Program Analysis HW 4

김도형

Step 0

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 $\underline{E}$.

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

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

Also for $\underline{C}$.

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

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

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

Step 1

Define an abstract domain $Value^\#$ as the product of three domains. First, a closed integer interval which range includes all the possible integer values. Second, a set of the rings of residue classes modulo 231010, which shows its remainder. Finally, a set of possible variables. Its partial order is defined by domain-wise inclusion. $\infty, -\infty$ is included to express open interval, and $Value^\#$ has an $\bot_{Value^\#} = (\bot, \emptyset, \emptyset)$. Remainder set has a $\top = 2^{Remainder}$. Galois connection is well-defined, since for arbitrary $V \in Value, v^\# \in Value^\#, \alpha_V(V) \sqsubseteq v^\# \iff V \sqsubseteq \gamma_V(v^\#)$. (This could be shown easily by each domain.)

Since $2^{Remainder}, 2^{Var}$ are CPOs, ($\because Remainder, Var$ are CPOs, the power set of both are also CPOs) if $(\mathbb{Z}_\infty \times \mathbb{Z}_\infty)_\bot$ is a CPO, then $Value^\#$ is also a CPO. To prove that, it is sufficient to show that an arbitrary chain has a least upper bound. For a chain $X_i = \langle a_i, b_i\rangle, \langle a_0, b_0\rangle \sqsubseteq \langle a_1, b_1\rangle \sqsubseteq \cdots \sqsubseteq \langle a_n, b_n\rangle \sqsubseteq \ldots$, as the partial order is defined by inclusion, $a_0 \geq a_1 \geq a_2 \geq \cdots \geq a_n \geq \ldots, b_0 \leq b_1 \leq b_2 \leq \cdots \leq b_n \leq \ldots$. Both $-a_i, b_i$ consists of a chain in $\mathbb{Z}_\infty$, thus have its least upper bounds $-l_a, l_b$ respectively. (It is trivial that $\mathbb{Z}_\infty$ is a CPO.) Hence, chain X_i has a least upper bound $\langle l_a, l_b\rangle$.

$Memory^\#$ can be defined by joining all the possible values variable-wise, and also has a $\bot$, which is an $\emptyset$. Proof of the fact that $Memory^\#$ is a CPO can be deduced from the fact that $Value^\#$ is a CPO, and also for Galois connection.

$$
\begin{aligned}
\mathbb{Z}_\infty &= \mathbb{Z} \cup \{-\infty, \infty\} \\
Remainder &= \mathbb{Z}_{231010} \\
Value^\# &= (\mathbb{Z}_\infty \times \mathbb{Z}_\infty)_\bot \times 2^{Remainder} \times 2^{Var} \\
Memory^\# &= Var \to Value^\#
\end{aligned}
$$

$$
\begin{aligned}
2^{Value} &\underset{\alpha_V}{\overset{\gamma_V}{\leftrightarrows}} Value^\# \\
\alpha_V(\emptyset) &= \bot_{Value^\#} \\
\alpha_V(V) &= (\langle \min(V), \max(V)\rangle, \text{remainders}(V), \text{variables}(V)) \\
&\quad (\text{remainders}(V) \text{ collects all the remainders divided by } 231010)
\end{aligned}
$$

$$
\begin{aligned}
\gamma_V(\bot_{Value^\#}) &= \emptyset \\
\gamma_V(\langle n_1, n_2\rangle, R, X) &= \{v \mid (n_1 \leq v \leq n_2) \wedge (\exists r \in R. v \equiv r \bmod 231010)\} \\
&\quad \cup \{x \mid x \in X\}
\end{aligned}
$$

$$
\begin{aligned}
2^{Memory} &\underset{\alpha}{\overset{\gamma}{\leftrightarrows}} Memory^\# \\
\alpha(M) &= \lambda x. \bigcup_{m \in M} \alpha_V(m(x)) \\
\gamma(m^\#) &= \{m \mid \forall x. m(x) \in \gamma_V(m^\#(x))\}
\end{aligned}
$$

Step 2

As Step 0, define the abstract domain for abstract semantics. Note that *fst, snd, trd* means the first, second, and third element of the given pair, which indicates the interval, the set of remainders, and the set of variables respectively.

