

15-312 Assignment 1

Andrew Carnegie
(andrew)

October 6, 2017

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

$$\begin{aligned}
reach_H((V, x.e)) &= \bigcup_{y \in FV(e) \setminus x} reach_H(V(y)) \\
reach_H(l) &= \{l\} \cup reach_H(H(l)) \\
reach_H(\langle v_1, v_2 \rangle) &= reach_H(v_1) \cup reach_H(v_2) \\
reach_H(-) &= \emptyset
\end{aligned}$$

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

$$size_H(v) = \dots$$

$$copy(H, L, v) = \dots$$

$$\begin{array}{c}
\frac{x \in \text{dom}(V)}{V, H, R, F \vdash x \Downarrow V(x), H, F}^{(S_1)} \quad \frac{}{V, H, R, F \vdash \bar{n} \Downarrow \text{val}(n), H, F}^{(S_2)} \\
\\
\frac{}{V, H, R, F \vdash \mathbf{T} \Downarrow \text{val}(\mathbf{T}), H, F}^{(S_3)} \quad \frac{}{V, H, R, F \vdash \mathbf{F} \Downarrow \text{val}(\mathbf{F}), H, F}^{(S_4)} \\
\\
\frac{}{V, H, R, F \vdash () \Downarrow \text{val}(\mathbf{Null}), H, F}^{(S_5)} \\
\\
\frac{V(x) = \mathbf{T} \quad g = \{l \in H \mid l \notin F \cup R \cup \text{locs}_{V,H}(e_1)\} \quad V, H, R, F \cup g \vdash e_1 \Downarrow v, H', F'}{V, H, R, F \vdash \text{if}(x; e_1; e_2) \Downarrow v, H', F'}^{(S_6)} \\
\\
\frac{V(x) = \mathbf{F} \quad g = \{l \in H \mid l \notin F \cup R \cup \text{locs}_{V,H}(e_2)\} \quad V, H, R, F \cup g \vdash e_2 \Downarrow v, H', F'}{V, H, R, F \vdash \text{if}(x; e_1; e_2) \Downarrow v, H', F'}^{(S_7)} \\
\\
\frac{l \in F \quad F' = F \setminus \{l\} \quad H' = H[l \mapsto (V, x.e)]}{V, H, R, F \vdash \text{lam}(x : \tau.e) \Downarrow l, H', F'}^{(S_8)} \\
\\
\frac{V(f) = (V_1, x.e) \quad V(x) = v_1 \quad 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'}^{(S_9)} \\
\\
\frac{V(x_1) = v_1 \quad 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}^{(S_{10})} \\
\\
\frac{g = \{l \in H \mid l \notin F \cup R \cup \text{locs}_{V,H}(e)\} \quad V(x) = \langle v_1, v_2 \rangle \quad V[x_1 \mapsto v_1, x_2 \mapsto v_2], H, R, F \cup g \vdash e \Downarrow v, H', F'}{V, H, R, F \vdash \text{case } x \{(x_1; x_2) \hookrightarrow e\} \Downarrow v, H', F'}^{(S_{11})} \\
\\
\frac{}{V, H, R, F \vdash \text{nil} \Downarrow \text{val}(\mathbf{Null}), H, F}^{(S_{12})} \\
\\
\frac{v = \langle V(x_1), V(x_2) \rangle \quad L \subseteq F \quad |L| = \text{size}_H(v) \quad F' = F \setminus L \quad H', l = \text{copy}(H, L, v)}{V, H, R, F \vdash \text{cons}(x_1; x_2) \Downarrow l, H', F'}^{(S_{13})} \\
\\
\frac{V(x) = \mathbf{Null} \quad g = \{l \in H \mid l \notin F \cup R \cup \text{locs}_{V,H}(e_1)\} \quad V, H, R, F \cup g \vdash e_1 \Downarrow v, H', F'}{V, H, R, F \vdash \text{case } x \{\text{nil} \hookrightarrow e_1 \mid \text{cons}(x_h; x_t) \hookrightarrow e_2\} \Downarrow v, H', F'}^{(S_{14})} \\
\\
\frac{V(x) = l \quad H(l) = \langle v_h, v_t \rangle \quad g = \{l \in H \mid l \notin F \cup R \cup \text{locs}_{V,H}(e_2)\} \quad V[x_h \mapsto v_h, x_t \mapsto v_t], H, R, F \cup g \vdash e_2 \Downarrow v, H', F'}{V, H, R, F \vdash \text{case } x \{\text{nil} \hookrightarrow e_1 \mid \text{cons}(x_h; x_t) \hookrightarrow e_2\} \Downarrow v, H', F'}^{(S_{15})} \\
\\
\frac{R' = R \cup \text{locs}_{V,H}(\text{lam}(x : \tau.e_2)) \quad V, H, R', F \vdash e_1 \Downarrow v_1, H_1, F_1 \quad V' = V[x \mapsto v_1] \quad R'' = R \cup \text{locs}_{V',H_1}(e_2) \quad g = \{l \in H_1 \mid l \notin R'' \cup F_1\} \quad V', H_1, R, F_1 \cup g \vdash e_2 \Downarrow v_2, H_2, F_2}{V, H, R, F \vdash \text{let}(e_1; x : \tau.e_2) \Downarrow v_2, H_2, F_2}^{(S_{16})}
\end{array}$$

