Verifying Generics and Delegates
(Technical Appendix)

Kasper Svendsen
IT University of Copenhagen
kasv@itu.dk

Lars Birkedal
IT Univeristy of Copenhagen
birkedal@itu.dk

Matthew Parkinson
University of Cambridge
Matthew.Parkinson@cl.cam.ac.uk

April 16, 2010

Contents

1 Programming Language **2**
1.1 Syntax . . . 2
1.2 Operational Semantics . . . 2
1.3 Metatheory . . . 4

2 Assertion Logic **5**
2.1 Syntax . . . 5
2.2 Typing rules . . . 7
2.3 Proof rules . . . 8
2.4 Semantics . . . 9
2.5 Metatheory . . . 12

3 Specification Logic **13**
3.1 Syntax . . . 13
3.2 Typing rules . . . 13
3.3 Proof rules . . . 14
3.4 Semantics . . . 17
3.5 Metatheory . . . 19

4 Examples **26**

This is a technical appendix to the paper with the same title.

1 Programming Language

1.1 Syntax

We use the notation $\bar{\mathsf{x}}$ for finite sequences.

G	::=	$\mathsf{C}\langle\overline{\mathsf{G}}\rangle \mid \mathsf{T}$	Generic class
L	::=	$\texttt{class}\ \mathsf{C}\langle\overline{\mathsf{T}}\rangle : \mathsf{G}\ \{\bar{\mathsf{G}}\bar{\mathsf{f}}; \bar{\mathsf{M}}\}$	Class definition
M	::=	$\mathsf{G}\ \mathsf{m}\ (\bar{\mathsf{G}}\bar{\mathsf{u}})\ \{\mathsf{B}\}$	Method definition
B	::=	$\bar{\mathsf{G}}\bar{\mathsf{z}}; \mathsf{s}; \texttt{return}\ \mathsf{r};$	Method body
s	::=		Statement
		$\mathsf{x}\ \texttt{=}\ \mathsf{y}$	assignment
		$\mathsf{x}\ \texttt{=}\ \texttt{null}$	initialization
		$\mathsf{x}\ \texttt{=}\ \mathsf{y}\texttt{.}\mathsf{f}$	field access
		$\mathsf{x}\texttt{.}\mathsf{f}\ \texttt{=}\ \mathsf{y}$	field update
		$\mathsf{x}\ \texttt{=}\ \mathsf{y}\texttt{.}\mathsf{m}(\bar{\mathsf{z}})$	method invocation
		$\mathsf{x}\ \texttt{=}\ (\mathsf{G})\mathsf{y}$	cast
		$\texttt{if}\ (\mathsf{x}\ \texttt{==}\ \mathsf{y})\ \{\mathsf{s}_1\}\ \texttt{else}\ \{\mathsf{s}_2\}$	conditional
		$\mathsf{x}\ \texttt{=}\ \texttt{new}\ \mathsf{C}\langle\bar{\mathsf{G}}\rangle()$	object creation
		$\mathsf{x}\ \texttt{=}\ \texttt{delegate}\ (\bar{\mathsf{G}}\bar{\mathsf{z}})\ \{\mathsf{B}\}$	inline delegate
		$\mathsf{x}\ \texttt{=}\ \texttt{delegate}\ \mathsf{y}\texttt{.}\mathsf{m}$	named delegate
		$\mathsf{x}\ \texttt{=}\ \mathsf{y}(\bar{\mathsf{z}})$	delegate application
		$\mathsf{s}_1; \mathsf{s}_2$	sequential composition

1.2 Operational Semantics

For the operational semantics we assume disjoint countably infinite sets of stack locations, $\mathbb{L}_s$, heap locations, $\mathbb{L}_h$, variables, $\mathbb{A}_p$, type variables $\mathbb{A}_t$, class identifiers, $\mathbb{C}$, method identifiers, $\mathbb{M}$, field identifiers, $\mathbb{F}$, and object identifiers, $\mathbb{O}$.

l	$\in$	$\mathbb{L}_s$	locations
o	$\in$	$\mathbb{O}$	object identifiers
v	$\in$	$\mathbb{V} = \mathbb{L}_h \uplus \mathbb{O} \uplus \{\texttt{null}\}$	values
$\mathsf{a}, \mathsf{b}, \mathsf{c}, \mathsf{r}, \mathsf{u}, \mathsf{x}, \mathsf{y}, \mathsf{z}$	$\in$	$\mathbb{A}_p$	variables
C, D	$\in$	$\mathbb{C}$	class identifiers
f	$\in$	$\mathbb{F}$	field identifiers
m	$\in$	$\mathbb{M}$	method identifiers
T	$\in$	$\mathbb{A}_t$	type variables
		$\mathbb{B} \stackrel{\text{def}}{=} L(\mathsf{s})$	statements
		$\mathbb{T} \stackrel{\text{def}}{=} \{w \in L(\mathsf{G}) \mid \text{FTV}(w) = \emptyset\}$	generic classes
δ	$\in$	$\mathbb{E}_t \stackrel{\text{def}}{=} \mathbb{A}_t \stackrel{\text{fin}}{\to} \mathbb{T}$	type environment
E	$\in$	$\mathbb{E}_p \stackrel{\text{def}}{=} \mathbb{A}_p \stackrel{\text{fin}}{\to} \mathbb{L}_s$	environment
C, S	$\in$	$\mathbb{S} \stackrel{\text{def}}{=} \mathbb{L}_s \stackrel{\text{fin}}{\to} \mathbb{V}$	stack
H	$\in$	$\mathbb{H} \stackrel{\text{def}}{=} (\mathbb{O} \times \mathbb{F} \stackrel{\text{fin}}{\to} \mathbb{V}) \times (\mathbb{O} \stackrel{\text{fin}}{\to} L(\mathsf{G})) \times (\mathbb{L}_h \stackrel{\text{fin}}{\to} \mathbb{D})$	heap
		$\mathbb{D} \stackrel{\text{def}}{=} (\mathbb{E}_t \times \mathbb{E}_p \times \mathbb{A}_p^* \times \mathbb{A}_p^* \times \mathbb{B} \times \mathbb{A}_p) \uplus (\mathbb{O} \times \mathbb{M})$	delegate
P	$\in$	$\mathbb{P} \stackrel{\text{def}}{=} (\mathbb{C} \stackrel{\text{fin}}{\to} \mathbb{A}_t^* \times \mathbb{F}^*) \times (\mathbb{C} \times \mathbb{M} \stackrel{\text{fin}}{\to} \mathbb{A}_p^* \times \mathbb{A}_p^* \times \mathbb{B} \times \mathbb{A}_p)$	program

where FTV is the set of free type variables. We use the notation A^* for the set of finite lists of A elements. We take the permutation action on to be atom-permutation on $\mathbb{A}_p$, $\mathbb{A}_t$, and $\mathbb{B}$, and the trivial action on $\mathbb{L}_s$, $\mathbb{O}$, $\mathbb{V}$, $\mathbb{C}$, $\mathbb{F}$, $\mathbb{M}$.

The operational semantics is given as a big-step semantics, with step-indices corresponding to a small-step semantics.

$$\frac{S' = S[E(\mathsf{x}) \mapsto S(E(\mathsf{y}))]}{(P, \delta, E, S, H, \mathsf{x} = \mathsf{y}) \Downarrow_1 (S', H)} \qquad \frac{S' = S[E(\mathsf{x}) \mapsto \text{null}]}{(P, \delta, E, S, H, \mathsf{x} = \texttt{null}) \Downarrow_1 S', H)}$$

$$\frac{S' = S[E(\mathsf{x}) \mapsto H(S(E(\mathsf{y})), \mathsf{f})]}{(P, \delta, E, S, H, \mathsf{x} = \mathsf{y}.\mathsf{f}) \Downarrow_1 (S', H)} \qquad \frac{H' = H[(S(E(\mathsf{x})), \mathsf{f}) \mapsto S(E(\mathsf{y}))]}{(P, \delta, E, S, H, \mathsf{x}.\mathsf{f} = \mathsf{y}) \Downarrow_1 (S, H')}$$

$$\frac{\begin{array}{c} H_t(E(S(\mathsf{y}))) = \mathsf{C}\langle \bar{\mathsf{G}} \rangle \qquad P(\mathsf{C}) = (\bar{\mathsf{T}}, \_) \qquad P(\mathsf{C}, \mathsf{m}) = (\bar{\mathsf{x}}, \bar{\mathsf{z}}, \mathsf{s}, \mathsf{r}) \\ \bar{l}_x, \bar{l}_z, l_t \notin \text{Dom}(S) \qquad E' = [\texttt{this} \mapsto l_t, \bar{\mathsf{x}} \mapsto \bar{l}_x, \bar{\mathsf{z}} \mapsto \bar{l}_z] \\ (P, [\bar{\mathsf{T}} \mapsto \bar{\mathsf{G}}], E', S[l_t \mapsto S(E(\mathsf{y})), \bar{l}_x \mapsto S(E(\bar{\mathsf{u}})), \bar{l}_z \mapsto \texttt{null}], H, \mathsf{s}) \Downarrow_n (S', H') \end{array}}{(P, \delta, E, S, H, \mathsf{x} = \mathsf{y}.\mathsf{m}(\bar{\mathsf{u}})) \Downarrow_{n+1} (S'[S(E(\mathsf{x})) \mapsto S'(E'(\mathsf{r}))], H')}$$

$$\frac{H_3(S(E(\mathsf{y}))) \leq [\![\mathsf{G}]\!](\delta) \qquad S' = S[E(\mathsf{x}) \mapsto S(E(\mathsf{y}))]}{(P, \delta, E, S, H, \mathsf{x} = (\mathsf{G})\mathsf{y}) \Downarrow_1 (S', H)} \qquad \frac{S(E(\mathsf{y})) = \text{null} \qquad S' = S[E(\mathsf{x}) \mapsto \text{null}]}{(P, \delta, E, S, H, \mathsf{x} = (\mathsf{G})\mathsf{y}) \Downarrow_1 (S', H)}$$

$$\frac{S(E(\mathsf{x})) = S(E(\mathsf{y})) \qquad (P, \delta, E, S, \mathsf{s}_1) \Downarrow_n (S', H')}{(P, \delta, E, S, H, \texttt{if } (\mathsf{x} == \mathsf{y}) \texttt{ then } \mathsf{s}_1 \texttt{ else } \mathsf{s}_2) \Downarrow_{n+1} (S', H')}$$

$$\frac{o \notin \text{Dom}(H_t) \qquad H' = H[o \mapsto \mathsf{C}\langle [\![\bar{\mathsf{G}}]\!](\delta) \rangle, (o, \bar{\mathsf{f}}) \mapsto \texttt{null}] \qquad P(\mathsf{C}) = (\bar{\mathsf{T}}, \bar{\mathsf{f}}) \qquad S' = S[E(\mathsf{x}) \mapsto o]}{(P, \delta, E, S, H, \mathsf{x} = \textbf{\textit{new}}\ \mathsf{C}\langle \bar{\mathsf{G}} \rangle()) \Downarrow_1 (S', H')}$$

$$\frac{l \notin \text{Dom}(H_c) \qquad S' = S[E(\mathsf{x}) \mapsto l] \qquad E_c = E|_{\text{FV}(\mathsf{s},\mathsf{r}) \setminus (\bar{\mathsf{x}} \cup \bar{\mathsf{z}})} \qquad H' = H[l \mapsto (\delta, E_c, \bar{\mathsf{x}}, \bar{\mathsf{z}}, \mathsf{s}, \mathsf{r})]}{(P, \delta, E, S, H, \mathsf{x} \texttt{ = delegate } (\bar{\mathsf{G}}\bar{\mathsf{x}})\ \{\bar{\mathsf{G}}\bar{\mathsf{z}}\texttt{; } \mathsf{s}\texttt{; return } \mathsf{r}\}) \Downarrow_1 (S', H')}$$

$$\frac{l \notin \text{Dom}(H_c) \qquad H' = H_c[l \mapsto (S(E(\mathsf{y})), \mathsf{m})] \qquad S' = S[E(\mathsf{x}) \mapsto l]}{(P, \delta, E, S, H, \mathsf{x} \texttt{ = delegate } \mathsf{y}.\mathsf{m}) \Downarrow_1 (S', H')}$$

$$\frac{\begin{array}{c} H_c(S(E(\mathsf{y}))) = (o, \mathsf{m}) \qquad H_t(o) = \mathsf{C}\langle \bar{\mathsf{G}} \rangle \qquad P(\mathsf{C}) = (\bar{\mathsf{T}}, \_) \qquad P(\mathsf{C}, \mathsf{m}) = (\bar{\mathsf{x}}, \bar{\mathsf{z}}, \mathsf{s}, \mathsf{r}) \\ \bar{l}_x, \bar{l}_z, l_t \notin \text{Dom}(S) \qquad E' = [\texttt{this} \mapsto l_t, \bar{\mathsf{x}} \mapsto \bar{l}_x, \bar{\mathsf{z}} \mapsto \bar{l}_z] \\ (P, [\bar{\mathsf{T}} \mapsto \bar{\mathsf{G}}], E', S[l_t \mapsto S(E(\mathsf{y})), \bar{l}_x \mapsto S(E(\bar{\mathsf{u}})), \bar{l}_z \mapsto \texttt{null}], H, \mathsf{s}) \Downarrow_n (S', H') \end{array}}{(P, \delta, E, S, H, \mathsf{x} = \mathsf{y}(\bar{\mathsf{u}})) \Downarrow_{n+1} (S'[S(E(\mathsf{x})) \mapsto S'(E'(\mathsf{r}))], H')}$$

$$\frac{\begin{array}{c} \bar{l}_x, \bar{l}_z \notin \text{Dom}(S) \qquad H_c(S(E(\mathsf{y}))) = (\delta_c, E_c, \bar{\mathsf{x}}, \bar{\mathsf{z}}, \mathsf{s}, \mathsf{r}) \\ (P, \delta_c, E_c[\bar{\mathsf{x}} \mapsto \bar{l}_x, \bar{\mathsf{z}} \mapsto \bar{l}_z], S[\bar{l}_x \mapsto S(E(\bar{\mathsf{u}})), \bar{l}_z \mapsto \text{null}], H, \mathsf{s}) \Downarrow_n (S', H') \end{array}}{(P, \delta, E, S, H, \mathsf{x} = \mathsf{y}(\bar{\mathsf{u}})) \Downarrow_{n+1} (S'[E(\mathsf{x}) \mapsto S'(E'(\mathsf{r}))], H')}$$

$$\frac{(P, \delta, E, S, H, \mathsf{s}_1) \Downarrow_n (S', H') \qquad (P, \delta, E, S', H', \mathsf{s}_2) \Downarrow_m T}{(P, \delta, E, S, H, \mathsf{s}_1; \mathsf{s}_2) \Downarrow_{n+m} T} \qquad \frac{(P, \delta, E, S, H, \mathsf{s}_1) \Downarrow_n \text{err}}{(P, \delta, E, S, H, \mathsf{s}_1; \mathsf{s}_2) \Downarrow_n \text{err}}$$

We use the notation $P(\mathsf{C})$ for $\pi_1(P)(\mathsf{C})$ and $P(\mathsf{C}, \mathsf{m})$ for $\pi_2(P)(\mathsf{C}, \mathsf{m})$. Furthermore, we use $[\bar{x} \mapsto \bar{\mathsf{y}}]$ as shorthand for $[x_1 \mapsto y_1, ..., x_n \mapsto y_n]$, with the implicit assumption that the two sequences have the same length. We omit most of the rules for exceptional termination.

