Modular Analysis

Joonhyup Lee

April 5, 2024

1 Syntax and Semantics

1.1 Abstract Syntax

$$
\begin{array}{rcll}
\text{Identifiers} & x & \in & \text{Var} \\
\text{Expression} & e & \rightarrow & x \mid \lambda x.e \mid e\ e & \lambda\text{-calculus} \\
& & \mid & e \rtimes e & \text{linked expression} \\
& & \mid & \varepsilon & \text{empty module} \\
& & \mid & x = e\ ;\ e & \text{(recursive) binding}
\end{array}
$$

Figure 1: Abstract syntax of the language.

1.2 Operational Semantics

$$
\begin{array}{rcll}
\text{Environment} & \sigma & \in & \text{Env} \\
\text{Location} & \ell & \in & \text{Loc} \\
\text{de Bruijn Index} & n & \in & \mathbb{N} \\
\text{Value} & v & \in & \text{Val} \triangleq \text{Env} + \text{Var} \times \text{Expr} \times \text{Env} \\
\text{Weak Value} & w & \in & \text{WVal} \triangleq \text{Val} + \underline{\text{Val}} \\
\text{Environment} & \sigma & \rightarrow & \bullet & \text{empty stack} \\
& & \mid & (x, w) :: \sigma & \text{weak value binding} \\
& & \mid & (x, \ell) :: \sigma & \text{free location binding} \\
& & \mid & (x, n) :: \sigma & \text{bound location binding} \\
\text{Value} & v & \rightarrow & \sigma & \text{exported environment} \\
& & \mid & \langle \lambda x.e, \sigma \rangle & \text{closure} \\
\text{Weak Value} & w & \rightarrow & v & \text{value} \\
& & \mid & \mu.v & \text{recursive value}
\end{array}
$$

Figure 2: Definition of the semantic domains.

$$\boxed{\sigma \vdash e \Downarrow v}$$

$$
\textsc{Id}\ \frac{\sigma(x) = v}{\sigma \vdash x \Downarrow v}
\qquad
\textsc{RecId}\ \frac{\sigma(x) = \mu.v}{\sigma \vdash x \Downarrow v^{\mu.v}}
\qquad
\textsc{Fn}\ \frac{}{\sigma \vdash \lambda x.e \Downarrow \langle \lambda x.e, \sigma \rangle}
\qquad
\textsc{App}\ \frac{\sigma \vdash e_1 \Downarrow \langle \lambda x.e, \sigma_1 \rangle \quad \sigma \vdash e_2 \Downarrow v_2 \quad (x, v_2) :: \sigma_1 \vdash e \Downarrow v}{\sigma \vdash e_1\ e_2 \Downarrow v}
$$

$$
\textsc{Link}\ \frac{\sigma \vdash e_1 \Downarrow \sigma_1 \quad \sigma_1 \vdash e_2 \Downarrow v}{\sigma \vdash e_1 \rtimes e_2 \Downarrow v}
\qquad
\textsc{Empty}\ \frac{}{\sigma \vdash \varepsilon \Downarrow \bullet}
\qquad
\textsc{Bind}\ \frac{\ell \notin \text{FLoc}(\sigma) \quad (x, \ell) :: \sigma \vdash e_1 \Downarrow v_1 \quad (x, \mu.\setminus^{\ell} v_1) :: \sigma \vdash e_1 \Downarrow \sigma_2}{\sigma \vdash x = e_1 ; e_2 \Downarrow (x, \mu.\setminus^{\ell} v_1) :: \sigma_2}
$$

Figure 3: The big-step operational semantics.

We use the locally nameless representation, and enforce that all values be *locally closed*. As a consequence, the big-step operational semantics will be *deterministic*, no matter what ℓ is chosen in the Bind rule.

1.3 Reconciling with Conventional Backpatching

$$
\begin{array}{rcll}
\text{Environment} & \sigma & \in & \text{MEnv} \triangleq \text{Var} \xrightarrow{\text{fin}} \text{Loc} \\
\text{Memory} & m & \in & \text{Mem} \triangleq \text{Loc} \xrightarrow{\text{fin}} \text{MVal} \\
\text{Allocated set} & L & \subseteq & \text{Loc} \\
\text{Value} & v & \in & \text{MVal} \triangleq \text{MEnv} + \text{Var} \times \text{Expr} \times \text{MEnv} \\
\text{Environment} & \sigma & \to & \bullet & \text{empty stack} \\
& & \mid & (x, \ell) :: \sigma & \text{location binding} \\
\text{Value} & v & \to & \sigma & \text{exported environment} \\
& & \mid & \langle \lambda x.e, \sigma \rangle & \text{closure}
\end{array}
$$

Figure 4: Definition of the semantic domains with memory.