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

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

$$\begin{aligned}
\underline{n}^{\#}\ m^{\#} &= (\langle n, n\rangle, \{n \,\%\, 231010\}, \emptyset) \\
\underline{E_1 + E_2}^{\#}\ m^{\#} &= (\underline{E_1}^{\#}\ m^{\#})\ +^{\#}\ (\underline{E_2}^{\#}\ m^{\#}) \\
\underline{E_1 * E_2}^{\#}\ m^{\#} &= (\underline{E_1}^{\#}\ m^{\#})\ *^{\#}\ (\underline{E_2}^{\#}\ m^{\#}) \\
\underline{-E}^{\#}\ m^{\#} &= -^{\#}(\underline{E}^{\#}\ m^{\#}) \\
\underline{E_1 < E_2}^{\#}\ m^{\#} &= (\underline{E_1}^{\#}\ m^{\#})\ <^{\#}\ (\underline{E_2}^{\#}\ m^{\#}) \\
\underline{x}^{\#}\ m^{\#} &= m^{\#}\ x \\
\underline{*x}^{\#}\ m^{\#} &= \bigsqcup_{y \in X}^{\#} m^{\#} y \qquad (X = trd(m^{\#} x)) \\
\underline{\&x}^{\#}\ m^{\#} &= (\bot, \emptyset, \{x\}) \\
\underline{\texttt{readInt}}^{\#}\ m^{\#} &= (\langle -\infty, \infty\rangle, \top, \emptyset)
\end{aligned}$$

$$\begin{aligned}
\bot_{Value^{\#}} +^{\#} v^{\#} &= \bot_{Value^{\#}} \quad \text{(commutative)} \\
(\langle n_1, n_2\rangle, R_1, X_1) +^{\#} (\langle n_1', n_2'\rangle, R_2, X_2) &= (\langle n_1 + n_1', n_2 + n_2'\rangle, \\
&\quad \{r_1 + r_2 \mid r_1 \in R_1, r_2 \in R_2\}, \emptyset)
\end{aligned}$$

$$\begin{aligned}
\bot_{Value^{\#}} *^{\#} v^{\#} &= \bot_{Value^{\#}} \quad \text{(commutative)} \\
(\langle n_1, n_2\rangle, R_1, X_1) *^{\#} (\langle n_1', n_2'\rangle, R_2, X_2) &= (\langle \min(n_1 n_1', n_1 n_2', n_2 n_1', n_2 n_2'), \\
&\quad \max(n_1 n_1', n_1 n_2', n_2 n_1', n_2 n_2')\rangle, \\
&\quad \{r_1 * r_2 \mid r_1 \in R_1, r_2 \in R_2\}, \emptyset)
\end{aligned}$$

$$\begin{aligned}
-^{\#} \bot_{Value^{\#}} &= \bot_{Value^{\#}} \\
-^{\#}(\langle n_1, n_2\rangle, R, X) &= (\langle -n_2, -n_1\rangle, \{-r \mid r \in R\}, \emptyset)
\end{aligned}$$

$$\begin{aligned}
\bot_{Value^{\#}} <^{\#} v^{\#} &= \bot_{Value^{\#}} \quad \text{(commutative)} \\
(\langle n_1, n_2\rangle, R_1, X_1) <^{\#} (\langle n_1', n_2'\rangle, R_2, X_2) &= \begin{cases} (\langle 1, 1\rangle, \{1\}, \emptyset) & (n_2 < n_1') \\ (\langle 0, 0\rangle, \{0\}, \emptyset) & (n_2' \le n_1) \\ (\langle 0, 1\rangle, \{0, 1\}, \emptyset) & \text{(otherwise)} \end{cases}
\end{aligned}$$

