Unifying Worlds and Resources

Ralf Jung, Derek Dreyer

Max Planck Institute for Software Systems (MPI-SWS),
Saarland University

August 30th
HOPE 2015, Vancouver

This talk

Iris

This talk

Iris

This talk

Iris' Model

This talk

Iris' *new* Model

This Talk

1. Explain Iris' model

This Talk

1. Explain part of Iris' model

This Talk

1. Explain part of Iris' model
2. Clean it up a little

This Talk

1. Explain part of Iris' model
2. Clean it up a little
3. Category Theory and Coq are here to *help you*

Iris

Iris

A new separation logic that

- can verify complex, lock-free concurrent data structures
- permits modular (thread-local) reasoning

What makes Iris different from...

- CSL [O'H07]
- RGSep [VP07]
- SAGL [FFS07]
- LRG [Fen09]
- CAP [DY+10]
- HLRG [Fu+10]
- CaReSL [TDB13]
- SCSL [LWN13]
- HoCAP [SBP13]
- iCAP [SB14]
- FCSL [Nan+14]
- TaDA [dDYG14]

What makes Iris different from...

- CSL [O'H07]
- CAP [DY+10]
- HLRG [Fu+10]
- CaReSL [TDB13]
- FCSL [Nan+14]
- TaDA [dDYG14]

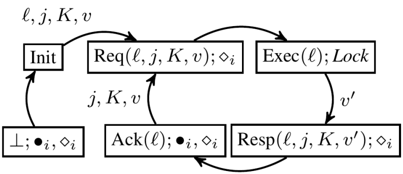
Focus on simplifying the foundations of concurrent reasoning

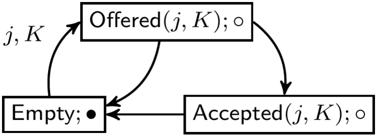
What makes Iris different from...

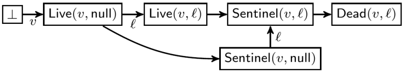
- CSL [O'H07]
- RGSep [VP07]
- SAGL [FFS07]
- LRG [Fen09]
- CAP [DY+10]
- HLRG [Fu+10]
- CaReSL [TDB13]
- SCSL [LWN13]
- HoCAP [SBP13]
- iCAP [SB14]
- FCSL [Nan+14]
- TaDA [dDYG14]

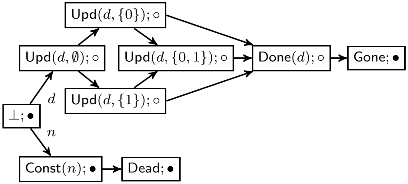
Common approach: "protocol" to deal with interference

STSs in CaReSL









Complex rules built-in as primitives

CaReSL: $$\frac{\mathcal{C} \vdash \forall b \overset{\text{rely}}{\sqsupseteq_\pi} b_0.\ \llparenthesis \pi[\![b]\!] * P \rrparenthesis\ i \Rrightarrow_{\mathrm{I}}\ a\ \llparenthesis x.\ \exists b' \overset{\text{guar}}{\sqsupseteq_\pi} b.\ \pi[\![b']\!] * Q \rrparenthesis}{\mathcal{C} \vdash \left\{ \boxed{b_0}^{n}_{\pi} * \triangleright P \right\}\ i \Rrightarrow\ a\ \left\{ x.\ \exists b'.\ \boxed{b'}^{n}_{\pi} * Q \right\}}\ \textsc{UpdIsl}$$

Complex rules built-in as primitives

CaReSL:
$$\frac{\mathcal{C} \vdash \forall b \overset{\text{rely}}{\sqsupseteq_\pi} b_0.\ (\!|\pi[\![b]\!] * P|\!)\ i \Rrightarrow_{\mathrm{I}} a\ (\!|x.\ \exists b' \overset{\text{guar}}{\sqsupseteq_\pi} b.\ \pi[\![b']\!] * Q|\!)}{\mathcal{C} \vdash \left\{ \boxed{b_0}^{n}_{\pi} * \triangleright P \right\}\ i \Rrightarrow a\ \left\{ x.\ \exists b'.\ \boxed{b'}^{n}_{\pi} * Q \right\}}\ \textsc{UpdIsl}$$

iCAP:
$$\frac{\begin{array}{c}\Gamma, \Delta \mid \Phi \vdash \mathsf{stable}(\mathsf{P}) \qquad \Gamma, \Delta \mid \Phi \vdash \forall y.\ \mathsf{stable}(\mathsf{Q}(y)) \\ \Gamma, \Delta \mid \Phi \vdash n \in C \qquad \Gamma, \Delta \mid \Phi \vdash \forall x \in X.\ (x, f(x)) \in \overline{T(A)} \vee f(x) = x \\ \Gamma \mid \Phi \vdash \forall x \in X.\ (\Delta).\langle \mathsf{P} * \circledast_{\alpha \in A} [\alpha]^{\mathsf{n}}_{g(\alpha)} * \triangleright I(x) \rangle\ c\ \langle \mathsf{Q}(x) * \triangleright I(f(x)) \rangle^{C \setminus \{n\}}\end{array}}{\begin{array}{c}\Gamma \mid \Phi \vdash (\Delta).\ \langle \mathsf{P} * \circledast_{\alpha \in A} [\alpha]^{\mathsf{n}}_{g(\alpha)} * \mathsf{region}(X, T, I, n) \rangle \\ c \\ \langle \exists x.\ \mathsf{Q}(x) * \mathsf{region}(\{f(x)\}, T, I, n) \rangle^{C}\end{array}}\ \textsc{Atomic}$$

TaDA:
$$\frac{\begin{array}{c}\text{Use atomic rule} \\ a \notin \mathcal{A} \quad \forall x \in X.\, (x, f(x)) \in \mathcal{T}_{\mathbf{t}}(\mathrm{G})^* \\ \lambda; \mathcal{A} \vdash \mathbb{V}x \in X.\, \langle p_p \mid I(\mathbf{t}^{\lambda}_{a}(x)) * p(x) * [\mathrm{G}]_a \rangle\ \mathbb{C}\ \exists\!\!\exists y \in Y.\, \langle q_p(x, y) \mid I(\mathbf{t}^{\lambda}_{a}(f(x))) * q(x, y) \rangle\end{array}}{\lambda + 1; \mathcal{A} \vdash \mathbb{V}x \in X.\, \langle p_p \mid \mathbf{t}^{\lambda}_{a}(x) * p(x) * [\mathrm{G}]_a \rangle\ \mathbb{C}\ \exists\!\!\exists y \in Y.\, \langle q_p(x, y) \mid \mathbf{t}^{\lambda}_{a}(f(x)) * q(x, y) \rangle}$$