$$\boxed{\sigma, m, L \vdash e \Downarrow v, m', L'}$$

$$
\textsc{Id}\ \frac{\sigma(x) = \ell \qquad m(\ell) = v}{\sigma, m, L \vdash x \Downarrow v, m, L}
\qquad
\textsc{Fn}\ \frac{}{\sigma, m, L \vdash \lambda x.e \Downarrow \langle \lambda x.e, \sigma \rangle, m, L}
$$

$$
\textsc{App}\ \frac{\begin{array}{c}\sigma, m, L \vdash e_1 \Downarrow \langle \lambda x.e, \sigma_1 \rangle, m_1, L_1 \qquad \sigma, m_1, L_1 \vdash e_2 \Downarrow v_2, m_2, L_2 \qquad \ell \notin \text{dom}(m_2) \cup L_2 \\ (x, \ell) :: \sigma_1, m_2[\ell \mapsto v_2], L_2 \vdash e \Downarrow v, m', L'\end{array}}{\sigma, m, L \vdash e_1\ e_2 \Downarrow v, m', L'}
$$

$$
\textsc{Link}\ \frac{\sigma, m, L \vdash e_1 \Downarrow \sigma_1, m_1, L_1 \qquad \sigma_1, m_1, L_1 \vdash e_2 \Downarrow v, m', L'}{\sigma, m, L \vdash e_1 \rtimes e_2 \Downarrow v, m', L'}
\qquad
\textsc{Empty}\ \frac{}{\sigma, m, L \vdash \varepsilon \Downarrow \bullet, m, L}
$$

$$
\textsc{Bind}\ \frac{\begin{array}{c}\ell \notin \text{dom}(m) \cup L \qquad (x, \ell) :: \sigma, m, L \cup \{\ell\} \vdash e_1 \Downarrow v_1, m_1, L_1 \\ (x, \ell) :: \sigma, m_1[\ell \mapsto v_1], L_1 \vdash e_2 \Downarrow \sigma_2, m', L'\end{array}}{\sigma, m, L \vdash x = e_1; e_2 \Downarrow (x, \ell) :: \sigma_2, m', L'}
$$

Figure 5: The big-step operational semantics with memory.

$$\boxed{w \sim_f v, m}$$

$$
\textsc{Eq-Nil}\ \frac{}{\bullet \sim_f \bullet}
\qquad
\textsc{Eq-ConsFree}\ \frac{\ell \notin \text{dom}(f) \qquad \ell \notin \text{dom}(m) \qquad \sigma \sim_f \sigma'}{(x, \ell) :: \sigma \sim_f (x, \ell) :: \sigma'}
\qquad
\textsc{Eq-ConsBound}\ \frac{f(\ell) = \ell' \qquad \ell' \in \text{dom}(m) \qquad \sigma \sim_f \sigma'}{(x, \ell) :: \sigma \sim_f (x, \ell') :: \sigma'}
$$

$$
\textsc{Eq-ConsWVal}\ \frac{m(\ell') = v' \qquad w \sim_f v' \qquad \sigma \sim_f \sigma'}{(x, w) :: \sigma \sim_f (x, \ell') :: \sigma'}
\qquad
\textsc{Eq-Clos}\ \frac{\sigma \sim_f \sigma'}{\langle \lambda x.e, \sigma \rangle \sim_f \langle \lambda x.e, \sigma' \rangle}
\qquad
\textsc{Eq-Rec}\ \frac{L \text{ finite} \qquad m(\ell') = v' \qquad \forall \ell \notin L,\ v^{\ell} \sim_{f[\ell \mapsto \ell']} v'}{\mu.v \sim_f v'}
$$

Figure 6: The equivalence relation between weak values in the original semantics and values in the semantics with memory. $f \in \text{Loc} \xrightarrow{\text{fin}} \text{Loc}$ tells what the free locations in w that were *opened* should be mapped to in memory. m is omitted for brevity.

The semantics in Figure 3 makes sense due to similarity with a conventional backpatching semantics as presented in Figure 5. We have defined a relation $\sim$ that satisfies:

$$\sim \subseteq \text{WVal} \times (\text{MVal} \times \text{Mem} \times \mathcal{P}(\text{Loc})) \qquad \bullet \sim (\bullet, \emptyset, \emptyset)$$

and the following theorem:

Theorem 1.1 (Equivalence of semantics)**.** For all $\sigma \in \text{Env}, \sigma' \in \text{MEnv} \times \text{Mem} \times \mathcal{P}(\text{Loc}), v \in \text{Val}, v' \in \text{MVal} \times \text{Mem} \times \mathcal{P}(\text{Loc})$, we have:

$$\sigma \sim \sigma' \text{ and } \sigma \vdash e \Downarrow v \Rightarrow \exists v' : v \sim v' \text{ and } \sigma' \vdash e \Downarrow v'$$
$$\sigma \sim \sigma' \text{ and } \sigma' \vdash e \Downarrow v' \Rightarrow \exists v : v \sim v' \text{ and } \sigma \vdash e \Downarrow v$$

The definition for $w \sim (\sigma, m, L)$ is:

$$w \sim_{\perp} (\sigma, m) \text{ and } \text{FLoc}(w) \subseteq L$$

where the definition for $\sim_f$ is given in Figure 6.