$$\begin{aligned}
\bot_{Value^{\#}} \sqcup^{\#} v^{\#} &= v^{\#} \quad \text{(commutative)} \\
(\langle n_1, n_2\rangle, R_1, X_1) \sqcup^{\#} (\langle n_1', n_2'\rangle, R_2, X_2) &= (\langle \min(n_1, n_1'), \max(n_2, n_2')\rangle, \\
&\quad R_1 \cup R_2, X_1 \cup X_2)
\end{aligned}$$

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

$$
\begin{array}{rcl}
\underline{x := E}^{\#}\ m^{\#} & = & m^{\#}\{x \mapsto^{\#} \underline{E}^{\#} m^{\#}\} \\
\underline{*x := E}^{\#}\ m^{\#} & = & \bigcup_{y \in X}^{\#} m^{\#}\{y \mapsto^{\#} \underline{E}^{\#} m^{\#}\} \qquad (X = \mathit{trd}(m^{\#} x)) \\
\underline{C_1; C_2}^{\#}\ m^{\#} & = & \underline{C_2}^{\#}\ (\underline{C_1}^{\#}\ m^{\#}) \\
\underline{\texttt{if}\ E\ C_1\ C_2}^{\#}\ m^{\#} & = & \underline{C_1}^{\#}(\mathcal{T}_E^{\#}\ m^{\#}) \cup^{\#} \underline{C_2}^{\#}(\mathcal{F}_E^{\#}\ m^{\#})
\end{array}
$$

$$
\begin{array}{rcl}
\underline{\texttt{repeat}\ C\ E}^{\#}\ m^{\#} & = & \text{(if defined as)} \\
\underline{C;\ \texttt{while}\ \neg E\ C}\ M & : & \mathcal{T}_E^{\#}\ (\mathsf{lfp}\ \lambda x.\ (\underline{C}^{\#} m^{\#}) \cup^{\#}\ \underline{C}^{\#}\ (\mathcal{F}_E^{\#}\ x)) \\
\underline{\texttt{while}\ \neg E\ C}\ M & : & \mathcal{T}_E^{\#}\ (\mathsf{lfp}\ \lambda x.\ m^{\#} \cup^{\#}\ \underline{C}^{\#}\ (\mathcal{F}_E^{\#}\ x))
\end{array}
$$

$$
\begin{array}{rcl}
\mathcal{T}_E^{\#}\ m^{\#} & = & \begin{cases} m^{\#} & \langle n_1, n_2\rangle = \mathit{fst}(\underline{E}^{\#} m^{\#}) \wedge x \neq 0 \wedge x \in [n_1, n_2] \\ \emptyset & \text{otherwise} \end{cases} \\
\mathcal{F}_E^{\#}\ m^{\#} & = & \begin{cases} m^{\#} & \langle n_1, n_2\rangle = \mathit{fst}(\underline{E}^{\#} m^{\#}) \wedge 0 \in [n_1, n_2] \\ \emptyset & \text{otherwise} \end{cases}
\end{array}
$$

$$
\begin{array}{rcl}
m_1^{\#} \cup^{\#} m_2^{\#} & = & \lambda x.(m_1^{\#} x \sqcup^{\#} m_2^{\#} x) \\
m^{\#}\{x \mapsto^{\#} v^{\#}\} & = & m^{\#}\{x \mapsto (v^{\#} \sqcup^{\#} m^{\#} x)\}
\end{array}
$$

Soundness of defined functions

Lemma 1. $\dot{+} \circ (\gamma_V \times \gamma_V) \sqsubseteq \gamma_V \circ +^{\#}$

Proof. $\forall v^{\#} \in Value^{\#}$.

