Topics in Programming Languages HW2

문순원

Syntax

$$
\begin{array}{rll}
\text{Variables} & \text{Var} & x \\
\text{Terms} & \text{Tm} & e ::= x \\
 & & \quad \mid n \mid -e \\
 & & \quad \mid \lambda x.e \mid e_1\ e_2 \\
 & & \quad \mid (e_1, e_2) \mid e\ \texttt{.fst} \mid e\ \texttt{.snd} \\
 & & \quad \mid \texttt{inl}.\ e \mid \texttt{inr}.\ e \mid \texttt{case}(e_0, x.e_1, y.e_2) \\
 & & \quad \mid \texttt{new}\ e \mid !\,e \mid e_1 \leftarrow e_2
\end{array}
$$

Statics

We restricts our type system to only allow first-order reference types. Defining logical relation for type systems with higher-order state requires more advanced techniques such as step-indexing (Dreyer et al. 2022) or parametric bisimulations (Hur et al. 2012).

$$
\begin{array}{rlr}
\text{First-order Types} & \text{FTy} & \tau, \sigma ::= \texttt{int} \mid \tau \times \sigma \mid \tau + \sigma \\
\text{Types} & \text{Ty} & A, B ::= \texttt{int} \mid A \to B \mid A \times B \mid A + B \mid \texttt{ref}\ \tau \\
\text{Contexts} & \text{Ctx} & \Gamma ::= \cdot \mid \Gamma, x : A
\end{array}
$$

We skip the definition of type system.

Dynamics

While we restrict our type system to first-order references, our operational semantics supports full higher-order references.

$$
\begin{array}{rll}
\text{Locations} & \text{Loc} & \ell \\
\text{Heaps} & \text{Heap} & h \\
\text{Environments} & \text{Env} & \rho \\
\text{Values} & \text{Val} & v ::= n \mid (\lambda x.e, \rho) \mid (v_1, v_2) \mid \texttt{inl}.\ v \mid \texttt{inr}.\ v \mid \ell \\
\text{Results} & \text{Res} & r ::= (h, v) \mid \texttt{err}
\end{array}
$$

The big-step evaluation relation $h, \rho \vdash e \Downarrow r$ is inductively defined.

Variable:

$$
\frac{x \in \text{dom}(\rho)}{h, \rho \vdash x \Downarrow (h, \rho(x))} \qquad \frac{x \notin \text{dom}(\rho)}{h, \rho \vdash x \Downarrow \texttt{err}}
$$

Integer:

$$
\frac{}{h, \rho \vdash n \Downarrow (h, n)} \qquad \frac{h, \rho \vdash e \Downarrow (h', n)}{h, \rho \vdash -e \Downarrow (h', -n)} \qquad \frac{h, \rho \vdash e \Downarrow \texttt{err}}{h, \rho \vdash -e \Downarrow \texttt{err}}
$$

Function:

$$\frac{}{h, \rho \vdash \lambda x.e \Downarrow (h, (\lambda x.e, \rho))} \qquad \frac{h, \rho \vdash e_1 \Downarrow \left(h', \left(\lambda x.e_f, \rho_f\right)\right) \quad h', \rho \vdash e_2 \Downarrow (h'', v) \quad h'', \rho_f[x \mapsto v] \vdash e_f \Downarrow r}{h, \rho \vdash e_1\, e_2 \Downarrow r}$$

$$\frac{h, \rho \vdash e_1 \Downarrow r_1 \quad r_1 \notin \left\{\left(h', \left(\lambda x.e_f, \rho_f\right)\right) \mid h', x, e_f, \rho_f\right\}}{h, \rho \vdash e_1\, e_2 \Downarrow \texttt{err}} \qquad \frac{h, \rho \vdash e_1 \Downarrow \left(h', \left(\lambda x.e_f, \rho_f\right)\right) \quad h', \rho \vdash e_2 \Downarrow \texttt{err}}{h, \rho \vdash e_1\, e_2 \Downarrow \texttt{err}}$$

Product:

$$\frac{h, \rho \vdash e_1 \Downarrow (h', v_1) \quad h', \rho \vdash e_2 \Downarrow (h'', v_2)}{h, \rho \vdash (e_1, e_2) \Downarrow (h'', (v_1, v_2))} \qquad \frac{h, \rho \vdash e_1 \Downarrow \texttt{err}}{h, \rho \vdash (e_1, e_2) \Downarrow \texttt{err}} \qquad \frac{h, \rho \vdash e_1 \Downarrow (h', v_1) \quad h', \rho \vdash e_2 \Downarrow \texttt{err}}{h, \rho \vdash (e_1, e_2) \Downarrow \texttt{err}}$$

$$\frac{h, \rho \vdash e \Downarrow (h', (v_1, v_2))}{h, \rho \vdash e\ \texttt{.fst} \Downarrow (h', v_1)} \qquad \frac{h, \rho \vdash e \Downarrow r_1 \quad r_1 \notin \{(h', (v_1, v_2)) \mid h', v_1, v_2\}}{h, \rho \vdash e\ \texttt{.fst} \Downarrow \texttt{err}}$$

$$\frac{h, \rho \vdash e \Downarrow (h', (v_1, v_2))}{h, \rho \vdash e\ \texttt{.snd} \Downarrow (h', v_2)} \qquad \frac{h, \rho \vdash e \Downarrow r_1 \quad r_1 \notin \{(h', (v_1, v_2)) \mid h', v_1, v_2\}}{h, \rho \vdash e\ \texttt{.snd} \Downarrow \texttt{err}}$$

Sum:

$$\frac{h, \rho \vdash e \Downarrow (h', v)}{h, \rho \vdash \texttt{inl.}\ e \Downarrow (h', \texttt{inl.}\ v)} \qquad \frac{h, \rho \vdash e \Downarrow \texttt{err}}{h, \rho \vdash \texttt{inl.}\ e \Downarrow \texttt{err}}$$

$$\frac{h, \rho \vdash e \Downarrow (h', v)}{h, \rho \vdash \texttt{inr.}\ e \Downarrow (h', \texttt{inr.}\ v)} \qquad \frac{h, \rho \vdash e \Downarrow \texttt{err}}{h, \rho \vdash \texttt{inr.}\ e \Downarrow \texttt{err}}$$

$$\frac{h, \rho \vdash e_0 \Downarrow (h', \texttt{inl.}\ v) \quad h', \rho[x \mapsto v] \vdash e_1 \Downarrow r}{h, \rho \vdash \texttt{case}(e_0, x.e_1, y.e_2) \Downarrow r} \qquad \frac{h, \rho \vdash e_0 \Downarrow (h', \texttt{inr.}\ v) \quad h', \rho[y \mapsto v] \vdash e_2 \Downarrow r}{h, \rho \vdash \texttt{case}(e_0, x.e_1, y.e_2) \Downarrow r}$$

$$\frac{h, \rho \vdash e_0 \Downarrow r_0 \quad r_0 \notin \{(h', \texttt{inl.}\ v) \mid h', v\} \cup \{(h', \texttt{inr.}\ v) \mid h', v\}}{h, \rho \vdash \texttt{case}(e_0, x.e_1, y.e_2) \Downarrow \texttt{err}}$$

Reference:

$$\frac{h, \rho \vdash e \Downarrow (h', v) \quad \ell \notin \operatorname{dom}(h')}{h, \rho \vdash \texttt{new}\ e \Downarrow (h'[\ell \mapsto v], \ell)} \qquad \frac{h, \rho \vdash e \Downarrow \texttt{err}}{h, \rho \vdash \texttt{new}\ e \Downarrow \texttt{err}}$$

$$\frac{h, \rho \vdash e \Downarrow (h', \ell) \quad \ell \in \operatorname{dom}(h')}{h, \rho \vdash \,!\, e \Downarrow (h', h'(\ell))} \qquad \frac{h, \rho \vdash e \Downarrow r_1 \quad r \notin \{(h', \ell) \mid \ell \in \operatorname{dom}(h')\}}{h, \rho \vdash \,!\, e \Downarrow \texttt{err}}$$

$$\frac{h, \rho \vdash e_1 \Downarrow (h', \ell) \quad h', \rho \vdash e_2 \Downarrow (h'', v)}{h, \rho \vdash e_1 \leftarrow e_2 \Downarrow (h''[\ell \mapsto v], v)}$$

$$\frac{h, \rho \vdash e_1 \Downarrow r_1 \quad r_1 \notin \{(h', \ell) \mid h', \ell\}}{h, \rho \vdash e_1 \leftarrow e_2 \Downarrow \texttt{err}} \qquad \frac{h, \rho \vdash e_1 \Downarrow (h', \ell) \quad h', \rho \vdash e_2 \Downarrow \texttt{err}}{h, \rho \vdash e_1 \leftarrow e_2 \Downarrow \texttt{err}}$$

Semantic model

We define the semantic model following (Dreyer et al. 2022). However, we use simpler definition of worlds since we're not interested in advanced properties of programs.