The proof of Theorem 1.1 uses some useful lemmas, such as:

Lemma 1.1 (Free locations not in f are free in memory)**.**

$$w \sim_f v', m \Rightarrow m|_{\text{FLoc}(w)-\text{dom}(f)} = \perp$$

Lemma 1.2 (Equivalence is preserved by extension of memory)**.**

$$w \sim_f v', m \text{ and } m \sqsubseteq m' \text{ and } m'|_{\text{FLoc}(w)-\text{dom}(f)} = \perp \Rightarrow w \sim_f v', m$$

Lemma 1.3 (Equivalence only cares about f on free locations)**.**

$$w \sim_f v', m \text{ and } f|_{\text{FLoc}(w)} = f|_{\text{FLoc}(w)} \Rightarrow w \sim_{f'} v', m$$

Lemma 1.4 (Extending equivalence on free locations)**.**

$$w \sim_f v', m \text{ and } \ell \notin \text{dom}(f) \text{ and } \ell \notin \text{dom}(m) \Rightarrow \forall u', w \sim_{f[\ell \mapsto \ell]} v', m[\ell \mapsto u']$$

Lemma 1.5 (Substitution of values)**.**

$$w \sim_f v', m \text{ and } f(\ell) = \ell' \text{ and } m(\ell') = u' \text{ and } u \sim_{f-\ell} u', m \Rightarrow w[u/\ell] \sim_{f-\ell} v', m$$

Lemma 1.6 (Substitution of locations)**.**

$$w \sim_f v', m \text{ and } \ell \in \text{dom}(f) \text{ and } \nu \notin \text{FLoc}(w) \Rightarrow w[\nu/\ell] \sim_{f \circ (\nu \leftrightarrow \ell)} v', m$$

2 Generating and Resolving Events

Now we formulate the semantics for generating events.

Event	E	$\rightarrow$	Init	initial environment
		$\mid$	$\mathsf{Read}(E, x)$	read event
		$\mid$	$\mathsf{Call}(E, v)$	call event
Environment	σ	$\rightarrow$	$\cdots$	
		$\mid$	$[E]$	answer to an event
Value	v	$\rightarrow$	$\cdots$	
		$\mid$	E	answer to an event

Figure 7: Definition of the semantic domains with events. All other semantic domains are equal to Figure 2.

We extend how to read weak values given an environment.

$$\bullet(x) \triangleq \perp \qquad ((x', \ell) :: \sigma)(x) \triangleq (x = x' ? \ell : \sigma(x))$$
$$[E](x) \triangleq \mathsf{Read}(E, x) \qquad ((x', w) :: \sigma)(x) \triangleq (x = x' ? w : \sigma(x))$$

Then we need to add only one rule to the semantics in Figure 3 for the semantics to incorporate events.

$$\frac{\substack{\textsc{AppEvent} \\ \sigma \vdash e_1 \Downarrow E \qquad \sigma \vdash e_2 \Downarrow v}}{\sigma \vdash e_1\, e_2 \Downarrow \mathsf{Call}(E, v)}$$

Now we need to formulate the *concrete linking* rules. The concrete linking rule $\sigma_0 \propto w$, given an answer σ_0 to the Init event, resolves all events within w to obtain a set of final results.

Concrete linking makes sense because of the following theorem. First define:

$$\text{eval}(e, \sigma) \triangleq \{v | \sigma \vdash e \Downarrow v\} \qquad \text{eval}(e, \Sigma) \triangleq \bigcup_{\sigma \in \Sigma} \text{eval}(e, \sigma) \qquad \sigma_0 \propto W \triangleq \bigcup_{w \in W} (\sigma_0 \propto w)$$

