

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{x} for finite sequences.

G	::= $C(\bar{G}) \mid T$	Generic class
L	::= $\text{class } C(\bar{T}) : G \{ \bar{G}f; \bar{M} \}$	Class definition
M	::= $G \ m(\bar{G}u) \{ B \}$	Method definition
B	::= $\bar{G}z; s; \text{return } r;$	Method body
s	::=	Statement
	$x = y$	assignment
	$x = \text{null}$	initialization
	$x = y.f$	field access
	$x.f = y$	field update
	$x = y.m(\bar{z})$	method invocation
	$x = (G)y$	cast
	$\text{if } (x == y) \{s_1\} \text{ else } \{s_2\}$	conditional
	$x = \text{new } C(\bar{G})()$	object creation
	$x = \text{delegate } (\bar{G}z) \{B\}$	inline delegate
	$x = \text{delegate } y.m$	named delegate
	$x = y(\bar{z})$	delegate application
	$s_1; s_2$	sequential composition

1.2 Operational Semantics

For the operational semantics we assume disjoint countably infinite sets of stack locations, L_s , heap locations, L_h , variables, A_p , type variables A_t , class identifiers, C , method identifiers, M , field identifiers, F , and object identifiers, O .

l	$\in L_s$	locations
o	$\in O$	object identifiers
v	$\in V = L_h \uplus O \uplus \{\text{null}\}$	values
a, b, c, r, u, x, y, z	$\in A_p$	variables
C, D	$\in C$	class identifiers
f	$\in F$	field identifiers
m	$\in M$	method identifiers
T	$\in A_t$	type variables
	$B \stackrel{\text{def}}{=} L(s)$	statements
	$T \stackrel{\text{def}}{=} \{w \in L(G) \mid \text{FTV}(w) = \emptyset\}$	generic classes
δ	$\in E_t \stackrel{\text{def}}{=} A_t \xrightarrow{\text{fin}} T$	type environment
E	$\in E_p \stackrel{\text{def}}{=} A_p \xrightarrow{\text{fin}} L_s$	environment
C, S	$\in S \stackrel{\text{def}}{=} L_s \xrightarrow{\text{fin}} V$	stack
H	$\in H \stackrel{\text{def}}{=} (O \times F \xrightarrow{\text{fin}} V) \times (O \xrightarrow{\text{fin}} L(G)) \times (L_h \xrightarrow{\text{fin}} D)$	heap
	$D \stackrel{\text{def}}{=} (E_t \times E_p \times A_p^* \times A_p^* \times B \times A_p) \uplus (O \times M)$	delegate
P	$\in P \stackrel{\text{def}}{=} (C \xrightarrow{\text{fin}} A_t^* \times F^*) \times (C \times M \xrightarrow{\text{fin}} A_p^* \times A_p^* \times B \times A_p)$	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 A_p , A_t , and B , and the trivial action on L_s , O , V , C , F , M .

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

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

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

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

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

$$\frac{S(E(x)) = S(E(y)) \quad (P, \delta, E, S, s_1) \Downarrow_n (S', H')}{(P, \delta, E, S, H, \text{if } (x == y) \text{ then } s_1 \text{ else } s_2) \Downarrow_{n+1} (S', H')}$$

$$\frac{o \notin \text{Dom}(H_t) \quad H' = H[o \mapsto C(\llbracket \bar{G} \rrbracket(\delta)), (o, \bar{f}) \mapsto \text{null}] \quad P(C) = (\bar{T}, \bar{f}) \quad S' = S[E(x) \mapsto o]}{(P, \delta, E, S, H, x = \text{new } C(\bar{G})()) \Downarrow_1 (S', H')}$$

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

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

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

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

$$\frac{(P, \delta, E, S, H, s_1) \Downarrow_n (S', H') \quad (P, \delta, E, S', H', s_2) \Downarrow_m T}{(P, \delta, E, S, H, s_1; s_2) \Downarrow_{n+m} T} \qquad \frac{(P, \delta, E, S, H, s_1) \Downarrow_n \text{err}}{(P, \delta, E, S, H, s_1; s_2) \Downarrow_n \text{err}}$$

We use the notation $P(C)$ for $\pi_1(P)(C)$ and $P(C, m)$ for $\pi_2(P)(C, m)$. Furthermore, we use $[\bar{x} \mapsto \bar{y}]$ as shorthand for $[x_1 \mapsto y_1, \dots, x_n \mapsto y_n]$, 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.

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

and

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

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

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

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

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

Lemma 4 (Heap frame property). *If*

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

and $(P, \delta, E, S, H_1, \mathfrak{s}) : \mathit{safe}_n$ then there exists a H'_1 such that $H' = H'_1 * H_2$ and

$$(P, \delta, E, S, H_1, \mathfrak{s}) \Downarrow_n (S', H'_1)$$

Lemma 5 (Stack frame property). *If*

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

and $(P, \delta, E, S_1, H, \mathfrak{s}) : \mathit{safe}_n$ then there exists an S'_1 such that $S' = S'_1 * S_2$ and

$$(P, \delta, E, S_1, H, \mathfrak{s}) \Downarrow_n (S'_1, H')$$

2 Assertion Logic

2.1 Syntax

ω, ω'	$::= \omega \rightarrow \omega' \mid \omega \times \omega' \mid \text{Prop} \mid \text{Class} \mid \text{Val} \mid \text{Int} \mid \text{Loc}$	Types
M, N, L, P, Q, R	$::= P \vee Q \mid P \wedge Q \mid P \Rightarrow Q \mid \top \mid \perp \mid \forall x : \omega. P \mid \exists x : \omega. P$	Propositions
	$\mid P * Q \mid P \multimap Q \mid \text{emp} \mid M.f \mapsto N \mid M =_\omega N$	
	$\mid L \xrightarrow{s} N \mid M \mapsto \langle (\bar{x}).\{P\}_{-}\{d.Q\} \rangle \mid M:N$	
	$\mid \lambda x : \omega. M \mid M N \mid x \mid \&x \mid \text{null}$	Other terms

The judgments of the assertion logic are of the forms:

$$\Delta; \phi; \psi \vdash M : \omega, \quad \Delta; \phi; \psi \vdash M = N : \omega, \quad \Delta; \phi; \psi \mid P_1, \dots, P_n \vdash Q$$

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:

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

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).

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

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

Definition 2 (Location substitution).

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

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

Definition 3 (Free variables).

