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

\{P\} \ C \ \{Q\}

Precondition  Command  Postcondition

Examples:

- \{x < y \land x, y \in \mathbb{Z}\} x := x + 1 \{x \leq y \land 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 } \{\bot\}
Hoare logic

\[ \{ P \} \ C \ { Q \} \]

Precondition  Command  Postcondition

Examples:
- \( \{ x < y \land x, y \in \mathbb{Z} \} \ x := x + 1 \ { x \leq y \land x, y \in \mathbb{Z} \} \)
- \( \{ \text{islist}(l) \} \ 	ext{sort\_in\_place}(l) \ { \forall i \leq j < |l|. \ l_i \leq l_j } \)
- \( \{ x > 0 \} \ \text{while } x > 0 \ \text{do} \ x := x + 1 \ \text{end} \ { \bot } \)
Hoare logic

\[ \{ P \} \quad C \quad \{ Q \} \]

Precondition  Command  Postcondition

Examples:

- \{ x < y \land x, y \in \mathbb{Z} \} \ x := x + 1 \ \{ x \leq y \land x, y \in \mathbb{Z} \} 
- \{ \text{islist}(l) \} \quad \text{sort\_in\_place}(l) \ \{ \forall i \leq j < |l|. \ l_i \leq l_j \} 
- \{ x > 0 \} \quad \text{while} \ x > 0 \ \text{do} \ x := x + 1 \ \text{end} \ \{ \bot \}
Hoare logic, cont’d

Entailment of assertions

\[ P' \vdash P \quad \{P\} \quad C \quad \{Q\} \quad Q \vdash Q' \]

\[ \frac{P' \vdash P \quad \{P\} \quad C \quad \{Q\} \quad Q \vdash Q'}{\{P'\} \quad C \quad \{Q'\}} \]

(Consequence)

\[ \frac{\{P\} \quad C \quad \{Q\} \quad \{Q\} \quad D \quad \{R\}}{\{P\} \quad C; \quad D \quad \{R\}} \]

(Sequencing)
The frame problem

\[ \text{Frame?} \]

\[
\begin{align*}
\{P\} C \{Q\} & \quad \{F \land P\} C \{F \land Q\}
\end{align*}
\]

✓ \{x \geq y\} \quad x := x + 1 \{x > y\}

✓ \{\text{sorted}(l) \land x \geq y\} \quad x := x + 1 \{\text{sorted}(l) \land x > y\}
The frame problem

\[
\frac{\{P\} \text{C} \{Q\}}{\{F \land P\} \text{C} \{F \land Q\}} \quad \text{(Frame?)}
\]

\[
\checkmark \quad \{x \geq y\} \quad x := x + 1 \{x > y\}
\]

\[
\checkmark \quad \{\text{sorted}(l) \land x \geq y\} \quad x := x + 1 \{\text{sorted}(l) \land x > y\}
\]

Nope!

\[
\checkmark \quad \{\text{pressable}(b)\} \quad \text{press}(b) \{\text{pressed}(b)\}
\]

\[
\times \quad \{\text{presses}(3) \land \text{pressable}(b)\} \quad \text{press}(b) \{\text{presses}(3) \land \text{pressed}(b)\}
\]
Separating conjunction (and implication)

Write $\triangledown \models P$ for “assertion $P$ holds in state fragment $\triangledown$".

\[
\begin{align*}
\bullet \models P & \quad \bullet \models Q \\
\bullet \models P \land Q
\end{align*}
\]

\[
\begin{align*}
\bullet \models P & \quad \triangledown \models Q \\
\triangledown \models P \land Q
\end{align*}
\]

\[
\begin{align*}
\bullet \models P & \\
\vdots & \\
\bullet \models Q & \\
\bullet \models P \rightarrow Q
\end{align*}
\]

\[
\begin{align*}
\triangledown \models P & \\
\vdots & \\
\triangledown \models Q & \\
\triangledown \models P \rightarrow* Q
\end{align*}
\]

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

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

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

$P \land Q \vdash R \iff P \vdash Q \rightarrow* R$
The frame rule

\[
\frac{\{P\} \quad C \quad \{Q\}}{\{F \ast P\} \quad C \quad \{F \ast Q\}} \quad \text{(Frame)}
\]

\[
\begin{align*}
\checkmark \quad \{x \geq y\} & \quad x := x + 1 \{x > y\} \\
\checkmark \quad \{\text{sorted}(l) \ast x \geq y\} & \quad x := x + 1 \{\text{sorted}(l) \ast x > y\}
\end{align*}
\]

