15-312 Assignment 1

Andrew Carnegie
(andrew)

October 25, 2017

Type	τ ::=		
	$\texttt{nat}$	$\texttt{nat}$	naturals
	$\texttt{unit}$	$\texttt{unit}$	unit
	$\texttt{bool}$	$\texttt{bool}$	boolean
	$\texttt{prod}(\tau_1;\tau_2)$	$\tau_1 \times \tau_2$	product
	$\texttt{arr}(\tau_1;\tau_2)$	$\tau_1 \to \tau_2$	function
	$\texttt{list}(\tau)$	$\tau\,\texttt{list}$	list
Exp	e ::=		
	x	x	variable
	$\texttt{nat}[n]$	$\overline{n}$	number
	$\texttt{unit}$	$()$	unit
	$\texttt{T}$	$\texttt{T}$	true
	$\texttt{F}$	$\texttt{F}$	false
	$\texttt{if}(x;e_1;e_2)$	$\texttt{if}\,x\,\texttt{then}\,e_1\,\texttt{else}\,e_2$	if
	$\texttt{lam}(x:\tau.e)$	$\lambda\, x:\tau.e$	abstraction
	$\texttt{ap}(f;x)$	$f(x)$	application
	$\texttt{tpl}(x_1;x_2)$	$\langle x_1, x_2\rangle$	pair
	$\texttt{case}(x_1,x_2.e_1)$	$\texttt{case}\ p\ \{(x_1;x_2) \hookrightarrow e_1\}$	match pair
	$\texttt{nil}$	$[]$	nil
	$\texttt{cons}(x_1;x_2)$	$x_1 :: x_2$	cons
	$\texttt{case}\{l\}(e_1;x,xs.e_2)$	$\texttt{case}\,l\,\{\texttt{nil} \hookrightarrow e_1 \mid \texttt{cons}(x;xs) \hookrightarrow e_2\}$	match list
	$\texttt{let}(e_1;x:\tau.e_2)$	$\texttt{let}\ x = e_1\ \texttt{in}\ e_2$	let
Val	v ::=		
	$\texttt{val}(n)$	n	numeric value
	$\texttt{val}(\texttt{T})$	$\texttt{T}$	true value
	$\texttt{val}(\texttt{F})$	$\texttt{F}$	false value
	$\texttt{val}(\texttt{Null})$	$\texttt{Null}$	null value
	$\texttt{val}(\texttt{cl}(V;x.e))$	$(V, x.e)$	function value
	$\texttt{val}(l)$	l	loc value
	$\texttt{val}(\texttt{pair}(v_1;v_2))$	$\langle v_1, v_2\rangle$	pair value
State	s ::=		
	$\texttt{alive}$	$\texttt{alive}$	live value
	$\texttt{dead}$	$\texttt{dead}$	dead value
Loc	l ::=		
	$\texttt{loc}(l)$	l	location
Var	l ::=		
	$\texttt{var}(x)$	x	variable

1 Paths and aliasing

Model dynamics using judgement of the form:

$$\boxed{V, H, R, F \ \vdash e \Downarrow v, H', F'}$$

Where $V : \mathsf{Var} \to \mathsf{Val} \times \mathsf{State}$, $H : \mathsf{Loc} \to \mathsf{Val}$, $R \subseteq \mathsf{Loc}$, and $F \subseteq \mathsf{Loc}$. This can be read as: under stack V, heap H, roots R, freelist F, the expression e evaluates to v, and engenders a new heap H' and freelist F'.

For a partial map $f : A \to B$, we write *dom* for the defined values of f. Sometimes we shorten $x \in dom(f)$ to $x \in f$. We write $f[x \mapsto y]$ for the extension of f where x is mapped to y, with the constraint that $x \notin dom(f)$. We write $f\{x \mapsto y\}$ for the update map, which is the same as the extension map, except that x is remapped to y when $x \in dom(f)$. Write $C \lhd f : C \to B$ for the domain restriction of f to C where $C \subseteq A$. Write $C \unlhd f : (A \setminus C) \to B$ for the domain anti-restriction of f to C.

Note that the stack maps each variable to a value v *and* a state s. If s is alive, then v can still be used, while `dead` indicates that v is already used and cannot be used again. We write $\overline{V} = \{x \in V \mid V(x) = (\_, \texttt{alive})\}$ for the variables in V that are alive, and $V^\star : \overline{V} \to \mathsf{Val}$ for the associated restricted map $x \mapsto fst(V(x))$ which projects out the value component of live variables.

Roots represents the set of locations required to compute the continuation *excluding* the current expression. We can think of roots as the heap allocations necessary to compute the context with a hole that will be filled by the current expression.

In order prove soundness of the type system, we need some auxiliary judgements to defining properties of a heap. Below we define $reach : Val \to \{\{Loc\}\}$ that maps stack values its the root *multiset*, the multiset of locations that's already on the stack.
Next we define reachability of values:

$$\begin{aligned}
&reach_H(\langle v_1, v_2\rangle) = reach_H(v_1) \uplus reach_H(v_2)\\
&reach_H(l) = \{l\} \uplus reach_H(H(l))\\
&reach_H(_) = \emptyset
\end{aligned}$$

For a multiset S, we write $\mu_S : S \to \mathbb{N}$ for the multiplicity function of S, which maps each element to the count of its occurence. If $\forall s \in S.\mu(s) = 1$, then S is a property set, and we denote it by $\mathsf{set}(S)$. Addtionally, $A \uplus B$ denotes counting union of sets where $\mu_{A\uplus B}(s) = \mu_A(s) + \mu_B(s)$, and $A \cup B$ denotes the usual union where $\mu_{A\cup B}(s) = \max(\mu_A(s), \mu_B(s))$. For the disjoint union of sets A and B, we write $A \sqcup B$.

