Take-Home Exam 1
4541.664A Program Analysis

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

1 Problem 1

1.1 Abstract syntax of C---

$$
\begin{array}{rcll}
E & \rightarrow & n & (n \in \mathbb{Z}) \\
 & | & x & \textit{variable} \\
 & | & E \texttt{ + } E & \\
 & | & \texttt{-}E & \\
 & | & \texttt{let } x\ E\ E & \textit{local binding} \\
 & | & \texttt{if } E\ E\ E &
\end{array}
$$

1.2 Collecting Semantics

1.2.1 Domains

Collecting semantics of C---($\mathcal{V}$) is defined on the following domains

$$
\begin{array}{rcl}
\mathcal{V} & \in & \mathit{Exp} \rightarrow 2^{\mathit{Env}} \rightarrow 2^{\mathbb{Z}} \\
\Sigma & \in & 2^{\mathit{Env}} \\
\sigma & \in & \mathit{Env} = \mathit{Var} \xrightarrow{\text{fin}} \mathbb{Z}
\end{array}
$$

1.2.2 Collecting semantics

Collecting semantics($\mathcal{V}$) is defined compositionally:

$$
\begin{array}{rcl}
\mathcal{V}\ n\ \Sigma & = & \{n\} \\
\mathcal{V}\ x\ \Sigma & = & \{\sigma x \mid \sigma \in \Sigma\} \\
\mathcal{V}\ E_1 \texttt{+} E_2 \Sigma & = & \{z_1 + z_2 \mid z_i \in \mathcal{V} E_i \Sigma\} \\
\mathcal{V}\ \texttt{-}E\Sigma & = & \{-z \mid z \in \mathcal{V} E \Sigma\} \\
\mathcal{V}\ \texttt{let}\ x\ E_1\ E_2\ \Sigma & = & \mathcal{V} E_2 \{\sigma\{x \mapsto v\} \mid \sigma \in \Sigma, v \in \mathcal{V} E_1 \Sigma\} \\
\mathcal{V}\ \texttt{if}\ E_1\ E_2\ E_3 & = & \mathcal{V} E_2 (\mathcal{B} E_1 \Sigma) \cup \mathcal{V} E_3 (\neg\mathcal{B} E_1 \Sigma) \\
\mathcal{B} E \Sigma & = & \cup\{\Sigma' \mid 0 \notin \mathcal{V} E \Sigma', \Sigma' \subseteq \Sigma\} \\
\neg\mathcal{B} E \Sigma & = & \cup\{\Sigma' \mid \{0\} = \mathcal{V} E \Sigma', \Sigma' \subseteq \Sigma\}
\end{array}
$$

We can rewrite above definition using operators $\dot{+}, \dot{-}, \cdot\{x \mapsto \cdot\}$ for simplicity:

$$
\begin{array}{rcl}
\dot{+} & \in & 2^{\mathbb{Z}} \times 2^{\mathbb{Z}} \to 2^{\mathbb{Z}} \\
\dot{+}\langle Z_1, Z_2\rangle & = & \{z_1 + z_2 \mid z_1 \in Z_1, z_2 \in Z_2\} \\
\\
\dot{-} & \in & 2^{\mathbb{Z}} \to 2^{\mathbb{Z}} \\
\dot{-}\langle Z\rangle & = & \{-z \mid z \in Z\} \\
\\
\cdot\{x \mapsto \cdot\} & \in & 2^{Env} \times 2^{\mathbb{Z}} \to 2^{Env} \\
\cdot\{x \mapsto \cdot\}\langle \Sigma, Z\rangle & = & \{\sigma\{x \mapsto v\} \mid \sigma \in \Sigma, v \in Z\}
\end{array}
$$

