Program Analysis HW 3

김도형

Step 1

First, define the concrete domain for collecting semantics.

$$\begin{array}{rcl} Value & = & \mathbb{Z} + Var \\ Memory & = & Loc \xrightarrow{\text{fin}} Value \\ Loc & = & Var \\ \underline{C} & \in & 2^{Memory} \to 2^{Memory} \\ \underline{E} & \in & 2^{Memory} \to 2^{Value} \end{array}$$

Next, define the semantics for $\underline{E}$.

$$\begin{array}{rcll} \underline{n}\, M & = & \{n\} & \\ \underline{E_1 + E_2}\, M & = & (\underline{E_1}\, M) \dot{+} (\underline{E_2}\, M) & \\ \underline{E_1 * E_2}\, M & = & (\underline{E_1}\, M) \dot{*} (\underline{E_2}\, M) & \\ \underline{-E}\, M & = & \dot{-}(\underline{E}\, M) & \\ \underline{E_1 < E_2}\, M & = & (\underline{E_1}\, M) \dot{<} (\underline{E_2}\, M) & \\ \underline{x}\, M & = & \{m\,(x) \mid m \in M\} & (= at_x M) \\ \underline{*x}\, M & = & \{m\,(m\,(x)) \mid m \in M\} & (= deref_x M) \\ \underline{\&x}\, M & = & \{x\} & (= loc_x M) \\ \underline{\texttt{readInt}}\, M & = & \mathbb{Z} & \end{array}$$

$$\begin{array}{rcl} V_1 \dot{+} V_2 & = & \{v_1 + v_2 \mid v_1 \in V_1,\, v_2 \in V_2\} \\ V_1 \dot{*} V_2 & = & \{v_1 * v_2 \mid v_1 \in V_1,\, v_2 \in V_2\} \\ \dot{-}V & = & \{-v \mid v \in V\} \\ V_1 \dot{<} V_2 & = & \{v_1 < v_2\,?\,1 : 0 \mid v_1 \in V_1,\, v_2 \in V_2\} \end{array}$$

Also for $\underline{C}$.

$$\begin{array}{rcl} \underline{x := E}\, M & = & \{m\{x \mapsto v\} \mid m \in M,\, v \in \underline{E}\,\{m\}\} \\ \underline{*x := E}\, M & = & \{m\{m(x) \mapsto v\} \mid m \in M,\, v \in \underline{E}\,\{m\}\} \\ \underline{C_1; C_2}\, M & = & \underline{C_2}\,(\underline{C_1}\, M) (= loc_x M) \\ \underline{\texttt{if}\ E\ C_1\ C_2}\, M & = & \underline{C_1}(\mathcal{T}_E\, M) \cup \underline{C_2}(\mathcal{F}_E\, M) \\ \underline{\texttt{repeat}\ C\ E}\, M & = & \end{array}$$

(if defined as)

$$\begin{array}{rcl} \underline{C;\ \texttt{while}\ \neg E\ C}\, M & : & \mathcal{T}_E\,(\mathsf{lfp}\,\lambda X.\, \underline{C}\, M \cup \underline{C}\,(\mathcal{F}_E\, X)) \\ \underline{\texttt{while}\ \neg E\ C}\, M & : & \mathcal{T}_E\,(\mathsf{lfp}\,\lambda X.\, M \cup \underline{C}\,(\mathcal{F}_E\, X)) \end{array}$$

$$\begin{array}{rcl} \mathcal{T}_E,\, \mathcal{F}_E & \in & 2^{Memory} \to 2^{Memory} \\ \mathcal{T}_E\, M & = & \{m \in M \mid \exists v. v \neq 0 \wedge v \in \underline{E}\,\{m\}\} \\ \mathcal{F}_E\, M & = & \{m \in M \mid 0 \in \underline{E}\,\{m\}\} \end{array}$$