Next, we define the predicates $\mathsf{no\_alias}$, $\mathsf{no\_ref}$, and $\mathsf{disjoint}$:

$\mathsf{no\_alias}(V, H)$**:** $\forall x, y \in \overline{V}$, $x \neq y$. Let $r_x = reach_H(\overline{V}(x))$, $r_y = reach_H(\overline{V}(y))$. Then:

1. $\mathsf{set}(r_x), \mathsf{set}(r_y)$

2. $r_x \cap r_y = \emptyset$

$\mathsf{no\_ref}(V, H, v)$**:** $(reach_H(v)) \cap (\bigcup_{x \in \overline{V}} reach_H(V(x))) = \emptyset$.

$\mathsf{disjoint}(\mathcal{C})$**:** $\forall X, Y \in \mathcal{C}.\ X \cap Y = \emptyset$

For a stack V and a heap H, whenever $\mathsf{no\_alias}(V, H)$ holds, visually, one can think of the situation as the following: the induced graph of heap H with variables on the stack as additional leaf nodes is a forest: a disjoint union of arborescences (directed trees); consequently, there is at most one path from a live variable on the stack V to a location in H by following the pointers.

Next, we define $locs_{V,H}$ using the previous notion of reachability. $size$ calculates the number of cells a value occupies. $copy(H, L, v)$ takes a heap H, a set of locations L, and a value v, and returns a new heap H' and a location l such that l maps to v in H'.

$$locs_{V,H}(e) = \bigcup_{x \in FV(e)} reach_H(V(x))$$

$$\begin{aligned}
&size(\langle v_1, v_2 \rangle) = size(v_1) + size(v_2) \\
&size(_) = 1
\end{aligned}$$

$$\begin{aligned}
&copy(H, L, \langle v_1, v_2 \rangle) = \\
&\quad \mathsf{let}\ L_1 \sqcup L_2 \subseteq L \\
&\quad\quad \mathsf{where}\ |L_1| = size(v_1)\ , |L_2| = size(v_2) \\
&\quad \mathsf{let}\ H_1 = copy(H, L_1, v_1) \\
&\quad \mathsf{let}\ H_2 = copy(H_1, L_2, v_2)\ \mathsf{in} \\
&\quad H_2[l \mapsto v] \\
&copy(H, L, v) = \\
&\quad \mathsf{let}\ l \in H\ \mathsf{in} \\
&\quad H[l \mapsto v]
\end{aligned}$$

2 Garbage collection semantics

$$\frac{V(x) = (v, \texttt{alive})}{V, H, R, F \ \vdash x \Downarrow v, H, F}(\mathrm{S}_1) \qquad \frac{}{V, H, R, F \ \vdash \overline{n} \Downarrow \texttt{val}(n), H, F}(\mathrm{S}_2)$$

$$\frac{}{V, H, R, F \ \vdash \texttt{T} \Downarrow \texttt{val}(\texttt{T}), H, F}(\mathrm{S}_3) \qquad \frac{}{V, H, R, F \ \vdash \texttt{F} \Downarrow \texttt{val}(\texttt{F}), H, F}(\mathrm{S}_4)$$

$$\frac{}{V, H, R, F \ \vdash () \Downarrow \texttt{val}(\texttt{Null}), H, F}(\mathrm{S}_5)$$

$$\frac{V(x) = \texttt{T} \qquad g = \{l \in H \mid l \notin F \cup R \cup \mathit{locs}_{V,H}(e_1)\} \qquad V, H, R, F \cup g \ \vdash e_1 \Downarrow v, H', F'}{V, H, R, F \ \vdash \texttt{if}(x; e_1; e_2) \Downarrow v, H', F'}(\mathrm{S}_6)$$

$$\frac{V(x) = \texttt{F} \qquad g = \{l \in H \mid l \notin F \cup R \cup \mathit{locs}_{V,H}(e_2)\} \qquad V, H, R, F \cup g \ \vdash e_2 \Downarrow v, H', F'}{V, H, R, F \ \vdash \texttt{if}(x; e_1; e_2) \Downarrow v, H', F'}(\mathrm{S}_7)$$

$$\frac{l \in F \qquad F' = F \setminus \{l\} \qquad H' = H[l \mapsto (V, x.e)]}{V, H, R, F \ \vdash \texttt{lam}(x : \tau.e) \Downarrow l, H', F'}(\mathrm{S}_8)$$

$$\frac{V(f) = (V_1, x.e) \qquad V(x) = v_1 \qquad V_1[x \mapsto v_1], H, R \ \vdash e \Downarrow v, H', F'}{V, H, R, F \ \vdash f(x) \Downarrow v, H', F'}(\mathrm{S}_9)$$

$$\frac{V(x_1) = v_1 \qquad V(x_2) = v_2}{V, H, R, F \ \vdash \langle x_1, x_2 \rangle \Downarrow \langle v_1, v_2 \rangle, H, F}(\mathrm{S}_{10})$$

$$\frac{\begin{array}{c} V(x) = \langle v_1, v_2 \rangle \\ g = \{l \in H \mid l \notin F \cup R \cup \mathit{locs}_{V,H}(e)\} \qquad V[x_1 \mapsto v_1, x_2 \mapsto v_2], H, R, F \cup g \ \vdash e \Downarrow v, H', F' \end{array}}{V, H, R, F \ \vdash \texttt{case}\ x\ \{(x_1; x_2) \hookrightarrow e\} \Downarrow v, H', F'}(\mathrm{S}_{11})$$