1.3 Metatheory

Lemma 1.

$$(P, \delta, E, S, H, \mathsf{s}) \Downarrow_n (S', H') \Rightarrow (P, \delta, \pi(E), S, \pi(H), \pi(\mathsf{s})) \Downarrow_n (S', \pi(H'))$$

and

$$(P, \delta, E, S, H, \mathsf{s}) : \mathit{safe}_n \Rightarrow (P, \delta, \pi(E), S, \pi(H), \pi(\mathsf{s})) : \mathit{safe}_n$$

Lemma 2. *If* $\mathsf{x} \notin FV(\mathsf{s})$ *then*

$$(P, \delta, E, S, H, \mathsf{s}) \Downarrow_n (S', H') \Rightarrow (P, \delta, E \setminus \mathsf{x}, S, H, \mathsf{s}) \Downarrow_n (S', H')$$

Lemma 3 (Safety monotonicity)**.** *If* $S_1 \# S_2$*,* $H_1 \# H_2$*, and* $(P, \delta, E, S_1, H_1, \mathsf{s}) : \mathit{safe}_n$ *then*

$$(P, \delta, E, S_1 * S_2, H_1 * H_2, \mathsf{s}) : \mathit{safe}_n$$

Lemma 4 (Heap frame property)**.** *If*

$$(P, \delta, E, S, H_1 * H_2, \mathsf{s}) \Downarrow_n (S', H')$$

and $(P, \delta, E, S, H_1, \mathsf{s}) : \mathit{safe}_n$ *then there exists a* H_1' *such that* $H' = H_1' * H_2$ *and*

$$(P, \delta, E, S, H_1, \mathsf{s}) \Downarrow_n (S', H_1')$$

Lemma 5 (Stack frame property)**.** *If*

$$(P, \delta, E, S_1 * S_2, H, \mathsf{s}) \Downarrow_n (S', H')$$

and $(P, \delta, E, S_1, H, \mathsf{s}) : \mathit{safe}_n$ *then there exists an* S_1' *such that* $S' = S_1' * S_2$ *and*

$$(P, \delta, E, S_1, H, \mathsf{s}) \Downarrow_n (S_1', H')$$

2 Assertion Logic

2.1 Syntax

$$
\begin{array}{rcll}
\omega, \omega' & ::= & \omega \to \omega' \mid \omega \times \omega' \mid \texttt{Prop} \mid \texttt{Class} \mid \texttt{Val} \mid \texttt{Int} \mid \texttt{Loc} & \text{Types} \\
\mathsf{M}, \mathsf{N}, \mathsf{L}, \mathsf{P}, \mathsf{Q}, \mathsf{R} & ::= & \mathsf{P} \vee \mathsf{Q} \mid \mathsf{P} \wedge \mathsf{Q} \mid \mathsf{P} \Rightarrow \mathsf{Q} \mid \top \mid \bot \mid \forall \mathsf{x} : \omega . \mathsf{P} \mid \exists \mathsf{x} : \omega . \mathsf{P} & \text{Propositions} \\
 & \mid & \mathsf{P} * \mathsf{Q} \mid \mathsf{P} \mathrel{-\!\!*} \mathsf{Q} \mid \texttt{emp} \mid \mathsf{M}.\mathsf{f} \mapsto \mathsf{N} \mid \mathsf{M} =_{\omega} \mathsf{N} & \\
 & \mid & \mathsf{L} \overset{s}{\mapsto} \mathsf{N} \mid \mathsf{M} \mapsto \langle (\bar{\mathsf{x}}).\{\mathsf{P}\}\_\{\mathsf{d}.\mathsf{Q}\}\rangle \mid \mathsf{M}{:}\mathsf{N} & \\
 & \mid & \lambda \mathsf{x} : \omega . \mathsf{M} \mid \mathsf{M}\ \mathsf{N} \mid \mathsf{x} \mid \&\mathsf{x} \mid \texttt{null} & \text{Other terms}
\end{array}
$$

The judgments of the assertion logic are of the forms:

$$\Delta; \phi; \psi \vdash \mathsf{M} : \omega, \quad \Delta; \phi; \psi \vdash \mathsf{M} = \mathsf{N} : \omega, \quad \Delta; \phi; \psi \mid \mathsf{P}_1, ..., \mathsf{P}_n \vdash \mathsf{Q}$$

where Δ is the type variable context, ϕ is the program variable context and ψ is the logic variable context, which are defined as follows:

$$
\begin{array}{rcll}
\Delta & ::= & \Delta, \mathsf{T} \mid \epsilon & \text{type variable context} \\
\phi & ::= & \phi, \mathsf{x} : \texttt{Val} \mid \epsilon & \text{program variable context} \\
\psi & ::= & \psi, \mathsf{a} : \omega \mid \epsilon & \text{logic variable context}
\end{array}
$$

Variables cannot be repeated in the program or logic variable context and the same variable cannot appear in both the program and logic variable context. Since program variables are always of type `Val` we will never write the type.

Definition 1 (Value substitution)**.**

$$
\begin{aligned}
(\mathsf{R} \mapsto \langle (\bar{\mathsf{u}}).\{\mathsf{P}\}\_\{\mathsf{d}.\mathsf{Q}\}\rangle)[\mathsf{M}/\mathsf{x}] &= \mathsf{R}[\mathsf{M}/\mathsf{x}] \mapsto \langle (\bar{\mathsf{u}}).\{\mathsf{P}[\mathsf{M}/\mathsf{x}]\}\_\{\mathsf{d}.\mathsf{Q}[\mathsf{M}/\mathsf{x}]\}\rangle \\
(\mathsf{L} \overset{s}{\mapsto} \mathsf{N})[\mathsf{M}/\mathsf{x}] &= \mathsf{L}[\mathsf{M}/\mathsf{x}] \overset{s}{\mapsto} \mathsf{N}[\mathsf{M}/\mathsf{x}] \\
\&\mathsf{y}[\mathsf{M}/\mathsf{x}] &= \&\mathsf{x} \\
\mathsf{y}[\mathsf{M}/\mathsf{x}] &= \begin{cases} \mathsf{M} & \textit{if } \mathsf{y} = \mathsf{x} \\ \mathsf{y} & \textit{otherwise} \end{cases}
\end{aligned}
$$

assuming $\bar{\mathsf{u}}$, d, *and* y *are fresh for* x.

Definition 2 (Location substitution)**.**

$$
\begin{aligned}
(\mathsf{R} \mapsto \langle (\bar{\mathsf{u}}).\{\mathsf{P}\}\_\{\mathsf{d}.\mathsf{Q}\}\rangle)[\mathsf{M}/\&\mathsf{x}] &= \mathsf{R}[\mathsf{M}/\&\mathsf{x}] \mapsto \langle (\bar{\mathsf{u}}).\{\mathsf{P}[\mathsf{M}/\&\mathsf{x}]\}\_\{\mathsf{d}.\mathsf{Q}[\mathsf{M}/\&\mathsf{x}]\}\rangle \\
(\mathsf{L} \overset{s}{\mapsto} \mathsf{N})[\mathsf{M}/\&\mathsf{x}] &= \mathsf{L}[\mathsf{M}/\&\mathsf{x}] \overset{s}{\mapsto} \mathsf{N}[\mathsf{M}/\&\mathsf{x}] \\
\&\mathsf{y}[\mathsf{M}/\&\mathsf{x}] &= \begin{cases} \mathsf{M} & \textit{if } \mathsf{x} = \mathsf{y} \\ \&\mathsf{y} & \textit{otherwise} \end{cases} \\
\mathsf{y}[\mathsf{M}/\&\mathsf{x}] &= \mathsf{y}
\end{aligned}
$$

assuming $\bar{\mathsf{u}}$, d, *and* y *are fresh for* x.

Definition 3 (Free variables)**.**

$$
\begin{aligned}
\mathrm{FV}(\mathsf{M} \mapsto \langle (\bar{\mathsf{u}}).\{\mathsf{P}\}\_\{\mathsf{d}.\mathsf{Q}\}\rangle) &= \mathrm{FV}(\mathsf{M}) \cup (\mathrm{FV}(\mathsf{P}) \cup \mathrm{FV}(\mathsf{Q})) \setminus (\bar{\mathsf{u}} \cup \{\mathsf{d}\}) \\
\mathrm{FV}(\mathsf{L} \overset{s}{\mapsto} \mathsf{N}) &= \mathrm{FV}(\mathsf{L}) \cup \mathrm{FV}(\mathsf{N}) \\
\mathrm{FV}(\&\mathsf{x}) &= \{\mathsf{x}\} \\
\mathrm{FV}(\mathsf{x}) &= \{\mathsf{x}\}
\end{aligned}
$$

Definition 4 (Free value variables)**.**

$$\begin{aligned}
\mathrm{FVV}(\mathsf{M} \mapsto \langle(\bar{\mathsf{u}}).\{\mathsf{P}\}_\{\mathsf{d}.\mathsf{Q}\}\rangle) &= \mathrm{FVV}(\mathsf{M}) \cup (\mathrm{FVV}(\mathsf{P}) \cup \mathrm{FVV}(\mathsf{Q})) \setminus (\bar{\mathsf{u}} \cup \{\mathsf{d}\}) \\
\mathrm{FVV}(\mathsf{L} \overset{s}{\mapsto} \mathsf{N}) &= \mathrm{FV}(\mathsf{L}) \cup \mathrm{FVV}(\mathsf{N}) \\
\mathrm{FVV}(\&\mathsf{x}) &= \emptyset \\
\mathrm{FVV}(\mathsf{x}) &= \{\mathsf{x}\}
\end{aligned}$$

Definition 5 (Free location variables)**.**

$$\begin{aligned}
\mathrm{FVA}(\mathsf{M} \mapsto \langle(\bar{\mathsf{u}}).\{\mathsf{P}\}_\{\mathsf{d}.\mathsf{Q}\}\rangle) &= \mathrm{FVA}(\mathsf{M}) \cup (\mathrm{FVA}(\mathsf{P}) \cup \mathrm{FVA}(\mathsf{Q})) \setminus (\bar{\mathsf{u}} \cup \{\mathsf{d}\}) \\
\mathrm{FVA}(\mathsf{L} \overset{s}{\mapsto} \mathsf{N}) &= \mathrm{FVA}(\mathsf{L}) \cup \mathrm{FVA}(\mathsf{N}) \\
\mathrm{FVA}(\&\mathsf{x}) &= \{\mathsf{x}\} \\
\mathrm{FVA}(\mathsf{x}) &= \emptyset
\end{aligned}$$

Definition 6 (Lookup)**.**

$$\mathit{lookup}\ \mathsf{L}\ \mathit{as}\ \mathsf{x}\ \mathit{in}\ \mathsf{P} \overset{def}{=} \exists \mathsf{x} : \mathit{Val}.\ (\mathsf{L} \mapsto \mathsf{x} * \mathsf{P})$$

2.2 Typing rules

Well-formed terms $\boxed{\Delta; \phi; \psi \vdash \mathsf{R} : \omega}$

$$\frac{\Delta; \phi; \psi \vdash \mathsf{M} : \mathtt{Val} \qquad \Delta; \phi; \psi, \bar{\mathsf{u}} : \mathtt{Val} \vdash \mathsf{P} : \mathtt{Prop} \qquad \Delta; \phi; \psi, \bar{\mathsf{u}} : \mathtt{Val}, \mathsf{d} : \mathtt{Val} \vdash \mathsf{Q} : \mathtt{Prop}}{\Delta; \phi; \psi \vdash \mathsf{M} \mapsto \langle (\bar{\mathsf{u}}).\{\mathsf{P}\}\_\{\mathsf{d}.\mathsf{Q}\}\rangle : \mathtt{Prop}}$$

$$\frac{\Delta; \phi; \psi, \mathsf{x} : \omega \vdash \mathsf{P} : \mathtt{Prop} \qquad Q \in \{\exists, \forall\}}{\Delta; \phi; \psi \vdash Q\mathsf{x} : \omega.\ \mathsf{P} : \mathtt{Prop}} \qquad \frac{\Delta; \phi; \psi \vdash \mathsf{L} : \mathtt{Loc} \qquad \Delta; \phi; \psi \vdash \mathsf{N} : \mathtt{Val}}{\Delta; \phi; \psi \vdash \mathsf{L} \overset{s}{\mapsto} \mathsf{N} : \mathtt{Prop}}$$

$$\frac{}{\Delta; \phi; \psi \vdash \top : \mathtt{Prop}} \qquad \frac{}{\Delta; \phi; \psi \vdash \bot : \mathtt{Prop}} \qquad \frac{}{\Delta; \phi; \psi \vdash \mathtt{emp} : \mathtt{Prop}}$$

$$\frac{op \in \{\wedge, \vee, *, -\!\!*, \Rightarrow\} \qquad \Delta; \phi; \psi \vdash \mathsf{P} : \mathtt{Prop} \qquad \Delta; \phi; \psi \vdash \mathsf{Q} : \mathtt{Prop}}{\Delta; \phi; \psi \vdash \mathsf{P}\ op\ \mathsf{Q} : \mathtt{Prop}}$$

$$\frac{\Delta; \phi; \psi \vdash \mathsf{M} : \mathtt{Val} \qquad \Delta; \phi; \psi \vdash \mathsf{N} : \mathtt{Class}}{\Delta; \phi; \psi \vdash \mathsf{M} : \mathsf{N} : \mathtt{Prop}} \qquad \frac{\mathsf{x} \in \phi}{\Delta; \phi; \psi \vdash \&\mathsf{x} : \mathtt{Loc}}$$

$$\frac{}{\Delta, \mathsf{T}; \phi; \psi \vdash \mathsf{T} : \mathtt{Class}} \qquad \frac{\Delta; \phi; \psi \vdash \bar{\mathsf{G}} : \mathtt{Class}}{\Delta; \phi; \psi \vdash \mathsf{C}\langle \bar{\mathsf{G}} \rangle : \mathtt{Class}} \qquad \frac{}{\Delta; \phi; \psi \vdash \mathtt{null} : \mathtt{Val}}$$

$$\frac{}{\Delta; \phi, \mathsf{x}; \psi \vdash \mathsf{x} : \mathtt{Val}} \qquad \frac{}{\Delta; \phi; \psi, \mathsf{a} : \omega \vdash \mathsf{a} : \omega}$$

$$\frac{\Delta; \phi; \psi, \mathsf{x} : \omega \vdash \mathsf{M} : \omega'}{\Delta; \phi; \psi \vdash \lambda \mathsf{x} : \omega.\ \mathsf{M} : \omega \to \omega'} \qquad \frac{\Delta; \phi; \psi \vdash \mathsf{M} : \omega \to \omega' \qquad \Delta; \phi; \psi \vdash \mathsf{M} : \omega}{\Delta; \phi; \psi \vdash \mathsf{M}\ \mathsf{N} : \omega'}$$

$$\frac{\Delta; \phi; \psi \vdash \mathsf{M} : \mathtt{Val} \qquad \Delta; \phi; \psi \vdash \mathsf{N} : \mathtt{Val}}{\Delta; \phi; \psi \vdash \mathsf{M}.\mathsf{f} \mapsto \mathsf{N} : \mathtt{Prop}} \qquad \frac{\Delta; \phi; \psi \vdash \mathsf{M} : \omega \qquad \Delta; \phi; \psi \vdash \mathsf{N} : \omega}{\Delta; \phi; \psi \vdash \mathsf{M} =_\omega \mathsf{N} : \mathtt{Prop}}$$

2.3 Proof rules

Standard HO Intuitionistic separation logic, extended with the following rules:

$$\frac{\Delta;\phi;\psi \vdash \mathsf{M} : \mathtt{Val} \qquad \Delta;\phi;\psi,\bar{\mathsf{u}} \mid \mathsf{P}' \vdash \mathsf{P} \qquad \Delta;\phi;\psi,\bar{\mathsf{u}},\mathsf{d} \mid \mathsf{Q} \vdash \mathsf{Q}'}{\Delta;\phi;\psi \mid \mathsf{M} \mapsto \langle(\bar{\mathsf{u}}).\{\mathsf{P}\}\_\{\mathsf{d}.\mathsf{Q}\}\rangle \vdash \mathsf{M} \mapsto \langle(\bar{\mathsf{u}}).\{\mathsf{P}'\}\_\{\mathsf{d}.\mathsf{Q}'\}\rangle}$$

$$\frac{\Delta;\phi;\psi \vdash \mathsf{L},\mathsf{L}' : \mathtt{Loc} \qquad \Delta;\phi;\psi,\mathsf{x} \vdash \mathsf{P},\mathsf{Q} : \mathtt{Prop}}{\Delta;\phi;\psi \mid \mathtt{lookup}\ \mathsf{L}\ \mathtt{as}\ \mathsf{x}\ \mathtt{in}\ \mathsf{P} * \mathtt{lookup}\ \mathsf{L}'\ \mathtt{as}\ \mathsf{x}\ \mathtt{in}\ \mathsf{Q} \vdash \mathsf{L} \neq \mathsf{L}'}$$

$$\frac{\Delta;\phi;\psi \vdash \mathsf{L} : \mathtt{Var} \qquad \Delta;\phi;\psi,\mathsf{x} \vdash \mathsf{P} : \mathtt{Prop} \qquad \Delta;\phi;\psi \vdash \mathsf{Q} : \mathtt{Prop}}{\Delta;\phi;\psi \mid (\mathtt{lookup}\ \mathsf{L}\ \mathtt{as}\ \mathsf{x}\ \mathtt{in}\ \mathsf{P}) * \mathsf{Q} \dashv\vdash \mathtt{lookup}\ \mathsf{L}\ \mathtt{as}\ \mathsf{x}\ \mathtt{in}\ (\mathsf{P} * \mathsf{Q})}$$

