15-312 Assignment 1

Andrew Carnegie
(andrew)

September 28, 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
$\texttt{tpl}(x_1;x_2)$	$\langle x_1, x_2\rangle$	tuple
$\texttt{fst}(x)$	$x \cdot \texttt{l}$	first projection
$\texttt{snd}(x)$	$x \cdot \texttt{r}$	second projection
$\texttt{nil}$	$[]$	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
$\texttt{val}(\texttt{cl}(V;x.e))$	$(V,x.e)^l$	function value
$\texttt{val}(l)$	l	loc value
$\texttt{val}(\texttt{pair}(v_1;v_2))$	$\langle v_1, v_2\rangle$	pair value

Loc l ::=		
$\texttt{loc}(l)$	l	location

1 Garbage collection semantics

Model dynamics using judgement of the form:

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

Where $V : VID \to Val$, $H : Loc \to Val$, and $R : \{Loc\}$. 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'.

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.

Below defines the size of reachable values and space for roots:

$$
\begin{aligned}
&reach_H(n^l) = \{l\} \\
&reach_H(\mathtt{T}^l) = \{l\} \\
&reach_H(\mathtt{F}^l) = \{l\} \\
&reach_H(\mathtt{Null}^l) = \{l\} \\
&reach_H((V, x.e)^l) = \{l\} \cup (\bigcup_{y \in FV(e) \setminus x} reach_H(V(y))) \\
&reach_H(l_1^{l_2}) = \{l_2\} \cup loc_H(H(l_1)) \\
&reach_H(\langle v_1, v_2 \rangle^L) = L \cup reach_H(v_1) \cup reach_H(v_2)
\end{aligned}
$$

$$loc_H(l) = \{l\} \cup reach_H(H(l))$$

$$space_H(R) = |\bigcup_{l \in R} loc_H(l)|$$

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

$$\frac{x \in dom(V)}{V,H,R,F \ \vdash x \Downarrow V(x), H, F}(\mathrm{S}_1) \qquad \frac{}{V,H,R,F \ \vdash \overline{n} \Downarrow \mathtt{val}(n), H, F}(\mathrm{S}_2)$$

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

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

$$\frac{V(x) = \mathtt{T}^l \qquad g = \{l \in H | l \notin F \cup R \cup locs_{V,H}(e_1)\} \qquad V,H,R,F \cup g \ \vdash e_1 \Downarrow v, H', F'}{V,H,R,F \ \vdash \mathtt{if}(x; e_1; e_2) \Downarrow v, H', F'}(\mathrm{S}_6)$$

$$\frac{V(x) = \mathtt{F}^l \qquad g = \{l \in H | l \notin F \cup R \cup locs_{V,H}(e_2)\} \qquad V,H,R,F \cup g \ \vdash e_2 \Downarrow v, H', F'}{V,H,R,F \ \vdash \mathtt{if}(x; e_1; e_2) \Downarrow v, H', F'}(\mathrm{S}_7)$$

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

$$\frac{V(f) = (V_1, x.e)^{l_1} \qquad V(x) = v_1 \qquad V_1[x \mapsto v_1], H, R \ \vdash e \Downarrow^s v, H'}{V,H,R,F \ \vdash f(x) \Downarrow v, H', F}(\mathrm{S}_9)$$

$$\frac{V(x_1) = v_1 \qquad V(x_2) = v_2 \qquad l \in F \qquad F' = F \setminus \{l\} \qquad H' = H[l \mapsto \langle v_1, v_2 \rangle^l]}{V,H,R,F \ \vdash \langle x_1, x_2 \rangle \Downarrow \langle v_1, v_2 \rangle^l, H', F'}(\mathrm{S}_{10})$$

$$\frac{V(x) = \langle v_1, v_2 \rangle^l}{V,H,R,F \ \vdash x \cdot \mathtt{l} \Downarrow v_1, H, F}(\mathrm{S}_{11}) \qquad \frac{V(x) = \langle v_1, v_2 \rangle^l}{V,H,R,F \ \vdash x \cdot \mathtt{r} \Downarrow v_2, H, F}(\mathrm{S}_{12})$$

$$\frac{}{V,H,R,F \ \vdash \mathtt{nil} \Downarrow \mathtt{val}(\mathtt{Null}), H, F}(\mathrm{S}_{13})$$

$$\frac{V(x_1) = v_1 \qquad V(x_2) = v_2 \qquad l \in F \qquad F' = F \setminus \{l\} \qquad H' = H[l \mapsto \langle v_1, v_2 \rangle]}{V,H,R,F \ \vdash \mathtt{cons}(x_1; x_2) \Downarrow l, H', F'}(\mathrm{S}_{14})$$