For modeling reference types, we have to define Kripke world that keep tracks invariants on heap.

$$\text{Worlds } W \in \text{World} \coloneqq \text{Loc} \overset{\text{fin}}{\rightharpoonup} \mathcal{P}(\text{Val})$$
$$\text{World Extension} \quad W_1 \sqsubseteq W_2 \coloneqq \forall \ell, X.\, W_1(\ell) = X \Rightarrow W_2(\ell) = X$$
$$\text{World Satisfaction} \;\; \text{wsat}(W, h) \coloneqq \forall \ell, X.\, W(\ell) = X \Rightarrow h(\ell) \in X$$

We define the value and term relation by structural recursion on the type syntax.

$$\mathcal{V}[\![-]\!] : \text{Ty} \to \mathcal{P}(\text{World} \times \text{Val})$$
$$\mathcal{E}[\![-]\!] : \text{Ty} \to \mathcal{P}(\text{World} \times \text{Env} \times \text{Tm})$$
$$\mathcal{G}[\![-]\!] : \text{Ctx} \to \mathcal{P}(\text{World} \times \text{Env})$$

$$\begin{aligned}
\mathcal{V}[\![\texttt{int}]\!] &\coloneqq \{(W, n) \mid W, n\} \\
\mathcal{V}[\![A \to B]\!] &\coloneqq \{(W, (\lambda x.e, \rho)) \mid \forall W', v.\, W \sqsubseteq W' \Rightarrow (W', v) \in \mathcal{V}[\![A]\!] \Rightarrow (W', \rho[x \mapsto v], e) \in \mathcal{E}[\![B]\!]\} \\
\mathcal{V}[\![A \times B]\!] &\coloneqq \{(W, (v_1, v_2)) \mid (W, v_1) \in \mathcal{V}[\![A]\!] \wedge (W, v_2) \in \mathcal{V}[\![B]\!]\} \\
\mathcal{V}[\![A + B]\!] &\coloneqq \{(W, \texttt{inl}.\, v) \mid (W, v) \in \mathcal{V}[\![A]\!]\} \cup \{(W, \texttt{inr}.\, v) \mid (W, v) \in \mathcal{V}[\![B]\!]\} \\
\mathcal{V}[\![\texttt{ref}\ \tau]\!] &\coloneqq \{(W, \ell) \mid W(\ell) = \{v \mid \vdash v : \tau\}\} \\
\mathcal{E}[\![A]\!] &\coloneqq \{(W, \rho, e) \mid \forall W', h, r.\, W \sqsubseteq W' \Rightarrow \text{wsat}(W', h) \Rightarrow h, \rho \vdash e \Downarrow r \Rightarrow \\
&\qquad \exists h_r, v_r, W_r.\, r = (h_r, v_r) \wedge W' \sqsubseteq W_r \wedge \text{wsat}(W_r, h_r) \wedge (W_r, v_r) \in \mathcal{V}[\![A]\!]\} \\
\mathcal{G}[\![\Gamma]\!] &\coloneqq \{(W, \rho) \mid \forall x : A \in \Gamma.\, (W, \rho(x)) \in \mathcal{V}[\![A]\!]\}
\end{aligned}$$

Now we define the semantic typing relation.

$$\Gamma \vDash e : A \coloneqq \forall W, \rho.\, (W, \rho) \in \mathcal{G}[\![\Gamma]\!] \Rightarrow (W, \rho, e) \in \mathcal{E}[\![A]\!]$$

Basic properties of logical relation

Lemma *(first-order types)*:
- If $\vdash v : \tau$, then $(W, v) \in \mathcal{V}[\![\tau]\!]$ for all W.
- If $(W, v) \in \mathcal{V}[\![\tau]\!]$, then $\vdash v : \tau$.

Proof: By induction on τ. □

Lemma *(monotonicity)*:
- If $(W, v) \in \mathcal{V}[\![A]\!]$ and $W \sqsubseteq W'$, then $(W', v) \in \mathcal{V}[\![A]\!]$.
- If $(W, \rho, e) \in \mathcal{E}[\![A]\!]$ and $W \sqsubseteq W'$, then $(W', \rho, e) \in \mathcal{E}[\![A]\!]$.
- If $(W, \rho) \in \mathcal{G}[\![\Gamma]\!]$ and $W \sqsubseteq W'$, then $(W', \rho) \in \mathcal{G}[\![\Gamma]\!]$.

Proof: The third statement is an easy corollary of the first statement. We focus on the first and the second statement. We prove these statements by mutual induction on A.

Case: Suppose $(W, v) \in \mathcal{V}[\![\texttt{int}]\!]$ and $W \sqsubseteq W'$ to show $(W', v) \in \mathcal{V}[\![\texttt{int}]\!]$. This case is immediate since worlds are irrelevant for $\mathcal{V}[\![\texttt{int}]\!]$.

Case: Suppose $(W, v) \in \mathcal{V}[\![A \to B]\!]$ and $W \sqsubseteq W'$ to show $(W', v) \in \mathcal{V}[\![A \to B]\!]$.

From $(W, v) \in \mathcal{V}[\![A \to B]\!]$, we have $v = (\lambda x.e, \rho)$ for some x, e, ρ.

Suppose $W' \sqsubseteq W''$ and $(W'', v') \in \mathcal{V}[\![A]\!]$ to show $(W'', \rho[x \mapsto v'], e) \in \mathcal{E}[\![B]\!]$.

By instantiating $(W, (\lambda x.e, \rho)) \in \mathcal{V}[\![A \to B]\!]$ with $W \sqsubseteq W' \sqsubseteq W''$ and $(W'', v') \in \mathcal{V}[\![A]\!]$, we have $(W'', \rho[x \mapsto v'], e) \in \mathcal{E}[\![B]\!]$.

Case: Suppose $(W, v) \in \mathcal{V}[\![A \times B]\!]$ and $W \sqsubseteq W'$ to show $(W', v) \in \mathcal{V}[\![A \times B]\!]$. This case is immediate from induction hypothesis.

Case: Suppose $(W, v) \in \mathcal{V}[\![A + B]\!]$ and $W \sqsubseteq W'$ to show $(W', v) \in \mathcal{V}[\![A + B]\!]$. This case is immediate from induction hypothesis.

Case: Suppose $(W, v) \in \texttt{ref}\ \tau$ and $W \sqsubseteq W'$ to show $(W', v) \in \mathcal{V}[\![\texttt{ref}\ \tau]\!]$. This case is immediate since future world W' contains all invariants of the current world W.

Case: Suppose $(W, \rho, e) \in \mathcal{E}[\![A]\!]$ and $W \sqsubseteq W'$ to show $(W', \rho, e) \in \mathcal{E}[\![A]\!]$.

We further suppose $W' \sqsubseteq W''$, $\mathrm{wsat}(W'', h), h, \rho \vdash e \Downarrow r$ to show $\exists h_r, v_r, W_r.\ r = (h_r, v_r) \wedge W'' \sqsubseteq W_r \wedge \mathrm{wsat}(W_r, h_r) \wedge (W_r, v_r) \in \mathcal{V}[\![A]\!]$.

