

Separation Logic Through a New Lens

Sarah Rovner-Frydman

Marlboro College

May 6, 2020

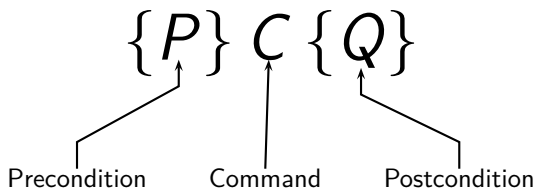
Table of Contents

- 1 Some background on separation logic
- 2 Optics in prosets
- 3 Optics for separation logic
- 4 Conclusion

Table of Contents

- 1 Some background on separation logic
- 2 Optics in prosets
- 3 Optics for separation logic
- 4 Conclusion

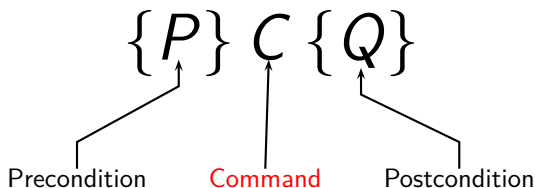
Hoare logic



Examples:

- $\{x < y \wedge x, y \in \mathbb{Z}\} x := x + 1 \{x \leq y \wedge x, y \in \mathbb{Z}\}$
- $\{\text{islist}(l)\} \text{sort_in_place}(l) \{\forall i \leq j < |l|. l_i \leq l_j\}$
- $\{x > 0\} \text{while } x > 0 \text{ do } x := x + 1 \text{ end } \{\perp\}$

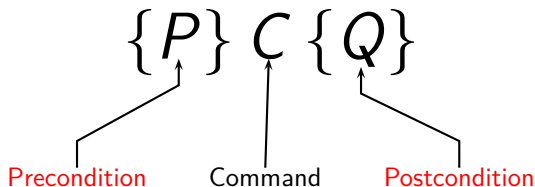
Hoare logic



Examples:

- $\{x < y \wedge x, y \in \mathbb{Z}\} x := x + 1 \{x \leq y \wedge x, y \in \mathbb{Z}\}$
- $\{\text{islist}(l)\} \text{sort_in_place}(l) \{\forall i \leq j < |l|. l_i \leq l_j\}$
- $\{x > 0\} \text{while } x > 0 \text{ do } x := x + 1 \text{ end } \{\perp\}$

Hoare logic

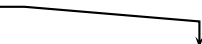


Examples:

- $\{x < y \wedge x, y \in \mathbb{Z}\} x := x + 1 \{x \leq y \wedge x, y \in \mathbb{Z}\}$
- $\{\text{islist}(l)\} \text{sort_in_place}(l) \{\forall i \leq j < |l|. l_i \leq l_j\}$
- $\{x > 0\} \text{while } x > 0 \text{ do } x := x + 1 \text{ end } \{\perp\}$

Hoare logic, cont'd

Entailment of assertions

$$\frac{P' \vdash P \quad \{P\} C \{Q\} \quad Q \vdash Q'}{\{P'\} C \{Q'\}} \quad \text{(Consequence)}$$


$$\frac{\{P\} C \{Q\} \quad \{Q\} D \{R\}}{\{P\} C; D \{R\}} \quad \text{(Sequencing)}$$

The frame problem

$$\frac{\{P\} C \{Q\}}{\{F \wedge P\} C \{F \wedge Q\}} \text{ (Frame?)}$$

- ✓ $\{x \geq y\} \quad x := x + 1 \{x > y\}$
- ✓ $\{\text{sorted}(l) \wedge x \geq y\} x := x + 1 \{\text{sorted}(l) \wedge x > y\}$

The frame problem

$$\frac{\{P\} C \{Q\}}{\{F \wedge P\} C \{F \wedge Q\}} \text{ (Frame?)}$$

- ✓ $\{x \geq y\} \quad x := x + 1 \{x > y\}$
- ✓ $\{\text{sorted}(l) \wedge x \geq y\} \quad x := x + 1 \{\text{sorted}(l) \wedge x > y\}$

Nope!