$$
\begin{array}{l}
\dot{+}((\gamma_V \times \gamma_V)(\bot_{Value^{\#}}, v^{\#})) = \gamma_V(\bot_{Value^{\#}}) \dot{+} \gamma_V(v^{\#}) = \emptyset \dot{+} \gamma_V(v^{\#}) = \emptyset \\
\gamma_V(+^{\#}(\bot_{Value^{\#}}, v^{\#})) = \gamma_V(\bot_{Value^{\#}} +^{\#} v^{\#}) = \gamma_V(\bot_{Value^{\#}}) = \emptyset
\end{array}
$$

$\forall(\langle n_1, n_2\rangle, R_1, X_1), (\langle n_1', n_2'\rangle, R_2, X_2) \in Value^{\#}$.

$$
\begin{array}{l}
\dot{+}((\gamma_V \times \gamma_V)((\langle n_1, n_2\rangle, R_1, X_1), (\langle n_1', n_2'\rangle, R_2, X_2))) \\
\quad = \gamma_V(\langle n_1, n_2\rangle, R_1, X_1) \dot{+} \gamma_V(\langle n_1', n_2'\rangle, R_2, X_2) \\
\quad = \{v_1 + v_2 \mid n_1 \leq v_1 \leq n_2 \wedge n_1' \leq v_2 \leq n_2' \wedge (\exists r_1 \in R_1 . \exists r_2 \in R_2 . v_1 \equiv r_1, v_2 \equiv r_2 \bmod 231010)\} \\
\quad \sqsubseteq \{v \mid n_1 + n_1' \leq v \leq n_2 + n_2' \wedge (\exists r \in R_1 + R_2 . v \equiv r \bmod 231010)\} \\
\quad = \gamma_V(\langle n_1 + n_1', n_2 + n_2'\rangle, R_1 + R_2, \emptyset) \\
\quad = \gamma_V((\langle n_1, n_2\rangle, R_1, X_1) +^{\#} (\langle n_1', n_2'\rangle, R_2, X_2)) \\
\quad = \gamma_V(+^{\#}((\langle n_1, n_2\rangle, R_1, X_1), (\langle n_1', n_2'\rangle, R_2, X_2)))
\end{array}
$$

$\therefore \dot{+} \circ (\gamma_V \times \gamma_V) \sqsubseteq \gamma_V \circ +^{\#}$ □

Lemma 2. $\dot{*} \circ (\gamma_V \times \gamma_V) \sqsubseteq \gamma_V \circ *^{\#}$

Proof. $\forall v^{\#} \in Value^{\#}$.

$$\dot{*}((\gamma_V \times \gamma_V)(\bot_{Value^{\#}}, v^{\#})) = \gamma_V(\bot_{Value^{\#}}) \dot{*} \gamma_V(v^{\#}) = \emptyset \dot{*} \gamma_V(v^{\#}) = \emptyset$$
$$\gamma_V(*^{\#}(\bot_{Value^{\#}}, v^{\#})) = \gamma_V(\bot_{Value^{\#}} *^{\#} v^{\#}) = \gamma_V(\bot_{Value^{\#}}) = \emptyset$$

$\forall(\langle n_1, n_2\rangle, R_1, X_1), (\langle n_1', n_2'\rangle, R_2, X_2) \in Value^{\#}$.

