Iris: Higher-Order Concurrent Separation Logic

Lecture 13: Weakest Preconditions and the Fancy Update Modality

Lars Birkedal

Aarhus University, Denmark

December 5, 2017

Overview

Earlier:

- Operational Semantics of $\lambda_{\mathrm{ref,conc}}$
  - e, $(h, e) \rightsquigarrow (h, e')$, and $(h, \mathcal{E}) \to (h', \mathcal{E}')$
- Basic Logic of Resources
  - $l \hookrightarrow v$, $P * Q$, $P \mathrel{-\!\!*} Q$, $\Gamma \mid P \vdash Q$
- Basic Separation Logic
  - $\{P\}\, e\, \{v.Q\}$: Prop, isList l xs, ADTs, foldr
- Later ($\triangleright$) and Persistent ($\square$) Modalities.
- Concurrency Intro, Invariants and Ghost State
- CAS, Spin Locks, Concurrent Counter Modules.

Today:

- Weakest preconditions and the fancy update modality
- Key Points:
  - Towards Iris base logic, used in Coq implementation and next week's case study.

Weakest Precondition

- Typing rule:

$$\frac{\mathcal{E} \subseteq \mathsf{InvName} \qquad \Gamma \vdash e : \mathit{Exp} \qquad \Gamma \vdash \Phi : \mathit{Val} \to \mathsf{Prop}}{\Gamma \vdash \mathsf{wp}_{\mathcal{E}}\, e\, \{\Phi\} : \mathsf{Prop}}$$

- Intended meaning of wp becomes clearer when we define Hoare triples in terms of it as

$$\{P\}\, e\, \{\Phi\}_{\mathcal{E}} \triangleq \Box\, (P \mathrel{-\!\!*} \mathsf{wp}_{\mathcal{E}}\, e\, \{\Phi\})\,.$$

- Thus, $\mathsf{wp}_{\mathcal{E}}\, e\, \{\Phi\}$ is indeed the *weakest* (*i.e.*, implied by any other) precondition such that e runs safely and, if it terminates with a value v, the assertion $\Phi(v)$ holds.
- Note the $\Box$ modality.
  - It guarantees that all the non-persistent resources required by e are contained in P.
  - (e may use other resources, governed by invariants, but those are indeed persistent.)

Structural Rules for $\mathsf{wp}_{\mathcal{E}}\ e\ \{\Phi\}$

WP-MONO

$$\frac{}{(\forall v.\, \Phi(v) \twoheadrightarrow \Psi(v)) * \mathsf{wp}_{\mathcal{E}}\ e\ \{\Phi\} \vdash \mathsf{wp}_{\mathcal{E}}\ e\ \{\Psi\}}$$

WP-FRAME

$$\frac{}{P * \mathsf{wp}_{\mathcal{E}}\ e\ \{\Phi\} \vdash \mathsf{wp}_{\mathcal{E}}\ e\ \{P * \Phi\}}$$

WP-FRAME-STEP

$$\frac{e \notin \mathit{Val}}{\triangleright P * \mathsf{wp}_{\mathcal{E}}\ e\ \{\Phi\} \vdash \mathsf{wp}_{\mathcal{E}}\ e\ \{P * \Phi\}}$$

WP-VAL

$$\frac{}{\Phi(v) \vdash \mathsf{wp}_{\mathcal{E}}\ v\ \{\Phi\}}$$

WP-BIND

$$\frac{}{\mathsf{wp}_{\mathcal{E}}\ e\ \{v.\, \mathsf{wp}_{\mathcal{E}}\ E[\,v\,]\ \{\Phi\}\} \vdash \mathsf{wp}_{\mathcal{E}}\ E[\,e\,]\ \{\Phi\}}$$

- Analogous to corresponding Hoare rules we have seen earlier.

Rules for Basic Language Constructs: style

- The rules for basic langauge constructs given with arbitrary postcondition.
- For instance,

$$\frac{\textsc{wp-store}}{\triangleright(\ell \hookrightarrow v) * \triangleright(\ell \hookrightarrow w \mathrel{-\!\!*} \Phi()) \vdash \mathsf{wp}_{\mathcal{E}}\,(\ell \leftarrow w)\,\{\Phi\}}$$

- Why ? Simplifies reasoning, in particular
  - allows for easy symbolic execution of programs.
  - avoids many uses of WP-MONO and WP-FRAME
  - (see notes for detailed example)

