SNU 4541.664A

HW6 디자인 모범답안

조립식

조성근, 윤용호

2011년 5월 20일

1 대상 언어

$$
\begin{array}{rcll}
C & \rightarrow & \texttt{skip} & \\
 & | & x \texttt{ := } E & \\
 & | & \texttt{*}x \texttt{ := } E & \\
 & | & C \texttt{ ; } C & \\
 & | & \texttt{if } E\ C\ C & \\
 & | & \texttt{while } E\ C & \\
E & \rightarrow & n & (n \in \mathbb{Z}) \\
 & | & \texttt{true} & \\
 & | & \texttt{false} & \\
 & | & x & \\
 & | & \texttt{*}x & \\
 & | & \texttt{\&}x & \\
 & | & E \texttt{ + } E & \\
 & | & \texttt{-} E & \\
 & | & E \texttt{ < } E &
\end{array}
$$

2 모듬의미

모듬 의미함수 $\mathcal{C}$는 아래와 같은 공간에서 조립식으로 정의된다.

$$
\begin{array}{rcl}
m \in \mathit{Memory} & = & \mathit{Loc} \stackrel{\text{fin}}{\to} \mathit{Value} \\
\mathit{Value} & = & \mathbb{Z} \cup \mathbb{B} \cup \mathit{Loc} \\
\mathit{Loc} & = & \mathit{Var} \\
\mathcal{C}\ C & \in & 2^{\mathit{Memory}} \to 2^{\mathit{Memory}} \\
\mathcal{V}\ E & \in & 2^{\mathit{Memory}} \to 2^{\mathit{Value}} \\
\mathcal{B}\ E & \in & 2^{\mathit{Memory}} \to 2^{\mathit{Memory}}
\end{array}
$$

$$M \in 2^{\mathit{Memory}}$$

$$
\begin{array}{rcl}
\mathcal{C}\ \texttt{skip}\ M & = & M \\
\mathcal{C}\ x\ \texttt{:=}\ E\ M & = & \{m\{x \mapsto v\} \mid m \in M \wedge v \in \mathcal{V}\ E\ M\} \\
\mathcal{C}\ \texttt{*}x\ \texttt{:=}\ E\ M & = & \{m\{m(x) \mapsto v\} \mid m \in M \wedge v \in \mathcal{V}\ E\ M\} \\
\mathcal{C}\ C_1\ \texttt{;}\ C_2\ M & = & \mathcal{C}\ C_2\ (\mathcal{C}\ C_1\ M) \\
\mathcal{C}\ \texttt{if}\ E\ C_1\ C_2\ M & = & \mathcal{C}\ C_1\ (\mathcal{B}\ E\ M) \cup \mathcal{C}\ C_2\ (\neg\mathcal{B}\ E\ M) \\
\mathcal{C}\ \texttt{while}\ E\ C\ M & = & \neg\mathcal{B}\ E\ (\mathit{fix}\lambda X.M \cup \mathcal{C}\ C\ (\mathcal{B}\ E\ X)) \\
\mathcal{V}\ n\ M & = & \{n\} \\
\mathcal{V}\ \texttt{true}\ M & = & \{\mathit{true}\} \\
\mathcal{V}\ \texttt{false}\ M & = & \{\mathit{false}\} \\
\mathcal{V}\ x\ M & = & \{m(x) \mid m \in M\} \\
\mathcal{V}\ \texttt{*}x\ M & = & \{m(m(x)) \mid m \in M\} \\
\mathcal{V}\ \texttt{\&}x\ M & = & \{x\} \\
\mathcal{V}\ E_1\ \texttt{+}\ E_2\ M & = & \{z_1 + z_2 \mid z_i \in \mathcal{V}\ E_i\ \{m\} \wedge m \in M\} \\
\mathcal{V}\ \texttt{-}\ E\ M & = & \{-z \mid z \in \mathcal{V}\ E\ M\} \\
\mathcal{V}\ E_1\ \texttt{<}\ E_2\ M & = & \{z_1 < z_2 \mid z_i \in \mathcal{V}\ E_i\ \{m\} \wedge m \in M\} \\
\mathcal{B}\ E\ M & = & \{m \mid \mathcal{V}\ E\ \{m\} \ni \mathit{true} \wedge m \in M\} \\
\neg\mathcal{B}\ E\ M & = & \{m \mid \mathcal{V}\ E\ \{m\} \ni \mathit{false} \wedge m \in M\}
\end{array}
$$

3 요약

3.1 갈로아 연결

3.1.1 $\hat{\mathbb{Z}}$

$$2^{\mathbb{Z}} \underset{\alpha_z}{\overset{\gamma_z}{\leftrightarrows}} \hat{\mathbb{Z}}$$

$Rest$은 11로 나눈 나머지의 집합이다.

$$Rest = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$$
$$\hat{\mathbb{Z}} = \{(a, b) \mid a \leq b \wedge a, b \in Rest\} \cup \{\bot, \top\}$$

부분적인 순서는 다음과 같다.

$$\forall a, b \in Rest : \bot \sqsubseteq (a, b) \sqsubseteq \top$$
$$(0, 10) = \top$$
$$\forall a_i, b_i \in Rest : \text{if } a_2 \leq a_1 \wedge b_1 \leq b_2 \text{ then } (a_1, b_1) \sqsubseteq (a_2, b_2)$$

$$\alpha_z Z = \begin{cases} \bot & \text{if } Z = \{\}, \\ \top & \text{if } min(\{n \bmod 11 \mid n \in Z\}) = 0 \wedge max(\{n \bmod 11 \mid n \in Z\}) = 10, \\ (a, b) & \text{if } min(\{n \bmod 11 \mid n \in Z\}) = a \wedge max(\{n \bmod 11 \mid n \in Z\}) = b. \end{cases}$$

$$\gamma_z \hat{z} = \begin{cases} \{\} & \text{if } \hat{z} = \bot, \\ \{11m + n \mid m \in \mathbb{Z} \wedge a \leq n \leq b\} & \text{if } \hat{z} = (a, b), \\ \{11m + n \mid m \in \mathbb{Z} \wedge 0 \leq n \leq 10\} & \text{if } \hat{z} = \top. \end{cases}$$

α_z, γ_z는 갈로아 연결이다.

3.1.2 $\hat{\mathbb{B}}$

$$2^{\mathbb{B}} \underset{\alpha_b}{\overset{\gamma_b}{\leftrightarrows}} \hat{\mathbb{B}}$$

$$\hat{\mathbb{B}} = \{\bot, \hat{true}, \hat{false}, \top\}$$

부분적인 순서는 다음과 같다.

$$\bot \sqsubseteq \hat{true} \sqsubseteq \top \qquad \bot \sqsubseteq \hat{false} \sqsubseteq \top$$

$$\alpha_b B = \begin{cases} \bot & \text{if } B = \{\}, \\ \hat{true} & \text{if } B = \{true\}, \\ \hat{false} & \text{if } B = \{false\}, \\ \top & \text{if } B = \{true, false\}. \end{cases}$$

$$\gamma_b \hat{b} = \begin{cases} \{\} & \text{if } \hat{b} = \bot, \\ \{true\} & \text{if } \hat{b} = \hat{true}, \\ \{false\} & \text{if } \hat{b} = \hat{false}, \\ \{true, false\} & \text{if } \hat{b} = \top. \end{cases}$$

α_b, γ_b는 갈로아 연결이다.

3.1.3 $\hat{Loc}$

$$2^{Loc} \underset{\alpha_l}{\overset{\gamma_l}{\leftrightarrows}} \hat{Loc}$$

$$\hat{Loc} = 2^{Loc}$$

부분적인 순서는 집합의 포함관계와 같다.

$$\alpha_l = id \qquad \gamma_l = \hat{id}$$

α_l, γ_l는 갈로아 연결이다.

