Logical Atomicity in Iris: the Good, the Bad, and the Ugly

Ralf Jung

MPI-SWS, Germany

Iris Workshop, October 2019

Logical Atomicity in Iris: the Good, ~~the Bad,~~ and the Ugly

Ralf Jung

MPI-SWS, Germany

Iris Workshop, October 2019

What is the right specification?

$$\mathtt{rec}\ \mathtt{inc}(x) = \mathtt{let}\ v = !x;$$
$$\mathtt{if}\ \mathtt{CAS}(x, v, v+1)\ \mathtt{then}\ v$$
$$\mathtt{else}\ \mathtt{inc}(x)$$

What is the right specification?

$$\texttt{rec}\ \texttt{inc}(x) = \texttt{let}\ v = !x;$$
$$\texttt{if}\ \texttt{CAS}(x, v, v+1)\ \texttt{then}\ v$$
$$\texttt{else}\ \texttt{inc}(x)$$

Compare-and-swap

What is the right specification?

$$\texttt{rec}\ \texttt{inc}(x) = \texttt{let}\ v = {!x};\ \texttt{if}\ \texttt{CAS}(x, v, v+1)\ \texttt{then}\ v\ \texttt{else}\ \texttt{inc}(x)$$

$$\precsim$$

$$\lambda x.\, \texttt{FAA}(x, 1)$$

What is the right specification?

$$\texttt{rec inc}(x) = \texttt{let}\ v = {!x};\ \texttt{if}\ \texttt{CAS}(x, v, v+1)\ \texttt{then}\ v\ \texttt{else inc}(x)$$

$$\precsim$$

Fetch-and-add

$$\lambda x.\ \texttt{FAA}(x, 1)$$

What is the right specification?

$$
\begin{aligned}
\texttt{rec}\ \texttt{inc}(x) = \texttt{let}\ v = {!x};\\
\texttt{if}\ \texttt{CAS}(x, v, v+1)\ \texttt{then}\ v\\
\texttt{else}\ \texttt{inc}(x)
\end{aligned}
$$

$$\precsim$$

$$\lambda x.\ \texttt{FAA}(x, 1)$$

What is the right specification?

$\mathtt{rec}\ \mathtt{inc}(x) = \mathtt{let}\ v = !x;$

Common approach:

- Use contextual refinement as spec
- Use linearizability to prove it

$\sim$

$\lambda x.\ \mathtt{FAA}(x, 1)$

$$\frac{\dfrac{\texttt{inc} \precsim \lambda x.\, \texttt{FAA}(x, 1)}{???}}{\{P\}\ \texttt{client}[\texttt{inc}]\ \{Q\}}$$

$$\frac{\dfrac{\texttt{inc} \precsim \lambda x.\, \texttt{FAA}(x, 1)}{???}}{\{P\}\ \texttt{client}[\texttt{inc}]\ \{Q\}}$$

$$\frac{???}{\{P\}\ \texttt{client}[\lambda x.\ \texttt{FAA}(x, 1)]\ \{Q\}}$$

Specification for `FAA`:

$$\{\ell \mapsto v\}\ \texttt{FAA}(\ell, 1)\ \{\ell \mapsto v + 1\}$$

Specification for FAA:

$$\{\ell \mapsto v\}\ \texttt{FAA}(\ell, 1)\ \{\ell \mapsto v + 1\}$$

However, we also have:

$$\{\ell \mapsto v\}\ \texttt{incS}(\ell)\ \{\ell \mapsto v + 1\}$$

where $\texttt{incS} \triangleq \lambda x.\ \texttt{let}\ v = !x;\ x \leftarrow v + 1$

Specification for $\texttt{FAA}$:

$$\{\ell \mapsto v\}\ \texttt{FAA}(\ell, 1)\ \{\ell \mapsto v + 1\}$$

However, we also have:

$$\{\ell \mapsto v\}\ \texttt{incS}(\ell)\ \{\ell \mapsto v + 1\}$$

where $\texttt{incS} \triangleq \lambda x.\ \texttt{let}\ v = \,!x;\ x \leftarrow v + 1$

but $\texttt{incS} \not\precsim \lambda x.\ \texttt{FAA}(x, 1)$!

Specification for `FAA`:

$$\{\ell \mapsto v\}\ \texttt{FAA}(\ell, 1)\ \{\ell \mapsto v + 1\}$$

There is something `FAA` has that `incS` does not:

but `incS` $\not\approx \lambda x.$ `FAA`$(x, 1)$:

Specification for FAA:

$$\{\ell \mapsto v\}\ \texttt{FAA}(\ell, 1)\ \{\ell \mapsto v + 1\}$$

There is something FAA has that incS does not: the invariant rule!

$$\frac{\{P * I\}\ \texttt{FAA}(x, 1)\ \{Q * I\}}{\boxed{I} \vdash \{P\}\ \texttt{FAA}(x, 1)\ \{Q\}}$$

but incS $\not\approx \lambda x.\, \texttt{FAA}(x, 1)$.

Key idea for logical atomicity

An operation is atomic if we can open invariants around it.

Key idea for logical atomicity

An operation is atomic if we can open invariants around it.

How can we open invariants around `inc`(x)?

Logically atomic Hoare triples

1. Define $\langle x.\, P \rangle\; e\; \langle Q \rangle$

Logically atomic Hoare triples

1. Define $\langle x.\, P\rangle\, e\, \langle Q\rangle$
2. Prove $\langle v.\, \ell \mapsto v\rangle\, \texttt{inc}(\ell)\, \langle \ell \mapsto v + 1\rangle$

Logically atomic Hoare triples

1. Define $\langle x.\, P \rangle\; e\; \langle Q \rangle$
2. Prove $\langle v.\, \ell \mapsto v \rangle\; \mathtt{inc}(\ell)\; \langle \ell \mapsto v + 1 \rangle$
3. Prove

$$\frac{\langle x.\, P * I \rangle\; e\; \langle Q * I \rangle}{\boxed{I} \vdash \langle x.\, P \rangle\; e\; \langle Q \rangle}$$

Logically atomic Hoare triples

1. Define $\langle x.\, P \rangle\; e\; \langle Q \rangle$
2. Prove $\langle v.\, \ell \mapsto v \rangle\; \texttt{inc}(\ell)\; \langle \ell \mapsto v + 1 \rangle$
3. Prove

$$\frac{\langle x.\, P * I \rangle\; e\; \langle Q * I \rangle}{\boxed{I} \vdash \langle x.\, P \rangle\; e\; \langle Q \rangle}$$

4. Profit!

Logically atomic Hoare triples

1. Define $\langle x.\ P \rangle\ e\ \langle Q \rangle$
2. Prove $\langle v.\ \ell \mapsto v \rangle\ \texttt{inc}(\ell)\ \langle \ell \mapsto v + 1 \rangle$
3.

Plan for this talk:

Logical atomicity v0.1, v0.2, v1

4. Profit!

Logical Atomicity, v0.1: the basics

Weaker Specification

$$\begin{aligned}\texttt{rec}\ \texttt{inc}(x) = \texttt{let}\ v = !x;\\ \texttt{if}\ \texttt{CAS}(x, v, v+1)\ \texttt{then}\ v\\ \texttt{else}\ \texttt{inc}(x)\end{aligned}$$

Weaker Specification

$$\langle v.\, \ell \mapsto v \rangle \; \texttt{inc}(\ell) \; \langle \ell \mapsto v + 1 \rangle$$

$$\ell \mapsto v \Rrightarrow \exists \gamma.\; \Box\, \mathsf{IsCtr}(\ell, \gamma) * \mathsf{CtrV}(\gamma, v)$$

$$\mathsf{IsCtr}(\ell, \gamma) \vdash \langle v.\, \mathsf{CtrV}(\gamma, v) \rangle \; \texttt{inc}(\ell) \; \langle \mathsf{CtrV}(\gamma, v + 1) \rangle$$

Weaker Specification

Abstract predicate seals off direct access to ℓ

$$\ell \mapsto v \Rrightarrow \exists \gamma.\ \Box\, \mathsf{IsCtr}(\ell, \gamma) * \mathsf{CtrV}(\gamma, v)$$

$$\mathsf{IsCtr}(\ell, \gamma) \vdash \langle v.\ \mathsf{CtrV}(\gamma, v) \rangle\ \mathtt{inc}(\ell)\ \langle \mathsf{CtrV}(\gamma, v + 1) \rangle$$

Weaker Specification

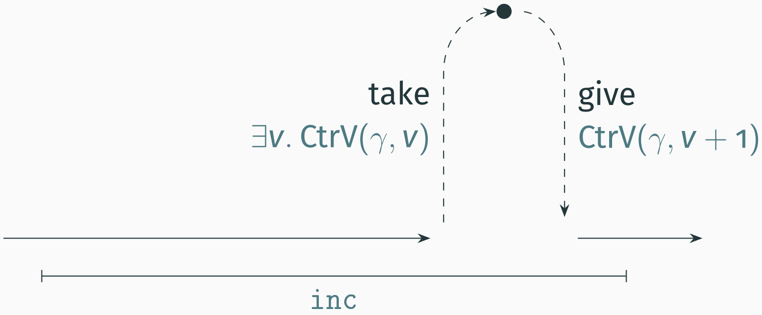
Abstract predicate seals off direct access to ℓ

$$\ell \mapsto v \Rrightarrow \exists \gamma.\ \Box\, \mathsf{IsCtr}(\ell, \gamma) * \mathsf{CtrV}(\gamma, v)$$

