Resource Analysis: Problem Set 5

Jan Hoffmann
Carnegie Mellon University

February 22, 2016

Due before 1:30pm on Monday, February 29

5.1 (8 Points) Resource Monoid

Recall the definition of the resource monoid $\mathcal{Q} = (\mathbb{Q}_{\geq 0} \times \mathbb{Q}_{\geq 0}, \cdot)$ where

$$(q, q') \cdot (p, p') = \begin{cases} (q + p - q',\ p') & \text{if } q' \leq p \\ (q,\ p' + q' - p) & \text{if } q' > p \end{cases}$$

Let $(q, q') = (r, r') \cdot (s, s')$. Prove the following statements.

1. $q \geq r$ and $q - q' = r - r' + s - s'$
2. If $(p, p') = (\bar{r}, r') \cdot (s, s')$ and $\bar{r} \geq r$ then $p \geq q$ and $p' = q'$
3. If $(p, p') = (r, r') \cdot (\bar{s}, s')$ and $\bar{s} \geq s$ then $p \geq q$ and $p' \leq q'$
4. $(r, r') \cdot ((s, s') \cdot (t, t')) = ((r, r') \cdot (s, s')) \cdot (t, t')$

5.2 (12 Points) Reasoning with the Cost Semantics

Consider the metric M_{app} that counts the number of function applications, that is,

$$\begin{aligned} M_{\text{app}}(\mathsf{app}) &= 1 \\ M_{\text{app}}(K) &= 0 \quad \text{if } K \neq \mathsf{app} \end{aligned}$$

Consider the function *omega*: $(X \to X) \to Y$ that is defined as follows.

```
let rec omega = fun x → omega x in omega (fun x → x)
```

Let e_{omega} be the above expression.

a) Prove that $\cdot; H\ _M\vdash e_{\text{omega}} \Downarrow \circ \mid (n, 0)$ for every $n \in \mathbb{N}$ and every heap H.

b) Prove that $\cdot; H\ _M\nvdash e_{\text{omega}} \Downarrow (\ell, H')$ for any ℓ and H'.

5.3 (18 Points) Resource-Based Type Safety

We will now use our effect-based cost semantics to show that *well-typed programs don't go wrong*: In a well-formed environment, a well-typed expression will either evaluate to a value of the right type or can make an infinite number of steps.

First, recall the definition of a *well-typed* environment. We write $H \vDash \ell : A$ to indicate that there exists a, necessarily unique, semantic value $a \in [\![A]\!]$ so that $H \vDash v \mapsto a : A$. An environment V and a heap H are *well-formed* with respect to a context Γ if $H \vDash V(x) : \Gamma(x)$ holds for every $x \in \mathrm{dom}(\Gamma)$. We then write $H \vDash V : \Gamma$.

The judgement $H \vDash v \mapsto a : A$ is defined by the following rules. Recall that the rules have to be interpreted coinductively.

$$\frac{X \in \mathcal{X} \qquad \ell \in \mathrm{dom}(H)}{H \vDash \ell \mapsto \ell : X} \text{ (V:TVAR)} \qquad\qquad \frac{}{H \vDash \mathrm{Null} \mapsto [] : \mathrm{L}(T)} \text{ (V:NIL)}$$

$$\frac{H(\ell) = (\ell_1, \ell_2) \qquad H \vDash \ell_1 \mapsto a_1 \qquad H \vDash \ell_2 \mapsto (a_2, \ldots, a_n) : \mathrm{L}(T)}{H \vDash \ell \mapsto [a_1, \ldots, a_n] : \mathrm{L}(T)} \text{ (V:CONS)}$$

$$\frac{H(\ell) = (\lambda x.e, V) \qquad \exists \Gamma .\, H \vDash V : \Gamma \wedge \Gamma \vdash \lambda x.e \vdash^m T_1 \to T_2}{H \vDash \ell \mapsto (\lambda x.e, V) : \Sigma \to T} \text{ (V:FUN)}$$

In this problem assume that M_E is the *steps metric*, which counts the number of evaluation steps. We then have $M_E^K = 1$ for all constants K.