Complex rules built-in as primitives

CaReSL: $$\frac{\mathcal{C} \vdash \forall b \overset{\text{rely}}{\sqsupseteq_\pi} b_0.\ \llparenthesis \pi[\![b]\!] * P \rrparenthesis\ i \Rrightarrow_{\mathrm{I}} a\ \llparenthesis x.\ \exists b' \overset{\text{guar}}{\sqsupseteq_\pi} b.\ \pi[\![b']\!] * Q \rrparenthesis}{\mathcal{C} \vdash \left\{ \boxed{b_0}^{n}_{\pi} * \triangleright P \right\}\ i \Rrightarrow a\ \left\{ x.\ \exists b'.\ \boxed{b'}^{n}_{\pi} * Q \right\}}\ \textsc{UpdIsl}$$

i

All you need are two simple primitives:

- *Monoids* to *express* protocols.
- *Invariants* to *enforce* protocols.

TaDA: $$\frac{\begin{array}{c}\text{Use atomic rule}\\ a \notin \mathcal{A} \quad \forall x \in X.\,(x, f(x)) \in \mathcal{T}_{\mathbf{t}}(\mathrm{G})^* \\ \lambda; \mathcal{A} \vdash \mathbb{V}x \in X.\,\langle p_p \mid I(\mathbf{t}_a^\lambda(x)) * p(x) * [\mathrm{G}]_a \rangle\ \mathbb{C}\ \exists\!\!\exists y \in Y.\,\langle q_p(x,y) \mid I(\mathbf{t}_a^\lambda(f(x))) * q(x,y) \rangle\end{array}}{\lambda + 1; \mathcal{A} \vdash \mathbb{V}x \in X.\,\langle p_p \mid \mathbf{t}_a^\lambda(x) * p(x) * [\mathrm{G}]_a \rangle\ \mathbb{C}\ \exists\!\!\exists y \in Y.\,\langle q_p(x,y) \mid \mathbf{t}_a^\lambda(f(x)) * q(x,y) \rangle}$$

Iris rules

$$\frac{\{R * P\}\ e\ \{R * Q\} \qquad e \text{ atomic}}{\boxed{R} \vdash \{P\}\ e\ \{Q\}}$$

Iris rules

$$\frac{\{R * P\}\ e\ \{R * Q\} \qquad e \text{ atomic}}{\boxed{R} \vdash \{P\}\ e\ \{Q\}}$$

Iris rules

$$\frac{\{R * P\}\ e\ \{R * Q\} \qquad e \text{ atomic}}{\boxed{R}^{\iota} \vdash \{P\}\ e\ \{Q\}}$$

$$R \Rrightarrow \exists \iota.\ \boxed{R}^{\iota}$$

Ghost state

Logical state, no physical representation

Ghost state

Logical state, no physical representation

- Permissions
- Capabilities
- Logical variables
- ...

Ghost state in Iris

Partial commutative monoid (PCM)

- Set M (carrier)
- An operation $\cdot$ on M (associative, commutative)
- A unit ε ("empty")
- A zero $\bot$ ("bottom", "undefined")

Ghost state in Iris

Partial commutative monoid (PCM)

- Set M (carrier)
- An operation $\cdot$ on M (associative, commutative)
- A unit ε ("empty")
- A zero $\perp$ ("bottom", "undefined")

Resource $a \in M$: Logical assertion $\boxed{a}$ ("own a")

Iris rules

$$\frac{\forall a_f.\ a \mathrel{\#} a_f \Rightarrow b \mathrel{\#} a_f}{\boxed{a} \Rrightarrow \boxed{b}}$$

where $a \mathrel{\#} b \triangleq a \cdot b \neq \bot$

Iris rules

$$\frac{\forall a_f.\ a \mathrel{\#} a_f \Rightarrow b \mathrel{\#} a_f}{\boxed{a} \Rrightarrow \boxed{b}}$$

$$\frac{a \cdot b = c}{\boxed{a} * \boxed{b} \Leftrightarrow \boxed{c}}$$

where $a \mathrel{\#} b \triangleq a \cdot b \neq \bot$

Iris rules

$$\frac{\forall a_f.\ a \# a_f \Rightarrow b \# a_f}{\boxed{a} \Rrightarrow \boxed{b}}$$

$$\frac{a \cdot b = c}{\boxed{a} * \boxed{b} \Leftrightarrow \boxed{c}} \qquad \boxed{\bot} \Rightarrow \text{False}$$

where $a \# b \triangleq a \cdot b \neq \bot$

Iris rules

$$\frac{\{R * P\}\ e\ \{R * Q\} \qquad e \text{ atomic}}{\boxed{R}^{\iota} \vdash \{P\}\ e\ \{Q\}} \qquad\qquad R \Rrightarrow \exists \iota.\ \boxed{R}^{\iota}$$

$$\frac{\forall a_f.\ a \mathrel{\#} a_f \Rightarrow b \mathrel{\#} a_f}{\boxed{a} \Rrightarrow \boxed{b}}$$

$$\frac{a \cdot b = c}{\boxed{a} * \boxed{b} \Leftrightarrow \boxed{c}} \qquad\qquad \boxed{\bot} \Rightarrow \text{False}$$

where $a \mathrel{\#} b \triangleq a \cdot b \neq \bot$

Iris rules

$$\{R * P\}\ e\ \{R * Q\}$$

e atomic

We can encode other common forms of ghost state

$$\boxed{a} * \boxed{b} \Leftrightarrow \boxed{c}$$

where $a \# b \triangleq a \cdot b \neq \bot$

Iris rules

$$\{R * P\}\ e\ \{R * Q\}$$

e atomic

We can encode other common forms of ghost state and derive the STS update rule

$$\frac{\forall c.\ \{\hat{c} \rightarrow^* c * \varphi(c) * P\}\ e\ \{v.\ \exists c'.\ c \rightarrow^* c' * \varphi(c') * Q\}}{\mathrm{STS}(\mathcal{S}, \varphi) \vdash \left\{\boxed{\geq \hat{c}} * P\right\}\ e\ \left\{v.\ \exists c'.\ \boxed{\geq c'} * Q\right\}}$$