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

Definition 4 (Free value variables).

$$\begin{aligned} \text{FVV}(M \mapsto \langle (\bar{u}), \{P\}, \{d, Q\} \rangle) &= \text{FVV}(M) \cup (\text{FVV}(P) \cup \text{FVV}(Q)) \setminus (\bar{u} \cup \{d\}) \\ \text{FVV}(L \xrightarrow{s} N) &= \text{FV}(L) \cup \text{FVV}(N) \\ \text{FVV}(\&x) &= \emptyset \\ \text{FVV}(x) &= \{x\} \end{aligned}$$

Definition 5 (Free location variables).

$$\begin{aligned} \text{FVA}(M \mapsto \langle (\bar{u}), \{P\}, \{d, Q\} \rangle) &= \text{FVA}(M) \cup (\text{FVA}(P) \cup \text{FVA}(Q)) \setminus (\bar{u} \cup \{d\}) \\ \text{FVA}(L \xrightarrow{s} N) &= \text{FVA}(L) \cup \text{FVA}(N) \\ \text{FVA}(\&x) &= \{x\} \\ \text{FVA}(x) &= \emptyset \end{aligned}$$

Definition 6 (Lookup).

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

2.2 Typing rules

Well-formed terms

$\Delta; \phi; \psi \vdash R : \omega$

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

$$\frac{\Delta; \phi; \psi, x : \omega \vdash P : \text{Prop} \quad Q \in \{\exists, \forall\}}{\Delta; \phi; \psi \vdash Qx : \omega. P : \text{Prop}} \qquad \frac{\Delta; \phi; \psi \vdash L : \text{Loc} \quad \Delta; \phi; \psi \vdash N : \text{Val}}{\Delta; \phi; \psi \vdash L \xrightarrow{s} N : \text{Prop}}$$

$$\overline{\Delta; \phi; \psi \vdash \top : \text{Prop}}$$

$$\overline{\Delta; \phi; \psi \vdash \perp : \text{Prop}}$$

$$\overline{\Delta; \phi; \psi \vdash \text{emp} : \text{Prop}}$$

$$\frac{op \in \{\wedge, \vee, *, \neg, \Rightarrow\} \quad \Delta; \phi; \psi \vdash P : \text{Prop} \quad \Delta; \phi; \psi \vdash Q : \text{Prop}}{\Delta; \phi; \psi \vdash P \text{ op } Q : \text{Prop}}$$

$$\frac{\Delta; \phi; \psi \vdash M : \text{Val} \quad \Delta; \phi; \psi \vdash N : \text{Class}}{\Delta; \phi; \psi \vdash M : N : \text{Prop}}$$

$$\frac{x \in \phi}{\Delta; \phi; \psi \vdash \&x : \text{Loc}}$$

$$\overline{\Delta, T; \phi; \psi \vdash T : \text{Class}}$$

$$\frac{\Delta; \phi; \psi \vdash \bar{G} : \text{Class}}{\Delta; \phi; \psi \vdash C(\bar{G}) : \text{Class}}$$

$$\overline{\Delta; \phi; \psi \vdash \text{null} : \text{Val}}$$

$$\overline{\Delta; \phi, x; \psi \vdash x : \text{Val}}$$

$$\overline{\Delta; \phi; \psi, a : \omega \vdash a : \omega}$$

$$\frac{\Delta; \phi; \psi, x : \omega \vdash M : \omega'}{\Delta; \phi; \psi \vdash \lambda x : \omega. M : \omega \rightarrow \omega'}$$

$$\frac{\Delta; \phi; \psi \vdash M : \omega \rightarrow \omega' \quad \Delta; \phi; \psi \vdash M : \omega}{\Delta; \phi; \psi \vdash M N : \omega'}$$

$$\frac{\Delta; \phi; \psi \vdash M : \text{Val} \quad \Delta; \phi; \psi \vdash N : \text{Val}}{\Delta; \phi; \psi \vdash M.f \mapsto N : \text{Prop}}$$

$$\frac{\Delta; \phi; \psi \vdash M : \omega \quad \Delta; \phi; \psi \vdash N : \omega}{\Delta; \phi; \psi \vdash M =_{\omega} N : \text{Prop}}$$

2.3 Proof rules

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

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

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

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

2.4 Semantics

Types

$\llbracket \omega \rrbracket \in \text{Set}$

$$\begin{aligned}
\llbracket \omega \rightarrow \omega' \rrbracket &= \llbracket \omega \rrbracket \rightarrow \llbracket \omega' \rrbracket \\
\llbracket \omega \times \omega' \rrbracket &= \llbracket \omega \rrbracket \times \llbracket \omega' \rrbracket \\
\llbracket \text{Prop} \rrbracket &= \{U \in \mathcal{P}^\uparrow(\mathbb{N} \times \mathbb{S} \times \mathbb{H}) \mid \forall \pi \in \text{Perm}(\mathbb{A}_p). \forall a \in U. \pi(a) \in U\} \\
\llbracket \text{Val} \rrbracket &= \text{Val} \\
\llbracket \text{Loc} \rrbracket &= \mathbb{L}_s \\
\llbracket \text{Class} \rrbracket &= \mathbb{T} \\
\llbracket \text{Int} \rrbracket &= \mathbb{Z}
\end{aligned}$$

where Val is the least set satisfying:

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

The order on $\mathbb{N} \times \mathbb{S} \times \mathbb{H}$ 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:

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

Contexts

$\llbracket \phi \rrbracket, \llbracket \psi \rrbracket, \llbracket \Delta \rrbracket \in \text{Set}$

$$\begin{aligned}
S \in \llbracket \phi \rrbracket &= \{(E, S) \in \mathbb{E}_p \times \mathbb{S} \mid E \text{ injective} \wedge \text{Dom}(E) = \phi \wedge \text{Rng}(E) = \text{Dom}(S)\} \\
\vartheta \in \llbracket \psi \rrbracket &= \Pi(x : \omega) \in \psi. \llbracket \omega \rrbracket \\
\delta \in \llbracket \Delta \rrbracket &= \{\delta \in \mathbb{E}_t \mid \text{Dom}(\delta) = \Delta\}
\end{aligned}$$