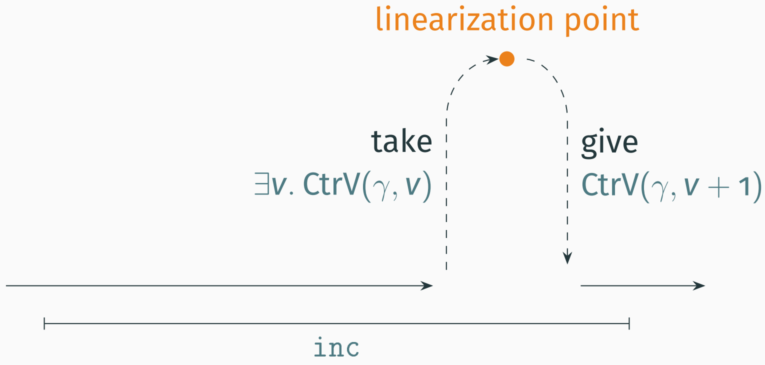
$$\mathsf{IsCtr}(\ell, \gamma) \vdash \langle v.\ \mathsf{CtrV}(\gamma, v) \rangle\ \mathtt{inc}(\ell)\ \langle \mathsf{CtrV}(\gamma, v + 1) \rangle$$

$$\forall v.\ \{\ell \mapsto v\}\ \texttt{incS}(\ell)\ \{\ell \mapsto v + 1\}$$

$$\mathsf{IsCtr}(\ell, \gamma) \vdash \langle v.\, \mathsf{CtrV}(\gamma, v) \rangle\ \mathtt{inc}(\ell)\ \langle \mathsf{CtrV}(\gamma, v + 1) \rangle$$

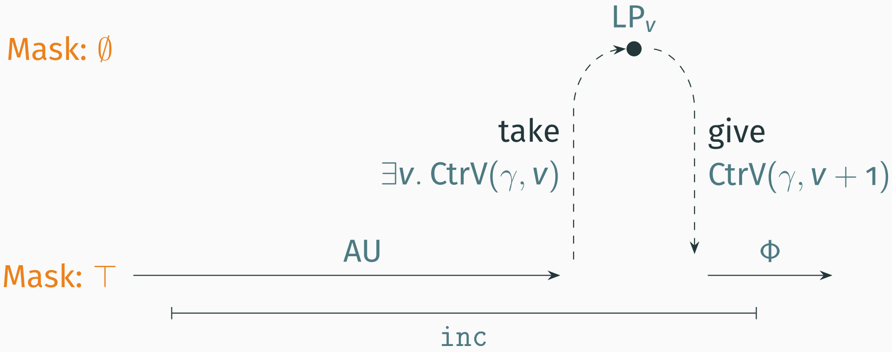


$$\mathsf{IsCtr}(\ell, \gamma) \vdash \langle v.\ \mathsf{CtrV}(\gamma, v) \rangle\ \mathtt{inc}(\ell)\ \langle \mathsf{CtrV}(\gamma, v+1) \rangle$$

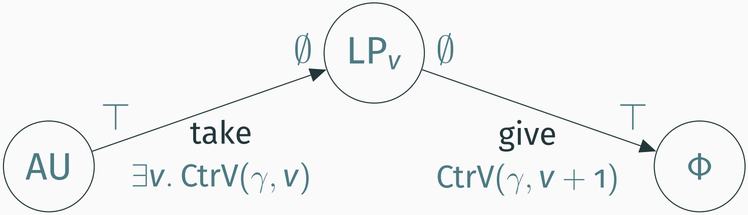


$$\langle v.\, \mathsf{CtrV}(\gamma, v)\rangle\ \texttt{inc}(\ell)\ \langle \mathsf{CtrV}(\gamma, v+1)\rangle^{\top} \triangleq$$

$$\forall \Phi.\, \mathsf{AU} \mathrel{-\!\!*} \mathsf{wp}\ \texttt{inc}(\ell)\ \{\Phi\}$$

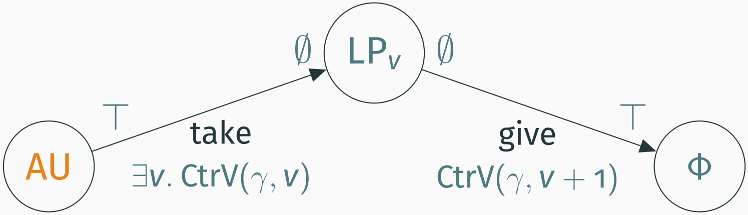


$$\langle v.\, \mathsf{CtrV}(\gamma, v)\rangle\ \mathtt{inc}(\ell)\ \langle \mathsf{CtrV}(\gamma, v+1)\rangle^{\top} \triangleq$$
$$\forall \Phi.\, \mathsf{AU} \mathrel{-\!\!*} \mathsf{wp}\ \mathtt{inc}(\ell)\ \{\Phi\}$$



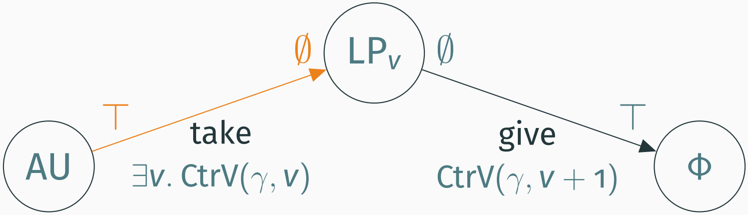
$$\forall \Phi.\ \mathsf{AU} \twoheadrightarrow* \mathsf{wp}\ \mathtt{inc}(\ell)\ \{\Phi\}$$

$\mathsf{AU} \triangleq$



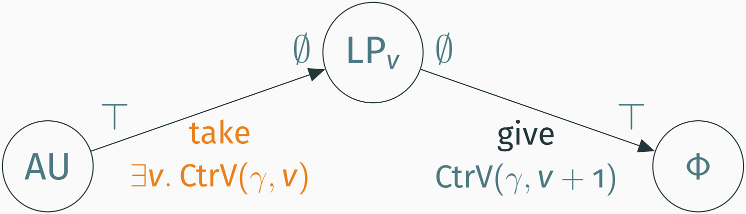
$$\forall \Phi.\, \mathsf{AU} \twoheadrightarrow \mathsf{wp}\; \mathtt{inc}(\ell)\; \{\Phi\}$$

$$\mathsf{AU} \triangleq {}^{\top}\!\Rrightarrow^{\emptyset}$$



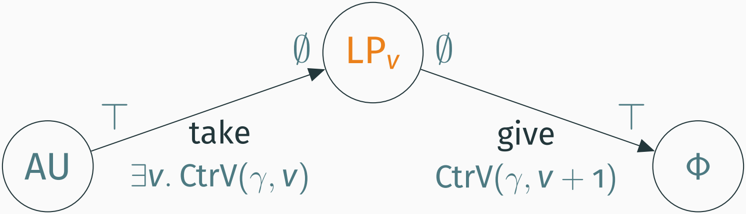
$$\forall \Phi.\, \mathsf{AU} \mathrel{-\!\!*} \mathsf{wp}\ \texttt{inc}(\ell)\ \{\Phi\}$$

$$\mathsf{AU} \triangleq {}^{\top}\!\!\Rrightarrow^{\emptyset} \exists v.\, \mathsf{CtrV}(\gamma, v)$$



$$\forall \Phi.\ \mathsf{AU} \mathrel{-\!\!*} \mathsf{wp}\ \texttt{inc}(\ell)\ \{\Phi\}$$

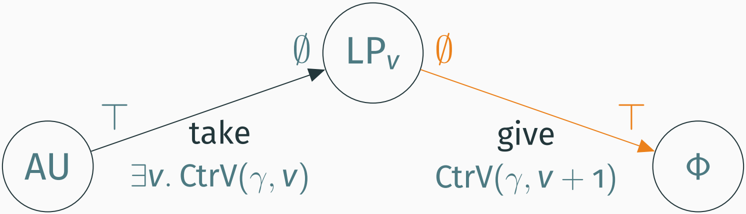
$$\mathsf{AU} \triangleq {}^{\top}\!\Rrightarrow^{\emptyset} \exists v.\ \mathsf{CtrV}(\gamma, v) * \mathsf{LP}_v$$



$$\forall \Phi.\ \mathsf{AU} \twoheadrightarrow \mathsf{wp}\ \mathtt{inc}(\ell)\ \{\Phi\}$$

$$\mathsf{AU} \triangleq {}^{\top}\!\Rrightarrow^{\emptyset} \exists v.\ \mathsf{CtrV}(\gamma, v) * \mathsf{LP}_v$$

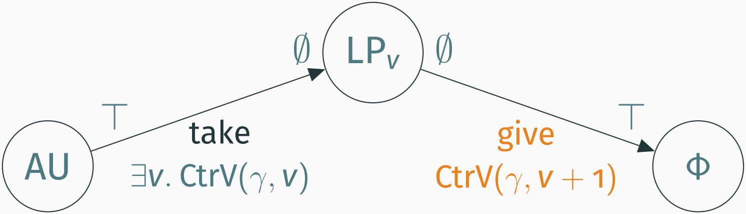
$$\mathsf{LP}_v \triangleq \qquad\qquad {}^{\emptyset}\!\Rrightarrow^{\top}$$



$$\forall \Phi.\ \mathsf{AU} \mathrel{-\!\!*} \mathsf{wp}\ \texttt{inc}(\ell)\ \{\Phi\}$$

$$\mathsf{AU} \triangleq {}^{\top}\!\Rrightarrow^{\emptyset} \exists v.\ \mathsf{CtrV}(\gamma, v) * \mathsf{LP}_v$$

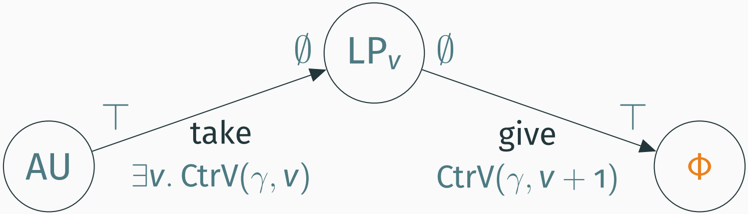
$$\mathsf{LP}_v \triangleq \mathsf{CtrV}(\gamma, v+1) \mathrel{-\!\!*} {}^{\emptyset}\!\Rrightarrow^{\top}$$



$$\forall \Phi.\ \mathsf{AU} \mathrel{-\!\!*} \mathsf{wp}\ \texttt{inc}(\ell)\ \{\Phi\}$$

$$\mathsf{AU} \triangleq {}^{\top}\!\!\Rrightarrow^{\emptyset} \exists v.\ \mathsf{CtrV}(\gamma, v) * \mathsf{LP}_v$$