2.4 Semantics

Types $\boxed{[\![\omega]\!] \in \mathrm{Set}}$

$$\begin{array}{rcl}
[\![\omega \to \omega']\!] & = & [\![\omega]\!] \to [\![\omega']\!] \\
[\![\omega \times \omega']\!] & = & [\![\omega]\!] \times [\![\omega']\!] \\
[\![\texttt{Prop}]\!] & = & \{U \in \mathcal{P}^{\uparrow}(\mathsf{N} \times \mathbb{S} \times \mathbb{H}) \mid \forall \pi \in \mathrm{Perm}(\mathbb{A}_p).\ \forall a \in U.\ \pi(a) \in U\} \\
[\![\texttt{Val}]\!] & = & \mathrm{Val} \\
[\![\texttt{Loc}]\!] & = & \mathbb{L}_s \\
[\![\texttt{Class}]\!] & = & \mathbb{T} \\
[\![\texttt{Int}]\!] & = & \mathbf{Z}
\end{array}$$

where Val is the least set satisfying:

$$\mathrm{Val} \cong \mathbb{V} \uplus \mathrm{Strings} \uplus \mathrm{Val} \times \mathrm{Val}$$

The order on $\mathsf{N} \times \mathbb{S} \times \mathbb{H}$ is given as follows:

$$(n, S, (h_v, h_t, h_c)) \leq (m, S', (h'_v, h'_t, h'_c)) \quad \text{iff} \quad m \leq n \wedge S \leq S' \wedge h_v \leq h'_v \wedge h_t \leq h'_t \wedge h_c \leq h'_c$$

where all the finite functions are ordered as follows:

$$f \leq g \quad \text{iff} \quad \mathrm{Dom}(f) \subseteq \mathrm{Dom}(g) \wedge \forall x \in \mathrm{Dom}(f).\ f(x) = g(x)$$

Contexts $\boxed{[\![\phi]\!], [\![\psi]\!], [\![\Delta]\!] \in \mathrm{Set}}$

$$\begin{array}{l}
S \in [\![\phi]\!] = \{(E, S) \in \mathbb{E}_p \times \mathbb{S} \mid E \text{ injective} \wedge \mathrm{Dom}(E) = \phi \wedge \mathrm{Rng}(E) = \mathrm{Dom}(S)\} \\
\vartheta \in [\![\psi]\!] = \Pi(\mathsf{x} : \omega) \in \psi.\ [\![\omega]\!] \\
\delta \in [\![\Delta]\!] = \{\delta \in \mathbb{E}_t \mid \mathrm{Dom}(\delta) = \Delta\}
\end{array}$$

Propositions and Terms $\boxed{[\![\Delta;\phi;\psi \vdash \mathsf{M} : \omega]\!] : [\![\Delta]\!] \times [\![\phi]\!] \times [\![\psi]\!] \to [\![\omega]\!]}$

$$
\begin{array}{rcl}
[\![\Delta;\phi;\psi \vdash \mathsf{C}\langle\bar{\mathsf{G}}\rangle : \mathtt{Class}]\!](\delta;(E,S);\vartheta) & = & \mathsf{C}\langle[\![\Delta;\phi;\psi \vdash \bar{\mathsf{G}} : \mathtt{Class}]\!](\delta;(E,S);\vartheta)\rangle \\
[\![\Delta;\phi;\psi \vdash \mathsf{e} : \mathsf{C} : \mathtt{Prop}]\!](\delta;(E,S);\vartheta) & = & \{(n,C,(h_v,h_t,h_c)) \in \mathsf{N}\times\mathbb{S}\times\mathbb{H} \mid \exists o \in \mathbb{O}, \mathsf{C} \in \mathbb{C}, \delta' \in \mathbb{E}_t. \\
 & & \quad in_{\mathbb{O}}(o) = [\![\Delta;\phi;\psi \vdash \mathsf{e} : \mathtt{Val}]\!](\delta;(E,S);\vartheta) \ \wedge \\
 & & \quad h_t(o) = [\![\Delta;\phi;\psi \vdash \mathsf{C} : \mathtt{Class}]\!](\delta;(E,S);\vartheta)\} \\
[\![\Delta;\phi;\psi \vdash \top : \mathtt{Prop}]\!](\delta;(E,S);\vartheta) & = & \mathsf{N}\times\mathbb{S}\times\mathbb{H} \\
[\![\Delta;\phi;\psi \vdash \bot : \mathtt{Prop}]\!](\delta;(E,S);\vartheta) & = & \emptyset \\
[\![\Delta;\phi;\psi \vdash \mathtt{emp} : \mathtt{Prop}]\!](\delta;(E,S);\vartheta) & = & \mathsf{N}\times\mathbb{S}\times\mathbb{H} \\
[\![\Delta;\phi;\psi \vdash \mathsf{P}\wedge\mathsf{Q} : \mathtt{Prop}]\!](\delta;(E,S);\vartheta) & = & [\![\Delta;\phi;\psi \vdash \mathsf{P} : \mathtt{Prop}]\!](\delta;(E,S);\vartheta) \cap [\![\Delta;\phi;\psi \vdash \mathsf{Q} : \mathtt{Prop}]\!](\delta;(E,S);\vartheta) \\
[\![\Delta;\phi;\psi \vdash \mathsf{P}\vee\mathsf{Q} : \mathtt{Prop}]\!](\delta;(E,S);\vartheta) & = & [\![\Delta;\phi;\psi \vdash \mathsf{P} : \mathtt{Prop}]\!](\delta;(E,S);\vartheta) \cup [\![\Delta;\phi;\psi \vdash \mathsf{Q} : \mathtt{Prop}]\!](\delta;(E,S);\vartheta) \\
[\![\Delta;\phi;\psi \vdash \mathsf{P}*\mathsf{Q} : \mathtt{Prop}]\!](\delta;(E,S);\vartheta) & = & \{(n,C,(h_v,h_t,h_c)) \in \mathsf{N}\times\mathbb{S}\times\mathbb{H} \mid \exists C_1,C_2,h_1,h_2. \\
 & & \quad C_1 \# C_2 \wedge h_1 \# h_2 \wedge C = C_1 \cup C_2 \wedge h_v = h_1 \cup h_2 \wedge \\
 & & \quad (n,C_1,(h_1,h_t,h_c)) \in [\![\Delta;\phi;\psi \vdash \mathsf{P} : \mathtt{Prop}]\!](\delta;(E,S);\vartheta) \ \wedge \\
 & & \quad (n,C_2,(h_2,h_t,h_c)) \in [\![\Delta;\phi;\psi \vdash \mathsf{Q} : \mathtt{Prop}]\!](\delta;(E,S);\vartheta)\} \\
[\![\Delta;\phi;\psi \vdash \mathsf{P}\Rightarrow\mathsf{Q} : \mathtt{Prop}]\!](\delta;(E,S);\vartheta) & = & \{B \in \mathsf{N}\times\mathbb{S}\times\mathbb{H} \mid \forall B' \geq B. \\
 & & \quad B' \in [\![\Delta;\phi;\psi \vdash \mathsf{P} : \mathtt{Prop}]\!](\delta;(E,S);\vartheta) \Rightarrow \\
 & & \quad B' \in [\![\Delta;\phi;\psi \vdash \mathsf{Q} : \mathtt{Prop}]\!](\delta;(E,S);\vartheta)\} \\
[\![\Delta;\phi;\psi \vdash \mathsf{M}.\mathsf{f} \mapsto \mathsf{N} : \mathtt{Prop}]\!](\delta;(E,S);\vartheta) & = & \{(n,C,(h_v,h_t,h_c)) \in \mathsf{N}\times\mathbb{S}\times\mathbb{H} \mid \exists o \in \mathbb{O}. \\
 & & \quad in_{Oid}(o) = [\![\Delta;\phi;\psi \vdash \mathsf{M} : \mathtt{Val}]\!](\delta;(E,S);\vartheta) \ \wedge \\
 & & \quad h_v(o,\mathsf{f}) = [\![\Delta;\phi;\psi \vdash \mathsf{N} : \mathtt{Val}]\!](\delta;(E,S);\vartheta)\} \\
[\![\Delta;\phi;\psi \vdash \forall \mathsf{a} : \omega.\mathsf{P} : \mathtt{Prop}]\!](\delta;(E,S);\vartheta) & = & \bigcap_{v\in[\![\omega]\!]} [\![\Delta;\phi;\psi,\mathsf{a} : \omega \vdash \mathsf{P} : \mathtt{Prop}]\!](\delta;(E,S);\vartheta,\mathsf{a}\mapsto v) \\
[\![\Delta;\phi;\psi \vdash \exists \mathsf{a} : \omega.\mathsf{P} : \mathtt{Prop}]\!](\delta;(E,S);\vartheta) & = & \bigcup_{v\in[\![\omega]\!]} [\![\Delta;\phi;\psi,\mathsf{a} : \omega \vdash \mathsf{P} : \mathtt{Prop}]\!](\delta;(E,S);\vartheta,\mathsf{a}\mapsto v) \\
[\![\Delta;\phi,\psi \vdash \mathsf{M} =_\omega \mathsf{N} : \mathtt{Prop}]\!](\delta;(E,S);\vartheta) & = & \{B \in \mathsf{N}\times\mathbb{S}\times\mathbb{H} \mid \\
 & & \quad [\![\Delta;\phi;\psi \vdash \mathsf{M} : \omega]\!](\delta;(E,S);\vartheta) = [\![\Delta;\phi;\psi \vdash \mathsf{N} : \omega]\!](\delta;(E,S);\vartheta)\} \\
[\![\Delta,\mathsf{T};\phi;\psi \vdash \mathsf{T} : \mathtt{Class}]\!](\delta;(E,S);\vartheta) & = & \delta(\mathsf{T}) \\
[\![\Delta;\phi,\mathsf{x};\psi \vdash \mathsf{x} : \mathtt{Val}]\!](\delta;(E,S);\vartheta) & = & S(E(\mathsf{x})) \\
[\![\Delta;\phi;\psi \vdash \mathtt{null} : \mathtt{Val}]\!](\delta;(E,S);\vartheta) & = & \mathrm{null} \\
[\![\Delta;\phi;\psi,\mathsf{a} : \omega \vdash \mathsf{a} : \omega]\!](\delta;(E,S);\vartheta) & = & \vartheta(\mathsf{a}) \\
[\![\Delta;\phi;\psi \vdash \lambda \mathsf{a} : \omega.\mathsf{M} : \omega \to \omega']\!](\delta;(E,S);\vartheta) & = & \lambda v : [\![\omega]\!].\ [\![\Delta;\phi;\psi,\mathsf{a} : \omega \vdash \mathsf{M} : \omega']\!](\delta;(E,S);\vartheta[\mathsf{a}\mapsto v]) \\
[\![\Delta;\phi;\psi \vdash \mathsf{M}\ \mathsf{N} : \omega]\!](\delta;(E,S),\vartheta) & = & ([\![\Delta;\phi;\psi \vdash \mathsf{M} : \omega' \to \omega]\!](\delta;(E,S);\vartheta))\ ([\![\Delta;\phi;\psi \vdash \mathsf{N} : \omega']\!](\delta;(E,S);\vartheta)) \\
[\![\Delta;\phi,\mathsf{x};\psi \vdash \&\mathsf{x} : \mathtt{Loc}]\!](\delta;(E,S);\vartheta) & = & E(\mathsf{x}) \\
[\![\Delta;\phi;\psi \vdash \mathsf{L} \overset{s}{\mapsto} \mathsf{N} : \mathtt{Prop}]\!](\delta;(E,S);\vartheta) & = & \{(n,C,H) \in \mathsf{N}\times\mathbb{S}\times\mathbb{H} \mid l \in \mathrm{Dom}(C) \wedge \\
 & & \qquad C(l) = [\![\Delta;\phi;\psi \vdash \mathsf{N} : \mathtt{Val}]\!](\delta;(E,S);\vartheta)\}
\end{array}
$$

where $l = [\![\Delta;\phi;\psi \vdash \mathsf{L} : \mathtt{Loc}]\!](\delta;(E,S);\vartheta)$.

$$
\begin{array}{l}
[\![\Delta;\phi;\psi \vdash \mathsf{M} \mapsto \langle(\bar{\mathsf{u}}).\{\mathsf{P}\}\_\{\mathsf{d}.\mathsf{Q}\}\rangle : \mathtt{Prop}]\!](\delta,(E,S),\vartheta) = \\
\quad \{(n,\_,(h_v,h_t,h_c)) \in \mathsf{N}\times\mathbb{S}\times\mathbb{H} \mid \exists o,\delta_c,E_c,\bar{\mathsf{x}},\bar{\mathsf{z}},\mathsf{s},\mathsf{r},\mathsf{C},\bar{\mathsf{G}},\bar{\mathsf{T}}. \\
\qquad h_c([\![\Delta;\phi;\psi \vdash \mathsf{M} : \mathtt{Val}]\!](\delta,(E,S),\vartheta) = (\delta_c,E_c,\bar{\mathsf{x}},\bar{\mathsf{z}},\mathsf{s},\mathsf{r}) \wedge \\
\qquad \forall m \le n.\ \forall k \le m.\ \forall C \in \mathbb{S}.\ \forall H \in \mathbb{H}.\ \forall \bar{l}_x,\bar{l}_z\ \in \mathrm{Loc} \setminus (\mathrm{Dom}(C) \cup \mathrm{Rng}(E_c)).\ \forall \bar{v}_x \in \mathrm{Val}. \\
\qquad (m-1,C,H) \in [\![\Delta;\phi;\psi,\bar{\mathsf{u}} \vdash \mathsf{P} : \mathtt{Prop}]\!](\delta,(E,S),\vartheta[\bar{\mathsf{u}} \mapsto \bar{v}_x])\ \Rightarrow \\
\qquad\quad (\delta_c; E_c', C[\bar{l}_x \mapsto \bar{v}_x, \bar{l}_z \mapsto \mathtt{null}], H, \mathsf{s}) : \mathtt{safe}_k \wedge \\
\qquad\quad (\delta_c; E_c', C[\bar{l}_x \mapsto \bar{v}_x, \bar{l}_z \mapsto \mathtt{null}], H, \mathsf{s}) \Downarrow_k (C', H')\ \Rightarrow \\
\qquad\qquad (m-k, C' \setminus \bar{l}_x; H') \in [\![\Delta;\phi;\psi,\bar{\mathsf{u}},\mathsf{d} \vdash \mathsf{Q} : \mathtt{Prop}]\!](\delta;(E,S),\vartheta[\bar{\mathsf{u}} \mapsto \bar{v}_x, \mathsf{d} \mapsto C'(E_c'(\mathsf{r}))]) \\
\quad \vee \\
\qquad h_c([\![\Delta;\phi;\psi \vdash \mathsf{M} : \mathtt{Val}]\!](\delta,(E,S),\vartheta) = (o,\mathsf{m}) \wedge h_t(o) = \mathsf{C}\langle\bar{\mathsf{G}}\rangle \wedge P(\mathsf{C}) = (\bar{\mathsf{T}},\_) \wedge P(\mathsf{C},\mathsf{m}) = (\bar{\mathsf{x}},\bar{\mathsf{z}},\mathsf{s},\mathsf{r}) \wedge \\
\qquad \forall m \le n.\ \forall k \le m.\ \forall C \in \mathsf{S}.\ \forall H \in \mathbb{H}.\ \forall \bar{l}_x,\bar{l}_z,l_t \in \mathbb{L}_s \setminus \mathrm{Dom}(C).\ \forall \bar{v}_x \in \mathbb{V}. \\
\qquad (m-1,C,H) \in [\![\Delta;\phi;\psi,\bar{\mathsf{u}} \vdash \mathsf{P} : \mathtt{Prop}]\!](\delta,(E,S),\vartheta[\bar{\mathsf{u}} \mapsto \bar{v}_x])\ \Rightarrow \\
\qquad\quad ([\bar{\mathsf{T}} \mapsto \bar{\mathsf{G}}], E', C[\bar{l}_u \mapsto \bar{v}_x, \bar{l}_z \mapsto \mathtt{null}, l_t \mapsto o], H, \mathsf{s}) : \mathtt{safe}_k \wedge \\
\qquad\quad ([\bar{\mathsf{T}} \mapsto \bar{\mathsf{G}}], E', C[\bar{l}_u \mapsto \bar{v}_x, \bar{l}_z \mapsto \mathtt{null}, l_t \mapsto o], H, \mathsf{s}) \Downarrow_k (C', H')\ \Rightarrow \\
\qquad\qquad (m-k, C' \setminus \bar{l}_x; H') \in [\![\Delta,\phi;\psi,\bar{\mathsf{u}},\mathsf{d} \vdash \mathsf{Q} : \mathtt{Prop}]\!](\delta,(E,S),\vartheta[\bar{\mathsf{u}} \mapsto \bar{v}_x, \mathsf{d} \mapsto C'(E'(\mathsf{r}))])
\end{array}
$$

where $E_c' = E_c[\bar{\mathsf{x}} \mapsto \bar{l}_x, \bar{\mathsf{z}} \mapsto \bar{l}_z]$ and $E' = [\mathtt{this} \mapsto l_t, \bar{\mathsf{x}} \mapsto \bar{l}_x, \bar{\mathsf{z}} \mapsto \bar{l}_z]$.