Prove the following theorem. It is sufficient if you prove the theorem for expressions of the form

$$\begin{array}{rcll} e & ::= & x & x \\ & & \mathrm{lam}(x.e) & \mathsf{fun}\ x \to e \\ & & \mathrm{app}(e_1, e_2) & e_1\ e_2 \\ & & \mathrm{let}(e_1, x.e_2) & \mathsf{let}\ x = e_1\ \mathsf{in}\ e_2 \\ & & \mathrm{rec}((f,x).e_f, f.e) & \mathsf{let\ rec}\ f\, x = e_f\ \mathsf{in}\ e \end{array}$$

Theorem 1 (Type Safety). *Let $H \vDash V : \Gamma$, $\Gamma \vdash^m e : T$, and let M_E be the steps metric. Then*

- *there is an $n \in \mathbb{N}$ such that $V; H\ {}_{M_E}\!\vdash e \Downarrow (\ell, H') \mid (n, 0)$, $H' \vDash V : \Gamma$, and $H' \vDash \ell : T$*
- *or $V; H\ {}_{M_E}\!\vdash e \Downarrow \circ \mid (m, 0)$ for every $m \in N$*

A consequence of the theorem is that resource bounds on the number of evaluation steps prove termination.

Hint: The following lemma can be proved by induction on n.

Lemma 1. *Let $H \vDash V : \Gamma$ and $\Gamma \vdash^m e : T$. If $V; H\ {}_{M_E}\!\vdash e \Downarrow \circ \mid (n, 0)$ then $V; H\ {}_{M_E}\!\vdash e \Downarrow \circ \mid (n+1, 0)$ or $V; H\ {}_{M_E}\!\vdash e \Downarrow (\ell, H') \mid (n+1, 0)$ for a location ell and an heap H'.*

$V; H\,{}_M{\vdash}\, e \Downarrow (\ell, H') \mid (q, q')$ In environment V and heap H, expression e evaluates to (ℓ, H'), the watermark resource usage is q and q' resources are available afterwards.

$$\frac{}{V; H\,{}_M{\vdash}\, x \Downarrow (\ell, H) \mid M^{\mathsf{var}}}\ (\textsc{Ee:Var}) \qquad \frac{H' = H, \ell \mapsto (\lambda x.e, V)}{V; H\,{}_M{\vdash}\, \mathrm{lam}(x.e) \Downarrow (\ell, H') \mid M^{\mathsf{abs}}}\ (\textsc{Ee:Abs})$$

$$\frac{\begin{array}{c} V; H\,{}_M{\vdash}\, e_1 \Downarrow (\ell_1, H_1) \mid (q_0, q_1) \qquad H(\ell_1) = (\lambda x.e, V') \\ V; H_1\,{}_M{\vdash}\, e_2 \Downarrow (\ell_2, H_2) \mid (q_2, q_3) \qquad V'[x \mapsto \ell_2]; H_2\,{}_M{\vdash}\, e \Downarrow (\ell, H') \mid (q_3, q_4) \end{array}}{V; H\,{}_M{\vdash}\, \mathrm{app}(e_1, e_2) \Downarrow (\ell, H') \mid M^{\mathsf{app}} \cdot (q_0, q_1) \cdot (q_2, q_3) \cdot (q_3, q_4)}\ (\textsc{Ee:App})$$

$$\frac{V, H\,{}_M{\vdash}\, e_1 \Downarrow (\ell_1, H_1) \mid (q_0, q_1) \qquad V[x \mapsto \ell_1], H_1\,{}_M{\vdash}\, e_2 \Downarrow (\ell, H') \mid (q_2, q_3)}{V; H\,{}_M{\vdash}\, \mathrm{let}(e_1, x.e_2) \Downarrow (\ell, H') \mid M^{\mathsf{let}} \cdot (q_0, q_1) \cdot (q_2, q_3)}\ (\textsc{Ee:Let})$$

$$\frac{H' = H, \ell \mapsto \mathrm{Null}}{V; H\,{}_M{\vdash}\, \mathrm{nil} \Downarrow (\ell, H') \mid M^{\mathsf{nil}}}\ (\textsc{Ee:Nil})$$