Step 2

Assume an abstract domain for D-nogoto language, $Memory^\#, Value^\#$ such that Galois connection between concrete domain and abstract domain is well-defined. Functions for manipulating $Memory^\#$ such as ${at_x}^\#$, ${deref_x}^\#$, ${loc_x}^\#, \mathcal{T}_E^\#, \mathcal{F}_E^\#, \cdot\{x \mapsto^\# \cdot\}, \cdot\{x \twoheadrightarrow^\# \cdot\}, \cup^\#$ or functions for manipulating $Value^\#$ such as $+^\#, *^\#, -^\#, <^\#$ are also assumed to be well-defined, including continuity and monotonicity.

$$2^{Memory} \underset{\alpha_M}{\overset{\gamma_M}{\leftrightarrows}} Memory^\# \qquad\qquad 2^{Value} \underset{\alpha_V}{\overset{\gamma_V}{\leftrightarrows}} Value^\#$$

Step 3

As Step 1, define the abstract domain for abstract semantics.

$$\begin{array}{rcl} \underline{C}^\# & \in & Memory^\# \to Memory^\# \\ \underline{E}^\# & \in & Memory^\# \to Value^\# \end{array}$$

Next, define the semantics for $\underline{E}^\#$.

$$\begin{array}{rcl} \underline{n}^\#\ m^\# & = & \alpha_V\{n\} \\ \underline{E_1 + E_2}^\#\ m^\# & = & (\underline{E_1}^\#\ m^\#)\ +^\#\ (\underline{E_2}^\#\ m^\#) \\ \underline{E_1 * E_2}^\#\ m^\# & = & (\underline{E_1}^\#\ m^\#)\ *^\#\ (\underline{E_2}^\#\ m^\#) \\ \underline{-E}^\#\ m^\# & = & -^\#(\underline{E}^\#\ m^\#) \\ \underline{E_1 < E_2}^\#\ m^\# & = & (\underline{E_1}^\#\ m^\#)\ <^\#\ (\underline{E_2}^\#\ m^\#) \\ \underline{x}^\#\ m^\# & = & {at_x}^\#\ m^\# \\ \underline{*x}^\#\ m^\# & = & {deref_x}^\#\ m^\# \\ \underline{\&x}^\#\ m^\# & = & {loc_x}^\#\ m^\# \\ \underline{\texttt{readInt}}^\#\ m^\# & = & \alpha_V\,\mathbb{Z} = \top_V \end{array}$$

Also for $\underline{C}^\#$.

$$\begin{array}{rcl} \underline{x := E}^\#\ m^\# & = & m^\#\{x \mapsto^\# \underline{E}^\# m^\#\} \\ \underline{*x := E}^\#\ m^\# & = & m^\#\{x \twoheadrightarrow^\# \underline{E}^\# m^\#\} \\ \underline{C_1; C_2}^\#\ m^\# & = & \underline{C_2}^\#\ (\underline{C_1}^\#\ m^\#) \\ \underline{\texttt{if}\ E\ C_1\ C_2}^\#\ m^\# & = & \underline{C_1}^\#(\mathcal{T}_E^\#\ m^\#) \cup^\# \underline{C_2}^\#(\mathcal{F}_E^\#\ m^\#) \\ \underline{\texttt{repeat}\ C\ E}^\#\ m^\# & = & \mathcal{T}_E^\#\ (\mathsf{lfp}\ \lambda x.\ m^\# \cup^\#\ \underline{C}^\#\ (\mathcal{F}_E^\#\ x)) \end{array}$$

Step 4

For functions $f_M^\#$ in ${at_x}^\#$, ${deref_x}^\#$, ${loc_x}^\#, \mathcal{T}_E^\#, \mathcal{F}_E^\#, \cdot\{x \mapsto^\# \cdot\}, \cdot\{x \twoheadrightarrow^\# \cdot\}, \cup^\#$ or $f_V^\#$ in $+^\#, *^\#, -^\#, <^\#$, assume that the soundness between concrete and abstract domain holds. For example, ${at_x} \circ \gamma_M \sqsubseteq \gamma_V \circ {at_x}^\#$. As the domain for each functions are certain, subscripts for α, γ will be abbreviated.

