Exorcis: Separating Angels from Demons in Logical Relations

Eugène Flesselle
Benjamin Peters Derek Dreyer

Iris Workshop 2026

Our Goal in this Work

We want to prove **effect-dependent (sequential) program transformations**

- Deduplicating computations w/ only read effects
- Reordering computations w/ effects on separate regions

We want to do this in the presence of **semantic typing**

- Should be possible to treat a term as "read-only" even if it does internal writes to global state, *so long as the writes are not observable*

Over 10 years ago, Benton et al. proposed "proof-relevant logical relations"

- Similar goals to ours, but pre-Iris, not mechanized, no higher-order state, no nondeterminism

We want to handle all these features in a beautiful Iris-style logic!

Effect-Dependent Program Transformations

$$\textsc{dedup}\ \frac{\Gamma \vDash e : \tau \mathbin{@} \varepsilon \qquad \mathsf{wrs}\,\varepsilon = \mathsf{als}\,\varepsilon = \emptyset}{\Gamma \vDash \mathtt{let}\ x = e\ \mathtt{in}\ (x, x) \lesssim (e, e) : \tau \times \tau \mathbin{@} \varepsilon}$$

Effect-Dependent Program Transformations

$$\textsc{reorder}\quad \frac{\Gamma \vDash e_1 : \tau_1 \mathbin{@} \varepsilon_1 \qquad \Gamma \vDash e_2 : \tau_2 \mathbin{@} \varepsilon_2 \qquad \mathsf{efs}\,\varepsilon_1 \;\#\#\; \mathsf{efs}\,\varepsilon_2}{\Gamma \vDash \mathtt{let}\, x_1 = e_1 \,\mathtt{in}\, (x_1, e_2) \lesssim \mathtt{let}\, x_2 = e_2 \,\mathtt{in}\, (e_1, x_2) : \tau_1 \times \tau_2 \mathbin{@} \varepsilon_1, \varepsilon_2}$$

Effect-Dependent Program Typing

Example (tmp-write $l\ v\ e$)

$$
\begin{array}{l}
\texttt{let}\ y = !\,l\ \texttt{in}\ \text{(* save *)} \\
l \leftarrow v; \qquad\qquad \text{(* modify *)} \\
\texttt{let}\ z = e\ \texttt{in} \\
l \leftarrow y; \qquad\qquad \text{(* restore *)} \\
z
\end{array}
$$

$$
\frac{\Gamma, l : \mathsf{ref}\, r\, \tau, x : \tau \vDash e : \tau_2 \,@\, \varepsilon}{\Gamma, l : \mathsf{ref}\, r\, \tau, x : \tau \vDash \mathsf{tmp\text{-}write}\ l\ x\ e : \tau_2 \,@\, \varepsilon, \mathsf{rd}\, r}
$$

Effect-Dependent Program Typing

Example (equi-write $l\ f$)

$$\begin{array}{l}\texttt{let}\ y = !\, l\ \texttt{in}\\ \texttt{let}\ z = f\ y\ \texttt{in}\\ l \leftarrow z;\\ z\end{array}$$

$$\frac{\Gamma, l : \mathsf{ref}\, r\, \tau, x : \tau \vDash f\ x \simeq x : \tau \mathbin{@} \varepsilon}{\Gamma, l : \mathsf{ref}\, r\, \tau \vDash \mathsf{equi\text{-}write}\ l\ f\ : \tau \mathbin{@} \varepsilon, \mathsf{rd}\, r}$$

State-of-the-art

	model	mechanized	program logic	transforms	tmp-write	equi-write	effectful ops	dynamic alloc	higher-order state	non-termination	non-determinism	racy concurrency
BentonKHB APLAS 06	denot	●	○	$\simeq$	●	○	●	○	○	○	○	○
BentonHN POPL 14	denot	○	○	$\preceq$ $\simeq$	●	●	●	●	○	●	○	○
BentonHN PPDP 16	denot	○	○	$\preceq$ $\preceq$	●	●	●	⊘	○	●	●	●
ThamsborgB ICFP 11	kripke	○	○	$\preceq$ $\preceq$	●	○	●	●	●	●	○	○
BaoJWBR OOPSLA 25	kripke	●	○	$\simeq$ $\preceq$	●	○	●	●	○	○	○	○
JespersenSB POPL 17	iris	○	○	$=$ $\preceq$	○	○	●	●	●	●	●	●
TimanySJB POPL 18	iris	●	○	$\preceq$ $\preceq$	○	○	○	●	●	●	○	○
SpiesGTJKBD ICFP 22	iris	●	⊘	$\preceq$ $\preceq$	○	○	⊘	⊘	●	●	●	⊘
Present	iris	●	●	$\preceq$	●	●	●	●	●	●	●	○

● compatible; ⊘ partially; ○ incompatible

$\preceq$ similar refinements; $\simeq$ similar equivalences; $\|$ parallelization

Our Contribution: Exorcis

The first
mechanized semantic model of effects

in a language with
non-termination, non-determinism,
dynamic allocation, and higher-order state;

validating program
transformations like deduplication and reordering,
as well as typings like tmp-write and equi-write;

with a high-level (Iris-based) program logic.

Key Challenge

Standard approach to relational reasoning in Iris is **ReLoC** [Frumin et al. 2018]
ReLoC supports **"lockstep"** reasoning:

- If you want to use $e_1 \leq e_2$ in order to prove some other $e_1' \leq e_2'$, you need e_1 and e_2 to simultaneously appear in **evaluation position** in e_1' and e_2'

Problem: "Lockstep" reasoning is not good enough for transformations like reordering

- ReLoC demands lockstep reasoning by tying **angelic** reasoning (verification of spec code) to **demonic** reasoning (verification of implementation) in logical relation

Key Ideas

1. We support reorderings by separating angelic from demonic reasoning:
   - Achieved by **moving the angelic reasoning entirely into the postcondition** of the logical relation for expressions
   - This is not a new idea: runST paper [Timany et al. 2018] employed this before, but only supported reordering of observably pure expressions

2. We support reorderings for **observably stateful** expressions by allowing the demonic and angelic states to diverge.
   - Achieved by enriching logical relation with explicit **"heapotheses"**

3. We support dynamic allocation, higher-order functions, etc. by **"turning everything into capital letters"**
   - Superficially like in Janine's talk, but the details are very different
   - Generalizing log. rel. from relations on values to relations on Iris value predicates!