By instantiating $(W, \rho, e) \in \mathcal{E}[\![A]\!]$ with $W \sqsubseteq W' \sqsubseteq W''$, $\mathrm{wsat}(W'', h)$, $h, \rho \vdash e \Downarrow r$, we conclude. □

Compatibility lemmas

Variable

Lemma *(variable)*: If $x : A \in \Gamma$, then $\Gamma \vDash x : A$.

Proof: Suppose $x : A \in \Gamma$ and $(W, \rho) \in \mathcal{G}[\![\Gamma]\!]$ to show $(W, \rho, x) \in \mathcal{E}[\![A]\!]$.

We further suppose $W \sqsubseteq W'$, $\mathrm{wsat}(W', h)$ and $h, \rho \vdash x \Downarrow r$ to show $\exists h_r, v_r, W_r.\ r = (h_r, v_r) \wedge W' \sqsubseteq W_r \wedge \mathrm{wsat}(W_r, h_r) \wedge (W_r, v_r) \in \mathcal{V}[\![A]\!]$.

By instantiating $(W, \rho) \in \mathcal{G}[\![\Gamma]\!]$ with $x : A \in \Gamma$, we have $(W, \rho(x)) \in \mathcal{V}[\![A]\!]$.

By case analysis on the derivation of $h, \rho \vdash x \Downarrow r$, there are two cases to consider.

Case:

$$\frac{x \in \mathrm{dom}(\rho)}{h, \rho \vdash x \Downarrow (h, \rho(x))}$$

By monotonicity, $W \sqsubseteq W'$, and $(W, \rho(x)) \in \mathcal{V}[\![A]\!]$, we have $(W', \rho(x)) \in \mathcal{V}[\![A]\!]$.

Choose $h_r = h$, $v_r = \rho(x)$, $W_r = W'$ to conclude.

Case:

$$\frac{x \notin \mathrm{dom}(\rho)}{h, \rho \vdash x \Downarrow \texttt{err}}$$

$(W, \rho(x)) \in \mathcal{V}[\![A]\!]$ contradicts with $x \notin \mathrm{dom}(\rho)$. □

Integer

Lemma *(integer literal)*: $\Gamma \vDash n : \texttt{int}$.

Proof: Suppose $(W, \rho) \in \mathcal{G}[\![\Gamma]\!]$ to show $(W, \rho, n) \in \mathcal{E}[\![A]\!]$.

We further suppose $W \sqsubseteq W'$, $\mathrm{wsat}(W', h)$ and $h, \rho \vdash n \Downarrow r$ to show $\exists h_r, v_r, W_r.\ r = (h_r, v_r) \wedge W' \sqsubseteq W_r \wedge \mathrm{wsat}(W_r, h_r) \wedge (W_r, v_r) \in \mathcal{V}[\![\texttt{int}]\!]$.

By case analysis on the derivation of $h, \rho \vdash n \Downarrow r$, there is one case to consider.

Case:

$$\frac{}{h, \rho \vdash n \Downarrow (h, n)}$$

Choose $h_r = h$, $v_r = n$, $W_r = W'$ to conclude. □

Lemma *(negation)*: If $\Gamma \vDash e : \texttt{int}$, then $\Gamma \vDash -e : \texttt{int}$.

Proof: Suppose $\Gamma \vDash e : \texttt{int}$ and $(W, \rho) \in \mathcal{G}[\![\Gamma]\!]$ to show $(W, \rho, -e) \in \mathcal{E}[\![\texttt{int}]\!]$.

We further suppose $W \sqsubseteq W'$, $\text{wsat}(W', h)$ and $h, \rho \vdash -e \Downarrow r$ to show $\exists h_r, v_r, W_r.\ r = (h_r, v_r) \land W' \sqsubseteq W_r \land \text{wsat}(W_r, h_r) \land (W_r, v_r) \in \mathcal{V}[\![\texttt{int}]\!]$.

By instantiating $\Gamma \vDash e : \texttt{int}$ with $(W, \rho) \in \mathcal{G}[\![\Gamma]\!]$, we have $(W, \rho, e) \in \mathcal{E}[\![\texttt{int}]\!]$.

By case analysis on the derivation of $h, \rho \vdash -e \Downarrow r$, there are two cases to consider.

Case:

$$\frac{h, \rho \vdash e \Downarrow (h', n)}{h, \rho \vdash -e \Downarrow (h', -n)}$$

By instantiating $(W, \rho, e) \in \mathcal{E}[\![\texttt{int}]\!]$ with $W \sqsubseteq W'$, $\text{wsat}(W', h)$, and $h, \rho \vdash e \Downarrow (h', n)$, we have $W' \sqsubseteq W'' \land \text{wsat}(W'', h') \land (W'', n) \in \mathcal{V}[\![\texttt{int}]\!]$ for some W''.

Choose $h_r = h'$, $v_r = -n$, $W_r = W''$ to conclude.

Case:

$$\frac{h, \rho \vdash e \Downarrow \texttt{err}}{h, \rho \vdash -e \Downarrow \texttt{err}}$$

By instantiating $(W, \rho, e) \in \mathcal{E}[\![\texttt{int}]\!]$ with $W \sqsubseteq W'$, $\text{wsat}(W', h)$, and $h, \rho \vdash e \Downarrow \texttt{err}$, we conclude contradiction. □

Function

Lemma *(λ-abstraction)*: If $\Gamma, x : A \vDash e : B$, then $\Gamma \vDash \lambda x.e : A \to B$.

Proof: Suppose $\Gamma, x : A \vDash e : B$ and $(W, \rho) \in \mathcal{G}[\![\Gamma]\!]$ to show $(W, \rho, \lambda x.e) \in \mathcal{E}[\![A \to B]\!]$.

We further suppose $W \sqsubseteq W'$, $\text{wsat}(W', h)$ and $h, \rho \vdash \lambda x.e \Downarrow r$ to show $\exists h_r, v_r, W_r.\ r = (h_r, v_r) \land W' \sqsubseteq W_r \land \text{wsat}(W_r, h_r) \land (W_r, v_r) \in \mathcal{V}[\![A \to B]\!]$.

By case analysis on the derivation of $h, \rho \vdash \lambda x.e \Downarrow r$, there is one case to consider.

Case:

$$\frac{}{h, \rho \vdash \lambda x.e \Downarrow (h, (\lambda x.e, \rho))}$$

Choose $h_r = h, v_r = (\lambda x.e, \rho), W_r = W'$.

The only non-trivial proof obligation is $(W', (\lambda x.e, \rho)) \in \mathcal{V}[\![A \to B]\!]$.

Suppose $W' \sqsubseteq W''$ and $(W'', v) \in \mathcal{V}[\![A]\!]$ to show $(W'', \rho[x \mapsto v], e) \in \mathcal{E}[\![B]\!]$.

By monotonicity, $W \sqsubseteq W' \sqsubseteq W''$, and $(W, \rho) \in \mathcal{G}[\![\Gamma]\!]$, we have $(W'', \rho) \in \mathcal{G}[\![\Gamma]\!]$.

By adjoining $(W'', \rho) \in \mathcal{G}[\![\Gamma]\!]$ with $(W'', v) \in \mathcal{V}[\![A]\!]$, we have $(W'', \rho[x \mapsto v]) \in \mathcal{G}[\![\Gamma, x : A]\!]$.

By instantiating $\Gamma, x : A \vDash e : B$ with $(W'', \rho[x \mapsto v]) \in \mathcal{G}[\![\Gamma, x : A]\!]$, we conclude $(W'', \rho[x \mapsto v], e) \in \mathcal{E}[\![B]\!]$. □

Lemma *(application)*: If $\Gamma \vDash e_1 : A \to B$ and $\Gamma \vDash e_2 : A$, then $\Gamma \vDash e_1\ e_2 : B$.

Proof: Suppose $\Gamma \vDash e_1 : A \to B$ and $\Gamma \vDash e_2 : A$ and $(W, \rho) \in \mathcal{G}[\![\Gamma]\!]$ to show $(W, \rho, e_1\ e_2) \in \mathcal{E}[\![B]\!]$.