$$\frac{}{V, H, R, F \ \vdash \texttt{nil} \Downarrow \texttt{val}(\texttt{Null}), H, F}(\mathrm{S}_{12})$$

$$\frac{\begin{array}{c} v = \langle V(x_1), V(x_2) \rangle \qquad L \sqcup \{l\} \subseteq F \\ |L| = \mathit{size}_H(v) \qquad F' = F \setminus (L \sqcup \{l\}) \qquad H' = \mathit{copy}(H, L, v) \qquad H'' = H'[l \mapsto v] \end{array}}{V, H, R, F \ \vdash \texttt{cons}(x_1; x_2) \Downarrow l, H'', F'}(\mathrm{S}_{13})$$

$$\frac{V(x) = \texttt{Null} \qquad g = \{l \in H \mid l \notin F \cup R \cup \mathit{locs}_{V',H}(e_1)\} \qquad V, H, R, F \cup g \ \vdash e_1 \Downarrow v, H', F'}{V, H, R, F \ \vdash \texttt{case}\, x\, \{\texttt{nil} \hookrightarrow e_1 \mid \texttt{cons}(x_h; x_t) \hookrightarrow e_2\} \Downarrow v, H', F'}(\mathrm{S}_{14})$$

$$\frac{\begin{array}{c} V(x) = (l, \texttt{alive}) \\ H(l) = \langle v_h, v_t \rangle \qquad V' = V\{x \mapsto (l, \texttt{dead})\} \qquad V'' = V'[x_h \mapsto (v_h, \texttt{alive}), x_t \mapsto (v_t, \texttt{alive})] \\ g = \{l \in H \mid l \notin F \cup R \cup \mathit{locs}_{V'',H}(e_2)\} \qquad V'', H, R, F \cup g \ \vdash e_2 \Downarrow v, H', F' \end{array}}{V, H, R, F \ \vdash \texttt{case}\, x\, \{\texttt{nil} \hookrightarrow e_1 \mid \texttt{cons}(x_h; x_t) \hookrightarrow e_2\} \Downarrow v, H', F'}(\mathrm{S}_{15})$$

$$\frac{\begin{array}{c} R' = R \cup \mathit{locs}_{V,H}(\texttt{lam}(x : \tau.e_2)) \qquad V, H, R', F \vdash e_1 \Downarrow v_1, H_1, F_1 \\ V' = V\{z \mapsto (l, \texttt{dead}) \mid z \in FV(e_1) \wedge V(z) = (l, \_)\} \qquad V'' = V'[x \mapsto (v_1, \texttt{alive})] \\ R'' = R \cup \mathit{locs}_{V',H_1}(e_2) \qquad g = \{l \in H_1 \mid l \notin R'' \cup F_1\} \qquad V'', H_1, R, F_1 \cup g \vdash e_2 \Downarrow v_2, H_2, F_2 \end{array}}{V, H, R, F \ \vdash \texttt{let}(e_1; x : \tau.e_2) \Downarrow v_2, H_2, F_2}(\mathrm{S}_{16})$$

3 Operational semantics

In order to prove the soundess of the type system, we also define a simplified operational semantics that does not account for garbage collection.

$$\boxed{V, H \vdash e \Downarrow v, H'}$$

This can be read as: under stack V, heap H the expression e evaluates to v, and engenders a new heap H'. We write the representative rules.

$$\frac{v = \langle V(x_1), V(x_2)\rangle \qquad H', l = \mathit{copy}(H, L, v)}{V, H \ \vdash \mathtt{cons}(x_1; x_2) \Downarrow l, H'} (\mathrm{S}_{17})$$

$$\frac{\begin{array}{c} V(x) = (l, \mathtt{alive}) \qquad H(l) = \langle v_h, v_t\rangle \qquad V' = V\{x \mapsto (l, \mathtt{dead})\} \\ V'' = V'[x_h \mapsto (v_h, \mathtt{alive}), x_t \mapsto (v_t, \mathtt{alive})] \qquad V'', H \ \vdash e_2 \Downarrow v, H' \end{array}}{V, H \ \vdash \mathtt{case}\, x\, \{\mathtt{nil} \hookrightarrow e_1 \mid \mathtt{cons}(x_h; x_t) \hookrightarrow e_2\} \Downarrow v, H'} (\mathrm{S}_{18})$$

$$\frac{V, H \vdash e_1 \Downarrow v_1, H_1 \qquad V' = V[x \mapsto v_1] \qquad V', H_1 \vdash e_2 \Downarrow v_2, H_2}{V, H \ \vdash \mathtt{let}(e_1; x : \tau.e_2) \Downarrow v_2, H_2} (\mathrm{S}_{19})$$

4 Type rules

The type system takes into account of garbaged collected cells by returning potential locally in a match construct. Since we are interested in the number of heap cells, all constants are assumed to be nonnegative.