3.1.4 $\hat{Value}$

$$2^{Value} \underset{\alpha_v}{\overset{\gamma_v}{\leftrightarrows}} \hat{Value}$$

$$\hat{Value} = \hat{\mathbb{Z}} \times \hat{\mathbb{B}} \times \hat{Loc}$$

부분적인 순서는 다음과 같다.

$$\forall \hat{z}, \hat{b}, \hat{l} : \bot \sqsubseteq (z, b, l) \sqsubseteq \top$$
$$(\bot_z, \bot_b, \bot_l) = \bot \quad (\top_z, \top_b, \top_l) = \top$$
$$\forall \hat{z_1}, \hat{b_1}, \hat{l_1}, \hat{z_2}, \hat{b_2}, \hat{l_2} : \text{if } z_1 \sqsubseteq z_2 \wedge b_1 \sqsubseteq b_2 \wedge l_1 \sqsubseteq l_2 \text{ then } (z_1, b_1, l_1) \sqsubseteq (z_2, b_2, l_2)$$

clfy(classify)함수를 정의한다. *clfy*함수는 $V \in 2^{Value}$를 인자로 받아 집합의 원소를 $(Z, B, L) \in \mathbb{Z} \times \mathbb{B} \times Loc$과 같이 나눈다. 그 역함수는 $clfy^{-1}$이다.

$$clfy(V) = (\{z \mid z \in \mathbb{Z} \wedge z \in V\}, \{b \mid b \in \mathbb{B} \wedge b \in V\}, \{l \mid l \in Loc \wedge l \in V\})$$
$$clfy^{-1}(Z, B, L) = Z \cup B \cup L$$

$$\alpha_v = (\alpha_z \times \alpha_b \times \alpha_l) \circ clfy \qquad \gamma_v = clfy^{-1} \circ (\gamma_z \times \gamma_b \times \gamma_l)$$

α_v, γ_v은 갈로아 연결이다.

3.1.5 $\hat{Memory}$

$$2^{Memory} \underset{\alpha_m}{\overset{\gamma_m}{\leftrightarrows}} \hat{Memory}$$
$$2^{Loc \overset{\text{fin}}{\to} Value} \underset{\alpha_m}{\overset{\gamma_m}{\leftrightarrows}} Loc \overset{\text{fin}}{\to} \hat{Value}$$

부분적인 순서는 다음과 같다.

$$\text{if } \forall l \in dom(m_1) : m_1(l) = \bot \vee m_1(l) \sqsubseteq m_2(l) \text{ then } m_1 \sqsubseteq m_2$$

$$\begin{aligned} \alpha_m &= \lambda M.\lambda l.\alpha_v(\{m(l) \mid l \in dom(m) \wedge m \in M\}) \\ \gamma_m &= \lambda \hat{m}.\{m \mid \forall l \in dom(m) : m(l) \in \gamma_v(\hat{m}(l))\} \end{aligned}$$

α_m, γ_m은 갈로아 연결이다.

3.2 요약 의미함수

$$\begin{aligned} \hat{\mathcal{C}}\ C &\in \hat{Memory} \to \hat{Memory} \\ \hat{\mathcal{V}}\ E &\in \hat{Memory} \to \hat{Value} \\ \hat{\mathcal{B}}\ E &\in \hat{Memory} \to \hat{Memory} \end{aligned}$$

$$\begin{aligned} \hat{\mathcal{C}}\ \texttt{skip}\ \hat{m} &= \hat{m} \\ \hat{\mathcal{C}}\ x\ \texttt{:=}\ E\ \hat{m} &= \hat{m}\{x \hookrightarrow \hat{\mathcal{V}}\ E\ \hat{m}\} \\ \hat{\mathcal{C}}\ \texttt{*}x\ \texttt{:=}\ E\ \hat{m} &= \begin{cases} \bot & \text{if } \hat{m}(x) = (\hat{z}, \hat{b}, \{\}), \\ \hat{m}\{y \hookrightarrow \hat{\mathcal{V}}\ E\ \hat{m}\} & \text{if } \hat{m}(x) = (\hat{z}, \hat{b}, \{y\}), \\ \hat{m}\{y_1 \hookrightarrow (\hat{\mathcal{V}}\ E\ \hat{m} \sqcup \hat{m}(y_1)\} \cdots \{y_n \hookrightarrow (\hat{\mathcal{V}}\ E\ \hat{m} \sqcup \hat{m}(y_n))\} & \\ & \text{if } \hat{m}(x) = (\hat{z}, \hat{b}, \{y_1, \cdots, y_n\}). \end{cases} \\ \hat{\mathcal{C}}\ C_1\ ;\ C_2\ \hat{m} &= \hat{\mathcal{C}}\ C_2\ (\hat{\mathcal{C}}\ C_1\ \hat{m}) \\ \hat{\mathcal{C}}\ \texttt{if}\ E\ C_1\ C_2\ \hat{m} &= \hat{\mathcal{C}}\ C_1\ (\hat{\mathcal{B}}\ E\ \hat{m}) \sqcup \hat{\mathcal{C}}\ C_2\ (\neg\hat{\mathcal{B}}\ E\ \hat{m}) \\ \hat{\mathcal{C}}\ \texttt{while}\ E\ C\ \hat{m} &= \neg\hat{\mathcal{B}}\ E\ (fix\lambda\hat{x}.\hat{m} \sqcup \hat{\mathcal{C}}\ C\ (\hat{\mathcal{B}}\ E\ \hat{x})) \end{aligned}$$

$$
\begin{array}{rcl}
\hat{\mathcal{V}}\ n\ \hat{m} & = & \alpha_v\{n\} \\
\hat{\mathcal{V}}\ \texttt{true}\ \hat{m} & = & \alpha_v\{true\} \\
\hat{\mathcal{V}}\ \texttt{false}\ \hat{m} & = & \alpha_v\{false\} \\
\hat{\mathcal{V}}\ x\ \hat{m} & = & \hat{m}(x) \\
\hat{\mathcal{V}}\ \texttt{*}x\ \hat{m} & = & \bigsqcup\{\hat{m}(y) \mid y \in \hat{l} \wedge \hat{m}(x) = (\hat{z}, \hat{b}, \hat{l})\} \\
\hat{\mathcal{V}}\ \texttt{\&}x\ \hat{m} & = & \alpha_v\{x\} \\
\hat{\mathcal{V}}\ E_1 \texttt{ + } E_2\ \hat{m} & = & (\hat{\mathcal{V}}\ E_1\ \hat{m}) \hat{+} (\hat{\mathcal{V}}\ E_2\ \hat{m}) \\
\hat{\mathcal{V}}\ \texttt{-}\ E\ \hat{m} & = & \hat{-}\ (\hat{\mathcal{V}}\ E\ \hat{m}) \\
\hat{\mathcal{V}}\ E_1 \texttt{ < } E_2\ \hat{m} & = & (\hat{\mathcal{V}}\ E_1\ \hat{m}) \hat{<} (\hat{\mathcal{V}}\ E_2\ \hat{m})
\end{array}
$$

$$
\hat{\mathcal{B}}\ E\ \hat{m} = \begin{cases}
\bot & \text{if } E = \texttt{false}, \\
\bot & \text{if } E = x \wedge \hat{m}(x) = (\hat{z}, \hat{b}, \hat{l}) \wedge \hat{b} \sqsubseteq \hat{false}, \\
\bot & \text{if } E = z_1 \texttt{ < } z_2 \wedge z_1 \geq z_2, \\
\hat{m}\{x \hat{\mapsto} (\bot_z, \hat{true}, \bot_l)\} & \text{if } E = x \wedge \hat{m}(x) = (\hat{z}, \top_b, \hat{l}), \\
\hat{m} & \text{otherwise.}
\end{cases}
$$

$$
\neg\hat{\mathcal{B}}\ E\ \hat{m} = \begin{cases}
\bot & \text{if } E = \texttt{true}, \\
\bot & \text{if } E = x \wedge \hat{m}(x) = (\hat{z}, \hat{b}, \hat{l}) \wedge \hat{b} \sqsubseteq \hat{true}, \\
\bot & \text{if } E = z_1 \texttt{ < } z_2 \wedge z_1 < z_2, \\
\hat{m}\{x \hat{\mapsto} (\bot_z, \hat{false}, \bot_l)\} & \text{if } E = x \wedge \hat{m}(x) = (\hat{z}, \top_b, \hat{l}), \\
\hat{m} & \text{otherwise.}
\end{cases}
$$

여기서 $\hat{+}$, $\hat{-}$, $\hat{<}$, $\cdot\{x \hat{\mapsto} \cdot\}$ 는 해당 연산들을 안전하게 요약한 것들임을 아래에서 보인다.