We further suppose $W \sqsubseteq W'$, $\mathrm{wsat}(W', h)$ and $h, \rho \vdash e_1\ e_2 \Downarrow r$ to show $\exists h_r, v_r, W_r.\ r = (h_r, v_r) \wedge W' \sqsubseteq W_r \wedge \mathrm{wsat}(W_r, h_r) \wedge (W_r, v_r) \in \mathcal{V}[\![B]\!]$.

By instantiating $\Gamma \vDash e_1 : A \to B$ with $(W, \rho) \in \mathcal{G}[\![\Gamma]\!]$, we have $(W, \rho, e_1) \in \mathcal{E}[\![A \to B]\!]$.

By instantiating $\Gamma \vDash e_2 : A$ with $(W, \rho) \in \mathcal{G}[\![\Gamma]\!]$, we have $(W, \rho, e_2) \in \mathcal{E}[\![A]\!]$.

By case analysis on the derivation of $h, \rho \vdash e_1\ e_2 \Downarrow r$, there are three cases to consider.

Case:

$$\frac{h, \rho \vdash e_1 \Downarrow \left(h', \left(\lambda x.e_f, \rho_f\right)\right) \qquad h', \rho \vdash e_2 \Downarrow (h'', v) \qquad h'', \rho_f[x \mapsto v] \vdash e_f \Downarrow r}{h, \rho \vdash e_1\ e_2 \Downarrow r}$$

By instantiating $(W, \rho, e_1) \in \mathcal{E}[\![A \to B]\!]$ with $W \sqsubseteq W'$, $\mathrm{wsat}(W', h)$, and $h, \rho \vdash e_1 \Downarrow \left(h', \left(\lambda x.e_f, \rho_f\right)\right)$, we have $W' \sqsubseteq W'' \wedge \mathrm{wsat}(W'', h') \wedge \left(W'', \left(\lambda x.e_f, \rho_f\right)\right) \in \mathcal{V}[\![A \to B]\!]$ for some W''.

By instantiating $(W, \rho, e_2) \in \mathcal{E}[\![A]\!]$ with $W \sqsubseteq W' \sqsubseteq W''$, $\mathrm{wsat}(W'', h')$, and $h', \rho \vdash e_2 \Downarrow (h'', v)$, we have $W'' \sqsubseteq W''' \wedge \mathrm{wsat}(W''', h'') \wedge (W''', v) \in \mathcal{V}[\![A]\!]$ for some W'''.

By instantiating $\left(W'', \left(\lambda x.e_f, \rho_f\right)\right) \in \mathcal{V}[\![A \to B]\!]$ with $W'' \sqsubseteq W'''$ and $(W''', v) \in \mathcal{V}[\![A]\!]$, we have $\left(W''', \rho_f[x \mapsto v], e_f\right) \in \mathcal{E}[\![B]\!]$.

By instantiating $\left(W''', \rho_f[x \mapsto v], e_f\right) \in \mathcal{E}[\![B]\!]$ with $W''' \sqsubseteq W'''$ and $\mathrm{wsat}(W''', h'')$, we have $r = (h''', v') \wedge W''' \sqsubseteq W'''' \wedge \mathrm{wsat}(W'''', h''') \wedge (W'''', v') \in \mathcal{V}[\![B]\!]$ for some h''', v', W''''.

Choose $h_r = h'''$, $v_r = v'$, $W_r = W''''$ to conclude.

Case:

$$\frac{h, \rho \vdash e_1 \Downarrow r_1 \qquad r_1 \notin \left\{\left(h', \left(\lambda x.e_f, \rho_f\right)\right) \mid h', x, e_f, \rho_f\right\}}{h, \rho \vdash e_1\ e_2 \Downarrow \texttt{err}}$$

By instantiating $(W, \rho, e_1) \in \mathcal{E}[\![A \to B]\!]$ with $W \sqsubseteq W'$, $\mathrm{wsat}(W', h)$, and $h, \rho \vdash e_1 \Downarrow r_1$, we conclude contradiction.

Case:

$$\frac{h, \rho \vdash e_1 \Downarrow \left(h', \left(\lambda x.e_f, \rho_f\right)\right) \qquad h', \rho \vdash e_2 \Downarrow \texttt{err}}{h, \rho \vdash e_1\ e_2 \Downarrow \texttt{err}}$$

By instantiating $(W, \rho, e_1) \in \mathcal{E}[\![A \to B]\!]$ with $W \sqsubseteq W'$, $\mathrm{wsat}(W', h)$, and $h, \rho \vdash e_1 \Downarrow \left(h', \left(\lambda x.e_f, \rho_f\right)\right)$, we have $W' \sqsubseteq W'' \wedge \mathrm{wsat}(W'', h') \wedge \left(W'', \left(\lambda x.e_f, \rho_f\right)\right) \in \mathcal{V}[\![A \to B]\!]$ for some W''.

By instantiating $(W, \rho, e_2) \in \mathcal{E}[\![A]\!]$ with $W \sqsubseteq W' \sqsubseteq W''$, $\mathrm{wsat}(W'', h')$, and $h', \rho \vdash e_2 \Downarrow \texttt{err}$, we conclude contradiction. □

Product

Lemma *(pair)*: If $\Gamma \vDash e_1 : A$ and $\Gamma \vDash e_2 : B$, then $\Gamma \vDash (e_1, e_2) : A \times B$.

Proof: Suppose $\Gamma \vDash e_1 : A$, $\Gamma \vDash e_2 : B$, and $(W, \rho) \in \mathcal{G}[\![\Gamma]\!]$ to show $(W, \rho, (e_1, e_2)) \in \mathcal{E}[\![A \times B]\!]$.

We further suppose $W \sqsubseteq W'$, $\mathrm{wsat}(W', h)$ and $h, \rho \vdash (e_1, e_2) \Downarrow r$ to show $\exists h_r, v_r, W_r.\ r = (h_r, v_r) \wedge W' \sqsubseteq W_r \wedge \mathrm{wsat}(W_r, h_r) \wedge (W_r, v_r) \in \mathcal{V}[\![A \times B]\!]$.

By instantiating $\Gamma \vDash e_1 : A$ with $(W, \rho) \in \mathcal{G}[\![\Gamma]\!]$, we have $(W, \rho, e_1) \in \mathcal{E}[\![A]\!]$.

By instantiating $\Gamma \vDash e_2 : B$ with $(W, \rho) \in \mathcal{G}[\![\Gamma]\!]$, we have $(W, \rho, e_2) \in \mathcal{E}[\![B]\!]$.

By case analysis on the derivation of $h, \rho \vdash (e_1, e_2) \Downarrow r$, there are three cases to consider.

Case:

$$\frac{h, \rho \vdash e_1 \Downarrow (h', v_1) \quad h', \rho \vdash e_2 \Downarrow (h'', v_2)}{h, \rho \vdash (e_1, e_2) \Downarrow (h'', (v_1, v_2))}$$

By instantiating $(W, \rho, e_1) \in \mathcal{E}[\![A]\!]$ with $W \sqsubseteq W'$, $\mathrm{wsat}(W', h)$, and $h, \rho \vdash e_1 \Downarrow (h', v_1)$, we have $W' \sqsubseteq W'' \land \mathrm{wsat}(W'', h') \land (W'', v_1) \in \mathcal{V}[\![A]\!]$ for some W''.

By instantiating $(W, \rho, e_2) \in \mathcal{E}[\![B]\!]$ with $W \sqsubseteq W' \sqsubseteq W''$, $\mathrm{wsat}(W'', h')$, and $h', \rho \vdash e_2 \Downarrow (h'', v_2)$, we have $W'' \sqsubseteq W''' \land \mathrm{wsat}(W''', h'') \land (W''', v_2) \in \mathcal{V}[\![B]\!]$ for some W'''.

Choose $h_r = h'', v_r = (v_1, v_2), W_r = W'''$.

The only non-trivial proof obligation is $(W''', (v_1, v_2)) \in \mathcal{V}[\![A \times B]\!]$.