$$\begin{aligned}
[[\Delta; \phi; \psi \vdash C(\bar{G}) : \mathbf{Class}]](\delta; (E, S); \vartheta) &= C([[\Delta; \phi; \psi \vdash \bar{G} : \mathbf{Class}]](\delta; (E, S); \vartheta)) \\
[[\Delta; \phi; \psi \vdash e : C : \mathbf{Prop}]](\delta; (E, S); \vartheta) &= \{(n, C, (h_v, h_t, h_c)) \in \mathbf{N} \times \mathbf{S} \times \mathbf{H} \mid \exists o \in \mathcal{O}, C \in \mathbf{C}, \delta' \in \mathbb{E}_t. \\
&\quad in_{\mathcal{O}}(o) = [[\Delta; \phi; \psi \vdash e : \mathbf{Val}]](\delta; (E, S); \vartheta) \wedge \\
&\quad h_t(o) = [[\Delta; \phi; \psi \vdash C : \mathbf{Class}]](\delta; (E, S); \vartheta)\} \\
[[\Delta; \phi; \psi \vdash \top : \mathbf{Prop}]](\delta; (E, S); \vartheta) &= \mathbf{N} \times \mathbf{S} \times \mathbf{H} \\
[[\Delta; \phi; \psi \vdash \perp : \mathbf{Prop}]](\delta; (E, S); \vartheta) &= \emptyset \\
[[\Delta; \phi; \psi \vdash \mathbf{emp} : \mathbf{Prop}]](\delta; (E, S); \vartheta) &= \mathbf{N} \times \mathbf{S} \times \mathbf{H} \\
[[\Delta; \phi; \psi \vdash P \wedge Q : \mathbf{Prop}]](\delta; (E, S); \vartheta) &= [[\Delta; \phi; \psi \vdash P : \mathbf{Prop}]](\delta; (E, S); \vartheta) \cap [[\Delta; \phi; \psi \vdash Q : \mathbf{Prop}]](\delta; (E, S); \vartheta) \\
[[\Delta; \phi; \psi \vdash P \vee Q : \mathbf{Prop}]](\delta; (E, S); \vartheta) &= [[\Delta; \phi; \psi \vdash P : \mathbf{Prop}]](\delta; (E, S); \vartheta) \cup [[\Delta; \phi; \psi \vdash Q : \mathbf{Prop}]](\delta; (E, S); \vartheta) \\
[[\Delta; \phi; \psi \vdash P * Q : \mathbf{Prop}]](\delta; (E, S); \vartheta) &= \{(n, C, (h_v, h_t, h_c)) \in \mathbf{N} \times \mathbf{S} \times \mathbf{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 P : \mathbf{Prop}]](\delta; (E, S); \vartheta) \wedge \\
&\quad (n, C_2, (h_2, h_t, h_c)) \in [[\Delta; \phi; \psi \vdash Q : \mathbf{Prop}]](\delta; (E, S); \vartheta)\} \\
[[\Delta; \phi; \psi \vdash P \Rightarrow Q : \mathbf{Prop}]](\delta; (E, S); \vartheta) &= \{B \in \mathbf{N} \times \mathbf{S} \times \mathbf{H} \mid \forall B' \geq B. \\
&\quad B' \in [[\Delta; \phi; \psi \vdash P : \mathbf{Prop}]](\delta; (E, S); \vartheta) \Rightarrow \\
&\quad B' \in [[\Delta; \phi; \psi \vdash Q : \mathbf{Prop}]](\delta; (E, S); \vartheta)\} \\
[[\Delta; \phi; \psi \vdash M.f \mapsto N : \mathbf{Prop}]](\delta; (E, S); \vartheta) &= \{(n, C, (h_v, h_t, h_c)) \in \mathbf{N} \times \mathbf{S} \times \mathbf{H} \mid \exists o \in \mathcal{O}. \\
&\quad in_{\mathcal{O}id}(o) = [[\Delta; \phi; \psi \vdash M : \mathbf{Val}]](\delta; (E, S); \vartheta) \wedge \\
&\quad h_v(o, f) = [[\Delta; \phi; \psi \vdash N : \mathbf{Val}]](\delta; (E, S); \vartheta)\} \\
[[\Delta; \phi; \psi \vdash \forall a : \omega.P : \mathbf{Prop}]](\delta; (E, S); \vartheta) &= \bigcap_{v \in [[\omega]]} [[\Delta; \phi; \psi, a : \omega \vdash P : \mathbf{Prop}]](\delta; (E, S); \vartheta, a \mapsto v) \\
[[\Delta; \phi; \psi \vdash \exists a : \omega.P : \mathbf{Prop}]](\delta; (E, S); \vartheta) &= \bigcup_{v \in [[\omega]]} [[\Delta; \phi; \psi, a : \omega \vdash P : \mathbf{Prop}]](\delta; (E, S); \vartheta, a \mapsto v) \\
[[\Delta; \phi; \psi \vdash M =_{\omega} N : \mathbf{Prop}]](\delta; (E, S); \vartheta) &= \{B \in \mathbf{N} \times \mathbf{S} \times \mathbf{H} \mid \\
&\quad [[\Delta; \phi; \psi \vdash M : \omega]](\delta; (E, S); \vartheta) = [[\Delta; \phi; \psi \vdash N : \omega]](\delta; (E, S); \vartheta)\} \\
[[\Delta, T; \phi; \psi \vdash T : \mathbf{Class}]](\delta; (E, S); \vartheta) &= \delta(T) \\
[[\Delta; \phi, x; \psi \vdash x : \mathbf{Val}]](\delta; (E, S); \vartheta) &= S(E(x)) \\
[[\Delta; \phi; \psi \vdash \mathbf{null} : \mathbf{Val}]](\delta; (E, S); \vartheta) &= \mathbf{null} \\
[[\Delta; \phi; \psi, a : \omega \vdash a : \omega]](\delta; (E, S); \vartheta) &= \vartheta(a) \\
[[\Delta; \phi; \psi \vdash \lambda a : \omega.M : \omega \rightarrow \omega']](\delta; (E, S); \vartheta) &= \lambda v : [[\omega]]. [[\Delta; \phi; \psi, a : \omega \vdash M : \omega']](\delta; (E, S); \vartheta[a \mapsto v]) \\
[[\Delta; \phi; \psi \vdash M N : \omega]](\delta; (E, S); \vartheta) &= ([[\Delta; \phi; \psi \vdash M : \omega' \rightarrow \omega]](\delta; (E, S); \vartheta)) ([[\Delta; \phi; \psi \vdash N : \omega']](\delta; (E, S); \vartheta)) \\
[[\Delta; \phi, x; \psi \vdash \&x : \mathbf{Loc}]](\delta; (E, S); \vartheta) &= E(x) \\
[[\Delta; \phi; \psi \vdash L \xrightarrow{s} N : \mathbf{Prop}]](\delta; (E, S); \vartheta) &= \{(n, C, H) \in \mathbf{N} \times \mathbf{S} \times \mathbf{H} \mid l \in \text{Dom}(C) \wedge \\
&\quad C(l) = [[\Delta; \phi; \psi \vdash N : \mathbf{Val}]](\delta; (E, S); \vartheta)\}
\end{aligned}$$

