Take-Home Exam 1
4541.664A Program Analysis

TAs
{msjin, pronto}@ropas.snu.ac.kr
Programming Research Lab

June 2, 2006

1 Problem 2.

1.1 Abstract Semantics

$$\begin{array}{rcl}
\hat{\mathcal{V}}\ n\ \hat{\Sigma} & = & \alpha_2\{n\} \\
\hat{\mathcal{V}}\ x\ \hat{\Sigma} & = & \alpha_2\{\sigma\ x \mid \sigma \in \gamma_1(\hat{\Sigma})\} \\
\hat{\mathcal{V}}\ E_1 + E_2\ \hat{\Sigma} & = & (\hat{\mathcal{V}}\ E_1\ \hat{\Sigma}) \hat{+} (\hat{\mathcal{V}}\ E_2\ \hat{\Sigma}) \\
\hat{\mathcal{V}}\ -\ E\ \hat{\Sigma} & = & \hat{-}(\hat{\mathcal{V}}\ E\ \hat{\Sigma}) \\
\hat{\mathcal{V}}\ \texttt{let}\ x\ E_1\ E_2\ \hat{\Sigma} & = & \hat{\mathcal{V}}\ E_2\ (\hat{\Sigma}\{x \hat{\mapsto} \hat{\mathcal{V}}\ E_1\ \hat{\Sigma}\}) \\
\hat{\mathcal{V}}\ \texttt{if}\ E_1\ E_2\ E_3\ \hat{\Sigma} & = & (\hat{\mathcal{V}}\ E_2\ \hat{\Sigma}) \sqcup (\hat{\mathcal{V}}\ E_3\ \hat{\Sigma})
\end{array}$$

Here,

$$\begin{array}{rcl}
\hat{+} & \in & \hat{\mathbb{Z}} \times \hat{\mathbb{Z}} \to \hat{\mathbb{Z}} \\
\hat{-} & \in & \hat{\mathbb{Z}} \to \hat{\mathbb{Z}} \\
.\{x \hat{\mapsto} .\} & \in & \hat{Env} \times \hat{\mathbb{Z}} \to \hat{Env}
\end{array}$$

are safely abstracted from concrete materials $+, -, .\{x \mapsto .\}$

1.2 Correctness Proof

To proof that the abstractions are correct, we have to show for all expression E

$$\alpha(\mathcal{V}\ E) \sqsubseteq \hat{\mathcal{V}}\ E$$

is hold. Here we assume α and γ is compositionally defined[1]:

$$\alpha = \lambda f.\alpha_2 \circ f \circ \gamma_1$$
$$\gamma = \lambda \hat{f}.\gamma_2 \circ \hat{f} \circ \alpha_1$$

For convenience, we define the following pair abstraction,

$$\begin{array}{rcl}
\alpha_{a \times b} & = & \lambda \langle A, B \rangle.\langle \alpha_a A, \alpha_b B \rangle \\
\gamma_{a \times b} & = & \lambda \langle A, B \rangle.\langle \gamma_a A, \gamma_b B \rangle
\end{array}$$

[1]Just soundness condition of α and γ is not enough for correctness proof, think of $\alpha(\mathcal{V}\ E) = \lambda \hat{\Sigma}.\top$, which is sound abstraction but we cannot prove the correctness with given abstract semantics.

- $e \to n$

$$\begin{aligned}
\alpha(\mathcal{V}\ n)\ \hat{\Sigma} &= (\alpha_2 \circ \mathcal{V}\ n \circ \gamma_1)\ \hat{\Sigma} && (\texttt{by def. of } \alpha) \\
&= \alpha_2(\mathcal{V}\ n\ (\gamma_1 \hat{\Sigma})) \\
&= \alpha_2\{n\} && (\texttt{be def. of } \mathcal{V}) \\
&= \hat{\mathcal{V}}\ n\ \hat{\Sigma}
\end{aligned}$$