Rules for Basic Language Constructs

$$\frac{}{\triangleright \Phi() * \triangleright \mathsf{wp}_{\mathcal{E}}\, e \,\{v.\, \mathsf{True}\} \vdash \mathsf{wp}_{\mathcal{E}}\ \mathsf{fork}\ \{e\}\ \{\Phi\}}\ \textsc{wp-fork}$$

$$\frac{}{\triangleright(\forall \ell.\, \ell \hookrightarrow v \twoheadrightarrow \Phi(\ell)) \vdash \mathsf{wp}_{\mathcal{E}}\, \mathsf{ref}(v)\, \{\Phi\}}\ \textsc{wp-alloc}$$

$$\frac{}{\triangleright(\ell \hookrightarrow v) * \triangleright(\ell \hookrightarrow v \twoheadrightarrow \Phi(v)) \vdash \mathsf{wp}_{\mathcal{E}}\ !\,\ell\, \{\Phi\}}\ \textsc{wp-load}$$

$$\frac{}{\triangleright(\ell \hookrightarrow v) * \triangleright(\ell \hookrightarrow w \twoheadrightarrow \Phi()) \vdash \mathsf{wp}_{\mathcal{E}}\, (\ell \leftarrow w)\, \{\Phi\}}\ \textsc{wp-store}$$

$$\frac{}{\triangleright(\ell \mapsto v) * \triangleright(\ell \mapsto w \twoheadrightarrow \Phi(\mathsf{true})) \vdash \mathsf{wp}_{\mathcal{E}}\, \mathsf{cas}(\ell, v, w)\, \{\Phi\}}\ \textsc{wp-CAS-suc}$$

$$\frac{}{v \neq v' \wedge \triangleright(\ell \mapsto v) * \triangleright(\ell \mapsto v \twoheadrightarrow \Phi(\mathsf{false})) \vdash \mathsf{wp}_{\mathcal{E}}\, \mathsf{cas}(\ell, v', w)\, \{\Phi\}}\ \textsc{wp-CAS-fail}$$

Rules for Basic Language Constructs

$$\frac{}{\triangleright\, \mathsf{wp}_{\mathcal{E}}\ e[v/x][(\mathsf{rec}\ f(x) = e)/f]\ \{\Phi\} \vdash \mathsf{wp}_{\mathcal{E}}\ (\mathsf{rec}\ f(x) = e)v\ \{\Phi\}}\ \textsc{wp-rec}$$

$$\frac{}{\triangleright\, \mathsf{wp}_{\mathcal{E}}\ v_i\ \{\Phi\} \vdash \mathsf{wp}_{\mathcal{E}}\ \pi_i\ (v_1, v_2)\ \{\Phi\}}\ \textsc{wp-proj}$$

$$\frac{}{\triangleright\, \mathsf{wp}_{\mathcal{E}}\ e_1\ \{\Phi\} \vdash \mathsf{wp}_{\mathcal{E}}\ \mathsf{if\ true\ then}\ e_1\ \mathsf{else}\ e_2\ \{\Phi\}}\ \textsc{wp-if-true}$$

$$\frac{}{\triangleright\, \mathsf{wp}_{\mathcal{E}}\ e_2\ \{\Phi\} \vdash \mathsf{wp}_{\mathcal{E}}\ \mathsf{if\ false\ then}\ e_1\ \mathsf{else}\ e_2\ \{\Phi\}}\ \textsc{wp-if-false}$$

$$\frac{}{\triangleright\, \mathsf{wp}_{\mathcal{E}}\ e_i\ [u/x_i]\ \{\Phi\} \vdash \mathsf{wp}_{\mathcal{E}}\ \mathsf{match\ inj}_i\ u\ \mathsf{with\ inj}_1\ x_1 \Rightarrow e_1 \mid \mathsf{inj}_2\ x_2 \Rightarrow e_2\ \mathsf{end}\ \{\Phi\}}\ \textsc{wp-match}$$

How about rules for invariants ?

- There are no rules for weakest preconditions for opening and closing invariants.
- Moving towards the Iris base logic, we disentangle manipulations of invariants from weakest preconditions / Hoare triples.
- Invariants will instead be manipulated by the so-called fancy update modality.