3.2.1 $\hat{+}$ 함수

$$\hat{+} \in \hat{Val} \times \hat{Val} \to \hat{Val}$$

$\hat{+}$	$(\bot_z, \hat{b_1}, \hat{l_1})$	$((m_1, n_1), \hat{b_1}, \hat{l_1})$	$(\top_z, \hat{b_1}, \hat{l_1})$
$(\bot_z, \hat{b_2}, \hat{l_2})$	$\bot$	$\bot$	$\bot$
$((m_2, n_2), \hat{b_2}, \hat{l_2})$	$\bot$	$(\hat{z}, \bot_b, \bot_l)$	$(\top_z, \bot_b, \bot_l)$
$(\top_z, \hat{b_2}, \hat{l_2})$	$\bot$	$(\top_z, \bot_b, \bot_l)$	$(\top_z, \bot_b, \bot_l)$

$$\hat{z} = \begin{cases} (m_1 + m_2, n_1 + n_2) & \text{if } 0 \leq m_1 + m_2 \leq 10 \wedge 0 \leq n_1 + n_2 \leq 10, \\ (m_1 + m_2 - 11, n_1 + n_2 - 11) & \text{if } 11 \leq m_1 + m_2 \leq 20 \wedge 11 \leq n_1 + n_2 \leq 20, \\ \top_z & \text{otherwise.} \end{cases}$$

Lemma 1. *$\hat{+}$은 $\dot{+}$을 안전하게 요약한 것이다.*

$$\forall \hat{v_1}, \hat{v_2} \in \hat{Value} : \left(\alpha_v \circ \dot{+} \circ (\gamma_v \times \gamma_v)\right)(\hat{v_1}, \hat{v_2}) \sqsubseteq \hat{+}(\hat{v_1}, \hat{v_2})$$

Proof. $\hat{v_1} = (\hat{z_1}, \hat{b_1}, \hat{l_1})$, $\hat{v_2} = (\hat{z_2}, \hat{b_2}, \hat{l_2})$라고 하자.

- **$\hat{z_1}$(또는 $\hat{z_2}$)가 $\bot_z$일 때**

$$\begin{aligned} \left(\alpha_v \circ \dot{+} \circ (\gamma_v \times \gamma_v)\right)(\hat{v_1}, \hat{v_2}) &= \left(\alpha_v \circ \dot{+} \circ (\mathit{clfy}^{-1} \times \mathit{clfy}^{-1})\right)((\{\}, B_1, L_1), (Z_2, B_2, L_2)) \\ &= \alpha_v\{\} \\ &= \bot \\ \hat{+}(\hat{v_1}, \hat{v_2}) &= \bot \end{aligned}$$

- **$\hat{z_1}$(또는 $\hat{z_2}$)가 $\top_z$일 때**

$$\begin{aligned} \left(\alpha_v \circ \dot{+} \circ (\gamma_v \times \gamma_v)\right)(\hat{v_1}, \hat{v_2}) &= \left(\alpha_v \circ \dot{+}\right)(V_1, V_2) \\ &= \alpha_v(V') \quad (\dot{+}\text{의 정의에 의해서 } V' \subseteq \mathbb{Z}\text{이다.}) \\ &= ((\alpha_z \times \alpha_b \times \alpha_l) \circ \mathit{clfy})(V') \\ &= (\alpha_z \times \alpha_b \times \alpha_l)(V', \{\}, \{\}) \\ &\sqsubseteq (\top_z, \bot_b, \bot_l) \\ \hat{+}(\hat{v_1}, \hat{v_2}) &= (\top_z, \bot_b, \bot_l) \end{aligned}$$

- **$\hat{z_1} = (m_1, n_1)$ 이고 $\hat{z_2} = (m_2, n_2)$이고** $0 \leq m_1 + m_2 \leq 10 \wedge 0 \leq n_1 + n_2 \leq$

10일 때

$$
\begin{aligned}
&\left(\alpha_v \circ \dot{+} \circ (\gamma_v \times \gamma_v)\right)(\hat{v_1}, \hat{v_2}) \\
&\quad = \quad \left(\alpha_v \circ \dot{+} \circ (\mathit{clfy}^{-1} \times \mathit{clfy}^{-1})\right) \\
&\qquad\quad ((\{11k_1 + z_1 \mid k_1 \in \mathbb{Z} \wedge m_1 \leq z_1 \leq n_1\}, B', L'), \\
&\qquad\qquad (\{11k_2 + z_2 \mid k_2 \in \mathbb{Z} \wedge m_2 \leq z_2 \leq n_2\}, B', L')) \\
&\quad = \quad \left(\alpha_v \circ \dot{+}\right) \\
&\qquad\quad ((\{11k_1 + z_1 \mid k_1 \in \mathbb{Z} \wedge m_1 \leq z_1 \leq n_1\} \cup B' \cup L'), \\
&\qquad\qquad (\{11k_2 + z_2 \mid k_2 \in \mathbb{Z} \wedge m_2 \leq z_2 \leq n_2\} \cup B' \cup L')) \\
&\quad = \quad \alpha_v\{11k + z \mid k \in \mathbb{Z} \wedge m_1 + m_2 \leq z \leq n_1 + n_2\} \\
&\quad = \quad ((m_1 + m_2, n_1 + n_2), \perp_b, \perp_l) \\
&\hat{+}(\hat{v_1}, \hat{v_2}) \\
&\quad = \quad ((m_1 + m_2, n_1 + n_2), \perp_b, \perp_l)
\end{aligned}
$$

- $\hat{z_1} = (m_1, n_1)$ 이고 $\hat{z_2} = (m_2, n_2)$이고 $11 \leq m_1 + m_2 \leq 20 \wedge 11 \leq n_1 + n_2 \leq 20$일 때

$$
\begin{aligned}
&\left(\alpha_v \circ \dot{+} \circ (\gamma_v \times \gamma_v)\right)(\hat{v_1}, \hat{v_2}) \\
&\quad = \quad \left(\alpha_v \circ \dot{+} \circ (\mathit{clfy}^{-1} \times \mathit{clfy}^{-1})\right) \\
&\qquad\quad ((\{11k_1 + z_1 \mid k_1 \in \mathbb{Z} \wedge m_1 \leq z_1 \leq n_1\}, B', L'), \\
&\qquad\qquad (\{11k_2 + z_2 \mid k_2 \in \mathbb{Z} \wedge m_2 \leq z_2 \leq n_2\}, B', L')) \\
&\quad = \quad \left(\alpha_v \circ \dot{+}\right) \\
&\qquad\quad ((\{11k_1 + z_1 \mid k_1 \in \mathbb{Z} \wedge m_1 \leq z_1 \leq n_1\} \cup B' \cup L'), \\
&\qquad\qquad (\{11k_2 + z_2 \mid k_2 \in \mathbb{Z} \wedge m_2 \leq z_2 \leq n_2\} \cup B' \cup L')) \\
&\quad = \quad \alpha_v\{11k + z \mid k \in \mathbb{Z} \wedge m_1 + m_2 \leq z \leq n_1 + n_2\} \\
&\quad = \quad ((m_1 + m_2 - 11, n_1 + n_2 - 11), \perp_b, \perp_l) \\
&\hat{+}(\hat{v_1}, \hat{v_2}) \\
&\quad = \quad ((m_1 + m_2 - 11, n_1 + n_2 - 11), \perp_b, \perp_l)
\end{aligned}
$$

- $\hat{z_1} = (m_1, n_1)$ 이고 $\hat{z_2} = (m_2, n_2)$이고 $0 \leq m_1 + m_2 \leq 10 \wedge 11 \leq n_1 + n_2 \leq$

