mathcal{C}^{op} \to \mathrm{ResAlg}$ such that

1. $\mathcal{C}$ is a category with **finite products**: for every $C_1, \ldots C_n$ in $\mathcal{C}$, $C_1 \times \cdots \times C_n$ exists.

[5] B. Biering, L. Birkedal, and N. Torp-Smith. BI Hyperdoctrines and Higher-order Separation Logic. ESOP 2005

An Algebraic Model of Predicate BBI: Structures

A **resource hyperdoctrine**[5] is a functor $\mathbb{P} : \mathcal{C}^{op} \to \mathrm{ResAlg}$ such that

1. $\mathcal{C}$ is a category with **finite products**: for every $C_1, \ldots C_n$ in $\mathcal{C}$, $C_1 \times \cdots \times C_n$ exists.
2. For each X, Γ in $\mathcal{C}$ there exists monotone maps $\exists X_\Gamma, \forall X_\Gamma : \mathbb{P}(\Gamma \times X) \to \mathbb{P}(\Gamma)$ satisfying **adjointness**

$$\exists X_\Gamma(a) \leq b \text{ iff } a \leq \mathbb{P}(\pi_{\Gamma,X})(b)$$

and **naturality** properties.

[5] B. Biering, L. Birkedal, and N. Torp-Smith. BI Hyperdoctrines and Higher-order Separation Logic. ESOP 2005

An Algebraic Model of Predicate BBI: Structures

A **resource hyperdoctrine**[5] is a functor $\mathbb{P} : \mathcal{C}^{op} \to \mathrm{ResAlg}$ such that

1. $\mathcal{C}$ is a category with **finite products**: for every $C_1, \ldots C_n$ in $\mathcal{C}$, $C_1 \times \cdots \times C_n$ exists.
2. For each X, Γ in $\mathcal{C}$ there exists monotone maps $\exists X_\Gamma, \forall X_\Gamma : \mathbb{P}(\Gamma \times X) \to \mathbb{P}(\Gamma)$ satisfying **adjointness**

$$\exists X_\Gamma(a) \leq b \text{ iff } a \leq \mathbb{P}(\pi_{\Gamma,X})(b)$$

   and **naturality** properties.
3. For each X in $\mathcal{C}$ there exists an element $=_X \in \mathbb{P}(X \times X)$ satisfying an **adjointness** property. Given diagonal map $\Delta_X : X \to X \times X$:

$$\top \leq \mathbb{P}(\Delta_X)(a) \text{ iff } =_X \leq a$$

[5] B. Biering, L. Birkedal, and N. Torp-Smith. BI Hyperdoctrines and Higher-order Separation Logic. ESOP 2005

An Algebraic Model of Predicate BBI: Interpretation of Terms

- Let $\mathbb{P} : \mathcal{C}^{op} \to \mathrm{ResAlg}$ be a resource hyperdoctrine.
- An object $[\![X]\!]$ of $\mathcal{C}$ is assigned to be the **type of values**.

An Algebraic Model of Predicate BBI: Interpretation of Terms

- Let $\mathbb{P} : \mathcal{C}^{op} \to \mathrm{ResAlg}$ be a resource hyperdoctrine.
- An object $[\![X]\!]$ of $\mathcal{C}$ is assigned to be the **type of values**.
- For a **context** $\Gamma = \{x_1, \ldots, x_n\}$, $[\![\Gamma]\!] = [\![X]\!]^n$.

An Algebraic Model of Predicate BBI: Interpretation of Terms

- Let $\mathbb{P} : \mathcal{C}^{op} \to \mathrm{ResAlg}$ be a resource hyperdoctrine.
- An object $[\![X]\!]$ of $\mathcal{C}$ is assigned to be the **type of values**.
- For a **context** $\Gamma = \{x_1, \ldots, x_n\}$, $[\![\Gamma]\!] = [\![X]\!]^n$.
- Each k-ary **function symbol** f is assigned to a morphism $[\![f]\!] : [\![X]\!]^k \to [\![X]\!]$ in $\mathcal{C}$.