Pretend the value interpretation is a unary predicate

$$\mathcal{V}[\![\cdot]\!] \in \mathit{Val} \to \mathit{iProp}$$

s.t. relatedness coincides with equality for values,
as in a **first-order** language.

- We will rely on this.
- We have made this compatible with a **higher-order** language.

Lockstep Relational Reasoning in ReLoc

Lockstep reasoning: permits
assumptions $\mathcal{E}_{\blacksquare}\, e\, e'\, \phi$ about unknown expressions e and e' to be used
if
both expressions appear in evaluation contexts of the proof goal.

Lockstep Relational Reasoning in ReLoc

Lockstep reasoning: permits
assumptions $\mathcal{E}_{\blacksquare}\, e\, e'\, \phi$ about unknown expressions e and e' to be used
if
both expressions appear in evaluation contexts of the proof goal.

$$\ell \mapsto_{\mathrm{I}} 3 * \ell \mapsto_{\mathrm{S}} 3 * \mathcal{E}_{\blacksquare}\, e\, e'\, [\![\mathsf{int}]\!] \vdash \mathcal{E}_{\blacksquare}\, (!\,\ell + e)\, (e' + !\,\ell)\, [\![\mathsf{int}]\!]$$

Lockstep Relational Reasoning in ReLoc

Lockstep reasoning: permits
assumptions $\mathcal{E}_{\blacksquare}\, e\, e'\, \phi$ about unknown expressions e and e' to be used
if
both expressions appear in evaluation contexts of the proof goal.

LOAD-IMPL

$$\frac{\ell \mapsto_{\mathrm{I}} v * \mathcal{E}_{\blacksquare}\, v\, e'\, \phi}{\ell \mapsto_{\mathrm{I}} v * \mathcal{E}_{\blacksquare}\, !\ell\, e'\, \phi}$$

$$\ell \mapsto_{\mathrm{I}} 3 * \ell \mapsto_{\mathrm{S}} 3 * \mathcal{E}_{\blacksquare}\, e\, e'\, [\![\mathsf{int}]\!] \vdash \mathcal{E}_{\blacksquare}\, (!\ell + e)\, (e' + !\ell)\, [\![\mathsf{int}]\!]$$

Lockstep Relational Reasoning in ReLoc

Lockstep reasoning: permits
assumptions $\mathcal{E}_{\blacksquare}\, e\, e'\, \phi$ about unknown expressions e and e' to be used
if
both expressions appear in evaluation contexts of the proof goal.

LOAD-IMPL

$$\frac{\ell \mapsto_{\mathrm{I}} v * \mathcal{E}_{\blacksquare}\, v\, e'\, \phi}{\ell \mapsto_{\mathrm{I}} v * \mathcal{E}_{\blacksquare}\, !\ell\, e'\, \phi}$$

$$\ell \mapsto_{\mathrm{I}} 3 * \ell \mapsto_{\mathrm{S}} 3 * \mathcal{E}_{\blacksquare}\, e\, e'\, [\![\mathsf{int}]\!] \vdash \mathcal{E}_{\blacksquare}\, (3 + e)\, (e' + !\ell)\, [\![\mathsf{int}]\!]$$

Lockstep Relational Reasoning in ReLoc

Lockstep reasoning: permits
assumptions $\mathcal{E}_\blacksquare\ e\ e'\ \phi$ about unknown expressions e and e' to be used
if
both expressions appear in evaluation contexts of the proof goal.

LOAD-IMPL

$$\frac{\ell \mapsto_{\mathrm{I}} v * \mathcal{E}_\blacksquare\ v\ e'\ \phi}{\ell \mapsto_{\mathrm{I}} v * \mathcal{E}_\blacksquare\ !\ell\ e'\ \phi}$$

BIND-MONO

$$\frac{\mathcal{E}_\blacksquare\ e\ e'\ [\![\mathsf{int}]\!] \qquad \forall z.\ \mathcal{E}_\blacksquare\ k[v]\ k'[v]\ \phi}{\mathcal{E}_\blacksquare\ k[e]\ k'[e']\ \phi}$$

$$\ell \mapsto_{\mathrm{I}} 3 * \ell \mapsto_{\mathrm{S}} 3 * \mathcal{E}_\blacksquare\ e\ e'\ [\![\mathsf{int}]\!] \vdash \mathcal{E}_\blacksquare\ (3 + e)\ (e' + !\,\ell)\ [\![\mathsf{int}]\!]$$

Lockstep Relational Reasoning in ReLoc

Lockstep reasoning: permits
assumptions $\mathcal{E}_\blacksquare\ e\ e'\ \phi$ about unknown expressions e and e' to be used
if
both expressions appear in evaluation contexts of the proof goal.

LOAD-IMPL

$$\frac{\ell \mapsto_{\mathrm{I}} v * \mathcal{E}_\blacksquare\ v\ e'\ \phi}{\ell \mapsto_{\mathrm{I}} v * \mathcal{E}_\blacksquare\ !\ell\ e'\ \phi}$$

BIND-MONO

$$\frac{\mathcal{E}_\blacksquare\ e\ e'\ [\![\mathsf{int}]\!] \qquad \forall z.\ \mathcal{E}_\blacksquare\ k[v]\ k'[v]\ \phi}{\mathcal{E}_\blacksquare\ k[e]\ k'[e']\ \phi}$$

$$\ell \mapsto_{\mathrm{I}} 3 * \ell \mapsto_{\mathrm{S}} 3 \vdash \mathcal{E}_\blacksquare\ (3 + z)\ (z + !\ell)\ [\![\mathsf{int}]\!]$$

Lockstep Relational Reasoning in ReLoc

Lockstep reasoning: permits
assumptions $\mathcal{E}_\blacksquare\, e\, e'\, \phi$ about unknown expressions e and e' to be used
if
both expressions appear in evaluation contexts of the proof goal.