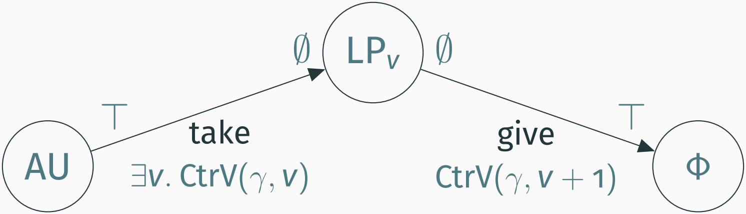
$$\mathsf{LP}_v \triangleq \mathsf{CtrV}(\gamma, v+1) \mathrel{-\!\!*} {}^{\emptyset}\!\!\Rrightarrow^{\top} \Phi$$



$$\forall \Phi.\, \mathsf{AU} \twoheadrightarrow* \mathsf{wp}\ \mathtt{inc}(\ell)\ \{\Phi\}$$

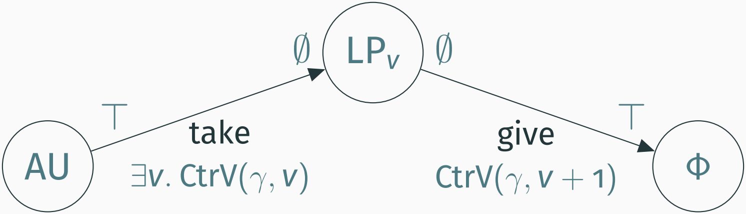
$$\mathsf{AU} \triangleq {}^{\top}\!\!\Rrightarrow^{\emptyset} \exists v.\, \mathsf{CtrV}(\gamma, v) * \mathsf{LP}_v$$

$$\mathsf{LP}_v \triangleq \mathsf{CtrV}(\gamma, v+1) \twoheadrightarrow* {}^{\emptyset}\!\!\Rrightarrow^{\top} \Phi$$



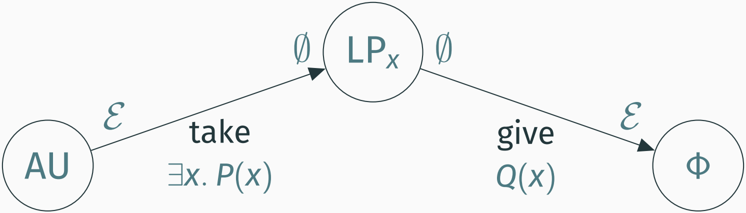
$$\forall \Phi.\ \mathsf{AU} \mathrel{-\!\!*} \mathsf{wp}\ \mathtt{inc}(\ell)\ \{\Phi\}$$

$$\mathsf{AU} \triangleq {}^{\top}\!\!\Rrightarrow^{\emptyset} \exists v.\ \mathsf{CtrV}(\gamma, v) * \left(\mathsf{CtrV}(\gamma, v+1)\ {}^{\emptyset}\!\!\equiv\!\!\!*^{\top}\ \Phi\right)$$



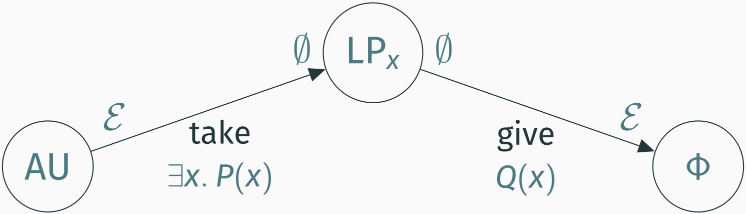
$$\langle x.\, P(x) \rangle\ e\ \langle Q(x) \rangle^{\mathcal{E}} \triangleq \forall \Phi.\ \mathsf{AU} \mathrel{-\!\!*} \mathsf{wp}\ e\ \{\Phi\}$$

$$\mathsf{AU} \triangleq {}^{\mathcal{E}}{\Rrightarrow}^{\emptyset}\, \exists x.\, P(x) * \left(Q(x)\ {}^{\emptyset}{\Rrightarrow\!\!*}^{\mathcal{E}}\ \Phi\right)$$



$$\langle x.\, P(x)\rangle\; e\; \langle Q(x)\rangle^{\mathcal{E}} \triangleq \forall \Phi.\, \mathsf{AU} \mathrel{-\!\!*} \mathsf{wp}\; e\; \{\Phi\}$$

$$\mathsf{AU} \triangleq {}^{\mathcal{E}}{\Rrightarrow}^{\emptyset}\, \exists x.\, P(x) * \left(Q(x)\; {}^{\emptyset}{\Rrightarrow\!\!*}^{\mathcal{E}}\, \Phi\right)$$



$$\langle x.\, P(x)\rangle\ e\ \langle Q(x)\rangle^{\mathcal{E}} \triangleq$$

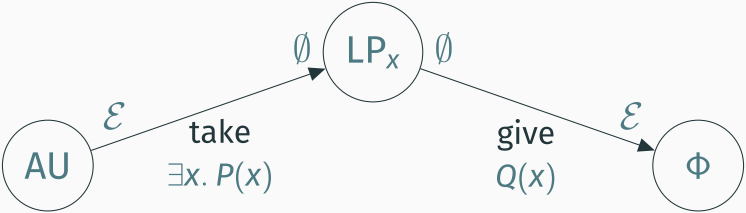
$$\forall \Phi.\ \left({}^{\mathcal{E}}{\Rrightarrow}^{\emptyset}\, \exists x.\, P(x) * \left(Q(x) \mathrel{-\!\!*} {}^{\emptyset}{\Rrightarrow}^{\mathcal{E}}\, \Phi\right)\right) \mathrel{-\!\!*} \mathsf{wp}_{\top}\ e\ \{\Phi\}$$

$$\forall x.\ \{P(x)\}\ e\ \{Q(x)\}_{\top} \iff$$

$$\forall \Phi.\ \left(\exists x.\, P(x) * \left(Q(x) \mathrel{-\!\!*} \Phi\right)\right) \mathrel{-\!\!*} \mathsf{wp}_{\top}\ e\ \{\Phi\}$$

$$\langle x.\, P(x)\rangle\ e\ \langle Q(x)\rangle^{\mathcal{E}} \triangleq \forall \Phi.\ \mathsf{AU} \mathrel{-\!\!*} \mathsf{wp}\ e\ \{\Phi\}$$

$$\mathsf{AU} \triangleq {}^{\mathcal{E}}{\Rrightarrow}^{\emptyset}\, \exists x.\, P(x) * \big(Q(x)\ {}^{\emptyset}{\Rrightarrow\!\!*}^{\mathcal{E}}\ \Phi\big)$$



Let us prove

$$\mathsf{IsCtr}(\ell, \gamma) \vdash$$
$$\langle v.\ \mathsf{CtrV}(\gamma, v) \rangle\ \mathtt{inc}(\ell)\ \langle \mathsf{CtrV}(\gamma, v+1) \rangle$$

Let us prove

$$\boxed{\exists v.\, \ell \mapsto v * \boxed{\bullet\, v}^{\gamma}}^{\mathcal{N}} \vdash$$

$$\left\langle v.\, \boxed{\circ\, v}^{\gamma} \right\rangle \texttt{inc}(\ell) \left\langle \boxed{\circ\, v + 1}^{\gamma} \right\rangle^{\top \setminus \mathcal{N}}$$

Let us prove

$$\boxed{\exists v.\, \ell \mapsto v * \boxed{\bullet\, v}^{\gamma}}^{\mathcal{N}} \vdash$$

$$\langle v.\ \boxed{\circ\, v}^{\gamma} \rangle\ \texttt{inc}(\ell)\ \langle \boxed{\circ\, v + 1}^{\gamma} \rangle^{\top \setminus \mathcal{N}}$$

$\mathsf{AU} \triangleq {}^{\top\setminus\mathcal{N}}\Rrightarrow^{\emptyset} \exists w.\ \boxed{\circ\, w}^{\gamma} * \mathsf{LP}_w \quad \mathsf{LP}_w \triangleq \boxed{\circ\, w+1}^{\gamma}\ {}^{\emptyset}\!\Rrightarrow\!\!*^{\top\setminus\mathcal{N}}\ \Phi$

Context: $\boxed{\exists w.\ \ell \mapsto w * \boxed{\bullet\, w}^{\gamma}}^{\mathcal{N}}$

$\{\mathsf{AU}\}_{\top}$

$\mathtt{inc}(\ell)$

$\{\Phi\}_{\top}$

$\mathsf{AU} \triangleq {}^{\top\setminus\mathcal{N}}\!\Rrightarrow^{\emptyset} \exists w.\, \boxed{\circ\, w}^{\gamma} * \mathsf{LP}_w \quad \mathsf{LP}_w \triangleq \boxed{\circ\, w+1}^{\gamma}\; {}^{\emptyset}\!\Rrightarrow\!\!*^{\top\setminus\mathcal{N}}\, \Phi$

Context: $\boxed{\exists w.\, \ell \mapsto w * \boxed{\bullet\, w}^{\gamma}}^{\mathcal{N}}$

$\{\mathsf{AU}\}_{\top}$

$\texttt{let}\ v = !\ell;$

$\texttt{CAS}(\ell, v, v+1)$ (success case)

$\mathsf{AU} \triangleq {}^{\top\setminus\mathcal{N}}\!\Rrightarrow^{\emptyset} \exists w.\, \boxed{\circ\, w}^{\gamma} * \mathsf{LP}_w \quad \mathsf{LP}_w \triangleq \boxed{\circ\, w+1}^{\gamma}\; {}^{\emptyset}\!\Rrightarrow\!\!*^{\top\setminus\mathcal{N}}\, \Phi$