Fancy Update Modality

- Typing for ${}^{\mathcal{E}_1}{\Rrightarrow}^{\mathcal{E}_2} P$:

$$\frac{\Gamma \vdash P : \mathsf{Prop}}{\Gamma \vdash {}^{\mathcal{E}_1}{\Rrightarrow}^{\mathcal{E}_2} P : \mathsf{Prop}}$$

- Intuition: ${}^{\mathcal{E}_1}{\Rrightarrow}^{\mathcal{E}_2} P$ contains resources r which, together with resources in invariants named $\mathcal{E}_1$, can be updated (via frame preserving update) to resources, which can be split into resources satisfying P and resources in invariants named $\mathcal{E}_2$.
- Subsumes the update modality:

$$\frac{\textsc{Fup-upd}}{\Rrightarrow P \vdash {}^{\mathcal{E}}{\Rrightarrow}^{\mathcal{E}} P}$$

Rules for fancy update modality

Intro + structural rules (analogous to those for the update modality):

$$\textsc{Fup-mono}\ \frac{P \vdash Q}{{}^{\mathcal{E}_1}{\Rrightarrow}^{\mathcal{E}_2} P \vdash {}^{\mathcal{E}_1}{\Rrightarrow}^{\mathcal{E}_2} Q}$$

$$\textsc{Fup-intro-mask}\ \frac{\mathcal{E}_2 \subseteq \mathcal{E}_1}{P \vdash {}^{\mathcal{E}_1}{\Rrightarrow}^{\mathcal{E}_2}\ {}^{\mathcal{E}_2}{\Rrightarrow}^{\mathcal{E}_1} P}$$

$$\textsc{Fup-trans}\ \frac{}{{}^{\mathcal{E}_1}{\Rrightarrow}^{\mathcal{E}_2}\ {}^{\mathcal{E}_2}{\Rrightarrow}^{\mathcal{E}_3} P \vdash {}^{\mathcal{E}_1}{\Rrightarrow}^{\mathcal{E}_3} P}$$

Derivable rule:

$$\textsc{Fup-intro}\ \frac{}{P \vdash {}^{\mathcal{E}}{\Rrightarrow}^{\mathcal{E}} P}$$

We write ${\Rrightarrow}_{\mathcal{E}} P$ for ${}^{\mathcal{E}}{\Rrightarrow}^{\mathcal{E}} P$.

Rules for fancy update modality

Framing:

$$\textsc{Fup-frame}\quad \frac{\mathcal{E}_f \text{ disjoint from } \mathcal{E}_1 \cup \mathcal{E}_2}{Q * {}^{\mathcal{E}_1}{\Rrightarrow}^{\mathcal{E}_2} P \vdash {}^{\mathcal{E}_1 \uplus \mathcal{E}_f}{\Rrightarrow}^{\mathcal{E}_2 \uplus \mathcal{E}_f} (Q * P)}$$

Simpler derivable rules:

$$\frac{}{Q * {}^{\mathcal{E}_1}{\Rrightarrow}^{\mathcal{E}_2} P \vdash {}^{\mathcal{E}_1}{\Rrightarrow}^{\mathcal{E}_2} (Q * P)} \qquad \frac{\mathcal{E}_1 \subseteq \mathcal{E}_2}{{\Rrightarrow}_{\mathcal{E}_1} P \vdash {\Rrightarrow}_{\mathcal{E}_2} P}$$

Rules for fancy update modality

Allocation and opening of invariants:

$$\textsc{Inv-alloc}\quad \frac{\mathcal{E}_1 \text{ infinite}}{\triangleright P \vdash {}^{\mathcal{E}_2}\!\Rrightarrow^{\mathcal{E}_2} \exists \iota \in \mathcal{E}_1.\, \boxed{P}^{\iota}}$$

$$\textsc{Inv-open}\quad \frac{\iota \in \mathcal{E}}{\boxed{P}^{\iota} \vdash {}^{\mathcal{E}}\!\Rrightarrow^{\mathcal{E}\setminus\{\iota\}} \left(\triangleright P * \left(\triangleright P \mathrel{-\!\!*} {}^{\mathcal{E}\setminus\{\iota\}}\!\Rrightarrow^{\mathcal{E}} \mathsf{True}\right)\right)}$$

The Inv-open rule is used not just to open invariants, but also to close them. It implies the following two rules:

$$\frac{\iota \in \mathcal{E}}{\boxed{P}^{\iota} \vdash {}^{\mathcal{E}}\!\Rrightarrow^{\mathcal{E}\setminus\{\iota\}} \triangleright P} \qquad \frac{\iota \in \mathcal{E}}{\boxed{P}^{\iota} \vdash {}^{\mathcal{E}}\!\Rrightarrow^{\mathcal{E}\setminus\{\iota\}} \left(\triangleright P \mathrel{-\!\!*} {}^{\mathcal{E}\setminus\{\iota\}}\!\Rrightarrow^{\mathcal{E}} \mathsf{True}\right)}$$