$$\boxed{a} * \boxed{b} \Leftrightarrow \boxed{c}$$

where $a \# b \triangleq a \cdot b \neq \bot$

Complex rules built-in as primitives

CaReSL: $$\frac{\mathcal{C} \vdash \forall b \overset{\text{rely}}{\sqsupseteq_\pi} b_0.\ (\!|\pi[\![b]\!] * P|\!)\ i \Rrightarrow_{\mathrm{I}} a\ (\!|x.\ \exists b' \overset{\text{guar}}{\sqsupseteq_\pi} b.\ \pi[\![b']\!] * Q|\!)}{\mathcal{C} \vdash \left\{ \boxed{b_0}^n_\pi * \triangleright P \right\}\ i \Rrightarrow a\ \left\{ x.\ \exists b'.\ \boxed{b'}^n_\pi * Q \right\}}\ \textsc{UpdIsl}$$

iCAP: $$\frac{\begin{array}{c}\Gamma, \Delta \mid \Phi \vdash \mathsf{stable}(\mathsf{P}) \qquad \Gamma, \Delta \mid \Phi \vdash \forall y.\ \mathsf{stable}(\mathsf{Q}(y)) \\ \Gamma, \Delta \mid \Phi \vdash n \in C \qquad \Gamma, \Delta \mid \Phi \vdash \forall x \in X.\ (x, f(x)) \in \overline{T(A)} \vee f(x) = x \\ \Gamma \mid \Phi \vdash \forall x \in X.\ (\Delta).\langle \mathsf{P} * \circledast_{\alpha \in A}[\alpha]^{\mathsf{n}}_{g(\alpha)} * \triangleright I(x)\rangle\ c\ \langle \mathsf{Q}(x) * \triangleright I(f(x))\rangle^{C \setminus \{n\}}\end{array}}{\begin{array}{c}\Gamma \mid \Phi \vdash (\Delta).\ \langle \mathsf{P} * \circledast_{\alpha \in A}[\alpha]^{\mathsf{n}}_{g(\alpha)} * \mathsf{region}(X, T, I, n)\rangle \\ c \\ \langle \exists x.\ \mathsf{Q}(x) * \mathsf{region}(\{f(x)\}, T, I, n)\rangle^C\end{array}}\ \textsc{Atomic}$$

TaDA: $$\frac{\begin{array}{c}\text{Use atomic rule} \\ a \notin \mathcal{A} \quad \forall x \in X.\ (x, f(x)) \in \mathcal{T}_{\mathbf{t}}(\mathrm{G})^* \\ \lambda; \mathcal{A} \vdash \mathbb{V} x \in X.\ \left\langle p_p \,\middle|\, I(\mathbf{t}^\lambda_a(x)) * p(x) * [\mathrm{G}]_a \right\rangle\ \mathbb{C}\ \exists\!\!\exists y \in Y.\ \left\langle q_p(x, y) \,\middle|\, I(\mathbf{t}^\lambda_a(f(x))) * q(x, y) \right\rangle\end{array}}{\lambda + 1; \mathcal{A} \vdash \mathbb{V} x \in X.\ \left\langle p_p \,\middle|\, \mathbf{t}^\lambda_a(x) * p(x) * [\mathrm{G}]_a \right\rangle\ \mathbb{C}\ \exists\!\!\exists y \in Y.\ \left\langle q_p(x, y) \,\middle|\, \mathbf{t}^\lambda_a(f(x)) * q(x, y) \right\rangle}$$

Iris rules

$$\frac{\{R * P\}\ e\ \{R * Q\} \qquad e \text{ atomic}}{\boxed{R}^{\iota} \vdash \{P\}\ e\ \{Q\}}$$

$$R \Rrightarrow \exists \iota.\ \boxed{R}^{\iota}$$

$$\frac{\forall a_f.\ a \# a_f \Rightarrow b \# a_f}{\boxed{a} \Rrightarrow \boxed{b}}$$

$$\frac{a \cdot b = c}{\boxed{a} * \boxed{b} \Leftrightarrow \boxed{c}}$$

$$\boxed{\bot} \Rightarrow \text{False}$$

where $a \# b \triangleq a \cdot b \neq \bot$

Iris rules

$$\frac{\{R * P\}\ e\ \{R * Q\} \quad e \text{ atomic}}{\boxed{R}^{\iota} \vdash \{P\}\ e\ \{Q\}}$$

$$R \Rrightarrow \exists \iota.\ \boxed{R}^{\iota}$$

Monoids and Invariants are all you need

$$\frac{a \cdot b = c}{\boxed{a} * \boxed{b} \Leftrightarrow \boxed{c}}$$

$$\boxed{\bot} \Rightarrow \text{False}$$

where $a \# b \triangleq a \cdot b \neq \bot$

Iris' Model

Semantic domain

$$Prop \triangleq \qquad ResMon \to \text{“}Bool\text{”}$$

Semantic domain

$$Prop \triangleq \qquad ResMon \xrightarrow{\text{mon}} \text{“}Bool\text{”}$$

Semantic domain

$$\mathit{Prop} \triangleq \mathit{Wld} \overset{\text{mon}}{\to} \mathit{ResMon} \overset{\text{mon}}{\to} \text{“}\mathit{Bool}\text{”}$$

Semantic domain

$$Prop \triangleq Wld \overset{\text{mon}}{\rightarrow} ResMon \overset{\text{mon}}{\rightarrow} \text{“}Bool\text{”}$$

$$\text{where } Wld \triangleq InvName \overset{\text{fin}}{\rightharpoonup} Prop$$

Roadmap

- Redundancies in the treatment of worlds and resources

Roadmap

- Redundancies in the treatment of worlds and resources
- How to treat them uniformly

Roadmap

- Redundancies in the treatment of worlds and resources
- How to treat them uniformly
- What is this good for?