Entailment $\boxed{[\![\Delta;\phi;\psi \mid \mathsf{P}_1,...,\mathsf{P}_n \vdash \mathsf{Q}]\!] : 2}$

$$
\begin{array}{l}
[\![\Delta;\phi;\psi \mid \mathsf{P}_1,...,\mathsf{P}_n \vdash \mathsf{Q}]\!] = \forall \delta \in [\![\Delta]\!].\ \forall (E,S) \in [\![\phi]\!].\ \forall \vartheta \in [\![\psi]\!]. \\
\qquad \left(\bigcap_{1 \le i \le n} [\![\Delta;\phi;\psi \vdash \mathsf{P}_i : \mathtt{Prop}]\!](\delta;(E,S);\vartheta) \right) \subseteq [\![\Delta;\phi;\psi \vdash \mathsf{Q} : \mathtt{Prop}]\!](\delta;(E,S);\vartheta)
\end{array}
$$

2.5 Metatheory

Lemma 6. *Let*

$$\mathbb{P} = \{U \in \mathcal{P}^{\uparrow}(\mathsf{N} \times \mathbb{S} \times \mathbb{H}) \mid \forall \pi \in \mathrm{Perm}(\mathbb{A}_p).\ \forall a \in U.\ \pi(a)\}$$

Then $(\mathbb{P}, \subseteq)$ *is a complete BI-algebra, with BI structure* $(I, *, -\!\!*)$ *given by:*

$$\begin{aligned} I &= \emptyset \\ U * V &= \{(n, C \cup C', (h_v \cup h'_v, h_t, h_c)) \mid C \# C' \wedge h_v \# h'_v \wedge \\ &\qquad (n, C, (h_v, h_t, h_c)) \in U \wedge (n, C', (h'_v, h_t, h_c)) \in V\} \\ U -\!\!* V &= \bigcup \{W \in [\![\mathtt{Prop}]\!] \mid W * U \subseteq V\} \end{aligned}$$

for $U, V \in [\![\mathtt{Prop}]\!]$.

Lemma 7 (Alpha renaming)**.** *If* $\Delta; \phi; \psi \vdash \mathsf{P} : \omega$ *then,*

$$\begin{aligned} &\forall \delta \in [\![\Delta]\!].\ \forall (E, S) \in [\![\phi]\!].\ \forall \vartheta \in [\![\psi]\!]. \\ &\quad [\![\Delta; \phi; \psi \vdash \mathsf{P} : \omega]\!](\delta; (E, S); \vartheta) = [\![\Delta; \pi(\phi); \pi(\psi) \vdash \pi(\mathsf{P}) : \omega]\!](\delta; (\pi(E), S); \pi(\vartheta)) \end{aligned}$$

Lemma 8 (Weakening and strengthening)**.** *If* $\Delta; \phi; \psi \vdash \mathsf{P} : \omega$*,* $\mathsf{x} \notin \phi \cup \psi$ *then,*

$$\begin{aligned} &\forall \delta \in [\![\Delta]\!].\ \forall (E, S) \in [\![\phi]\!].\ \forall \vartheta \in [\![\psi]\!].\ \forall l \in \mathbb{L}_s \setminus \mathrm{Rng}(S).\ \forall v_1 \in \mathrm{Val}.\ \forall v_2 \in [\![\omega']\!]. \\ &\quad [\![\Delta; \phi; \psi \vdash \mathsf{P} : \omega]\!](\delta; (E, S); \vartheta) = [\![\Delta; \phi, \mathsf{x}; \psi \vdash \mathsf{P} : \omega]\!](\delta; (E[\mathsf{x} \mapsto l], S[l \mapsto v_1]); \vartheta) \\ &\qquad\qquad = [\![\Delta; \phi; \psi, \mathsf{x} : \omega' \vdash \mathsf{P} : \omega]\!](\delta; (E, S); \vartheta[\mathsf{x} \mapsto v_2]) \end{aligned}$$

Lemma 9. *If* $\Delta; \phi; \psi \vdash \mathsf{P} : \omega$ *then,*

$$\begin{aligned} &\forall \delta \in [\![\Delta]\!].\ \forall E, S_1, S_2.\ \forall \vartheta \in [\![\psi]\!].\ ((E, S_1), (E, S_2) \in [\![\phi]\!] \wedge \forall \mathsf{x} \in \mathrm{FVV}(\mathsf{P}).\ S_1(E(\mathsf{x})) = S_2(E(\mathsf{x}))) \ \Rightarrow \\ &\quad [\![\Delta; \phi; \psi \vdash \mathsf{P} : \omega]\!](\delta; (E, S_1); \vartheta) = [\![\Delta; \phi; \psi \vdash \mathsf{P} : \omega]\!](\delta; (E, S_2); \vartheta) \end{aligned}$$

Lemma 10 (Substitution (Logical variable))**.** *If* $\Delta; \phi; \psi, \mathsf{a} : \omega \vdash \mathsf{P} : \omega'$ *and* $\Delta; \phi; \psi \vdash \mathsf{M} : \omega$ *then,*

$$\begin{aligned} &\forall \delta \in [\![\Delta]\!].\ \forall (E, S) \in [\![\phi]\!].\ \forall \vartheta \in [\![\psi]\!]. \\ &\quad [\![\Delta; \phi; \psi, \mathsf{a} : \omega \vdash \mathsf{P} : \omega']\!](\delta; (E, S); \vartheta, \mathsf{a} \mapsto [\![\Delta; \phi; \psi \vdash \mathsf{M} : \omega]\!](\delta; (E, S); \vartheta)) = [\![\Delta; \phi; \psi \vdash \mathsf{P}[\mathsf{M}/\mathsf{a}] : \omega']\!](\delta; (E, S); \vartheta) \end{aligned}$$

Lemma 11 (Substitution (Program variable))**.** *If* $\Delta; \phi, \mathsf{x}; \psi \vdash \mathsf{P} : \omega$ *and* $\Delta; \phi, \mathsf{x}; \psi \vdash \mathsf{M} : \mathtt{Val}$ *then,*

$$\begin{aligned} &\forall \delta \in [\![\Delta]\!].\ \forall (E, S) \in [\![\phi, \mathsf{x}]\!].\ \forall \vartheta \in [\![\psi]\!]. \\ &\quad [\![\Delta; \phi, \mathsf{x}; \psi \vdash \mathsf{P} : \omega]\!](\delta; (E, S[E(\mathsf{x}) \mapsto [\![\Delta; \phi, \mathsf{x}; \psi \vdash \mathsf{M} : \mathtt{Val}]\!](\delta; (E, S); \vartheta)]); \vartheta) = [\![\Delta; \phi, \mathsf{x}; \psi \vdash \mathsf{P}[\mathsf{M}/\mathsf{x}] : \omega]\!](\delta; (E, S); \vartheta) \end{aligned}$$

Lemma 12 (Splitting)**.** *If* $\Delta; \phi, \mathsf{x}; \psi \vdash \mathsf{P} : \omega$ *then,*

$$\begin{aligned} &\forall \delta \in [\![\Delta]\!].\ \forall (E, S) \in [\![\phi]\!].\ \forall \vartheta \in [\![\psi]\!].\ \forall l \in \mathbb{L}_s \setminus \mathrm{Dom}(S).\ \forall v \in \mathbb{V}. \\ &\quad [\![\Delta; \phi, \mathsf{x}; \psi \vdash \mathsf{P} : \omega]\!](\delta; (E[x \mapsto l], S[l \mapsto v]); \vartheta) = [\![\Delta; \phi; \psi, \mathsf{x} : \mathtt{Val}, \mathsf{y} : \mathtt{Loc} \vdash \mathsf{P}[\mathsf{y}/\&\mathsf{x}] : \omega]\!](\delta; (E, S); \vartheta[\mathsf{x} \mapsto v, \mathsf{y} \mapsto l]) \end{aligned}$$

Corollary 1 (Splitting)**.** *If* $\Delta; \phi; \psi, \mathsf{x} : \mathtt{Val} \vdash \mathsf{P} : \omega$ *then,*

$$\begin{aligned} &\forall \delta \in [\![\Delta]\!].\ \forall (E, S) \in [\![\phi]\!].\ \forall \vartheta \in [\![\psi]\!].\ \forall l \in \mathbb{L}_s \setminus \mathrm{Dom}(S).\ \forall v \in \mathrm{Val}. \\ &\quad [\![\Delta; \phi, \mathsf{x}; \psi \vdash \mathsf{P} : \omega]\!](\delta; (E[\mathsf{x} \mapsto l], S[l \mapsto v]); \vartheta) = [\![\Delta; \phi; \psi, \mathsf{x} : \mathtt{Val} \vdash \mathsf{P} : \omega]\!](\delta; (E, S); \vartheta[\mathsf{x} \mapsto v]) \end{aligned}$$

Lemma 13. *If* $\Delta; \phi; \psi \vdash \mathsf{L} : \mathtt{Loc}$ *and* $\Delta; \phi; \psi, \mathsf{x} : \mathtt{Val} \vdash \mathsf{P} : \mathtt{Prop}$ *then,*

$$\begin{aligned} &\forall \delta \in [\![\Delta]\!].\ \forall (E, S) \in [\![\phi]\!].\ \forall \vartheta \in [\![\psi]\!]. \\ &\quad [\![\Delta; \phi; \psi \vdash \mathtt{lookup}\ \mathsf{L}\ \mathtt{as}\ \mathsf{x}\ \mathtt{in}\ \mathsf{P} : \mathtt{Prop}]\!](\delta; (E, S); \vartheta) = \\ &\qquad \{(n, C, H) \in \mathsf{N} \times \mathbb{S} \times \mathbb{H} \mid l \in \mathrm{Dom}(C) \wedge \\ &\qquad\quad (n, C \setminus l, H) \in [\![\Delta; \phi; \psi, \mathsf{x} : \mathtt{Val} \vdash \mathsf{P} : \mathtt{Prop}]\!](\delta; (E, S); \vartheta[\mathsf{x} \mapsto C(l)])\} \end{aligned}$$

where $l = [\![\Delta; \phi; \psi \vdash \mathsf{L} : \mathtt{Loc}]\!](\delta; (E, S); \vartheta)$.

3 Specification Logic

3.1 Syntax

$$\begin{array}{lcll} \mathsf{S}, \mathsf{T} & ::= & \{\mathsf{P}\}\mathtt{s}\{\mathsf{Q}\} \triangleleft \mathsf{M} \mid \{\mathsf{P}\}\mathtt{s}\{\mathtt{d}.\mathsf{Q}\} \triangleleft \mathsf{M} & \text{Specifications} \\ \mathsf{M} & \in & \mathcal{P}_{fin}(\mathbb{A}_p) & \end{array}$$

$$\begin{array}{lcll} MS & ::= & \mathsf{C}\langle\Delta\rangle.\mathsf{m} : \langle(\phi;\psi).\{\mathsf{P}\}\_\{\mathtt{d}.\mathsf{Q}\}\rangle & \text{method specification} \\ \Gamma & ::= & \Gamma, MS \mid \epsilon & \text{program context} \end{array}$$

We use the notation $\Gamma(\mathsf{C})$ to lookup C's type variables and $\Gamma(\mathsf{C}, \mathsf{m})$ to lookup m's specification.

3.2 Typing rules

Well-formed Specifications $\boxed{\Delta; \phi; \psi \vdash \mathsf{S} : \mathtt{Spec}}$

$$\frac{\Delta; \phi; \psi \vdash \mathsf{P} : \mathtt{Prop} \qquad \Delta; \phi; \psi \vdash \mathsf{Q} : \mathtt{Prop} \qquad \mathsf{M} \subseteq \phi}{\Delta; \phi; \psi \vdash \{\mathsf{P}\}\mathtt{s}\{\mathsf{Q}\} \triangleleft \mathsf{M} : \mathtt{Spec}}$$

$$\frac{\Delta; \phi; \psi \vdash \mathsf{P} : \mathtt{Prop} \qquad \Delta; \phi; \psi, \mathtt{d} : \mathtt{Val} \vdash \mathsf{Q} : \mathtt{Prop} \qquad \mathsf{M} \subseteq \phi}{\Delta; \phi; \psi \vdash \{\mathsf{P}\}\mathsf{B}\{\mathtt{d}.\mathsf{Q}\} \triangleleft \mathsf{M} : \mathtt{Spec}}$$

Well-formed Contexts $\boxed{\Gamma : \mathtt{Context}}$

$$\frac{\Delta; -; \psi, \phi, \mathtt{this} \vdash \mathsf{P} : \mathtt{Prop} \qquad \Delta; -; \psi, \phi, \mathtt{this}, \mathtt{d} \vdash \mathsf{Q} : \mathtt{Prop}}{\mathsf{C}\langle\Delta\rangle.\mathsf{m} : \langle(\phi;\psi).\{\mathsf{P}\}\_\{\mathtt{d}.\mathsf{Q}\}\rangle : \mathtt{Context\text{-}Spec}}$$

Note that we do not allow P and Q to refer to the location of `this` or ϕ.

$$\frac{}{\epsilon : \mathtt{Context}} \qquad \frac{\Gamma : \mathtt{Context} \qquad MS : \mathtt{Context\text{-}Spec}}{\Gamma, MS : \mathtt{Context}}$$