20일 때

$$
\begin{aligned}
\left(\alpha_v \circ \dot{+} \circ (\gamma_v \times \gamma_v)\right)(\hat{v_1}, \hat{v_2}) &= \left(\alpha_v \circ \dot{+}\right)(V_1, V_2) \\
&= \alpha_v(V') \quad (\dot{+}\text{의 정의에 의해서 } V' \subseteq \mathit{Rest}\text{이다.}) \\
&= ((\alpha_z \times \alpha_b \times \alpha_l) \circ \mathit{clfy})(V') \\
&= (\alpha_z \times \alpha_b \times \alpha_l)(V', \{\}, \{\}) \\
&\sqsubseteq (\top_z, \bot_b, \bot_l) \\
\hat{+}(\hat{v_1}, \hat{v_2}) &= (\top_z, \bot_b, \bot_l)
\end{aligned}
$$

□

3.2.2 $\hat{-}$ 함수

$$\hat{-} \in \hat{Val} \to \hat{Val}$$

	$(\bot_z, \hat{b}, \hat{l})$	$((0,0), \hat{b}, \hat{l})$	$((0,n), \hat{b}, \hat{l})$	$((m,n), \hat{b}, \hat{l})$
$\hat{-}$	$\bot$	$((0,0), \bot_b, \bot_l)$	$(\top_z, \bot_b, \bot_l)$	$((11-n, 11-m), \bot_b, \bot_l)$

단, $1 \leq m, n \leq 10$이다.

Lemma 2. *$\hat{-}$은 $\dot{-}$을 안전하게 요약한 것이다.*

$$\forall \hat{v} \in \hat{Value} : \left(\alpha_v \circ \dot{-} \circ \gamma_v\right) \hat{v} \sqsubseteq \hat{-}\hat{v}$$

Proof. $\hat{v} = (\hat{z}, \hat{b}, \hat{l})$라고 하자.

- $\hat{z}$가 $\bot_z$일 때

$$
\begin{aligned}
\left(\alpha_v \circ \dot{-} \circ \gamma_v\right) \hat{v} &= \left(\alpha_v \circ \dot{-} \circ \mathit{clfy}^{-1}\right)(\{\}, B, L) \\
&= \alpha_v\{\} \\
&= \bot \\
\hat{-}\hat{v} &= \bot
\end{aligned}
$$

- $\hat{z} = (0,0)$일 때

$$
\begin{aligned}
\left(\alpha_v \circ \dot{-} \circ \gamma_v\right) \hat{v} &= \left(\alpha_v \circ \dot{-} \circ \mathit{clfy}^{-1}\right)(\{11m \mid m \in \mathbb{Z}\}, B, L) \\
&= \alpha_v\{11m \mid m \in \mathbb{Z}\} \\
&= ((\alpha_z, \alpha_b, \alpha_l) \circ \mathit{clfy})\{11m \mid m \in \mathbb{Z}\} \\
&= (\alpha_z, \alpha_b, \alpha_l)(\{11m \mid m \in \mathbb{Z}\}, \{\}, \{\}) \\
&= ((0,0), \bot_b, \bot_l) \\
\hat{-}\hat{v} &= ((0,0), \bot_b, \bot_l)
\end{aligned}
$$

- $\hat{z} = (0, k)$**이고** $1 \leq k \leq 10$**일 때**

$$\begin{aligned}
\left(\alpha_v \circ \dot{-} \circ \gamma_v\right) \hat{v} &= \left(\alpha_v \circ \dot{-} \circ \mathit{clfy}^{-1}\right) (\{11m + n \mid m \in \mathbb{Z} \wedge 0 \leq n \leq k\}, B, L) \\
&= \alpha_v \{11m + n \mid m \in \mathbb{Z} \wedge (n = 0 \vee 11 - k \leq n \leq 10)\} \\
&= ((0, 10), \bot_b, \bot_l) \\
&= (\top_z, \bot_b, \bot_l) \\
\hat{-}\hat{v} &= (\top_z, \bot_b, \bot_l)
\end{aligned}$$

- $\hat{z} = (k_1, k_2)$**이고** $1 \leq k_1, k_2 \leq 10$**일 때**

$$\begin{aligned}
\left(\alpha_v \circ \dot{-} \circ \gamma_v\right) \hat{v} &= \left(\alpha_v \circ \dot{-} \circ \mathit{clfy}^{-1}\right) (\{11m + n \mid m \in \mathbb{Z} \wedge k_1 \leq n \leq k_2\}, B, L) \\
&= \alpha_v \{11m + n \mid m \in \mathbb{Z} \wedge 11 - k_2 \leq n \leq 11 - k_1\} \\
&= ((11 - k_2, 11 - k_1), \bot_b, \bot_l) \\
\hat{-}\hat{v} &= ((11 - k_2, 11 - k_1), \bot_b, \bot_l)
\end{aligned}$$

□

3.2.3 $\hat{<}$ 함수

$$\hat{<} \in \hat{Val} \times \hat{Val} \to \hat{Val}$$

$\hat{+}$	$(\bot_z, \hat{b_1}, \hat{l_1})$	otherwise
$(\bot_z, \hat{b_2}, \hat{l_2})$	$\bot$	$\bot$
otherwise	$\bot$	$(\bot_z, \top_b, \bot_l)$

Lemma 3. *$\hat{<}$은 $\dot{<}$을 안전하게 요약한 것이다.*

$$\forall \hat{v_1}, \hat{v_2} \in \hat{\mathit{Value}} : (\alpha_v \circ \dot{<} \circ (\gamma_v \times \gamma_v)) (\hat{v_1}, \hat{v_2}) \sqsubseteq \hat{<}(\hat{v_1}, \hat{v_2})$$

Proof. $\hat{v_1} = (\hat{z_1}, \hat{b_1}, \hat{l_1})$, $\hat{v_2} = (\hat{z_2}, \hat{b_2}, \hat{l_2})$라고 하자.

- $\hat{z_1}$**(또는** $\hat{z_2}$**)가** $\bot_z$**일 때**

$$\begin{aligned}
(\alpha_v \circ \dot{<} \circ (\gamma_v \times \gamma_v)) (\hat{v_1}, \hat{v_2}) &= \left(\alpha_v \circ \dot{<} \circ (\mathit{clfy}^{-1} \times \mathit{clfy}^{-1})\right) ((\{\}, B_1, L_1), (Z_2, B_2, L_2)) \\
&= \alpha_v \{\} \\
&= \bot \\
\hat{+}(\hat{v_1}, \hat{v_2}) &= \bot
\end{aligned}$$

- **그 밖의 경우**

$$
\begin{aligned}
(\alpha_v \circ \dot{<} \circ (\gamma_v \times \gamma_v))\,(\hat{v_1}, \hat{v_2}) &= \left(\alpha_v \circ \dot{<} \circ (\mathit{clfy}^{-1} \times \mathit{clfy}^{-1})\right)((Z_1, B_1, L_1), (Z_2, B_2, L_2)) \\
&= \alpha_v(B') \quad (\dot{<}\text{의 정의에 의해서 } B' \subseteq \mathbb{B}\text{이다.}) \\
&= ((\alpha_z \times \alpha_b \times \alpha_l) \circ \mathit{clfy})(B') \\
&= (\alpha_z \times \alpha_b \times \alpha_l)(\{\}, B', \{\}) \\
&\sqsubseteq (\bot_z, \top_b, \bot_l) \\
\hat{<}(\hat{v_1}, \hat{v_2}) &= (\bot_z, \top_b, \bot_l)
\end{aligned}
$$

□

3.2.4 $\cdot\{x \hat{\mapsto} \cdot\}$ 함수

$$\cdot\{x \hat{\mapsto} \cdot\} \in (\hat{\mathit{Memory}} \times \hat{\mathit{Value}}) \to \hat{\mathit{Memory}}$$

Lemma 4. *$\cdot\{x \hat{\mapsto} \cdot\}$은 $\cdot\{x \dot{\mapsto} \cdot\}$를 안전하게 요약한 것이다.*