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.

$$\begin{array}{c}
\frac{n \in \mathbb{Z}}{\Sigma; \emptyset \mid_q n : \text{nat}} (\text{L:ConstI}) \quad \frac{}{\Sigma; \emptyset \mid_q () : \text{unit}} (\text{L:ConstU}) \quad \frac{}{\Sigma; \emptyset \mid_q \text{T} : \text{bool}} (\text{L:ConstT}) \\
\\
\frac{}{\Sigma; \emptyset \mid_q \text{F} : \text{bool}} (\text{L:ConstF}) \quad \frac{}{\Sigma; x : B \mid_q x : B} (\text{L:Var}) \\
\\
\frac{\Sigma; \Gamma \mid_{q'}^q e_t : B \quad \Sigma; \Gamma \mid_{q'}^q e_f : B}{\Sigma; \Gamma, x : \text{bool} \mid_{q'}^q \text{if } x \text{ then } e_t \text{ else } e_f : B} (\text{L:Cond}) \\
\\
\frac{}{\Sigma; x_1 : A_1, x_2 : A_2 \mid_q^q \langle x_1, x_2 \rangle : (A_1, A_2)} (\text{L:Pair}) \\
\\
\frac{\Sigma; \Gamma, x_1 : A_1, x_2 : A_2 \mid_{q'}^q e : B}{\Sigma; \Gamma, x : (A_1, A_2) \mid_{q'}^q \text{case } x \{ (x_1; x_2) \hookrightarrow e \} : B} (\text{L:MatP}) \quad \frac{}{\Sigma; \emptyset \mid_q \text{nil} : L^p(A)} (\text{L:Nil}) \\
\\
\frac{}{\Sigma; \Gamma, x_h : A, x_t : L^p(A) \mid_{\frac{q+p+1}{q}}^{\frac{q+p+1}{q}} \text{cons}(x_h; x_t) : L^p(A)} (\text{L:Cons}) \\
\\
\frac{\Sigma; \Gamma \mid_{q'}^q e_1 : B \quad \Sigma; \Gamma, x_h : A, x_t : L^p(A) \mid_{\frac{q+p+1}{q'}}^{\frac{q+p+1}{q}} e_2 : B}{\Sigma; \Gamma, x : L^p(A) \mid_{q'}^q \text{case } x \{ \text{nil} \hookrightarrow e_1 \mid \text{cons}(x_h; x_t) \hookrightarrow e_2 \} : B} (\text{L:MatL}) \\
\\
\frac{\Sigma; \Gamma_1 \mid_{\frac{p}{q}}^{\frac{p}{q}} e_1 : A \quad \Sigma; \Gamma_2, x : A \mid_{q'}^{\frac{p}{q}} e_2 : B}{\Sigma; \Gamma_1, \Gamma_2 \mid_{q'}^q \text{let}(e_1; x : \tau.e_2) : B} (\text{L:Let})
\end{array}$$