- ✓ $\{\text{pressable}(b)\} \quad \text{press}(b) \{\text{pressed}(b)\}$
- ✗ $\{\text{presses}(3) \wedge \text{pressable}(b)\} \quad \text{press}(b) \{\text{presses}(3) \wedge \text{pressed}(b)\}$

Separating conjunction (and implication)

Write $\blacktriangleright \models P$ for “assertion P holds in **state fragment** \blacktriangleright ”.

$$\frac{\bullet \models P \quad \bullet \models Q}{\bullet \models P \wedge Q}$$

$$\frac{\blacktriangleleft \models P \quad \blacktriangleright \models Q}{\bullet \models P * Q}$$

$$\frac{\begin{array}{c} \bullet \models P \\ \vdots \\ \bullet \models Q \end{array}}{\bullet \models P \rightarrow Q}$$

$$\frac{\begin{array}{c} \blacktriangleleft \models P \\ \vdots \\ \bullet \models Q \end{array}}{\blacktriangleright \models P * Q}$$

$$P \wedge Q \vdash R \iff P \vdash Q \rightarrow R$$

$$P * Q \vdash R \iff P \vdash Q * R$$

The frame rule

$$\frac{\{P\} C \{Q\}}{\{F * P\} C \{F * Q\}} \text{ (Frame)}$$

- ✓ $\{x \geq y\} \quad x := x + 1 \{x > y\}$
- ✓ $\{\text{sorted}(l) * x \geq y\} \quad x := x + 1 \{\text{sorted}(l) * x > y\}$

The rule instance that was previously unsound now has a **vacuously true** conclusion instead.

- ✓ $\{\text{pressable}(b)\} \quad \text{press}(b) \{\text{pressed}(b)\}$
- ✓ $\{\text{presses}(3) * \text{pressable}(b)\} \quad \text{press}(b) \{\text{presses}(3) * \text{pressed}(b)\}$

Spatial information

$$P * Q \dashv\vdash Q * P$$
$$(P * Q) * R \dashv\vdash P * (Q * R)$$

Spatial information

$$P * Q \dashv\vdash Q * P$$
$$(P * Q) * R \dashv\vdash P * (Q * R)$$

$$2^2 = 4 \vdash (2^2 = 4) * (2^2 = 4)$$
$$l_3 = 5 \not\vdash (l_3 = 5) * (l_3 = 5) \quad \exists i.l_i = 5 \not\vdash (\exists i.l_i = 5) * (\exists i.l_i = 5)$$

Spatial information

$$P * Q \dashv\vdash Q * P$$
$$(P * Q) * R \dashv\vdash P * (Q * R)$$

$$2^2 = 4 \vdash (2^2 = 4) * (2^2 = 4)$$
$$l_3 = 5 \not\vdash (l_3 = 5) * (l_3 = 5) \quad \exists i.l_i = 5 \not\vdash (\exists i.l_i = 5) * (\exists i.l_i = 5)$$

$$(P \multimap Q) * P \vdash Q \quad Q \vdash P \multimap P * Q$$
$$p_1 = 3 \vdash p_2 = 4 \multimap p = (3, 4) \quad l_3 = 5 \vdash l_3 = 5 \multimap \perp$$

Spatial information, manipulation of

An admissible rule:

$$\frac{R \vdash (Q * R') * P \quad \{P\} C \{Q\}}{\{R\} C \{R'\}} \text{ (Ramify)}$$

the ramification [...] asserts [...] that the “global” assertion R becomes R' after a “local” transformation from P to Q .

Aquinas Hobor and Jules Villard. *The Ramifications of Sharing in Data Structures*. 2013. DOI: [10.1145/2429069.2429131](https://doi.org/10.1145/2429069.2429131)

A similar concept is described by Qinxiang Cao et al. *Proof Pearl: Magic Wand as Frame*. 2019. arXiv: [1909.08789](https://arxiv.org/abs/1909.08789) [cs.PL]

Spatial information, manipulation of

This looks an awful lot like a lens!

$$\frac{R \vdash (Q \multimap R') * P \quad \{P\} C \{Q\}}{\{R\} C \{R'\}} \text{ (Ramify)}$$

the ramification [...] asserts [...] that the “global” assertion R becomes R' after a “local” transformation from P to Q .