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

$$\begin{aligned}
& \llbracket \Delta; \phi; \psi \vdash \mathbf{M} \mapsto \langle (\bar{u}).\{\mathbf{P}\}_{-\{\mathbf{d.Q}\}} \rangle : \mathbf{Prop} \rrbracket (\delta, (E, S), \vartheta) = \\
& \{ (n, -, (h_v, h_t, h_c)) \in \mathbf{N} \times \mathbf{S} \times \mathbf{H} \mid \exists o, \delta_c, E_c, \bar{x}, \bar{z}, \mathbf{s}, \mathbf{r}, \mathbf{C}, \bar{\mathbf{G}}, \bar{\mathbf{T}}. \\
& \quad h_c(\llbracket \Delta; \phi; \psi \vdash \mathbf{M} : \mathbf{Val} \rrbracket (\delta, (E, S), \vartheta)) = (\delta_c, E_c, \bar{x}, \bar{z}, \mathbf{s}, \mathbf{r}) \wedge \\
& \quad \forall m \leq n. \forall k \leq m. \forall C \in \mathbf{S}. \forall H \in \mathbf{H}. \forall \bar{l}_x, \bar{l}_z \in \mathbf{Loc} \setminus (\mathbf{Dom}(C) \cup \mathbf{Rng}(E_c)). \forall \bar{v}_x \in \mathbf{Val}. \\
& \quad (m-1, C, H) \in \llbracket \Delta; \phi; \psi, \bar{u} \vdash \mathbf{P} : \mathbf{Prop} \rrbracket (\delta, (E, S), \vartheta[\bar{u} \mapsto \bar{v}_x]) \Rightarrow \\
& \quad (\delta_c; E'_c, C[\bar{l}_x \mapsto \bar{v}_x, \bar{l}_z \mapsto \mathbf{null}], H, \mathbf{s}) : \mathbf{safe}_k \wedge \\
& \quad (\delta_c; E'_c, C[\bar{l}_x \mapsto \bar{v}_x, \bar{l}_z \mapsto \mathbf{null}], H, \mathbf{s}) \Downarrow_k (C', H') \Rightarrow \\
& \quad (m-k, C' \setminus \bar{l}_x; H') \in \llbracket \Delta; \phi; \psi, \bar{u}, \mathbf{d} \vdash \mathbf{Q} : \mathbf{Prop} \rrbracket (\delta; (E, S), \vartheta[\bar{u} \mapsto \bar{v}_x, \mathbf{d} \mapsto C'(E'_c(\mathbf{r}))])
\end{aligned}$$

\vee

$$\begin{aligned}
& h_c(\llbracket \Delta; \phi; \psi \vdash \mathbf{M} : \mathbf{Val} \rrbracket (\delta, (E, S), \vartheta)) = (o, \mathbf{m}) \wedge h_t(o) = \mathbf{C}(\bar{\mathbf{G}}) \wedge P(\mathbf{C}) = (\bar{\mathbf{T}}, -) \wedge P(\mathbf{C}, \mathbf{m}) = (\bar{x}, \bar{z}, \mathbf{s}, \mathbf{r}) \wedge \\
& \forall m \leq n. \forall k \leq m. \forall C \in \mathbf{S}. \forall H \in \mathbf{H}. \forall \bar{l}_x, \bar{l}_z, l_t \in \mathbf{L}_s \setminus \mathbf{Dom}(C). \forall \bar{v}_x \in \mathbf{V}. \\
& (m-1, C, H) \in \llbracket \Delta; \phi; \psi, \bar{u} \vdash \mathbf{P} : \mathbf{Prop} \rrbracket (\delta, (E, S), \vartheta[\bar{u} \mapsto \bar{v}_x]) \Rightarrow \\
& (\bar{\mathbf{T}} \mapsto \bar{\mathbf{G}}], E', C[\bar{l}_u \mapsto \bar{v}_x, \bar{l}_z \mapsto \mathbf{null}, l_t \mapsto o], H, \mathbf{s}) : \mathbf{safe}_k \wedge \\
& (\bar{\mathbf{T}} \mapsto \bar{\mathbf{G}}], E', C[\bar{l}_u \mapsto \bar{v}_x, \bar{l}_z \mapsto \mathbf{null}, l_t \mapsto o], H, \mathbf{s}) \Downarrow_k (C', H') \Rightarrow \\
& (m-k, C' \setminus \bar{l}_x; H') \in \llbracket \Delta; \phi; \psi, \bar{u}, \mathbf{d} \vdash \mathbf{Q} : \mathbf{Prop} \rrbracket (\delta, (E, S), \vartheta[\bar{u} \mapsto \bar{v}_x, \mathbf{d} \mapsto C'(E'(\mathbf{r}))])
\end{aligned}$$

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

Entailment

$$\boxed{\llbracket \Delta; \phi; \psi \mid \mathbf{P}_1, \dots, \mathbf{P}_n \vdash \mathbf{Q} \rrbracket : 2}$$

$$\llbracket \Delta; \phi; \psi \mid \mathbf{P}_1, \dots, \mathbf{P}_n \vdash \mathbf{Q} \rrbracket = \forall \delta \in \llbracket \Delta \rrbracket. \forall (E, S) \in \llbracket \phi \rrbracket. \forall \vartheta \in \llbracket \psi \rrbracket.$$

$$\left(\bigcap_{1 \leq i \leq n} \llbracket \Delta; \phi; \psi \vdash \mathbf{P}_i : \mathbf{Prop} \rrbracket (\delta; (E, S); \vartheta) \right) \subseteq \llbracket \Delta; \phi; \psi \vdash \mathbf{Q} : \mathbf{Prop} \rrbracket (\delta; (E, S); \vartheta)$$

2.5 Metatheory

Lemma 6. *Let*

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

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

$$\begin{aligned} I &= \emptyset \\ U * V &= \{(n, C \cup C', (h_v \cup h'_v, h_t, h_c)) \mid C \# C' \wedge h_v \# h'_v \wedge \\ &\quad (n, C, (h_v, h_t, h_c)) \in U \wedge (n, C', (h'_v, h_t, h_c)) \in V\} \\ U -* V &= \bigcup \{W \in \llbracket \text{Prop} \rrbracket \mid W * U \subseteq V\} \end{aligned}$$

for $U, V \in \llbracket \text{Prop} \rrbracket$.

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

$$\begin{aligned} \forall \delta \in \llbracket \Delta \rrbracket. \forall (E, S) \in \llbracket \phi \rrbracket. \forall \vartheta \in \llbracket \psi \rrbracket. \\ \llbracket \Delta; \phi; \psi \vdash P : \omega \rrbracket(\delta; (E, S); \vartheta) = \llbracket \Delta; \pi(\phi); \pi(\psi) \vdash \pi(P) : \omega \rrbracket(\delta; (\pi(E), S); \pi(\vartheta)) \end{aligned}$$

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

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

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

$$\begin{aligned} \forall \delta \in \llbracket \Delta \rrbracket. \forall E, S_1, S_2. \forall \vartheta \in \llbracket \psi \rrbracket. ((E, S_1), (E, S_2)) \in \llbracket \phi \rrbracket \wedge \forall x \in \text{FVV}(P). S_1(E(x)) = S_2(E(x)) \Rightarrow \\ \llbracket \Delta; \phi; \psi \vdash P : \omega \rrbracket(\delta; (E, S_1); \vartheta) = \llbracket \Delta; \phi; \psi \vdash P : \omega \rrbracket(\delta; (E, S_2); \vartheta) \end{aligned}$$