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

\[
\begin{align*}
\checkmark \quad \{\text{pressable}(b)\} & \quad \text{press}(b) \{\text{pressed}(b)\} \\
\checkmark \quad \{\text{presses}(3) \ast \text{pressable}(b)\} & \quad \text{press}(b) \{\text{presses}(3) \ast \text{pressed}(b)\}
\end{align*}
\]
Spatial information

\( P \star Q \parallel Q \star P \)

\((P \star Q) \star R \parallel P \star (Q \star R)\)
Spatial information

\[ P \ast Q \vdash Q \ast P \]
\[ (P \ast Q) \ast R \vdash P \ast (Q \ast R) \]

\[ 2^2 = 4 \vdash (2^2 = 4) \ast (2^2 = 4) \]
\[ l_3 = 5 \not\vdash (l_3 = 5) \ast (l_3 = 5) \]
\[ \exists i. l_i = 5 \not\vdash (\exists i. l_i = 5) \ast (\exists i. l_i = 5) \]
Spatial information

$P * Q \iff Q * P$

$(P * Q) * R \iff P * (Q * R)$

$2^2 = 4 \vdash (2^2 = 4) * (2^2 = 4)$

$l_3 = 5 \not\vdash (l_3 = 5) * (l_3 = 5)$

$\exists i. l_i = 5 \not\vdash (\exists i. l_i = 5) * (\exists i. l_i = 5)$

$(P \rightarrow Q) * P \vdash Q \quad Q \vdash P \rightarrow P * Q$

$p_1 = 3 \vdash p_2 = 4 \leadsto p = (3, 4)$

$l_3 = 5 \vdash l_3 = 5 \leadsto \bot$
An admissible rule:

\[
R \vdash (Q \rightarrow R') \ast P \quad \{P\} \ C \{Q\} \\
\{R\} \ C \{R'\}
\]

(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

This looks an awful lot like a lens!

\[
\frac{R \vdash (Q \rightarrow R') \ast P}{\{P\} C \{Q\}} \quad \text{(Ramify)} \quad \{R\} C \{R'\}
\]

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


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

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

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

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

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

$$s[...]t \star u \triangleq sut$$
Fix a preordered monoid $M$ and preordered left $M$-sets $X, Y$.

**Definition (Clarke et al., §2)**

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

- 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

\[(a \triangleright b) \rightsquigarrow (s \triangleright t) \triangleq \exists C \in M. \ (s \leq C\{a\}) \land (C\{b\} \leq t)\]

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

\[\text{("m" \triangleright "mad") \rightsquigarrow ("me" \triangleright "made") \rightsquigarrow ("Edit me!" \triangleright "Edit made!")}\]
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).

\[
\frac{a' \leq a \quad a \ R \ b \quad b \leq b'}{a' \ R \ b'} \quad (1) \quad \frac{a \ R \ b}{C\{a\} \ R \ C\{b\}} \quad (2)
\]

Theorem (Clarke et al., §4.4)

TFAE:

- \((a \Rightarrow b) \rightsquigarrow (s \Rightarrow t)\)
- 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

\(("ACT" \Rightarrow "CAT") \rightsquigarrow ("hello ACT" \Rightarrow "hello CAT")\)
... and we have profunctor optics

We’ve been working $\Omega$-enriched

<table>
<thead>
<tr>
<th>$\Omega$-enriched special case</th>
<th>General concept</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proset</td>
<td>Category</td>
</tr>
<tr>
<td>Preordered monoid</td>
<td>Monoidal category</td>
</tr>
<tr>
<td>Preordered $\mathcal{M}$-set</td>
<td>$\mathcal{M}$-actegory</td>
</tr>
<tr>
<td>Existential</td>
<td>Coend</td>
</tr>
<tr>
<td>$\leq$-respecting relation</td>
<td>Profunctor</td>
</tr>
<tr>
<td>$\leq$, context-respecting relation</td>
<td>Tambara module</td>
</tr>
<tr>
<td>Inequality in $\text{Optic}_{X,Y}$</td>
<td>Hom-set in $\text{Optic}_{C,D}$</td>
</tr>
</tbody>
</table>