Step 5

First, prove the soundness of E, $\forall E\colon \underline{E} \circ \gamma \sqsubseteq \gamma \circ \underline{E}^{\#}$. For abbreviation, left/right hand side will be written as (L), (R). Proof is done by structural induction on E, and duplication function which gets one argument and returns a pair of same arguments, such as $f(a) = (a, a)$ is introduced freely.

n :

(L) $m^{\#} = \underline{n}(\gamma\, m^{\#}) = \{n\}$
(R) $m^{\#} = \gamma(\underline{n}^{\#}\, m^{\#}) = \gamma(\alpha\{n\})$
$\therefore$ (L) $\sqsubseteq$ (R)

x :

(L) $m^{\#} = \underline{x}(\gamma\, m^{\#}) = (at_x \circ \gamma)m^{\#}$
(R) $m^{\#} = \gamma(\underline{x}^{\#}\, m^{\#}) = (\gamma \circ {at_x}^{\#})m^{\#}$
$\therefore$ (L) $\sqsubseteq$ (R)

$*x$:

(L) $m^{\#} = \underline{*x}(\gamma\, m^{\#}) = (deref_x \circ \gamma)m^{\#}$
(R) $m^{\#} = \gamma(\underline{*x}^{\#}\, m^{\#}) = (\gamma \circ {deref_x}^{\#})m^{\#}$
$\therefore$ (L) $\sqsubseteq$ (R)

$\&x$:

(L) $m^{\#} = \underline{\&x}(\gamma\, m^{\#}) = (loc_x \circ \gamma)m^{\#}$
(R) $m^{\#} = \gamma(\underline{\&x}^{\#}\, m^{\#}) = (\gamma \circ {loc_x}^{\#})m^{\#}$
$\therefore$ (L) $\sqsubseteq$ (R)

`readInt` :

(L) $m^{\#} = \underline{\texttt{readInt}}(\gamma\, m^{\#}) = \mathbb{Z}$
(R) $m^{\#} = \gamma(\underline{\texttt{readInt}}^{\#}\, m^{\#}) = \gamma(\top) = \mathbb{Z}$
$\therefore$ (L) $\sqsubseteq$ (R)

$E_1 + E_2$:

Assume that $\underline{E_1} \circ \gamma \sqsubseteq \gamma \circ {\underline{E_1}}^{\#}$, $\underline{E_2} \circ \gamma \sqsubseteq \gamma \circ {\underline{E_2}}^{\#}$

$$
\begin{aligned}
\text{(L)} &= \dot{+} \circ (\underline{E_1} \times \underline{E_2}) \circ \gamma \\
&= \dot{+} \circ ((\underline{E_1} \circ \gamma) \times (\underline{E_2} \circ \gamma)) \\
&\sqsubseteq \dot{+} \circ (({\gamma \circ \underline{E_1}}^{\#}) \times ({\gamma \circ \underline{E_2}}^{\#})) && \text{(by assumption and monotonicity of } \dot{+}) \\
&= \dot{+} \circ (\gamma \times \gamma) \circ ({\underline{E_1}}^{\#} \times {\underline{E_2}}^{\#}) \\
&\sqsubseteq \gamma \circ +^{\#} \circ ({\underline{E_1}}^{\#} \times {\underline{E_2}}^{\#}) && \text{(by soundness of } +^{\#}) \\
&= \gamma \circ {\underline{E_1 + E_2}}^{\#} = \text{(R)}
\end{aligned}
$$

$E_1 * E_2$, $E_1 < E_2$:

Same as $E_1 + E_2$.

$-E$:

Assume that $\underline{E} \circ \gamma \sqsubseteq \gamma \circ \underline{E}^{\#}$

$$
\begin{aligned}
\text{(L)} &= \dot{-} \circ \underline{E} \circ \gamma \\
&\sqsubseteq \dot{-} \circ \gamma \circ \underline{E}^{\#} && \text{(by assumption and monotonicity of } \dot{-}) \\
&\sqsubseteq \gamma \circ -^{\#} \circ \underline{E}^{\#} && \text{(by soundness of } -^{\#}) \\
&= \gamma \circ \underline{-E}^{\#} = \text{(R)}
\end{aligned}
$$

Next, prove the soundness of C, $\forall C\colon \underline{C}\circ\gamma \sqsubseteq \gamma\circ\underline{C}^{\#}$. For abbreviation, left/right hand side will be written as (L), (R), and id means identity function. Proof is done by structural induction on C, and duplication function which gets one argument and returns a pair of same arguments, such as $f(a) = (a, a)$ is introduced freely.