$$\begin{aligned}
&\dot{*}((\gamma_V \times \gamma_V)((\langle n_1, n_2\rangle, R_1, X_1), (\langle n_1', n_2'\rangle, R_2, X_2))) \\
&\quad = \gamma_V(\langle n_1, n_2\rangle, R_1, X_1) \dot{*} \gamma_V(\langle n_1', n_2'\rangle, R_2, X_2) \\
&\quad = \{v_1 * v_2 \mid n_1 \le v_1 \le n_2 \wedge n_1' \le v_2 \le n_2' \wedge (\exists r_1 \in R_1 . \exists r_2 \in R_2 . v_1 \equiv r_1, v_2 \equiv r_2 \bmod 231010)\} \\
&\quad \sqsubseteq \{v \mid min(n_1 n_1', n_1 n_2', n_2 n_1', n_2 n_2') \le v \le max(n_1 n_1', n_1 n_2', n_2 n_1', n_2 n_2') \wedge (\exists r \in R_1 * R_2 . v \equiv r \bmod 231010)\} \\
&\quad = \gamma_V(\langle min(n_1 n_1', n_1 n_2', n_2 n_1', n_2 n_2'), max(n_1 n_1', n_1 n_2', n_2 n_1', n_2 n_2')\rangle, R_1 * R_2, \emptyset) \\
&\quad = \gamma_V((\langle n_1, n_2\rangle, R_1, X_1) *^{\#} (\langle n_1', n_2'\rangle, R_2, X_2)) \\
&\quad = \gamma_V(*^{\#}((\langle n_1, n_2\rangle, R_1, X_1), (\langle n_1', n_2'\rangle, R_2, X_2)))
\end{aligned}$$

$\therefore \dot{*} \circ (\gamma_V \times \gamma_V) \sqsubseteq \gamma_V \circ *^{\#}$ □

Lemma 3. $\dot{-} \circ \gamma_V \sqsubseteq \gamma_V \circ -^{\#}$

Proof.

$$\dot{-}(\gamma_V(\bot_{Value^{\#}})) = \dot{-}(\emptyset) = \emptyset$$
$$\gamma_V(-^{\#}(\bot_{Value^{\#}})) = \gamma_V(\bot_{Value^{\#}}) = \emptyset$$

$\forall(\langle n_1, n_2\rangle, R, X) \in Value^{\#}$.

$$\begin{aligned}
\dot{-}(\gamma_V(\langle n_1, n_2\rangle, R, X)) &= \{-v \mid v \in \gamma_V(\langle n_1, n_2\rangle, R, X)\} \\
&= \{-v \mid n_1 \le v \le n_2 \wedge (\exists r \in R . v \equiv r \bmod 231010)\} \\
&= \{v \mid -n_2 \le v \le -n_1 \wedge (\exists r \in -R . v \equiv r \bmod 231010)\} \\
&= \gamma_V(\langle -n_2, -n_1\rangle, -R, X) \\
&= \gamma_V(-^{\#}(\langle n_1, n_2\rangle, R, X))
\end{aligned}$$

$\therefore \dot{-} \circ \gamma_V \sqsubseteq \gamma_V \circ -^{\#}$ □

Lemma 4. $\dot{<} \circ (\gamma_V \times \gamma_V) \sqsubseteq \gamma_V \circ <^{\#}$

Proof. $\forall v^{\#} \in Value^{\#}$.

$$\dot{<}((\gamma_V \times \gamma_V)(\bot_{Value^{\#}}, v^{\#})) = \gamma_V(\bot_{Value^{\#}}) \dot{<} \gamma_V(v^{\#}) = \emptyset \dot{<} \gamma_V(v^{\#}) = \emptyset$$
$$\gamma_V(<^{\#} (\bot_{Value^{\#}}, v^{\#})) = \gamma_V(\bot_{Value^{\#}} <^{\#} v^{\#}) = \gamma_V(\bot_{Value^{\#}}) = \emptyset$$

$\forall(\langle n_1, n_2\rangle, R_1, X_1), (\langle n_1', n_2'\rangle, R_2, X_2) \in Value^{\#}$.