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

$$\forall \delta \in \llbracket \Delta \rrbracket. \forall (E, S) \in \llbracket \phi \rrbracket. \forall \vartheta \in \llbracket \psi \rrbracket.$$

$$\llbracket \Delta; \phi; \psi, a : \omega \vdash P : \omega' \rrbracket(\delta; (E, S); \vartheta, a \mapsto \llbracket \Delta; \phi; \psi \vdash M : \omega \rrbracket(\delta; (E, S); \vartheta)) = \llbracket \Delta; \phi; \psi \vdash P[M/a] : \omega' \rrbracket(\delta; (E, S); \vartheta)$$

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

$$\forall \delta \in \llbracket \Delta \rrbracket. \forall (E, S) \in \llbracket \phi, x \rrbracket. \forall \vartheta \in \llbracket \psi \rrbracket.$$

$$\llbracket \Delta; \phi, x; \psi \vdash P : \omega \rrbracket(\delta; (E, S[E(x) \mapsto \llbracket \Delta; \phi, x; \psi \vdash M : \text{Val} \rrbracket(\delta; (E, S); \vartheta)]); \vartheta) = \llbracket \Delta; \phi, x; \psi \vdash P[M/x] : \omega \rrbracket(\delta; (E, S); \vartheta)$$

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

$$\forall \delta \in \llbracket \Delta \rrbracket. \forall (E, S) \in \llbracket \phi \rrbracket. \forall \vartheta \in \llbracket \psi \rrbracket. \forall l \in \mathbb{L}_s \setminus \text{Dom}(S). \forall v \in \mathbb{V}.$$

$$\llbracket \Delta; \phi, x; \psi \vdash P : \omega \rrbracket(\delta; (E[x \mapsto l], S[l \mapsto v]); \vartheta) = \llbracket \Delta; \phi; \psi, x : \text{Val}, y : \text{Loc} \vdash P[y/\&x] : \omega \rrbracket(\delta; (E, S); \vartheta[x \mapsto v, y \mapsto l])$$

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

$$\forall \delta \in \llbracket \Delta \rrbracket. \forall (E, S) \in \llbracket \phi \rrbracket. \forall \vartheta \in \llbracket \psi \rrbracket. \forall l \in \mathbb{L}_s \setminus \text{Dom}(S). \forall v \in \text{Val}.$$

$$\llbracket \Delta; \phi, x; \psi \vdash P : \omega \rrbracket(\delta; (E[x \mapsto l], S[l \mapsto v]); \vartheta) = \llbracket \Delta; \phi; \psi, x : \text{Val} \vdash P : \omega \rrbracket(\delta; (E, S); \vartheta[x \mapsto v])$$

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

$$\forall \delta \in \llbracket \Delta \rrbracket. \forall (E, S) \in \llbracket \phi \rrbracket. \forall \vartheta \in \llbracket \psi \rrbracket.$$

$$\begin{aligned} \llbracket \Delta; \phi; \psi \vdash \text{lookup } L \text{ as } x \text{ in } P : \text{Prop} \rrbracket(\delta; (E, S); \vartheta) = \\ \{(n, C, H) \in \mathbb{N} \times \mathbb{S} \times \mathbb{H} \mid l \in \text{Dom}(C) \wedge \\ (n, C \setminus l, H) \in \llbracket \Delta; \phi; \psi, x : \text{Val} \vdash P : \text{Prop} \rrbracket(\delta; (E, S); \vartheta[x \mapsto C(l)])\} \end{aligned}$$

where $l = \llbracket \Delta; \phi; \psi \vdash L : \text{Loc} \rrbracket(\delta; (E, S); \vartheta)$.

3 Specification Logic

3.1 Syntax

$$\begin{aligned}
 S, T & ::= \{P\}S\{Q\} \triangleleft M \mid \{P\}S\{d.Q\} \triangleleft M && \text{Specifications} \\
 M & \in \mathcal{P}_{fin}(\mathbb{A}_p) \\
 MS & ::= C\langle\Delta\rangle.m : \langle(\phi; \psi).\{P\}_-\{d.Q\}\rangle && \text{method specification} \\
 \Gamma & ::= \Gamma, MS \mid \epsilon && \text{program context}
 \end{aligned}$$

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

3.2 Typing rules

Well-formed Specifications

$$\boxed{\Delta; \phi; \psi \vdash S : \text{Spec}}$$

$$\frac{\Delta; \phi; \psi \vdash P : \text{Prop} \quad \Delta; \phi; \psi \vdash Q : \text{Prop} \quad M \subseteq \phi}{\Delta; \phi; \psi \vdash \{P\}S\{Q\} \triangleleft M : \text{Spec}}$$

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

Well-formed Contexts

$$\boxed{\Gamma : \text{Context}}$$

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

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

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

3.3 Proof rules

Statements

$$\boxed{\Gamma; \phi; \psi \vdash \{P\}_s \{Q\} \triangleleft M}$$

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

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

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

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

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

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

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

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

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

$$\frac{\Gamma; \Delta; \phi, x, y; \psi \vdash \{P \wedge x = y\}_{s_1} \{Q\} \triangleleft M_1 \quad \Gamma; \Delta; \phi, x, y; \psi \vdash \{P \wedge \neg(x = y)\}_{s_2} \{Q\} \triangleleft M_2}{\Gamma; \Delta; \phi, x, y; \psi \vdash \{P\} \text{if } (x == y) \{s_1\} \text{ else } \{s_2\} \{Q\} \triangleleft M_1 \cup M_2}$$

Structural Rules

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

$$\frac{\Gamma; \Delta; \phi; \psi, a : \omega \vdash \{P\}s\{Q\} \triangleleft M_2 \quad a \notin FV(P)}{\Gamma; \Delta; \phi; \psi \vdash \{P\}s\{\forall a : \omega. Q\} \triangleleft M_2}$$

$$\frac{\Gamma; \Delta; \phi; \psi \vdash \{P\}s_1\{Q\} \triangleleft M_1 \quad \Gamma; \Delta; \phi; \psi \vdash \{Q\}s_2\{R\} \triangleleft M_2}{\Gamma; \Delta; \phi; \psi \vdash \{P\}s_1; s_2\{R\} \triangleleft M_1 \cup M_2} \quad (\text{seq})$$

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

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

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

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

$$\frac{\Gamma; \Delta; \phi; \psi \vdash \{P_1\}s\{Q_1\} \triangleleft M_1 \quad \Gamma; \Delta; \phi; \psi \vdash \{P_2\}s\{Q_2\} \triangleleft M_2 \quad op \in \{\wedge, \vee\}}{\Gamma; \Delta; \phi; \psi \vdash \{P_1 \text{ op } P_2\}s\{Q_1 \text{ op } Q_2\} \triangleleft M_1 \cup M_2}$$