LOAD-IMPL

$$\frac{\ell \mapsto_{\mathrm{I}} v * \mathcal{E}_\blacksquare\, v\, e'\, \phi}{\ell \mapsto_{\mathrm{I}} v * \mathcal{E}_\blacksquare\, !\ell\, e'\, \phi}$$

BIND-MONO

$$\frac{\mathcal{E}_\blacksquare\, e\, e'\, [\![\mathsf{int}]\!] \qquad \forall z.\, \mathcal{E}_\blacksquare\, k[v]\, k'[v]\, \phi}{\mathcal{E}_\blacksquare\, k[e]\, k'[e']\, \phi}$$

LOAD-SPEC

$$\frac{\ell \mapsto_{\mathrm{S}} v * \mathcal{E}_\blacksquare\, e\, v\, \phi}{\ell \mapsto_{\mathrm{S}} v * \mathcal{E}_\blacksquare\, e\, !\ell\, \phi}$$

$$\ell \mapsto_{\mathrm{I}} 3 * \ell \mapsto_{\mathrm{S}} 3 \vdash \mathcal{E}_\blacksquare\, (3 + z)\, (z + !\ell)\, [\![\mathsf{int}]\!]$$

Lockstep Relational Reasoning in ReLoc

Lockstep reasoning: permits
assumptions $\mathcal{E}_\blacksquare\ e\ e'\ \phi$ about unknown expressions e and e' to be used
if
both expressions appear in evaluation contexts of the proof goal.

LOAD-IMPL

$$\frac{\ell \mapsto_{\mathrm{I}} v * \mathcal{E}_\blacksquare\ v\ e'\ \phi}{\ell \mapsto_{\mathrm{I}} v * \mathcal{E}_\blacksquare\ !\ell\ e'\ \phi}$$

BIND-MONO

$$\frac{\mathcal{E}_\blacksquare\ e\ e'\ [\![\mathsf{int}]\!] \qquad \forall z.\ \mathcal{E}_\blacksquare\ k[v]\ k'[v]\ \phi}{\mathcal{E}_\blacksquare\ k[e]\ k'[e']\ \phi}$$

LOAD-SPEC

$$\frac{\ell \mapsto_{\mathrm{S}} v * \mathcal{E}_\blacksquare\ e\ v\ \phi}{\ell \mapsto_{\mathrm{S}} v * \mathcal{E}_\blacksquare\ e\ !\ell\ \phi}$$

$$\ell \mapsto_{\mathrm{I}} 3 * \ell \mapsto_{\mathrm{S}} 3 \vdash \mathcal{E}_\blacksquare\ (3 + z)\ (z + 3)\ [\![\mathsf{int}]\!]$$

Lockstep Relational Reasoning in ReLoc

Lockstep reasoning: permits
assumptions $\mathcal{E}_\blacksquare\ e\ e'\ \phi$ about unknown expressions e and e' to be used
if
both expressions appear in evaluation contexts of the proof goal.

LOAD-IMPL

$$\frac{\ell \mapsto_{\mathrm{I}} v * \mathcal{E}_\blacksquare\ v\ e'\ \phi}{\ell \mapsto_{\mathrm{I}} v * \mathcal{E}_\blacksquare\ !\ell\ e'\ \phi}$$

BIND-MONO

$$\frac{\mathcal{E}_\blacksquare\ e\ e'\ [\![\mathsf{int}]\!] \qquad \forall z.\ \mathcal{E}_\blacksquare\ k[v]\ k'[v]\ \phi}{\mathcal{E}_\blacksquare\ k[e]\ k'[e']\ \phi}$$

LOAD-SPEC

$$\frac{\ell \mapsto_{\mathrm{S}} v * \mathcal{E}_\blacksquare\ e\ v\ \phi}{\ell \mapsto_{\mathrm{S}} v * \mathcal{E}_\blacksquare\ e\ !\ell\ \phi}$$

$$\ell \mapsto_{\mathrm{I}} 3 * \ell \mapsto_{\mathrm{S}} 5 \vdash 3 + z = z + 3$$

Non-Lockstep Relational Reasoning in ReLoc?

ReLoc permits
assumptions $\mathcal{E}_{\blacksquare}\, e\, e'\, \phi$ about unknown expressions e and e' to be used
if and only if
both expressions appear in evaluation contexts of the proof goal.

$$\mathcal{E}_{\blacksquare}\, e\, e'\, \phi \triangleq \forall k.\, \mathsf{spec}\, k[e'] \mathrel{-\!\!*} \mathsf{wp}\, e\, \{v.\, \mathsf{spec}\, k[v] * \phi\, v\}$$

Ephemeral spec $k[e']$ identifies the current specification expression being evaluated.

Inherently incompatible with transformations to "unknown code" evaluation order.

$$\mathcal{E}_{\blacksquare}\, e_1\, e_1' \, [\![\mathsf{unit}]\!] * \mathcal{E}_{\blacksquare}\, e_2\, e_2' \, [\![\mathsf{unit}]\!] \not\vdash \mathcal{E}_{\blacksquare}\, (e_1; e_2)\, (e_2'; e_1') \, [\![\mathsf{unit}]\!]$$

Non-Lockstep Expression Relation

$$\mathcal{E}_{\blacksquare}\ e\ e'\ \phi \triangleq \forall k.\ \mathsf{spec}\ k[e'] \mathrel{-\!\!*} \mathsf{wp}\ e\ \{v.\ \mathsf{spec}\ k[v] * \phi\ v\}$$

Non-Lockstep Expression Relation

Separate the demonic and angelic program "executions".

$$\mathcal{E}_{\blacksquare\curvearrowleft}\, e\, e'\, \phi \triangleq \mathsf{wp}\, e \left\{ v.\, (\forall k.\, \mathsf{spec}\, k[e'] \mathrel{-\!\!*} \dot{\Rrightarrow} \mathsf{spec}\, k[v]) * \phi\, v \right\}$$