Then the following holds:

$$\boxed{\infty \in \text{Env} \to \text{Event} \to \mathcal{P}(\text{Val})}$$

$$\begin{aligned}
\sigma_0 \infty \mathsf{Init} &\triangleq \{\sigma_0\} \\
\sigma_0 \infty \mathsf{Read}(E, x) &\triangleq \{v_+ | \sigma_+ \in \sigma_0 \infty E \land \sigma_+(x) = v_+\} \\
&\cup \{{v_+}^{\mu.v_+} | \sigma_+ \in \sigma_0 \infty E \land \sigma_+(x) = \mu.v_+\} \\
\sigma_0 \infty \mathsf{Call}(E, v) &\triangleq \{v'_+ | \langle \lambda x.e, \sigma_+ \rangle \in \sigma_0 \infty E \land v_+ \in \sigma_0 \infty v \land (x, v_+) :: \sigma_+ \vdash e \Downarrow v'_+\} \\
&\cup \{\mathsf{Call}(E_+, v_+) | E_+ \in \sigma_0 \infty E \land v_+ \in \sigma_0 \infty v\}
\end{aligned}$$

$$\boxed{\infty \in \text{Env} \to \text{Env} \to \mathcal{P}(\text{Env})}$$

$$\begin{aligned}
\sigma_0 \infty \bullet &\triangleq \{\bullet\} \\
\sigma_0 \infty (x, \ell) :: \sigma &\triangleq \{(x, \ell) :: \sigma_+ | \sigma_+ \in \sigma_0 \infty \sigma\} \\
\sigma_0 \infty (x, w) :: \sigma &\triangleq \{(x, w_+) :: \sigma_+ | w_+ \in \sigma_0 \infty w \land \sigma_+ \in \sigma_0 \infty \sigma\} \\
\sigma_0 \infty [E] &\triangleq \{\sigma_+ | \sigma_+ \in \sigma_0 \infty E\} \cup \{[E_+] | E_+ \in \sigma_0 \infty E\}
\end{aligned}$$

$$\boxed{\infty \in \text{Env} \to \text{Val} \to \mathcal{P}(\text{Val})}$$

$$\sigma_0 \infty \langle \lambda x.e, \sigma \rangle \triangleq \{\langle \lambda x.e, \sigma_+ \rangle | \sigma_+ \in \sigma_0 \infty \sigma\}$$

$$\boxed{\infty \in \text{Env} \to \text{WVal} \to \mathcal{P}(\text{WVal})}$$

$$\sigma_0 \infty \mu.v \triangleq \{\mu.^{\setminus \ell} v_+ | \ell \notin \text{FLoc}(v) \cup \text{FLoc}(\sigma_0) \land v_+ \in \sigma_0 \infty v^{\ell}\}$$

Figure 8: Definition for concrete linking.

Theorem 2.1 (Soundness of concrete linking)**.** Given $e \in \text{Expr}, \sigma \in \text{Env}, v \in \text{Val}$,

$$\forall \sigma_0 \in \text{Env} : \text{eval}(e, \sigma_0 \infty \sigma) \subseteq \sigma_0 \infty \text{eval}(e, \sigma)$$

The proof of Theorem 2.1 uses some useful lemmas, such as:

Lemma 2.1 (Linking distributes under substitution)**.** Let σ_0 be the external environment that is linked with locally closed weak values w and u. For all $\ell \notin \text{FLoc}(\sigma_0)$, we have:

$$\forall w_+, u_+ : w_+ \in \sigma_0 \infty w \land u_+ \in \sigma_0 \infty u \Rightarrow \{u_+ \leftarrow \ell\} w_+ \in \sigma_0 \infty \{u \leftarrow \ell\} w$$

Lemma 2.2 (Linking is compatible with reads)**.** Let σ_0 be the external environment that is linked with some environment σ. Let v be the value obtained from reading x from σ. Let $\text{unfold} : \text{WVal} \to \text{Val}$ be defined as:

$$\text{unfold}(\mu.v) \triangleq v^{\mu.v} \qquad \text{unfold}(v) \triangleq v$$

Then for all $\sigma_+ \in \sigma_0 \infty \sigma$, we have:

$$\exists w_+ \in \text{WVal} : \sigma_+(x) = w_+ \land \text{unfold}(w_+) \in \sigma_0 \infty v$$

3 CFA

$$
\begin{array}{rccl}
\text{Program point} & p & \in & \mathbb{P} \triangleq \{\text{finite set of program points}\} \\
\text{Labelled expression} & pe & \in & \mathbb{P} \times \text{Expr} \\
\text{Labelled location} & \ell^p & \in & \mathbb{P} \times \text{Loc} \\
\text{Collecting semantics} & t & \in & \mathbb{T} \triangleq \mathbb{P} \to \mathcal{P}(\text{Env} + \text{Env} \times \text{Val}) \\
\text{Labelled expression} & pe & \to & \{p : e\} \\
\text{Expression} & e & \to & x \mid \lambda x.pe \mid pe\ pe \mid pe \rtimes pe \mid \varepsilon \mid x = pe; pe
\end{array}
$$