$$\begin{aligned}
&\dot{<}((\gamma_V \times \gamma_V)((\langle n_1, n_2\rangle, R_1, X_1), (\langle n_1', n_2'\rangle, R_2, X_2))) \\
&\quad = \gamma_V(\langle n_1, n_2\rangle, R_1, X_1) \dot{<} \gamma_V(\langle n_1', n_2'\rangle, R_2, X_2) \\
&\quad = \{v_1 < v_2 \,?\, 1 : 0 \mid v_1 \in \gamma_V(\langle n_1, n_2\rangle),\ v_2 \in \gamma_V(\langle n_1', n_2'\rangle)\} \\
&\quad \sqsubseteq \gamma_V((\langle n_1, n_2\rangle, R_1, X_1) <^{\#} (\langle n_1', n_2'\rangle, R_2, X_2)) \quad \text{(by definition of } <^{\#}\text{, each case is trivial)} \\
&\quad = \gamma_V(<^{\#} ((\langle n_1, n_2\rangle, R_1, X_1), (\langle n_1', n_2'\rangle, R_2, X_2)))
\end{aligned}$$

$\therefore \dot{<} \circ (\gamma_V \times \gamma_V) \sqsubseteq \gamma_V \circ <^{\#}$ □

Lemma 5. $\cup \circ (\gamma_V \times \gamma_V) \sqsubseteq \gamma_V \circ \sqcup^\#$

Proof. $\forall v^\# \in Value^\#$.

$$\cup((\gamma_V \times \gamma_V)(\bot_{Value^\#}, v^\#)) = \gamma_V(\bot_{Value^\#}) \cup \gamma_V(v^\#) = \emptyset \cup \gamma_V(v^\#) = \gamma_V(v^\#)$$
$$\gamma_V(\sqcup^\#(\bot_{Value^\#}, v^\#)) = \gamma_V(\bot_{Value^\#} \sqcup^\# v^\#) = \gamma_V(v^\#)$$

$\forall(\langle n_1, n_2\rangle, R_1, X_1), (\langle n_1', n_2'\rangle, R_2, X_2) \in Value^\#$.

$$\begin{aligned}
&\cup((\gamma_V \times \gamma_V)((\langle n_1, n_2\rangle, R_1, X_1), (\langle n_1', n_2'\rangle, R_2, X_2))) \\
&\quad= \gamma_V(\langle n_1, n_2\rangle, R_1, X_1) \cup \gamma_V(\langle n_1', n_2'\rangle, R_2, X_2) \\
&\quad= \{v \mid (n_1 \le v \le n_2 \wedge (\exists r \in R_1. v \equiv r \bmod 231010)) \vee (n_1' \le v \le n_2' \wedge (\exists r \in R_2. v \equiv r \bmod 231010))\} \\
&\qquad\quad \cup \{x \mid x \in X_1 \cup X_2\} \\
&\quad\sqsubseteq \{v \mid \min(n_1, n_1') \le v \le \max(n_2, n_2') \wedge (\exists r \in R_1 \cup R_2. v \equiv r \bmod 231010)\} \cup \{x \mid x \in X_1 \cup X_2\} \\
&\quad= \gamma_V(\langle \min(n_1, n_1'), \max(n_2, n_2')\rangle, R_1 \cup R_2, X_1 \cup X_2) \\
&\quad= \gamma_V((\langle n_1, n_2\rangle, R_1, X_1) \sqcup^\# (\langle n_1', n_2'\rangle, R_2, X_2)) \\
&\quad= \gamma_V(\sqcup^\#((\langle n_1, n_2\rangle, R_1, X_1), (\langle n_1', n_2'\rangle, R_2, X_2)))
\end{aligned}$$

$\therefore \cup \circ(\gamma_V \times \gamma_V) \sqsubseteq \gamma_V \circ \sqcup^\#$ □

Lemma 6. $\cup \circ (\gamma \times \gamma) \sqsubseteq \gamma \circ \cup^\#$

Proof. $\forall m^\# \in Memory^\#$.

$$\cup((\gamma \times \gamma)(\emptyset, m^\#)) = \gamma(\emptyset) \cup \gamma(m^\#) = \emptyset \cup \gamma(m^\#) = \gamma(m^\#)$$
$$\gamma(\cup^\#(\emptyset, m^\#)) = \gamma(\emptyset \cup^\# m^\#) = \gamma(m^\#)$$