By monotonicity, $W'' \sqsubseteq W'''$, and $(W'', v_1) \in \mathcal{V}[\![A]\!]$, we have $(W''', v_1) \in \mathcal{V}[\![A]\!]$

By combining $(W''', v_1) \in \mathcal{V}[\![A]\!]$ and $(W''', v_2) \in \mathcal{V}[\![B]\!]$, we conclude $(W''', (v_1, v_2)) \in \mathcal{V}[\![A \times B]\!]$.

Case:

$$\frac{h, \rho \vdash e_1 \Downarrow \texttt{err}}{h, \rho \vdash (e_1, e_2) \Downarrow \texttt{err}}$$

By instantiating $(W, \rho, e_1) \in \mathcal{E}[\![A]\!]$ with $W \sqsubseteq W'$, $\mathrm{wsat}(W', h)$, and $h, \rho \vdash e_1 \Downarrow \texttt{err}$, we conclude contradiction.

Case:

$$\frac{h, \rho \vdash e_1 \Downarrow (h', v_1) \quad h', \rho \vdash e_2 \Downarrow \texttt{err}}{h, \rho \vdash (e_1, e_2) \Downarrow \texttt{err}}$$

By instantiating $(W, \rho, e_1) \in \mathcal{E}[\![A]\!]$ with $W \sqsubseteq W'$, $\mathrm{wsat}(W', h)$, and $h, \rho \vdash e_1 \Downarrow (h', v_1)$, we have $W' \sqsubseteq W'' \land \mathrm{wsat}(W'', h') \land (W'', v_1) \in \mathcal{V}[\![A]\!]$ for some W''.

By instantiating $(W, \rho, e_2) \in \mathcal{E}[\![B]\!]$ with $W \sqsubseteq W' \sqsubseteq W''$, $\mathrm{wsat}(W'', h')$, and $h', \rho \vdash e_2 \Downarrow \texttt{err}$, we conclude contradiction.

□

Lemma *(fst)*: If $\Gamma \vDash e : A \times B$, then $\Gamma \vDash e\ \texttt{.fst} : A$.

Proof: Suppose $\Gamma \vDash e : A \times B$ and $(W, \rho) \in \mathcal{G}[\![\Gamma]\!]$ to show $(W, \rho, e\ \texttt{.fst}) \in \mathcal{E}[\![A]\!]$.

We further suppose $W \sqsubseteq W'$, $\mathrm{wsat}(W', h)$, and $h, \rho \vdash e\ \texttt{.fst} \Downarrow r$ to show $\exists h_r, v_r, W_r.\ r = (h_r, v_r) \land W' \sqsubseteq W_r \land \mathrm{wsat}(W_r, h_r) \land (W_r, v_r) \in \mathcal{V}[\![A]\!]$.

By instantiating $\Gamma \vDash e : A \times B$ with $(W, \rho) \in \mathcal{G}[\![\Gamma]\!]$, we have $(W, \rho, e) \in \mathcal{E}[\![A \times B]\!]$.

By case analysis on the derivation of $h, \rho \vdash e\ \texttt{.fst} \Downarrow r$, there two cases to consider.

Case:

$$\frac{h, \rho \vdash e \Downarrow (h', (v_1, v_2))}{h, \rho \vdash e\ \texttt{.fst} \Downarrow (h', v_1)}$$

By instantiating $(W, \rho, e) \in \mathcal{E}[\![A \times B]\!]$ with $W \sqsubseteq W'$, $\mathrm{wsat}(W', h)$, and $h, \rho \vdash e \Downarrow (h', (v_1, v_2))$, we have $W' \sqsubseteq W'' \wedge \mathrm{wsat}(W'', h') \wedge (W'', (v_1, v_2)) \in \mathcal{V}[\![A \times B]\!]$ for some W''.

By unfolding the definition of $(W'', (v_1, v_2)) \in \mathcal{V}[\![A \times B]\!]$, we have $(W'', v_1) \in \mathcal{V}[\![A]\!]$.

Choose $h_r = h', v_r = v_1, W_r = W''$ to conclude.

Case:

$$\frac{h, \rho \vdash e \Downarrow r_1 \quad r_1 \notin \{(h', (v_1, v_2)) \mid h', v_1, v_2\}}{h, \rho \vdash e\ \texttt{.fst} \Downarrow \texttt{err}}$$

By instantiating $(W, \rho, e) \in \mathcal{E}[\![A \times B]\!]$ with $W \sqsubseteq W'$, $\mathrm{wsat}(W', h)$, and $h, \rho \vdash e \Downarrow r_1$, we conclude contradiction. □

Lemma *(snd)*: If $\Gamma \vDash e : A \times B$, then $\Gamma \vDash e\ \texttt{.snd} : B$.

Proof: Suppose $\Gamma \vDash e : A \times B$ and $(W, \rho) \in \mathcal{G}[\![\Gamma]\!]$ to show $(W, \rho, e\ \texttt{.snd}) \in \mathcal{E}[\![B]\!]$.

We further suppose $W \sqsubseteq W'$, $\mathrm{wsat}(W', h)$, and $h, \rho \vdash e\ \texttt{.snd} \Downarrow r$ to show $\exists h_r, v_r, W_r.\ r = (h_r, v_r) \wedge W' \sqsubseteq W_r \wedge \mathrm{wsat}(W_r, h_r) \wedge (W_r, v_r) \in \mathcal{V}[\![B]\!]$.

By instantiating $\Gamma \vDash e : A \times B$ with $(W, \rho) \in \mathcal{G}[\![\Gamma]\!]$, we have $(W, \rho, e) \in \mathcal{E}[\![A \times B]\!]$.

By case analysis on the derivation of $h, \rho \vdash e\ \texttt{.snd} \Downarrow r$, there two cases to consider.

Case:

$$\frac{h, \rho \vdash e \Downarrow (h', (v_1, v_2))}{h, \rho \vdash e\ \texttt{.snd} \Downarrow (h', v_2)}$$

By instantiating $(W, \rho, e) \in \mathcal{E}[\![A \times B]\!]$ with $W \sqsubseteq W'$, $\mathrm{wsat}(W', h)$, and $h, \rho \vdash e \Downarrow (h', (v_1, v_2))$, we have $W' \sqsubseteq W'' \wedge \mathrm{wsat}(W'', h') \wedge (W'', (v_1, v_2)) \in \mathcal{V}[\![A \times B]\!]$ for some W''.

By unfolding the definition of $(W'', (v_1, v_2)) \in \mathcal{V}[\![A \times B]\!]$, we have $(W'', v_2) \in \mathcal{V}[\![B]\!]$.

Choose $h_r = h', v_r = v_2, W_r = W''$ to conclude.

Case:

$$\frac{h, \rho \vdash e \Downarrow r_1 \quad r_1 \notin \{(h', (v_1, v_2)) \mid h', v_1, v_2\}}{h, \rho \vdash e\ \texttt{.snd} \Downarrow \texttt{err}}$$

By instantiating $(W, \rho, e) \in \mathcal{E}[\![A \times B]\!]$ with $W \sqsubseteq W'$, $\mathrm{wsat}(W', h)$, and $h, \rho \vdash e \Downarrow r_1$, we conclude contradiction. □

Sum

Lemma *(inl)*: If $\Gamma \vDash e : A$, then $\Gamma \vDash \texttt{inl.}\ e : A + B$.

Proof: Suppose $\Gamma \vDash e : A$ and $(W, \rho) \in \mathcal{G}[\![\Gamma]\!]$ to show $(W, \rho, \texttt{inl.}\ e) \in \mathcal{E}[\![A + B]\!]$.

We further suppose $W \sqsubseteq W'$, $\mathrm{wsat}(W', h)$ and $h, \rho \vdash \texttt{inl.}\ e \Downarrow r$ to show $\exists h_r, v_r, W_r.\ r = (h_r, v_r) \wedge W' \sqsubseteq W_r \wedge \mathrm{wsat}(W_r, h_r) \wedge (W_r, v_r) \in \mathcal{V}[\![A + B]\!]$.

By instantiating $\Gamma \vDash e : A$ with $(W, \rho) \in \mathcal{G}[\![\Gamma]\!]$, we have $(W, \rho, e) \in \mathcal{E}[\![A]\!]$.