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 $H \models V : \Gamma$. If $\Sigma; \Gamma \mid_{q'}^q e : B$ and $V, H, R, F \vdash e \Downarrow v, H', F'$, then*

1. $|F| - |F'| \leq \Phi_{V,H}(\Gamma) + q - (\Phi_{H'}(v : B) + q')$
2. $\text{locs}_{V,H}(e) \cap (R \cup F) = \emptyset$

Proof. Induction on the evaluation judgement.

Case 1: E:Var

$$\begin{aligned}
V, H, R, F &\vdash x \Downarrow V(x), H, F && \text{(admissibility)} \\
\Sigma; x : B &\Big|_{\frac{q}{q'}} x : B && \text{(admissibility)} \\
|F| - |F'| &&& (1) \\
&= |F| - |F| && \text{(ad.)} \\
&= 0 && (2) \\
\Phi_{V,H}(\Gamma) + q - (\Phi_{H'}(v : B) + q') &&& (3) \\
&= \Phi_{V,H}(x : B) + q - (\Phi_H(V(x) : B) + q) && \text{(ad.)} \\
&= \Phi_H(V(x) : B) + q - (\Phi_H(V(x) : B) + q) && \text{(def. of } \Phi_{V,H}) \\
&= 0 && (4) \\
|F| - |F'| &\leq \Phi_{V,H}(\Gamma) + q - (\Phi_{H'}(v : B) + q') && ((3),(5))
\end{aligned}$$

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

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

Case 4: E:App

Case 5: E:CondT

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

Case 6: E:CondF Similar to E:CondT

Case 7: E:Let

$$\begin{aligned}
V, H, R', F \vdash e_1 \Downarrow v_1, H_1, F_1 & \quad (\text{ad.}) \\
\Sigma; \Gamma_1 \mid \frac{q}{p} e_1 : A & \quad (\text{ad.}) \\
H \models V : \Gamma_1 & \quad (\Gamma_1 \subseteq \Gamma) \\
|F| - |F_1| \leq \Phi_{V,H}(\Gamma_1) + q - (\Phi_{H_1}(v_1 : A) + p) & \quad (\text{IH}) \\
V', H_1, R, F_1 \cup g \vdash e_2 \Downarrow v_2, H_2, F_2 & \quad (\text{ad.}) \\
\Sigma; \Gamma_2, x : A \mid \frac{p}{q'} e_2 : B & \quad (\text{ad.}) \\
H_1 \models v_1 : A \text{ and} & \quad (\text{Theorem 3.3.4}) \\
H_1 \models V : \Gamma_2 & \quad (???) \\
H_1 \models V' : \Gamma_2, x : A & \quad (\text{def of } \models) \\
|F_1 \cup g| - |F_2| \leq \Phi_{V',H_1}(\Gamma_2, x : A) + p - (\Phi_{H_2}(v_2 : B) + q') & \quad (\text{IH}) \\
|F_1| - |F_2| \leq \Phi_{V',H_1}(\Gamma_2, x : A) + p - (\Phi_{H_2}(v_2 : B) + q') & \\
\text{summing the inequalities:} & \\
|F| - |F_1| + |F_1| - |F_2| \leq \Phi_{V,H}(\Gamma_1) + q - (\Phi_{H_1}(v_1 : A) + p) + \Phi_{V',H_1}(\Gamma_2, x : A) + p - (\Phi_{H_2}(v_2 : B) + q') & \\
|F| - |F_2| \leq \Phi_{V,H}(\Gamma_1) + q - \Phi_{H_1}(v_1 : A) + \Phi_{V',H_1}(\Gamma_2, x : A) - (\Phi_{H_2}(v_2 : B) + q') & \\
= \Phi_{V,H}(\Gamma_1) + \Phi_{V',H_1}(\Gamma_2) + q - \Phi_{H_1}(v_1 : A) + \Phi_{V',H_1}(x : A) - (\Phi_{H_2}(v_2 : B) + q') & \\
& \quad (\text{def of } \Phi_{V,H}) \\
= \Phi_{V,H}(\Gamma_1) + \Phi_{V,H}(\Gamma_2) + q - \Phi_{H_1}(v_1 : A) + \Phi_{V',H_1}(x : A) - (\Phi_{H_2}(v_2 : B) + q') & \\
& \quad (\text{Lemma 4.3.3}) \\
= \Phi_{V,H}(\Gamma) + q - \Phi_{H_1}(v_1 : A) + \Phi_{H_1}(v_1 : A) - (\Phi_{H_2}(v_2 : B) + q') & \quad (\text{def of } \Phi_{V,H}) \\
= \Phi_{V,H}(\Gamma) + q - (\Phi_{H_2}(v_2 : B) + q') &
\end{aligned}$$