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

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

Method definitions

$$\boxed{\Gamma \vdash M : \Gamma'}$$

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

$$\frac{\Gamma; \Delta; \phi; \psi \vdash \{P\}s\{Q\} \triangleleft M_1 \quad \Gamma; \Delta; \phi; \psi \vdash \{Q\}s; \text{return } x\{d.R\} \triangleleft M_2}{\Gamma; \Delta; \phi; \psi \vdash \{P\}s; s; \text{return } x\{d.R\} \triangleleft M_1 \cup M_2}$$

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

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

$$\frac{\text{this}, \bar{u} \notin M \cup FVA(P, Q) \quad MS = C(\Delta).m : \langle (\bar{u}; \psi). \{P\} - \{d.Q\} \rangle}{\Gamma, MS; \Delta; \bar{u}, \text{this}; \psi \vdash \{P\}\bar{G}\bar{z}; s; \text{return } x\{d.Q\} \triangleleft M} \quad \Gamma, MS; \Delta \vdash G m(\bar{G}\bar{u}) \{ \bar{G}\bar{z}; s \text{ return } x; \} : MS$$

Class definitions

$$\boxed{\Gamma \vdash L : \Gamma'}$$

$$\frac{\forall i \in \text{Dom}(\bar{M}). \Gamma; \bar{T} \vdash M_i : \Gamma_i}{\Gamma \vdash \text{class } C(\bar{T}) : D \{ \text{public } \bar{C}f; \bar{M} \} : \bar{\Gamma}}$$

Programs

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

$$\frac{\forall i \in \text{Dom}(\bar{L}). \Gamma_i \vdash L_i : \Gamma_i \quad \bar{\Gamma}; -, \bar{x}; \psi \vdash \{P\}s\{Q\} \triangleleft M}{\bar{\Gamma}; \psi \vdash \{P\}\bar{L}; \bar{C} \bar{x}; s\{Q\} \triangleleft M}$$

3.4 Semantics

Specifications

$$\boxed{\llbracket \Delta; \phi; \psi \vdash S : \text{Spec} \rrbracket : \llbracket \Delta \rrbracket \times \llbracket \phi \rrbracket \times \llbracket \psi \rrbracket \rightarrow \{U \in \mathcal{P}^{\downarrow}(\mathbf{N}) \mid 0 \in U\}}$$

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

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

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

Context Specification

$$\boxed{\llbracket MS : \text{Context-Spec} \rrbracket : \{U \in \mathcal{P}^{\downarrow}(\mathbf{N}) \mid 0 \in U\}}$$

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

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

Context

$$\boxed{\llbracket \Gamma : \text{Context} \rrbracket : \{U \in \mathcal{P}^{\downarrow}(\mathbf{N}) \mid 0 \in U\}}$$

$$\llbracket \Gamma : \text{Context} \rrbracket = \bigcap_{MS \in \Gamma} \llbracket MS : \text{Context-Spec} \rrbracket$$

Entailment

$$\boxed{\llbracket \Gamma; \Delta; \phi; \psi \vdash S : \text{Spec} \rrbracket : 2}$$

$$\begin{aligned} \llbracket \Gamma; \Delta; \phi; \psi \vdash S : \text{Spec} \rrbracket &= \forall n \in \mathbf{N}. \forall (E, S) \in \llbracket \phi \rrbracket. \forall \vartheta \in \llbracket \psi \rrbracket. \forall \delta \in \llbracket \Delta \rrbracket. \\ n \in \llbracket \Gamma : \text{Context} \rrbracket &\Rightarrow n+1 \in \llbracket \Gamma; \Delta; \phi; \psi \vdash S : \text{Spec} \rrbracket (\delta; (E, S); \vartheta) \end{aligned}$$

Others

$$\llbracket \Gamma; \bar{T} \vdash \text{public } C \text{ m}(\bar{C}\bar{u}) \text{ B} : MS \rrbracket = \forall n \in \mathbf{N}. n \in \llbracket \Gamma : \text{Context} \rrbracket \Rightarrow n + 1 \in \llbracket C(\bar{T}).\text{m} : MS : \text{Context-Spec} \rrbracket$$

$$\begin{aligned} \llbracket \Gamma \vdash \text{class } C(\bar{T}) : G \{ \text{public } \bar{C}\bar{f}; \bar{M} \} : MS_K, \bar{M}S \rrbracket = \\ \text{Dom}(\bar{M}S) = \text{Dom}(\bar{M}) \wedge \forall i \in \text{Dom}(\bar{M}). \llbracket \Gamma; \bar{T} \vdash \bar{M}_i : \bar{M}S_i \rrbracket \end{aligned}$$

$$\llbracket \bar{\Gamma}; \psi \vdash \{P\}\bar{L}; \bar{C}\bar{x}; s\{Q\} \triangleleft M \rrbracket = \llbracket \bar{\Gamma}; -; \bar{x}; \psi \vdash \{P\}s\{Q\} \triangleleft M \rrbracket \wedge \forall i \in \text{Dom}(\bar{L}). \llbracket \Gamma \vdash \bar{L}_i : \Gamma_i \rrbracket$$

3.5 Metatheory

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

Lemma 15. *If $\forall i \in \text{Dom}(\bar{L}). \llbracket \Gamma \vdash \bar{L}_i : \Gamma_i \rrbracket$ then $\llbracket \Gamma : \text{Context} \rrbracket = \mathbb{N}$.*

Lemma 16. *Rule (α) is sound.*

$$\forall \pi \in \text{Perm}(\mathbb{A}_p). \llbracket \Gamma; \Delta; \phi; \psi \vdash \{P\}s\{Q\} \triangleleft M \rrbracket = \llbracket \Gamma; \Delta; \pi(\phi); \pi(\psi) \vdash \{\pi(P)\}\pi(s)\{\pi(Q)\} \triangleleft \pi(M) \rrbracket$$

Proof. Let $n, m, k \in \mathbb{N}$ such that $k \leq m \leq n + 1$. Assume $n \in \llbracket \Gamma : \text{Context} \rrbracket$,

$$(m - 1, C, H) \in \llbracket \Delta; \pi(\phi); \pi(\psi) \vdash \pi(P) : \text{Prop} \rrbracket(\delta; (E, S); \vartheta)$$

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

$$(m - 1, C, \pi^{-1}(H)) \in \llbracket \Delta; \phi; \psi \vdash P : \text{Prop} \rrbracket(\delta; (\pi^{-1}(E), S); \pi^{-1}(\vartheta))$$

Hence,

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

and thus by alpha-renaming,

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

Correctness: If

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

then by alpha-renaming,

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

and thus,

$$(m - k, S' \setminus \pi^{-1}(E)(\phi), \pi^{-1}(H')) \in \llbracket \Delta; \phi; \psi \vdash Q : \text{Prop} \rrbracket(\delta; (\pi^{-1}(E), S' \upharpoonright_{\pi^{-1}(E)(\phi)}); \pi^{-1}(\vartheta))$$