Non-Lockstep Expression Relation

Separate the demonic and angelic weakest-preconditions.

$$\mathcal{E}_{\blacksquare\!\!\curvearrowright}\, e\, e'\, \phi \triangleq \mathsf{wp}_{\mathrm{I}}\, e\, \{v.\, \mathsf{wp}_{\mathrm{S}}\, e'\, \{v\} * \phi\, v\}$$

Non-Lockstep Expression Relation

Separate the demonic and angelic weakest-preconditions.

$$\mathcal{E}_{\blacksquare\curvearrowright}\, e\, e'\, \phi \triangleq \mathsf{wp}_{\mathrm{I}}\, e\, \{v.\, \mathsf{wp}_{\mathrm{S}}\, e'\, \{v\} * \phi\, v\}$$

Comparable approach to that of [Timany et al. 2018] and [Spies et al. 2022].

Compatibility with Effectful Operations?

The reference invariant, relating the states at any given time, is great to relate loads executed at the same time.

$$\boxed{\exists v.\, \ell \mapsto_{\mathrm{I}} v * \ell \mapsto_{\mathrm{S}} v * \tau\, v} \vdash \mathcal{E}_{\blacksquare}\ !\ell\ !\ell\ \tau$$

Compatibility with Effectful Operations?

The reference invariant, relating the states at any given time, is not so great to relate loads executed at different times.

$$\boxed{\exists v.\, \ell \mapsto_{\mathrm{I}} v * \ell \mapsto_{\mathrm{S}} v * \tau\, v} \not\vdash \mathcal{E}_{\blacksquare\curvearrowleft}\ !\ell\ !\ell\ \tau$$

Compatibility with Effectful Operations?

The reference invariant, relating the states at any given time, is not so great to relate loads executed at different times.

$$\boxed{\exists v.\, \ell \mapsto_{\mathrm{I}} v * \ell \mapsto_{\mathrm{S}} v * \tau\, v} \not\vdash \mathsf{wp}_{\mathrm{I}}\ !\,\ell\,\{v.\, \mathsf{wp}_{\mathrm{S}}\ !\,\ell\,\{v\} * \tau\, v\}$$

Compatibility with Effectful Operations?

The reference invariant, relating the states at any given time, is not so great to relate loads executed at different times.

$$\boxed{\exists v.\, \ell \mapsto_{\mathrm{I}} v * \ell \mapsto_{\mathrm{S}} v * \tau\, v} \vdash \mathsf{wp}_{\mathrm{I}}\ !\,\ell\,\{v.\ \mathsf{wp}_{\mathrm{S}}\ !\,\ell\,\{v\} * \tau\, v\}$$

Compatibility with Effectful Operations?

The reference invariant, relating the states at any given time, is not so great to relate loads executed at different times.

$$\boxed{\exists v.\, \ell \mapsto_{\mathrm{I}} v * \ell \mapsto_{\mathrm{S}} v * \tau\, v} \not\vdash \mathsf{wp}_{\mathrm{I}}\ !\,\ell\ \{v.\ \mathsf{wp}_{\mathrm{S}}\ !\,\ell\ \{v\} * \tau\, v\}$$

Compatibility with Effectful Operations?

The reference invariant, relating the states at any given time,
is not so great to relate loads executed at different times.

$$\boxed{\exists v.\, \ell \mapsto_{\mathrm{I}} v * \ell \mapsto_{\mathrm{S}} v * \tau\, v} \not\vdash \mathcal{E}_{\blacksquare\!\curvearrowleft}\ !\ell\ !\ell\ \tau$$

Separate the hypotheses about the demonic and angelic state of the heap.

$$\vdash \mathcal{E}\ [\![\ell : \tau]\!]\ !\ell\ !\ell\ \Phi$$

$$[\![\ell : \tau]\!] \approx \{\, h \mid \tau\ h[\ell]\,\} \in \mathit{Heap} \to \mathit{iProp}$$

Heapotheses

We **separately**
relate (the fragments of) the initial/final heaps of the evaluation, and
assert these agree with the ambient demonic/angelic ghost state of the wps.

$$\Sigma \in \mathit{Heap} \to \mathit{iProp}$$

$$\mathcal{E}\,\Sigma\,e\,e'\,\phi \triangleq \forall h.\,\Sigma\,h \mathrel{-\!\!*} \{h\}_{\mathrm{I}}\,e\,\{h', v.\,\{h\}_{\mathrm{S}}\,e'\,\{h', v\} * \Sigma\,h' * \phi\,v\}$$

$$\{h\}_b\,e\,\{h', v.\,\phi\} \triangleq \Box_b(\boxed{\circ h}^b \mathrel{-\!\!*} \mathsf{wp}_b\,e\,\{v.\,\exists h'.\,\boxed{\circ h'}^b * \phi\,h'\,v\}\,)$$

Reordering Effectful Computations

$$\textsc{reorder}\ \frac{*_{j=1,2}\ \mathcal{E}\ \Sigma_j\ (e_j \preccurlyeq e'_j)\ [\![\mathsf{unit}]\!]}{\mathcal{E}\ (\Sigma_1 \otimes \Sigma_2)\ (e_1; e_2 \preccurlyeq e'_2; e'_1)\ [\![\mathsf{unit}]\!]}$$

$$\Sigma_1 \otimes \Sigma_2 \triangleq \{\ h_1 * h_2 \mid \Sigma_1\, h_1 * \Sigma\, h_2\ \}$$

Reordering Effectful Computations

$$\textsc{SEQ-SEP}\quad \frac{\begin{array}{c} *_{j=1,2}\, \{h_j\}_b\ e_j\ \{h'_j, () \mid \Sigma_j\, h'_j\} \\ \forall h'_1, h'_2.\ \Sigma_1\, h'_1 * \Sigma_2\, h'_2 \mathrel{-\!\!*} \Sigma\, (h'_1 * h'_2) \end{array}}{\{h_1 * h_2\}_b\ e_1; e_2\ \{h', () \mid \Sigma\, h'\}}$$