$\forall \hat{m} \in \hat{\mathit{Memory}}, \hat{v} \in \hat{\mathit{Value}} : (\alpha_m \circ \cdot\{x \dot{\mapsto} \cdot\} \circ (\gamma_m \times \gamma_v))\,(\hat{m}, \hat{v}) \sqsubseteq \cdot\{x \hat{\mapsto} \cdot\}(\hat{m}, \hat{v})$

Proof.

$$
\begin{aligned}
&(\alpha_m \circ \cdot\{x \dot{\mapsto} \cdot\} \circ (\gamma_m \times \gamma_v))\,(\hat{m}, \hat{v}) \\
&\quad = (\alpha_m \circ \cdot\{x \dot{\mapsto} \cdot\})\,(\gamma_m\ \hat{m}, \gamma_v\ \hat{v}) \\
&\quad = \alpha_m((\gamma_m\ \hat{m})\{x \dot{\mapsto} \gamma_v\ \hat{v}\}) \\
&\quad = \alpha_m(\{m \mid \forall l \in \mathit{dom}(m) : m(l) \in \gamma_v(\hat{m}(l))\}\{x \dot{\mapsto} \gamma_v\ \hat{v}\}) \\
&\cdot\{x \hat{\mapsto} \cdot\}(\hat{m}, \hat{v}) \\
&\quad = \hat{m}\{x \hat{\mapsto} \hat{v}\}
\end{aligned}
$$

여기서 $\{m \mid \forall l \in \mathit{dom}(m) : m(l) \in \gamma_v(\hat{m}(l))\}\{x \dot{\mapsto} \gamma_v\ \hat{v}\}$을 M이라고 하면, $m \in M$인 모든 m이 다음을 만족한다.

$$
m(l) \in \begin{cases} \gamma_v\ (\hat{m}(l)) & \text{if } l \neq x, \\ \gamma_v\ \hat{v} & \text{if } l = x. \end{cases}
$$

$(\alpha_m(M))(l)$은 α_m의 정의에 따라서 $\alpha_v(\{m(l) \mid l \in dom(m) \wedge m \in M\})$이고 다음을 만족한다.

$$\alpha_v(\{m(l) \mid l \in dom(m) \wedge m \in M\}) \sqsubseteq \begin{cases} \alpha_v(\gamma_v\ (\hat{m}(l))) & \text{if } l \neq x, \\ \alpha_v(\gamma_v(\hat{v})) & \text{if } l = x. \end{cases}$$

그러므로

$$\begin{aligned} \alpha_m(M) &\sqsubseteq \alpha_v \circ \gamma_v \circ (\hat{m}\{x \hat{\mapsto} \hat{v}\}) \\ &\sqsubseteq \hat{m}\{x \hat{\mapsto} \hat{v}\}. && (\alpha_v \circ \gamma_v \sqsubseteq \hat{id}\text{이므로}) \end{aligned}$$

□

3.3 안전성 증명

Lemma 5. $\forall E : \alpha(\mathcal{V}\ E) \sqsubseteq \hat{\mathcal{V}}\ E$

Proof. E에 대한 귀납법으로 증명한다.

- $E = n$**일 때**

$$\begin{aligned} (\alpha(\mathcal{V}\ n))\hat{m} &= (\alpha_v \circ (\mathcal{V}\ n) \circ \gamma_m)\hat{m} \\ &= \alpha_v\{n\} \\ \hat{\mathcal{V}}\ n\ \hat{m} &= \alpha_v\{n\} \end{aligned}$$

- $E = \texttt{true}$**(또는** $\texttt{false}$**)일 때**

$$\begin{aligned} (\alpha(\mathcal{V}\ \texttt{true}))\hat{m} &= (\alpha_v \circ (\mathcal{V}\ \texttt{true}) \circ \gamma_m)\hat{m} \\ &= \alpha_v\{true\} \\ \hat{\mathcal{V}}\ \texttt{true}\ \hat{m} &= \alpha_v\{true\} \end{aligned}$$

- $E = x$**일 때**

$$\begin{aligned} (\alpha(\mathcal{V}\ x))\hat{m} &= (\alpha_v \circ (\mathcal{V}\ x) \circ \gamma_m)\hat{m} \\ &= (\alpha_v \circ (\mathcal{V}\ x))(\gamma_m(\hat{m})) \\ &= \alpha_v\{m(x) \mid m \in \gamma_m(\hat{m})\} \\ &= \alpha_v\{m(x) \mid \forall l \in dom(m) : m(l) \in \gamma_v(\hat{m}(l))\} && (\gamma_m\text{의 정의에 의해서}) \\ &\sqsubseteq \alpha_v(\gamma_v(\hat{m}(x))) \\ &\sqsubseteq \hat{m}(x) && (\alpha_v \circ \gamma_v \sqsubseteq \hat{id}\text{이므로}) \\ \hat{\mathcal{V}}\ x\ \hat{m} &= \hat{m}(x) \end{aligned}$$

- $E = *x$일 때

$$
\begin{array}{rcll}
(\alpha(\mathcal{V}\ *x))\hat{m} & = & (\alpha_v \circ (\mathcal{V}\ *x) \circ \gamma_m)\hat{m} & \\
& = & (\alpha_v \circ (\mathcal{V}\ *x))(\gamma_m(\hat{m})) & \\
& = & \alpha_v\{m(m(x)) \mid m \in \gamma_m(\hat{m})\} & \\
& = & \alpha_v\{m(m(x)) \mid \forall l \in dom(m) : m(l) \in \gamma_v(\hat{m}(l))\} & (\gamma_m\text{의 정의에 의해서}) \\
& \sqsubseteq & \alpha_v(\gamma_v(\hat{m}(m(x)))) & \\
& \sqsubseteq & \hat{m}(m(x)) & (\alpha_v \circ \gamma_v \sqsubseteq \hat{id}\text{이므로}) \\
\hat{\mathcal{V}}\ *x\ \hat{m} & = & \bigsqcup\{\hat{m}(y) \mid y \in \hat{l} \wedge \hat{m}(x) = (\hat{z}, \hat{b}, \hat{l})\} &
\end{array}
$$

여기서 $m(x) \in \gamma_v(\hat{m}(x))$이므로 $\hat{m}(x) = (\hat{z}, \hat{b}, \hat{l})$이라고 하면 $m(x) \in \gamma_v(\hat{z}, \hat{b}, \hat{l})$이다. 여기서 $m(x) \in dom(x) \subseteq Loc$이므로 $m(x) \in \gamma_l(\hat{l}) = \hat{l}$이다. 그러므로

$$
\begin{array}{rcl}
\hat{m}(m(x)) & = & \bigsqcup\{\hat{m}(m(x))\} \\
& \sqsubseteq & \bigsqcup\{\hat{m}(y) \mid y \in \hat{l} \wedge \hat{m}(x) = (\hat{z}, \hat{b}, \hat{l})\}.
\end{array}
$$

- $E = \&x$일 때

$$
\begin{array}{rcl}
(\alpha(\mathcal{V}\ \&x))\hat{m} & = & (\alpha_v \circ (\mathcal{V}\ \&x) \circ \gamma_m)\hat{m} \\
& = & (\alpha_v \circ (\mathcal{V}\ \&x))(\gamma_m(\hat{m})) \\
& = & \alpha_v\{x\} \\
\hat{\mathcal{V}}\ \&x\ \hat{m} & = & \alpha_v\{x\}
\end{array}
$$

- $E = E_1 + E_2$일 때

$$
\begin{array}{rcll}
\alpha(\mathcal{V}\ E_1 + E_2) & = & \alpha_v \circ \mathcal{V}\ E_1 + E_2 \circ \gamma_m & \\
& = & \alpha_v \circ \dot{+} \circ (\mathcal{V}\ E_1 \times \mathcal{V}\ E_2) \circ \gamma_m & \\
& = & \alpha_v \circ \dot{+} \circ ((\mathcal{V}\ E_1 \circ \gamma_m) \times (\mathcal{V}\ E_2 \circ \gamma_m)) & \\
& \sqsubseteq & \alpha_v \circ \dot{+} \circ \Big((\gamma_v \circ \hat{\mathcal{V}}\ E_1) \times (\gamma_v \circ \hat{\mathcal{V}}\ E_2)\Big) & (\text{귀납가정에 의해서}) \\
& = & \alpha_v \circ \dot{+} \circ (\gamma_v \times \gamma_v) \circ (\hat{\mathcal{V}}\ E_1 \times \hat{\mathcal{V}}\ E_2) & \\
& \sqsubseteq & \hat{+} \circ (\hat{\mathcal{V}}\ E_1 \times \hat{\mathcal{V}}\ E_2) & (\hat{+}\text{는 안전한 요약이므로}) \\
\hat{\mathcal{V}}\ E_1 + E_2 & = & \hat{+} \circ (\hat{\mathcal{V}}\ E_1 \times \hat{\mathcal{V}}\ E_2) &
\end{array}
$$

