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 $Q = (\mathbb{Q}_{\geq 0} \times \mathbb{Q}_{\geq 0}, \cdot)$ 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 $M_{\text{app}}$ that counts the number of function applications, that is,

$$M_{\text{app}}(\text{app}) = 1$$

$$M_{\text{app}}(K) = 0 \text{ if } K \neq \text{app}$$

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

let rec $\omega = \text{fun } x \rightarrow \omega \omega x \text{ in } \omega \omega (\text{fun } x \rightarrow x)$

Let $e_{\omega}$ be the above expression.

a) Prove that $\cdot : H_{M} \vdash e_{\omega} \Downarrow \circ (n, 0)$ for every $n \in \mathbb{N}$ and every heap $H$.

b) Prove that $\cdot : H_{M} \vdash e_{\omega} \Downarrow (\ell, H')$ for any $\ell$ 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 $H \Downarrow v : A$ to indicate that there exists a, necessarily unique, semantic value $a \in [A]$ so that $H \Downarrow v \rightarrow a : A$. An environment $V$ and a heap $H$ are well-formed with respect to a context $\Gamma$ if $H \Downarrow V(x) : \Gamma(x)$ holds for every $x \in \text{dom}(\Gamma)$. We then write $H \Downarrow V : \Gamma$.

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

\[
\begin{align*}
X \in X' & \quad \ell \in \text{dom}(H) \\
\frac{}{H \Downarrow \ell \rightarrow \ell : X} & \quad \text{(V:VAR)} \\
\frac{}{H \Downarrow \text{Null} \rightarrow [] : L(T)} & \quad \text{(V:NIL)} \\
\frac{H(\ell) = (\ell_1, \ell_2) \quad H \Downarrow \ell_1 \rightarrow a_1 \quad H \Downarrow \ell_2 \rightarrow (a_2, \ldots, a_n) : L(T)}{H \Downarrow \ell \rightarrow [a_1, \ldots, a_n] : L(T)} & \quad \text{(V:CONS)} \\
\frac{H(\ell) = (\lambda x.e, V) \quad \exists \Gamma. H \Downarrow V : \Gamma \land \Gamma \vdash \lambda x.e \vdash^m T_1 \rightarrow T_2}{H \Downarrow \ell \rightarrow (\lambda x.e, V) : \Sigma \rightarrow T} & \quad \text{(V:FUN)}
\end{align*}
\]

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

\[
e ::= x \quad \text{fun } x \rightarrow e \\
\text{app}(e_1, e_2) \quad e_1 \ e_2 \\
\text{let}(e_1, x. e_2) \quad \text{let } x = e_1 \text{ in } e_2 \\
\text{rec}((f, x). e_f, f.e) \quad \text{let } \text{rec } f x = e_f \text{ in } e
\]

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

- there is an $n \in \mathbb{N}$ such that $V ; H_M \Downarrow e \Downarrow (\ell, H') \mid (n,0)$, $H' \Downarrow V : \Gamma$, and $H' \Downarrow \ell : T$

- or $V ; H_M \Downarrow e \Downarrow \circ \mid (m,0)$ for every $m \in \mathbb{N}$

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 $H \Downarrow V : \Gamma$ and $\Gamma \vdash^m e : T$. If $V ; H_M \Downarrow e \Downarrow \circ \mid (n,0)$ then $V ; H_M \Downarrow e \Downarrow \circ \mid (n + 1,0)$ or $V ; H_M \Downarrow e \Downarrow (\ell, H') \mid (n + 1,0)$ for a location $\ell$ and an heap $H'$. 


In environment $V$ and heap $H$, expression $e$ evaluates to $(\ell', H')$, the watermark resource usage is $q$ and $q'$ resources are available afterwards.

$$V; H_M \vdash e \downarrow (\ell, H') \mid (q, q')$$

### Rules

**Rule (EE:VAR)**

$$V; H_M \vdash x \downarrow (\ell, H) \mid M^\text{Val}$$

**Rule (EE:ABS)**

$$V; H_M \vdash \lambda x. e, V \downarrow (\ell, H') \mid M^\text{Abs}$$

**Rule (EE:APP)**

$$V; H_M \vdash e_1 \downarrow (\ell, H_1) \mid (q_0, q_1) \quad H(\ell_1) = (\lambda x. e, V')$$

$$V; H_M \vdash e_2 \downarrow (\ell_2, H_2) \mid (q_2, q_3) \quad V'(x \mapsto \ell_2) ; H'; M^\text{App} \vdash e_2 \downarrow (\ell, H') \mid (q_2, q_3)$$

**Rule (EE:LET)**

$$V; H_M \vdash \text{let}(e_1, x.e_2) \downarrow (\ell, H') \mid M^\text{let} \downarrow (q_0, q_1) \mid (q_2, q_3)$$

**Rule (EE:NIL)**

$$H' = H, \ell \mapsto \text{Null}$$

**Rule (EE:CONS)**

$$V; H_M \vdash e_1 \downarrow (\ell_1, H_1) \mid (q_0, q_1)$$

$$V; H_M \vdash e_2 \downarrow (\ell_2, H_2) \mid (q_2, q_3)$$

$$V; H_M \vdash \text{cons}(e_1, e_2) \downarrow (\ell, H') \mid M^\text{Cons} \downarrow (q_0, q_1) \mid (q_2, q_3)$$

**Rule (EE:MAT1)**

$$V; H_M \vdash \text{matL}(e, e_1, (x_1, x_2), e_2) \downarrow (\ell_1, H_1) \mid M^\text{matL} \downarrow (q_0, q_1) \mid (q_2, q_3)$$

**Rule (EE:MAT2)**

$$V; H_M \vdash \text{matL}(e, e_1, (x_1, x_2), e_2) \downarrow (\ell_1, H_1) \mid M^\text{matL} \downarrow (q_0, q_1) \mid (q_2, q_3)$$

**Rule (EE:REC)**

$$V' = V[f \mapsto \ell_f] \quad H' = H, \ell_f \mapsto (\lambda x. e_f, V')$$

$$V'; H'_M \vdash e \downarrow (\ell', H'') \mid (q, q')$$

**Figure 1:** Rules of the effect-based cost semantics.
After evaluating expression \( e \) in environment \( V \) and heap \( H \) for several steps, the watermark resource usage is \( q \) and \( q' \) resources are available.

![Equations and expressions in a table format](image)

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