By case analysis on the derivation of $h, \rho \vdash \texttt{inl.}\ e \Downarrow r$, there are two cases to consider.

Case:

$$\frac{h, \rho \vdash e \Downarrow (h', v)}{h, \rho \vdash \texttt{inl.}\ e \Downarrow (h', \texttt{inl.}\ v)}$$

By instantiating $(W, \rho, e) \in \mathcal{E}[\![A]\!]$ with $W \sqsubseteq W'$, $\text{wsat}(W', h)$, and $h, \rho \vdash e \Downarrow (h', v)$, we have $W' \sqsubseteq W'' \land \text{wsat}(W'', h') \land (W'', v) \in \mathcal{V}[\![A]\!]$ for some W''.

From $(W'', v) \in \mathcal{V}[\![A]\!]$, we have $(W'', \texttt{inl.}\ v) \in \mathcal{V}[\![A + B]\!]$.

Choose $h_r = h', v_r = \texttt{inl.}\ v, W_r = W''$ to conclude.

Case:

$$\frac{h, \rho \vdash e \Downarrow \texttt{err}}{h, \rho \vdash \texttt{inl.}\ e \Downarrow \texttt{err}}$$

By instantiating $(W, \rho, e) \in \mathcal{E}[\![A]\!]$ with $W \sqsubseteq W'$, $\text{wsat}(W', h)$, and $h, \rho \vdash e \Downarrow \texttt{err}$, we conclude contradiction. □

Lemma *(inr)*: If $\Gamma \vDash e : B$, then $\Gamma \vDash \texttt{inr.}\ e : A + B$.

Proof: Suppose $\Gamma \vDash e : B$ and $(W, \rho) \in \mathcal{G}[\![\Gamma]\!]$ to show $(W, \rho, \texttt{inr.}\ e) \in \mathcal{E}[\![A + B]\!]$.

We further suppose $W \sqsubseteq W'$, $\text{wsat}(W', h)$ and $h, \rho \vdash \texttt{inr.}\ e \Downarrow r$ to show $\exists h_r, v_r, W_r.\ r = (h_r, v_r) \land W' \sqsubseteq W_r \land \text{wsat}(W_r, h_r) \land (W_r, v_r) \in \mathcal{V}[\![A + B]\!]$.

By instantiating $\Gamma \vDash e : B$ with $(W, \rho) \in \mathcal{G}[\![\Gamma]\!]$, we have $(W, \rho, e) \in \mathcal{E}[\![B]\!]$.

By case analysis on the derivation of $h, \rho \vdash \texttt{inr.}\ e \Downarrow r$, there are two cases to consider.

Case:

$$\frac{h, \rho \vdash e \Downarrow (h', v)}{h, \rho \vdash \texttt{inr.}\ e \Downarrow (h', \texttt{inr.}\ v)}$$

By instantiating $(W, \rho, e) \in \mathcal{E}[\![B]\!]$ with $W \sqsubseteq W'$, $\text{wsat}(W', h)$, and $h, \rho \vdash e \Downarrow (h', v)$, we have $W' \sqsubseteq W'' \land \text{wsat}(W'', h') \land (W'', v) \in \mathcal{V}[\![B]\!]$ for some W''.

From $(W'', v) \in \mathcal{V}[\![B]\!]$, we have $(W'', \texttt{inr.}\ v) \in \mathcal{V}[\![A + B]\!]$.

Choose $h_r = h', v_r = \texttt{inr.}\ v, W_r = W''$ to conclude.

Case:

$$\frac{h, \rho \vdash e \Downarrow \texttt{err}}{h, \rho \vdash \texttt{inr.}\ e \Downarrow \texttt{err}}$$

By instantiating $(W, \rho, e) \in \mathcal{E}[\![B]\!]$ with $W \sqsubseteq W'$, $\text{wsat}(W', h)$, and $h, \rho \vdash e \Downarrow \texttt{err}$, we conclude contradiction. □

Lemma *(case)*: If $\Gamma \vDash e_0 : A + B$ and $\Gamma, x : A \vDash e_1 : C$, and $\Gamma, y : B \vDash e_2 : C$, then $\Gamma \vDash \texttt{case}(e_0, x.e_1, y.e_2) : C$.

Proof: Suppose $\Gamma \vDash e_0 : A + B$ and $\Gamma, x : A \vDash e_1 : C$ and $\Gamma, y : B \vDash e_2 : C$, and $(W, \rho) \in \mathcal{G}[\![\Gamma]\!]$ to show $(W, \rho, \texttt{case}(e_0, x.e_1, y.e_2)) \in \mathcal{E}[\![C]\!]$.

We further suppose $W \sqsubseteq W'$, $\text{wsat}(W', h)$, and $h, \rho \vdash \texttt{case}(e_0, x.e_1, y.e_2) \Downarrow r$ to show $\exists h_r, v_r, W_r.\ r = (h_r, v_r) \land W' \sqsubseteq W_r \land \text{wsat}(W_r, h_r) \land (W_r, v_r) \in \mathcal{V}[\![C]\!]$.

By instantiating $\Gamma \vDash e_0 : A + B$ with $(W, \rho) \in \mathcal{G}[\![\Gamma]\!]$, we have $(W, \rho, e_0) \in \mathcal{E}[\![A + B]\!]$.

By case analysis on the derivation of $h, \rho \vdash \texttt{case}(e_0, x.e_1, y.e_2) \Downarrow r$, there are three cases to consider.

Case:

$$\frac{h, \rho \vdash e_0 \Downarrow (h', \texttt{inl.}\ v) \quad h', \rho[x \mapsto v] \vdash e_1 \Downarrow r}{h, \rho \vdash \texttt{case}(e_0, x.e_1, y.e_2) \Downarrow r}$$

By instantiating $(W, \rho, e_0) \in \mathcal{E}[\![A + B]\!]$ with $W \sqsubseteq W'$, $\mathrm{wsat}(W', h)$, and $h, \rho \vdash e_0 \Downarrow \texttt{inl.}\ v$, we have $W' \sqsubseteq W'' \wedge \mathrm{wsat}(W'', h') \wedge (W'', \texttt{inl.}\ v) \in \mathcal{V}[\![A + B]\!]$ for some W''.

From $(W'', \texttt{inl.}\ v) \in \mathcal{V}[\![A + B]\!]$, we have $(W'', v) \in \mathcal{V}[\![A]\!]$.

By monotonicity, $W \sqsubseteq W' \sqsubseteq W''$, and $(W, \rho) \in \mathcal{G}[\![\Gamma]\!]$, we have $(W'', \rho) \in \mathcal{G}[\![\Gamma]\!]$.

By adjoining $(W'', \rho) \in \mathcal{G}[\![\Gamma]\!]$ with $(W'', v) \in \mathcal{V}[\![A]\!]$, we have $(W'', \rho[x \mapsto v]) \in \mathcal{G}[\![\Gamma, x : A]\!]$.

By instantiating $\Gamma, x : A \vDash e_1 : C$ with $(W'', \rho[x \mapsto v]) \in \mathcal{G}[\![\Gamma, x : A]\!]$, we have $(W'', \rho[x \mapsto v], e_1) \in \mathcal{E}[\![C]\!]$.

By instantiating $(W'', \rho[x \mapsto v], e_1) \in \mathcal{E}[\![C]\!]$ with $W'' \sqsubseteq W''$, $\mathrm{wsat}(W'', h')$, and $h', \rho[x \mapsto v] \vdash e_1 \Downarrow r$, we have $r = (h'', v') \wedge W'' \sqsubseteq W''' \wedge \mathrm{wsat}(W''', h'') \wedge (W''', v') \in \mathcal{V}[\![C]\!]$ for some h'', v', W'''.

Choose $h_r = h'', v_r = v', W_r = W'''$ to conclude.