$$\boxed{\text{Step} : \mathbb{T} \to \mathbb{T}}$$

$$\text{Step}(t) \triangleq \bigcup_{p \in \mathbb{P}} \text{step}(t, p)$$

$$\boxed{\text{step} : (\mathbb{T} \times \mathbb{P}) \to \mathbb{T}}$$

$$
\begin{aligned}
\text{step}(t,p) &\triangleq [p \mapsto \{(\sigma, v) | \sigma \in t(p) \text{ and } \sigma(x) = v\}] && \text{when } \{p : x\} \\
&\cup [p \mapsto \{(\sigma, v^{\mu.v}) | \sigma \in t(p) \text{ and } \sigma(x) = \mu.v\}] \\
\text{step}(t,p) &\triangleq [p \mapsto \{(\sigma, \langle \lambda x.p', \sigma\rangle) | \sigma \in t(p)\}] && \text{when } \{p : \lambda x.p'\} \\
\text{step}(t,p) &\triangleq [p_1 \mapsto \{\sigma \in \text{Env} | \sigma \in t(p)\}] && \text{when } \{p : p_1\ p_2\} \\
&\cup [p_2 \mapsto \{\sigma \in \text{Env} | \sigma \in t(p)\}] \\
&\cup \bigcup_{\sigma \in t(p)} \bigcup_{(\sigma, \langle \lambda x.p', \sigma_1\rangle) \in t(p_1)} [p' \mapsto \{(x, v_2) :: \sigma_1 | (\sigma, v_2) \in t(p_2)\}] \\
&\cup [p \mapsto \bigcup_{\sigma \in t(p)} \bigcup_{(\sigma, \langle \lambda x.p', \sigma_1\rangle) \in t(p_1)} \bigcup_{(\sigma, v_2) \in t(p_2)} \{(\sigma, v) | ((x, v_2) :: \sigma_1, v) \in t(p')\}] \\
&\cup [p \mapsto \bigcup_{\sigma \in t(p)} \{(\sigma, \mathsf{Call}(E_1, v_2)) | (\sigma, E_1) \in t(p_1) \text{ and } (\sigma, v_2) \in t(p_2)\}] \\
\text{step}(t,p) &\triangleq [p_1 \mapsto \{\sigma | \sigma \in t(p)\}] && \text{when } \{p : p_1 \rtimes p_2\} \\
&\cup [p_2 \mapsto \bigcup_{\sigma \in t(p)} \{\sigma_1 | (\sigma, \sigma_1) \in t(p_1)\}] \\
&\cup [p \mapsto \bigcup_{\sigma \in t(p)} \bigcup_{(\sigma, \sigma_1) \in t(p_1)} \{(\sigma, v_2) | (\sigma_1, v_2) \in t(p_2)\}] \\
\text{step}(t,p) &\triangleq [p \mapsto \{(\sigma, \bullet) | \sigma \in t(p)\}] && \text{when } \{p : \varepsilon\} \\
\text{step}(t,p) &\triangleq [p_1 \mapsto \bigcup_{\sigma \in t(p)} \{(x, \ell^{p_1}) :: \sigma | \ell \notin \text{FLoc}(\sigma)\}] && \text{when } \{p : x = p_1; p_2\} \\
&\cup [p_2 \mapsto \bigcup_{\sigma \in t(p)} \{(x, \mu.\,{}^{\backslash \ell^{p_1}} v_1) :: \sigma | ((x, \ell^{p_1}) :: \sigma, v_1) \in t(p_1)\}] \\
&\cup [p \mapsto \bigcup_{\sigma \in t(p)} \bigcup_{((x, \ell^{p_1}) :: \sigma, v_1) \in t(p_1)} \{(\sigma, (x, \mu.\,{}^{\backslash \ell^{p_1}} v_1) :: \sigma_2) | ((x, \mu.\,{}^{\backslash \ell^{p_1}} v_1) :: \sigma, \sigma_2) \in t(p_2)\}]
\end{aligned}
$$

The proof tree t computed by

$$t \triangleq \text{lfp}(\lambda t.\text{Step}(t) \cup t_{\text{init}}) \quad \text{where } t_{\text{init}} = [p_0 \mapsto \{\sigma_0\}]$$

contains all derivations of the form $\sigma_0 \vdash p_0 \Downarrow v_0$ for some v_0. That is, (σ, v) is contained in $t_0(p)$ if and only if $\sigma \vdash p \Downarrow v$ must be contained in a valid derivation for the judgment $\sigma_0 \vdash p_0 \Downarrow v_0$.