Reordering Effectful Computations

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{*_{j=1,2}\ \mathcal{E}\ \Sigma_j\ (e_j \preccurlyeq e'_j)\ [\![\mathsf{unit}]\!]}}{}}{}}{}}{\mathcal{E}\ (\Sigma_1 \otimes \Sigma_2)\ (e_1; e_2 \preccurlyeq e'_2; e'_1)\ [\![\mathsf{unit}]\!]}$$

Reordering Effectful Computations

$$\frac{\ast_{j=1,2}\ \mathcal{E}\ \Sigma_j\ (e_j \preccurlyeq e'_j)\ [\![\mathsf{unit}]\!]}{\forall h_1, h_2.\ \ast_{j=1,2}\ \Sigma_j\ h_j \twoheadrightarrow \overline{\{h_1 * h_2\}_{\mathrm{I}}\ e_1; e_2\ \{h', () \mid \{h_1 * h_2\}_{\mathrm{S}}\ e'_2; e'_1\ \{h', ()\} * (\Sigma_1 \otimes \Sigma_2)\ h'\}}}{\mathcal{E}\ (\Sigma_1 \otimes \Sigma_2)\ (e_1; e_2 \preccurlyeq e'_2; e'_1)\ [\![\mathsf{unit}]\!]}$$

Reordering Effectful Computations

$$\dfrac{\dfrac{\dfrac{}{*_{j=1,2}\ \mathcal{E}\ \Sigma_j\ (e_j \preccurlyeq e'_j)\ [\![\mathsf{unit}]\!]}}{*_{j=1,2}\ \forall h_j.\ \Sigma_j\ h_j \mathrel{-\!\!*} \{h_j\}_{\mathrm{I}}\ e_j\ \{\ h'_j, () \mid \{h_j\}_{\mathrm{S}}\ e'_j\ \{h'_j, ()\} * \Sigma_j\ h'_j\}}}{}$$

$$\dfrac{\dfrac{}{\forall h_1, h_2.\ *_{j=1,2}\ \Sigma_j\ h_j \mathrel{-\!\!*} \overline{\{h_1 * h_2\}_{\mathrm{I}}\ e_1; e_2\ \{h', () \mid \{h_1 * h_2\}_{\mathrm{S}}\ e'_2; e'_1\ \{h', ()\} * (\Sigma_1 \otimes \Sigma_2)\ h'\}}}}{\mathcal{E}\ (\Sigma_1 \otimes \Sigma_2)\ (e_1; e_2 \preccurlyeq e'_2; e'_1)\ [\![\mathsf{unit}]\!]}$$

Reordering Effectful Computations

$$\frac{\ast_{j=1,2}\ \mathcal{E}\ \Sigma_j\ (e_j \preccurlyeq e'_j)\ [\![\mathsf{unit}]\!]}{\ast_{j=1,2}\ \forall h_j.\ \Sigma_j\ h_j \mathrel{-\!\!\ast} \{h_j\}_{\mathrm{I}}\ e_j\ \{\ h'_j, () \mid \{h_j\}_{\mathrm{S}}\ e'_j\ \{h'_j, ()\} \ast \Sigma_j\ h'_j\}}$$

$$\frac{\forall h_1, h_2.\ \ast_{j=1,2}\ \Sigma_j\ h_j \mathrel{-\!\!\ast} \overline{\{h_1 \ast h_2\}_{\mathrm{I}}\ e_1; e_2\ \{h', () \mid \{h_1 \ast h_2\}_{\mathrm{S}}\ e'_2; e'_1\ \{h', ()\} \ast (\Sigma_1 \otimes \Sigma_2)\ h'\}}}{\mathcal{E}\ (\Sigma_1 \otimes \Sigma_2)\ (e_1; e_2 \preccurlyeq e'_2; e'_1)\ [\![\mathsf{unit}]\!]}$$

Reordering Effectful Computations

$$\dfrac{\dfrac{\dfrac{}{*_{j=1,2}\ \mathcal{E}\ \Sigma_j\ (e_j \preccurlyeq e'_j)\ [\![\mathsf{unit}]\!]}}{*_{j=1,2}\ \forall h_j.\ \Sigma_j\ h_j \mathrel{-\!\!*} \{h_j\}_{\mathrm{I}}\ e_j\ \{\ h'_j, () \mid \{h_j\}_{\mathrm{S}}\ e'_j\ \{h'_j, ()\} * \Sigma_j\ h'_j\}}}{}}{}$$

$$\dfrac{\forall h_1, h_2.\ *_{j=1,2}\ \Sigma_j\ h_j \mathrel{-\!\!*} \dfrac{}{\{h_1 * h_2\}_{\mathrm{I}}\ e_1; e_2\ \{h', () \mid \{h_1 * h_2\}_{\mathrm{S}}\ e'_2; e'_1\ \{h', ()\} * (\Sigma_1 \otimes \Sigma_2)\ h'\}}}{\mathcal{E}\ (\Sigma_1 \otimes \Sigma_2)\ (e_1; e_2 \preccurlyeq e'_2; e'_1)\ [\![\mathsf{unit}]\!]}$$

Reordering Effectful Computations

$$\dfrac{\dfrac{\dfrac{\dfrac{}{*_{j=1,2}\ \mathcal{E}\ \Sigma_j\ (e_j \preccurlyeq e'_j)\ [\![\mathsf{unit}]\!]}}{*_{j=1,2}\ \forall h_j.\ \Sigma_j\ h_j \mathrel{-\!\!*} \{h_j\}_{\mathrm{I}}\ e_j\ \{\ h'_j, () \mid \{h_j\}_{\mathrm{S}}\ e'_j\ \{h'_j, ()\} * \Sigma_j\ h'_j\}} \qquad \dfrac{}{*_{j=1,2}\ (\{h_j\}_{\mathrm{S}}\ e'_j\ \{h'_j, ()\} * \Sigma_j\ h'_j)}}{}}{\forall h_1, h_2.\ *_{j=1,2}\ \Sigma_j\ h_j \mathrel{-\!\!*} \{h_1{*}h_2\}_{\mathrm{I}}\ e_1; e_2\ \{h', () \mid \{h_1{*}h_2\}_{\mathrm{S}}\ e'_2; e'_1\ \{h', ()\} * (\Sigma_1{\otimes}\Sigma_2)\ h'\}} \qquad \dfrac{\dfrac{}{\{h_1{*}h_2\}_{\mathrm{S}}\ e'_2; e'_1\ \{h'_1{*}h'_2, ()\}} * (\Sigma_1{\otimes}\Sigma_2)\ (h'_1{*}h'_2)}{}}{\mathcal{E}\ (\Sigma_1 \otimes \Sigma_2)\ (e_1; e_2 \preccurlyeq e'_2; e'_1)\ [\![\mathsf{unit}]\!]}$$