- $e \to x$

$$\begin{aligned}
\alpha(\mathcal{V}\ x)\ \hat{\Sigma} &= (\alpha_2 \circ \mathcal{V}\ x \circ \gamma_1)\ \hat{\Sigma} && (\texttt{by def. of } \alpha) \\
&= \alpha_2(\mathcal{V}\ x\ (\gamma_1 \hat{\Sigma})) \\
&= \alpha_2\{\sigma\ x \mid \sigma \in \gamma_1 \hat{\Sigma}\} && (\texttt{by def. of } \mathcal{V}) \\
&= \hat{\mathcal{V}}\ x\ \hat{\Sigma}
\end{aligned}$$

- $e \to E_1 + E_2$

  by I.H

  $\alpha(\mathcal{V}\ E_1) \sqsubseteq \hat{\mathcal{V}}\ E_1 \Rightarrow \alpha_2(\mathcal{V} E_1 (\gamma_1 \hat{\Sigma})) \sqsubseteq (\hat{\mathcal{V}} E_1)\hat{\Sigma}$

  $\alpha(\mathcal{V}\ E_2) \sqsubseteq \hat{\mathcal{V}}\ E_2 \Rightarrow \alpha_2(\mathcal{V} E_2 (\gamma_1 \hat{\Sigma})) \sqsubseteq (\hat{\mathcal{V}} E_2)\hat{\Sigma}$

  Let $\dot{+}$ to be $\lambda\langle a, b\rangle.\{v_1 + v_2 | v_1 \in a, v_2 \in b\}$

  Because $\hat{+}$ is sound operator, $id \sqsubseteq \gamma_{2\times 2} \circ \alpha_{2\times 2}$ and $\alpha_2 \circ \dot{+}$ is monotonic, following is true.

$$\begin{aligned}
& \hat{+} \sqsupseteq \alpha_2 \circ \dot{+} \gamma_{2\times 2} \\
\Rightarrow\ & \hat{+} \circ \alpha_{2\times 2} \sqsupseteq \alpha_2 \circ \dot{+} \quad \cdots (1)
\end{aligned}$$

$$\begin{aligned}
\alpha(\mathcal{V}\ E_1 + E_2)\ \hat{\Sigma} &= (\alpha_2 \circ \mathcal{V}\ E_1 + E_2 \circ \gamma_1)\ \hat{\Sigma} && (\texttt{by def. of } \alpha) \\
&= \alpha_2(\mathcal{V}\ E_1 + E_2\ (\gamma_1 \hat{\Sigma})) \\
&= \alpha_2\{z_1 + z_2 \mid z_i \in \mathcal{V}\ E_i\ \Sigma\} && (\texttt{by def. of } \mathcal{V}) \\
&= (\alpha_2 \circ \dot{+})\langle \mathcal{V}\ E_1\ (\gamma_1 \hat{\Sigma}), \mathcal{V}\ E_2\ (\gamma_1 \hat{\Sigma})\rangle \\
&\sqsubseteq (\hat{+} \circ \alpha_{2\times 2})\langle \mathcal{V}\ E_1\ (\gamma_1 \hat{\Sigma}), \mathcal{V}\ E_2\ (\gamma_1 \hat{\Sigma})\rangle && (\texttt{by (1) }) \\
&= \hat{+}\langle \alpha_2(\mathcal{V}\ E_1\ (\gamma_1 \hat{\Sigma})), \alpha_2(\mathcal{V}\ E_2\ (\gamma_1 \hat{\Sigma}))\rangle \\
&\sqsubseteq \hat{+}\langle \hat{\mathcal{V}}\ E_1\ \hat{\Sigma}, \hat{\mathcal{V}}\ E_2\ \hat{\Sigma}\rangle && (\texttt{by I.H.}) \\
&= (\hat{\mathcal{V}}\ E_1\ \hat{\Sigma}) \hat{+} (\hat{\mathcal{V}}\ E_2\ \hat{\Sigma}) \\
&= \hat{\mathcal{V}}\ E_1 + E_2\ \hat{\Sigma} && (\texttt{by def. of } \hat{\mathcal{V}})
\end{aligned}$$