Semantic domain

$$\mathit{Prop} \triangleq \mathit{Wld} \xrightarrow{\text{mon}} \mathit{ResMon} \xrightarrow{\text{mon}} \text{“}\mathit{Bool}\text{”}$$

where $\mathit{Wld} \triangleq \mathit{InvName} \xrightarrow{\text{fin}} \mathit{Prop}$

Step-indexing as a category: c.o.f.e.s

Complete Ordered Families of Equivalences

Prop

Step-indexing as a category: c.o.f.e.s

Complete Ordered Families of Equivalences

$$\left(Prop, \stackrel{n}{=}_{n \in \mathbb{N}}\right)$$

Step-indexing as a category: c.o.f.e.s

Complete Ordered Families of Equivalences

$$(Prop, \overset{n}{=}_{n \in \mathbb{N}})$$

$$P \overset{n+1}{=} Q \Rightarrow P \overset{n}{=} Q$$

$$P = Q \Leftrightarrow \forall n.\ P \overset{n}{=} Q$$

Step-indexing as a category: c.o.f.e.s

Complete Ordered Families of Equivalences

$$(Prop, \overset{n}{=}_{n \in \mathbb{N}})$$

$$P \overset{n+1}{=} Q \Rightarrow P \overset{n}{=} Q$$

$$P = Q \Leftrightarrow \forall n.\ P \overset{n}{=} Q$$

$$(X, \overset{n}{=}_{n \in \mathbb{N}})$$

Step-indexing as a category: c.o.f.e.s

Complete Ordered Families of Equivalences

$$(Prop, \stackrel{n}{=}_{n\in\mathbb{N}}) \xrightarrow{\textit{non-expansive}\text{ function}} (X, \stackrel{n}{=}_{n\in\mathbb{N}})$$

$$P \stackrel{n+1}{=} Q \Rightarrow P \stackrel{n}{=} Q$$
$$P = Q \Leftrightarrow \forall n.\ P \stackrel{n}{=} Q$$

Step-indexing as a category: c.o.f.e.s

Complete Ordered Families of Equivalences

$$(Prop, \overset{n}{=}_{n\in\mathbb{N}}) \xrightarrow{\textit{non-expansive}\text{ function}} (X, \overset{n}{=}_{n\in\mathbb{N}})$$

$$P \overset{n+1}{=} Q \Rightarrow P \overset{n}{=} Q$$

$$P = Q \Leftrightarrow \forall n.\ P \overset{n}{=} Q$$

$$P \overset{n}{=} Q \Rightarrow f(P) \overset{n}{=} f(Q)$$

Step-indexing as a category: c.o.f.e.s

Complete Ordered Families of Equivalences

$$(Prop, \stackrel{n}{=}_{n\in\mathbb{N}}) \xrightarrow{\textit{non-expansive}\text{ function}} (X, \stackrel{n}{=}_{n\in\mathbb{N}})$$

$$P \stackrel{n+1}{=} Q \Rightarrow P \stackrel{n}{=} Q$$
$$P = Q \Leftrightarrow \forall n.\ P \stackrel{n}{=} Q$$

$$P \stackrel{n}{=} Q \Rightarrow f(P) \stackrel{n}{=} f(Q)$$

Category of c.o.f.e.s and non-expansive functions

Semantic domain

$$\mathit{Prop} \cong \mathit{Wld} \xrightarrow{\text{mon}} \mathit{ResMon} \xrightarrow{\text{mon}} \text{``}\mathit{Bool}\text{''}$$

where $\mathit{Wld} \triangleq \mathit{InvName} \xrightarrow{\text{fin}} \blacktriangleright \mathit{Prop}$

Semantic domain

$$\mathit{Prop} \cong \mathit{Wld} \xrightarrow{\text{mon}} \mathit{ResMon} \xrightarrow{\text{mon}} \mathcal{P}^{+,\downarrow}(\mathbb{N})$$

$$\text{where } \mathit{Wld} \triangleq \mathit{InvName} \xrightarrow{\text{fin}} \blacktriangleright \mathit{Prop}$$

Semantic domain

$$\mathit{Prop} \cong \mathit{Wld} \xrightarrow{\text{mon}} \mathit{ResMon} \xrightarrow{\text{mon}} \begin{array}{c}\omega\\ | \\ \vdots \\ | \\ 2 \\ | \\ 1\end{array}$$

where $\mathit{Wld} \triangleq \mathit{InvName} \overset{\text{fin}}{\rightharpoonup} \blacktriangleright \mathit{Prop}$

Semantic domain

Every domain has to be a c.o.f.e., and
every function must be non-expansive

where $Wld = InvName \to \blacktriangleright Prop$

Interpretation: Monoids and invariants

$$[\![P]\!] : \mathit{Prop} = \mathit{Wld} \overset{\text{mon}}{\to} \mathit{ResMon} \overset{\text{mon}}{\to} \mathcal{P}^{+,\downarrow}(\mathbb{N})$$

Interpretation: Monoids and invariants

$$[\![P]\!] : \mathit{Prop} = \mathit{Wld} \overset{\text{mon}}{\to} \mathit{ResMon} \overset{\text{mon}}{\to} \mathcal{P}^{+,\downarrow}(\mathbb{N})$$

$$[\![\, \boxed{a} \,]\!]\, w\, r\, n \triangleq r \sqsupseteq a$$

Interpretation: Monoids and invariants

$$[\![P]\!] : \mathit{Prop} = \mathit{Wld} \overset{\text{mon}}{\to} \mathit{ResMon} \overset{\text{mon}}{\to} \mathcal{P}^{+,\downarrow}(\mathbb{N})$$

$\exists b.\ a \cdot b = r$

$$[\![\boxed{a}]\!]\ w\ r\ n \triangleq r \sqsupseteq a$$

Interpretation: Monoids and invariants

$$[\![P]\!] : \mathit{Prop} = \mathit{Wld} \stackrel{\text{mon}}{\rightarrow} \mathit{ResMon} \stackrel{\text{mon}}{\rightarrow} \mathcal{P}^{+,\downarrow}(\mathbb{N})$$

$\exists b.\ a \cdot b = r$

$$[\![\, \boxed{a} \,]\!]\, w\, r\, n \triangleq r \sqsupseteq a$$

$$[\![\, \boxed{P}^{\iota} \,]\!]\, w\, r\, n \triangleq w(\iota) \stackrel{n}{=} [\![P]\!]$$

Interpretation: Standard connectives

$$[\![P \wedge Q]\!]\, w\, r\, n \triangleq [\![P]\!]\, w\, r\, n \wedge [\![Q]\!]\, w\, r\, n$$

Interpretation: Standard connectives

$$[\![P \land Q]\!]\, w\, r\, n \triangleq [\![P]\!]\, w\, r\, n \land [\![Q]\!]\, w\, r\, n$$

$$\begin{aligned}[\![P * Q]\!]\, w\, r\, n \triangleq\ & \exists r_1, r_2.\ r_1 \cdot r_2 = r \land \\ & [\![P]\!]\, w\, r_1\, n \land [\![Q]\!]\, w\, r_2\, n\end{aligned}$$