3.3 Proof rules

Statements $\boxed{\Gamma; \phi; \psi \vdash \{\mathsf{P}\}\mathsf{s}\{\mathsf{Q}\} \triangleleft \mathsf{M}}$

$$\frac{\Delta; \phi, \mathsf{x}, \mathsf{y}; \psi \vdash \mathsf{P} : \texttt{Prop}}{\Gamma; \Delta; \phi, \mathsf{x}, \mathsf{y}; \psi \vdash \{[\mathsf{y}/\mathsf{x}]\mathsf{P}\}\mathsf{x} \texttt{ = } \mathsf{y}\{\mathsf{P}\} \triangleleft \{\mathsf{x}\}}$$

$$\frac{\Delta; \phi, \mathsf{x}; \psi \vdash \mathsf{P} : \texttt{Prop}}{\Gamma; \Delta; \phi, \mathsf{x}; \psi \vdash \{[\texttt{null}/\mathsf{x}]\mathsf{P}\}\mathsf{x} = \texttt{null}\{\mathsf{P}\} \triangleleft \{\mathsf{x}\}}$$

$$\frac{}{\Gamma; \Delta; \phi, \mathsf{x}, \mathsf{y}; \vdash \{\mathsf{x}.\mathsf{f} \mapsto \_\}\mathsf{x}.\mathsf{f} = \mathsf{y}\{\mathsf{x}.\mathsf{f} \mapsto \mathsf{y}\} \triangleleft \emptyset}$$

$$\frac{}{\Gamma; \Delta; \phi, \mathsf{x}, \mathsf{y}; \mathsf{a} \vdash \{\mathsf{y}.\mathsf{f} \mapsto \mathsf{a}\}\mathsf{x} = \mathsf{y}.\mathsf{f}\{\mathsf{y}.\mathsf{f} \mapsto \mathsf{a} \wedge \mathsf{x} = \mathsf{a}\} \triangleleft \{\mathsf{x}\}}$$

$$\frac{fields(\mathsf{C}) = f_1, ..., f_n}{\Gamma; \Delta; \mathsf{x}; - \vdash \{\texttt{emp}\}\mathsf{x} = \texttt{new } \mathsf{C}\langle\Delta\rangle()\{\mathsf{x} : \mathsf{C}\langle\Delta\rangle \wedge \mathsf{x}.f_1 \mapsto \texttt{null} * \cdots * \mathsf{x}.f_n \mapsto \texttt{null}\} \triangleleft \{\mathsf{x}\}}$$

$$\frac{\Gamma(\mathsf{C}) = \Delta \qquad \Gamma(\mathsf{C}, \mathsf{m}) = \langle(\bar{\mathsf{x}}; \psi).\{\mathsf{P}\}\_\{\mathsf{d}.\mathsf{Q}\}\rangle}{\Gamma; \Delta; \mathsf{r}, \mathsf{y}, \bar{\mathsf{u}}; \psi \vdash \{[\bar{\mathsf{u}}/\bar{\mathsf{x}}, \mathsf{y}/\texttt{this}]\mathsf{P} \wedge \mathsf{y} : \mathsf{C}\langle\Delta\rangle\}\mathsf{r} = \mathsf{y}.\mathsf{m}(\bar{\mathsf{u}})\{[\bar{\mathsf{u}}/\bar{\mathsf{x}}, \mathsf{y}/\texttt{this}, \mathsf{r}/\mathsf{d}]\mathsf{Q}\} \triangleleft \{\mathsf{r}\}}$$

$$\frac{\Gamma(\mathsf{C}) = \Delta \qquad \Gamma(\mathsf{C}, \mathsf{m}) = \langle(\bar{\mathsf{u}}; \psi).\{\mathsf{P}\}\_\{\mathsf{d}.\mathsf{Q}\}\rangle}{\Gamma; \Delta; \mathsf{x}, \mathsf{y}; - \vdash \{\mathsf{y} : \mathsf{C}\langle\Delta\rangle\}\mathsf{x} = \mathsf{y}.\mathsf{m}\{\forall\psi.\ \mathsf{x} \mapsto \langle(\bar{\mathsf{u}}).\{\mathsf{P}[\mathsf{y}/\texttt{this}]\}\_\{\mathsf{d}.\mathsf{Q}[\mathsf{y}/\texttt{this}]\}\rangle\} \triangleleft \{\mathsf{x}\}}$$

$$\frac{\begin{array}{c}\bar{\mathsf{u}} \notin \mathsf{M} \qquad \bar{\mathsf{u}} \notin \mathrm{FVA}(\mathsf{P}, \mathsf{Q}) \qquad \bar{\mathsf{y}} \subseteq \mathrm{FV}(\mathsf{B}) \qquad \Gamma; \Delta; \bar{\mathsf{y}}, \bar{\mathsf{u}}; \psi \vdash \{\mathsf{P}\}\mathsf{B}\{\mathsf{d}.\mathsf{Q}\} \triangleleft \mathsf{M}\end{array}}{\begin{array}{l}\Gamma; \Delta; \bar{\mathsf{y}}, \mathsf{x}; \psi, \bar{l} \vdash \{\bar{l} = \&\bar{\mathsf{y}}\} \\ \qquad \mathsf{x} = \texttt{delegate}(\bar{\mathsf{G}}\bar{\mathsf{u}})\ \{\mathsf{B}\} \\ \qquad \{\mathsf{x} \mapsto \langle(\bar{\mathsf{u}}).\{\texttt{lookup } \bar{l} \texttt{ as } \bar{\mathsf{z}} \texttt{ in } \mathsf{P}[\bar{l}/\&\bar{\mathsf{y}}][\bar{\mathsf{z}}/\bar{\mathsf{y}}]\}\_\{\mathsf{d}.\texttt{lookup } \bar{l} \texttt{ as } \bar{\mathsf{z}} \texttt{ in } \mathsf{Q}[\bar{l}/\&\bar{\mathsf{y}}][\bar{\mathsf{z}}/\bar{\mathsf{y}}]\}\rangle\} \triangleleft \{\mathsf{x}\}\end{array}} \text{(anondel)}$$

$$\frac{\mathsf{R} = \mathsf{y} \mapsto \langle(\bar{\mathsf{u}}).\{\mathsf{P}\}\_\{\mathsf{d}.\mathsf{Q}\}\rangle \qquad \mathsf{x} \notin \mathrm{FV}(\mathsf{R}) \qquad \mathsf{y} \in \phi}{\Gamma; \Delta; \phi, \bar{\mathsf{x}}, \mathsf{x}; \psi \vdash \{\mathsf{R} * \mathsf{P}[\bar{\mathsf{x}}/\bar{\mathsf{u}}]\}\mathsf{x} = \mathsf{y}(\bar{\mathsf{x}})\{\mathsf{R} * \mathsf{Q}[\bar{\mathsf{x}}/\bar{\mathsf{u}}, \mathsf{r}/\mathsf{d}]\} \triangleleft \{\mathsf{x}\}} \text{(delcall)}$$

$$\frac{\Gamma; \Delta; \phi, \mathsf{x}, \mathsf{y}; \psi \vdash \{\mathsf{P} \wedge \mathsf{x} = \mathsf{y}\}\mathsf{s}_1\{\mathsf{Q}\} \triangleleft \mathsf{M}_1 \qquad \Gamma; \Delta; \phi, \mathsf{x}, \mathsf{y}; \psi \vdash \{\mathsf{P} \wedge \neg(\mathsf{x} = \mathsf{y})\}\mathsf{s}_2\{\mathsf{Q}\} \triangleleft \mathsf{M}_2}{\Gamma; \Delta; \phi, \mathsf{x}, \mathsf{y}; \psi \vdash \{\mathsf{P}\}\texttt{if } (\mathsf{x} \texttt{ == } \mathsf{y})\ \{\mathsf{s}_1\}\ \texttt{else}\ \{\mathsf{s}_2\}\{\mathsf{Q}\} \triangleleft \mathsf{M}_1 \cup \mathsf{M}_2}$$

Structural Rules $\boxed{\Gamma;\Delta;\phi;\psi \vdash \{\mathsf{P}\}\mathsf{s}\{\mathsf{Q}\} \triangleleft \mathsf{M}}$

$$\frac{\Gamma;\Delta;\phi;\psi,\mathsf{a}:\omega \vdash \{\mathsf{P}\}\mathsf{s}\{\mathsf{Q}\} \triangleleft \mathsf{M}_2 \qquad \mathsf{a} \notin FV(\mathsf{P})}{\Gamma;\Delta;\phi;\psi \vdash \{\mathsf{P}\}\mathsf{s}\{\forall \mathsf{a}:\omega.\mathsf{Q}\} \triangleleft \mathsf{M}_2}$$

$$\frac{\Gamma;\Delta;\phi;\psi \vdash \{\mathsf{P}\}\mathsf{s}_1\{\mathsf{Q}\} \triangleleft \mathsf{M}_1 \qquad \Gamma;\Delta;\phi;\psi \vdash \{\mathsf{Q}\}\mathsf{s}_2\{\mathsf{R}\} \triangleleft \mathsf{M}_2}{\Gamma;\Delta;\phi;\psi \vdash \{\mathsf{P}\}\mathsf{s}_1;\mathsf{s}_2\{\mathsf{R}\} \triangleleft \mathsf{M}_1 \cup \mathsf{M}_2} \quad (\text{seq})$$

$$\frac{\Delta;\phi;\psi \mid \mathsf{P} \vdash \mathsf{P}' \qquad \Gamma;\Delta;\phi;\psi \vdash \{\mathsf{P}'\}\mathsf{s}\{\mathsf{Q}'\} \triangleleft \mathsf{M} \qquad \Delta;\phi;\psi \mid \mathsf{Q}' \vdash \mathsf{Q}}{\Gamma;\Delta;\phi;\psi \vdash \{\mathsf{P}\}\mathsf{s}\{\mathsf{Q}\} \triangleleft \mathsf{M}}$$

$$\frac{\Delta;\phi;\psi \vdash \mathsf{R} : \mathtt{Prop} \qquad \Gamma;\Delta;\phi;\psi \vdash \{\mathsf{P}\}\mathsf{s}\{\mathsf{Q}\} \triangleleft \mathsf{M} \qquad \mathrm{FVV}(\mathsf{R}) \cap \mathsf{M} = \emptyset}{\Gamma;\Delta;\phi;\psi \vdash \{\mathsf{P} * \mathsf{R}\}\mathsf{s}\{\mathsf{Q} * \mathsf{R}\} \triangleleft \mathsf{M}} \quad (\text{frame})$$

$$\frac{\Gamma;\Delta;\phi;\psi \vdash \{\mathsf{P}\}\mathsf{s}\{\mathsf{Q}\} \triangleleft \mathsf{M}}{\Gamma;\Delta;\phi,\mathsf{x};\psi \vdash \{\mathsf{P}\}\mathsf{s}\{\mathsf{Q}\} \triangleleft \mathsf{M}}$$

$$\frac{\Gamma;\Delta;\phi;\psi \vdash \{\mathsf{P}\}\mathsf{s}\{\mathsf{Q}\} \triangleleft \mathsf{M}}{\Gamma;\Delta;\pi(\phi);\pi(\psi) \vdash \{\pi(\mathsf{P})\}\pi(\mathsf{s})\{\pi(\mathsf{Q})\} \triangleleft \pi(\mathsf{M})} \quad (\alpha)$$

$$\frac{\Gamma;\Delta;\phi;\psi \vdash \{\mathsf{P}_1\}\mathsf{s}\{\mathsf{Q}_1\} \triangleleft \mathsf{M}_1 \qquad \Gamma;\Delta;\phi;\psi \vdash \{\mathsf{P}_2\}\mathsf{s}\{\mathsf{Q}_2\} \triangleleft \mathsf{M}_2 \qquad op \in \{\wedge,\vee\}}{\Gamma;\Delta;\phi;\psi \vdash \{\mathsf{P}_1\ op\ \mathsf{P}_2\}\mathsf{s}\{\mathsf{Q}_1\ op\ \mathsf{Q}_2\} \triangleleft \mathsf{M}_1 \cup \mathsf{M}_2}$$

$$\frac{\Gamma;\Delta;\phi;\psi,\mathsf{x}:\omega \vdash \{\mathsf{P}\}\mathsf{s}\{\mathsf{Q}\} \triangleleft \mathsf{M} \qquad \Delta;\phi;\psi \vdash \mathsf{R} : \omega \qquad \mathrm{FV}(\mathsf{R}) \cap \mathsf{M} = \emptyset}{\Gamma;\Delta;\phi;\psi \vdash \{\mathsf{P}[\mathsf{R}/\mathsf{x}]\}\mathsf{s}\{\mathsf{Q}[\mathsf{R}/\mathsf{x}]\} \triangleleft \mathsf{M}}$$

$$\frac{\Gamma;\Delta;\phi;\psi \vdash \{\mathtt{lookup}\ l\ \mathtt{as}\ \mathsf{x}\ \mathtt{in}\ \mathsf{P}\}\mathsf{s}\{\mathtt{lookup}\ l\ \mathtt{as}\ \mathsf{x}\ \mathtt{in}\ \mathsf{Q}\} \triangleleft \mathsf{M}}{\Gamma;\Delta;\phi,\mathsf{x};\psi \vdash \{\&\mathsf{x} = l \wedge \mathsf{P}\}\mathsf{s}\{\mathsf{Q}\} \triangleleft \mathsf{M} \cup \{\mathsf{x}\}} \quad (\text{lookup})$$

Method definitions $\boxed{\Gamma \vdash \mathsf{M} : \Gamma'}$

$$\frac{}{\Gamma;\Delta,\phi,\mathsf{x};\psi \vdash \{\mathsf{P}[\mathsf{x}/\mathsf{d}]\}\mathtt{return}\ \mathsf{x};\{\mathsf{d}.\mathsf{P}\} \triangleleft \emptyset}$$

$$\frac{\Gamma;\Delta;\phi;\psi \vdash \{\mathsf{P}\}\mathsf{s}\{\mathsf{Q}\} \triangleleft \mathsf{M}_1 \qquad \Gamma;\Delta;\phi;\psi \vdash \{\mathsf{Q}\}\mathsf{s};\mathtt{return}\ \mathsf{x}\{\mathsf{d}.\mathsf{R}\} \triangleleft \mathsf{M}_2}{\Gamma;\Delta;\phi;\psi \vdash \{\mathsf{P}\}\mathsf{s};\mathsf{s};\mathtt{return}\ \mathsf{x}\{\mathsf{d}.\mathsf{R}\} \triangleleft \mathsf{M}_1 \cup \mathsf{M}_2}$$

$$\frac{\Delta;\phi;\psi \mid \mathsf{P} \vdash \mathsf{P}' \qquad \Gamma;\Delta;\phi;\psi \vdash \{\mathsf{P}'\}\mathsf{B}\{\mathsf{d}.\mathsf{Q}'\} \triangleleft \mathsf{M} \qquad \Delta;\phi;\psi \mid \mathsf{Q}' \vdash \mathsf{Q}}{\Gamma;\Delta;\phi;\psi \vdash \{\mathsf{P}\}\mathsf{B}\{\mathsf{d}.\mathsf{Q}\} \triangleleft \mathsf{M}}$$

$$\frac{\Gamma;\Delta;\phi,\bar{\mathsf{z}};\psi \vdash \{\mathsf{P} \wedge \bar{\mathsf{z}} = \mathtt{null}\}\mathsf{s};\mathtt{return}\ \mathsf{x}\{\mathsf{d}.\mathsf{Q}\} \triangleleft \mathsf{M}}{\Gamma;\Delta;\phi;\psi \vdash \{\mathsf{P}\}\bar{\mathsf{G}}\bar{\mathsf{z}};\mathsf{s};\mathtt{return}\ \mathsf{x}\{\mathsf{d}.\exists \bar{l} : \mathtt{Var}.\ \mathtt{lookup}\ \bar{l}\ \mathtt{as}\ \bar{\mathsf{z}}\ \mathtt{in}\ \mathsf{Q}[\bar{l}/\&\bar{\mathsf{z}}]\} \triangleleft \mathsf{M} \setminus \bar{\mathsf{z}}} \quad (\text{localvar})$$

$$\frac{\begin{array}{c}\mathtt{this},\bar{\mathsf{u}} \notin \mathsf{M} \cup \mathrm{FVA}(\mathsf{P},\mathsf{Q}) \\ MS = \mathsf{C}\langle\Delta\rangle.\mathsf{m} : \langle(\bar{\mathsf{u}};\psi).\{\mathsf{P}\}\_\{\mathsf{d}.\mathsf{Q}\}\rangle \\ \Gamma, MS;\Delta;\bar{\mathsf{u}},\mathtt{this};\psi \vdash \{\mathsf{P}\}\bar{\mathsf{G}}\bar{\mathsf{z}};\mathsf{s};\mathtt{return}\ \mathsf{x}\{\mathsf{d}.\mathsf{Q}\} \triangleleft \mathsf{M}\end{array}}{\Gamma, MS;\Delta \vdash \mathsf{G}\ \mathsf{m}(\bar{\mathsf{G}}\bar{\mathsf{u}})\ \{\bar{\mathsf{G}}\bar{\mathsf{z}};\ \mathsf{s}\ \mathtt{return}\ \mathsf{x};\} : MS}$$

Class definitions $\boxed{\Gamma \vdash \mathsf{L} : \Gamma'}$

$$\frac{\forall i \in \mathrm{Dom}(\bar{\mathsf{M}}).\ \Gamma; \bar{\mathsf{T}} \vdash \mathsf{M}_i : \Gamma_i}{\Gamma \vdash \texttt{class}\ \mathsf{C}\langle\bar{\mathsf{T}}\rangle : \mathsf{D}\ \{\texttt{public}\ \bar{\mathsf{C}}\bar{\mathsf{f}}; \bar{\mathsf{M}}\} : \bar{\Gamma}}$$

Programs $\boxed{\psi \vdash \{\mathsf{P}\}\bar{\mathsf{L}}; \bar{\mathsf{C}}\ \bar{\mathsf{x}}; \mathsf{s}\{\mathsf{Q}\} \triangleleft \mathsf{M}}$

$$\frac{\forall i \in \mathrm{Dom}(\bar{L}).\ \Gamma_i \vdash \mathsf{L}_i : \Gamma_i \qquad \bar{\Gamma}; -; \bar{\mathsf{x}}; \psi \vdash \{\mathsf{P}\}\mathsf{s}\{\mathsf{Q}\} \triangleleft \mathsf{M}}{\bar{\Gamma}; \psi \vdash \{\mathsf{P}\}\bar{\mathsf{L}}; \bar{\mathsf{C}}\ \bar{\mathsf{x}}; \mathsf{s}\{\mathsf{Q}\} \triangleleft \mathsf{M}}$$