$x := E$:

$$\begin{aligned}
\text{(L)} &= \cdot\{x \mapsto \cdot\} \circ (id \times \underline{E}) \circ \gamma \\
&= \cdot\{x \mapsto \cdot\} \circ ((id \circ \gamma) \times (\underline{E} \circ \gamma)) \\
&\sqsubseteq \cdot\{x \mapsto \cdot\} \circ ((\gamma \circ id) \times (\gamma \circ \underline{E}^{\#})) && \text{(by soundness of } \underline{E} \text{ and monotonicity of } \cdot\{x \mapsto \cdot\}) \\
&= \cdot\{x \mapsto \cdot\} \circ (\gamma \times \gamma) \circ (id \times \underline{E}^{\#}) \\
&\sqsubseteq \gamma \circ \cdot\{x \mapsto^{\#} \cdot\} \circ (id \times \underline{E}^{\#}) && \text{(by soundness of } \cdot\{x \mapsto^{\#} \cdot\}) \\
&= \gamma \circ \underline{x := E}^{\#} = \text{(R)}
\end{aligned}$$

$*x := E$:

Same as $x := E$.

$C_1; C_2$:

Assume that $\underline{C_1} \circ \gamma \sqsubseteq \gamma \circ \underline{C_1}^{\#}$, $\underline{C_2} \circ \gamma \sqsubseteq \gamma \circ \underline{C_2}^{\#}$

$$\begin{aligned}
\text{(L)} &= \underline{C_1; C_2} \circ \gamma \\
&= \underline{C_2} \circ \underline{C_1} \circ \gamma \\
&\sqsubseteq \underline{C_2} \circ \gamma \circ \underline{C_1}^{\#} && \text{(by assumption and monotonicity of } \underline{C_2}) \\
&\sqsubseteq \gamma \circ \underline{C_2}^{\#} \circ \underline{C_1}^{\#} && \text{(by assumption)} \\
&= \gamma \circ \underline{C_1; C_2}^{\#} = \text{(R)}
\end{aligned}$$

`if` $E\, C_1\, C_2$:

Assume that $\underline{C_1} \circ \gamma \sqsubseteq \gamma \circ \underline{C_1}^{\#}$, $\underline{C_2} \circ \gamma \sqsubseteq \gamma \circ \underline{C_2}^{\#}$, $\underline{\mathcal{T}_E} \circ \gamma \sqsubseteq \gamma \circ \underline{\mathcal{T}_E}^{\#}$, $\underline{\mathcal{F}_E} \circ \gamma \sqsubseteq \gamma \circ \underline{\mathcal{F}_E}^{\#}$

$$\begin{aligned}
\text{(L)} &= \cup \circ ((\underline{C_1} \circ \mathcal{T}_E) \times (\underline{C_2} \circ \mathcal{F}_E)) \circ \gamma \\
&= \cup \circ ((\underline{C_1} \circ \mathcal{T}_E \circ \gamma) \times (\underline{C_2} \circ \mathcal{F}_E \circ \gamma)) \\
&\sqsubseteq \cup \circ ((\underline{C_1} \circ \gamma \circ \underline{\mathcal{T}_E}^{\#}) \times (\underline{C_2} \circ \gamma \circ \underline{\mathcal{F}_E}^{\#})) && \text{(by assumption and monotonicity of } \cup, \underline{C_1}, \underline{C_2}) \\
&\sqsubseteq \cup \circ ((\gamma \circ \underline{C_1}^{\#} \circ \underline{\mathcal{T}_E}^{\#}) \times (\gamma \circ \underline{C_2}^{\#} \circ \underline{\mathcal{F}_E}^{\#})) && \text{(by assumption)} \\
&= \cup \circ (\gamma \times \gamma) \circ ((\underline{C_1}^{\#} \circ \underline{\mathcal{T}_E}^{\#}) \times (\underline{C_2}^{\#} \circ \underline{\mathcal{F}_E}^{\#})) \\
&\sqsubseteq \gamma \circ \cup^{\#} \circ ((\underline{C_1}^{\#} \circ \underline{\mathcal{T}_E}^{\#}) \times (\underline{C_2}^{\#} \circ \underline{\mathcal{F}_E}^{\#})) && \text{(by soundness of } \cup^{\#}) \\
&= \gamma \circ \underline{\texttt{if}\ E\, C_1\, C_2}^{\#} = \text{(R)}
\end{aligned}$$