$$
\begin{array}{rcl}
\mathcal{V}\ n\ \Sigma & = & \{n\} \\
\mathcal{V}\ x\ \Sigma & = & \{\sigma x \mid \sigma \in \Sigma\} \\
\mathcal{V}\ E_1\texttt{+}E_2\Sigma & = & \dot{+}\langle \mathcal{V}E_1\Sigma, \mathcal{V}E_2\Sigma\rangle \\
\mathcal{V}\ \texttt{-}E\Sigma & = & \dot{-}\langle \mathcal{V}E\Sigma\rangle \\
\mathcal{V}\ \texttt{let}\ x\ E_1\ E_2\ \Sigma & = & (\mathcal{V}E_2 \circ \cdot\{x \mapsto \cdot\})\langle \Sigma, \mathcal{V}E_1\Sigma\rangle \\
\mathcal{V}\ \texttt{if}\ E_1\ E_2\ E_3 & = & \mathcal{V}E_2(\mathcal{B}E_1\Sigma) \cup \mathcal{V}E_3(\neg\mathcal{B}E_1\Sigma) \\
\mathcal{B}E\Sigma & = & \cup\{\Sigma' \mid 0 \notin \mathcal{V}E\Sigma', \Sigma' \subseteq \Sigma\} \\
\neg\mathcal{B}E\Sigma & = & \cup\{\Sigma' \mid \{0\} = \mathcal{V}E\Sigma', \Sigma' \subseteq \Sigma\}
\end{array}
$$

1.3 Abstract Semantics

1.3.1 Domains

Abstract semantics of `C---`($\hat{\mathcal{V}}$) is defined on the following domains

$$
\begin{array}{rcl}
\hat{\mathcal{V}} & \in & Exp \to \hat{Env} \to \hat{\mathbb{Z}} \\
\hat{\Sigma} & \in & \hat{Env}
\end{array}
$$

1.3.2 Galois connection

We assume that two Galois connections - $2^{Env} \underset{\alpha_1}{\overset{\gamma_1}{\leftrightarrows}} \hat{Env}$, $2^{\mathbb{Z}} \underset{\alpha_2}{\overset{\gamma_2}{\leftrightarrows}} \hat{\mathbb{Z}}$ - are established. Thus the Galois connection $2^{Env} \to 2^{\mathbb{Z}} \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} \hat{Env} \to \hat{\mathbb{Z}}$ can be defined compositionally with $\alpha_1, \gamma_1, \alpha_2, \gamma_2$.

$$
\begin{array}{rcl}
\alpha(m) & = & \alpha_2 \circ m \circ \gamma_1 \\
\gamma(\hat{m}) & = & \gamma_2 \circ \hat{m} \circ \alpha_1
\end{array}
$$

1.3.3 Abstract semantics

Abstract semantics of `C---` is defined compositionally:

$$
\begin{array}{rcl}
\hat{\mathcal{V}} n \hat{\Sigma} & = & \alpha_2\{n\} \\
\hat{\mathcal{V}}\ x\ \hat{\Sigma} & = & \alpha_2\{\sigma x \mid \sigma \in \gamma_1 \hat{\Sigma}\} \\
\hat{\mathcal{V}}\ E_1\texttt{+}E_2 \hat{\Sigma} & = & \alpha_2(\dot{+}\langle \gamma_2(\hat{\mathcal{V}} E_1 \hat{\Sigma}),\ \gamma_2(\mathcal{V} E_2 \hat{\Sigma})\rangle) \\
\hat{\mathcal{V}}\ \texttt{-}E \hat{\Sigma} & = & \alpha_2(\dot{-}\langle \gamma_2(\hat{\mathcal{V}} E \hat{\Sigma})\rangle) \\
\hat{\mathcal{V}}\ \texttt{let}\ x\ E_1\ E_2\ \hat{\Sigma} & = & (\hat{\mathcal{V}} E_2 \circ \alpha_1 \circ \cdot\{x \mapsto \cdot\})\langle \gamma_1 \hat{\Sigma}, \gamma_2(\hat{\mathcal{V}} E_1 \hat{\Sigma})\rangle \\
\hat{\mathcal{V}}\ \texttt{if}\ E_1\ E_2\ E_3 & = & \hat{\mathcal{V}} E_2(\alpha_1(\mathcal{B} E_1(\gamma_1 \hat{\Sigma}))) \sqcup \hat{\mathcal{V}} E_3(\alpha_1(\mathcal{B} E_1(\gamma_1 \hat{\Sigma})))
\end{array}
$$

1.4 Proof of correctness

To show the correctness of abstract semantics it's sufficient to show (1) in abstract interpretation framework.