  $\therefore \hat{\mathcal{V}}\ E_1 + E_2\ \hat{\Sigma} \sqsupseteq \alpha(\mathcal{V}\ E_1 + E_2)\ \hat{\Sigma}$

- $e \to -E$

  by I.H

  $\alpha(\mathcal{V}\ E) \sqsubseteq \hat{\mathcal{V}}\ E \Rightarrow \alpha_2(\mathcal{V} E (\gamma_1 \hat{\Sigma})) \sqsubseteq (\hat{\mathcal{V}} E)\hat{\Sigma}$

  Let $\dot{-}$ to be $\lambda Z.\{-z | z \in Z\}$

  $\hat{+}$ is sound operator, $id \sqsubseteq \gamma \circ \alpha$ and $\alpha_2 \circ \dot{+}$ is monotonic

$$\begin{aligned}
& \hat{-} \sqsupseteq \alpha_2 \circ \dot{-} \circ \gamma_2 \\
\Rightarrow\ & \hat{-} \circ \alpha_2 \sqsupseteq \alpha_2 \circ \dot{-} \quad \cdots (1)
\end{aligned}$$

$$
\begin{array}{rcll}
\alpha(\mathcal{V}\ -E)\ \hat{\Sigma} & = & (\alpha_2 \circ (\mathcal{V}\ -E) \circ \gamma_0)\ \hat{\Sigma} & \texttt{(by def. of } \alpha\texttt{)} \\
& = & \alpha_2(\mathcal{V}\ -E\ (\gamma_1 \hat{\Sigma})) & \\
& = & \alpha_2\{-z \mid z \in \mathcal{V}\ E\ \Sigma\} & \texttt{(by def. of}\mathcal{V}\texttt{)} \\
& = & (\alpha_2 \circ \dot{-})(\mathcal{V}\ E\ (\gamma_1 \hat{\Sigma})) & \texttt{(by def. of } \dot{-}\texttt{)} \\
& \sqsubseteq & (\hat{-} \circ \alpha_2)(\mathcal{V}\ E\ (\gamma_1 \hat{\Sigma})) & \texttt{(by (1))} \\
& = & \hat{-}(\alpha_2(\mathcal{V}\ E\ (\gamma_1 \hat{\Sigma}))) & \\
& \sqsubseteq & \hat{-}(\hat{\mathcal{V}}\ E\ \hat{\Sigma}) & \texttt{(by I.H. and mono. of } \hat{-}\texttt{)} \\
& = & \hat{\mathcal{V}}\ -E\ \hat{\Sigma} & \texttt{(by def. of } \hat{\mathcal{V}}\texttt{)}
\end{array}
$$

$\therefore \hat{\mathcal{V}}\ -E\ \hat{\Sigma} \sqsupseteq \alpha(\mathcal{V}\ -E)\ \hat{\Sigma}$

- $e \rightarrow \texttt{let}\ x\ E_1\ E_2$

  by I.H

  $\alpha(\mathcal{V}\ E_1) \sqsubseteq \hat{\mathcal{V}}\ E_1 \Rightarrow \alpha_2(\mathcal{V}E_1(\gamma_1\hat{\Sigma})) \sqsubseteq (\hat{\mathcal{V}}E_1)\hat{\Sigma}$

  $\alpha(\mathcal{V}\ E_2) \sqsubseteq \hat{\mathcal{V}}\ E_2 \Rightarrow \alpha_2(\mathcal{V}E_2(\gamma_1\hat{\Sigma})) \sqsubseteq (\hat{\mathcal{V}}E_2)\hat{\Sigma}$

  Let { x $\mapsto$.} $= \lambda\langle\Sigma, V\rangle.\{\sigma\{x \mapsto v\} | \sigma \in \Sigma, v \in V\}$