Interpretation: Future worlds, framing

$$\llbracket P \Rightarrow Q \rrbracket \, w \; r \; n \triangleq \forall w' \succcurlyeq w, r' \sqsupseteq r, n' \leq n. \\ \llbracket P \rrbracket \, w' \; r' \; n' \Rightarrow \llbracket Q \rrbracket \, w' \; r' \; n'$$

Interpretation: Future worlds, framing

$$\llbracket P \Rightarrow Q \rrbracket\, w\, r\, n \triangleq \forall w' \succcurlyeq w, r' \sqsupseteq r, n' \leq n. \\ \llbracket P \rrbracket\, w'\, r'\, n' \Rightarrow \llbracket Q \rrbracket\, w'\, r'\, n'$$

Interpretation: Future worlds, framing

$$[\![P \Rightarrow Q]\!]\, w\, r\, n \triangleq \forall w' \succcurlyeq w, r' \sqsupseteq r, n' \leq n.\; [\![P]\!]\, w'\, r'\, n' \Rightarrow [\![Q]\!]\, w'\, r'\, n'$$

$$P \Rrightarrow Q \quad \approx \quad P \Rightarrow \mathsf{vs}(Q)$$

$$[\![\mathsf{vs}(Q)]\!]\, w\, r\, n \triangleq \forall w' \succcurlyeq w, r_f \# r.\; \ldots \Rightarrow \exists w'' \succcurlyeq w', r'' \# r_f.\; \ldots \wedge [\![Q]\!]\, w''\, r''\, n$$

Q holds after a ghost move

Interpretation: Future worlds, framing

$$\llbracket P \Rightarrow Q \rrbracket\, w\, r\, n \triangleq \forall w' \succcurlyeq w, r' \sqsupseteq r, n' \leq n.$$
$$\llbracket P \rrbracket\, w'\, r'\, n' \Rightarrow \llbracket Q \rrbracket\, w'\, r'\, n'$$

$$P \Rrightarrow Q \quad \approx \quad P \Rightarrow \mathsf{vs}(Q)$$

$$\llbracket \mathsf{vs}(Q) \rrbracket\, w\, r\, n \triangleq \forall w' \succcurlyeq w, r_f \# r.\ \ldots \Rightarrow$$
$$\exists w'' \succcurlyeq w', r'' \# r_f.\ \ldots \wedge \llbracket Q \rrbracket\, w''\, r''\, n$$

Environment picks

Interpretation: Future worlds, framing

$$[\![P \Rightarrow Q]\!]\, w\, r\, n \triangleq \forall w' \succcurlyeq w, r' \sqsupseteq r, n' \leq n. \\ [\![P]\!]\, w'\, r'\, n' \Rightarrow [\![Q]\!]\, w'\, r'\, n'$$

$$P \Rrightarrow Q \quad \approx \quad P \Rightarrow \mathsf{vs}(Q)$$

$$[\![\mathsf{vs}(Q)]\!]\, w\, r\, n \triangleq \forall w' \succcurlyeq w, r_f \# r.\ \ldots \Rightarrow \\ \exists w'' \succcurlyeq w', r'' \# r_f.\ \ldots \wedge [\![Q]\!]\, w''\, r''\, n$$

We pick

Interpretation: Future worlds, framing

$$[\![P \Rrightarrow Q]\!]\, w\, r\, n \triangleq \forall w' \succsim w, r' \sqsupseteq r, n' \leq n.$$

$r'\, n'$

$P \Rrightarrow$

$[\![\mathrm{vs}(Q)]\!]$

$\wedge\, [\![Q]\!]\, w''\, r''\, n$

Frame-preserving update:

$$\frac{\forall a_f.\; a \# a_f \Rightarrow b \# a_f}{\boxed{a} \Rrightarrow \boxed{b}}$$

Interpretation: Future worlds, framing

$$\llbracket P \Rightarrow Q \rrbracket\, w\, r\, n \triangleq \forall w' \succcurlyeq w, r' \sqsupseteq r, n' \leq n.$$
$$\llbracket P \rrbracket\, w'\, r'\, n' \Rightarrow \llbracket Q \rrbracket\, w'\, r'\, n'$$

$$P \Rrightarrow Q \quad \approx \quad P \Rightarrow \mathsf{vs}(Q)$$

$$\llbracket \mathsf{vs}(Q) \rrbracket\, w\, r\, n \triangleq \forall w' \succcurlyeq w, r_f \# r.\ \ldots \Rightarrow$$
$$\exists w'' \succcurlyeq w', r'' \# r_f.\ \ldots \wedge \llbracket Q \rrbracket\, w''\, r''\, n$$

Unifying Worlds and Resources

The new domain

$$\mathit{Prop} \cong \mathit{Wld} \xrightarrow{\text{mon}} \mathit{ResMon} \xrightarrow{\text{mon}} \begin{array}{c}\omega\\ |\\ \vdots\\ |\\ 2\\ |\\ 1\end{array}$$

$$\mathit{Wld} \triangleq \mathit{InvName} \overset{\text{fin}}{\rightharpoonup} \blacktriangleright \mathit{Prop}$$

The new domain

$$\mathit{Prop} \cong \mathit{Mon} \xrightarrow{\text{mon}} \begin{array}{c}\omega\\ |\\ \vdots\\ |\\ 2\\ |\\ 1\end{array}$$

$$\mathit{Mon} \triangleq (\underbrace{\mathit{InvName} \xrightharpoonup{\text{fin}} \blacktriangleright \mathit{Prop}}_{\mathit{Wld}}) \times \mathit{ResMon}$$

The new domain

ω

$\vdots$

Need: Monoid structure for worlds

Wld

The new domain

Need: Monoid structure for worlds

Managing agreement of invariants

The new domain

$$\mathit{Prop} \cong \mathit{Mon} \xrightarrow{\mathrm{mon}} \begin{array}{c}\omega \\ | \\ \vdots \\ | \\ 2 \\ | \\ 1\end{array}$$

$$\mathit{Mon} \triangleq \underbrace{(\mathit{InvName} \xrightarrow{\mathrm{fin}} \textsc{Ag}(\blacktriangleright \mathit{Prop}))}_{\mathit{Wld}} \times \mathit{ResMon}$$