Reordering Effectful Computations

$$\dfrac{\dfrac{\dfrac{}{\ast_{j=1,2}\ \mathcal{E}\ \Sigma_j\ (e_j \preccurlyeq e'_j)\ [\![\mathsf{unit}]\!]}}{\ast_{j=1,2}\ \forall h_j.\ \Sigma_j\ h_j \mathrel{-\!\!*} \{h_j\}_{\mathrm{I}}\ e_j\ \{\ h'_j, () \mid \{h_j\}_{\mathrm{S}}\ e'_j\ \{h'_j, ()\} \ast \Sigma_j\ h'_j\}}}{\ast_{j=1,2}\ (\{h_j\}_{\mathrm{S}}\ e'_j\ \{h'_j, ()\} \ast \Sigma_j\ h'_j)}}{\forall h_1, h_2.\ \ast_{j=1,2}\ \Sigma_j\ h_j \mathrel{-\!\!*} \{h_1 \ast h_2\}_{\mathrm{I}}\ e_1; e_2\ \{h', () \mid \{h_1 \ast h_2\}_{\mathrm{S}}\ e'_2; e'_1\ \{h', ()\} \ast (\Sigma_1 \otimes \Sigma_2)\ h'\}}}{\mathcal{E}\ (\Sigma_1 \otimes \Sigma_2)\ (e_1; e_2 \preccurlyeq e'_2; e'_1)\ [\![\mathsf{unit}]\!]}$$

$$\dfrac{\dfrac{}{\{h_1 \ast h_2\}_{\mathrm{S}}\ e'_2; e'_1\ \{h'_1 \ast h'_2, ()\}} \ast (\Sigma_1 \otimes \Sigma_2)\ (h'_1 \ast h'_2)}{\forall h_1, h_2.\ \ast_{j=1,2}\ \Sigma_j\ h_j \mathrel{-\!\!*} \{h_1 \ast h_2\}_{\mathrm{I}}\ e_1; e_2\ \{h', () \mid \{h_1 \ast h_2\}_{\mathrm{S}}\ e'_2; e'_1\ \{h', ()\} \ast (\Sigma_1 \otimes \Sigma_2)\ h'\}}$$

Reordering Effectful Computations

$$\dfrac{\dfrac{\dfrac{}{*_{j=1,2}\ \mathcal{E}\ \Sigma_j\ (e_j \preccurlyeq e'_j)\ [\![\mathsf{unit}]\!]}}{*_{j=1,2}\ \forall h_j.\ \Sigma_j\ h_j \mathrel{-\!\!*} \{h_j\}_{\mathrm{I}}\ e_j\ \{\ h'_j, () \mid \{h_j\}_{\mathrm{S}}\ e'_j\ \{h'_j, ()\} * \Sigma_j\ h'_j\}} \quad \dfrac{}{*_{j=1,2}\ (\{h_j\}_{\mathrm{S}}\ e'_j\ \{h'_j, ()\} * \Sigma_j\ h'_j)}}{\forall h_1, h_2.\ *_{j=1,2}\ \Sigma_j\ h_j \mathrel{-\!\!*} \{h_1 * h_2\}_{\mathrm{I}}\ e_1; e_2\ \{h', () \mid \{h_1 * h_2\}_{\mathrm{S}}\ e'_2; e'_1\ \{h', ()\} * (\Sigma_1 \otimes \Sigma_2)\ h'\}} \quad \dfrac{\dfrac{}{\{h_1 * h_2\}_{\mathrm{S}}\ e'_2; e'_1\ \{h'_1 * h'_2, ()\}} * (\Sigma_1 \otimes \Sigma_2)\ (h'_1 * h'_2)}{\mathcal{E}\ (\Sigma_1 \otimes \Sigma_2)\ (e_1; e_2 \preccurlyeq e'_2; e'_1)\ [\![\mathsf{unit}]\!]}$$

Reordering Effectful Computations

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\ast_{j=1,2}\ \mathcal{E}\ \Sigma_j\ (e_j \preccurlyeq e'_j)\ [\![\mathsf{unit}]\!]}}{\ast_{j=1,2}\ \forall h_j.\ \Sigma_j\ h_j \mathrel{-\!\!*} \{h_j\}_{\mathrm{I}}\ e_j\ \{\ h'_j, () \mid \{h_j\}_{\mathrm{S}}\ e'_j\ \{h'_j, ()\} \ast \Sigma_j\ h'_j\}}}{\ast_{j=1,2}\ (\{h_j\}_{\mathrm{S}}\ e'_j\ \{h'_j, ()\} \ast \Sigma_j\ h'_j)}}{\{h_2 \ast h_1\}_{\mathrm{S}}\ e'_2; e'_1\ \{h'_2 \ast h'_1, ()\}}}{\{h_1 \ast h_2\}_{\mathrm{S}}\ e'_2; e'_1\ \{h'_1 \ast h'_2, ()\} \ast (\Sigma_1 \otimes \Sigma_2)\ (h'_1 \ast h'_2)}}{\forall h_1, h_2.\ \ast_{j=1,2}\ \Sigma_j\ h_j \mathrel{-\!\!*} \{h_1 \ast h_2\}_{\mathrm{I}}\ e_1; e_2\ \{h', () \mid \{h_1 \ast h_2\}_{\mathrm{S}}\ e'_2; e'_1\ \{h', ()\} \ast (\Sigma_1 \otimes \Sigma_2)\ h'\}}}{\mathcal{E}\ (\Sigma_1 \otimes \Sigma_2)\ (e_1; e_2 \preccurlyeq e'_2; e'_1)\ [\![\mathsf{unit}]\!]}$$

