Separation Logic Through a New Lens

Sarah Rovner-Frydman

Marlboro College

May 6, 2020

Table of Contents

Table of Contents

Hoare logic

$$\{P\}\; C\; \{Q\}$$

Precondition Command Postcondition

Examples:

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

Hoare logic

$$\{\underbrace{P}_{\text{Precondition}}\}\ \underbrace{C}_{\text{Command}}\ \{\underbrace{Q}_{\text{Postcondition}}\}$$

Examples:

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

Hoare logic

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

Precondition Command Postcondition

Examples:

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

Hoare logic, cont'd

Entailment of assertions

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

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

The frame problem

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

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

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

The frame problem

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

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

Nope!

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

Separating conjunction (and implication)

Write $\text{◗} \models P$ for “assertion P holds in state fragment ◗”.

$$\frac{\text{●} \models P \qquad \text{●} \models Q}{\text{●} \models P \land Q} \qquad\qquad \frac{\text{◖} \models P \qquad \text{◗} \models Q}{\text{●} \models P * Q}$$

$$\frac{\begin{array}{c}\text{●} \models P \\ \vdots \\ \text{●} \models Q\end{array}}{\text{●} \models P \to Q} \qquad\qquad \frac{\begin{array}{c}\text{◖} \models P \\ \vdots \\ \text{●} \models Q\end{array}}{\text{◗} \models P \mathrel{-\!\!*} Q}$$

$$P \land Q \vdash R \iff P \vdash Q \to R \qquad\qquad P * Q \vdash R \iff P \vdash Q \mathrel{-\!\!*} R$$

The frame rule

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

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

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

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

✓ $\{\text{pressable}(b)\}\ \text{press}(b)\ \{\text{pressed}(b)\}$

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

Spatial information

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

Spatial information

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

$$2^2 = 4 \vdash (2^2 = 4) * (2^2 = 4)$$
$$l_3 = 5 \nvdash (l_3 = 5) * (l_3 = 5) \qquad \exists i. l_i = 5 \nvdash (\exists i. l_i = 5) * (\exists i. l_i = 5)$$

Spatial information

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

$$2^2 = 4 \vdash (2^2 = 4) * (2^2 = 4)$$
$$l_3 = 5 \nvdash (l_3 = 5) * (l_3 = 5) \qquad \exists i. l_i = 5 \nvdash (\exists i. l_i = 5) * (\exists i. l_i = 5)$$

$$(P \mathrel{-\!\!*} Q) * P \vdash Q \qquad Q \vdash P \mathrel{-\!\!*} P * Q$$
$$p_1 = 3 \vdash p_2 = 4 \mathrel{-\!\!*} p = (3, 4) \qquad l_3 = 5 \vdash l_3 = 5 \mathrel{-\!\!*} \bot$$

Spatial information, manipulation of

An admissible rule:

$$\frac{R \vdash (Q \mathrel{-\!\!*} R') * P \qquad \{P\}\, C\, \{Q\}}{\{R\}\, C\, \{R'\}} \text{ (Ramify)}$$

> *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

A similar concept is described by Qinxiang Cao et al. *Proof Pearl: Magic Wand as Frame*. 2019. arXiv: 1909.08789 [cs.PL]

Spatial information, manipulation of

This looks an awful lot like a lens!

$$\frac{R \vdash (Q \mathrel{-\!\!*} R') * P \qquad \{P\}\, C\, \{Q\}}{\{R\}\, C\, \{R'\}} \text{ (Ramify)}$$

> *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

A similar concept is described by Qinxiang Cao et al. *Proof Pearl: Magic Wand as Frame*. 2019. arXiv: 1909.08789 [cs.PL]

This sounds an awful lot like a lens!

Table of Contents

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 $\mathcal{C} \in \mathbf{M}$, $a \in X$, write $\mathcal{C}\{a\}$ for $\mathcal{C} \star a$. Think of elements of $\mathbf{M}$ as nestable contexts into which we can place elements of X.

$$\circ\{a\} = a \qquad (\mathcal{C}_1 \cdot \mathcal{C}_2)\{a\} = \mathcal{C}_1\{\mathcal{C}_2\{a\}\}$$

$\mathbf{M}$ itself canonically has the left regular action $\mathcal{C}_1 \star \mathcal{C}_2 \triangleq \mathcal{C}_1 \cdot \mathcal{C}_2$, and then the monoid laws say:

$$\mathcal{C} = \mathcal{C}\{\circ\} = \circ\{\mathcal{C}\} \qquad (\mathcal{C}_1\{\mathcal{C}_2\{\circ\}\})\{\mathcal{C}_3\{\circ\}\} = \mathcal{C}_1\{\mathcal{C}_2\{\mathcal{C}_3\{\circ\}\}\}$$

Also, we can rewrite the second action law as

$$(\mathcal{C}_1\{\mathcal{C}_2\{\circ\}\})\{a\} = \mathcal{C}_1\{\mathcal{C}_2\{a\}\}$$

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 $s[\ldots]t$
- Operation of **M**: nesting. Identity is ""[...]"".

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

- Action on the set of strings: insertion.

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

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 $\mathbf{Optic}_{X,Y}$.

- 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

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

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

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

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).

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

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

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

. . . 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	Coend
$\leq$-respecting relation	Profunctor
$\leq$-, context-respecting relation	Tambara module
Inequality in $\mathbf{Optic}_{X,Y}$	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 $\mathbf{M}$-set	$\mathbf{M}$-actegory
Existential	Coend
$\leq$-respecting relation	Profunctor
$\leq$-, context-respecting relation	Tambara module
Inequality in $\mathbf{Optic}_{X,Y}$	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]

Table of Contents

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).

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

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).

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

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_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 $\mathbf{Optic}_{\mathcal{S},\mathcal{S}}$, we have

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

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 $-\{b\} : \mathbf{M} \to Y$ has a right adjoint $-[b \mapsto \circ] : Y \to \mathbf{M}$, 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 $-\{b\} : \mathbf{M} \to Y$ has a right adjoint $-[b \mapsto \circ] : Y \to \mathbf{M}$, 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 $-\{b\} : \mathbf{M} \to Y$ has a right adjoint $-[b \mapsto \circ] : Y \to \mathbf{M}$, so

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

Then (Riley, §4.4)

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

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

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

And combining with last slide:

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

Table of Contents

. . . 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, Xs, Ys, and Rs
- 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 $\exists \dashv \Delta \dashv \forall$

Future directions

- One useful $\mathbf{M}$ is $\mathrm{End}(A)$, where A is an object of the category $\mathcal{S}$-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 $\mathbf{Optic}_{X,Y}$.
- 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?