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

$$(m - k, S' \setminus E(\pi(\phi)), H') \in \llbracket \Delta; \pi(\phi); \pi(\psi) \vdash \pi(Q) : \text{Prop} \rrbracket(\delta; (E, S' \upharpoonright_{E(\pi(\phi))}); \vartheta)$$

□

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

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

Proof. Let $n, m, k \in \mathbb{N}$ such that $k \leq m \leq n + 1$. Assume $n \in \llbracket \Gamma : \mathbf{Context} \rrbracket$,

$$(m - 1, C_1, H_1) \in \llbracket \Delta; \phi; \psi \vdash P : \mathbf{Prop} \rrbracket(\delta; (E, S); \vartheta)$$

$$(m - 1, C_2, H_2) \in \llbracket \Delta; \phi; \psi \vdash R : \mathbf{Prop} \rrbracket(\delta; (E, S); \vartheta)$$

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

By assumption,

$$\llbracket \Delta; \phi; \psi \vdash \{P\} \mathbf{s} \{Q\} \triangleleft M \rrbracket(\delta; (E, S); \vartheta, n + 1)$$

and thus,

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

and by safety monotonicity,

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

Correctness: If

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

then by the stack and heap frame properties it follows that there exists a S'_1 and H'_1 such that,

$$(E, C_1 \uplus S, H_1, \mathbf{s}) \Downarrow_k (S'_1, H'_1)$$

and $S' = C_2 \uplus S'_1$ and $H' = H_2 \uplus H'_1$. Hence,

$$(m - k, S'_1 \setminus E(\phi), H'_1) \in \llbracket \Delta; \phi; \psi \vdash Q : \mathbf{Prop} \rrbracket(\delta; (E, S'_1|_{E(\phi)}); \vartheta)$$

Furthermore,

$$\llbracket \Delta; \phi; \psi \vdash R : \mathbf{Prop} \rrbracket(\delta; (E, S); \vartheta) = \llbracket \Delta; \phi; \psi \vdash R : \mathbf{Prop} \rrbracket(\delta; (E, S'_1|_{E(\phi)}); \vartheta)$$

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

$$(m - k, C_2 \setminus E(\phi), H_2) \in \llbracket \Delta; \phi; \psi \vdash R : \mathbf{Prop} \rrbracket(\delta; (E, S'_1|_{E(\phi)}); \vartheta)$$

and thus finally,

$$(m - k, (S'_1 \uplus C_2) \setminus E(\phi), H'_1 \uplus H_2) \in \llbracket \Delta; \phi; \psi \vdash P * R : \mathbf{Prop} \rrbracket(\delta; (E, S'_1|_{E(\phi)}); \vartheta)$$

□

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

$$\frac{\Gamma; \Delta; \phi; \psi \vdash \{P\}s_1\{Q\} \triangleleft M_1 \quad \Gamma; \Delta; \phi; \psi \vdash \{Q\}s_2\{R\} \triangleleft M_2}{\Gamma; \Delta; \phi; \psi \vdash \{P\}s_1; s_2\{R\} \triangleleft M_1 \cup M_2}$$

Proof. Let $n, m, k \in \mathbb{N}$ such that $k \leq m \leq n + 1$. Assume $n \in \llbracket \Gamma : \text{Context} \rrbracket$,

$$(m - 1, C, H) \in \llbracket \Delta; \phi; \psi \vdash P : \text{Prop} \rrbracket(\delta; (E, S); \vartheta)$$

and $C \# S$.

Safety: By assumption,

$$\llbracket \Delta; \phi; \psi \vdash \{P\}s_1\{Q\} \triangleleft M_1 \rrbracket(\delta; (E, S); \vartheta; n + 1)$$

and thus,

$$(E; C \uplus S; H; s_1) : \text{safe}_m$$

Hence, for any $l \leq k$ if $(E; C \uplus S; H; s_1; s_2) \Downarrow_l \text{err}$ then there exists l_1, l_2, S' , and H' such that,

$$(E; C \uplus S; H; s_1) \Downarrow_{l_1} (S', H')$$

$$(E; S'; H'; s_2) \Downarrow_{l_2} \text{err}$$

and $l = l_1 + l_2$. Hence,

$$(m - l_1; S' \setminus E(\phi); H') \in \llbracket \Delta; \phi; \psi \vdash Q : \text{Prop} \rrbracket(\delta; (E, S'|_{E(\phi)}); \vartheta)$$

and thus

$$(E; (S' \setminus E(\phi)) \uplus S'|_{E(\phi)}; H'; s_2) : \text{safe}_{m-l_1+1}$$

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

$$(E; S'; H'; s_2) \not\Downarrow_{l_2} \text{err}$$

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,

$$(m - k_1; S'' \setminus E(\phi); H'') \in \llbracket \Delta; \phi; \psi \vdash Q : \text{Prop} \rrbracket(\delta; (E, S''|_{E(\phi)}); \vartheta)$$

Furthermore, by assumption,

$$\llbracket \Delta; \phi; \psi \vdash \{Q\}s_2\{R\} \triangleleft M_2 \rrbracket(\delta; (E, S''|_{E(\phi)}); \vartheta; n + 1)$$

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

$$(m - k_1 + 1 - k_2; S' \setminus E(\phi); H') \in \llbracket \Delta; \phi; \psi \vdash R : \text{Prop} \rrbracket(\delta; (E, S'|_{E(\phi)}); \vartheta)$$

and by upwards-closure:

$$(m - k; S' \setminus E(\phi); H') \in \llbracket \Delta; \phi; \psi \vdash R : \text{Prop} \rrbracket(\delta; (E, S'|_{E(\phi)}); \vartheta)$$

□

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

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

Proof. Let $n, m, k \in \mathbb{N}$ such that $k \leq m \leq n + 1$. Assume $n \in \llbracket \Gamma : \text{Context} \rrbracket$,

$$(m - 1; C; H) \in \llbracket \Delta; \phi, x; \psi \vdash \&x = l \wedge P : \text{Prop} \rrbracket(\delta; (E, S); \vartheta)$$

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

$$(m - 1; C; H) \in \llbracket \Delta; \phi, x; \psi \vdash P : \text{Prop} \rrbracket(\delta; (E, S); \vartheta)$$

and by splitting,

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

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

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

and by assumption:

$$\llbracket \Delta; \phi; \psi \vdash \{\text{lookup } l \text{ as } x \text{ in } P\} \mathfrak{s} \{\text{lookup } l \text{ as } x \text{ in } Q\} \triangleleft M \rrbracket(\delta; (E|_\phi; S \setminus E(x)); \vartheta; n + 1)$$

Safety: Hence,

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

and by weakening,

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

Correctness: Furthermore, if

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

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

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

and thus,

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

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

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

and by splitting,

$$(m - k; S' \setminus E(\phi, x); H') \in \llbracket \Delta; \phi, x; \psi \vdash Q : \text{Prop} \rrbracket(\delta; (E, S'|_{E(\phi, x)}); \vartheta)$$