3.4 Semantics

Specifications

$$\boxed{[\![\Delta; \phi; \psi \vdash S : \texttt{Spec}]\!] : [\![\Delta]\!] \times [\![\phi]\!] \times [\![\psi]\!] \to \{U \in \mathcal{P}^{\downarrow}(\mathsf{N}) \mid 0 \in U\}}$$

$$\begin{aligned}
&[\![\Delta; \phi; \psi \vdash \{\mathsf{P}\}\mathtt{s}\{\mathsf{Q}\} \triangleleft \mathsf{M} : \texttt{Spec}]\!](\delta; (E, S); \vartheta) = \{n \in \mathsf{N} \mid \\
&\quad \forall m \leq n.\ \forall k \leq m.\ \forall C \in \mathbb{S}.\ \forall H \in \mathbb{H}. \\
&\qquad (m-1, C, H) \in [\![\Delta; \phi; \psi \vdash \mathsf{P} : \texttt{Prop}]\!](\delta; (E, S); \vartheta) \wedge C \# S \ \Rightarrow \\
&\qquad\quad (\delta; E; C \uplus S; H; \mathtt{s})) : \mathtt{safe}_k \ \wedge \\
&\qquad\quad (\delta; E; C \uplus S; H; \mathtt{s}) \Downarrow_k (S'; H') \Rightarrow \\
&\qquad\qquad (m-k; S' \setminus E(\phi); H') \in [\![\Delta; \phi; \psi \vdash \mathsf{Q} : \texttt{Prop}]\!](\delta; (E, S'|_{E(\phi)}); \vartheta) \ \wedge \\
&\qquad\qquad \forall \mathtt{x} \in \phi \setminus \mathsf{M}.\ S(E(\mathtt{x})) = S'(E(\mathtt{x}))\}
\end{aligned}$$

$$\begin{aligned}
&[\![\Delta; \phi; \psi \vdash \{\mathsf{P}\}\bar{\mathsf{G}}\bar{\mathtt{z}};\ \mathtt{s}; \mathtt{return}\ \mathtt{x}\{\mathtt{d}.\mathsf{Q}\} \triangleleft \mathsf{M} : \texttt{Spec}]\!](\delta; (E, S); \vartheta) = \{n \in \mathsf{N} \mid \\
&\quad \forall m \leq n.\ \forall k \leq m.\ \forall C \in \mathbb{S}.\ \forall H \in \mathbb{H}.\ \forall \bar{l}_z \in \mathrm{Loc} \setminus (\mathrm{Dom}(C) \cup \mathrm{Dom}(S)). \\
&\qquad (m-1, C, H) \in [\![\Delta; \phi; \psi \vdash \mathsf{P} : \texttt{Prop}]\!](\delta, (E, S); \vartheta) \wedge C \# S \ \Rightarrow \\
&\qquad\quad (\delta; E'; C \uplus S[\bar{l}_z \mapsto \mathtt{null}]; H; \mathtt{s}) : \mathtt{safe}_k \ \wedge \\
&\qquad\quad (\delta; E'; C \uplus S[\bar{l}_z \mapsto \mathtt{null}]; H; \mathtt{s}) \Downarrow_k (S'; H') \Rightarrow \\
&\qquad\qquad (m-k; S' \setminus E(\phi); H') \in [\![\Delta; \phi; \psi \vdash \mathsf{Q} : \texttt{Prop}]\!](\delta; (E, S'|_{E(\phi)}); \vartheta[\mathtt{d} \mapsto S'(E'(\mathtt{x}))]) \ \wedge \\
&\qquad\qquad \forall \mathtt{x} \in \phi \setminus \mathsf{M}.\ S(E(\mathtt{x})) = S'(E(\mathtt{x}))\}
\end{aligned}$$

where $E' = E[\bar{\mathtt{z}} \mapsto \bar{l}_z]$.

Context Specification

$$\boxed{[\![MS : \texttt{Context-Spec}]\!] : \{U \in \mathcal{P}^{\downarrow}(\mathsf{N}) \mid 0 \in U\}}$$

$$\begin{aligned}
&[\![\mathsf{C}\langle\Delta\rangle.\mathsf{m} : \langle(\bar{\mathsf{u}}; \psi).\{\mathsf{P}\}_\{\mathtt{d}.\mathsf{Q}\}\rangle : \texttt{Context-Spec}]\!] = \{n \in \mathsf{N} \mid \\
&\quad \forall m \leq n.\ \forall k \leq m.\ \forall \bar{\mathtt{x}}, \bar{\mathtt{z}}, \mathtt{s}, \mathtt{r}.\ \forall C \in \mathbb{S}.\ \forall \vartheta \in [\![\psi]\!].\ \forall \delta \in [\![\Delta]\!].\ \forall l_t, \bar{l}_x, \bar{l}_z \notin \mathrm{Dom}(C).\ \forall v_t, \bar{v}_x \in \mathbb{V}. \\
&\quad P(\mathsf{C}) = (\Delta, _) \wedge P(\mathsf{C}, \mathsf{m}) = (\bar{\mathtt{x}}, \bar{\mathtt{z}}, \mathtt{s}, \mathtt{r}) \ \wedge \\
&\quad (m-1, C, H) \in [\![\Delta; -; \psi, \mathtt{this}, \bar{\mathsf{u}} \vdash \mathsf{P} : \texttt{Prop}]\!](\delta; ([], []); \vartheta[\mathtt{this} \mapsto v_t, \bar{\mathsf{u}} \mapsto \bar{v}_x]) \ \Rightarrow \\
&\qquad (\delta; E, C[l_t \mapsto v_t, \bar{l}_x \mapsto \bar{v}_x, \bar{l}_z \mapsto \mathtt{null}], H, \mathtt{s}) : \mathtt{safe}_k \ \wedge \\
&\qquad (\delta; E, C[l_t \mapsto v_t, \bar{l}_x \mapsto \bar{v}_x, \bar{l}_z \mapsto \mathtt{null}], H, \mathtt{s})) \Downarrow_k (S', H') \ \Rightarrow \\
&\qquad\quad (m-k, S' \setminus l_t \cup \bar{l}_z, H') \in [\![\Delta; -; \psi, \mathtt{this}, \bar{\mathsf{u}}, \mathtt{d} \vdash \mathsf{Q} : \texttt{Prop}]\!](\delta, ([], []); \vartheta[\mathtt{this} \mapsto v_t, \bar{\mathsf{u}} \mapsto \bar{v}_x, \mathtt{d} \mapsto S'(E(\mathsf{r}))])\}
\end{aligned}$$

where $E = [\mathtt{this} \mapsto l_t, \bar{\mathtt{x}} \mapsto \bar{l}_x, \bar{\mathtt{z}} \mapsto \bar{l}_z]$.

Context

$$\boxed{[\![\Gamma : \texttt{Context}]\!] : \{U \in \mathcal{P}^{\downarrow}(\mathsf{N}) \mid 0 \in U\}}$$

$$[\![\Gamma : \texttt{Context}]\!] = \bigcap_{MS \in \Gamma} [\![MS : \texttt{Context-Spec}]\!]$$

Entailment

$$\boxed{[\![\Gamma; \Delta; \phi; \psi \vdash \mathsf{S} : \texttt{Spec}]\!] : 2}$$

$$\begin{aligned}
&[\![\Gamma; \Delta; \phi; \psi \vdash \mathsf{S} : \texttt{Spec}]\!] = \forall n \in \mathsf{N}.\ \forall (E, S) \in [\![\phi]\!].\ \forall \vartheta \in [\![\psi]\!].\ \forall \delta \in [\![\Delta]\!]. \\
&\qquad n \in [\![\Gamma : \texttt{Context}]\!] \Rightarrow n + 1 \in [\![\Gamma; \Delta; \phi; \psi \vdash \mathsf{S} : \texttt{Spec}]\!](\delta; (E, S); \vartheta)
\end{aligned}$$

Others

$$[\![\Gamma; \bar{\mathsf{T}} \vdash \texttt{public}\ \mathsf{C}\ \mathsf{m}(\bar{\mathsf{C}}\bar{\mathsf{u}})\ \mathsf{B} : MS]\!] = \forall n \in \mathsf{N}.\ n \in [\![\Gamma : \texttt{Context}]\!] \Rightarrow n+1 \in [\![\mathsf{C}\langle\bar{\mathsf{T}}\rangle.\mathsf{m} : MS : \texttt{Context-Spec}]\!]$$

$$\begin{aligned}[\![\Gamma \vdash \texttt{class}\ \mathsf{C}\langle\bar{\mathsf{T}}\rangle : \mathsf{G}\ \{\texttt{public}\ \bar{\mathsf{C}}\bar{\mathsf{f}}; \bar{\mathsf{M}}\} : MS_K, \bar{MS}]\!] = \\ \mathrm{Dom}(\bar{MS}) = \mathrm{Dom}(\bar{\mathsf{M}}) \wedge \forall i \in \mathrm{Dom}(\bar{\mathsf{M}}).\ [\![\Gamma; \bar{\mathsf{T}} \vdash \bar{\mathsf{M}}_i : \bar{MS}_i]\!]\end{aligned}$$

$$[\![\bar{\Gamma}; \psi \vdash \{\mathsf{P}\}\bar{\mathsf{L}}; \bar{\mathsf{C}}\bar{\mathsf{x}}; \mathsf{s}\{\mathsf{Q}\} \triangleleft \mathsf{M}]\!] = [\![\bar{\Gamma}; -; \bar{\mathsf{x}}; \psi \vdash \{\mathsf{P}\}\mathsf{s}\{\mathsf{Q}\} \triangleleft \mathsf{M}]\!] \wedge \forall i \in \mathrm{Dom}(\bar{\mathsf{L}}).\ [\![\Gamma \vdash \bar{\mathsf{L}}_i : \Gamma_i]\!]$$

3.5 Metatheory

Lemma 14. *If* $\Gamma; \Delta; \phi; \psi \vdash \{\mathsf{P}\}\mathsf{s}\{\mathsf{Q}\} \triangleleft \mathsf{M}$ *then* $FV(\mathsf{s}) \subseteq \phi$.

Lemma 15. *If* $\forall i \in \mathrm{Dom}(\bar{\mathsf{L}}).\ [\![\Gamma \vdash \bar{\mathsf{L}}_i : \Gamma_i]\!]$ *then* $[\![\Gamma : \mathit{Context}]\!] = \mathsf{N}$.

Lemma 16. *Rule* (α) *is sound.*

$$\forall \pi \in \mathrm{Perm}(\mathbb{A}_p).\ [\![\Gamma; \Delta; \phi; \psi \vdash \{\mathsf{P}\}\mathsf{s}\{\mathsf{Q}\} \triangleleft \mathsf{M}]\!] = [\![\Gamma; \Delta; \pi(\phi); \pi(\psi) \vdash \{\pi(\mathsf{P})\}\pi(\mathsf{s})\{\pi(\mathsf{Q})\} \triangleleft \pi(\mathsf{M})]\!]$$

Proof. Let $n, m, k \in \mathsf{N}$ such that $k \leq m \leq n+1$. Assume $n \in [\![\Gamma : \mathtt{Context}]\!]$,

$$(m-1, C, H) \in [\![\Delta; \pi(\phi); \pi(\psi) \vdash \pi(\mathsf{P}) : \mathtt{Prop}]\!](\delta; (E, S); \vartheta)$$

and $C \# S$. By alpha-renaming and equivariance it follows that,

$$(m-1, C, \pi^{-1}(H)) \in [\![\Delta; \phi; \psi \vdash \mathsf{P} : \mathtt{Prop}]\!](\delta; (\pi^{-1}(E), S); \pi^{-1}(\vartheta))$$

Hence,

$$(\pi^{-1}(E), C \uplus S, \pi^{-1}(H), \mathsf{s}) : \mathtt{safe}_m$$

and thus by alpha-renaming,

$$(E, C \uplus S, H, \pi(\mathsf{s})) : \mathtt{safe}_m$$

Correctness: If

$$(E, C \uplus S, H, \pi(\mathsf{s})) \Downarrow_k (S', H')$$

then by alpha-renaming,

$$(\pi^{-1}(E), C \uplus S, \pi^{-1}(H), \mathsf{s}) \Downarrow_k (S', \pi^{-1}(H'))$$

and thus,

$$(m-k, S' \setminus \pi^{-1}(E)(\phi), \pi^{-1}(H')) \in [\![\Delta; \phi; \psi \vdash \mathsf{Q} : \mathtt{Prop}]\!](\delta; (\pi^{-1}(E), S'|_{\pi^{-1}(E)(\phi)}); \pi^{-1}(\vartheta))$$

and by alpha-renaming and equivariance we thus have that,

$$(m-k, S' \setminus E(\pi(\phi)), H') \in [\![\Delta; \pi(\phi); \pi(\psi) \vdash \pi(\mathsf{Q}) : \mathtt{Prop}]\!](\delta; (E, S'|_{E(\pi(\phi))}); \vartheta)$$

□

Lemma 17. *Rule* (frame) *is sound.*

$$\frac{\Gamma; \Delta; \phi; \psi \vdash \mathsf{R} : \mathit{Prop} \qquad \Gamma; \Delta; \phi; \psi \vdash \{\mathsf{P}\}\mathtt{s}\{\mathsf{Q}\} \triangleleft \mathsf{M} \qquad \mathrm{FVV}(\mathsf{R}) \cap \mathsf{M} = \emptyset}{\Gamma; \Delta; \phi; \psi \vdash \{\mathsf{P} * \mathsf{R}\}\mathtt{s}\{\mathsf{Q} * \mathsf{R}\} \triangleleft \mathsf{M}}$$

Proof. Let $n, m, k \in \mathsf{N}$ such that $k \leq m \leq n+1$. Assume $n \in [\![\Gamma : \mathtt{Context}]\!]$,

$$(m-1, C_1, H_1) \in [\![\Delta; \phi; \psi \vdash \mathsf{P} : \mathtt{Prop}]\!](\delta; (E, S); \vartheta)$$

$$(m-1, C_2, H_2) \in [\![\Delta; \phi; \psi \vdash \mathsf{R} : \mathtt{Prop}]\!](\delta; (E, S); \vartheta)$$

$C_1 \# C_2$, $H_1 \# H_2$, and $(C_1 \uplus C_2) \# S$.

By assumption,

$$[\![\Delta; \phi; \psi \vdash \{\mathsf{P}\}\mathtt{s}\{\mathsf{Q}\} \triangleleft \mathsf{M}]\!](\delta; (E, S); \vartheta, n+1)$$

and thus,

$$(E, C_1 \uplus S, H_1, \mathtt{s}) : \mathtt{safe}_m$$

and by safety monotonicity,

$$(E, C_1 \uplus C_2 \uplus S, H_1 \uplus H_2, \mathtt{s}) : \mathtt{safe}_m$$

Correctness: If

$$(E, C_1 \uplus C_2 \uplus S, H_1 \uplus H_2, \mathtt{s}) \Downarrow_k (S', H')$$

then by the stack and heap frame properties it follows that there exists a S_1' and H_1' such that,

$$(E, C_1 \uplus S, H_1, \mathtt{s}) \Downarrow_k (S_1', H_1')$$

and $S' = C_2 \uplus S_1'$ and $H' = H_2 \uplus H_1'$. Hence,

$$(m-k, S_1' \setminus E(\phi), H_1') \in [\![\Delta; \phi; \psi \vdash \mathsf{Q} : \mathtt{Prop}]\!](\delta; (E, S'|_{E(\phi)}); \vartheta)$$

Furthermore,

$$[\![\Delta; \phi; \psi \vdash \mathsf{R} : \mathtt{Prop}]\!](\delta; (E, S); \vartheta) = [\![\Delta; \phi; \psi \vdash \mathsf{R} : \mathtt{Prop}]\!](\delta; (E, S'|_{E(\phi)}); \vartheta)$$

since $\forall \mathsf{x} \in \mathrm{FVV}(\mathsf{R})$. $S(E(\mathsf{x})) = S'(E(\mathsf{x}))$ and thus, by upwards-closure,

$$(m-k, C_2 \setminus E(\phi), H_2) \in [\![\Delta; \phi; \psi \vdash \mathsf{R} : \mathtt{Prop}]\!](\delta; (E, S'|_{E(\phi)}); \vartheta)$$

and thus finally,

$$(m-k, (S_1' \uplus C_2) \setminus E(\phi), H_1' \uplus H_2) \in [\![\Delta; \phi; \psi \vdash \mathsf{P} * \mathsf{R} : \mathtt{Prop}]\!](\delta; (E, S'|_{E(\phi)}); \vartheta)$$

□

Lemma 18. *Rule* (seq) *is sound.*

$$\frac{\Gamma;\Delta;\phi;\psi \vdash \{\mathsf{P}\}\mathsf{s}_1\{\mathsf{Q}\} \triangleleft \mathsf{M}_1 \qquad \Gamma;\Delta;\phi;\psi \vdash \{\mathsf{Q}\}\mathsf{s}_2\{\mathsf{R}\} \triangleleft \mathsf{M}_2}{\Gamma;\Delta;\phi;\psi \vdash \{\mathsf{P}\}\mathsf{s}_1;\mathsf{s}_2\{\mathsf{R}\} \triangleleft \mathsf{M}_1 \cup \mathsf{M}_2}$$

Proof. Let $n, m, k \in \mathsf{N}$ such that $k \leq m \leq n+1$. Assume $n \in [\![\Gamma : \texttt{Context}]\!]$,

$$(m-1, C, H) \in [\![\Delta;\phi;\psi \vdash \mathsf{P} : \texttt{Prop}]\!](\delta;(E,S);\vartheta)$$

and $C \# S$.