Fancy update modality and weakest preconditions

Weakest preconditions are closed under fancy updates:

$$\textsc{wp-vup}\quad \dfrac{}{\mathrel{|\!\!\Rrightarrow}_{\mathcal{E}} \mathsf{wp}_{\mathcal{E}}\; e \,\{v. \mathrel{|\!\!\Rrightarrow}_{\mathcal{E}} \Phi(v)\} \vdash \mathsf{wp}_{\mathcal{E}}\; e \,\{\Phi\}}$$

Example: used to update ghost state, e.g., we can derive:b

$$\dfrac{a \leadsto b}{\mathsf{wp}_{\mathcal{E}}\; e \,\{v. \Phi(v) * \boxed{a}^{\gamma}\} \vdash \mathsf{wp}\; e \,\{v. \Phi(v) * \boxed{b}^{\gamma}\}}$$

Fancy update modality and weakest preconditions

The following plays a role similar to that played by HT-INV-OPEN earlier.

WP-ATOMIC

$$\frac{e \text{ is an atomic expression}}{{}^{\mathcal{E}_1}{\Rrightarrow}^{\mathcal{E}_2} \mathsf{wp}_{\mathcal{E}_2}\, e\, \{v.\, {}^{\mathcal{E}_2}{\Rrightarrow}^{\mathcal{E}_1} \Phi(v)\} \vdash \mathsf{wp}_{\mathcal{E}_1}\, e\, \{\Phi\}}$$

Can use it to derive the following rule for accessing invariants using the weakest precondition assertion.

WP-INV-OPEN

$$\frac{e \text{ is an atomic expression}}{\boxed{I}^{\iota} * \left(\triangleright I \mathrel{-\!\!*} \mathsf{wp}_{\mathcal{E}\setminus\{\iota\}}\, e\, \{v.\, \triangleright I * \Phi(v)\}\right) \vdash \mathsf{wp}_{\mathcal{E}}\, e\, \{\Phi\}}$$

which can then be used to derive HT-INV-OPEN (see notes).

Fancy update modality and weakest preconditions

Finally, we have the following, which generalizes the earlier HT-FRAME-ATOMIC.

WP-FRAME-STEP

$$\frac{e \notin Val \qquad \mathcal{E}_2 \subseteq \mathcal{E}_1}{\left({}^{\mathcal{E}_1}{\Rrightarrow}^{\mathcal{E}_2} \triangleright {}^{\mathcal{E}_2}{\Rrightarrow}^{\mathcal{E}_1} P\right) * \mathsf{wp}_{\mathcal{E}_2}\, e \,\{\Phi\} \vdash \mathsf{wp}_{\mathcal{E}_1}\, e\, \{P * \Phi\}}$$

Note: no specific rule for allocating invariants in connection with weakest preconditions – allocation is handled separately by fancy update modality which then interacts with weakest preconditions via the above rules.

Fancy view shift

- Define fancy view shift:

$$P \;{}^{\mathcal{E}_1}\!\Rrightarrow^{\mathcal{E}_2} Q \triangleq \Box(P \mathrel{-\!\!*} {}^{\mathcal{E}_1}\!\models\!\!\Rrightarrow^{\mathcal{E}_2} Q).$$

- If $\mathcal{E}_1 = \mathcal{E}_2$ we write $P \Rrightarrow_{\mathcal{E}_1} Q$ for $P \;{}^{\mathcal{E}_1}\!\Rrightarrow^{\mathcal{E}_1} Q$.
- Hoare triples and fancy view shifts: final generalization of rule of consequence:

$$\textsc{Ht-csq}\quad \frac{S \vdash P' \;{}^{\mathcal{E}}\!\Rrightarrow^{\mathcal{E}} P \qquad S \vdash \{P\}\, e\, \{v.Q\}_{\mathcal{E}} \qquad S \vdash \forall v.\, Q(v) \;{}^{\mathcal{E}}\!\Rrightarrow^{\mathcal{E}} Q'(v)}{S \vdash \{P'\}\, e\, \{v.Q'\}_{\mathcal{E}}}$$

  - Compared to earlier, the generalization is the use of the fancy view shift, which allows to use invariants in $\mathcal{E}$ when showing the view shift.