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'| \\
&= |F| - |F \setminus \{l\}| \tag{ad.} \\
&= 1 \\
&\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) \tag{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)) \tag{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)) \tag{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))) \\
&\hspace{15em} \tag{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))) \\
&\hspace{15em} \tag{Lemma 4.3.3} \\
&= 1
\end{aligned}$$

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

$$V(x) = \langle v_h, v_t \rangle \quad (\text{ad.})$$

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

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

$$\text{let } V' = V[x_h \mapsto v_h, x_t \mapsto v_t]$$

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

$$H \models V(x) : L^p(A) \quad (\text{def of W.D.E})$$

$$H'' \models v_h : A, H'' \models v_t : L^p(A) \quad (\text{ad.})$$

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

$$H \models V' : \Gamma', x_h : A, x_t : L^p(A) \quad (\text{def of W.D.E})$$

$$|F \cup g| - |F'| \leq \Phi_{V,H}(\Gamma', x_h : A, x_t : L^p(A)) + q + p + 1 - (\Phi_{H'}(v : B) + q') \quad (\text{IH})$$

$$= \Phi_{V,H}(\Gamma') + \Phi_H(v_h : A) + \Phi_H(v_t : L^p(A)) + p + q + 1 - (\Phi_{H'}(v : B) + q') \\ (\text{def of } \Phi_{V,H})$$

$$= \Phi_{V,H}(\Gamma') + \Phi_H(\langle v_h, v_t \rangle^L : L^p(A)) + q + 1 - (\Phi_{H'}(v : B) + q') \quad (\text{Lemma 4.1.1})$$

$$= \Phi_{V,H}(\Gamma', z : L^p(A)) + q + 1 - (\Phi_{H'}(v : B) + q') \quad (\text{def of } \Phi_{V,H})$$

$$= \Phi_{V,H}(\Gamma) + q + 1 - (\Phi_{H'}(v : B) + q') \quad (\text{Lemma 4.1.1})$$

Looking at x , we have:

$$locs_{V,H}(x) \not\subseteq R \cup locs_{V,H}(e_2) \quad (\text{Heap linearity})$$

Then,

$$locs_{V,H}(x) \subseteq g \quad (\text{def of } g)$$

Furthermore,

$$|locs_{V,H}(z)| \geq 1 \quad (\text{def of } locs_{V,H})$$

$$|g| \geq 1 \quad (locs_{V,H} \subseteq g)$$

$$|F \cup g| - |F'| \\ = |F| + |g| - |F'| \quad (F, g \text{ disjoint})$$

Hence,

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

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

□