  Because operator $\cdot\{x \hat{\mapsto} \cdot\}$ is sound operator, $id \sqsubseteq \gamma \circ \alpha$ and $\alpha_1 \circ \cdot\{x \mapsto \cdot\}$ is monotonic

$$
\begin{array}{rl}
& \cdot\{x \hat{\mapsto} \cdot\} \sqsupseteq \alpha_1 \circ \cdot\{x \mapsto \cdot\} \circ \gamma_{1\times 2} \\
\Rightarrow & \cdot\{x \hat{\mapsto} \cdot\} \circ \alpha_{1\times 2} \sqsupseteq \alpha_1 \circ \cdot\{x \mapsto \cdot\} \quad \cdots (1)
\end{array}
$$

$$
\begin{array}{rcll}
\alpha(\mathcal{V}\ \texttt{let}\ x\ E_1\ E_2)\ \hat{\Sigma} & = & (\alpha_2 \circ \mathcal{V}\ \texttt{let}\ x\ E_1\ E_2)\ \hat{\Sigma} & \texttt{(by def. of } \alpha\texttt{)} \\
& = & \alpha_2(\mathcal{V}\ \texttt{let}\ x\ E_1\ E_2\ (\gamma_1\hat{\Sigma})) & \\
& = & \alpha_2(\mathcal{V}\ E_2\{\sigma\{x \mapsto v\} \mid \sigma \in \gamma_1\hat{\Sigma}, v \in \mathcal{V}\ E_1\ (\gamma_1\hat{\Sigma})\}) & \texttt{(by def. of } \mathcal{V}\texttt{)} \\
& = & (\alpha_2 \circ \mathcal{V}E_2 \circ \cdot\{x \mapsto \cdot\})(\gamma_1\hat{\Sigma}, \mathcal{V}\ E_1\ \gamma_1\hat{\Sigma}) & \texttt{(by def. of } \cdot\{x \mapsto \cdot\}\texttt{)} \\
& \sqsubseteq & (\alpha_2 \circ \gamma(\hat{\mathcal{V}}E_2) \circ \cdot\{x \mapsto \cdot\})(\gamma_1\hat{\Sigma}, \mathcal{V}\ E_1\ \gamma_1\hat{\Sigma}) & \texttt{(by I.H. \& mono. of } \alpha_2\texttt{)} \\
& = & (\alpha_2 \circ \gamma_2 \circ \hat{\mathcal{V}}E_2 \circ \alpha_1 \circ \cdot\{x \mapsto \cdot\})(\gamma_1\hat{\Sigma}, \mathcal{V}\ E_1\ \gamma_1\hat{\Sigma}) & \texttt{(by def. of } \gamma\texttt{)} \\
& \sqsubseteq & (\hat{\mathcal{V}}E_2 \circ \alpha_1 \circ \cdot\{x \mapsto \cdot\})(\gamma_1\hat{\Sigma}, \mathcal{V}\ E_1\ \gamma_1\hat{\Sigma}) & \texttt{(by } \alpha_2 \circ \gamma_2 \sqsubseteq id\ \texttt{\&} \\
& & & \texttt{assume } \hat{\mathcal{V}}E_2 \texttt{ is monotone)} \\
& \sqsubseteq & (\hat{\mathcal{V}}E_2 \circ \cdot\{x \hat{\mapsto} \cdot\} \circ \alpha_{1\times 2})(\gamma_1\hat{\Sigma}, \mathcal{V}\ E_1\ \gamma_1\hat{\Sigma}) & \texttt{(by (1))} \\
& = & \hat{\mathcal{V}}E_2(\cdot\{x \hat{\mapsto} \cdot\}(\alpha_1(\gamma_1\hat{\Sigma}), \alpha_2(\mathcal{V}\ E_1\ \gamma_1\hat{\Sigma}))) & \\
& \sqsubseteq & \hat{\mathcal{V}}E_2(\cdot\{x \hat{\mapsto} \cdot\}(\hat{\Sigma}, \hat{\mathcal{V}}\ E_1\ \hat{\Sigma}))) & \texttt{(by } \alpha_1 \circ \gamma_1 \sqsubseteq \texttt{ id \& I.H.} \\
& & & \texttt{\& } \hat{\mathcal{V}}E2, \cdot\{x \hat{\mapsto} \cdot\} \texttt{ are monotone.} \\
& = & \hat{\mathcal{V}}\ E_2(\hat{\Sigma}\{x \hat{\mapsto} \hat{\mathcal{V}}\ E_1\hat{\Sigma}\}) & \texttt{(by def. of } \cdot\{x \hat{\mapsto} \cdot\}\texttt{)} \\
& = & \hat{\mathcal{V}}\ \texttt{let}\ E_1\ E_2\ \hat{\Sigma} &
\end{array}
$$