A monoid for worlds (1st attempt)

$$\text{Ag}(X) \triangleq X$$

A monoid for worlds (1st attempt)

$$\textsc{Ag}(X) \triangleq X$$

$$P \cdot Q \triangleq \begin{cases} P & \text{if } P = Q \\ \bot & \text{if } P \neq Q \end{cases}$$

Future worlds

$$
\begin{array}{c|c|c|c|c|c|l}
\multicolumn{1}{c}{} & \multicolumn{1}{c}{\iota_0} & \multicolumn{1}{c}{\iota_1} & \multicolumn{1}{c}{\iota_2} & \multicolumn{1}{c}{\iota_3} & \multicolumn{1}{c}{\iota_4} & \\
\cline{2-6}
 & P_0 & & & & P_4 & w \\
\cline{2-6}
\end{array}
$$

$$
\begin{array}{c|c|c|c|c|c|l}
\cline{2-6}
\preccurlyeq & P_0 & P_1 & & P_3 & P_4 & w' \\
\cline{2-6}
\end{array}
$$

Future worlds

$$
\begin{array}{c|c|c|c|c|c|c}
 & \iota_0 & \iota_1 & \iota_2 & \iota_3 & \iota_4 & \\
\cline{2-6}
 & P_0 & & & & P_4 & w \\
\cline{2-6}
\multicolumn{7}{c}{} \\
\cline{2-6}
\cdot & P_0 & P_1 & & P_3 & P_4 & w_f \\
\cline{2-6}
\hline
\multicolumn{7}{c}{} \\
\cline{2-6}
= & P_0 & P_1 & & P_3 & P_4 & w' \\
\cline{2-6}
\end{array}
$$

Interpretation: Implication

$$\llbracket P \Rightarrow Q \rrbracket\, w\, r\, n \triangleq \forall w' \succcurlyeq w, r' \sqsupseteq r, n' \leq n.$$
$$\llbracket P \rrbracket\, w'\, r'\, n' \Rightarrow \llbracket Q \rrbracket\, w'\, r'\, n'$$

$$\Downarrow$$

$$\llbracket P \Rightarrow Q \rrbracket\, m\, n \triangleq \forall m' \sqsupseteq m, n' \leq n.\ \llbracket P \rrbracket\, m'\, n' \Rightarrow \llbracket Q \rrbracket\, m'\, n'$$

$\boxed{(w, r)}$ $\boxed{w' \sqsupseteq w \land r' \sqsupseteq r}$

Interpretation: View Shift

$$
\begin{aligned}
[\![\mathsf{vs}(P)]\!]\, w\; r\; n \triangleq\; & \forall w' \succcurlyeq w, r_f \# r.\ \ldots \Rightarrow \\
& \exists w'' \succcurlyeq w', r'' \# r_f.\ \ldots \wedge [\![P]\!]\, w''\; r''\; n
\end{aligned}
$$

Framing worlds

$$
\begin{array}{c|c|c|c|c|c|c}
 & \iota_0 & \iota_1 & \iota_2 & \iota_3 & \iota_4 & \\
\cline{2-6}
 & P_0 & & & & P_4 & w \\
\cline{2-6}
\cdot & P_0 & P_1 & & P_3 & P_4 & w_f \\
\hline
= & P_0 & P_1 & & P_3 & P_4 & w'
\end{array}
$$

Framing worlds

$$
\begin{array}{c|c|c|c|c|c|c}
 & \iota_0 & \iota_1 & \iota_2 & \iota_3 & \iota_4 & \\
\hline
 & P_0 & & & & P_4 & w \\
\cdot & P_0 & P_1 & & P_3 & P_4 & w_f \\
\hline
= & P_0 & P_1 & & P_3 & P_4 & w' \\
\preccurlyeq & P_0 & P_1 & P_2 & P_3 & P_4 & w''
\end{array}
$$

Framing worlds

	ℓ_0	ℓ_1	ℓ_2	ℓ_3	ℓ_4	
	P_0				P_4	w
$\#$	P_0	P_1		P_3	P_4	w_f
$\#$	P_0	P_1	P_2	P_3	P_4	w''

Interpretation: View Shift

$$
\begin{aligned}
[\![\mathsf{vs}(P)]\!]\, w\; r\; n \triangleq\; & \forall w' \succcurlyeq w, r_f \# r.\ \ldots \Rightarrow \\
& \exists w'' \succcurlyeq w', r'' \# r_f.\ \ldots \wedge [\![P]\!]\, w''\; r''\; n
\end{aligned}
$$

$$\Downarrow$$

$$
\begin{aligned}
[\![\mathsf{vs}(P)]\!]\, m\; n \triangleq\; & \forall m_f \# m.\ \ldots \Rightarrow \\
& \exists m'' \# m_f.\ \ldots \wedge [\![P]\!]\, m''\; n
\end{aligned}
$$

$\boxed{(w, r)}$ $\boxed{w_f \# w \wedge r_f \# r'}$

Interpretation: View Shift

$$\llbracket \mathsf{vs}(P) \rrbracket\, w\, r\, n \triangleq \forall w' \succcurlyeq w, r_f \# r.\ \ldots \Rightarrow$$
$$\exists w'' \succcurlyeq w', r'' \# r_f.\ \ldots \wedge \llbracket P \rrbracket\, w''\, r''\, n$$
$$\Downarrow$$
$$\llbracket \mathsf{vs}(P) \rrbracket\, m\, n \triangleq \forall m_f \# m.\ \ldots \Rightarrow$$
$$\exists m'' \# m_f.\ \ldots \wedge \llbracket P \rrbracket\, m''\, n$$

$\boxed{(w, r)}$

$\boxed{w'' \# w_f \wedge r'' \# r_f}$

A monoid for worlds (1st attempt)

$$\textsc{Ag}(X) \triangleq X$$

$$P \cdot Q \triangleq \begin{cases} P & \text{if } P = Q \\ \bot & \text{if } P \neq Q \end{cases}$$

$\textsc{Ag}(X)$ is a c.o.f.e.
Composition must be non-expansive!

A monoid for worlds (1st attempt)

$$\textsc{Ag}(X) \triangleq X$$

$$P \cdot Q \triangleq \begin{cases} P & \text{if } P = Q \\ \bot & \text{if } P \neq Q \end{cases}$$

$\textsc{Ag}(X)$ is a c.o.f.e.
Composition must be non-expansive!