$$\frac{n \in \mathbb{Z}}{\Sigma; \emptyset \left|\frac{q}{q}\right. n : \texttt{nat}}\text{(L:ConstI)} \qquad \frac{}{\Sigma; \emptyset \left|\frac{q}{q}\right. () : \texttt{unit}}\text{(L:ConstU)} \qquad \frac{}{\Sigma; \emptyset \left|\frac{q}{q}\right. \texttt{T} : \texttt{bool}}\text{(L:ConstT)}$$

$$\frac{}{\Sigma; \emptyset \left|\frac{q}{q}\right. \texttt{F} : \texttt{bool}}\text{(L:ConstF)} \qquad \frac{}{\Sigma; x : B \left|\frac{q}{q}\right. x : B}\text{(L:Var)}$$

$$\frac{\Sigma; \Gamma \left|\frac{q}{q'}\right. e_t : B \qquad \Sigma; \Gamma \left|\frac{q}{q'}\right. e_f : B}{\Sigma; \Gamma, x : \texttt{bool} \left|\frac{q}{q'}\right. \texttt{if}\, x\, \texttt{then}\, e_t\, \texttt{else}\, e_f : B}\text{(L:Cond)}$$

$$\frac{}{\Sigma; x_1 : A_1, x_2 : A_2 \left|\frac{q}{q}\right. \langle x_1, x_2 \rangle : A_1 \times A_2}\text{(L:Pair)}$$

$$\frac{\Sigma; \Gamma, x_1 : A_1, x_2 : A_2 \left|\frac{q}{q'}\right. e : B}{\Sigma; \Gamma, x : (A_1, A_2) \left|\frac{q}{q'}\right. \texttt{case}\, x\, \{(x_1; x_2) \hookrightarrow e\} : B}\text{(L:MatP)} \qquad \frac{}{\Sigma; \emptyset \left|\frac{q}{q}\right. \texttt{nil} : L^p(A)}\text{(L:Nil)}$$

$$\frac{}{\Sigma; \Gamma, x_h : A, x_t : L^p(A) \left|\frac{q+p+1}{q}\right. \texttt{cons}(x_h; x_t) : L^p(A)}\text{(L:Cons)}$$

$$\frac{\Sigma; \Gamma \left|\frac{q}{q'}\right. e_1 : B \qquad \Sigma; \Gamma, x_h : A, x_t : L^p(A) \left|\frac{q+p+1}{q'}\right. e_2 : B}{\Sigma; \Gamma, x : L^p(A) \left|\frac{q}{q'}\right. \texttt{case}\, x\, \{\texttt{nil} \hookrightarrow e_1 \mid \texttt{cons}(x_h; x_t) \hookrightarrow e_2\} : B}\text{(L:MatL)}$$

$$\frac{\Sigma; \Gamma_1 \left|\frac{q}{p}\right. e_1 : A \qquad \Sigma; \Gamma_2, x : A \left|\frac{p}{q'}\right. e_2 : B}{\Sigma; \Gamma_1, \Gamma_2 \left|\frac{q}{q'}\right. \texttt{let}(e_1; x : \tau.e_2) : B}\text{(L:Let)}$$

Now if we take $\dagger : L^p(A) \mapsto L(A)$ as the map that erases resource annotations, we obtain a simpler typing judgement $\boxed{\Sigma^\dagger; \Gamma^\dagger \vdash e : B^\dagger}$.

5 Soundness for garbage collection semantics

We simplify the soundness proof of the type system for the general metric to one with monotonic resource. (No function types for now)

Lemma 1.1. *If* $\Sigma; \Gamma \left|\frac{q}{q'}\right. e : B$*, then* $\Sigma^\dagger; \Gamma^\dagger \vdash e : B^\dagger$.

Lemma 1.2. *If* $V, H, R, F \vdash e \Downarrow v, H', F'$*, then* $\forall x \in V$, $reach_H(V(x)) = reach_{H'}(V(x))$.

Proof. Induction on the evaluation judgement. □

Lemma 1.3. *For all stacks* V *and heaps* H*, if* $V, H, R, F \vdash e \Downarrow v, H', F'$, $\Sigma^\dagger; \Gamma^\dagger \vdash e : B^\dagger$, $H \vDash V : \Gamma$, $\mathsf{no\_alias}(V, H)$*, and* $\mathsf{disjoint}(\{R, F, locs_{V,H}(e)\})$*, then* $\mathsf{set}(reach_{H'}(v))$, $\mathsf{disjoint}(\{R, F', reach_{H'}(v)\})$, $\mathsf{no\_ref}(FV(e) \trianglelefteq V, H, v)$*, and* $\mathsf{no\_alias}(V, H')$.

Proof. Nested induction on the evaluation judgement and the typing judgement.

Case 1: E:Var

$$ \tag{1} $$

Case 2: E:Const* Due to similarity, we show only for E:ConstI

Case 4: E:App

Case 5: E:CondT

$$
\begin{aligned}
&\Gamma = \Gamma', x : \texttt{bool} && \text{(ad.)}\\
&H \vDash V : \Gamma' && \text{(def of W.F.E)}\\
&\Sigma; \Gamma' \left|\frac{q}{q'}\right. e_t : B && \text{(ad.)}\\
&V, H, R, F \cup g \ \vdash e_t \Downarrow v, H', F' && \text{(ad.)}\\
&|F \cup g| - |F'| \leq \Phi_{V,H}(\Gamma) + q - (\Phi_{H'}(v : B) + q') && \text{(IH)}\\
&|F| - |F'| \leq \Phi_{V,H}(\Gamma) + q - (\Phi_{H'}(v : B) + q')
\end{aligned}
$$

Case 6: E:CondF Similar to E:CondT

Case 7: E:Let

$V, H, R, F \ \vdash \texttt{let}(e_1; x : \tau.e_2) \Downarrow v_2, H_2, F_2$ (case)

$V, H, R', F \vdash e_1 \Downarrow v_1, H_1, F_1$ (ad.)

$\Sigma; \Gamma_1, \Gamma_2 \vdash \texttt{let}(e_1; x : \tau.e_2) : B$ (case)

$\Sigma; \Gamma_1 \vdash e_1 : A$ (ad.)

$\Sigma; \Gamma_2, x : A \vdash e_2 : B$ (ad.)