An Algebraic Model of Predicate BBI: Interpretation of Terms

- Let $\mathbb{P} : \mathcal{C}^{op} \to \mathrm{ResAlg}$ be a resource hyperdoctrine.
- An object $[\![X]\!]$ of $\mathcal{C}$ is assigned to be the **type of values**.
- For a **context** $\Gamma = \{x_1, \ldots, x_n\}$, $[\![\Gamma]\!] = [\![X]\!]^n$.
- Each k-ary **function symbol** f is assigned to a morphism $[\![f]\!] : [\![X]\!]^k \to [\![X]\!]$ in $\mathcal{C}$.
- Interpretation of terms t in context Γ to morphisms $[\![t]\!] : [\![\Gamma]\!] \to [\![X]\!]$ is given inductively.

An Algebraic Model of Predicate BBI: Interpretation of Terms

- Let $\mathbb{P} : \mathcal{C}^{op} \to \mathrm{ResAlg}$ be a resource hyperdoctrine.
- An object $[\![X]\!]$ of $\mathcal{C}$ is assigned to be the **type of values**.
- For a **context** $\Gamma = \{x_1, \ldots, x_n\}$, $[\![\Gamma]\!] = [\![X]\!]^n$.
- Each k-ary **function symbol** f is assigned to a morphism $[\![f]\!] : [\![X]\!]^k \to [\![X]\!]$ in $\mathcal{C}$.
- Interpretation of terms t in context Γ to morphisms $[\![t]\!] : [\![\Gamma]\!] \to [\![X]\!]$ is given inductively.

$$[\![x_i]\!] = \pi_i : [\![\Gamma]\!] \to [\![X]\!]$$

$$[\![f(t)]\!] : [\![\Gamma]\!] \xrightarrow{[\![t]\!]} [\![X]\!] \xrightarrow{[\![f]\!]} [\![X]\!]$$

An Algebraic Model of Predicate BBI: Interpretation of Formulas

- Each m-ary **predicate symbol** P is assigned to an element $[\![P]\!] \in \mathbb{P}([\![X]\!]^m)$.
- Formulae in context Γ are inductively assigned to elements of $\mathbb{P}([\![\Gamma]\!])$:

An Algebraic Model of Predicate BBI: Interpretation of Formulas

- Each m-ary **predicate symbol** P is assigned to an element $[\![P]\!] \in \mathbb{P}([\![X]\!]^m)$.
- Formulae in context Γ are inductively assigned to elements of $\mathbb{P}([\![\Gamma]\!])$:

$$[\![Pt]\!] = \mathbb{P}([\![t]\!])([\![P]\!])$$

$$[\![t = t']\!] = \mathbb{P}(\langle [\![t]\!], [\![t']\!] \rangle)(=_{[\![X]\!]})$$

$$[\![\varphi * \psi]\!] = [\![\varphi]\!] *_{\mathbb{P}([\![\Gamma]\!])} [\![\psi]\!]$$

$$[\![\exists x \varphi]\!] = \exists [\![X]\!]_{[\![\Gamma]\!]}([\![\varphi]\!])$$

Theorem

Predicate BBI is sound and complete for interpretations on resource hyperdoctrines.

A Relational Model of Predicate BBI: Structures

An **indexed resource frame** is a functor $\mathcal{R} : \mathcal{C} \to \mathrm{ResFr}$ such that:

- $\mathcal{C}$ is a category with finite products.
- For all objects Γ, Γ', X and morphisms $s : \Gamma \to \Gamma'$ the following commutative square

$$\begin{array}{ccc} \mathcal{R}(\Gamma \times X) & \xrightarrow{\mathcal{R}(\pi_{\Gamma,X})} & \mathcal{R}(\Gamma) \\ \Big\downarrow{\scriptstyle \mathcal{R}(s \times id_X)} & & \Big\downarrow{\scriptstyle \mathcal{R}(s)} \\ \mathcal{R}(\Gamma' \times X) & \xrightarrow[\mathcal{R}(\pi_{\Gamma',X})]{} & \mathcal{R}(\Gamma') \end{array}$$

satisfies the **quasi-pullback**[6] property.