But it is not:
Let $P_1 \overset{n}{=} P_2$, $P_1 \overset{n+1}{\neq} P_2$

A monoid for worlds (1st attempt)

$$\textsc{Ag}(X) \triangleq X$$

$$P \cdot Q \triangleq \begin{cases} P & \text{if } P = Q \\ \bot & \text{if } P \neq Q \end{cases}$$

$\textsc{Ag}(X)$ is a c.o.f.e.
Composition must be non-expansive!

But it is not:
Let $P_1 \overset{n}{=} P_2$, $P_1 \overset{n+1}{\neq} P_2$:
$P_1 \cdot P_1 = P_1$

A monoid for worlds (1st attempt)

$$\mathrm{A\scriptstyle G}(X) \triangleq X$$

$$P \cdot Q \triangleq \begin{cases} P & \text{if } P = Q \\ \bot & \text{if } P \neq Q \end{cases}$$

$\mathrm{A\scriptstyle G}(X)$ is a c.o.f.e.
Composition must be non-expansive!

But it is not:
Let $P_1 \overset{n}{=} P_2$, $P_1 \overset{n+1}{\neq} P_2$:
$P_1 \cdot P_1 = P_1$, but
$P_1 \cdot P_2 = \bot$

A monoid for worlds (1st attempt)

$$\textsc{Ag}(X) \triangleq X$$

$$P \cdot Q \triangleq \begin{cases} P & \text{if } P = Q \end{cases}$$

Composition of *similar* elements must preserve the "degree of definedness"

Composition must be non-expansive!

Let $P_1 \overset{n}{=} P_2$, $P_1 \overset{n+1}{\neq} P_2$:

$P_1 \cdot P_1 = P_1$, but
$P_1 \cdot P_2 = \bot$

The agreement monoid (fixed)

$$\text{A}\textsc{g}(X) \triangleq \{ \qquad\qquad X \}$$

The agreement monoid (fixed)

$$\textsc{Ag}(X) \triangleq \{\text{“}\mathit{Bool}\text{”} \times X\}$$

The agreement monoid (fixed)

$$\textsc{Ag}(X) \triangleq \{(V, P) \in \mathcal{P}^{+,\downarrow}(\mathbb{N}) \times X\}$$

The agreement monoid (fixed)

$$\mathrm{AG}(X) \triangleq \{(V, P) \in \mathcal{P}^{+,\downarrow}(\mathbb{N}) \times X\}$$

Quotient: $(V_1, P_1) = (V_2, P_2)$ if $V_1 = V_2 \wedge \forall n \in V_1.\ P_1 \overset{n}{=} P_2$

The agreement monoid (fixed)

$$\textsc{Ag}(X) \triangleq \{(V, P) \in \mathcal{P}^{+,\downarrow}(\mathbb{N}) \times X\}$$

Quotient: $(V_1, P_1) = (V_2, P_2)$ if $V_1 = V_2 \wedge \forall n \in V_1.\ P_1 \overset{n}{=} P_2$

Embedding: $\widehat{P} \triangleq (\mathbb{N}, P)$

The agreement monoid (fixed)

$$\textsc{Ag}(X) \triangleq \{(V, P) \in \mathcal{P}^{+,\downarrow}(\mathbb{N}) \times X\}$$

Quotient: $(V_1, P_1) = (V_2, P_2)$ if $V_1 = V_2 \land \forall n \in V_1.\ P_1 \overset{n}{=} P_2$

Embedding: $\widehat{P} \triangleq (\mathbb{N}, P)$

Let $P_1 \overset{n}{=} P_2$, $P_1 \overset{n+1}{\neq} P_2$:

The agreement monoid (fixed)

$$\mathrm{AG}(X) \triangleq \{(V, P) \in \mathcal{P}^{+,\downarrow}(\mathbb{N}) \times X\}$$

Quotient: $(V_1, P_1) = (V_2, P_2)$ if $V_1 = V_2 \land \forall n \in V_1.\ P_1 \overset{n}{=} P_2$

Embedding: $\widehat{P} \triangleq (\mathbb{N}, P)$

Let $P_1 \overset{n}{=} P_2$, $P_1 \overset{n+1}{\neq} P_2$:

$$\begin{aligned} &\widehat{P_1} \cdot \widehat{P_2} \\ &= (\{\leq n\}, P_1) \end{aligned}$$

The agreement monoid (fixed)

$$\mathrm{AG}(X) \triangleq \{(V, P) \in \mathcal{P}^{+,\downarrow}(\mathbb{N}) \times X\}$$

Quotient: $(V_1, P_1) = (V_2, P_2)$ if $V_1 = V_2 \land \forall n \in V_1.\ P_1 \overset{n}{=} P_2$

Embedding: $\widehat{P} \triangleq (\mathbb{N}, P)$

Let $P_1 \overset{n}{=} P_2$, $P_1 \overset{n+1}{\neq} P_2$:

$$\begin{aligned} &\widehat{P_1} \cdot \widehat{P_2} \\ &= (\{\leq n\}, P_1) \\ &\overset{n}{=} \widehat{P_1} \cdot \widehat{P_1} \end{aligned}$$

The agreement monoid (fixed)

$$\mathrm{A}\textsc{g}(X) \triangleq \{(V, P) \in \mathcal{P}^{+,\downarrow}(\mathbb{N}) \times X\}$$

Quotient: $(V_1, P_1) = (V_2, P_2)$ if $V_1 = V_2 \land \forall n \in V_1.\ P_1 \stackrel{n}{=} P_2$

Embedding: $\widehat{P} \triangleq (\mathbb{N}, P)$

Let $P_1 \stackrel{n}{=} P_2$, $P_1 \stackrel{n+1}{\neq} P_2$:

$$\begin{aligned} &\widehat{P_1} \cdot \widehat{P_2} \\ &= (\{\leq n\}, P_1) \\ &\stackrel{n}{=} (\mathbb{N}, P_1) \\ &= \widehat{P_1} \cdot \widehat{P_1} \end{aligned}$$

The agreement monoid (fixed)

$$\mathrm{AG}(X) \triangleq \{(V, P) \in \mathcal{P}^{+,\downarrow}(\mathbb{N}) \times X\}$$

Quotient: $(V_1, P_1) = (V_2, P_2)$ if $V_1 = V_2 \wedge \forall n \in V_1.\ P_1 \overset{n}{=} P_2$

Embedding: $\widehat{P} \triangleq (\mathbb{N}, P)$

Let $P_1 \overset{n}{=} P_2$, $P_1 \overset{n+1}{\neq} P_2$:

$$\begin{aligned} &\widehat{P_1} \cdot \widehat{P_2} \\ &= (\{\leq n\}, P_1) \\ &\overset{n}{=} (\mathbb{N}, P_1) \\ &= \widehat{P_1} \cdot \widehat{P_1} \end{aligned}$$