□

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

$$\frac{\bar{u} \cup \bar{y} = \text{FV}(\mathbf{B}) \quad \Gamma; \Delta; \bar{y}, \bar{u}; \psi \vdash \{\mathbf{P}\}\mathbf{B}\{\mathbf{d}, \mathbf{Q}\} \triangleleft \mathbf{M} \quad \bar{u} \notin \mathbf{M}}{\Delta; \bar{y}; \psi, \bar{u} \vdash \mathbf{P} : \mathbf{Prop} \quad \Delta; \bar{y}; \psi, \bar{u}, \mathbf{d} \vdash \mathbf{Q} : \mathbf{Prop}}$$

$$\Gamma; \Delta; \bar{y}, \mathbf{x}; \psi, \bar{l} \vdash \{\bar{l} = \&\bar{y}\}\mathbf{x} = \lambda \bar{u}. \{\mathbf{B}\}; \{\mathbf{x} \mapsto \langle (\bar{u}).\{\text{lookup } \bar{l} \text{ as } \bar{z} \text{ in } \mathbf{P}[\bar{l}/\&\bar{y}][\bar{z}/\bar{y}]\} - \{\mathbf{d}.\text{lookup } \&l \text{ as } \bar{z} \text{ in } \mathbf{Q}[\bar{l}/\&\bar{y}][\bar{z}/\bar{y}]\}\} \triangleleft \{\mathbf{x}\}$$

Proof. Let $n, m, k \in \mathbb{N}$ such that $k \leq m \leq n + 1$. Assume $n \in \llbracket \Gamma : \text{Context} \rrbracket$,

$$(m - 1, C, H) \in \llbracket \Delta; \bar{y}, \mathbf{x}; \psi, \bar{l} \vdash \bar{l} = \&\bar{y} : \mathbf{Prop} \rrbracket(\delta; (E, S); \vartheta)$$

and $C \# S$. If,

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

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

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

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

Hence,

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

and by strengthening and renaming,

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

and splitting,

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

Futhermore, by assumption,

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

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

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

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

Correctness: If,

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

then,

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

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

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

and weakening,

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

and hence,

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

□

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

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

Proof. Let $n, m, k \in \mathbb{N}$ such that $k \leq m \leq n + 1$. Assume $n \in \llbracket \Gamma : \text{Context} \rrbracket$,

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

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

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

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

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

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

and

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

Hence,

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

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

Correctness: If

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

then

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

and $S' = S''[E(x) \mapsto S''(E'_c(r))]$ and $H' = H''$. By the stack and heap frame property there exists C'_2 and H'_2 such that,

$$(\delta_c, E'_c; C_2[\bar{l}_u \mapsto S(E(\bar{x})), \bar{l}_z \mapsto \text{null}]; H_2; s) \Downarrow_{k-1} (C'_2, H'_2)$$

and $S'' = C_1 \uplus S \uplus C'_2$ and $H'' = H_1 \uplus H'_2$. Hence,

$$((m-1)-(k-1); C'_2 \setminus \bar{l}_u; H'_2) \in \llbracket \Delta; \phi, \bar{x}; \psi, \bar{u}, d \vdash Q : \text{Prop} \rrbracket(\delta; (E|_{\phi, \bar{x}}, S|_{E(\phi, \bar{x})}); \vartheta[\bar{u} \mapsto S(E(\bar{x})), d \mapsto C'_2(E'_c(r))])$$

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

$$(m - k; C'_2 \setminus \bar{l}_u; H'_2) \in \llbracket \Delta; \phi, \bar{x}; \psi, x \vdash Q[\bar{x}/\bar{u}, x/d] : \text{Prop} \rrbracket(\delta; (E|_{\phi, \bar{x}}, S''|_{E(\phi, \bar{x})}); \vartheta[x \mapsto C'_2(E'_c(r))])$$

and by splitting again,

$$(m - k; C'_2 \setminus \bar{l}_u; H'_2) \in \llbracket \Delta; \phi, \bar{x}, x; \psi \vdash Q[\bar{x}/\bar{u}, x/d] : \text{Prop} \rrbracket(\delta; (E, S''|_{E(\phi, \bar{x})}[E(x) \mapsto C'_2(E'_c(r))]); \vartheta)$$

Hence, by upwards-closure,

$$(m - k; (S \uplus C'_2) \setminus E(\phi, \bar{x}, x); H'_2) \in \llbracket \Delta; \phi, \bar{x}, x; \psi \vdash Q[\bar{x}/\bar{u}, x/d] : \text{Prop} \rrbracket(\delta; (E, S'|_{E(\phi, \bar{x}, x)}); \vartheta)$$

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

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

□

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

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

Proof. Let $n, m, k \in \mathbb{N}$ such that $k \leq m \leq n + 1$. Assume $n \in \llbracket \Gamma : \mathit{Context} \rrbracket$,

$$(m - 1; C; H) \in \llbracket \Delta; \phi; \psi \vdash P : \mathit{Prop} \rrbracket(\delta; (E, S); \vartheta)$$

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

$$(m - 1; C; H) \in \llbracket \Delta; \phi; \bar{z}; \psi \vdash P : \mathit{Prop} \rrbracket(\delta; (E', S'); \vartheta)$$

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

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

and if,

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

then

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

splitting the zs into their values and locations we get:

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

and thus, by definition,

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

□

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  $\wedge$  list(front, xs, P) * list(tail, ys, P) }
    { xs = []  $\wedge$  list(tail, ys, P) }
    { list(tail, xs@ys, P) }
    return tail;
    { r. list(r, xs@ys, P) }
  } else {
    { front != null  $\wedge$  list(front, xs, P) * list(tail, ys, P) }
    {  $\exists v, xs', n, x. xs = v::xs' \wedge$  front.next  $\mapsto$  n * front.item  $\mapsto$  x * P(x, v) * list(n, xs', P) * list(tail, ys, P) }
    tmp2 = front.next;
    {  $\exists v, xs', x. xs = v::xs' \wedge$  front.next  $\mapsto$  tmp2 * front.item  $\mapsto$  x * P(x, v) * list(tmp2, xs', P) * list(tail, ys, P) }
    tmp = append<X>(tmp2, tail);
    {  $\exists v, xs', x. xs = v::xs' \wedge$  front.next  $\mapsto$  tmp2 * front.item  $\mapsto$  x * P(x, v) * list(tmp, xs'@ys, P) }
    front.next = tmp;
    {  $\exists v, xs', x. xs = v::xs' \wedge$  front.next  $\mapsto$  tmp * front.item  $\mapsto$  x * P(x, v) * list(tmp, xs'@ys, P) }
    { list(front, xs@ys, P) }
    return front;
    { r. list(r, xs@ys, P) }
  }
}
```