Context: $\boxed{\exists w.\, \ell \mapsto w * \boxed{\bullet\, w}^{\gamma}}^{\mathcal{N}}$

$\{\mathsf{AU}\}_{\top}$

$\{\ell \mapsto w * \boxed{\bullet\, w}^{\gamma} * \mathsf{AU}\}_{\top\setminus\mathcal{N}}$

$\texttt{let}\; v = {!\ell};$

$\{\mathsf{AU}\}_{\top}$

$\texttt{CAS}(\ell, v, v+1)$ (success case)

$\mathsf{AU} \triangleq {}^{\top\setminus\mathcal{N}}\!\!\Rrightarrow^{\emptyset} \exists w.\ \boxed{\circ\, w}^{\gamma} * \mathsf{LP}_w \quad \mathsf{LP}_w \triangleq \boxed{\circ\, w + 1}^{\gamma}\ {}^{\emptyset}\!\!\Rrightarrow\!\!*^{\top\setminus\mathcal{N}}\ \Phi$

Context: $\boxed{\exists w.\ \ell \mapsto w * \boxed{\bullet\, w}^{\gamma}}^{\mathcal{N}}$

$\{\mathsf{AU}\}_{\top}$

$\texttt{CAS}(\ell, v, v+1)$ (success case)

$\mathsf{AU} \triangleq {}^{\top\setminus\mathcal{N}}\Rrightarrow^{\emptyset} \exists w.\ \boxed{\circ\, w}^{\gamma} * \mathsf{LP}_w \quad \mathsf{LP}_w \triangleq \boxed{\circ\, w+1}^{\gamma}\ {}^{\emptyset}\!\!\Rrightarrow\!\!\!*^{\top\setminus\mathcal{N}}\ \Phi$

Context: $\boxed{\exists w.\ \ell \mapsto w * \boxed{\bullet\, w}^{\gamma}}^{\mathcal{N}}$

$\{\mathsf{AU}\}_{\top}$

$\{\ell \mapsto w * \boxed{\bullet\, w}^{\gamma} * \mathsf{AU}\}_{\top\setminus\mathcal{N}}$

$\texttt{CAS}(\ell, v, v+1)$ (success case)

$\mathsf{AU} \triangleq {}^{\top\setminus\mathcal{N}}\!\Rrightarrow^{\emptyset} \exists w.\ [\circ\, w]^{\gamma} * \mathsf{LP}_w \quad \mathsf{LP}_w \triangleq [\circ\, w+1]^{\gamma}\ {}^{\emptyset}\!\Rrightarrow^{\top\setminus\mathcal{N}} \Phi$

Context: $\boxed{\exists w.\ \ell \mapsto w * [\bullet\, w]^{\gamma}}^{\mathcal{N}}$

$\{\mathsf{AU}\}_{\top}$

$\{\ell \mapsto w * [\bullet\, w]^{\gamma} * \mathsf{AU}\}_{\top\setminus\mathcal{N}}$

$\mathtt{CAS}(\ell, v, v+1)$ (success case)

$\{\ell \mapsto v+1 * [\bullet\, v]^{\gamma} * \mathsf{AU}\}_{\top\setminus\mathcal{N}}$

$\mathsf{AU} \triangleq {}^{\top\setminus\mathcal{N}}\Rrightarrow^{\emptyset} \exists w.\, \boxed{\circ\, w}^{\gamma} * \mathsf{LP}_w \quad \mathsf{LP}_w \triangleq \boxed{\circ\, w+1}^{\gamma}\, {}^{\emptyset}\!\!\Rrightarrow\!\!\ast^{\top\setminus\mathcal{N}}\, \Phi$

Context: $\boxed{\exists w.\, \ell \mapsto w * \boxed{\bullet\, w}^{\gamma}}^{\mathcal{N}}$

$\{\mathsf{AU}\}_{\top}$

$\{\ell \mapsto w * \boxed{\bullet\, w}^{\gamma} * \mathsf{AU}\}_{\top\setminus\mathcal{N}}$

$\texttt{CAS}(\ell, v, v+1)$ (success case)

$\{\ell \mapsto v+1 * \boxed{\bullet\, v}^{\gamma} * \mathsf{AU}\}_{\top\setminus\mathcal{N}}$

$\mathsf{AU} \triangleq {}^{\top\setminus\mathcal{N}}{\Rrightarrow}^{\emptyset}\, \exists w.\, \boxed{\circ\, w}^{\gamma} * \mathsf{LP}_w \qquad \mathsf{LP}_w \triangleq \boxed{\circ\, w + 1}^{\gamma}\; {}^{\emptyset}{\Rrightarrow\!\!*}^{\top\setminus\mathcal{N}}\, \Phi$

Context: $\fbox{$\exists w.\, \ell \mapsto w * \boxed{\bullet\, w}^{\gamma}$}^{\mathcal{N}}$

$\{\mathsf{AU}\}_{\top}$

$\quad \{\ell \mapsto w * \boxed{\bullet\, w}^{\gamma} * \mathsf{AU}\}_{\top\setminus\mathcal{N}}$

$\quad \mathtt{CAS}(\ell, v, v + 1)$ (success case)

$\quad \{\ell \mapsto v + 1 * \boxed{\bullet\, v}^{\gamma} * \mathsf{AU}\}_{\top\setminus\mathcal{N}}$

$\qquad \{\ell \mapsto v + 1 * \boxed{\bullet\, v \cdot \circ\, w}^{\gamma} * \mathsf{LP}_w\}_{\emptyset}$

$$\mathsf{AU} \triangleq {}^{\top\setminus\mathcal{N}}\!\Rrightarrow^{\emptyset} \exists w.\, \boxed{\circ\, w}^{\gamma} * \mathsf{LP}_w \qquad \mathsf{LP}_w \triangleq \boxed{\circ\, w + 1}^{\gamma}\; {}^{\emptyset}\!\Rrightarrow\!\!*^{\top\setminus\mathcal{N}}\, \Phi$$

Context: $\boxed{\exists w.\, \ell \mapsto w * \boxed{\bullet\, w}^{\gamma}}^{\mathcal{N}}$

$$\{\mathsf{AU}\}_{\top}$$

$$\{\ell \mapsto w * \boxed{\bullet\, w}^{\gamma} * \mathsf{AU}\}_{\top\setminus\mathcal{N}}$$

$\texttt{CAS}(\ell, v, v+1)$ (success case)

$$\{\ell \mapsto v + 1 * \boxed{\bullet\, v}^{\gamma} * \mathsf{AU}\}_{\top\setminus\mathcal{N}}$$

$$\{\ell \mapsto v + 1 * \boxed{\bullet\, v \cdot \circ\, w}^{\gamma} * \mathsf{LP}_w\}_{\emptyset}$$

$\mathsf{AU} \triangleq {}^{\top\setminus\mathcal{N}}{\Rrightarrow}^{\emptyset}\, \exists w.\, \boxed{\circ w}^{\gamma} * \mathsf{LP}_w \quad \mathsf{LP}_w \triangleq \boxed{\circ w + 1}^{\gamma}\ {}^{\emptyset}{\Rrightarrow\!\!*}^{\top\setminus\mathcal{N}}\ \Phi$

Context: $\boxed{\exists w.\, \ell \mapsto w * \boxed{\bullet w}^{\gamma}}^{\mathcal{N}}$

$\{\mathsf{AU}\}_{\top}$

$\{\ell \mapsto w * \boxed{\bullet w}^{\gamma} * \mathsf{AU}\}_{\top\setminus\mathcal{N}}$

$\mathtt{CAS}(\ell, v, v+1)$ (success case)

$\{\ell \mapsto v + 1 * \boxed{\bullet v}^{\gamma} * \mathsf{AU}\}_{\top\setminus\mathcal{N}}$

$\{\ell \mapsto v + 1 * \boxed{\bullet v \cdot \circ v}^{\gamma} * \mathsf{LP}_v\}_{\emptyset}$

$\mathrm{AU} \triangleq {}^{\top\setminus\mathcal{N}}\Rrightarrow^{\emptyset} \exists w.\, \boxed{\circ\, w}^{\gamma} * \mathrm{LP}_w \quad \mathrm{LP}_w \triangleq \boxed{\circ\, w + 1}^{\gamma}\; {}^{\emptyset}\!\!\Rrightarrow\!\!*^{\top\setminus\mathcal{N}}\, \Phi$

Context: $\boxed{\exists w.\, \ell \mapsto w * \boxed{\bullet\, w}^{\gamma}}^{\mathcal{N}}$

$\{\mathrm{AU}\}_{\top}$

$\quad \{\ell \mapsto w * \boxed{\bullet\, w}^{\gamma} * \mathrm{AU}\}_{\top\setminus\mathcal{N}}$

$\quad \texttt{CAS}(\ell, v, v+1)$ (success case)

$\quad \{\ell \mapsto v + 1 * \boxed{\bullet\, v}^{\gamma} * \mathrm{AU}\}_{\top\setminus\mathcal{N}}$

$\qquad \{\ell \mapsto v + 1 * \boxed{\bullet\, v \cdot \circ\, v}^{\gamma} * \mathrm{LP}_v\}_{\emptyset}$

$\mathrm{AU} \triangleq {}^{\top\setminus\mathcal{N}}\Rrightarrow^{\emptyset} \exists w.\, \boxed{\circ w}^{\gamma} * \mathrm{LP}_w \quad \mathrm{LP}_w \triangleq \boxed{\circ w + 1}^{\gamma}\ {}^{\emptyset}\!\!\Rrightarrow\!\!\ast^{\top\setminus\mathcal{N}}\ \Phi$