$\forall m_1^\#, m_2^\# \in Memory^\#$.

$$\begin{aligned}
&\cup((\gamma \times \gamma)(m_1^\#, m_2^\#)) = \gamma(m_1^\#) \cup \gamma(m_2^\#) \\
&\quad= \{m \mid \forall x. m(x) \in \gamma_V(m_1^\#(x))\} \cup \{m \mid \forall x. m(x) \in \gamma_V(m_2^\#(x))\} \\
&\quad= \{m \mid \forall x. m(x) \in \gamma_V(m_1^\#(x)) \cup \gamma_V(m_2^\#(x))\} \\
&\quad\sqsubseteq \{m \mid \forall x. m(x) \in \gamma_V(m_1^\#(x) \sqcup^\# m_2^\#(x))\} \quad \text{(by Lemma 5)} \\
&\quad= \gamma(\lambda x.(m_1^\#(x) \sqcup^\# m_2^\#(x))) \\
&\quad= \gamma(m_1^\# \cup^\# m_2^\#) \\
&\quad= \gamma(\cup^\#(m_1^\#, m_2^\#))
\end{aligned}$$

$\therefore \cup \circ(\gamma \times \gamma) \sqsubseteq \gamma \circ \cup^\#$ □

Lemma 7. $\mathcal{T}_E \circ \gamma \sqsubseteq \gamma \circ \mathcal{T}_E^\#$

Proof.

$$\mathcal{T}_E(\gamma(\emptyset)) = \mathcal{T}_E(\emptyset) = \emptyset$$
$$\gamma(\mathcal{T}_E^\#(\emptyset)) = \gamma(\emptyset) = \emptyset$$

$\forall m^\# \in Memory^\#$.

$$\begin{aligned}
\mathcal{T}_E(\gamma(m^\#)) &= \mathcal{T}_E(\{m \mid \forall x. m(x) \in \gamma_V(m^\#(x))\}) \\
&\sqsubseteq \{m \mid \forall x. m(x) \in \gamma_V(\mathcal{T}_E^\#(m^\#(x)))\} \quad \text{(by definition of } \mathcal{T}_E^\#\text{, each case is trivial)} \\
&= \gamma(\mathcal{T}_E^\#(m^\#))
\end{aligned}$$

$\therefore \mathcal{T}_E \circ \gamma \sqsubseteq \gamma \circ \mathcal{T}_E^\#$ □

Lemma 8. $\mathcal{F}_E \circ \gamma \sqsubseteq \gamma \circ \mathcal{F}_E^\#$

Proof. Same as proof of Lemma 6. □

Soundness of E

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) $m^{\#} = \gamma_V(\underline{n}^{\#}\, m^{\#}) = \gamma_V(\langle n, n\rangle, \emptyset) = \{n\}$
$\therefore$ (L) $\sqsubseteq$ (R)

x :
(L) $m^{\#} = \underline{x}(\gamma(m^{\#})) = \{m(x) \mid m \in \gamma(m^{\#})\} = \{m(x) \mid \forall x'.m(x') \in \gamma_V(m^{\#}(x'))\} = \gamma_V(m^{\#}(x))$
(R) $m^{\#} = \gamma_V(\underline{x}^{\#}\, m^{\#}) = \gamma_V(m^{\#}(x))$
$\therefore$ (L) $\sqsubseteq$ (R)

$*x$:
(L) $m^{\#} = \underline{*x}(\gamma(m^{\#})) = \{m(m(x)) \mid m \in \gamma(m^{\#})\} = \{m(m(x)) \mid \forall y.m(y) \in \gamma_V(m^{\#}(y))\}$
$\sqsubseteq \gamma(\bigsqcup^{\#}_{y \in trd(m^{\#}x)} m^{\#}y)$ ($\because$ joining every values from variables that x could hold)
$= \gamma(\underline{*x}^{\#}\, m^{\#}) =$ (R) $m^{\#}$
$\therefore$ (L) $\sqsubseteq$ (R)