Reordering Effectful Computations

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\ast_{j=1,2}\ \mathcal{E}\ \Sigma_j\ (e_j \preccurlyeq e'_j)\ [\![\mathsf{unit}]\!]}}{\ast_{j=1,2}\ \forall h_j.\ \Sigma_j\ h_j \mathrel{-\!\!*} \{h_j\}_{\mathrm{I}}\ e_j\ \{\ h'_j, () \mid \{h_j\}_{\mathrm{S}}\ e'_j\ \{h'_j, ()\} \ast \Sigma_j\ h'_j\}}}{\ast_{j=1,2}\ (\{h_j\}_{\mathrm{S}}\ e'_j\ \{h'_j, ()\} \ast \Sigma_j\ h'_j)}}{\{h_2 \ast h_1\}_{\mathrm{S}}\ e'_2; e'_1\ \{h'_2 \ast h'_1, ()\}}}{\{h_1 \ast h_2\}_{\mathrm{S}}\ e'_2; e'_1\ \{h'_1 \ast h'_2, ()\} \ast (\Sigma_1 \otimes \Sigma_2)\ (h'_1 \ast h'_2)}}{\forall h_1, h_2.\ \ast_{j=1,2}\ \Sigma_j\ h_j \mathrel{-\!\!*} \{h_1 \ast h_2\}_{\mathrm{I}}\ e_1; e_2\ \{h', () \mid \{h_1 \ast h_2\}_{\mathrm{S}}\ e'_2; e'_1\ \{h', ()\} \ast (\Sigma_1 \otimes \Sigma_2)\ h'\}}}{\mathcal{E}\ (\Sigma_1 \otimes \Sigma_2)\ (e_1; e_2 \preccurlyeq e'_2; e'_1)\ [\![\mathsf{unit}]\!]}$$

Reordering Effectful Computations

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{*_{j=1,2}\ \mathcal{E}\ \Sigma_j\ (e_j \preccurlyeq e'_j)\ [\![\mathsf{unit}]\!]}}{*_{j=1,2}\ \forall h_j.\ \Sigma_j\ h_j \mathrel{-\!\!*} \{h_j\}_{\mathrm{I}}\ e_j\ \{\ h'_j, () \mid \{h_j\}_{\mathrm{S}}\ e'_j\ \{h'_j, ()\} * \Sigma_j\ h'_j\}}}{*_{j=1,2}\ (\{h_j\}_{\mathrm{S}}\ e'_j\ \{h'_j, ()\} * \Sigma_j\ h'_j)}}{\{h_2{*}h_1\}_{\mathrm{S}}\ e'_2; e'_1\ \{h'_2{*}h'_1, ()\}}}{\{h_1{*}h_2\}_{\mathrm{S}}\ e'_2; e'_1\ \{h'_1{*}h'_2, ()\} * (\Sigma_1 \otimes \Sigma_2)\ (h'_1{*}h'_2)}}{\forall h_1, h_2.\ *_{j=1,2}\ \Sigma_j\ h_j \mathrel{-\!\!*} \{h_1{*}h_2\}_{\mathrm{I}}\ e_1; e_2\ \{h', () \mid \{h_1{*}h_2\}_{\mathrm{S}}\ e'_2; e'_1\ \{h', ()\} * (\Sigma_1 \otimes \Sigma_2)\ h'\}}}{\mathcal{E}\ (\Sigma_1 \otimes \Sigma_2)\ (e_1; e_2 \preccurlyeq e'_2; e'_1)\ [\![\mathsf{unit}]\!]}$$

Towards Tmp-write

$$\mathcal{E}_{rd}\,\Sigma\,e\,e'\,\phi \approx \forall h.\,\Sigma\,h \mathrel{-\!\!*} \mathcal{E}\,\{h\}\,E\,\Phi$$

$$\mathcal{E}_{rd}\,[\![\ell : \tau]\!]\,e\,e'\,\phi \equiv \forall v.\,\triangleright\,\tau\,v \mathrel{-\!\!*} \{\ell \mapsto v\}_{\mathrm{I}}\,e\,\{\ell \mapsto v, w \mid \{\ell \mapsto v\}_{\mathrm{S}}\,e'\,\{\ell \mapsto v, w\} * \phi\,w\}$$

Towards Equi-write

$$\mathsf{SemType} \triangleq \mathsf{Class}\ \mathit{Val} \to \mathit{iProp}_{\square}$$
$$\mathsf{Class}\ \mathit{Val} \triangleq \mathit{Val} \to \mathit{bProp}_{\square}$$

$$[\![\mathsf{ratio}]\!] \triangleq \{\, Q_q \mid q \in \mathbb{Q} \,\} \qquad \in \mathsf{SemType}$$
$$Q_q \triangleq \{\, \mathtt{pair}\, z_1\, z_2 \mid z_1/z_2 = q \,\} \qquad \in \mathsf{Class}\ \mathit{Val}$$

$$L \mapsto V \triangleq \forall \ell.\, L\, \ell \mathrel{-\!\!*} \exists v.\, V\, v * \ell \mapsto v \qquad \in \mathit{bProp} \triangleq B \to \mathit{iProp}$$

Towards Equi-write

$$\mathsf{SemType} \triangleq \mathsf{Class}\ \mathit{Val} \to \mathit{iProp}_{\square}$$
$$\mathsf{Class}\ \mathit{Val} \triangleq \mathit{Val} \to \mathit{bProp}_{\square}$$

$$[\![\mathsf{ratio}]\!] \triangleq \{\, Q_q \mid q \in \mathbb{Q} \,\} \qquad \in \mathsf{SemType}$$
$$Q_q \triangleq \{\, \mathtt{pair}\ z_1\ z_2 \mid z_1/z_2 = q \,\} \qquad \in \mathsf{Class}\ \mathit{Val}$$

$$L \mapsto_b V \triangleq \forall \ell.\, L\, \ell\, b \mathrel{-\!\!*} \exists v.\, V\, v\, b * \ell \mapsto_b v \in \mathit{bProp} \triangleq B \to \mathit{iProp}$$