Context: $\boxed{\exists w.\, \ell \mapsto w * \boxed{\bullet w}^{\gamma}}^{\mathcal{N}}$

$$
\begin{aligned}
&\{\mathrm{AU}\}_{\top} \\
&\quad \{\ell \mapsto w * \boxed{\bullet w}^{\gamma} * \mathrm{AU}\}_{\top\setminus\mathcal{N}} \\
&\quad \texttt{CAS}(\ell, v, v+1) \qquad \text{(success case)} \\
&\quad \{\ell \mapsto v + 1 * \boxed{\bullet v}^{\gamma} * \mathrm{AU}\}_{\top\setminus\mathcal{N}} \\
&\qquad \{\ell \mapsto v + 1 * \boxed{\bullet v \cdot \circ v}^{\gamma} * \mathrm{LP}_v\}_{\emptyset} \\
&\qquad \{\ell \mapsto v + 1 * \boxed{\bullet v + 1 \cdot \circ v + 1}^{\gamma} * \mathrm{LP}_v\}_{\emptyset}
\end{aligned}
$$

$\mathsf{AU} \triangleq {}^{\top\setminus\mathcal{N}}\!\!\Rrightarrow^{\emptyset} \exists w.\, \boxed{\circ\, w}^{\gamma} * \mathsf{LP}_w \qquad \mathsf{LP}_w \triangleq \boxed{\circ\, w+1}^{\gamma}\; {}^{\emptyset}\!\!\Rrightarrow\!\!*^{\top\setminus\mathcal{N}}\, \Phi$

Context: $\boxed{\exists w.\, \ell \mapsto w * \boxed{\bullet\, w}^{\gamma}}^{\mathcal{N}}$

$\{\mathsf{AU}\}_{\top}$

$\{\ell \mapsto w * \boxed{\bullet\, w}^{\gamma} * \mathsf{AU}\}_{\top\setminus\mathcal{N}}$

$\texttt{CAS}(\ell, v, v+1)$ (success case)

$\{\ell \mapsto v+1 * \boxed{\bullet\, v}^{\gamma} * \mathsf{AU}\}_{\top\setminus\mathcal{N}}$

$\{\ell \mapsto v+1 * \boxed{\bullet\, v \cdot \circ\, v}^{\gamma} * \mathsf{LP}_v\}_{\emptyset}$

$\{\ell \mapsto v+1 * \boxed{\bullet\, v+1 \cdot \circ\, v+1}^{\gamma} * \mathsf{LP}_v\}_{\emptyset}$

$\{\ell \mapsto v+1 * \boxed{\bullet\, v+1}^{\gamma} * \Phi\}_{\top\setminus\mathcal{N}}$

$\mathsf{AU} \triangleq {}^{\top\setminus\mathcal{N}}\Rrightarrow^{\emptyset} \exists w.\, \boxed{\circ w}^{\gamma} * \mathsf{LP}_w \quad \mathsf{LP}_w \triangleq \boxed{\circ w+1}^{\gamma}\ {}^{\emptyset}\!\Rrightarrow\!\!*^{\top\setminus\mathcal{N}}\ \Phi$

Context: $\boxed{\exists w.\, \ell \mapsto w * \boxed{\bullet w}^{\gamma}}^{\mathcal{N}}$

$$
\begin{array}{l}
\{\mathsf{AU}\}_{\top} \\
\quad \{\ell \mapsto w * \boxed{\bullet w}^{\gamma} * \mathsf{AU}\}_{\top\setminus\mathcal{N}} \\
\quad \texttt{CAS}(\ell, v, v+1) \qquad \text{(success case)} \\
\quad \{\ell \mapsto v+1 * \boxed{\bullet v}^{\gamma} * \mathsf{AU}\}_{\top\setminus\mathcal{N}} \\
\qquad \{\ell \mapsto v+1 * \boxed{\bullet v \cdot \circ v}^{\gamma} * \mathsf{LP}_v\}_{\emptyset} \\
\qquad \{\ell \mapsto v+1 * \boxed{\bullet v+1 \cdot \circ v+1}^{\gamma} * \mathsf{LP}_v\}_{\emptyset} \\
\quad \{\ell \mapsto v+1 * \boxed{\bullet v+1}^{\gamma} * \Phi\}_{\top\setminus\mathcal{N}} \\
\{\Phi\}_{\top}
\end{array}
$$

$\mathsf{AU} \triangleq {}^{\top\setminus\mathcal{N}}{\Rrightarrow}^{\emptyset}\, \exists w.\, \boxed{\circ\, w}^{\gamma} * \mathsf{LP}_w \qquad \mathsf{LP}_w \triangleq \boxed{\circ\, w + 1}^{\gamma}\; {}^{\emptyset}{\Rrightarrow}^{\top\setminus\mathcal{N}}\, \Phi$

Context: $\boxed{\exists w.\, \ell \mapsto w * \boxed{\bullet\, w}^{\gamma}}^{\mathcal{N}}$

$\{\mathsf{AU}\}_{\top}$

We now have

$$\mathsf{IsCtr}(\ell, \gamma) \vdash$$
$$\langle v.\, \mathsf{CtrV}(\gamma, v)\rangle\ \mathtt{inc}(\ell)\ \langle \mathsf{CtrV}(\gamma, v+1)\rangle$$

$\{\Phi\}_{\top}$

$\mathsf{AU} \triangleq {}^{\top\setminus\mathcal{N}}\!\Rrightarrow^{\emptyset} \exists w.\, \boxed{\circ\, w}^{\gamma} * \mathsf{LP}_w \quad \mathsf{LP}_w \triangleq \boxed{\circ\, w+1}^{\gamma}\; {}^{\emptyset}\!\Rrightarrow\!\!*^{\top\setminus\mathcal{N}}\, \Phi$

Context: $\boxed{\exists w.\, \ell \mapsto w * \boxed{\bullet\, w}^{\gamma}}^{\mathcal{N}}$

$\{\mathsf{AU}\}_{\top}$

We now have

$$\mathsf{IsCtr}(\ell, \gamma) \vdash$$
$$\langle v.\, \mathsf{CtrV}(\gamma, v)\rangle\ \texttt{inc}(\ell)\ \langle \mathsf{CtrV}(\gamma, v+1)\rangle$$

What about the invariant rule?

$\{\Phi\}_{\top}$

Invariant rule

Given: $\langle P \rangle\ e\ \langle Q \rangle^{\top}$

$$\frac{\langle x.\, P * I \rangle\ e\ \langle Q * I \rangle^{\mathcal{E}} \qquad \mathcal{N} \subseteq \mathcal{E}}{\boxed{I}^{\mathcal{N}} \vdash \langle x.\, P \rangle\ e\ \langle Q \rangle^{\mathcal{E} \setminus \mathcal{N}}}$$

Invariant rule

Given: $\langle P \rangle\, e\, \langle Q \rangle^{\top}$

Show: $\boxed{P * \ldots \vee Q * \ldots}^{\mathcal{N}} \vdash \{\ldots\}\, e\, \{\ldots\}$

Invariant rule

Given: $\langle P \rangle\ e\ \langle P \rangle^{\top}$

Show: $\boxed{P}^{\mathcal{N}} \vdash \{\mathrm{True}\}\ e\ \{\mathrm{True}\}$

Invariant rule

Given: $\forall \Phi.\ \left({}^{\top}{\models\!\!\!\Rrightarrow}^{\emptyset} P * (P \mathrel{-\!\!*} {}^{\emptyset}{\models\!\!\!\Rrightarrow}^{\top} \Phi) \right) \mathrel{-\!\!*} \mathrm{wp}\ e\ \{\Phi\}$

Show: $\boxed{P}^{\mathcal{N}} \vdash \{\mathrm{True}\}\ e\ \{\mathrm{True}\}$

Invariant rule

Given: $\forall \Phi.\ \left({}^{\top}\!\!\Rrightarrow^{\emptyset} P * (P \twoheadrightarrow {}^{\emptyset}\!\!\Rrightarrow^{\top} \Phi) \right) \twoheadrightarrow \mathsf{wp}\ e\ \{\Phi\}$

Show: $\boxed{P}^{\mathcal{N}} \vdash \mathsf{wp}\ e\ \{\mathsf{True}\}$

Invariant rule

Given: $\forall \Phi.\ \left({}^{\top}\!\!\Rrightarrow^{\emptyset} P * (P \twoheadrightarrow {}^{\emptyset}\!\!\Rrightarrow^{\top} \Phi) \right) \twoheadrightarrow \mathrm{wp}\ e\ \{\Phi\}$

Show: $\boxed{P}^{\mathcal{N}} \vdash \mathrm{wp}\ e\ \{\mathrm{True}\}$

It suffices to show:

$$\boxed{P}^{\mathcal{N}} \vdash {}^{\top}\!\!\Rrightarrow^{\emptyset} P * (P \twoheadrightarrow {}^{\emptyset}\!\!\Rrightarrow^{\top} \mathrm{True})$$

Invariant rule

Given: $\forall\Phi.\ \left({}^{\top}{\Rrightarrow}^{\emptyset} P * (P -\!\!* {}^{\emptyset}{\Rrightarrow}^{\top} \Phi)\right) -\!\!* \mathsf{wp}\ e\ \{\Phi\}$

Show: $\boxed{P}^{\mathcal{N}} \vdash \mathsf{wp}\ e\ \{\mathsf{True}\}$

It suffices to show:

$$\boxed{P}^{\mathcal{N}} \vdash {}^{\top}{\Rrightarrow}^{\emptyset} P * (P -\!\!* {}^{\emptyset}{\Rrightarrow}^{\top} \mathsf{True})$$

This is (almost) the invariant accessor!