Suppose $\mathsf{no\_alias}(V, H), \mathsf{disjoint}(\{R, F, locs_{V,H}(e)\})$, and $H \vDash V : \Gamma$

$H \vDash V : \Gamma_1$ (def of W.D.E)

$F \cap R' = \emptyset$ ($F \cap locs_{V,H}(e) = \emptyset$ and $locs_{V,H}(e_1) \subseteq locs_{V,H}(e)$)

$R' \cap locs_{V,H}(e_1) = \emptyset$ ($\mathsf{no\_alias}(V, H)$)

$F \cap locs_{V,H}(e_1) = \emptyset$ (Sp.)

Thus we have $\mathsf{disjoint}(R', F, locs_{V,H}(e_1))$

By IH, $\mathsf{set}(reach_{H_1}(v_1)), \mathsf{disjoint}(\{R', F_1, reach_{H_1}(v_1)\}), \mathsf{no\_ref}(V, H, v)$, and $\mathsf{no\_alias}(V, H_1)$

$(F_1 \cup g) \cap R = \emptyset$ (since $F_1 \cap R' = \emptyset$ together with def. of g and R')

NTS $R \cap locs_{V',H_1}(e_2) = \emptyset$

Let $l \in locs_{V',H_1}(e_2)$ be arb.

case: $l \in reach_{H_1}(V'(x'))$ for some $x' \in FV(e_2)$ where $x' \neq x$

$x' \in V$ (def of V')

$l \in reach_H(V(x'))$ (Lemma 1.2)

$x' \in FV(e)$ (def of FV)

$l \in locs_{V,H}(e)$ (def of $locs_{V,H}$)

$l \notin R$ ($\mathsf{disjoint}(\{R, F, locs_{V,H}(e)\})$)

case : $l \in reach_{H_1}(V'(x))$

$l \in reach_{H_1}(v_1)$ (def of V')

$l \notin R'$ ($\mathsf{disjoint}(\{R', F_1, reach_{H_1}(v_1)\})$)

$l \notin R$ (since $R \subseteq R'$)

Thus $R \cap locs_{V',H_1}(e_2) = \emptyset$

$(F_1 \cup g) \cap R = \emptyset$ (by def of g and $\mathsf{disjoint}(\{R', F_1, reach_{H_1}(v_1)\})$)

Hence $\mathsf{disjoint}(\{R, F_1 \cup g, locs_{V',H_1}(e_2)\})$

$H \vDash V : \Gamma_2$ (def of W.D.E)

NTS $\mathsf{no\_alias}(V', H_1)$

TODO

$V', H_1, R, F_1 \cup g \vdash e_2 \Downarrow v_2, H_2, F_2$ (ad.)

By IH, $\mathsf{set}(reach_{H_2}(v_2)), \mathsf{disjoint}(\{R, F_2, reach_{H_2}(v_2)\}), \mathsf{no\_ref}(V', H_2, v_2),$ and $\mathsf{no\_alias}(V', H_2)$

$\mathsf{no\_ref}(V, H_2, v_2)$ and $\mathsf{no\_alias}(V, H_2)$ ($\overline{V} \subseteq \overline{V}'$)

Case 13: E:MatCons

$V(x) = (l, \mathtt{alive})$ (ad.)

$H(l) = \langle v_h, v_t \rangle$ (ad.)

$\Gamma = \Gamma', x : L(A)$ (ad.)

$\Sigma; \Gamma', x_h : A, x_t : L(A) \vdash e_2 : B$ (ad.)

$V'', H, R, F \cup g \ \vdash e_2 \Downarrow v_2, H_2, F'$ (ad.)

Suppose $H \vDash V : \Gamma, \mathsf{no\_alias}(V, H),$ and $, \mathsf{disjoint}(\{F, R, locs_{V,H}(e)\})$

$H \vDash V(x) : L(A)$ (def of W.D.E)

$H'' \vDash v_h : A, \ H'' \vDash v_t : L(A)$ (ad.)

$H \vDash v_h : A, \ H \vDash v_t : L(A)$ (???)

$H \vDash V'' : \Gamma', x_h : A, x_t : L(A)$ (def of W.D.E)

NTS $\mathsf{no\_alias}(V'', H)$

Let $x_1, x_2 \in \overline{V}'', x_1 \neq x_2, r_{x_1} = reach_H(\overline{V}''(x_1)), r_{x_2} = reach_H(\overline{V}''(x_2))$

case: $x_1 \notin \{x_h, x_t\}, x_2 \notin \{x_h, x_t\}$

$(1), (2)$ from $\mathsf{no\_alias}(V, H)$

case: $x_1 = x_h, x_2 \notin \{x_h, x_t\}$

$\mathsf{set}(r_{x_1})$ (since $\mathsf{set}(H(l))$ from $\mathsf{no\_alias}(V, H)$)

$\mathsf{set}(r_{x_2})$ (since $\mathsf{no\_alias}(V, H)$)

AFSOC, suppose $l' \in r_{x_1} \cap r_{x_2}$

but $reach_H(\overline{V}(x)) \cap r_{x_2} = \emptyset$, contradiction (def of $reach$)

hence $r_{x_1} \cap r_{x_2} = \emptyset$

case: $x_1 = x_h, x_2 = x_t$

$\mathsf{set}(r_{x_1})$ since $\mathsf{set}(H(l))$ from $\mathsf{no\_alias}(V, H)$

$\mathsf{set}(r_{x_2})$ since $\mathsf{set}(H(l))$ from $\mathsf{no\_alias}(V, H)$