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

A Relational Model of Predicate BBI: Kripke Semantics

- Terms interpreted the same as in hyperdoctrine.
- Predicate symbol P assigned to a **subset** $[\![P]\!] \subseteq \mathcal{R}([\![X]\!]^m)$.

A Relational Model of Predicate BBI: Kripke Semantics

- Terms interpreted the same as in hyperdoctrine.
- Predicate symbol P assigned to a **subset** $[\![P]\!] \subseteq \mathcal{R}([\![X]\!]^m)$.
- Satisfaction of φ in context Γ calculated at $a \in \mathcal{R}([\![\Gamma]\!])$.
- Intuitively: a contains a vector of values supplied to evaluate φ.
- $a, \Gamma \vDash Pt_1 \dots t_m$ iff $\mathcal{R}(\langle [\![t_1]\!], \dots, [\![t_m]\!] \rangle)(a) \in [\![P]\!]$.

A Relational Model of Predicate BBI: Kripke Semantics

- Terms interpreted the same as in hyperdoctrine.
- Predicate symbol P assigned to a **subset** $[\![P]\!] \subseteq \mathcal{R}([\![X]\!]^m)$.
- Satisfaction of φ in context Γ calculated at $a \in \mathcal{R}([\![\Gamma]\!])$.
- Intuitively: a contains a vector of values supplied to evaluate φ.
- $a, \Gamma \vDash Pt_1 \dots t_m$ iff $\mathcal{R}(\langle [\![t_1]\!], \dots, [\![t_m]\!] \rangle)(a) \in [\![P]\!]$.
- $a, \Gamma \vDash \varphi * \psi$ iff $\exists b, c \in \mathcal{R}([\![\Gamma]\!])$ s.t. $a \in b \circ_{\mathcal{R}([\![\Gamma]\!])} c$ and $b, \Gamma \vDash \phi$ and $c, \Gamma \vDash \psi$

A Relational Model of Predicate BBI: Kripke Semantics

- Terms interpreted the same as in hyperdoctrine.
- Predicate symbol P assigned to a **subset** $[\![P]\!] \subseteq \mathcal{R}([\![X]\!]^m)$.
- Satisfaction of φ in context Γ calculated at $a \in \mathcal{R}([\![\Gamma]\!])$.
- Intuitively: a contains a vector of values supplied to evaluate φ.
- $a, \Gamma \vDash Pt_1 \dots t_m$ iff $\mathcal{R}(\langle [\![t_1]\!], \dots, [\![t_m]\!] \rangle)(a) \in [\![P]\!]$.
- $a, \Gamma \vDash \varphi * \psi$ iff $\exists b, c \in \mathcal{R}([\![\Gamma]\!])$ s.t. $a \in b \circ_{\mathcal{R}([\![\Gamma]\!])} c$ and $b, \Gamma \vDash \phi$ and $c, \Gamma \vDash \psi$
- $a, \Gamma \vDash \exists x \varphi$ iff $\exists a' \in \mathcal{R}([\![\Gamma]\!] \times [\![X]\!])$ s.t. $\mathcal{R}(\pi_{[\![\Gamma]\!],[\![X]\!]})(a') = a$ and $a', \Gamma \cup \{x\} \vDash \varphi$.
- Existential clause: find a vector of values a' extending a by one, such that a' sufficient to evaluate φ once binding of $\exists$ removed.

The Store-Heap Model is an Indexed Resource Frame

- Recall the Heap resource frame: $(\mathrm{Heaps}, \cdot, \{[]\})$.
- Define $\mathrm{Store} : \mathrm{Set} \to \mathrm{ResFr}$ by

$$\mathrm{Store}(X) = (X \times \mathrm{Heaps}, (=, \cdot), X \times \{[]\})$$

$$(x, h)(=, \cdot)(y, h') = \begin{cases} \emptyset & \text{if } x \neq y \text{ or } \neg h \# h' \\ \{(x, h \cdot h')\} & \text{otherwise .} \end{cases}$$

- Each $\mathrm{Store}(\mathrm{X})$ is a resource frame.