$$\frac{\begin{array}{c} V; H\,{}_M{\vdash}\, e_1 \Downarrow (\ell_1, H_1) \mid (q_0, q_1) \\ V; H_1\,{}_M{\vdash}\, e_2 \Downarrow (\ell_2, H_2) \mid (q_2, q_3) \qquad H' = H_2, \ell \mapsto (\ell_1, \ell_2) \end{array}}{V; H\,{}_M{\vdash}\, \mathrm{cons}(e_1, e_2) \Downarrow (\ell, H') \mid M^{\mathsf{cons}} \cdot (q_0, q_1) \cdot (q_2, q_3)}\ (\textsc{Ee:Cons})$$

$$\frac{V; H\,{}_M{\vdash}\, e \Downarrow (\ell, H') \mid (q_0, q_1) \qquad H'(\ell) = \mathrm{Null} \qquad V; H'\,{}_M{\vdash}\, e_1 \Downarrow (\ell_1, H_1) \mid (q_2, q_3)}{V; H\,{}_M{\vdash}\, \mathrm{matL}(e, e_1, (x_1, x_2).e_2) \Downarrow (\ell_1, H_1) \mid M_1^{\mathsf{matL}} \cdot (q_0, q_1) \cdot (q_2, q_3)}\ (\textsc{Ee:MatL1})$$

$$\frac{\begin{array}{c} V; H\,{}_M{\vdash}\, e \Downarrow (\ell, H') \mid (q_0, q_1) \\ H'(\ell) = (\ell_1, \ell_2) \qquad V[x_1 \mapsto \ell_1, x_2 \mapsto \ell_2]; H'\,{}_M{\vdash}\, e_2 \Downarrow (\ell, H') \mid (q_2, q_3) \end{array}}{V; H\,{}_M{\vdash}\, \mathrm{matL}(e, e_1, (x_1, x_2).e_2) \Downarrow (\ell_1, H_1) \mid M_2^{\mathsf{matL}} \cdot (q_0, q_1) \cdot (q_2, q_3)}\ (\textsc{Ee:MatL2})$$

$$\frac{V' = V[f \mapsto \ell_f] \qquad H' = H, \ell_f \mapsto (\lambda x.e_f, V') \qquad V'; H'\,{}_M{\vdash}\, e \Downarrow (\ell', H'') \mid (q, q')}{V; H\,{}_M{\vdash}\, \mathrm{rec}((f, x).e_f, f.e) \Downarrow (\ell', H'') \mid M^{\mathsf{rec}} \cdot (q, q')}\ (\textsc{Ee:Rec})$$

Figure 1: Rules of the effect-based cost semantics.

$V; H \;{}_M\!\vdash e \Downarrow \circ \mid (q, q')$	After evaluating expression e in environment V and heap H for several steps, the watermark resource usage is q and q' resources are available.

$$\frac{}{V; H \;{}_M\!\vdash e \Downarrow \circ \mid 0}\ (\textsc{Ep:Abort}) \qquad \frac{V; H \;{}_M\!\vdash e_1 \Downarrow \circ \mid (q_0, q_1)}{V; H \;{}_M\!\vdash \mathrm{app}(e_1, e_2) \Downarrow \circ \mid M^{\mathsf{app}} \cdot (q_0, q_1)}\ (\textsc{Ep:App1})$$

$$\frac{V; H \;{}_M\!\vdash e_1 \Downarrow (\ell_1, H_1) \mid (q_0, q_1) \qquad V; H_1 \;{}_M\!\vdash e_2 \Downarrow \circ \mid (q_2, q_3)}{V; H \;{}_M\!\vdash \mathrm{app}(e_1, e_2) \Downarrow \circ \mid M^{\mathsf{app}} \cdot (q_0, q_1) \cdot (q_2, q_3)}\ (\textsc{Ep:App2})$$

$$\frac{\begin{array}{c} V; H \;{}_M\!\vdash e_1 \Downarrow (\ell_1, H_1) \mid (q_0, q_1) \qquad H(\ell_1) = (\lambda x.e, V') \\ V; H_1 \;{}_M\!\vdash e_2 \Downarrow (\ell_2, H_2) \mid (q_2, q_3) \qquad V'[x \mapsto \ell_2]; H_2 \;{}_M\!\vdash e \Downarrow \circ \mid (q_3, q_4) \end{array}}{V; H \;{}_M\!\vdash \mathrm{app}(e_1, e_2) \Downarrow \circ \mid M^{\mathsf{app}} \cdot (q_0, q_1) \cdot (q_2, q_3) \cdot (q_3, q_4)}\ (\textsc{Ep:App3})$$