$\therefore \hat{\mathcal{V}}\ \texttt{let}\ E_1\ E_2\ \hat{\Sigma} \sqsupseteq \alpha(\mathcal{V}\ \texttt{let}\ E_1\ E_2)\ \hat{\Sigma}$

- $e \rightarrow \texttt{if}\ E_1\ E_2\ E_3$

  by I.H

$\alpha(\mathcal{V}\ E_1) \sqsubseteq \hat{\mathcal{V}}\ E_1 \Rightarrow \alpha_2(\mathcal{V}E_1(\gamma_1\hat{\Sigma})) \sqsubseteq (\hat{\mathcal{V}}E_1)\hat{\Sigma}$
$\alpha(\mathcal{V}\ E_2) \sqsubseteq \hat{\mathcal{V}}\ E_2 \Rightarrow \alpha_2(\mathcal{V}E_2(\gamma_1\hat{\Sigma})) \sqsubseteq (\hat{\mathcal{V}}E_2)\hat{\Sigma}$
$\alpha(\mathcal{V}\ E_3) \sqsubseteq \hat{\mathcal{V}}\ E_3 \Rightarrow \alpha_3(\mathcal{V}E_3(\gamma_1\hat{\Sigma})) \sqsubseteq (\hat{\mathcal{V}}E_3)\hat{\Sigma}$

$$
\begin{array}{rcll}
\alpha(\mathcal{V}\ \texttt{if}\ E_1\ E_2\ E_3)\ \hat{\Sigma} & = & (\alpha_2 \circ \mathcal{V}\ \texttt{if}\ E_1\ E_2\ E_3 \circ \gamma_1)\ \hat{\Sigma} & (\texttt{by def. of } \alpha) \\
& = & \alpha_2(\mathcal{V}\ \texttt{if}\ E_1\ E_2\ E_3\ (\gamma_1\hat{\Sigma})) & \\
& = & \alpha_2(\mathcal{V}\ E_2\ (\mathcal{B}\ E_1\ \gamma_1\hat{\Sigma}) \cup \mathcal{V}\ E_3\ (\neg\mathcal{B}\ E_1\ \gamma_1\hat{\Sigma})) & \\
& = & \alpha_2(\mathcal{V}\ E_2\ (\mathcal{B}\ E_1\ \gamma_1\hat{\Sigma})) \sqcup \alpha_2(\mathcal{V}\ E_3\ (\neg\mathcal{B}\ E_1\ \gamma_1\hat{\Sigma})) & (\alpha_2\ \texttt{is cont.}) \\
& \sqsubseteq & \alpha_2(\mathcal{V}\ E_2\ (\gamma_1\hat{\Sigma})) \sqcup \alpha_2(\mathcal{V}\ E_3\ (\gamma_1\hat{\Sigma})) & (\texttt{by def. of } \mathcal{B}) \\
& \sqsubseteq & (\hat{\mathcal{V}}\ E_2\ \hat{\Sigma}) \sqcup (\hat{\mathcal{V}}\ E_3\ \hat{\Sigma}) & (\texttt{by I.H.})
\end{array}
$$

$\therefore \hat{\mathcal{V}}\ \texttt{if}\ E_1\ E_2\ E_3\ \hat{\Sigma} \sqsupseteq \alpha(\mathcal{V}\ \texttt{if}\ E_1\ E_2\ E_3)\ \hat{\Sigma}$

□