Invariant rule

Given: $\forall \Phi.\ \left({}^{\top}\!\Rrightarrow^{\emptyset} P * (P -\!\!* \ {}^{\emptyset}\!\Rrightarrow^{\top} \Phi) \right) -\!\!* \ \mathrm{wp}\ e\ \{\Phi\}$

$$\frac{\langle x.\, P * I \rangle\ e\ \langle Q * I \rangle^{\mathcal{E}} \qquad \mathcal{N} \subseteq \mathcal{E}}{\boxed{I}^{\mathcal{N}} \vdash \langle x.\, P \rangle\ e\ \langle Q \rangle^{\mathcal{E} \setminus \mathcal{N}}}$$

$$\boxed{P}^{\mathcal{N}} \vdash {}^{\top}\!\Rrightarrow^{\emptyset} P * (P -\!\!* \ {}^{\emptyset}\!\Rrightarrow^{\top} \mathrm{True})$$

This is (almost) the invariant accessor!

Logically atomic Hoare triples

1. Define $\langle x.\, P \rangle\ e\ \langle Q \rangle$
2. Prove $\langle v.\, \mathsf{CtrV}(\gamma, v) \rangle\ \mathtt{inc}(\ell)\ \langle \mathsf{CtrV}(\gamma, v+1) \rangle$
3. Prove

$$\frac{\langle x.\, P * I \rangle\ e\ \langle Q * I \rangle}{\boxed{I} \vdash \langle x.\, P \rangle\ e\ \langle Q \rangle}$$

Goals achieved... for weaker spec

Logically atomic Hoare triples

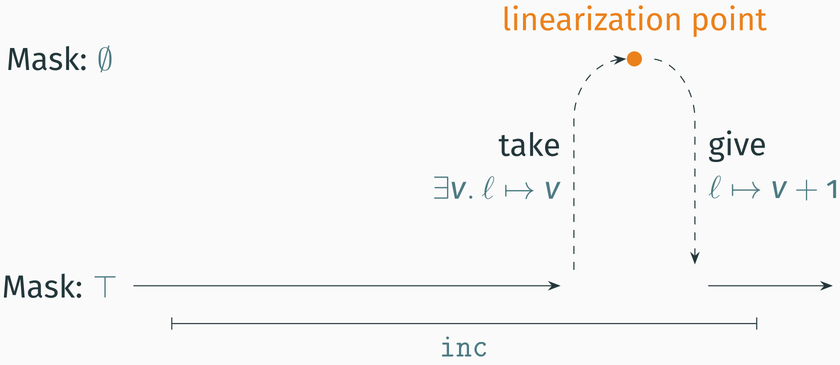
1. Define $\langle x.\, P\rangle\; e\; \langle Q\rangle$
2. Prove $\langle v.\, \mathsf{CtrV}(\gamma, v)\rangle\; \texttt{inc}(\ell)\; \langle \mathsf{CtrV}(\gamma, v+1)\rangle$
3. Prove

$$\frac{\langle x.\, P * I\rangle\; e\; \langle Q * I\rangle}{\boxed{I} \vdash \langle x.\, P\rangle\; e\; \langle Q\rangle}$$

Goals achieved... for weaker spec

What about $\langle v.\, \ell \mapsto v\rangle\; \texttt{inc}(\ell)\; \langle \ell \mapsto v+1\rangle$?

$$\langle v.\, \ell \mapsto v \rangle\ \mathtt{inc}(\ell)\ \langle \ell \mapsto v + 1 \rangle^{\top}$$



$\langle v.\, \ell \mapsto v \rangle\ \texttt{inc}(\ell)\ \langle \ell \mapsto v + 1 \rangle^{\top}$

We can only use the atomic update **once**, at the **linearization point**!

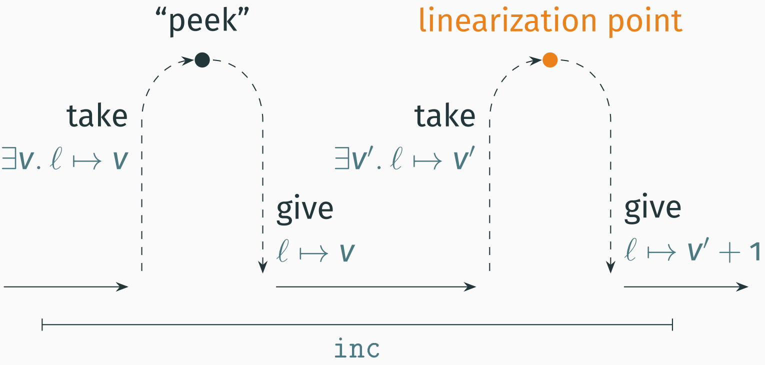
$$
\begin{aligned}
\texttt{rec}\ \texttt{inc}(x) = {} & \texttt{let}\ v = {!x};\\
& \texttt{if}\ \texttt{CAS}(x, v, v + 1)\ \texttt{then}\ v\\
& \texttt{else}\ \texttt{inc}(x)
\end{aligned}
$$

inc

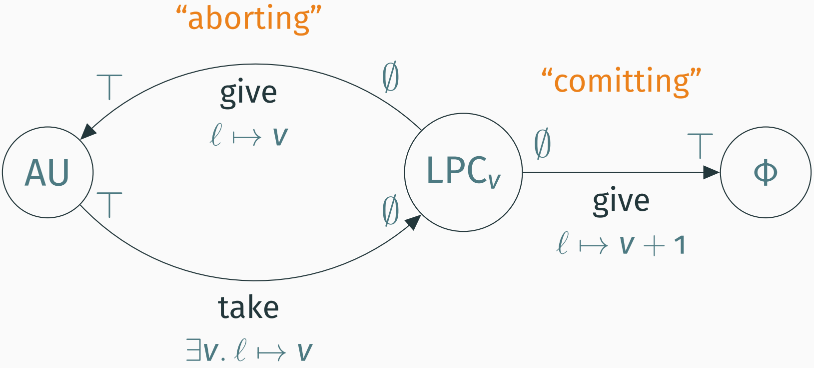
Logical Atomicity, v0.2: aborting

(the Good)

$$\langle v.\, \ell \mapsto v \rangle\ \texttt{inc}(\ell)\ \langle \ell \mapsto v + 1 \rangle^{\top}$$

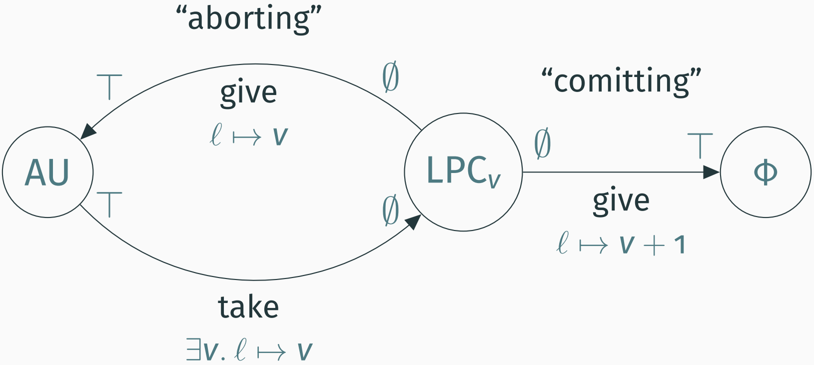


$$\langle \mathbf{v}.\, \ell \mapsto \mathbf{v} \rangle\ \texttt{inc}(\ell)\ \langle \ell \mapsto \mathbf{v} + 1 \rangle^{\top}$$



$$\mathrm{AU} \triangleq {}^{\top}\!\Rrightarrow^{\emptyset} \exists v.\, \ell \mapsto v * \mathrm{LPC}_v$$

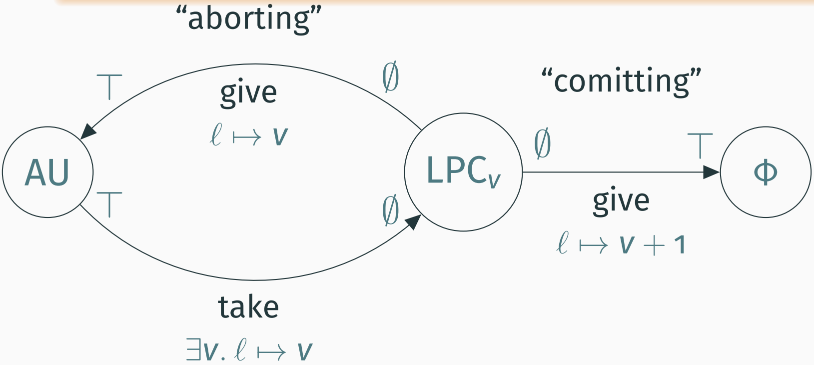
$$\mathrm{LPC}_v \triangleq \left(\ell \mapsto v + 1 \mathrel{-\!\!*} {}^{\emptyset}\!\Rrightarrow^{\top} \Phi\right)$$



$$\mathsf{AU} \triangleq {}^{\top}\!\Rrightarrow^{\emptyset} \exists v.\, \ell \mapsto v * \mathsf{LPC}_v$$

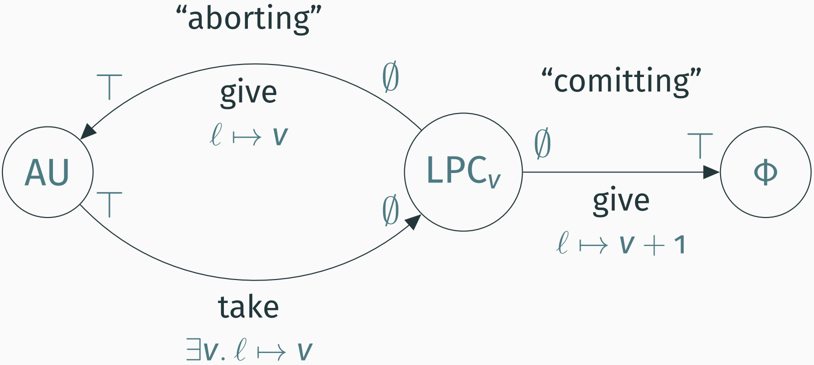
$$\mathsf{LPC}_v \triangleq \quad \wedge\left(\ell \mapsto v + 1 \mathrel{-\!\!*} {}^{\emptyset}\!\Rrightarrow^{\top} \Phi\right)$$