AFSOC, suppose $l' \in r_{x_1} \cap r_{x_2}$

but then $\mu_{reach_H(l)}(l') \geq 2$, and $\mathsf{set}(H(l))$ does not hold.

hence $r_{x_1} \cap r_{x_2} = \emptyset$

case: otherwise

similar to the above

Thus we have $\mathsf{no\_alias}(V'', H)$

$(F \cup g) \cap R = \emptyset$ (since $F \cap R = \emptyset$ and by def of g)

NTS $R \cap locs_{V'',H}(e_2) = \emptyset$

Let $l' \in locs_{V'',H}(e_2)$ be arb.

case: $l' \in reach_H(V''(x'))$ for some $x' \in FV(e_2)$ where $x' \notin \{x_h, x_t\}$

$x' \in V$ (def of V'')

$l' \in reach_H(V(x'))$

$x' \in FV(e)$ (def of FV)

$l' \in locs_{V,H}(e)$ (def of $locs_{V,H}$)

$l' \notin R$ ($\mathsf{disjoint}(\{R, F, locs_{V,H}(e)\})$)

case: $l' \in reach_H(V''(x_h))$

$l' \in reach_H(v_h)$

$l' \in reach_H(V^\star(x))$ (def of $reach$)

$l' \in locs_{V,H}(e)$ (def of $locs_{V,H}$)

$l' \notin R$ (since $\mathsf{disjoint}(\{F, R, locs_{V,H}(e)\})$)

case: $l' \in reach_H(V''(x_t))$

similar to above

Hence $R \cap locs_{V'',H}(e_2) = \emptyset$

$F \cap locs_{V'',H}(e_2) = \emptyset$ (Similar to above)

$g \cap locs_{V'',H}(e_2) = \emptyset$ (def. of g)

$(F \cup g) \cap locs_{V'',H}(e_2) = \emptyset$

Thus $\mathsf{disjoint}(\{R, F \cup g, locs_{V'',H}(e_2)\})$

By IH, $\mathsf{set}(reach_{H'}(v)), \mathsf{disjoint}(\{R, F', reach_{H'}(v)\}), \mathsf{no\_ref}(V'', H', v)$, and $\mathsf{no\_alias}(V'', H')$

NTS $\mathsf{no\_ref}(V, H', v)$

Let $l' \in reach_{H'}(\overline{V}(x))$ be arb

$l' \in reach_H(l)$ (Lemma 1.2, ad.)

Then $l' \in reach_{H'}(v_h)$ or $l' \in reach_{H'}(v_t)$ (def of $reach$)

Wlog $l' \in reach_{H'}(v_h)$

$l' \in reach_{H'}(V''(x_h))$ (def of V'')

$l' \notin reach_{H'}(v)$ ($\mathsf{no\_ref}(V'', H', v)$)

$(reach_{H'}(v)) \cap (\bigcup_{x' \in \overline{V} \setminus x} reach_{H'}(V(x'))) = \emptyset$ ($\mathsf{no\_ref}(V'', H', v)$)

$(reach_{H'}(v)) \cap (\bigcup_{x' \in \overline{V}} reach_{H'}(V(x'))) = \emptyset$

$\mathsf{no\_ref}(V, H', v)$

NTS $\mathsf{no\_alias}(V, H')$

Let $x_1, x_2 \in \overline{V}, x_1 \neq x_2, r_{x_1} = reach_H(\overline{V}(x_1)), r_{x_2} = reach_H(\overline{V}(x_2))$ be arb.

case: $x_1 \neq x, x_2 \neq x$

$(1), (2)$ ($\mathsf{no\_alias}(V'', H')$)

case: $x_1 = x, x_2 \neq x$

$\mathsf{set}(r_{x_1})$ ($\mathsf{no\_alias}(V'', H')$)

$\mathsf{set}(r_{x_2})$ ($\mathsf{no\_alias}(V'', H')$)

case: otherwise

similar to above

Thus $\mathsf{no\_alias}(V, H')$

Thus $\mathsf{no\_ref}(V, H', v)$ and $\mathsf{no\_alias}(V, H')$

□

Task 1.4 (Soundness)**.** *let* $H \vDash V : \Gamma$, $\Sigma; \Gamma \left|\frac{q}{q'}\right. e : B$, *and* $V, H \vdash e \Downarrow v, H'$. *Then* $\forall C \in \mathbb{Q}^+$ *and* $\forall F, R \subseteq \mathsf{Loc}$, *if* $\mathsf{no\_alias}(V, H)$, $\mathsf{disjoint}(\{R, F, locs_{V,H}(e)\})$, *and* $|F| \geq \Phi_{V,H}(\Gamma) + q + C$, *then there exists* $F' \subseteq \mathsf{Loc}$ *s.t.*

1. $V, H, R, F \vdash e \Downarrow v, H', F'$
2. $|F'| \geq \Phi_{H'}(v : B) + q' + C$

Proof. Induction on the evaluation judgement.