$$\frac{V(z) = \mathtt{Null}^l \qquad g = \{l \in H | l \notin F \cup R \cup locs_{V,H}(e_1)\} \qquad V,H,R,F \cup g \ \vdash e_1 \Downarrow v, H', F'}{V,H,R,F \ \vdash \mathtt{case}\, z \, \{\mathtt{nil} \hookrightarrow e_1 \mid \mathtt{cons}(x_h; x_t) \hookrightarrow e_2\} \Downarrow v, H', F'}(\mathrm{S}_{15})$$

$$\frac{\begin{array}{c} V(z) = \langle v_h, v_t \rangle^l \\ g = \{l \in H | l \notin F \cup R \cup locs_{V,H}(e_2)\} \qquad V[x_h \mapsto v_h, x_t \mapsto v_t], H, R, F \cup g \ \vdash e_2 \Downarrow v, H', F' \end{array}}{V,H,R,F \ \vdash \mathtt{case}\, z \, \{\mathtt{nil} \hookrightarrow e_1 \mid \mathtt{cons}(x_h; x_t) \hookrightarrow e_2\} \Downarrow v, H', F'}(\mathrm{S}_{16})$$

$$\frac{\begin{array}{c} R' = R \cup locs_{V,H}(\mathtt{lam}(x : \tau.e_2)) \qquad V, H, R', F \vdash e_1 \Downarrow v_1, H_1, F_1 \qquad V' = V[x \mapsto v_1] \\ R'' = R \cup locs_{V',H_1}(e_2) \qquad g = \{l \in H_1 | l \notin R'' \cup F_1\} \qquad V', H_1, R, F_1 \cup g \vdash e_2 \Downarrow v_2, H_2, F_2 \end{array}}{V,H,R,F \ \vdash \mathtt{let}(e_1; x : \tau.e_2) \Downarrow v_2, H_2, F_2}(\mathrm{S}_{17})$$

2 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.

$$\frac{n \in \mathbb{Z}}{\Sigma; \emptyset \left|\frac{q}{q}\right. n : int} \text{ L:CONSTI}$$

$$\frac{}{\Sigma; x : B \left|\frac{q}{q}\right. x : B} \text{ L:VAR}$$

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

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

3 Soundness for heap allocation

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

Task 1.1 (Soundness)**.** *let* $H \vDash V : \Gamma$ *and* $\Sigma; \Gamma \left|\frac{q}{q'}\right. e : B$ *If* $V, H, R, F \vdash e \Downarrow v, H', F'$*, then*

$$|F| - |F'| \leq \Phi_{V,H}(\Gamma) + q - (\Phi_{H'}(v : B) + q') \tag{1}$$

Proof. Induction on the evaluation judgement.

Case 1: E:Var

$$\begin{aligned}
& V, H, R, F \vdash x \Downarrow V(x), H, F && \text{(admissibility)}\\
& \Sigma; x : B \left|\frac{p}{p}\right. x : B && \text{(admissibility)}\\
& |F| - |F'| && (2)\\
& \quad = |F| - |F| && \text{(ad.)}\\
& \quad = 0 && (3)\\
& \Phi_{V,H}(\Gamma) + q - (\Phi_{H'}(v : B) + q') && (4)\\
& \quad = \Phi_{V,H}(x : B) + p - (\Phi_H(V(x) : B) + p) && \text{(ad.)}\\
& \quad = \Phi_H(V(x) : B) + p - (\Phi_H(V(x) : B) + p) && \text{(def. of } \Phi_{V,H})\\
& \quad = 0 && (5)\\
& |F| - |F'| \leq \Phi_{V,H}(\Gamma) + q - (\Phi_{H'}(v : B) + q') && ((3),(5))
\end{aligned}$$

Case 2: E:ConstU

Case 3: E:ConstI

Case 4: E:App

Case 5: E:CondT

Case 6: E:CondF

Case 7: E:Let

$$
\begin{array}{ll}
V, H, R', F \vdash e_1 \Downarrow v_1, H_1, F_1 & \text{(ad.)} \\
\Sigma; \Gamma_1 \left|\frac{q}{p}\right. e_1 : A & \text{(ad.)} \\
H \vDash V : \Gamma_1 & (\Gamma_1 \subseteq \Gamma) \\
|F| - |F_1| \leq \Phi_{V,H}(\Gamma_1) + q - (\Phi_{H_1}(v_1 : A) + p) & \text{(IH)} \\
V', H_1, R, F_1 \cup g \vdash e_2 \Downarrow v_2, H_2, F_2 & \text{(ad.)} \\
\Sigma; \Gamma_2, x : A \left|\frac{p}{q'}\right. e_2 : B & \text{(ad.)} \\
H_1 \vDash v_1 : A \text{ and} & \text{(Theorem 3.3.4)} \\
H_1 \vDash V : \Gamma_2 & \text{(???)} \\
H_1 \vDash V' : \Gamma_2, x : A & \text{(def of } \vDash) \\
|F_1 \cup g| - |F_2| \leq \Phi_{V',H_1}(\Gamma_2, x : A) + p - (\Phi_{H_2}(v_2 : B) + q') & \text{(IH)} \\
|F_1| - |F_2| \leq \Phi_{V',H_1}(\Gamma_2, x : A) + p - (\Phi_{H_2}(v_2 : B) + q') &
\end{array}
$$