`repeat` $C\ E$:

Assume that $\underline{C} \circ \gamma \sqsubseteq \gamma \circ \underline{C}^{\#}$, $\underline{\mathcal{T}_E} \circ \gamma \sqsubseteq \gamma \circ \underline{\mathcal{T}_E}^{\#}$, $\underline{\mathcal{F}_E} \circ \gamma \sqsubseteq \gamma \circ \underline{\mathcal{F}_E}^{\#}$

(L) $m^{\#} = \underline{\mathcal{T}_E}(\mathsf{lfp}\lambda X.\gamma\, m^{\#} \cup \underline{C}(\mathcal{F}_E\, X))$

(R) $m^{\#} = \gamma \circ \underline{\mathcal{T}_E}^{\#}(\mathsf{lfp}\lambda x.m^{\#} \cup^{\#} \underline{C}^{\#}(\underline{\mathcal{F}_E}^{\#} x))$

Let $F = \lambda X.\gamma\, m^{\#} \cup \underline{C}(\mathcal{F}_E\, X), F^{\#} = \lambda x.m^{\#} \cup^{\#} \underline{C}^{\#}(\underline{\mathcal{F}_E}^{\#} x))$

If $F \circ \gamma \sqsubseteq \gamma \circ F^{\#}$, then by Fixpoint Transfer Theorem, $\mathsf{lfp}\ F \sqsubseteq \gamma \circ \mathsf{lfp}\ F^{\#}$.

Then, (L) $m^{\#} = \underline{\mathcal{T}_E}(\mathsf{lfp}\ F) \sqsubseteq \underline{\mathcal{T}_E}(\gamma \circ \mathsf{lfp}\ F^{\#}) \sqsubseteq \gamma \circ \underline{\mathcal{T}_E}^{\#}(\mathsf{lfp}\ F^{\#}) =$ (R) $m^{\#}$.

Proof of $F \circ \gamma \sqsubseteq \gamma \circ F^{\#}$ follows,

$$
\begin{aligned}
(\mathrm{L})\ m_1^{\#} &= (F \circ \gamma)\ m_1^{\#} \\
&= \gamma\ m^{\#} \cup \underline{C}((\underline{\mathcal{F}_E} \circ \gamma)\ m_1^{\#}) \\
&\sqsubseteq \gamma\ m^{\#} \cup \underline{C}((\gamma \circ \underline{\mathcal{F}_E}^{\#})\ m_1^{\#}) && \text{(by assumption and monotonicity of } \underline{C}) \\
&\sqsubseteq \gamma\ m^{\#} \cup (\gamma \circ \underline{C}^{\#})(\underline{\mathcal{F}_E}^{\#}\ m_1^{\#}) && \text{(by assumption and associativity of function composition)} \\
&= (\cup \circ \gamma)(m^{\#},\ (\underline{C}^{\#}(\underline{\mathcal{F}_E}^{\#}\ m_1^{\#})) \\
&\sqsubseteq (\gamma \circ \cup^{\#})(m^{\#},\ (\underline{C}^{\#}(\underline{\mathcal{F}_E}^{\#}\ m_1^{\#})) && \text{(by soundness of } \cup^{\#}) \\
&= \gamma(m^{\#} \cup^{\#} (\underline{C}^{\#}(\underline{\mathcal{F}_E}^{\#}\ m_1^{\#})) \\
&= \gamma(F^{\#} m_1^{\#}) = (\mathrm{R})\ m_1^{\#}
\end{aligned}
$$