Aquinas Hobor and Jules Villard. *The Ramifications of Sharing in Data Structures*. 2013. DOI: [10.1145/2429069.2429131](https://doi.org/10.1145/2429069.2429131)

A similar concept is described by Qinxiang Cao et al. *Proof Pearl: Magic Wand as Frame*. 2019. arXiv: [1909.08789](https://arxiv.org/abs/1909.08789) [cs.PL]

This sounds an awful lot like a lens!

Table of Contents

- 1 Some background on separation logic
- 2 Optics in prosets
- 3 Optics for separation logic
- 4 Conclusion

Monoid actions as a model of “context”

Say we have a monoid $\mathbf{M} = (M, \cdot, 1)$ and a set X with a left \mathbf{M} -action \star . Write $\circ \triangleq 1$, and for $C \in \mathbf{M}$, $a \in X$, write $C\{a\}$ for $C \star a$. Think of elements of \mathbf{M} as **nestable contexts** into which we can place elements of X .

$$\circ\{a\} = a \quad (C_1 \cdot C_2)\{a\} = C_1\{C_2\{a\}\}$$

\mathbf{M} itself canonically has the **left regular action** $C_1 \star C_2 \triangleq C_1 \cdot C_2$, and then the monoid laws say:

$$C = C\{\circ\} = \circ\{C\} \quad (C_1\{C_2\{\circ\}\})\{C_3\{\circ\}\} = C_1\{C_2\{C_3\{\circ\}\}\}$$

Also, we can rewrite the second action law as

$$(C_1\{C_2\{\circ\}\})\{a\} = C_1\{C_2\{a\}\}$$

A running example

Here's a simple/archetypal example of a monoid action where this point of view makes a lot of sense.

- Elements of **M**: pairs of strings. They're a **prefix** and a **suffix**; write (s, t) as $s[...]$ t
- Operation of **M**: **nesting**. Identity is $""[...]"$.

$$s[...]$$
$$t \cdot u[...]$$
$$v \triangleq su[...]$$
$$vt$$

- Action on the set of strings: **insertion**.

$$s[...]$$
$$t \star u \triangleq sut$$

A definition

Fix a **preordered** monoid \mathbf{M} and **preordered** left \mathbf{M} -sets X, Y .

Definition (Clarke et al., §2)

We define a proset **Optic** $_{X,Y}$.

- The underlying set is just $X \times Y$, but we write an element (a, b) as $(a \triangleright b)$.
- We'll write \rightsquigarrow for the ordering rather than \leq . It is defined by

$$(a \triangleright b) \rightsquigarrow (s \triangleright t) \triangleq \exists C \in \mathbf{M}. (s \leq C\{a\}) \wedge (C\{b\} \leq t)$$

Example: \mathbf{M} is the monoid of string contexts, X and Y are both the \mathbf{M} -set of strings, all three objects with the discrete preorder (i.e., \leq is $=$). Then

$$("m" \triangleright "mad") \rightsquigarrow ("me" \triangleright "made") \rightsquigarrow ("Edit me!" \triangleright "Edit made!")$$

Applying \rightsquigarrow

Definition

A relation $R \subseteq X \times Y$ is \leq -respecting if it satisfies (1) and it is context-respecting if it satisfies (2).

$$\frac{a' \leq a \quad a R b \quad b \leq b'}{a' R b'} \quad (1) \qquad \frac{a R b}{C\{a\} R C\{b\}} \quad (2)$$

Theorem (Clarke et al., §4.4)

TFAE:

- $(a \triangleright b) \rightsquigarrow (s \triangleright t)$
- For every \leq -respecting, context-respecting $R \subseteq X \times Y$,
 $a R b \rightarrow s R t$.