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

1.4.1 Proof

$\alpha(\mathcal{V}E) \sqsubseteq \hat{\mathcal{V}}E$ is proved by structural induction on E.

Throughout the proof, two forms of induction hypothesis are used

$$
\begin{array}{rcll}
\mathcal{V}E & \sqsubseteq & \gamma(\hat{\mathcal{V}}E) & (i.h.1) \\
\mathcal{V}E(\gamma_1\hat{\Sigma}) & \sqsubseteq & \gamma_2(\hat{\mathcal{V}}E\hat{\Sigma}) & (i.h.2)
\end{array}
$$

$(i.h.1)$ is obtained by the Galois connection of α, γ.

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

$(i.h.2)$ is obtained by the following equivalents.

$$\alpha(\mathcal{V}E) \sqsubseteq \hat{\mathcal{V}}E \Leftrightarrow \alpha_2 \circ \mathcal{V}E \circ \gamma_1 \sqsubseteq \hat{\mathcal{V}}E \qquad \textit{(by def. of } \alpha) \tag{1}$$

Because of (1), we can show the correctness by showing that, for all $\hat{\Sigma}$, the following is hold:

$$\alpha_2(\mathcal{V}E(\gamma_1\hat{\Sigma})) \sqsubseteq \hat{\mathcal{V}}E\hat{\Sigma} \tag{2}$$

From (2) the following is hold by Galois connection

$$\alpha_2(\mathcal{V}E(\gamma_1\hat{\Sigma})) \sqsubseteq \hat{\mathcal{V}}E\hat{\Sigma} \Leftrightarrow \mathcal{V}E(\gamma_1\hat{\Sigma}) \sqsubseteq \gamma_2(\hat{\mathcal{V}}E\hat{\Sigma})$$

$\underline{E \to n}$,

$$
\begin{array}{rcll}
\alpha(\mathcal{V}n)\hat{\Sigma} & = & (\alpha_2 \circ \mathcal{V}n \circ \gamma_1)\hat{\Sigma} & \textit{(by def. } \alpha) \\
& = & \alpha_2(\mathcal{V}n(\gamma_1\hat{\Sigma})) & \\
& = & \alpha_2\{n\} & \textit{(by def. } \mathcal{V}) \\
& = & \hat{\mathcal{V}}n\hat{\Sigma} & \textit{(by def. } \hat{\mathcal{V}})
\end{array}
$$

$\underline{E \to x}$,

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

$\underline{E \to E_1\texttt{+}E_2}$,

$$\begin{array}{rcll}
\alpha(\mathcal{V}E_1\texttt{+}E_2)\hat{\Sigma} & = & (\alpha_2 \circ \mathcal{V}E_1\texttt{+}E_2 \circ \gamma_1)\hat{\Sigma} & (\textit{by def. } \alpha) \\
 & = & \alpha_2(\mathcal{V}E_1\texttt{+}E_2(\gamma_1\hat{\Sigma})) & \\
 & = & \alpha_2(\dot{+}\langle \mathcal{V}E_1(\gamma_1\hat{\Sigma}), \mathcal{V}E_1(\gamma_1\hat{\Sigma})\rangle) & (\textit{by def. } \mathcal{V}) \\
 & \sqsubseteq & \alpha_2(\dot{+}\langle \gamma_2(\hat{\mathcal{V}}E_1\hat{\Sigma}), \gamma_2(\hat{\mathcal{V}}E_1\hat{\Sigma})\rangle) & (\textit{by monotonicity of } \alpha_2, \dot{+} \textit{ and i.h.}2) \\
 & = & \hat{\mathcal{V}}E_1\texttt{+}E_2\hat{\Sigma} & (\textit{by def. } \hat{\mathcal{V}})
\end{array}$$