Case:

$$\frac{h, \rho \vdash e_0 \Downarrow (h', \texttt{inr.}\ v) \quad h', \rho[y \mapsto v] \vdash e_2 \Downarrow r}{h, \rho \vdash \texttt{case}(e_0, x.e_1, y.e_2) \Downarrow r}$$

By instantiating $(W, \rho, e_0) \in \mathcal{E}[\![A + B]\!]$ with $W \sqsubseteq W'$, $\mathrm{wsat}(W', h)$, and $h, \rho \vdash e_0 \Downarrow \texttt{inr.}\ v$, we have $W' \sqsubseteq W'' \wedge \mathrm{wsat}(W'', h') \wedge (W'', \texttt{inr.}\ v) \in \mathcal{V}[\![A + B]\!]$ for some W''.

From $(W'', \texttt{inr.}\ v) \in \mathcal{V}[\![A + B]\!]$, we have $(W'', v) \in \mathcal{V}[\![B]\!]$.

By monotonicity, $W \sqsubseteq W' \sqsubseteq W''$, and $(W, \rho) \in \mathcal{G}[\![\Gamma]\!]$, we have $(W'', \rho) \in \mathcal{G}[\![\Gamma]\!]$.

By adjoining $(W'', \rho) \in \mathcal{G}[\![\Gamma]\!]$ with $(W'', v) \in \mathcal{V}[\![B]\!]$, we have $(W'', \rho[y \mapsto v]) \in \mathcal{G}[\![\Gamma, y : B]\!]$.

By instantiating $\Gamma, y : B \vDash e_2 : C$ with $(W'', \rho[y \mapsto v]) \in \mathcal{G}[\![\Gamma, y : B]\!]$, we have $(W'', \rho[y \mapsto v], e_2) \in \mathcal{E}[\![C]\!]$.

By instantiating $(W'', \rho[y \mapsto v], e_2) \in \mathcal{E}[\![C]\!]$ with $W'' \sqsubseteq W''$, $\mathrm{wsat}(W'', h')$, and $h', \rho[y \mapsto v] \vdash e_2 \Downarrow r$, we have $r = (h'', v') \wedge W'' \sqsubseteq W''' \wedge \mathrm{wsat}(W''', h'') \wedge (W''', v') \in \mathcal{V}[\![C]\!]$ for some h'', v', W'''.

Choose $h_r = h'', v_r = v', W_r = W'''$ to conclude.

Case:

$$\frac{h, \rho \vdash e_0 \Downarrow r_0 \quad r_0 \notin \{(h', \texttt{inl.}\ v) \mid h', v\} \cup \{(h', \texttt{inr.}\ v) \mid h', v\}}{h, \rho \vdash \texttt{case}(e_0, x.e_1, y.e_2) \Downarrow \texttt{err}}$$

By instantiating $(W, \rho, e_0) \in \mathcal{E}[\![A + B]\!]$ with $W \sqsubseteq W'$, $\mathrm{wsat}(W', h)$, and $h, \rho \vdash e_0 \Downarrow r_0$, we conclude contradiction. □

Reference

Lemma *(new)*: If $\Gamma \vDash e : \tau$, then $\Gamma \vDash \texttt{new}\ e : \texttt{ref}\ \tau$.

Proof: Suppose $\Gamma \vDash e : \tau$ and $(W, \rho) \in \mathcal{G}[\![\Gamma]\!]$ to show $(W, \rho, \texttt{new}\ e) \in \mathcal{E}[\![\texttt{ref}\ \tau]\!]$.

We further suppose $W \sqsubseteq W', \mathrm{wsat}(W', h), h, \rho \vdash \texttt{new}\ e \Downarrow r$ to show $\exists h_r, v_r, W_r.\ r = (h_r, v_r) \wedge W' \sqsubseteq W_r \wedge \mathrm{wsat}(W_r, h_r) \wedge (W_r, v_r) \in \mathcal{V}[\![\texttt{ref}\ \tau]\!]$.

By instantiating $\Gamma \vDash e : \tau$ with $(W, \rho) \in \mathcal{G}[\![\Gamma]\!]$, we have $(W, \rho, e) \in \mathcal{E}[\![\tau]\!]$.

By case analysis on the derivation of $h, \rho \vdash \texttt{new}\ e \Downarrow r$, there are two cases to consider.

Case:

$$\frac{h, \rho \vdash e \Downarrow (h', v) \qquad \ell \notin \mathrm{dom}(h')}{h, \rho \vdash \texttt{new}\ e \Downarrow (h'[\ell \mapsto v], \ell)}$$

By instantiating $(W, \rho, e) \in \mathcal{E}[\![\tau]\!]$ with $W \sqsubseteq W'$, $\mathrm{wsat}(W', h)$, and $h, \rho \vdash e \Downarrow (h', v)$, we have $W' \sqsubseteq W'' \wedge \mathrm{wsat}(W'', h') \wedge (W'', v) \in \mathcal{V}[\![\tau]\!]$ for some W''.

From $(W'', v) \in \mathcal{V}[\![\tau]\!]$, we have $\vdash v : \tau$.

From $\ell \notin \mathrm{dom}(h')$ and $\mathrm{wsat}(W'', h')$, we have $\ell \notin \mathrm{dom}(W'')$

Let $W''' := W''[\ell \mapsto \{v \mid \vdash v : \tau\}]$.

Since we allocated to a fresh location, we have $W'' \sqsubseteq W'''$.

By combining $\mathrm{wsat}(W'', h')$ and $\vdash v : \tau$, we have $\mathrm{wsat}(W''', h'[\ell \mapsto v])$.

From the definition of value relation, we have $(W''', \ell) \in \mathcal{V}[\![\texttt{ref}\ \tau]\!]$.

Choose $h_r = h'[\ell \mapsto v], v_r = \ell, W_r = W'''$ to conclude.

Case:

$$\frac{h, \rho \vdash e \Downarrow \texttt{err}}{h, \rho \vdash \texttt{new}\ e \Downarrow \texttt{err}}$$

By instantiating $(W, \rho, e) \in \mathcal{E}[\![\tau]\!]$ with $W \sqsubseteq W'$, $\mathrm{wsat}(W', h)$, and $h, \rho \vdash e \Downarrow \texttt{err}$, we conclude contradiction. □

Lemma *(load)*: If $\Gamma \vDash e : \texttt{ref}\ \tau$, then $\Gamma \vDash\ !\,e : \tau$.

Proof: Suppose $\Gamma \vDash e : \texttt{ref}\ \tau$ and $(W, \rho) \in \mathcal{G}[\![\Gamma]\!]$ to show $(W, \rho, !\,e) \in \mathcal{E}[\![\tau]\!]$.

We further suppose $W \sqsubseteq W', \mathrm{wsat}(W', h), h, \rho \vdash\ !\,e \Downarrow r$ to show $\exists h_r, v_r, W_r.\ r = (h_r, v_r) \wedge W' \sqsubseteq W_r \wedge \mathrm{wsat}(W_r, h_r) \wedge (W_r, v_r) \in \mathcal{V}[\![\tau]\!]$.

By instantiating $\Gamma \vDash e : \texttt{ref}\ \tau$ with $(W, \rho) \in \mathcal{G}[\![\Gamma]\!]$, we have $(W, \rho, e) \in \mathcal{E}[\![\texttt{ref}\ \tau]\!]$.

By case analysis on the derivation of $h, \rho \vdash\ !\,e \Downarrow r$, there are two cases to consider.

Case:

$$\frac{h, \rho \vdash e \Downarrow (h', \ell) \qquad \ell \in \mathrm{dom}(h')}{h, \rho \vdash\ !\,e \Downarrow (h', h'(\ell))}$$

By instantiating $(W, \rho, e) \in \mathcal{E}[\![\texttt{ref}\ \tau]\!]$ with $W \sqsubseteq W', \mathrm{wsat}(W', h), h, \rho \vdash e \Downarrow (h', \ell)$, we have $W' \sqsubseteq W'', \mathrm{wsat}(W'', h'), (W'', \ell) \in \mathcal{V}[\![\texttt{ref}\ \tau]\!]$ for some W''.

From $(W'', \ell) \in \mathcal{V}[\![\texttt{ref}\ \tau]\!]$, we have $W''(\ell) = \{v \mid \vdash v : \tau\}$.