For references on profunctor optics, see

...and we have profunctor optics

We’ve been working **depleted**

<table>
<thead>
<tr>
<th>Depleted special case</th>
<th>General concept</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proset</td>
<td>Category</td>
</tr>
<tr>
<td>Preordered monoid</td>
<td>Monoidal category</td>
</tr>
<tr>
<td>Preordered $M$-set</td>
<td>$M$-actegory</td>
</tr>
<tr>
<td>Existential</td>
<td>Coend</td>
</tr>
<tr>
<td>$\leq$-respecting relation</td>
<td>Profunctor</td>
</tr>
<tr>
<td>$\leq$-, context-respecting relation</td>
<td>Tambara module</td>
</tr>
</tbody>
</table>

Inequality in $\text{Optic}_{X,Y}$ | Hom-set in $\text{Optic}_{C,D}$

For references on profunctor optics, see

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 $S$ be the proset of assertions, with $\vdash$ as the ordering.

$$H_C \subseteq S \times S$$

$$P \ H_C \ Q \triangleq \{P\} \ C \{Q\}$$

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

$$\frac{P' \vdash P \quad \{P\} \ C \{Q\} \quad Q \vdash Q'}{\{P'\} \ C \{Q'\}} \quad \text{(Consequence)}$$
Let $S$ be the proset of assertions, with $\vdash$ as the ordering.

$$H_C \subseteq S \times S$$

$$P \ H_C \ Q \triangleq \{P\} \ C \{Q\}$$

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

$$\frac{P' \leq P}{P' \ H_C \ Q'} \quad \frac{P \ H_C \ Q \quad Q \leq Q'}{P' \ H_C \ Q'} \quad \text{(Consequence)}$$
Hoare triples as Tambara modules

Let our monoid of contexts be $S$ itself under the operation $\ast$. So $S$ also forms a preordered left $S$-set under the left regular action $(C \ast P \triangleq C \ast P)$. 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 $S$-set to itself.

\[
\begin{array}{c}
\{P\} 
C 
\{Q\} \\
\{F \ast P\} 
C 
\{F \ast Q\}
\end{array}
\] (Frame)
Let our monoid of contexts be $S$ itself under the operation $\ast$. So $S$ also forms a preordered left $S$-set under the left regular action $(C \ast P \triangleq C \ast P)$. 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 $S$-set to itself.

\[
\begin{array}{c}
P \xrightarrow{H_C} Q \\
F\{P\} H_C F\{Q\}
\end{array}
\quad \text{(Frame)}
\]
Hoare triples as Tambara modules

Let our monoid of contexts be $S$ itself under the operation $\ast$. So $S$ also forms a preordered left $S$-set under the left regular action $(C \ast P \triangleq C \ast P)$. 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 $S$-set to itself.

\[
\frac{P \ H_C \ Q}{F\{P\} \ H_C \ F\{Q\}} \tag{Frame}
\]

Using $\leadsto$ from Optic$_{S,S}$, we have

\[
(P \triangleright Q) \leadsto (R \triangleright R') \quad \{P\} \ C \ {Q}\]

\[
\{R\} \ C \ {R'}
\]
Concrete representations for optic inequalities

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

$$\forall t \in Y. \ C\{b\} \leq t \iff C \leq t[b \mapsto \circ].$$
Concrete representations for optic inequalities

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

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

Then (Riley, §4.4)

$$(a \triangleright b) \leadstooverline{(s \triangleright t)} \iff s \leq t[b \mapsto \circ]\{a\}$$
Concrete representations for optic inequalities

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

$$-\{Q\} = (- * Q) \dashv (Q \dashv -)$$

$$\therefore \ R'[Q \mapsto \circ]\{P\} = (Q \dashv R') * P$$

$$\therefore \ (P \triangleright Q) \rightsquigarrow (R \triangleright R)' \iff R \vdash (Q \dashv R') * P$$

And combining with last slide:

$$\begin{array}{c}
R \vdash (Q \dashv R') * P \\
\{P\} C \{Q\} \\
\{R\} C \{R'\}\end{array} \quad (\text{Ramify})$$
1. Some background on separation logic

2. Optics in prosets

3. Optics for separation logic

4. Conclusion
The Ramify rule drops out of “Use $\rightsquigarrow$ to focus a proof when the statement is $a \vdash R b$, 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 $\exists \vdash \Delta \vdash \forall$.
One useful $M$ is $\text{End}(A)$, where $A$ is an object of the category $S$-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 $\text{Optic}_{X,Y}$.

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?