Safety: By assumption,

$$[\![\Delta;\phi;\psi \vdash \{\mathsf{P}\}\mathsf{s}_1\{\mathsf{Q}\} \triangleleft \mathsf{M}_1]\!](\delta;(E,S);\vartheta;n+1)$$

and thus,

$$(E; C \uplus S; H; \mathsf{s}_1) : \texttt{safe}_m$$

Hence, for any $l \leq k$ if $(E; C \uplus S; H; \mathsf{s}_1\ \mathsf{s}_2) \Downarrow_l \text{err}$ then there exists l_1, l_2, S', and H' such that,

$$(E; C \uplus S; H; \mathsf{s}_1) \Downarrow_{l_1} (S', H')$$

$$(E; S'; H'; \mathsf{s}_2) \Downarrow_{l_2} \text{err}$$

and $l = l_1 + l_2$. Hence,

$$(m - l_1; S' \setminus E(\phi); H') \in [\![\Delta;\phi;\psi \vdash \mathsf{Q} : \texttt{Prop}]\!](\delta;(E, S'|_{E(\phi)});\vartheta)$$

and thus

$$(E; (S' \setminus E(\phi)) \uplus S'|_{E(\phi)}; H', \mathsf{s}_2) : \texttt{safe}_{m-l_1+1}$$

Since $l_1 + l_2 = l \leq k \leq m$ it follows that $l_2 \leq m - l_1 + 1$ and thus

$$(E; S'; H', \mathsf{s}_2) \not\Downarrow_{l_2} \text{err}$$

which is a contradiction.

Correctness: If

$$(E; C \uplus S; H; s_1; s_2) \Downarrow_k (S', H')$$

then there exists k_1, k_2, S'', and H'' such that,

$$(E; C \uplus S; H; s_1) \Downarrow_{k_1} (S'', H'')$$

$$(E; S'', H''; s_2) \Downarrow_{k_2} (S', H')$$

and $k = k_1 + k_2$. Hence,

$$(m - k_1; S'' \setminus E(\phi); H'') \in [\![\Delta;\phi;\psi \vdash \mathsf{Q} : \texttt{Prop}]\!](\delta;(E, S''|_{E(\phi)});\vartheta)$$

Furthermore, by assumption,

$$[\![\Delta;\phi;\psi \vdash \{\mathsf{Q}\}\mathsf{s}_2\{\mathsf{R}\} \triangleleft \mathsf{M}_2]\!](\delta;(E, S''|_{E(\phi)});\vartheta;n+1)$$

Since $1 \leq k_1$ we have it follows that $k_2 \leq (m - k_1 + 1) \leq n + 1$ and thus,

$$(m - k_1 + 1 - k_2; S' \setminus E(\phi); H') \in [\![\Delta;\phi;\psi \vdash \mathsf{R} : \texttt{Prop}]\!](\delta;(E, S'|_{E(\phi)});\vartheta)$$

and by upwards-closure:

$$(m - k; S' \setminus E(\phi); H') \in [\![\Delta;\phi;\psi \vdash \mathsf{R} : \texttt{Prop}]\!](\delta;(E, S'|_{E(\phi)});\vartheta)$$

□

Lemma 19. *Rule* (lookup) *is sound.*

$$\frac{\Gamma;\Delta;\phi;\psi \vdash \{\,\mathit{lookup}\ l\ \mathit{as}\ \mathsf{x}\ \mathit{in}\ \mathsf{P}\}\mathsf{s}\{\,\mathit{lookup}\ l\ \mathit{as}\ \mathsf{x}\ \mathit{in}\ \mathsf{Q}\} \triangleleft \mathsf{M}}{\Gamma;\Delta;\phi,\mathsf{x};\psi \vdash \{\&\mathsf{x} = l \wedge \mathsf{P}\}\mathsf{s}\{\mathsf{Q}\} \triangleleft \mathsf{M} \cup \{\mathsf{x}\}}$$

Proof. Let $n, m, k \in \mathsf{N}$ such that $k \leq m \leq n+1$. Assume $n \in [\![\Gamma : \texttt{Context}]\!]$,

$$(m-1; C; H) \in [\![\Delta;\phi,\mathsf{x};\psi \vdash \&\mathsf{x} = l \wedge \mathsf{P} : \texttt{Prop}]\!](\delta;(E,S);\vartheta)$$

and $C \# S$. Then $\vartheta(l) = E(\mathsf{x})$ and,

$$(m-1; C; H) \in [\![\Delta;\phi,\mathsf{x};\psi \vdash \mathsf{P} : \texttt{Prop}]\!](\delta;(E,S);\vartheta)$$

and by splitting,

$$(m-1; C; H) \in [\![\Delta;\phi;\psi,\mathsf{x} \vdash \mathsf{P} : \texttt{Prop}]\!](\delta;(E|_\phi, S \setminus E(\mathsf{x}));\vartheta[\mathsf{x} \mapsto S(E(\mathsf{x}))])$$

By the definition of `lookup` it thus follows that,

$$(m-1; C[E(\mathsf{x}) \mapsto S(E(\mathsf{x}))]; H) \in [\![\Delta;\phi;\psi \vdash \texttt{lookup}\ l\ \texttt{as}\ \mathsf{x}\ \texttt{in}\ \mathsf{P} : \texttt{Prop}]\!](\delta;(E|_\phi, S \setminus E(\mathsf{x}));\vartheta)$$

and by assumption:

$$[\![\Delta;\phi;\psi \vdash \{\texttt{lookup}\ l\ \texttt{as}\ \mathsf{x}\ \texttt{in}\ \mathsf{P}\}\mathsf{s}\{\texttt{lookup}\ l\ \texttt{as}\ \mathsf{x}\ \texttt{in}\ \mathsf{Q}\} \triangleleft \mathsf{M}]\!](\delta;(E|_\phi; S \setminus E(\mathsf{x}));\vartheta; n+1)$$

Safety: Hence,

$$(E|_\phi; (C[E(\mathsf{x}) \mapsto S(E(\mathsf{x}))) \uplus (S \setminus E(\mathsf{x})); H; \mathsf{s}) : \texttt{safe}_k$$

and by weakening,

$$(E; C \uplus S; H; \mathsf{s}) : \texttt{safe}_k$$

Correctness: Furthermore, if

$$(E; C \uplus S; H; \mathsf{s}) \Downarrow_k (S', H')$$

then since $\mathsf{x} \notin \mathrm{FV}(\mathsf{s})$ it follows that,

$$(E|_\phi; C \uplus S; H; \mathsf{s}) \Downarrow_k (S', H')$$

and thus,

$$(m-k; S' \setminus E(\phi); H') \in [\![\Delta;\phi;\psi \vdash \texttt{lookup}\ l\ \texttt{as}\ \mathsf{x}\ \texttt{in}\ \mathsf{Q} : \texttt{Prop}]\!](\delta;(E|_\phi, S'|_{E(\phi)});\vartheta)$$

By the definition of `lookup` we thus have that $E(\mathsf{x}) \in \mathrm{Dom}(S' \setminus E(\phi))$ and

$$(m-k; S' \setminus E(\phi,\mathsf{x}); H') \in [\![\Delta;\phi;\psi,\mathsf{x} \vdash \mathsf{Q} : \texttt{Prop}]\!](\delta;(E|_\phi, S'|_{E(\phi)});\vartheta[\mathsf{x} \mapsto (S' \setminus E(\phi))(E(\mathsf{x}))])$$

and by splitting,

$$(m-k; S' \setminus E(\phi,\mathsf{x}); H') \in [\![\Delta;\phi,\mathsf{x};\psi \vdash \mathsf{Q} : \texttt{Prop}]\!](\delta;(E, S'|_{E(\phi,\mathsf{x})});\vartheta)$$

□

Lemma 20. *Rule* (anondel) *is sound.*

$$\frac{\bar{\mathsf{u}} \cup \bar{\mathsf{y}} = \mathrm{FV}(\mathsf{B}) \qquad \Gamma; \Delta; \bar{\mathsf{y}}, \bar{\mathsf{u}}; \psi \vdash \{\mathsf{P}\}\mathsf{B}\{\mathsf{d}.\mathsf{Q}\} \triangleleft \mathsf{M} \qquad \bar{\mathsf{u}} \notin \mathsf{M} \qquad \Delta; \bar{\mathsf{y}}; \psi, \bar{\mathsf{u}} \vdash \mathsf{P} : \mathit{Prop} \qquad \Delta; \bar{\mathsf{y}}; \psi, \bar{\mathsf{u}}, \mathsf{d} \vdash \mathsf{Q} : \mathit{Prop}}{\Gamma; \Delta; \bar{\mathsf{y}}, \mathsf{x}; \psi, \bar{l} \vdash \{\bar{l} = \&\bar{\mathsf{y}}\}\mathsf{x} = \lambda\bar{\mathsf{u}}.\ \{\mathsf{B}\}; \{\mathsf{x} \mapsto \langle(\bar{\mathsf{u}}).\{\mathit{lookup}\ \bar{l}\ \mathit{as}\ \bar{\mathsf{z}}\ \mathit{in}\ \mathsf{P}[\bar{l}/\&\bar{\mathsf{y}}][\bar{\mathsf{z}}/\bar{\mathsf{y}}]\}\_\{\mathsf{d}.\mathit{lookup}\ \&l\ \mathit{as}\ \bar{\mathsf{z}}\ \mathit{in}\ \mathsf{Q}[\bar{l}/\&\bar{\mathsf{y}}][\bar{\mathsf{z}}/\bar{\mathsf{y}}]\}\rangle\} \triangleleft \{\mathsf{x}\}}$$

Proof. Let $n, m, k \in \mathsf{N}$ such that $k \leq m \leq n+1$. Assume $n \in [\![\Gamma : \mathtt{Context}]\!]$,

$$(m-1, C, H) \in [\![\Delta; \bar{\mathsf{y}}, \mathsf{x}; \psi, \bar{l} \vdash \bar{l} = \&\bar{\mathsf{y}} : \mathtt{Prop}]\!](\delta; (E, S); \vartheta)$$

and $C \# S$. If,

$$(E; C \uplus S; H; \mathsf{x} = \lambda\bar{\mathsf{u}}.\{\mathsf{B}\};) \Downarrow_k (S', H')$$

then $S' = C \uplus S[E(\mathsf{x}) \mapsto l]$ and $H' = H[l \mapsto (\delta, E_c, \mathsf{B})])$ where $E_c = E|_{\bar{\mathsf{y}}}$, $k = 1$ and $l \notin \mathrm{Dom}(C \uplus S)$.

Let $k' \leq m' \leq m-1$, $C_c \in \mathbb{S}, H_c \in \mathbb{H}, \bar{l}_x, \bar{l}_z \in \mathrm{Loc} \setminus (\mathrm{Dom}(C_c) \cup \mathrm{Rng}(E_c)), \bar{v}_x \in \mathbb{V}$ such that,

$$(m'-1, C_c, H_c) \in [\![\Delta; \bar{\mathsf{y}}, \mathsf{x}; \psi, \bar{l}, \bar{\mathsf{u}} \vdash \mathtt{lookup}\ \bar{l}\ \mathtt{as}\ \bar{\mathsf{z}}\ \mathtt{in}\ \mathsf{P}[\bar{l}/\&\bar{\mathsf{y}}][\bar{\mathsf{z}}/\bar{\mathsf{y}}] : \mathtt{Prop}]\!](\delta; (E, S'); \vartheta[\bar{\mathsf{u}} \mapsto \bar{v}_x])$$

Hence,

$$(m'-1, C_c \setminus E(\bar{\mathsf{y}}), H_c) \in [\![\Delta; \bar{\mathsf{y}}, \mathsf{x}; \psi, \bar{l}, \bar{\mathsf{u}}, \bar{\mathsf{z}} \vdash \mathsf{P}[\bar{l}/\&\bar{\mathsf{y}}][\bar{\mathsf{z}}/\bar{\mathsf{y}}] : \mathtt{Prop}]\!](\delta; (E, S'); \vartheta[\bar{\mathsf{u}} \mapsto \bar{v}_x, \bar{\mathsf{z}} \mapsto C_c(E(\bar{\mathsf{y}}))])$$

and by strengthening and renaming,

$$(m'-1, C_c \setminus E(\bar{\mathsf{y}}), H_c) \in [\![\Delta; -; \psi, \bar{l}, \bar{\mathsf{u}}, \bar{\mathsf{y}} \vdash \mathsf{P}[\bar{l}/\&\bar{\mathsf{y}}] : \mathtt{Prop}]\!](\delta; ([], []); \vartheta[\bar{\mathsf{u}} \mapsto \bar{v}_x, \bar{\mathsf{y}} \mapsto C_c(E(\bar{\mathsf{y}}))])$$

and splitting,

$$(m'-1, C_c \setminus E(\bar{\mathsf{y}}), H_c) \in [\![\Delta; \bar{\mathsf{y}}, \bar{\mathsf{u}}; \psi \vdash \mathsf{P} : \mathtt{Prop}]\!](\delta; ([\bar{\mathsf{y}} \mapsto E(\bar{\mathsf{y}}), \bar{\mathsf{u}} \mapsto \bar{l}_u], [E(\bar{\mathsf{y}}) \mapsto C_c(E(\bar{\mathsf{y}})), \bar{l}_u \mapsto \bar{v}_x]); \vartheta|_\psi)$$

Futhermore, by assumption,

$$[\![\Delta; \bar{\mathsf{y}}, \bar{\mathsf{u}}; \psi \vdash \{\mathsf{P}\}\mathsf{B}\{\mathsf{Q}\} \triangleleft \mathsf{M}]\!](\delta; ([\bar{\mathsf{y}} \mapsto E(\bar{\mathsf{y}}), \bar{\mathsf{u}} \mapsto \bar{l}_u], [E(\bar{\mathsf{y}}) \mapsto C_c(E(\bar{\mathsf{y}})), \bar{l}_u \mapsto \bar{v}_x]); \vartheta|_\psi; n+1)$$

and since $k' \leq m' \leq n+1$,

$$(\delta, E'; C_c \setminus E(\bar{\mathsf{y}}) \uplus [E(\bar{\mathsf{y}}) \mapsto C_c(E(\bar{\mathsf{y}})), \bar{l}_u \mapsto \bar{v}_x, \bar{l}_z \mapsto \mathtt{null}]; H_c, \mathsf{s}) : \mathtt{safe}_{k'}$$

where $E' = [\bar{\mathsf{y}} \mapsto E(\bar{\mathsf{y}}), \bar{\mathsf{u}} \mapsto \bar{l}_u, \bar{\mathsf{z}} \mapsto \bar{l}_z]$. Safety follows by safety monotonicity.