$$
\begin{array}{rccl}
\text{Abstract event} & E^\# & \in & \text{Event}^\# \\
\text{Abstract environment} & \sigma^\# & \in & \text{Env}^\# \triangleq (\text{Var} \xrightarrow{\text{fin}} \mathcal{P}(\mathbb{P})) \times \mathcal{P}(\text{Event}^\#) \\
\text{Abstract closure} & \langle \lambda x.p, p'\rangle & \in & \text{Clos}^\# \triangleq \text{Var} \times \mathbb{P} \times \mathbb{P} \\
\text{Abstract value} & v^\# & \in & \text{Val}^\# \triangleq \text{Env}^\# \times \mathcal{P}(\text{Clos}^\#) \\
\text{Abstract semantics} & t^\# & \in & \mathbb{T}^\# \triangleq \mathbb{P} \to \text{Env}^\# \times \text{Val}^\# \\
\text{Abstract event} & E^\# & \to & \mathsf{Init}^\# \mid \mathsf{Read}^\#(p, x) \mid \mathsf{Call}^\#(p, p)
\end{array}
$$

The concretization function γ that sends an element of $\mathbb{T}^\#$ to $\mathbb{T}$ is defined as:

$$\gamma(t^\#) \triangleq \lambda p.\{\sigma | \sigma \leq (t^\#(p).1, t^\#)\} \cup \{(\sigma, v) | v \leq (t^\#(p).2, t^\#)\}$$

where $\leq$ is the concretization relation that is inductively defined in Figure 9.

$$\boxed{\sigma \le_f (\sigma^\#, t^\#)}$$

$$\frac{}{\bullet \le \sigma^\#}\textsc{Conc-Nil} \qquad \frac{E \le (\sigma^\#, \emptyset)}{[E] \le \sigma^\#}\textsc{Conc-ENil} \qquad \frac{p \in \sigma^\#.1(x) \quad \sigma \le \sigma^\#}{(x, \ell^p) :: \sigma \le \sigma^\#}\textsc{Conc-ConsLoc} \qquad \frac{p \in \sigma^\#.1(x) \quad w \le t^\#(p).2 \quad \sigma \le \sigma^\#}{(x, w) :: \sigma \le \sigma^\#}\textsc{Conc-ConsWVal}$$

$$\boxed{w \le (v^\#, t^\#)}$$

$$\frac{\langle \lambda x.p, p' \rangle \in v^\#.2 \quad \sigma \le t^\#(p').1}{\langle \lambda x.p, \sigma \rangle \le v^\#}\textsc{Conc-Clos} \qquad \frac{L \text{ finite} \quad \forall \ell \notin L,\ v^{\ell^p} \le t^\#(p).2 \text{ and } v^{\ell^p} \le v^\#}{\mu.v \le v^\#}\textsc{Conc-Rec}$$

$$\frac{\mathsf{Init}^\# \in v^\#.1.2}{\mathsf{Init} \le v^\#}\textsc{Conc-Init} \qquad \frac{\mathsf{Read}^\#(p, x) \in v^\#.1.2 \quad [E] \le t^\#(p).1}{\mathsf{Read}(E, x) \le v^\#}\textsc{Conc-Read} \qquad \frac{\mathsf{Call}^\#(p_1, p_2) \in v^\#.1.2 \quad E \le t^\#(p_1).2 \quad v \le t^\#(p_2).2}{\mathsf{Call}(E, v) \le v^\#}\textsc{Conc-Call}$$

Figure 9: The concretization relation between weak values and abstract values. $t^\#$ is omitted.

Now the abstract semantic function can be given.

$$\boxed{\text{Step}^\# : \mathbb{T}^\# \to \mathbb{T}^\#}$$

$$\text{Step}^\#(t^\#) \triangleq \bigsqcup_{p \in \mathbb{P}} \text{step}^\#(t^\#, p)$$