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

`readInt` :
(L) $m^{\#} = \underline{\texttt{readInt}}(\gamma\, m^{\#}) = \mathbb{Z}$
(R) $m^{\#} = \gamma(\underline{\texttt{readInt}}^{\#}\, m^{\#}) = \gamma(\langle -\infty, \infty\rangle, \emptyset) = \mathbb{Z}$
$\therefore$ (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 $\underline{E} \circ \gamma \sqsubseteq \gamma \circ \underline{E}^{\#}$

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

Soundness of C

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.

$x := E$:

$$\begin{aligned}
(\mathrm{L})m^{\#} &= \{m\{x \mapsto v\} \mid m \in \gamma(m^{\#}), v \in \underline{E}\{m\}\} \\
&\sqsubseteq \{m\{x \mapsto v\} \mid \forall y.m(y) \in \gamma_V(m^{\#}(y)), v \in \gamma_V(\underline{E}^{\#}m^{\#})\} \quad \text{(by definition of } \gamma) \\
&= \{m \mid \forall y.(y \neq x \Rightarrow m(y) \in \gamma_V(m^{\#}(y))) \wedge m(x) \in \gamma_V(\underline{E}^{\#}m^{\#})\} \\
&= \gamma(m^{\#}\{x \mapsto \underline{E}^{\#}m^{\#}\}) \quad \text{(by definition of } \gamma) \\
&\sqsubseteq \gamma(m^{\#}\{x \mapsto (\underline{E}^{\#}m^{\#} \sqcup^{\#} m^{\#}x)\}) \\
&= \gamma(m^{\#}\{x \mapsto^{\#} \underline{E}^{\#}m^{\#}\}) \\
&= \gamma(\underline{x := E}^{\#}m^{\#}) = (\mathrm{R})m^{\#}
\end{aligned}$$

$*x := E$:

$$\begin{aligned}
(\mathrm{L})m^{\#} &= \{m\{m(x) \mapsto v\} \mid m \in \gamma(m^{\#}), v \in \underline{E}\{m\}\} \\
&\sqsubseteq \{m\{x' \mapsto v\} \mid \forall z.m(z) \in \gamma_V(m^{\#}(z)), v \in \gamma_V(\underline{E}^{\#}m^{\#}), x' \in \mathit{trd}(m^{\#}(x))\} \\
&\quad \text{(by definition of } \gamma\text{, and the set of variables } m(x) \text{ holds is included in } m^{\#}(x)) \\
&= \{m \mid \forall z.(z \notin \mathit{trd}(m^{\#}(x)) \Rightarrow m(z) \in \gamma_V(m^{\#}(z))) \wedge (z \in \mathit{trd}(m^{\#}(x)) \Rightarrow m(z) \in \gamma_V(\underline{E}^{\#}m^{\#}))\} \\
&\sqsubseteq \{m \mid \forall z.m(z) \in \gamma_V((\bigcup_{y \in trd(m^{\#}x)}^{\#} m^{\#}\{y \mapsto (m^{\#}(y) \sqcup^{\#} \underline{E}^{\#}m^{\#})\})(z))\} \\
&\quad \text{(by joining abstract memories)} \\
&= \{m \mid \forall z.m(z) \in \gamma_V((\bigcup_{y \in trd(m^{\#}x)}^{\#} m^{\#}\{y \mapsto^{\#} \underline{E}^{\#}m^{\#}\})(z))\} \\
&= \gamma(\bigcup_{y \in trd(m^{\#}x)}^{\#} m^{\#}\{y \mapsto^{\#} \underline{E}^{\#}m^{\#}\}) \\
&= \gamma(\underline{x := E}^{\#}m^{\#}) = (\mathrm{R})m^{\#}
\end{aligned}$$

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

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

`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,

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