In general:

$$\begin{aligned} &(V_1, P_1) \cdot (V_2, P_2) \\ &\triangleq (V_1 \cap V_2 \cap \\ &\quad \{n \mid P_1 \overset{n}{=} P_2\}, P_1) \end{aligned}$$

The agreement monoid (fixed)

$$\mathrm{AG}(X) \triangleq \{(V, P) \in \mathcal{P}^{+,\downarrow}(\mathbb{N}) \times X\}$$

Quotient: $(V_1, P_1) = (V_2, P_2)$ if $V_1 = V_2 \land \forall n \in V_1.\ P_1 \stackrel{n}{=} P_2$

This monoid has the right equations, and composition is non-expansive!

$$= (\{\leq n\}, P_1)$$

$$\stackrel{n}{=} (\mathbb{N}, P_1)$$

$$= \widehat{P_1} \cdot \widehat{P_1}$$

$$\triangleq (V_1 \cap V_2 \cap \{n \mid P_1 \stackrel{n}{=} P_2\}, P_1)$$

The agreement monoid (almost fixed)

$$\textsc{Ag}(X) \triangleq \{(V, P) \in \mathcal{P}^{+,\downarrow}(\mathbb{N}) \times X\}$$

Quotient: $(V_1, P_1) = (V_2, P_2)$ if $V_1 = V_2 \wedge \forall n \in V_1.\ P_1 \overset{n}{=} P_2$

Embedd

Let $P_1 \overset{n}{=}$

Mechanization in Coq is slightly more complex

$_2, P_2)$

$= (\{\leq n\}, P_1)$ $\triangleq (V_1 \cap V_2 \cap$

$\overset{n}{=} (\mathbb{N}, P_1)$ $\{n \mid P_1 \overset{n}{=} P_2\}, P_1)$

$= \widehat{P_1} \cdot \widehat{P_1}$

The new domain

$$\mathit{Prop} \cong \mathit{Mon} \xrightarrow{\text{mon}} \begin{array}{c} \omega \\ | \\ \vdots \\ | \\ 2 \\ | \\ 1 \end{array}$$

$$\mathit{Mon} \triangleq \underbrace{(\mathit{InvName} \xrightarrow{\text{fin}} \textsc{Ag}(\blacktriangleright \mathit{Prop}))}_{\mathit{Wld}} \times \mathit{ResMon}$$

The new domain

$$\mathit{Prop} \cong \mathit{Mon} \xrightarrow{\text{mon}} \begin{array}{c} \omega \\ | \\ \vdots \\ | \\ 2 \\ | \\ 1 \end{array}$$

$$\mathit{Mon} \triangleq \underbrace{(\mathit{InvName} \xrightarrow{\text{fin}} \textsc{Ag}(\blacktriangleright \mathit{Prop}))}_{\mathit{Wld}} \times \mathit{ResMon}$$

$\textsc{Ag}$ needs to be functorial

The new domain

$$\mathit{Prop} \cong \mathit{Mon} \xrightarrow{\text{mon}} \begin{array}{c}\omega\\ | \\ \vdots \\ | \\ 2 \\ | \\ 1\end{array}$$

$$\mathit{Mon} \triangleq \underbrace{(\mathit{InvName} \xrightarrow{\text{fin}} \textsc{Ag}(\blacktriangleright \mathit{Prop}))}_{\mathit{Wld}} \times \mathit{ResMon}$$

$\textsc{Ag}$ needs to be functorial in a non-expansive way

Category Theory and Coq

Changing the core domain of our model…

Category Theory and Coq

Changing the core domain of our model. . .

. . . without fully grasping its construction.

Category Theory and Coq

Changing the core domain of our model. . .
. . . without fully grasping its construction.

Category theory: Intuition
Coq: Certainty

So what?

May help to do speculation

So what?

May help to do speculation

- Advanced proof technique for linearizability

So what?

May help to do speculation

- Advanced proof technique for linearizability
- *Not* currently supported by Iris

So what?

May help to do speculation

- Advanced proof technique for linearizability
- *Not* currently supported by Iris
- Model: Need *multiple parallel* worlds and resources

Take-away

Take-away

Monoids* are all you need,
and

* and step-indexing

Take-away

Monoids* are all you need, and Category theory is your friend

* and step-indexing

References I

[dDYG14] Pedro da Rocha Pinto, Thomas Dinsdale-Young, and Philippa Gardner. "TaDA: A Logic for Time and Data Abstraction". In: *ECOOP*. 2014.

[DY+10] T. Dinsdale-Young et al. "Concurrent abstract predicates". In: *ECOOP*. 2010.

[Fen09] Xinyu Feng. "Local rely-guarantee reasoning". In: *POPL*. 2009.

[FFS07] Xinyu Feng, Rodrigo Ferreira, and Zhong Shao. "On the relationship between concurrent separation logic and assume-guarantee reasoning". In: *ESOP*. 2007.

[Fu+10] Ming Fu et al. "Reasoning about optimistic concurrency using a program logic for history". In: *CONCUR*. 2010.

[LWN13] Ruy Ley-Wild and Aleksandar Nanevski. "Subjective Auxiliary State for Coarse-Grained Concurrency". In: *POPL*. 2013.

[Nan+14] Aleksandar Nanevski et al. "Communicating State Transition Systems for Fine-Grained Concurrent Resources". In: *ESOP*. 2014.

[O'H07] P.W. O'Hearn. "Resources, concurrency, and local reasoning". In: *TCS* 375.1 (2007), pp. 271–307.

References II

[SB14] Kasper Svendsen and Lars Birkedal. "Impredicative Concurrent Abstract Predicates". In: *ESOP*. 2014.

[SBP13] Kasper Svendsen, Lars Birkedal, and Matthew J. Parkinson. "Modular Reasoning about Separation of Concurrent Data Structures". In: *ESOP*. 2013, pp. 169–188.

[TDB13] Aaron Turon, Derek Dreyer, and Lars Birkedal. "Unifying refinement and Hoare-style reasoning in a logic for higher-order concurrency". In: *ICFP*. 2013.

[VP07] V. Vafeiadis and M. Parkinson. "A marriage of rely/guarantee and separation logic". In: *CONCUR*. 2007.