Case 1: E:Var

$V, H, R, F \vdash x \Downarrow V(x), H, F$ (admissibility)

$\Sigma; x : B \left|\frac{q}{q}\right. x : B$ (admissibility)

$|F| - |F'|$ (2)

$$\begin{aligned}
&= |F| - |F| && \text{(ad.)}\\
&= 0 && (3)\\
&\Phi_{V,H}(\Gamma) + q - (\Phi_{H'}(v:B) + q') && (4)\\
&\quad = \Phi_{V,H}(x:B) + q - (\Phi_H(V(x):B) + q) && \text{(ad.)}\\
&\quad = \Phi_H(V(x):B) + q - (\Phi_H(V(x):B) + q) && \text{(def. of } \Phi_{V,H})\\
&\quad = 0 && (5)\\
&|F| - |F'| \le \Phi_{V,H}(\Gamma) + q - (\Phi_{H'}(v:B) + q') && ((3),(5))
\end{aligned}$$

Case 2: E:Const* Due to similarity, we show only for E:ConstI

$$\begin{aligned}
&|F| - |F'| = |F| - |F| && \text{(ad.)}\\
&\quad = 0 &&\\
&\Phi_{V,H}(\Gamma) + q - (\Phi_{H'}(v:B) + q') = \Phi_{V,H}(\emptyset) + q - (\Phi_H(v:int) + q) && \text{(ad.)}\\
&\quad = 0 && \text{(def of } \Phi_{V,H})\\
&|F| - |F'| \le \Phi_{V,H}(\Gamma) + q - (\Phi_{H'}(v:B) + q') &&
\end{aligned}$$

Case 4: E:App

Case 5: E:CondT

$$\begin{aligned}
&\Gamma = \Gamma', x : \texttt{bool} && \text{(ad.)}\\
&H \vDash V : \Gamma' && \text{(def of W.F.E)}\\
&\Sigma; \Gamma' \left|\tfrac{q}{q'}\right. e_t : B && \text{(ad.)}\\
&V, H, R, F \cup g \;\vdash e_t \Downarrow v, H', F' && \text{(ad.)}\\
&|F \cup g| - |F'| \le \Phi_{V,H}(\Gamma) + q - (\Phi_{H'}(v:B) + q') && \text{(IH)}\\
&|F| - |F'| \le \Phi_{V,H}(\Gamma) + q - (\Phi_{H'}(v:B) + q') &&
\end{aligned}$$

Case 6: E:CondF Similar to E:CondT

Case 7: E:Let

$$\begin{aligned}
&V, H \;\vdash e \Downarrow v_2, H_2 && \text{(case)}\\
&V, H \vdash e_1 \Downarrow v_1, H_1 && \text{(ad.)}\\
&\Sigma; \Gamma_1 \left|\tfrac{q}{p}\right. e_1 : A && \text{(ad.)}\\
&H \vDash V : \Gamma_1 && (\Gamma_1 \subseteq \Gamma)
\end{aligned}$$

Let $C \in \mathbb{Q}^+, F, R \subseteq \mathsf{Loc}$ be arb.

Suppose $\mathsf{no\_alias}(V,H), \mathsf{disjoint}(\{R, F, locs_{V,H}(e)\}),$ and $|F| \ge \Phi_{V,H}(\Gamma) + q + C$

NTF F' s.t.

1.$V, H, R, F \vdash e \Downarrow v_2, H_2, F'$ and

2.$|F'| \ge \Phi_{H_2}(v_2 : B) + q' + C$

Let $R' = R \cup locs_{V,H}(\mathtt{lam}(x : \tau.e_2))$

$\mathsf{disjoint}(\{R', F, locs_{V,H}(e_1)\})$ (Similar to case in Lemma 1.2)

Instantiate IH with $C = C + \Phi_{V,H}(\Gamma_2), F = F, R = R',$ we get F'' s.t.

1.$V, H, R', F \vdash e_1 \Downarrow v_1, H_1, F''$ and

2.$|F''| \geq \Phi_{H_1}(v_1 : A) + p + C + \Phi_{V',H_1}(\Gamma_2)$

Where $|F| \geq \Phi_{V,H}(\Gamma_1) + q + C + \Phi_{V,H}(\Gamma_2)$ since $|F| \geq \Phi_{V,H}(\Gamma) + q + C$

For the second premise:

$\Sigma; \Gamma_2, x : A \left|\frac{p}{q'}\right. e_2 : B$ (ad.)

$H_1 \vDash v_1 : A$ and (Theorem 3.3.4)

$H_1 \vDash V : \Gamma_2$ (???)

$H_1 \vDash V' : \Gamma_2, x : A$ (def of $\vDash$)

$V', H_1 \vdash e_2 \Downarrow v_2, H_2$ (ad.)

Let $g = \{l \in H_1 \mid l \notin F_1 \cup R \cup locs_{V',H_1}(e_2)\}$

Then we have $\mathsf{no\_alias}(V', H_1)$ and $\mathsf{disjoint}(\{R, F'' \cup g, locs_{V',H_1}(e_2)\})$

(similar to case in Lemma 1.2)

Instantiate IH with $C = C, F = F'' \cup g, R = R,$ we get $F^{(3)}$ s.t.

1.$V', H_1, R, F'' \cup g \vdash e_2 \Downarrow v_2, H_2, F^{(3)}$

2.$|F^{(3)}| \geq \Phi_{H_2}(v_2 : B) + q' + C$

Where we verify the precondition $|F'' \cup g| \geq \Phi_{V',H_1}(\Gamma_2, x : A) + p + C$

$$
\begin{aligned}
|F'' \cup g| &\geq |F''| \\
&\geq \Phi_{H_1}(v_1 : A) + p + C + \Phi_{V,H}(\Gamma_2) && \text{(IH)} \\
&= \Phi_{H_1}(v_1 : A) + p + C + \Phi_{V',H_1}(\Gamma_2) && \text{(Lemma 4.3.3)} \\
&= \Phi_{V',H_1}(\Gamma_2, x : A) + p + C && \text{(def of } \Phi)
\end{aligned}
$$

Take $F' = F^{(3)}$

$V, H, R, F \vdash e \Downarrow v_2, H_2, F'$ and (E:Let)

$|F'| \geq \Phi_{H_2}(v_2 : B) + q' + C$ (from IH)

Case 8: E:Pair Similar to E:Const*

Case 9: E:MatP Similar to E:MatCons

Case 10: E:Nil Similar to E:Const*

Case 11: E:Cons

$$
\begin{aligned}
&|F| - |F'| \\
&\quad = |F| - |F \setminus \{l\}| && \text{(ad.)} \\
&\quad = 1
\end{aligned}
$$

$\Phi_{V,H}(\Gamma) + q - (\Phi_{H'}(v : B) + q')$

$= \Phi_{V,H}(x_h : A, x_t : L^p(A)) + q + p + 1 - (\Phi_{H'}(v : L^p(A)) + q)$ (ad.)