$\underline{E \to \texttt{-}E}$,

$$\begin{array}{rcll}
\alpha(\mathcal{V}\texttt{-}E)\hat{\Sigma} & = & (\alpha_2 \circ \mathcal{V}\texttt{-}E \circ \gamma_1)\hat{\Sigma} & (\textit{by def. } \alpha) \\
 & = & \alpha_2(\mathcal{V}\texttt{-}E(\gamma_1\hat{\Sigma})) & \\
 & = & \alpha_2(\dot{-}\langle \mathcal{V}E(\gamma_1\hat{\Sigma})\rangle) & (\textit{by def. } \mathcal{V}) \\
 & \sqsubseteq & \alpha_2(\dot{-}\langle \gamma_2(\hat{\mathcal{V}}E\hat{\Sigma})\rangle) & (\textit{by monotonicity of } \alpha_2, \dot{-} \textit{ and i.h.}2) \\
 & = & \hat{\mathcal{V}}\texttt{-}E\hat{\Sigma} & (\textit{by def. } \hat{\mathcal{V}})
\end{array}$$

$\underline{E \to \texttt{let}\ x\ E_1\ E_2}$,

$$\begin{array}{rcll}
\alpha(\mathcal{V}\texttt{let}\ x\ E_1\ E_2)\hat{\Sigma} & = & (\alpha_2 \circ \mathcal{V}\texttt{let}\ x\ E_1\ E_2 \circ \gamma_1)\hat{\Sigma} & (\textit{by def. } \mathcal{V}) \\
 & = & \alpha_2(\mathcal{V}\texttt{let}\ x\ E_1\ E_2(\gamma_1\hat{\Sigma})) & \\
 & = & \alpha_2((\mathcal{V}E_2 \circ \cdot\{x \mapsto \cdot\})\langle \gamma_1\hat{\Sigma}, \mathcal{V}E_1(\gamma_1\hat{\Sigma})\rangle) & (\textit{by def. } \mathcal{V}) \\
 & \sqsubseteq & \alpha_2((\mathcal{V}E_2 \circ \cdot\{x \mapsto \cdot\})\langle \gamma_1\hat{\Sigma}, \gamma_2(\hat{\mathcal{V}}E_1\hat{\Sigma})\rangle) & \\
 & & \quad (\textit{by monotonicity of } \alpha_2, \mathcal{V}E, \cdot\{x \mapsto \cdot\} \textit{ and i.h.}2) & \\
 & \sqsubseteq & \alpha_2((\gamma(\hat{\mathcal{V}}E_2) \circ \cdot\{x \mapsto \cdot\})\langle \gamma_1\hat{\Sigma}, \gamma_2(\hat{\mathcal{V}}E_1\hat{\Sigma})\rangle) & \\
 & & \quad (\textit{by monotonicity of } \alpha_2 \textit{ and i.h.}1) & \\
 & = & \alpha_2((\gamma_2 \circ \hat{\mathcal{V}}E_2 \circ \alpha_1) \circ \cdot\{x \mapsto \cdot\})\langle \gamma_1\hat{\Sigma}, \gamma_2(\hat{\mathcal{V}}E_1\hat{\Sigma})\rangle) & (\textit{by def. } \gamma) \\
 & = & (\alpha_2 \circ \gamma_2 \circ \hat{\mathcal{V}}E_2 \circ \alpha_1 \circ \cdot\{x \mapsto \cdot\})\langle \gamma_1\hat{\Sigma}, \gamma_2(\hat{\mathcal{V}}E_1\hat{\Sigma})\rangle) & \\
 & \sqsubseteq & (\hat{\mathcal{V}}E_2 \circ \alpha_1 \circ \cdot\{x \mapsto \cdot\})\langle \gamma_1\hat{\Sigma}, \gamma_2(\hat{\mathcal{V}}E_1\hat{\Sigma})\rangle) & (\textit{by } \alpha_2 \circ \gamma_2 \sqsubseteq \textit{id}) \\
 & = & \hat{\mathcal{V}}\texttt{let}\ x\ E_1\ E_2\hat{\Sigma} & (\textit{by def.}\hat{\mathcal{V}})
\end{array}$$