"Additive" conjunction ≅ Internal choice



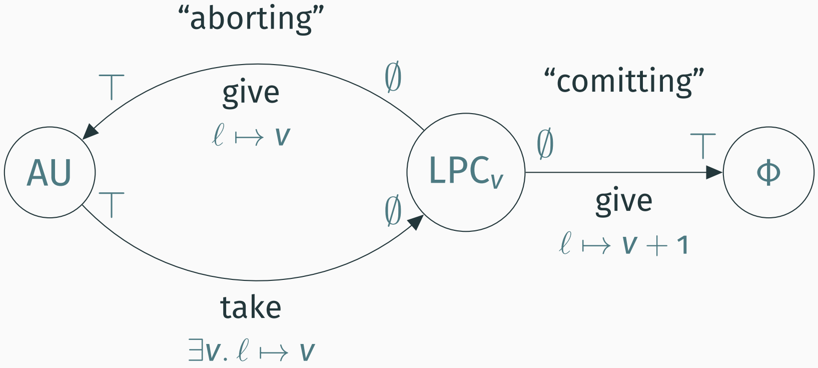
$$\mathrm{AU} \triangleq {}^{\top}{\models\!\!\!\Rrightarrow}^{\emptyset} \exists v.\, \ell \mapsto v * \mathrm{LPC}_v$$

$$\mathrm{LPC}_v \triangleq \left(\ell \mapsto v \mathrel{-\!\!*} {}^{\emptyset}{\models\!\!\!\Rrightarrow}^{\top} \mathrm{AU}\right) \wedge \left(\ell \mapsto v + 1 \mathrel{-\!\!*} {}^{\emptyset}{\models\!\!\!\Rrightarrow}^{\top} \Phi\right)$$



$$\mathsf{AU} \triangleq {}^{\top}\!\!\Rrightarrow^{\emptyset} \exists v.\, \ell \mapsto v * \mathsf{LPC}_v$$

$$\mathsf{LPC}_v \triangleq \left(\ell \mapsto v \mathrel{-\!\!*} {}^{\emptyset}\!\!\Rrightarrow^{\top} \mathsf{AU}\right) \land \left(\ell \mapsto v + 1 \mathrel{-\!\!*} {}^{\emptyset}\!\!\Rrightarrow^{\top} \Phi\right)$$



Logically atomic Hoare triples

1. Define $\langle x.\, P\rangle\; e\; \langle Q\rangle$
2. Prove $\langle v.\, \ell \mapsto v\rangle\; \mathtt{inc}(\ell)\; \langle \ell \mapsto v+1\rangle$
3. Prove

$$\frac{\langle x.\, P * I\rangle\; e\; \langle Q * I\rangle}{\boxed{I} \vdash \langle x.\, P\rangle\; e\; \langle Q\rangle}$$

4. Profit!

Logically atomic Hoare triples

1. Define $\langle x.\, P \rangle\; e\; \langle Q \rangle$
2. Prove $\langle v.\, \ell \mapsto v \rangle\; \mathtt{inc}(\ell)\; \langle \ell \mapsto v + 1 \rangle$
3. Prove

$$\frac{\langle x.\, P * I \rangle\; e\; \langle Q * I \rangle}{\boxed{I} \vdash \langle x.\, P \rangle\; e\; \langle Q \rangle}$$

4. ~~Profit!~~ Publish!

Related work: HOCAP

$$\frac{\forall X.\ \mathsf{x}_{\mathsf{cont}} \overset{1/2}{\longmapsto} X * P \sqsubseteq \mathsf{x}_{\mathsf{cont}} \overset{1/2}{\longmapsto} X \cup \{y\} * Q}{\{\mathsf{bag}(x) * P\}x.\mathsf{Push}(y)\{\mathsf{bag}(x) * Q\}}$$

Related work: HOCAP

$$\frac{\forall X.\ \mathsf{x}_{\mathsf{cont}} \overset{1/2}{\longmapsto} X * P \sqsubseteq \mathsf{x}_{\mathsf{cont}} \overset{1/2}{\longmapsto} X \cup \{y\} * Q}{\{\mathsf{bag}(x) * P\}x.\mathsf{Push}(y)\{\mathsf{bag}(x) * Q\}}$$

$$\mathsf{IsCtr}(\ell, \gamma) \vdash \left(\forall v.\ \boxed{\bullet v}^{\gamma} \Rrightarrow\!\!*_{\top\setminus\mathcal{N}} \boxed{\bullet v + 1}^{\gamma} * \Phi\right) \mathrel{-\!\!*} \mathsf{wp}_{\top}\ \mathtt{inc}(\ell)\ \{\Phi\}$$

Related work: HOCAP

Iris-style logically atomic spec:

$$\mathsf{IsCtr}(\ell, \gamma) \vdash \langle v.\, \mathsf{CtrV}(\gamma, v) \rangle\ \mathtt{inc}(\ell)\ \langle \mathsf{CtrV}(\gamma, v + 1) \rangle^{\top \setminus \mathcal{N}}$$

$$\boxed{\circ\, v}^{\gamma}$$

HOCAP-style logically atomic spec:

$$\mathsf{IsCtr}(\ell, \gamma) \vdash \left(\forall v.\, \boxed{\bullet\, v}^{\gamma} \Rrightarrow\!\!*_{\top \setminus \mathcal{N}} \boxed{\bullet\, v + 1}^{\gamma} * \Phi \right) -\!\!* \\ \mathsf{wp}_{\top}\ \mathtt{inc}(\ell)\ \{\Phi\}$$

Related work: HOCAP

Iris-style logically atomic spec:

$$\langle v.\, \ell \mapsto v \rangle \; \texttt{inc}(\ell) \; \langle \ell \mapsto v + 1 \rangle^{\top}$$

HOCAP-style logically atomic spec:

???

Related work: HOCAP

Iris-style logically atomic spec:

$$\langle v.\, \ell \mapsto v \rangle\ \texttt{inc}(\ell)\ \langle \ell \mapsto v + 1 \rangle^{\top}$$

HOC

HOCAP-style logical atomicity is a pattern, not an abstraction—it is unclear how to even state the invariant rule.

Related work: TaDA

- has invariant rule, aborting and arbitrary pre-/postconditions

Related work: TaDA

- has invariant rule, aborting and arbitrary pre-/postconditions

Open region rule

$$\frac{\lambda; \mathcal{A} \vdash \mathbb{V}x \in X. \left\langle p_p \,\middle|\, I(\mathbf{t}_a^\lambda(x)) * p(x) \right\rangle \ \mathbb{C} \quad \exists\!\!\exists y \in Y. \left\langle q_p(x,y) \,\middle|\, I(\mathbf{t}_a^\lambda(x)) * q(x,y) \right\rangle}{\lambda + 1; \mathcal{A} \vdash \mathbb{V}x \in X. \left\langle p_p \,\middle|\, \mathbf{t}_a^\lambda(x) * p(x) \right\rangle \ \mathbb{C} \quad \exists\!\!\exists y \in Y. \left\langle q_p(x,y) \,\middle|\, \mathbf{t}_a^\lambda(x) * q(x,y) \right\rangle}$$

Related work: TaDA

- has invariant rule, aborting and arbitrary pre-/postconditions
- ties atomicity to level of abstraction

Open region rule

$$\frac{\lambda; \mathcal{A} \vdash \mathbb{A} x \in X. \left\langle p_p \,\middle|\, I(\mathbf{t}_a^\lambda(x)) * p(x) \right\rangle \; \mathbb{C} \quad \mathbb{E} y \in Y. \left\langle q_p(x, y) \,\middle|\, I(\mathbf{t}_a^\lambda(x)) * q(x, y) \right\rangle}{\lambda + 1; \mathcal{A} \vdash \mathbb{A} x \in X. \left\langle p_p \,\middle|\, \mathbf{t}_a^\lambda(x) * p(x) \right\rangle \; \mathbb{C} \quad \mathbb{E} y \in Y. \left\langle q_p(x, y) \,\middle|\, \mathbf{t}_a^\lambda(x) * q(x, y) \right\rangle}$$

Related work: TaDA

- has invariant rule, aborting and arbitrary pre-/postconditions
- ties atomicity to level of abstraction

TaDA cannot prove

$$\langle v.\, \ell \mapsto v \rangle\ \texttt{inc}(\ell)\ \langle \ell \mapsto v + 1 \rangle^{\top}$$

as there is no abstraction!

Logically Atomic Case Studies

- Increment

Logically Atomic Case Studies

- Increment on abstract heap

Logically Atomic Case Studies

- Increment on abstract heap
- Elimination Stack on abstract heap

Logically Atomic Case Studies

- Increment on abstract heap
- Elimination Stack on abstract heap
- Flat Combiner (by Zhen)

Logically Atomic Case Studies

- Increment on abstract heap
- Elimination Stack on abstract heap
- Flat Combiner (by Zhen)
- Atomic snapshot (by Marianna)
- RDCSS (by Marianna, Rodolphe and Gaurav)

Logically Atomic Case Studies

- Increment on abstract heap
- Elimination Stack on abstract heap
- Flat Combiner (by Zhen)
- Atomic snapshot (by Marianna)
- RDCSS (by Marianna, Rodolphe and Gaurav)
- Herlihy-Wing-Queue (by Rodolphe, Derek, Gaurav)

Logically Atomic Case Studies

- Increment on abstract heap
- Elimination Stack on abstract heap
- Flat Combiner (by Zhen)
- Atomic snapshot (by Marianna)
- RDCSS (by Marianna, Rodolphe and Gaurav)
- Herlihy-Wing-Queue (by Rodolphe, Derek, Gaurav)

Logically Atomic Case Studies

- Increment on abstract heap
- Elimination Stack on abstract heap
- F
- A
- R … v)
- Herlihy-Wing-Queue (by Rodolphe, Derek, Gaurav)

Many of these use helping, which logical atomicity v0.2 does not support!