Correctness: If,

$$(\delta, E'; C_c[\bar{l}_u \mapsto \bar{v}_x, \bar{l}_z \mapsto \mathtt{null}]; H_c; \mathsf{s}) \Downarrow_{k'} (S'', H'')$$

then,

$$(m'-k', S'' \setminus E'(\bar{\mathsf{u}}, \bar{\mathsf{y}}), H'') \in [\![\Delta; \bar{\mathsf{y}}, \bar{\mathsf{u}}; \psi, \mathsf{d} \vdash \mathsf{Q} : \mathtt{Prop}]\!](\delta; ([\bar{\mathsf{y}} \mapsto E(\bar{\mathsf{y}}), \bar{\mathsf{u}} \mapsto \bar{l}_u], S''|_{E'(\bar{\mathsf{u}}, \bar{\mathsf{y}})}); \vartheta|_\psi[\mathsf{d} \mapsto S''(E'(\mathsf{r}))])$$

and since $\bar{\mathsf{u}} \notin \mathsf{M}$, $S''(\bar{l}_u) = \bar{v}_x$. By splitting and renaming we thus have that,

$$(m'-k', S''\setminus E'(\bar{\mathsf{y}}, \bar{\mathsf{u}}), H'') \in [\![\Delta; -; \psi, \bar{l}, \bar{\mathsf{z}}, \bar{\mathsf{u}}, \mathsf{d} \vdash \mathsf{Q}[\bar{l}/\&\bar{\mathsf{y}}][\bar{\mathsf{z}}/\bar{\mathsf{y}}] : \mathtt{Prop}]\!](\delta; ([], []); \vartheta[\bar{\mathsf{z}} \mapsto S''(E(\bar{\mathsf{y}})), \bar{\mathsf{u}} \mapsto \bar{v}_x, \mathsf{d} \mapsto S''(E'(\mathsf{r}))])$$

and weakening,

$$(m'-k', S''\setminus E(\bar{\mathsf{y}}, \bar{\mathsf{u}}), H'') \in [\![\Delta; \bar{\mathsf{y}}, \mathsf{x}; \psi, \bar{l}, \bar{\mathsf{z}}, \bar{\mathsf{u}} \vdash \mathsf{Q}[\bar{l}/\&\bar{\mathsf{y}}][\bar{\mathsf{z}}/\bar{\mathsf{y}}] : \mathtt{Prop}]\!](\delta; (E, S'); \vartheta[\bar{\mathsf{z}} \mapsto S''(E(\bar{\mathsf{y}})), \bar{\mathsf{u}} \mapsto \bar{v}_x, \mathsf{d} \mapsto S''(E'(\mathsf{r}))])$$

and hence,

$$(m'-k', S''\setminus \bar{l}_u, H'') \in [\![\Delta; \bar{\mathsf{y}}, \mathsf{x}; \psi, \bar{l}, \bar{\mathsf{u}}, \mathsf{d} \vdash \mathtt{lookup}\ \bar{l}\ \mathtt{as}\ \bar{\mathsf{z}}\ \mathtt{in}\ \mathsf{Q}[\bar{l}/\&\bar{\mathsf{y}}][\bar{\mathsf{z}}/\bar{\mathsf{y}}] : \mathtt{Prop}]\!](\delta; (E, S'); \vartheta[\bar{\mathsf{u}} \mapsto \bar{v}_x, \mathsf{d} \mapsto S''(E'(\mathsf{r}))])$$

□

Lemma 21. *Rule* (delcall) *is sound.*

$$\frac{\mathsf{R} = \mathsf{y} \mapsto \langle(\bar{\mathsf{u}}).\{\mathsf{P}\}\_\{\mathsf{d}.\mathsf{Q}\}\rangle \qquad \mathsf{x} \notin \mathrm{FV}(\mathsf{R}) \qquad \mathsf{y} \in \phi}{\Gamma; \Delta; \phi, \bar{\mathsf{x}}, \mathsf{x}; \psi \vdash \{\mathsf{R} * \mathsf{P}[\bar{\mathsf{x}}/\bar{\mathsf{u}}]\}\mathsf{x} = \mathsf{y}(\bar{\mathsf{x}}); \{\mathsf{R} * \mathsf{Q}[\bar{\mathsf{x}}/\bar{\mathsf{u}}, \mathsf{x}/\mathsf{d}]\} \triangleleft \{\mathsf{x}\}}$$

Proof. Let $n, m, k \in \mathsf{N}$ such that $k \leq m \leq n+1$. Assume $n \in [\![\Gamma : \mathtt{Context}]\!]$,

$$(m-1; C_1; H_1) \in [\![\Delta; \phi, \bar{\mathsf{x}}, \mathsf{x}; \psi \vdash \mathsf{y} \mapsto \langle(\bar{\mathsf{u}}).\{\mathsf{P}\}\_\{\mathsf{d}.\mathsf{Q}\}\rangle : \mathtt{Prop}]\!](\delta; (E, S); \vartheta)$$

$$(m-1; C_2; H_2) \in [\![\Delta; \phi, \bar{\mathsf{x}}, \mathsf{x}; \psi \vdash \mathsf{P}[\bar{\mathsf{x}}/\bar{\mathsf{u}}] : \mathtt{Prop}]\!](\delta; (E, S); \vartheta)$$

$$H_1(E(\mathsf{y})) = (\delta_c, E_c, \bar{\mathsf{u}}, \bar{\mathsf{z}}, \mathsf{s}, \mathsf{r})$$

$C_1 \# C_2$, $H_1 \# H_2$, and $(C_1 \uplus C_2) \# S$.

By strengthening, splitting, renaming and upwards-closure it follows that,

$$(m-1; C_1; H_1) \in [\![\Delta; \phi, \bar{\mathsf{x}}; \psi \vdash \mathsf{y} \mapsto \langle(\bar{\mathsf{u}}).\{\mathsf{P}\}\_\{\mathsf{d}.\mathsf{Q}\}\rangle : \mathtt{Prop}]\!](\delta; (E|_{\phi,\bar{\mathsf{x}}}, S|_{E(\phi,\bar{\mathsf{x}})}); \vartheta)$$

and

$$(m-2; C_2; H_2) \in [\![\Delta; \phi, \bar{\mathsf{x}}; \psi, \bar{\mathsf{u}} \vdash \mathsf{P} : \mathtt{Prop}]\!](\delta; (E|_{\phi,\bar{\mathsf{x}}}, S|_{E(\phi,\bar{\mathsf{x}})}); \vartheta[\bar{\mathsf{u}} \mapsto S(E(\bar{\mathsf{x}}))])$$

Hence,

$$(\delta_c, E_c'; C_2[\bar{l}_u \mapsto S(E(\bar{\mathsf{x}})), \bar{l}_z \mapsto \mathtt{null}]; H_2; \mathsf{s}) : \mathtt{safe}_{m-1}$$

where $E_c' = E_c[\bar{\mathsf{u}} \mapsto \bar{l}_u, \bar{\mathsf{z}} \mapsto \bar{l}_z]$.

Correctness: If

$$(\delta_c, E; C \uplus S; H, \mathsf{x} = \mathsf{y}(\bar{\mathsf{x}});) \Downarrow_k (S', H')$$

then

$$(\delta_c, E_c'; C \uplus S[\bar{l}_u \mapsto S(E(\bar{\mathsf{x}})), \bar{l}_z \mapsto \mathtt{null}]; H; \mathsf{s}) \Downarrow_{k-1} (S'', H'')$$

and $S' = S''[E(\mathsf{x}) \mapsto S''(E_c'(\mathsf{r}))]$ and $H' = H''$. By the stack and heap frame property there exists C_2' and H_2' such that,

$$(\delta_c, E_c'; C_2[\bar{l}_u \mapsto S(E(\bar{\mathsf{x}})), \bar{l}_z \mapsto \mathtt{null}]; H_2; \mathsf{s}) \Downarrow_{k-1} (C_2', H_2')$$

and $S'' = C_1 \uplus S \uplus C_2'$ and $H'' = H_1 \uplus H_2'$. Hence,

$$((m-1)-(k-1); C_2' \backslash \bar{l}_u; H_2') \in [\![\Delta; \phi, \bar{\mathsf{x}}; \psi, \bar{\mathsf{u}}, \mathsf{d} \vdash \mathsf{Q} : \mathtt{Prop}]\!](\delta; (E|_{\phi,\bar{\mathsf{x}}}, S|_{E(\phi,\bar{\mathsf{x}})}); \vartheta[\bar{\mathsf{u}} \mapsto S(E(\bar{\mathsf{x}})), \mathsf{d} \mapsto C_2'(E_c'(\mathsf{r}))])$$

Since $S''(E(\phi, \bar{\mathsf{x}})) = S(E(\phi, \bar{\mathsf{x}}))$, by splitting and renaming it follows that,

$$(m-k; C_2' \setminus \bar{l}_u; H_2') \in [\![\Delta; \phi, \bar{\mathsf{x}}; \psi, \mathsf{x} \vdash \mathsf{Q}[\bar{\mathsf{x}}/\bar{\mathsf{u}}, \mathsf{x}/\mathsf{d}] : \mathtt{Prop}]\!](\delta; (E|_{\phi,\bar{\mathsf{x}}}, S''|_{E(\phi,\bar{\mathsf{x}})}); \vartheta[\mathsf{x} \mapsto C_2'(E_c'(\mathsf{r}))])$$

and by splitting again,

$$(m-k; C_2' \setminus \bar{l}_u; H_2') \in [\![\Delta; \phi, \bar{\mathsf{x}}, \mathsf{x}; \psi \vdash \mathsf{Q}[\bar{\mathsf{x}}/\bar{\mathsf{u}}, \mathsf{x}/\mathsf{d}] : \mathtt{Prop}]\!](\delta; (E, S''|_{E(\phi,\bar{\mathsf{x}})}[E(\mathsf{x}) \mapsto C_2'(E_c'(\mathsf{r}))]); \vartheta)$$

Hence, by upwards-closure,

$$(m-k; (S \uplus C_2') \setminus E(\phi, \bar{\mathsf{x}}, \mathsf{x}); H_2') \in [\![\Delta; \phi, \bar{\mathsf{x}}, \mathsf{x}; \psi \vdash \mathsf{Q}[\bar{\mathsf{x}}/\bar{\mathsf{u}}, \mathsf{x}/\mathsf{d}] : \mathtt{Prop}]\!](\delta; (E, S'|_{E(\phi,\bar{\mathsf{x}},\mathsf{x})}); \vartheta)$$

and since $1 \leq k$ and $\mathsf{x} \notin \mathrm{FV}(\mathsf{R})$ it follows by upwards-closure and strengthening and weakening that,

$$(m-k; C_1; H_1) \in [\![\Delta; \phi, \bar{\mathsf{x}}, \mathsf{x}; \psi \vdash \mathsf{y} \mapsto \langle(\bar{\mathsf{u}}).\{\mathsf{P}\}\_\{\mathsf{d}.\mathsf{Q}\}\rangle : \mathtt{Prop}]\!](\delta; (E, S'|_{E(\phi,\bar{\mathsf{x}},\mathsf{x})}); \vartheta)$$

□

Lemma 22. *Rule* (localvar) *is sound.*

$$\frac{\Gamma; \Delta; \phi, \bar{\mathsf{z}}; \psi \vdash \{\mathsf{P} \wedge \bar{\mathsf{z}} = \mathit{null}\}\mathsf{s}; \mathit{return}\ \mathsf{x}\{\mathsf{d}.\mathsf{Q}\} \triangleleft \mathsf{M}}{\Gamma; \Delta; \phi; \psi \vdash \{\mathsf{P}\}\bar{\mathsf{G}}\bar{\mathsf{z}}; \mathsf{s}; \mathit{return}\ \mathsf{x}\{\mathsf{d}.\exists \bar{l} : \mathit{Var}.\ \mathit{lookup}\ \bar{l}\ \mathit{as}\ \bar{\mathsf{z}}\ \mathit{in}\ \mathsf{Q}[\bar{l}/\&\bar{\mathsf{z}}]\} \triangleleft \mathsf{M} \setminus \bar{\mathsf{z}}}$$

Proof. Let $n, m, k \in \mathsf{N}$ such that $k \leq m \leq n+1$. Assume $n \in [\![\Gamma : \mathtt{Context}]\!]$,

$$(m-1; C; H) \in [\![\Delta; \phi; \psi \vdash \mathsf{P} : \mathtt{Prop}]\!](\delta; (E, S); \vartheta)$$

$C \# S$ and $\bar{l}_z \in \mathbb{L}_s \setminus \mathrm{Dom}(C \uplus S)$. By weakening,

$$(m-1; C; H) \in [\![\Delta; \phi, \bar{\mathsf{z}}; \psi \vdash \mathsf{P} : \mathtt{Prop}]\!](\delta; (E', S'); \vartheta)$$

for $E' = E[\bar{\mathsf{z}} \mapsto \bar{l}_z]$ and $S' = S[\bar{l}_z \mapsto \mathtt{null}]$. Since $C \# S'$,

$$(E', C \uplus S', H, \mathsf{s}) : \mathtt{safe}_k$$

and if,

$$(E', C \uplus S', H, \mathsf{s}) \Downarrow_k (S'', H'')$$

then

$$(m-k; S'' \setminus E'(\phi, \bar{\mathsf{z}}); H') \in [\![\Delta; \phi, \bar{\mathsf{z}}; \psi, \mathsf{d} \vdash \mathsf{Q} : \mathtt{Prop}]\!](\delta; (E', S'_{E'(\phi, \bar{\mathsf{z}})}); \vartheta[\mathsf{d} \mapsto S''(E'(\mathsf{x}))])$$

splitting the zs into their values and locations we get:

$$(m-k; S'' \setminus E'(\phi, \bar{\mathsf{z}}); H') \in [\![\Delta; \phi; \psi, \bar{\mathsf{z}}, \bar{l}, \mathsf{d} \vdash \mathsf{Q}[\bar{l}/\&\bar{\mathsf{z}}] : \mathtt{Prop}]\!](\delta; (E'|_\phi, S'_{E'(\phi)}); \vartheta[\mathsf{d} \mapsto S''(E'(\mathsf{x})), \bar{\mathsf{z}} \mapsto S''(\bar{l}_z), \bar{l} \mapsto \bar{l}_z])$$

and thus, by definition,

$$(m-k, S'' \setminus E'(\phi); H') \in [\![\Delta; \phi; \psi, \bar{l}, \mathsf{d} \vdash \mathtt{lookup}\ \bar{l}\ \mathtt{as}\ \bar{\mathsf{z}}\ \mathtt{in}\ \mathsf{Q}[\bar{l}/\&\bar{\mathsf{z}}] : \mathtt{Prop}]\!](\delta; (E'|_\phi, S'_{E'(\phi)}); \vartheta[\mathsf{d} \mapsto S''(E'(\mathsf{x})), \bar{l} \mapsto \bar{l}_z])$$

□

4 Examples

Proof outline of append

```
public static Node⟨X⟩ append⟨X⟩(Node⟨X⟩ front, Node⟨X⟩ tail) {
  Node⟨X⟩ tmp, tmp2;
  { list(front, xs, P) ∗ list(tail, ys, P) }
  if(front == null) {
    { front = null ∧ list(front, xs, P) ∗ list(tail, ys, P) }
    { xs = [] ∧ list(tail, ys, P) }
    { list(tail, xs@ys, P) }
    return tail;
    { r. list(r, xs@ys, P) }
  } else {
    { front != null ∧ list(front, xs, P) ∗ list(tail, ys, P) }
    { ∃v, xs', n, x. xs = v::xs' ∧ front.next ↦ n ∗ front.item ↦ x ∗ P(x, v) ∗ list(n, xs', P) ∗ list(tail, ys, P) }
    tmp2 = front.next;
    { ∃v, xs', x. xs = v::xs' ∧ front.next ↦ tmp2 ∗ front.item ↦ x ∗ P(x, v) ∗ list(tmp2, xs', P) ∗ list(tail, ys, P) }
    tmp = append⟨X⟩(tmp2, tail);
    { ∃v, xs', x. xs = v::xs' ∧ front.next ↦ tmp2 ∗ front.item ↦ x ∗ P(x, v) ∗ list(tmp, xs'@ys, P) }
    front.next = tmp;
    { ∃v, xs', x. xs = v::xs' ∧ front.next ↦ tmp ∗ front.item ↦ x ∗ P(x, v) ∗ list(tmp, xs'@ys, P) }
    { list(front, xs@ys, P) }
    return front;
    { r. list(r, xs@ys, P) }
  }
}
```