The Store-Heap Model is an Indexed Resource Frame

- Recall the Heap resource frame: $(\mathrm{Heaps}, \cdot, \{[]\})$.
- Define $\mathrm{Store} : \mathrm{Set} \to \mathrm{ResFr}$ by

$$\mathrm{Store}(X) = (X \times \mathrm{Heaps}, (=, \cdot), X \times \{[]\})$$

$$(x, h)(=, \cdot)(y, h') = \begin{cases} \emptyset & \text{if } x \neq y \text{ or } \neg h \# h' \\ \{(x, h \cdot h')\} & \text{otherwise .} \end{cases}$$

- Each $\mathrm{Store}(\mathrm{X})$ is a resource frame.
- An n-ary store $s = [x_1 \rightharpoonup a_1, \ldots, x_n \rightharpoonup a_n]$ with heap h is encoded as $((a_1, \ldots, a_n), h) \in \mathrm{Store}(\mathrm{Val}^n)$.
- The Kripke semantics on Store coincides with the usual semantics of Separation Logic.

Stone Duality for Separation Logic

Recap

- The propositional basis for Separation Logic is **BBI**.
- **BBI** can be interpreted in resource algebras and resource frames, and these structures are dual to each other when we add topology.
- A resource hyperdoctrine is a special functor $\mathbb{P} : \mathcal{C}^{op} \to \mathrm{ResAlg}$.
- An indexed resource frame is a special functor $\mathcal{R} : \mathcal{C} \to \mathrm{ResFr}$.
- Separation Logic is a signature of Predicate BBI, which can be interpreted in resource hyperdoctrines and indexed resource frames.
- The memory model of Separation Logic is an indexed resource frame.

Adding Topology

An **indexed resource space** is a functor $\mathcal{R} : \mathcal{C} \to \mathrm{ResSp}$ such that:

- $\mathcal{R}$ is an indexed resource frame.
- For every diagonal map $\Delta_X : X \to X \times X$, $Ran(\Delta_X)$ is clopen.
- For every pair of objects X, Γ, $\mathcal{R}(\pi_{\Gamma,X})$ maps open sets to open sets[7] .

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

Recall: A Formal Definition of Duality

Duality for **BBI** gives us

- **a pair of functors** $F : \mathrm{ResAlg} \to \mathrm{ResSp}^{op}$ and $G : \mathrm{ResSp}^{op} \to \mathrm{ResAlg}$
- together with natural transformations $\epsilon : Id_{\mathrm{ResSp}^{op}} \to FG$ and $\eta : \mathrm{Id}_{\mathrm{ResAlg}} \to GF$
- such that every component $\epsilon_D : D \to FG(D)$, $\eta_C : C \to GF(C)$ is an isomorphism.

Putting it all together

- Take a resource hyperdoctrine $\mathbb{P} : \mathcal{C}^{op} \to \mathrm{ResAlg}$.

Putting it all together

- Take a resource hyperdoctrine $\mathbb{P} : \mathcal{C}^{op} \to \mathrm{ResAlg}$.
- Composing with $F : \mathrm{ResAlg} \to \mathrm{ResSp}^{op}$ gives an indexed resource space $F \circ \mathbb{P} : \mathcal{C} \to \mathrm{ResSp}$.

Putting it all together

- Take a resource hyperdoctrine $\mathbb{P} : \mathcal{C}^{op} \to \mathrm{ResAlg}$.
- Composing with $F : \mathrm{ResAlg} \to \mathrm{ResSp}^{op}$ gives an indexed resource space $F \circ \mathbb{P} : \mathcal{C} \to \mathrm{ResSp}$.
- Take an indexed resource space $\mathcal{R} : \mathcal{C} \to \mathrm{ResSp}$.

Putting it all together

- Take a resource hyperdoctrine $\mathbb{P} : \mathcal{C}^{op} \to \mathrm{ResAlg}$.
- Composing with $F : \mathrm{ResAlg} \to \mathrm{ResSp}^{op}$ gives an indexed resource space $F \circ \mathbb{P} : \mathcal{C} \to \mathrm{ResSp}$.
- Take an indexed resource space $\mathcal{R} : \mathcal{C} \to \mathrm{ResSp}$.
- Composing with $G : \mathrm{ResSp}^{op} \to \mathrm{ResAlg}$ gives a resource hyperdoctrine $G \circ \mathcal{R} : \mathcal{C}^{op} \to \mathrm{ResAlg}$ with $=_X$ given by $Ran(\mathcal{R}(\Delta_X))$ and $\exists X_\Gamma$ given by $\mathcal{R}(\pi_{\Gamma,X})$.