Logical Atomicity, v1: laters

(the Ugly)

Helping occurs when one threads' linearization point is executed by another thread.

Helping occurs when one threads' linearization point is executed by another thread.

$\boxed{\ldots * \mathsf{AU} * \ldots}$

Helping occurs when one threads' linearization point is executed by another thread.

▷ AU is useless!

... ∗ AU ∗ ...

Laterability

A proposition P is laterable if it can be split into "something persistent" and "something later"

Laterability

A proposition P is laterable if it can be split into "something persistent" and "something later"

$$\text{create:} \quad \triangleright I \Rrightarrow\!\!\!*_{\mathcal{E}} \boxed{I}^{\mathcal{N}}$$

$$\text{open:} \quad \boxed{I}^{\mathcal{N}} \quad {}^{\mathcal{N}}\!\Rrightarrow\!\!\!*^{\top} \triangleright I$$

$$\text{close:} \quad \boxed{I}^{\mathcal{N}} * \triangleright I \; {}^{\top}\!\Rrightarrow\!\!\!*^{\mathcal{N}}$$

Laterability

A proposition P is laterable if it can be split into "something persistent" and "something later"

Laterable assertions P can be losslessly put into an invariant:

$$P \Rrightarrow \exists Q. \boxed{Q} * (\triangleright Q \Rrightarrow P)$$

Laterability

A proposition P is laterable if it can be split into "something persistent" and "something later":

$$\text{laterable}(P) \triangleq P \twoheadrightarrow\!\!* \; \exists Q.\ \triangleright Q * \Box(\triangleright Q \twoheadrightarrow\!\!* \diamond P)$$

Laterable assertions P can be losslessly put into an invariant:

$$P \Rrightarrow \exists Q.\ \boxed{Q} * (\triangleright Q \Rrightarrow P)$$

$$\text{laterable}(\triangleright P) \qquad \frac{\text{timeless}(P)}{\text{laterable}(P)} \qquad \frac{\text{persistent}(P)}{\text{laterable}(P)}$$

$$\text{laterable}(\triangleright P) \qquad \frac{\text{timeless}(P)}{\text{laterable}(P)} \qquad \frac{\text{persistent}(P)}{\text{laterable}(P)}$$

$$\frac{\text{laterable}(P) \qquad \text{laterable}(Q)}{\text{laterable}(P * Q)}$$

timeless(P) persistent(P)

Needed for helping:

laterable(AU)

$$\text{laterable}(\text{make\_laterable}(P))$$

$$\text{make\_laterable}(P) \vdash P$$

$$\text{laterable}(\text{make\_laterable}(P))$$

$$\text{make\_laterable}(P) \vdash P$$

$$\frac{\text{laterable}(\Gamma) \qquad \Diamond\,\Gamma \vdash P}{\Gamma \vdash \text{make\_laterable}(P)}$$

$$\text{laterable}(\text{make\_laterable}(P))$$

$$\text{make\_laterable}(P) \triangleq$$
$$\exists Q.\ \triangleright Q * \Box(\triangleright Q -\!\!* P)$$

$$\Gamma \vdash \text{make\_laterable}(P)$$

Defining logically atomic triples (v1)

$$\langle x.\, P(x)\rangle\; e\; \langle v.\, Q(x,v)\rangle^{\mathcal{E}} \triangleq \forall \Phi.\, \mathsf{AU} \twoheadrightarrow* \mathsf{wp}_{\top}\, e\, \{\Phi\}$$

$$\mathsf{AU} \triangleq \nu U.\, \mathsf{make\_laterable}\Big({}^{\mathcal{E}}{\Rrightarrow}^{\emptyset}\, \exists x.\, P(x) * \\ \big(\big(P(x)\; {}^{\emptyset}{\equiv\!\!*}^{\mathcal{E}}\, U\big) \wedge \big(\forall v.\, Q(x,v)\; {}^{\emptyset}{\equiv\!\!*}^{\mathcal{E}}\, \Phi(v)\big)\big)\Big)$$

Defining logically atomic triples (v1)

$$\langle x.\, P(x)\rangle\; e\; \langle v.\, Q(x,v)\rangle^{\mathcal{E}} \triangleq \forall \Phi.\, \mathsf{AU} \mathrel{-\!\!*} \mathsf{wp}_{\top}\; e\; \{\Phi\}$$

$$\mathsf{AU} \triangleq \nu U.\, \mathsf{make\_laterable}\Big({}^{\mathcal{E}}{\Rrightarrow}^{\emptyset}\, \exists x.\, P(x) * \Big(\big(P(x) \;{}^{\emptyset}{\equiv\!\!*}^{\mathcal{E}}\; U\big) \wedge \big(\forall v.\, Q(x,v) \;{}^{\emptyset}{\equiv\!\!*}^{\mathcal{E}}\; \Phi(v)\big)\Big)\Big)$$

Defining logically atomic triples (v1)

$$\langle x.\, P(x) \rangle\ e\ \langle v.\, Q(x,v) \rangle^{\mathcal{E}} \triangleq \forall \Phi.\, \mathsf{AU} \mathrel{-\!\!*} \mathsf{wp}_{\top}\ e\ \{\Phi\}$$

$$\mathsf{AU} \triangleq \nu U.\, \mathsf{make\_laterable}\Big({}^{\mathcal{E}}\!\!\Rrightarrow^{\emptyset} \exists x.\, P(x) * \Big(\big(P(x) \;{}^{\emptyset}\!\!\Rrightarrow\!\!*^{\mathcal{E}}\; U\big) \wedge \big(\forall v.\, Q(x,v) \;{}^{\emptyset}\!\!\Rrightarrow\!\!*^{\mathcal{E}}\; \Phi(v)\big) \Big) \Big)$$

Defining logically atomic triples (v1)

$$\langle x.\, P(x)\rangle\; e\; \langle v.\, Q(x,v)\rangle^{\mathcal{E}} \triangleq \forall \Phi.\, \mathsf{AU} \mathrel{-\!\!*} \mathsf{wp}_{\top}\; e\; \{\Phi\}$$

$$\mathsf{AU} \triangleq \nu U.\, \mathsf{make\_laterable}\Big({}^{\mathcal{E}}\!\Rrightarrow^{\emptyset} \exists x.\, P(x) * \big((P(x) \;{}^{\emptyset}\!\!\Rrightarrow\!\!*^{\mathcal{E}}\, U) \wedge (\forall v.\, Q(x,v) \;{}^{\emptyset}\!\!\Rrightarrow\!\!*^{\mathcal{E}}\, \Phi(v)) \big) \Big)$$

Defining logically atomic triples (v1)

$$\langle x.\, P(x) \rangle \; e \; \langle v.\, Q(x,v) \rangle^{\mathcal{E}} \triangleq \forall \Phi.\, \mathsf{AU} \mathrel{-\!\!*} \mathsf{wp}_{\top}\, e \, \{\Phi\}$$

$$\mathsf{AU} \triangleq \nu U.\, \text{make\_laterable}\Big({}^{\mathcal{E}}\!\!\Rrightarrow^{\emptyset} \exists x.\, P(x) * \big((P(x) \; {}^{\emptyset}\!\!\Rrightarrow\!\!*^{\mathcal{E}}\, U) \wedge (\forall v.\, Q(x,v) \; {}^{\emptyset}\!\!\Rrightarrow\!\!*^{\mathcal{E}}\, \Phi(v)) \big) \Big)$$

Laterable atomic updates?

Ugly introduction rule:

$$\frac{\mathsf{laterable}(\Gamma) \qquad {}^{\mathcal{E}}{\models\!\!\!\Rrightarrow}^{\top}\, \exists x.\, P(x) * \Big(\big(P(x) \;{}^{\emptyset}\!\!\Rrightarrow\!\!\ast^{\mathcal{E}}\, \Gamma\big) \wedge \big(\forall v.\, Q(x,v) \;{}^{\emptyset}\!\!\Rrightarrow\!\!\ast^{\mathcal{E}}\, \Phi(v)\big)\Big)}{\Gamma \vdash \mathsf{AU}}$$

Laterable atomic updates?

Ugly introduction rule:

$$\frac{\mathsf{laterable}(\Gamma) \qquad {}^{\mathcal{E}}{\models\!\!\!\Rightarrow}^{\top}\, \exists x.\, P(x) * \Big(\big(P(x)\ {}^{\emptyset}{\equiv\!\!\ast}^{\mathcal{E}}\ \Gamma\big) \land \big(\forall v.\, Q(x, v)\ {}^{\emptyset}{\equiv\!\!\ast}^{\mathcal{E}}\ \Phi(v)\big) \Big)}{\Gamma \vdash \mathsf{AU}}$$

Laterable atomic updates?

Ugly introduction rule:

$$\frac{\mathrm{laterable}(\Gamma)\qquad {}^{\mathcal{E}}{\models\!\!\Rrightarrow}^{\top}\, \exists x.\, P(x) * \Big(\big(P(x)\ {}^{\emptyset}{\Rrightarrow\!\!*}^{\mathcal{E}}\ \Gamma\big) \land \big(\forall v.\, Q(x,v)\ {}^{\emptyset}{\Rrightarrow\!\!*}^{\mathcal{E}}\ \Phi(v)\big) \Big)}{\Gamma \vdash \mathrm{AU}}$$

Laterable atomic updates!

We can now do helping:

$$\mathsf{AU} \Rrightarrow\!\!\ast\; \exists Q.\ \triangleright Q * (\triangleright Q \Rrightarrow \mathsf{AU})$$

$$\Rrightarrow\!\!\ast\; \boxed{\ldots * Q * \ldots} * (\triangleright Q \Rrightarrow \mathsf{AU})$$

Logical Atomicity lets us give

- concise and powerful
- Hoare-style specifications
- to concurrent data structures
- that make use of helping.