$$\boxed{\text{step}^\# : (\mathbb{T}^\# \times \mathbb{P}) \to \mathbb{T}^\#}$$

$$\begin{aligned}
\text{step}^\#(t^\#, p) &\triangleq [p \mapsto \bigsqcup_{p' \in t^\#(p).1.1(x)} (\bot, t^\#(p').2)] && \text{when } \{p : x\} \\
&\sqcup [p \mapsto (\bot, (([], \{\mathsf{Read}^\#(p, x)\}), \emptyset))] && \text{if } t^\#(p).1.2 \neq \emptyset \\
\text{step}^\#(t^\#, p) &\triangleq [p \mapsto (\bot, (\bot, \{\langle \lambda x.p', p \rangle\}))] && \text{when } \{p : \lambda x.p'\} \\
\text{step}^\#(t^\#, p) &\triangleq [p_1 \mapsto (t^\#(p).1, \bot)] && \text{when } \{p : p_1\ p_2\} \\
&\sqcup [p_2 \mapsto (t^\#(p).1, \bot)] \\
&\sqcup \bigsqcup_{\langle \lambda x.p', p'' \rangle \in t^\#(p_1).2.2} [p' \mapsto (t^\#(p'').1 \sqcup ([x \mapsto \{p_2\}], \emptyset), \bot)] \\
&\sqcup [p \mapsto \bigsqcup_{\langle \lambda x.p', _ \rangle \in t^\#(p_1).2.2} (\bot, t^\#(p').2)] \\
&\sqcup [p \mapsto (\bot, (([], \{\mathsf{Call}^\#(p_1, p_2)\}), \emptyset))] && \text{if } t^\#(p_1).2.1.2 \neq \emptyset \\
\text{step}^\#(t^\#, p) &\triangleq [p_1 \mapsto (t^\#(p).1, \bot)] && \text{when } \{p : p_1 \rtimes p_2\} \\
&\sqcup [p_2 \mapsto (t^\#(p_1).2.1, \bot)] \\
&\sqcup [p \mapsto (\bot, t^\#(p_2).2)] \\
\text{step}^\#(t^\#, p) &\triangleq \bot && \text{when } \{p : \varepsilon\} \\
\text{step}^\#(t^\#, p) &\triangleq [p_1 \mapsto (t^\#(p).1 \sqcup ([x \mapsto \{p_1\}], \emptyset), \bot)] && \text{when } \{p : x = p_1; p_2\} \\
&\sqcup [p_2 \mapsto (t^\#(p).1 \sqcup ([x \mapsto \{p_1\}], \emptyset), \bot)] \\
&\sqcup [p \mapsto (\bot, (t^\#(p_2).2.1 \sqcup ([x \mapsto \{p_1\}], \emptyset), \emptyset))]
\end{aligned}$$

The abstract proof tree $t^\#$ computed by

$$t^\# \triangleq \text{lfp}(\lambda t^\#.\text{Step}^\#(t^\#) \sqcup t^\#_{\text{init}}) \quad \text{where } t_{\text{init}} \subseteq \gamma(t^\#_{\text{init}})$$

is a sound abstraction of t.

Now we define a sound linking operator that abstracts $\propto$. Assume we have

$$\sigma_0 \le (\sigma^\#_0, t^\#_0) \quad t \subseteq \gamma(t^\#)$$

we define:

$$\sigma_0 \propto t \triangleq \lambda p. (\sigma_0 \propto t(p))$$

We want to define $\infty^\#$ so that the following holds:

$$\sigma_0 \infty t \subseteq \gamma((\sigma_0^\#, t_0^\#) \infty^\# t^\#)$$

This is defined by

$$(\sigma_0^\#, t_0^\#) \infty^\# t^\# \triangleq \mathrm{lfp}(\lambda t_+^\#. \mathrm{Step}^\#(t_+^\#) \sqcup \mathrm{Link}^\#(\sigma_0^\#, \mathsf{E}(t^\#), t_+^\#) \sqcup t_0^\# \sqcup \mathsf{V}(t^\#))$$

where

$$\mathsf{E}(t^\#) \in \mathbb{P} \to \mathcal{P}(\mathrm{Event}^\#)^2 \quad \mathsf{V}(t^\#) \in \mathbb{T}^\# \quad \mathrm{Link}^\#(\sigma^\#, \mathcal{E}, t^\#) \in \mathbb{T}^\#$$

are defined by

$$\mathsf{E}(t^\#) \triangleq \lambda p.(t^\#(p).1.2, t^\#(p).2.1.2) \quad \mathsf{V}(t^\#) \triangleq \lambda p.((t^\#(p).1.1, \emptyset), ((t^\#(p).2.1.1, \emptyset), t^\#(p).2.2))$$

and

$$\mathrm{Link}^\#(\sigma^\#, \mathcal{E}, t^\#) \triangleq \bigsqcup_{E^\# \in \mathcal{E}(p).1} \mathrm{link}_1^\#(\sigma^\#, E^\#, t^\#, p) \sqcup \bigsqcup_{E^\# \in \mathcal{E}(p).2} \mathrm{link}_2^\#(\sigma^\#, E^\#, t^\#, p)$$

where

$$\mathrm{link}_1^\#(\sigma^\#, E^\#, t^\#, p) \in \mathbb{T}^\# \quad \mathrm{link}_2^\#(\sigma^\#, E^\#, t^\#, p) \in \mathbb{T}^\#$$