- $E = -\ E'$일 때

$$
\begin{array}{rcll}
\alpha(\mathcal{V}\ -\ E') & = & \alpha_v \circ (\mathcal{V}\ -\ E') \circ \gamma_m & \\
& = & \alpha_v \circ \dot{-} \circ (\mathcal{V}\ E') \circ \gamma_m & \\
& \sqsubseteq & \alpha_v \circ \dot{-} \circ \gamma_v \circ (\hat{\mathcal{V}}\ E') & (\text{귀납가정에 의해서}) \\
& \sqsubseteq & \hat{-} \circ (\hat{\mathcal{V}}\ E') & (\hat{-}\text{는 안전한 요약이므로}) \\
\hat{\mathcal{V}}\ -\ E' & = & \hat{-} \circ (\hat{\mathcal{V}}\ E') &
\end{array}
$$

- $E = E_1 < E_2$일 때 $E = E_1 + E_2$일 때의 증명과 유사하므로 생략한다.

□

Lemma 6. $\forall E : \alpha(\mathcal{B}\ E) \sqsubseteq \hat{\mathcal{B}}\ E$

Proof. E에 대한 귀납법으로 증명한다.

- $E = \texttt{false}$일 때

$$\begin{aligned}
(\alpha(\mathcal{B}\ \texttt{false}))\ \hat{m} &= (\alpha_m \circ \mathcal{B}\ \texttt{false} \circ \gamma_m)\hat{m} \\
&= \alpha_m\{m \mid \mathcal{V}\ \texttt{false}\ \{m\} \ni \mathit{true} \wedge m \in \gamma_m(\hat{m})\} \\
&= \alpha_m\{m \mid \{\mathit{false}\} \ni \mathit{true} \wedge m \in \gamma_m(\hat{m})\} \\
&= \alpha_m\{\} \\
&= \bot \\
\hat{\mathcal{B}}\ \texttt{false}\ \hat{m} &= \bot
\end{aligned}$$

- $E = x \wedge \hat{m}(x) = (\hat{z}, \hat{b}, \hat{l}) \wedge \hat{b} \sqsubseteq \hat{false}$일 때

$$\begin{aligned}
(\alpha(\mathcal{B}\ x))\ \hat{m} &= (\alpha_m \circ \mathcal{B}\ x \circ \gamma_m)\hat{m} \\
&= \alpha_m\{m \mid \mathcal{V}\ x\ \{m\} \ni \mathit{true} \wedge m \in \gamma_m(\hat{m})\} \\
&= \alpha_m\{m \mid \{m(x)\} \ni \mathit{true} \wedge m \in \gamma_m(\hat{m})\}
\end{aligned}$$

여기서 $m \in \gamma_m(\hat{m})$이므로,

$$\begin{aligned}
m(x) &\in \gamma_v(\hat{m}(x)) \\
&= \gamma_v(\hat{z}, \hat{b}, \hat{l}) \\
&= \gamma_z(\hat{z}) \cup \gamma_b(\hat{b}) \cup \gamma_l(\hat{l}) \\
&\sqsubseteq \gamma_z(\hat{z}) \cup \gamma_b(\hat{false}) \cup \gamma_l(\hat{l}) \quad \text{(가정에 의해서)} \\
&= \gamma_z(\hat{z}) \cup \{false\} \cup \gamma_l(\hat{l}).
\end{aligned}$$

$$\begin{aligned}
(\alpha(\mathcal{B}\ x))\ \hat{m} &= \alpha_m\{m \mid \{m(x)\} \ni \mathit{true} \wedge m \in \gamma_m(\hat{m})\} \\
&= \alpha_m\{\} \\
&= \bot \\
\hat{\mathcal{B}}\ x\ \hat{m} &= \bot
\end{aligned}$$

- $E = z_1 < z_2 \wedge z_1 \geq z_2$일 때

$$
\begin{aligned}
(\alpha(\mathcal{B}\ z_1 < z_2))\ \hat{m} &= (\alpha_m \circ \mathcal{B}\ z_1 < z_2 \circ \gamma_m)\hat{m} \\
&= \alpha_m\{m \mid \mathcal{V}\ z_1 < z_2\ \{m\} \ni \mathit{true} \wedge m \in \gamma_m(\hat{m})\} \\
&= \alpha_m\{m \mid \{\mathit{false}\} \ni \mathit{true} \wedge m \in \gamma_m(\hat{m})\} \\
&= \alpha_m\{\} \\
&= \bot \\
\hat{\mathcal{B}}\ z_1 < z_2\ \hat{m} &= \bot
\end{aligned}
$$

- $E = x \wedge \hat{m}(x) = (\hat{z}, \top, \hat{l})$일 때

$$
\begin{aligned}
(\alpha(\mathcal{B}\ x))\ \hat{m} &= (\alpha_m \circ \mathcal{B}\ x \circ \gamma_m)\hat{m} \\
&= \alpha_m\{m \mid \mathcal{V}\ x\ \{m\} \ni \mathit{true} \wedge m \in \gamma_m(\hat{m})\} \\
&= \alpha_m\{m \mid \{m(x)\} \ni \mathit{true} \wedge m \in \gamma_m(\hat{m})\} \\
&= \alpha_m\{m \mid m(x) = \mathit{true} \wedge m \in \gamma_m(\hat{m})\} \\
&= X
\end{aligned}
$$

$y \neq x$인 y에 대해서

$$
\begin{aligned}
X(y) &\sqsubseteq ((\alpha_m \circ \gamma_m)(\hat{m}))(y) \\
&\sqsubseteq \hat{m}(y). \qquad\qquad (\alpha_m \circ \gamma_m \sqsubseteq \hat{id}\ \text{이므로})
\end{aligned}
$$

$y = x$인 y에 대해서

$$
\begin{aligned}
X(y) &= (\alpha_m\{m \mid m(x) = \mathit{true} \wedge m \in \gamma_m(\hat{m})\})(y) \\
&= \alpha_v\{m(y) \mid y \in \mathit{dom}(m) \wedge m(x) = \mathit{true} \wedge m \in \gamma_m(\hat{m})\} \\
&= \alpha_v\{\mathit{true}\} \\
&= (\bot_z, \hat{\mathit{true}}, \bot_l).
\end{aligned}
$$

그러므로

$$X \sqsubseteq \hat{m}\{x \hat{\mapsto} (\bot, \hat{\mathit{true}}, \bot)\}.$$

$$\hat{\mathcal{B}}\ x\ \hat{m} = \hat{m}\{x \hat{\mapsto} (\bot_z, \hat{\mathit{true}}, \bot_l)\}$$

- **그 밖의 경우**

$$
\begin{array}{rcll}
(\alpha(\mathcal{B}\ E))\hat{m} & = & (\alpha_m \circ (\mathcal{B}\ E) \circ \gamma_m)\hat{m} & \\
& = & \alpha_m\{m \mid \mathcal{V}\ E\ \{m\} \ni \mathit{true}, m \in \gamma_m\ \hat{m}\} & \\
& \sqsubseteq & \alpha_m(\gamma_m\ \hat{m}) & \\
& \sqsubseteq & \hat{m} & (\alpha_m \circ \gamma_m \sqsubseteq \hat{id}\text{이므로}) \\
\hat{\mathcal{B}}\ E\ \hat{m} & = & \hat{m} &
\end{array}
$$

□

Lemma 7. $\forall E : \alpha(\neg\mathcal{B}\ E) \sqsubseteq \neg\hat{\mathcal{B}}\ E$

Lemma 6의 증명과 유사하므로 생략한다.