By instantiating $\mathrm{wsat}(W'', h')$ with $W''(\ell) = \{v \mid \vdash v : \tau\}$, we have $\vdash h'(\ell) : \tau$.

Then we have $(W'', h'(\ell)) \in \mathcal{V}[\![\tau]\!]$.

Choose $h_r = h', v_r = h'(\ell), W_r = W''$ to conclude.

Case:

$$\frac{h, \rho \vdash e \Downarrow r_1 \qquad r \notin \{(h', \ell) \mid \ell \in \mathrm{dom}(h')\}}{h, \rho \vdash \,!\,e \Downarrow \texttt{err}}$$

By instantiating $(W, \rho, e) \in \mathcal{E}[\![\texttt{ref}\ \tau]\!]$ with $W \sqsubseteq W'$, $\mathrm{wsat}(W', h)$, $h, \rho \vdash e \Downarrow r_1$, we conclude contradiction. □

Lemma *(store)*: If $\Gamma \vDash e_1 : \texttt{ref}\ \tau$ and $\Gamma \vDash e_2 : \tau$, then $\Gamma \vDash e_1 \leftarrow e_2 : \tau$.

Proof: Suppose $\Gamma \vDash e_1 : \texttt{ref}\ \tau$, $\Gamma \vDash e_2 : \tau$, and $(W, \rho) \in \mathcal{G}[\![\Gamma]\!]$ to show $(W, \rho, e_1 \leftarrow e_2) \in \mathcal{E}[\![\tau]\!]$.

We further suppose $W \sqsubseteq W'$, $\mathrm{wsat}(W', h)$, $h, \rho \vdash e_1 \leftarrow e_2 \Downarrow r$ to show $\exists h_r, v_r, W_r.\ r = (h_r, v_r) \land W' \sqsubseteq W_r \land \mathrm{wsat}(W_r, h_r) \land (W_r, v_r) \in \mathcal{V}[\![\tau]\!]$.

By instantiating $\Gamma \vDash e_1 : \texttt{ref}\ \tau$ with $(W, \rho) \in \mathcal{G}[\![\Gamma]\!]$, we have $(W, \rho, e_1) \in \mathcal{E}[\![\texttt{ref}\ \tau]\!]$.

By instantiating $\Gamma \vDash e_2 : \tau$ with $(W, \rho) \in \mathcal{G}[\![\Gamma]\!]$, we have $(W, \rho, e_2) \in \mathcal{E}[\![\tau]\!]$.

By case analysis on the derivation of $h, \rho \vdash e_1 \leftarrow e_2 \Downarrow r$, there are three cases to consider.

Case:

$$\frac{h, \rho \vdash e_1 \Downarrow (h', \ell) \qquad h', \rho \vdash e_2 \Downarrow (h'', v)}{h, \rho \vdash e_1 \leftarrow e_2 \Downarrow (h''[\ell \mapsto v], v)}$$

By instantiating $(W, \rho, e_1) \in \mathcal{E}[\![\texttt{ref}\ \tau]\!]$ with $W \sqsubseteq W'$, $\mathrm{wsat}(W', h)$, and $h, \rho \vdash e_1 \Downarrow (h', \ell)$, we have $W' \sqsubseteq W''$, $\mathrm{wsat}(W'', h')$, $(W'', \ell) \in \mathcal{V}[\![\texttt{ref}\ \tau]\!]$ for some W''.

By instantiating $(W, \rho, e_2) \in \mathcal{E}[\![\tau]\!]$ with $W \sqsubseteq W' \sqsubseteq W''$, $\mathrm{wsat}(W'', h')$, and $h', \rho \vdash e_2 \Downarrow (h'', v)$, we have $W'' \sqsubseteq W'''$, $\mathrm{wsat}(W''', h'')$, $(W''', v) \in \mathcal{V}[\![\tau]\!]$ for some W'''.

From $(W''', v) \in \mathcal{V}[\![\tau]\!]$, we have $\vdash v : \tau$.

By monotonicity, $W'' \sqsubseteq W'''$, and $(W'', \ell) \in \mathcal{V}[\![\texttt{ref}\ \tau]\!]$, we have $(W''', \ell) \in \mathcal{V}[\![\texttt{ref}\ \tau]\!]$.

From $(W''', \ell) \in \mathcal{V}[\![\texttt{ref}\ \tau]\!]$, we have $W'''(\ell) = \{v \mid \vdash v : \tau\}$.

By combining $\mathrm{wsat}(W''', h'')$, $W'''(\ell) = \{v \mid \vdash v : \tau\}$, and $\vdash v : \tau$, we have $\mathrm{wsat}(W''', h''[\ell \mapsto v])$.

Choose $h_r = h''[\ell \mapsto v]$, $v_r = v$, $W_r = W'''$ to conclude.

Case:

$$\frac{h, \rho \vdash e_1 \Downarrow r_1 \qquad r_1 \notin \{(h', \ell) \mid h', \ell\}}{h, \rho \vdash e_1 \leftarrow e_2 \Downarrow \texttt{err}}$$

By instantiating $(W, \rho, e_1) \in \mathcal{E}[\![\texttt{ref}\ \tau]\!]$ with $W \sqsubseteq W'$, $\mathrm{wsat}(W', h)$, and $h, \rho \vdash e_1 \Downarrow r_1$, we conclude contradiction.

Case:

$$\frac{h, \rho \vdash e_1 \Downarrow (h', \ell) \qquad h', \rho \vdash e_2 \Downarrow \texttt{err}}{h, \rho \vdash e_1 \leftarrow e_2 \Downarrow \texttt{err}}$$

By instantiating $(W, \rho, e_1) \in \mathcal{E}[\![\texttt{ref}\ \tau]\!]$ with $W \sqsubseteq W'$, $\mathrm{wsat}(W', h)$, and $h, \rho \vdash e_1 \Downarrow (h', \ell)$, we have $W' \sqsubseteq W''$, $\mathrm{wsat}(W'', h')$, $(W'', \ell) \in \mathcal{V}[\![\texttt{ref}\ \tau]\!]$ for some W''.

By instantiating $(W, \rho, e_2) \in \mathcal{E}[\![\tau]\!]$ with $W \sqsubseteq W' \sqsubseteq W''$, $\mathrm{wsat}(W'', h')$, and $h', \rho \vdash e_2 \Downarrow \texttt{err}$, we conclude contradiction. □

Fundamental theorem and safety

Theorem *(Fundamental theorem of logical relation)*: If $\Gamma \vdash e : A$, then $\Gamma \vDash e : A$

Proof: The proof is by induction on the typing derivation. For each case, apply the matching compatibility lemma. □

Theorem *(Adequacy)*: If $\vDash e : A$ and $\emptyset, \emptyset \vdash e \Downarrow r$, then there are W, h, and v such that $r = (h, v)$, $\mathrm{wsat}(W, h)$, and $(W, v) \in \mathcal{V}[\![A]\!]$.

Proof: Immediate from the definition of semantic typing and expression relation. □

Theorem *(Safety)*: If $\vdash e : A$ and $\emptyset, \emptyset \vdash e \Downarrow r$, then there are W, h, and v such that $r = (h, v)$, $\mathrm{wsat}(W, h)$, and $(W, v) \in \mathcal{V}[\![A]\!]$.

Proof: Corollary of the fundamental theorem and adequacy. □

Bibliography

Dreyer, Derek, Simon Spies, Lennard Gäher, Ralf Jung, Jan-Oliver Kaiser, Hoang-Hai Dang, David Swasey, and Jan Menz. 2022. *Semantics of Type Systems Lecture Notes*. https://plv.mpi-sws.org/semantics-course/.

Hur, Chung-Kil, Derek Dreyer, Georg Neis, and Viktor Vafeiadis. 2012. “The Marriage of Bisimulations and Kripke Logical Relations”. In *Proceedings of the 39th Annual ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages*, 59–72. POPL '12. Philadelphia, PA, USA: Association for Computing Machinery. https://doi.org/10.1145/2103656.2103666.