are defined by

$$\begin{aligned}
\mathrm{link}_1^\#(\sigma^\#, E^\#, t^\#, p) &\triangleq [p \mapsto (\sigma^\#, \bot)] && \text{when } E^\# = \mathsf{Init}^\# \\
\mathrm{link}_1^\#(\sigma^\#, E^\#, t^\#, p) &\triangleq [p \mapsto \bigsqcup_{p'' \in t^\#(p').1.1(x)} (t^\#(p'').2.1, \bot)] && \text{when } E^\# = \mathsf{Read}^\#(p', x) \\
&\sqcup [p \mapsto (([], \{\mathsf{Read}^\#(p, x)\}), \bot)] && \text{if } t^\#(p).1.2 \neq \emptyset \\
\mathrm{link}_1^\#(\sigma^\#, E^\#, t^\#, p) &\triangleq \bigsqcup_{\langle \lambda x.p', p'' \rangle \in t^\#(p_1).2.2} [p' \mapsto (t^\#(p'').1 \sqcup ([x \mapsto \{p_2\}], \emptyset), \bot)] && \text{when } E^\# = \mathsf{Call}^\#(p_1, p_2) \\
&\sqcup [p \mapsto \bigsqcup_{\langle \lambda x.p', _ \rangle \in t^\#(p_1).2.2} (t^\#(p').2.1, \bot)] \\
&\sqcup [p \mapsto (([], \{\mathsf{Call}^\#(p_1, p_2)\}), \bot)] && \text{if } t^\#(p_1).2.1.2 \neq \emptyset \\
\mathrm{link}_2^\#(\sigma^\#, E^\#, t^\#, p) &\triangleq [p \mapsto (\bot, (\sigma^\#, \emptyset))] && \text{when } E^\# = \mathsf{Init}^\# \\
\mathrm{link}_2^\#(\sigma^\#, E^\#, t^\#, p) &\triangleq [p \mapsto \bigsqcup_{p'' \in t^\#(p').1.1(x)} (\bot, t^\#(p'').2)] && \text{when } E^\# = \mathsf{Read}^\#(p', x) \\
&\sqcup [p \mapsto (\bot, (([], \{\mathsf{Read}^\#(p, x)\}), \emptyset))] && \text{if } t^\#(p).1.2 \neq \emptyset \\
\mathrm{link}_2^\#(\sigma^\#, E^\#, t^\#, p) &\triangleq \bigsqcup_{\langle \lambda x.p', p'' \rangle \in t^\#(p_1).2.2} [p' \mapsto (t^\#(p'').1 \sqcup ([x \mapsto \{p_2\}], \emptyset), \bot)] && \text{when } E^\# = \mathsf{Call}^\#(p_1, p_2) \\
&\sqcup [p \mapsto \bigsqcup_{\langle \lambda x.p', _ \rangle \in t^\#(p_1).2.2} (\bot, t^\#(p').2)] \\
&\sqcup [p \mapsto (\bot, (([], \{\mathsf{Call}^\#(p_1, p_2)\}), \emptyset))] && \text{if } t^\#(p_1).2.1.2 \neq \emptyset
\end{aligned}$$

Lemma 3.1 (Substitution of values)**.**

$$w \leq (v^\#, t^\#) \text{ and } u \leq (t^\#(p).2, t^\#) \Rightarrow w[u/\ell^p] \leq (v^\#, t^\#)$$

Lemma 3.2 (Sound step$^\#$)**.**

$$\forall p, t, t^\# : t \subseteq \gamma(t^\#) \Rightarrow \mathrm{step}(t, p) \cup t \subseteq \gamma(\mathrm{step}^\#(t^\#, p) \sqcup t^\#)$$

Lemma 3.3 (Sound Step$^\#$)**.**

$$\forall t_{\mathrm{init}}, t^\# : t_{\mathrm{init}} \subseteq \gamma(t^\#) \text{ and } \mathrm{Step}^\#(t^\#) \sqsubseteq t^\# \Rightarrow \mathrm{lfp}(\lambda t.\mathrm{Step}(t) \cup t_{\mathrm{init}}) \subseteq \gamma(t^\#)$$

Lemma 3.4 (Sound Link$^\#$)**.** For each $\sigma_0, \sigma_0^\#, t_0^\#, t, t^\#, t_+^\#$, if:

1. $\sigma_0 \leq (\sigma_0^\#, t_0^\#)$
2. $t \subseteq \gamma(t^\#)$
3. $\mathrm{Step}^\#(t_+^\#) \sqcup \mathrm{Link}^\#(\sigma_0^\#, \mathsf{E}(t^\#), t_+^\#) \sqcup t_0^\# \sqcup \mathsf{V}(t^\#) \sqsubseteq t_+^\#$

we have:

$$\forall w, w_+ \in \sigma_0 \infty w, p : [w \in t(p) \Rightarrow w_+ \leq (t_+^\#(p).1, t_+^\#)] \text{ and } [(\_, w) \in t(p) \Rightarrow w_+ \leq (t_+^\#(p).2, t_+^\#)]$$