summing the inequalities:

$$|F| - |F_1| + |F_1| - |F_2| \leq \Phi_{V,H}(\Gamma_1) + q - (\Phi_{H_1}(v_1 : A) + p) + \Phi_{V',H_1}(\Gamma_2, x : A) + p - (\Phi_{H_2}(v_2 : B) + q')$$

$$
\begin{aligned}
|F| - |F_2| &\leq \Phi_{V,H}(\Gamma_1) + q - \Phi_{H_1}(v_1 : A) + \Phi_{V',H_1}(\Gamma_2, x : A) - (\Phi_{H_2}(v_2 : B) + q') \\
&= \Phi_{V,H}(\Gamma_1) + \Phi_{V',H_1}(\Gamma_2) + q - \Phi_{H_1}(v_1 : A) + \Phi_{V',H_1}(x : A) - (\Phi_{H_2}(v_2 : B) + q') && \text{(def of } \Phi_{V,H}) \\
&= \Phi_{V,H}(\Gamma_1) + \Phi_{V,H}(\Gamma_2) + q - \Phi_{H_1}(v_1 : A) + \Phi_{V',H_1}(x : A) - (\Phi_{H_2}(v_2 : B) + q') && \text{(Lemma 4.3.3)} \\
&= \Phi_{V,H}(\Gamma) + q - \Phi_{H_1}(v_1 : A) + \Phi_{H_1}(v_1 : A) - (\Phi_{H_2}(v_2 : B) + q') && \text{(def of } \Phi_{V,H}) \\
&= \Phi_{V,H}(\Gamma) + q - (\Phi_{H_2}(v_2 : B) + q')
\end{aligned}
$$

Case 8: E:Pair

Case 9: E:MatP

Case 10: E:Nil

Case 11: E:Cons

Case 12: E:MatNil

Case 13: E:MatCons

$$V(z) = \langle v_h, v_t \rangle^L \tag{ad.}$$
$$\Gamma = \Gamma', x : L^p(A) \tag{ad.}$$
$$\Sigma; \Gamma', x_h : A, x_t : L^p(A) \,\Big|\frac{q+p+K^{cons}}{q'}\; e_2 : B \tag{ad.}$$
let $V' = V[x_h \mapsto v_h, x_t \mapsto v_t]$
$$V', H, R, F \cup g \vdash e_2 \Downarrow v_2, H_2, F' \tag{ad.}$$
$$H \vDash V' : \Gamma', x_h : A, x_t : L^p(A) \tag{Lemma*}$$
$$|F \cup g| - |F'| \leq \Phi_{V,H}(\Gamma', x_h : A, x_t : L^p(A)) + q + p + K^{cons} - (\Phi_{H'}(v : B) + q') \tag{IH}$$
$$= \Phi_{V,H}(\Gamma') + \Phi_H(v_h : A) + \Phi_H(v_t : L^p(A)) + p + q + 1 - (\Phi_{H'}(v : B) + q') \tag{def of $\Phi_{V,H}$}$$
$$= \Phi_{V,H}(\Gamma') + \Phi_H(\langle v_h, v_t \rangle^L : L^p(A)) + q + 1 - (\Phi_{H'}(v : B) + q') \tag{Lemma 4.1.1}$$
$$= \Phi_{V,H}(\Gamma', z : L^p(A)) + q + 1 - (\Phi_{H'}(v : B) + q') \tag{def of $\Phi_{V,H}$}$$
$$= \Phi_{V,H}(\Gamma) + q + 1 - (\Phi_{H'}(v : B) + q') \tag{Lemma 4.1.1}$$
Looking at z, we have:
$$locs_{V,H}(z) \nsubseteq R \cup locs_{V,H}(e_2) \tag{Heap linearity}$$
Then,
$$locs_{V,H}(z) \subseteq g \tag{def of g}$$
Furthermore,
$$|locs_{V,H}(z)| \geq 1 \tag{def of $locs_{V,H}$}$$
$$|g| \geq 1 \tag{$locs_{V,H} \subseteq g$}$$
$$|F \cup g| - |F'|$$
$$= |F| + |g| - |F'| \tag{F, g disjoint}$$
Hence,
$$|F| + |g| - |F'| \leq \Phi_{V,H}(\Gamma) + q + 1 - (\Phi_{H'}(v : B) + q')$$
$$|F| - |F'| \leq \Phi_{V,H}(\Gamma) + q + 1 - |g| - (\Phi_{H'}(v : B) + q')$$
$$\leq \Phi_{V,H}(\Gamma) + q - (\Phi_{H'}(v : B) + q') \tag{$|g| \geq 1$}$$

□