Example: Use “is an anagram of” for R and consider

$$(\text{"ACT"} \triangleright \text{"CAT"}) \rightsquigarrow (\text{"hello ACT"} \triangleright \text{"hello CAT"})$$

... and we have profunctor optics

We've been working Ω -enriched

Ω -enriched special case	General concept
Proset	Category
Preordered monoid	Monoidal category
Preordered \mathbf{M} -set	\mathbf{M} -actegory
Existential \leq -respecting relation	Coend
\leq -, context-respecting relation	Profunctor
Inequality in $\mathbf{Optic}_{X,Y}$	Tambara module
	Hom-set in $\mathbf{Optic}_{C,D}$

For references on profunctor optics, see

- Bryce Clarke et al. *Profunctor optics, a categorical update*. 2020. arXiv: 2001.07488 [cs.PL]
- Mitchell Riley. *Categories of Optics*. 2018. arXiv: 1809.00738 [math.CT]

... and we have profunctor optics

We've been working **depleted**

Depleted special case	General concept
Proset	Category
Preordered monoid	Monoidal category
Preordered M -set	M -actegory
Existential \leq -respecting relation	Coend
\leq -, context-respecting relation	Profunctor
Inequality in Optic _{X,Y}	Tambara module
	Hom-set in Optic _{C,D}

For references on profunctor optics, see

- Bryce Clarke et al. *Profunctor optics, a categorical update*. 2020. arXiv: 2001.07488 [cs.PL]
- Mitchell Riley. *Categories of Optics*. 2018. arXiv: 1809.00738 [math.CT]

Table of Contents

- 1 Some background on separation logic
- 2 Optics in prosets
- 3 Optics for separation logic**
- 4 Conclusion

Hoare triples as profunctors

Let \mathcal{S} be the proset of assertions, with \vdash as the ordering.

$$H_C \subseteq \mathcal{S} \times \mathcal{S}$$
$$P H_C Q \triangleq \{P\} C \{Q\}$$

Then Hoare logic's rule of consequence states exactly that H_C is \leq -respecting (i.e., a depleted profunctor).

$$\frac{P' \vdash P \quad \{P\} C \{Q\} \quad Q \vdash Q'}{\{P'\} C \{Q'\}} \text{ (Consequence)}$$

Hoare triples as profunctors

Let \mathcal{S} be the proset of assertions, with \vdash as the ordering.

$$H_C \subseteq \mathcal{S} \times \mathcal{S}$$
$$P H_C Q \triangleq \{P\} C \{Q\}$$

Then Hoare logic's rule of consequence states exactly that H_C is \leq -respecting (i.e., a depleted profunctor).

$$\frac{P' \leq P \quad P H_C Q \quad Q \leq Q'}{P' H_C Q'} \text{ (Consequence)}$$

Hoare triples as Tambara modules

Let our monoid of contexts be \mathcal{S} itself under the operation $*$. So \mathcal{S} also forms a preordered left \mathcal{S} -set under the left regular action $(\mathcal{C} \star P \triangleq \mathcal{C} * P)$. Then separation logic's frame rule states exactly that $H_{\mathcal{C}}$ is context-respecting (i.e., a depleted Tambara module) as a relation from this \mathcal{S} -set to itself.

$$\frac{\{P\} C \{Q\}}{\{F * P\} C \{F * Q\}} \text{ (Frame)}$$

Hoare triples as Tambara modules

Let our monoid of contexts be \mathcal{S} itself under the operation $*$. So \mathcal{S} also forms a preordered left \mathcal{S} -set under the left regular action $(\mathcal{C} \star P \triangleq \mathcal{C} * P)$. Then separation logic's frame rule states exactly that H_C is context-respecting (i.e., a depleted Tambara module) as a relation from this \mathcal{S} -set to itself.

$$\frac{P H_C Q}{F\{P\} H_C F\{Q\}} \text{ (Frame)}$$

Hoare triples as Tambara modules

Let our monoid of contexts be \mathcal{S} itself under the operation $*$. So \mathcal{S} also forms a preordered left \mathcal{S} -set under the left regular action $(\mathcal{C} \star P \triangleq \mathcal{C} * P)$. Then separation logic's frame rule states exactly that H_C is context-respecting (i.e., a depleted Tambara module) as a relation from this \mathcal{S} -set to itself.