$= \Phi_{V,H}(x_h : A, x_t : L^p(A)) + p + 1 - \Phi_{H'}(v : L^p(A)))$

$= \Phi_H(V(x_h) : A) + \Phi_H(V(x_t) : L^p(A)) + p + 1 - \Phi_{H'}(v : L^p(A)))$ (def of $\Phi_{V,H}$)

$= \Phi_H(v_h : A) + \Phi_H(v_t : L^p(A)) + p + 1 - \Phi_{H'}(v : L^p(A)))$ (ad.)

$= \Phi_H(v_h : A) + \Phi_H(v_t : L^p(A)) + p + 1 - (p + \Phi_{H'}(v_h : A) + \Phi_{H'}(v_t : L^p(A)))$ (Lemma 4.1.1)

$= \Phi_H(v_h : A) + \Phi_H(v_t : L^p(A)) + p + 1 - (p + \Phi_H(v_h : A) + \Phi_H(v_t : L^p(A)))$ (Lemma 4.3.3)

$= 1$

Hence,

$|F| - |F'| \leq \Phi_{V,H}(\Gamma) + q - (\Phi_{H'}(v : B) + q')$

Case 12: E:MatNil Similar to E:Cond*

Case 13: E:MatCons

$V(x) = (l, \texttt{alive})$ (ad.)

$H(l) = \langle v_h, v_t \rangle$ (ad.)

$\Gamma = \Gamma', x : L^p(A)$ (ad.)

$\Sigma; \Gamma', x_h : A, x_t : L^p(A) \mid\frac{q+p+1}{q'} e_2 : B$ (ad.)

$V'', H \vdash e_2 \Downarrow v, H'$ (ad.)

Let $C \in \mathbb{Q}^+, F, R \subseteq \mathsf{Loc}$ be arb.

$H \vDash V(x) : L^p(A)$ (def of W.D.E)

$H'' \vDash v_h : A,\ H'' \vDash v_t : L^p(A)$ (ad.)

$H \vDash v_h : A,\ H \vDash v_t : L^p(A)$ (???)

$H \vDash V'' : \Gamma', x_h : A, x_t : L^p(A)$ (def of W.D.E)

Suppose $\mathsf{no\_alias}(V, H), \mathsf{disjoint}(\{R, F, locs_{V,H}(e)\})$, and $|F| \geq \Phi_{V,H}(\Gamma) + q + C$

NTF F' s.t.

1.$V, H, R, F \vdash e \Downarrow v, H', F'$ and

2.$|F'| \geq \Phi_{H'}(v : B) + q' + C$

Let $g = \{l \in H \mid l \notin F \cup R \cup locs_{V'',H}(e_2)\}$

We want to g nonempty, in particular, that $l \in g$

$l \notin F \cup R$ ($\mathsf{disjoint}(\{R, F, locs_{V,H}(e)\})$)

AFSOC $l \in locs_{V'',H}(e_2)$

Then $l \in reach_H(\overline{V}''(x'))$ for some $x' \neq x$

$x' \in \{x_h, x_t\}$ (since $reach_H(\overline{V}(x')) \cap reach_H(\bar{(}Vx)) = \emptyset$ from $\mathsf{no\_alias}(V, H)$)

WLOG let $x' = x_h$

But then $\mu_{reach_H(\overline{V}(x))}(l) \geq 2$ and $\mathsf{set}(reach_(\overline{V}(x)))$ doesn't hold

$l \notin locs_{V'',H}(e_2)$

Hence $l \in g$

Next, we have $\mathsf{no\_alias}(V'', H)$ and $\mathsf{disjoint}(\{R, F \cup g, locs_{V'',H}(e_2)\})$

(similar to case in Lemma 1.2)

By IH with $C' = C, F'' = F \cup g$ and the above conditions, we have: $F^{(3)}$ s.t.

1.$V'', H, R, F \cup g \vdash e_2 \Downarrow v, H', F^{(3)}$

2.$|F^{(3)}| \geq \Phi_{H'}(v : B) + q' + C$

Where we also verify the precondition that $|F''| \geq \Phi_{V'',H}(\Gamma', x_h : A, x_t : L^p(A)) + q + p + 1 + C'$:

$$
\begin{aligned}
|F''| &= |F \cup g| \\
&= |F| + |g| && (F \text{ and } g \text{ disjoint}) \\
&\geq \Phi_{V,H}(\Gamma) + q + C + |g| && \text{(Sp.)} \\
&= \Phi_{V,H}(\Gamma', x_h : A, x_t : L^p(A)) + p + q + C + |g| && \text{(Lemma 4.1.1)} \\
&= \Phi_{V,H}(\Gamma', x_h : A, x_t : L^p(A)) + p + q + C + 1 && (g \text{ nonempty})
\end{aligned}
$$

Now take $F' = F^{(3)}$

$V, H, R, F \ \vdash e \Downarrow v, H', F'$ (E:MatCons)

$|F'| \geq \Phi_{H'}(v : B) + q' + C$ (From the IH)

$\square$