Related Work

- J. Thamsborg, L. Birkedal, A KLR for effect-based program transformations, ICFP 11
  - Support non-lockstep reasoning
  - Non-obvious how to support equi-write
- Krogh-Jespersen et al., A Relational Model of Types-and-Effects in HO CSL, POPL 17
  - Verify parallelization thm. with Iris (on paper) using invariants & token reasoning
  - Non-obvious how to support equi-write and tmp-write
- A. Timany et al., A Logical Relation for Monadic Encapsulation of State, POPL 18
  - Support non-lockstep reasoning in Iris about **pure** expressions
- S. Spies et al., Later Credits: Resourceful Reasoning for the Later Modality, ICFP 22
  - Support non-lockstep reasoning in Iris about **pure** expressions in an **impure** language
- E. D'Osualdo, Proving Hypersafety Compositionally, OOPSLA 22
  - Support non-lockstep reasoning for hypersafety (but not hyperliveness) properties in a **first-order** language

bProp Heapotheses

$$H \in \mathit{bProp} \triangleq B \to \mathit{iProp}$$
$$\Sigma \in \mathit{bProp} \to \mathit{iProp}$$

$$\mathcal{E}\,\Sigma\,e\,e'\,\phi \triangleq \forall H.\,\Sigma\,H \twoheadrightarrow \{H\}_{\mathrm{I}}\,e\,\{H', v.\,\{H\}_{\mathrm{S}}\,e'\,\{H', v\} * \Sigma\,H' * \phi\,v\}$$

$$\{H\}_b\,e\,\{H', v.\,\phi\} \triangleq \Box_b(\,H\,b \twoheadrightarrow \mathsf{wp}_b\,e\,\{v.\,\exists H'.\,H'\,b * \phi\,H'\,v\}\,)$$

Example $H \in \mathit{bProp}$ for Executing Loads

$$\ell \mapsto v = \lambda b.\, \ell \mapsto_b v \in \mathit{bProp}$$

$$\textsc{load}\ \frac{\triangleright_b\, \Omega\, (\ell \mapsto v)\, v}{\{\ell \mapsto v\}_b\, !\, \ell\, \{H, w.\, \Omega\, H\, w\}}$$

Example $\Sigma \in \mathit{bProp} \to \mathit{iProp}$ for Relating Loads

$$[\![\ell : \tau]\!] \triangleq \{\, \ell \mapsto v \mid \triangleright\, \tau\, v \,\} \in \mathit{bProp} \to \mathit{iProp}$$

$$\dfrac{\dfrac{\forall v.\ \triangleright\, \tau\, v \mathrel{-\!\!*} \{\ell \mapsto v\}_{\mathrm{I}}\, !\, \ell\, \{\ell \mapsto v', w \mid \{\ell \mapsto v\}_{\mathrm{S}}\, !\, \ell\, \{\ell \mapsto v', w\} * \triangleright\, \tau\, v' * \tau\, w\}}{\forall H.\ [\![\ell : \tau]\!]\, H \mathrel{-\!\!*} \{H\}_{\mathrm{I}}\, !\, \ell\, \{H', w.\ \{H\}_{\mathrm{S}}\, !\, \ell\, \{H', w\} * [\![\ell : \tau]\!]\, H' * \tau\, w\}}}{\mathcal{E}\, [\![\ell : \tau]\!]\, !\, \ell\, !\, \ell\, \tau}\ \mathcal{E}\text{-LOAD}$$

$$\dfrac{\text{LOAD}\ \overline{\triangleright(\{\ell \mapsto v\}_{\mathrm{S}}\, !\, \ell\, \{\ell \mapsto v, v\}\ *\ \overline{\tau\, v}\ *\ \overline{\tau\, v}\ )}}{\forall v.\ \triangleright\, \tau\, v \mathrel{-\!\!*} \{\ell \mapsto v\}_{\mathrm{I}}\, !\, \ell\, \{\ell \mapsto v', w \mid \{\ell \mapsto v\}_{\mathrm{S}}\, !\, \ell\, \{\ell \mapsto v', w\} * \triangleright\, \tau\, v' * \tau\, w\}}\ \text{LOAD}$$

Exorcising the Value Interpretation

$$E \in \mathsf{Class}\ \mathit{Expr}$$
$$V \in \mathsf{Class}\ \mathit{Val} \triangleq \mathit{Val} \to \mathit{bProp}$$
$$\Phi \in \mathsf{Class}\ \mathit{Val} \to \mathit{iProp}$$

$$\mathcal{E}\,\Sigma\,E\,\Phi \triangleq \forall H.\,\Sigma\,H \twoheadrightarrow \{H\}_{\mathrm{I}}\,E\,\{H', V.\,\{H\}_{\mathrm{S}}\,E\,\{H', V\} * \Sigma\,H' * \Phi\,V\}$$

$$\{H\}_b\,E\,\{H', V.\,\Phi\} \triangleq \Box_b(\,H\,b \twoheadrightarrow \mathsf{WP}_b\,E\,\{V.\,\exists H'.\,H'\,b * \Phi\,H'\,V\}\,)$$
$$\mathsf{WP}_b\,E\,\{\Phi\} \triangleq \forall e.\,E\,e\,b \twoheadrightarrow \mathsf{wp}_b\,E\,\{v.\,\exists V.\,V\,v\,b * \Phi\,V\}$$

$$\mathcal{E}\,\{\top\}\,E\,[\![A]\!] \vdash \forall e, e'.\,E\,e\,\mathrm{I} * E\,e'\,\mathrm{S} \twoheadrightarrow \ulcorner \emptyset \vDash e \leq_{ctx} e' : A \urcorner$$