Recall: A Formal Definition of Duality

Duality for **BBI** gives us

- a pair of functors $F : \mathrm{ResAlg} \to \mathrm{ResSp}^{op}$ and $G : \mathrm{ResSp}^{op} \to \mathrm{ResAlg}$
- together with **natural transformations** $\epsilon : Id_{\mathrm{ResSp}^{op}} \to FG$ and $\eta : \mathrm{Id}_{\mathrm{ResAlg}} \to GF$
- such that every component $\epsilon_D : D \to FG(D)$, $\eta_C : C \to GF(C)$ is an **isomorphism**.

Putting it all together

- Take a resource hyperdoctrine $\mathbb{P} : \mathcal{C}^{op} \to \mathrm{ResAlg}$.
- Composing with $F : \mathrm{ResAlg} \to \mathrm{ResSp}^{op}$ gives an indexed resource space $F \circ \mathbb{P} : \mathcal{C} \to \mathrm{ResSp}$.
- Take an indexed resource space $\mathcal{R} : \mathcal{C} \to \mathrm{ResSp}$.
- Composing with $G : \mathrm{ResSp}^{op} \to \mathrm{ResAlg}$ gives a resource hyperdoctrine $G \circ \mathcal{R} : \mathcal{C}^{op} \to \mathrm{ResAlg}$ with $=_X$ given by $Ran(\mathcal{R}(\Delta_X))$ and $\exists X_\Gamma$ given by $\mathcal{R}(\pi_{\Gamma,X})$..
- **BBI** duality: $\mathbb{P}$ isomorphic to $GF \circ \mathbb{P}$, $\mathcal{R}$ isomorphic to $FG \circ \mathcal{R}$.

[8] S. Docherty and D. Pym. A Stone-Type Duality Theorem for Separation Logic via its Underlying Bunched Logics. MFPS 2017

Putting it all together

- Take a resource hyperdoctrine $\mathbb{P} : \mathcal{C}^{op} \to \mathrm{ResAlg}$.
- Composing with $F : \mathrm{ResAlg} \to \mathrm{ResSp}^{op}$ gives an indexed resource space $F \circ \mathbb{P} : \mathcal{C} \to \mathrm{ResSp}$.
- Take an indexed resource space $\mathcal{R} : \mathcal{C} \to \mathrm{ResSp}$.
- Composing with $G : \mathrm{ResSp}^{op} \to \mathrm{ResAlg}$ gives a resource hyperdoctrine $G \circ \mathcal{R} : \mathcal{C}^{op} \to \mathrm{ResAlg}$ with $=_X$ given by $Ran(\mathcal{R}(\Delta_X))$ and $\exists X_\Gamma$ given by $\mathcal{R}(\pi_{\Gamma,X})$..
- **BBI** duality: $\mathbb{P}$ isomorphic to $GF \circ \mathbb{P}$, $\mathcal{R}$ isomorphic to $FG \circ \mathcal{R}$.
- Morphisms: slightly more complicated - see paper[8]!

[8] S. Docherty and D. Pym. A Stone-Type Duality Theorem for Separation Logic via its Underlying Bunched Logics. MFPS 2017

Stone Duality for Resource Hyperdoctrines

Theorem

The categories of resource hyperdoctrines and indexed resource spaces are dually equivalent.

Conclusions

- Resource hyperdoctrines generalize the syntax of Separation Logic.
- Indexed resource spaces generalize the semantics of Separation Logic.
- This work gives a complete algebraic and topological foundation for the **assertion language** of Separation Logic.
- **Duality** strengthens soundness and completeness and allows transfer of results between the two perspectives.

Further Work

- Next: extension with structure to interpret the Hoare logic component of Separation Logic.
- And then: interpretation of computationally important properties like the **frame rule** and **bi-abduction** in this framework.
- And possibly: **Concurrent** Separation Logic?
- Thanks for listening!