Lemma 8 (Correctness)**.** $\forall C : \alpha(\mathcal{C}\ C) \sqsubseteq \hat{\mathcal{C}}\ C$

Proof. C에 대한 귀납법으로 증명한다.

- $C = \texttt{skip}$**일 때**

$$
\begin{array}{rcll}
\alpha(\mathcal{C}\ \texttt{skip}) & = & \alpha_m \circ (\mathcal{C}\ \texttt{skip}) \circ \gamma_m & \\
& = & \alpha_m \circ id \circ \gamma_m & \\
& \sqsubseteq & \hat{id} & (\alpha_m \circ \gamma_m \sqsubseteq id\text{이므로}) \\
\hat{\mathcal{C}}\ \texttt{skip} & = & \hat{id} &
\end{array}
$$

- $C = x\ \texttt{:=}\ E$**일 때**

$$
\begin{array}{rcll}
\alpha(\mathcal{C}\ x\ \texttt{:=}\ E) & = & \alpha_m \circ (\mathcal{C}\ x\ \texttt{:=}\ E) \circ \gamma_m & \\
& = & \alpha_m \circ \cdot\{x \dot{\mapsto} \cdot\} \circ (id \times \mathcal{V}\ E) \circ \gamma_m & \\
& \sqsubseteq & \alpha_m \circ \cdot\{x \dot{\mapsto} \cdot\} \circ (\gamma_m \times \gamma_v) \circ (\hat{id} \times \hat{\mathcal{V}}\ E) & (\text{Lemma 5에 의해서}) \\
& \sqsubseteq & \cdot\{x \hat{\dot{\mapsto}} \cdot\} \circ (\hat{id} \times \hat{\mathcal{V}}\ E) & (\cdot\{x \hat{\dot{\mapsto}} \cdot\}\text{은 안전한 요약이므로}) \\
\hat{\mathcal{C}}\ x\ \texttt{:=}\ E & = & \cdot\{x \hat{\dot{\mapsto}} \cdot\} \circ (\hat{id} \times \hat{\mathcal{V}}\ E) &
\end{array}
$$

- $C = *x\ \texttt{:=}\ E$**일 때**

$$
\begin{array}{rcl}
(\alpha(\mathcal{C}\ *x\ \texttt{:=}\ E))(\hat{m}) & = & (\alpha_m \circ (\mathcal{C}\ *x\ \texttt{:=}\ E) \circ \gamma_m)(\hat{m}) \\
& = & \alpha_m\{m\{m(x) \mapsto v\} \mid m \in \gamma_m(\hat{m}) \wedge v \in \mathcal{V}\ E\ \gamma_m(\hat{m})\}
\end{array}
$$

- $\hat{m}(x) = (\hat{z}, \hat{b}, \{\})$일 때

$$
\begin{aligned}
&(\alpha(\mathcal{C} *x := E))(\hat{m}) \\
&\quad = \alpha_m\{m\{m(x) \mapsto v\} \mid m \in \gamma_m(\hat{m}) \wedge v \in \mathcal{V}\ E\ \gamma_m(\hat{m})\} \\
&\quad = \alpha_m\{\} && (m(x) \in \{\}\text{이므로}) \\
&\quad = \bot \\
&\hat{\mathcal{C}} *x := E\ \hat{m} \\
&\quad = \bot
\end{aligned}
$$

- $\hat{m}(x) = (\hat{z}, \hat{b}, \{y\})$일 때

$$
\begin{aligned}
&(\alpha(\mathcal{C} *x := E))(\hat{m}) \\
&\quad = \alpha_m\{m\{m(x) \mapsto v\} \mid m \in \gamma_m(\hat{m}) \wedge v \in \mathcal{V}\ E\ \gamma_m(\hat{m})\} \\
&\quad = \alpha_m\{m\{y \mapsto v\} \mid m \in \gamma_m(\hat{m}) \wedge v \in \mathcal{V}\ E\ \gamma_m(\hat{m})\} && (m(x) \in \{y\}\text{이므로}) \\
&\quad = (\alpha_m \circ \cdot\{y \dot{\mapsto} \cdot\} \circ (id \times \mathcal{V}\ E) \circ \gamma_m)(\hat{m}) \\
&\quad \sqsubseteq (\alpha_m \circ \cdot\{y \dot{\mapsto} \cdot\} \circ (\gamma_m \times \gamma_v) \circ (\hat{id} \times \hat{\mathcal{V}}\ E))(\hat{m}) && (\text{Lemma 5에 의해서}) \\
&\quad \sqsubseteq (\cdot\{y \hat{\mapsto} \cdot\} \circ (\hat{id} \times \hat{\mathcal{V}}\ E))(\hat{m}) && (\cdot\{x \hat{\mapsto} \cdot\}\text{은 안전한 요약이므로}) \\
&\quad = \hat{m}\{y \hat{\mapsto} \hat{\mathcal{V}}\ E\ \hat{m}\} \\
&\hat{\mathcal{C}} *x := E\ \hat{m} \\
&\quad = \hat{m}\{y \hat{\mapsto} \hat{\mathcal{V}}\ E\ \hat{m}\}
\end{aligned}
$$

- $\hat{m}(x) = (\hat{z}, \hat{b}, \{y_1, \cdots, y_n\})$일 때

$$
\begin{aligned}
&(\alpha(\mathcal{C} *x := E))(\hat{m}) \\
&\quad = \alpha_m\{m\{m(x) \mapsto v\} \mid m \in \gamma_m(\hat{m}) \wedge v \in \mathcal{V}\ E\ \gamma_m(\hat{m})\} \\
&\quad = X
\end{aligned}
$$

$X(l) = \alpha_v\{(m\{m(x) \mapsto v\})(l) \mid l \in dom(m) \wedge m \in \gamma_m(\hat{m}) \wedge v \in \mathcal{V}\ E\ \gamma_m(\hat{m})\}$

$m \in \gamma_m(\hat{m})$이므로 $m(x) \in \{y_1, \cdots, y_n\}$이다. $l \neq y_i$라면,

$$
\begin{aligned}
X(l) &= \alpha_v\{m(l) \mid l \in dom(m) \wedge m \in \gamma_m(\hat{m})\} \\
&\sqsubseteq (\alpha_v \circ \gamma_v)(\hat{m}(l)) && (m(l) \in \gamma_v(\hat{m}(l))\text{이므로}) \\
&\sqsubseteq \hat{m}(l). && (\alpha_v \circ \gamma_v \sqsubseteq \hat{id}\text{이므로})
\end{aligned}
$$

$l = y_i$라면,

$$
\begin{aligned}
X(l) &= \alpha_v(\{m(l) \mid l \in dom(m) \wedge m \in \gamma_m(\hat{m})\} \cup \{v \mid v \in \mathcal{V}\ E\ \gamma_m(\hat{m})\}) \\
&\sqsubseteq (\alpha_v\{m(l) \mid l \in dom(m) \wedge m \in \gamma_m(\hat{m})\}) \sqcup (\alpha_v\{v \mid v \in \mathcal{V}\ E\ \gamma_m(\hat{m})\}) \\
&\sqsubseteq (\alpha_v \circ \gamma_v)(\hat{m}(l)) \sqcup (\alpha_v \circ \mathcal{V}\ E\ \circ \gamma_m)(\hat{m}) && (m(l) \in \gamma_v(\hat{m}(l))\text{이므로}) \\
&\sqsubseteq \hat{m}(l) \sqcup (\alpha_v \circ \mathcal{V}\ E\ \circ \gamma_m)(\hat{m}) && (\alpha_v \circ \gamma_v \sqsubseteq \hat{id}\text{이므로}) \\
&\sqsubseteq \hat{m}(l) \sqcup (\hat{\mathcal{V}}\ E\ \hat{m}). && (\text{Lemma 5에 의해서})
\end{aligned}
$$