$$\frac{P H_C Q}{F\{P\} H_C F\{Q\}} \text{ (Frame)}$$

Using \rightsquigarrow from **Optic** $_{\mathcal{S}, \mathcal{S}}$, we have

$$\frac{(P \triangleright Q) \rightsquigarrow (R \triangleright R') \quad \{P\} C \{Q\}}{\{R\} C \{R'\}}$$

Concrete representations for optic inequalities

Say we have an arbitrary \mathbf{M}, X, Y as in the setup for $\mathbf{Optic}_{X,Y}$. Let $b \in Y$. Suppose $- \{b\} : \mathbf{M} \rightarrow Y$ has a right adjoint $- [b \mapsto \circ] : Y \rightarrow \mathbf{M}$, so

$$\forall t \in Y. \mathcal{C}\{b\} \leq t \iff \mathcal{C} \leq t[b \mapsto \circ].$$

Concrete representations for optic inequalities

Say we have an arbitrary \mathbf{M}, X, Y as in the setup for $\mathbf{Optic}_{X,Y}$. Let $b \in Y$. Suppose $- \{b\} : \mathbf{M} \rightarrow Y$ has a right adjoint $- [b \mapsto \circ] : Y \rightarrow \mathbf{M}$, so

$$\forall t \in Y. \mathcal{C}\{b\} \leq t \iff \mathcal{C} \leq t[b \mapsto \circ].$$

Then (Riley, §4.4)

$$(a \triangleright b) \rightsquigarrow (s \triangleright t) \iff s \leq t[b \mapsto \circ]\{a\}$$

Concrete representations for optic inequalities

Say we have an arbitrary \mathbf{M}, X, Y as in the setup for $\mathbf{Optic}_{X,Y}$. Let $b \in Y$. Suppose $- \{b\} : \mathbf{M} \rightarrow Y$ has a right adjoint $- [b \mapsto \circ] : Y \rightarrow \mathbf{M}$, so

$$\forall t \in Y. C\{b\} \leq t \iff C \leq t[b \mapsto \circ].$$

Then (Riley, §4.4)

$$(a \triangleright b) \rightsquigarrow (s \triangleright t) \iff s \leq t[b \mapsto \circ]\{a\}$$

When $\mathbf{M} = X = Y = \mathcal{S}$:

$$\begin{aligned} -\{Q\} &= (- * Q) \dashv (Q * -) \\ \therefore R' [Q \mapsto \circ] \{P\} &= (Q * R') * P \\ \therefore (P \triangleright Q) \rightsquigarrow (R \triangleright R)' &\iff R \vdash (Q * R') * P \end{aligned}$$

And combining with last slide:

$$\frac{R \vdash (Q * R') * P \quad \{P\} C \{Q\}}{\{R\} C \{R'\}} \text{ (Ramify)}$$

Table of Contents

- 1 Some background on separation logic
- 2 Optics in prosets
- 3 Optics for separation logic
- 4 Conclusion**

...so what?

- The Ramify rule drops out of “Use \rightsquigarrow to focus a proof when the statement is $a R b$, for a depleted Tambara module R ” and “Having an adjunction lets you express \rightsquigarrow in one of your original prosets” if you plug in the correct \mathbf{M}, X, Y, R
- Tambara modules, adjunctions, actions, etc have tons of categorical structure useful for building all kinds of other \mathbf{M} s, X s, Y s, and R s
- **Altogether**: depleted optics and Tambara modules give a unified framework for 1. exploiting category-theoretic constructions to manufacture different kinds of ramification-style rules; 2. relating the definitions involved in the different kinds to each other
- You would not *believe* how much mileage I've gotten out of $\exists \vdash \Delta \vdash \forall$

Future directions

- One useful \mathbf{M} is $\text{End}(A)$, where A is an object of the category $\mathcal{S}\text{-Mat}$ as on [the nLab page “quantaloid”](#)—but it would be *more* useful to use the whole category instead of one endomorphism monoid, if that only fit into the definition of $\mathbf{Optic}_{X,Y}$.
- Investigate a proof assistant ergonomics perspective explicitly. Could you build a useful set of Coq tactics that make use of these definitions?
- Look for other places in the depleted world where optics might be hiding. Maybe the example with strings suggests relevance to formal grammars?