$\underline{E \to \texttt{if}\ E_1\ E_2\ E_3}$,

$$
\begin{array}{rcll}
\alpha(\mathcal{V}\texttt{if}\ E_1\ E_2\ E_3)\hat{\Sigma} & = & (\alpha_2 \circ \mathcal{V}\texttt{if}\ E_1\ E_2\ E_3 \circ \gamma_1)\hat{\Sigma} & (\textit{by def. } \alpha) \\
& = & \alpha_2(\mathcal{V}\texttt{if}\ E_1\ E_2\ E_3(\gamma_1\hat{\Sigma})) & \\
& = & \alpha_2(\mathcal{V}E_2(\mathcal{B}E_1(\gamma_1\hat{\Sigma})) \cup \mathcal{V}E_3(\neg\mathcal{B}E_1(\gamma_1\hat{\Sigma})) & (\textit{by def. } \mathcal{V}) \\
& = & \alpha_2(\mathcal{V}E_2(\mathcal{B}E_1(\gamma_1\hat{\Sigma}))) \sqcup \alpha_2(\mathcal{V}E_3(\neg\mathcal{B}E_1(\gamma_1\hat{\Sigma}))) & (\because \alpha_2 \textit{ is continuous}) \\
& \sqsubseteq & \alpha_2((\gamma(\hat{\mathcal{V}}E_2))(\mathcal{B}E_1(\gamma_1\hat{\Sigma}))) \sqcup \alpha_2((\gamma(\hat{\mathcal{V}}E_3))(\neg\mathcal{B}E_1(\gamma_1\hat{\Sigma}))) & \\
& & \quad (\textit{by monotonicity of } \alpha_2 \textit{ and i.h.} 1) & \\
& = & (\alpha_2 \circ (\gamma(\hat{\mathcal{V}}E_2)))(\mathcal{B}E_1(\gamma_1\hat{\Sigma})) & \\
& & \sqcup\ (\alpha_2 \circ (\gamma(\hat{\mathcal{V}}E_3)))(\neg\mathcal{B}E_1(\gamma_1\hat{\Sigma})) & \\
& = & (\alpha_2 \circ \gamma_2 \circ \hat{\mathcal{V}}E_2 \circ \alpha_1)(\mathcal{B}E_1(\gamma_1\hat{\Sigma})) & \\
& & \sqcup\ (\alpha_2 \circ \gamma_2 \circ \hat{\mathcal{V}}E_3 \circ \alpha_1)(\neg\mathcal{B}E_1(\gamma_1\hat{\Sigma})) & (\textit{by def. } \gamma) \\
& \sqsubseteq & (\hat{\mathcal{V}}E_2 \circ \alpha_1)(\mathcal{B}E_1(\gamma_1\hat{\Sigma}))\ \sqcup\ (\hat{\mathcal{V}}E_3 \circ \alpha_1)(\neg\mathcal{B}E_1(\gamma_1\hat{\Sigma})) & (\because\ \alpha_2 \circ \gamma_2 \sqsubseteq \textit{id}) \\
& = & \hat{\mathcal{V}}E_2(\alpha_1(\mathcal{B}E_1(\gamma_1\hat{\Sigma})))\ \sqcup\ \hat{\mathcal{V}}E_3(\alpha_1(\neg\mathcal{B}E_1(\gamma_1\hat{\Sigma}))) & \\
& = & \hat{\mathcal{V}}\texttt{if}\ E_1\ E_2\ E_3\hat{\Sigma} & (\textit{by def. } \hat{\mathcal{V}})
\end{array}
$$

□