$$\frac{V, H \;{}_M\!\vdash e_1 \Downarrow \circ \mid (q_0, q_1)}{V; H \;{}_M\!\vdash \mathrm{let}(e_1, x.e_2) \Downarrow \circ \mid M^{\mathsf{let}} \cdot (q_0, q_1)}\ (\textsc{Ep:Let1})$$

$$\frac{V, H \;{}_M\!\vdash e_1 \Downarrow (\ell_1, H_1) \mid (q_0, q_1) \qquad V[x \mapsto \ell_1], H_1 \;{}_M\!\vdash e_2 \Downarrow \circ \mid (q_2, q_3)}{V; H \;{}_M\!\vdash \mathrm{let}(e_1, x.e_2) \Downarrow \circ \mid M^{\mathsf{let}} \cdot (q_0, q_1) \cdot (q_2, q_3)}\ (\textsc{Ep:Let2})$$

$$\frac{V; H \;{}_M\!\vdash e_1 \Downarrow \circ \mid (q_0, q_1)}{V; H \;{}_M\!\vdash \mathrm{cons}(e_1, e_2) \Downarrow \circ \mid M^{\mathsf{cons}} \cdot (q_0, q_1)}\ (\textsc{Ep:Cons1})$$

$$\frac{V; H \;{}_M\!\vdash e_1 \Downarrow (\ell_1, H_1) \mid (q_0, q_1) \qquad V; H_1 \;{}_M\!\vdash e_2 \Downarrow \circ \mid (q_2, q_3)}{V; H \;{}_M\!\vdash \mathrm{cons}(e_1, e_2) \Downarrow \circ \mid M^{\mathsf{cons}} \cdot (q_0, q_1) \cdot (q_2, q_3)}\ (\textsc{Ep:Cons2})$$

$$\frac{V; H \;{}_M\!\vdash e \Downarrow \circ \mid (q_0, q_1)}{V; H \;{}_M\!\vdash \mathrm{matL}(e, e_1, (x_1, x_2).e_2) \Downarrow \circ \mid M_1^{\mathsf{matL}} \cdot (q_0, q_1)}\ (\textsc{Ep:MatL0})$$

$$\frac{V; H \;{}_M\!\vdash e \Downarrow (\ell, H') \mid (q_0, q_1) \qquad H'(\ell) = \mathrm{Null} \qquad V; H' \;{}_M\!\vdash e_1 \Downarrow \circ \mid (q_2, q_3)}{V; H \;{}_M\!\vdash \mathrm{matL}(e, e_1, (x_1, x_2).e_2) \Downarrow \circ \mid M_1^{\mathsf{matL}} \cdot (q_0, q_1) \cdot (q_2, q_3)}\ (\textsc{Ep:MatL1})$$

$$\frac{\begin{array}{c} V; H \;{}_M\!\vdash e \Downarrow (\ell, H') \mid (q_0, q_1) \\ H'(\ell) = (\ell_1, \ell_2) \qquad V[x_1 \mapsto \ell_1, x_2 \mapsto \ell_2]; H' \;{}_M\!\vdash e_2 \Downarrow \circ \mid (q_2, q_3) \end{array}}{V; H \;{}_M\!\vdash \mathrm{matL}(e, e_1, (x_1, x_2).e_2) \Downarrow \circ \mid M_2^{\mathsf{matL}} \cdot (q_0, q_1) \cdot (q_2, q_3)}\ (\textsc{Ep:MatL2})$$

$$\frac{V' = V[f \mapsto \ell_f] \qquad H' = H, \ell_f \mapsto (\lambda x.e_f, V') \qquad V'; H' \;{}_M\!\vdash e \Downarrow \circ \mid (q, q')}{V; H \;{}_M\!\vdash \mathrm{rec}((f, x).e_f, f.e) \Downarrow \circ \mid M^{\mathsf{rec}} \cdot (q, q')}\ (\textsc{Ep:Rec})$$

Figure 2: Rules of the partial effect-based cost semantics.