그러므로

$$X = \hat{m}\{y_1 \hookrightarrow (\hat{\mathcal{V}}\ E\ \hat{m} \sqcup \hat{m}(y_1)\} \cdots \{y_n \hookrightarrow (\hat{\mathcal{V}}\ E\ \hat{m} \sqcup \hat{m}(y_n))\}.$$

$$\begin{aligned}
&\hat{\mathcal{C}}\ *x\ \texttt{:=}\ E\ \hat{m} \\
&\quad = \quad \hat{m}\{y_1 \hookrightarrow (\hat{\mathcal{V}}\ E\ \hat{m} \sqcup \hat{m}(y_1)\} \cdots \{y_n \hookrightarrow (\hat{\mathcal{V}}\ E\ \hat{m} \sqcup \hat{m}(y_n))\}
\end{aligned}$$

- $C = C_1\ ;\ C_2$일 때

$$\begin{aligned}
\hat{\mathcal{C}}\ C_1\ ;\ C_2 &= (\hat{\mathcal{C}}\ C_2) \circ (\hat{\mathcal{C}}\ C_1) \\
\alpha(\mathcal{C}\ C_1\ ;\ C_2) &= \alpha_m \circ (\mathcal{C}\ C_1\ ;\ C_2) \circ \gamma_m \\
&= \alpha_m \circ (\mathcal{C}\ C_2) \circ (\mathcal{C}\ C_1) \circ \gamma_m \\
&\sqsubseteq \alpha_m \circ (\mathcal{C}\ C_2) \circ \gamma_m \circ (\hat{\mathcal{C}}\ C_1) \quad \text{(귀납가정에 의해서)} \\
&\sqsubseteq (\hat{\mathcal{C}}\ C_2) \circ (\hat{\mathcal{C}}\ C_1) \quad \text{(귀납가정에 의해서)}
\end{aligned}$$

- $C = \texttt{if}\ E\ C_1\ C_2$일 때

$$\begin{aligned}
&\hat{\mathcal{C}}\ \texttt{if}\ E\ C_1\ C_2 \\
&\quad = \quad \sqcup \circ \Big((\hat{\mathcal{C}}\ C_1 \circ \alpha_m \circ \mathcal{B}\ E \circ \gamma_m) \times (\hat{\mathcal{C}}\ C_2 \circ \alpha_m \circ \neg\mathcal{B}\ E \circ \gamma_m) \Big) \\
&\alpha(\mathcal{C}\ \texttt{if}\ E\ C_1\ C_2) \\
&\quad = \quad \alpha_m \circ \mathcal{C}\ \texttt{if}\ E\ C_1\ C_2 \circ \gamma_m \\
&\quad = \quad \alpha_m \circ \cup \circ ((\mathcal{C}\ C_1 \circ \mathcal{B}\ E \circ \gamma_m) \times (\mathcal{C}\ C_2 \circ \neg\mathcal{B}\ E \circ \gamma_m)) \\
&\quad = \quad \sqcup \circ (\alpha_m \times \alpha_m) \circ ((\mathcal{C}\ C_1 \circ \mathcal{B}\ E \circ \gamma_m) \times (\mathcal{C}\ C_2 \circ \neg\mathcal{B}\ E \circ \gamma_m)) \\
&\quad = \quad \sqcup \circ ((\alpha_m \circ \mathcal{C}\ C_1 \circ \mathcal{B}\ E \circ \gamma_m) \times (\alpha_m \circ \mathcal{C}\ C_2 \circ \neg\mathcal{B}\ E \circ \gamma_m)) \\
&\quad \sqsubseteq \quad \sqcup \circ ((\alpha_m \circ \mathcal{C}\ C_1 \circ \gamma_m \circ \alpha_m \circ \mathcal{B}\ E \circ \gamma_m) \times (\alpha_m \circ \mathcal{C}\ C_2 \circ \gamma_m \circ \alpha_m \circ \neg\mathcal{B}\ E \circ \gamma_m)) \\
&\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad (\gamma_m \circ \alpha_m \sqsupseteq id\text{이므로}) \\
&\quad \sqsubseteq \quad \sqcup \circ \Big((\hat{\mathcal{C}}\ C_1 \circ \alpha_m \circ \mathcal{B}\ E \circ \gamma_m) \times (\hat{\mathcal{C}}\ C_2 \circ \alpha_m \circ \neg\mathcal{B}\ E \circ \gamma_m) \Big) \\
&\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \text{(귀납가정에 의해서)}
\end{aligned}$$

- $C = \texttt{while}\ E\ C'$일 때

$$\begin{aligned}
\hat{\mathcal{C}}\ \texttt{while}\ E\ C'\ \hat{m} &= \neg\hat{\mathcal{B}}\ E\ (\mathit{fix}(\hat{F} \stackrel{\text{let}}{=} \lambda\hat{x}.\hat{m} \sqcup \hat{\mathcal{C}}\ C'\ (\hat{\mathcal{B}}\ E\ \hat{x}))) \\
(\alpha(\mathcal{C}\ \texttt{while}\ E\ C'))\ \hat{m} &= (\alpha_m \circ \mathcal{C}\ \texttt{while}\ E\ C' \circ \gamma_m)\ \hat{m} \\
&= (\alpha_m \circ \neg\mathcal{B}\ E)\ (\mathit{fix}(F \stackrel{\text{let}}{=} \lambda X.\gamma_m\ \hat{m} \cup \mathcal{C}\ C'\ (\mathcal{B}\ E\ X)))
\end{aligned}$$

여기서 $\alpha_m \circ F \sqsubseteq \hat{F} \circ \alpha_m$을 다음과 같이 보일 수 있다.

$$\begin{aligned}
\alpha_m \circ F &= \alpha_m \circ (\lambda X.\gamma_m\ \hat{m} \cup \mathcal{C}\ C'\ (\mathcal{B}\ E\ X)) \\
&= \lambda X.\alpha_m(\gamma_m\ \hat{m}) \sqcup \alpha_m(\mathcal{C}\ C'\ (\mathcal{B}\ E\ X)) \\
\hat{F} \circ \alpha_m &= (\lambda\hat{x}.\hat{m} \sqcup \hat{\mathcal{C}}\ C'\ (\hat{\mathcal{B}}\ E\ \hat{x})) \circ \alpha_m \\
&= \lambda X.\hat{m} \sqcup \hat{\mathcal{C}}\ C'\ (\hat{\mathcal{B}}\ E\ (\alpha_m X))
\end{aligned}$$

$$
\begin{array}{rcll}
\alpha_m(\gamma_m\ \hat{m}) & \sqsubseteq & \hat{m} & (\alpha_m \circ \gamma_m \sqsubseteq id\text{이므로}) \\
\alpha_m \circ (\mathcal{C}\ C') \circ (\mathcal{B}\ E) & \sqsubseteq & \alpha_m \circ (\mathcal{C}\ C') \circ \gamma_m \circ \alpha_m \circ (\mathcal{B}\ E) & (\gamma_m \circ \alpha_m \sqsupseteq id\text{이므로}) \\
& \sqsubseteq & (\hat{\mathcal{C}}\ C') \circ \alpha_m \circ (\mathcal{B}\ E) & (\text{귀납가정에 의해서}) \\
& \sqsubseteq & (\hat{\mathcal{C}}\ C') \circ \alpha_m \circ (\mathcal{B}\ E) \circ \gamma_m \circ \alpha_m & (\gamma_m \circ \alpha_m \sqsupseteq id\text{이므로}) \\
& \sqsubseteq & (\hat{\mathcal{C}}\ C') \circ (\hat{\mathcal{B}}\ E) \circ \alpha_m & (\text{Lemma 6에 의해서})
\end{array}
$$

그러므로 $\alpha_m \circ F \sqsubseteq \hat{F} \circ \alpha_m$이다.

"Fixpoint Transfer Theorem"에 의해 $\alpha_m(\mathit{fix}F) \sqsubseteq \mathit{fix}\hat{F}$ 이고, $\hat{\mathcal{B}}\ E$와 $\neg\hat{\mathcal{B}}\ E$가 안전하므로 위의 두 개 사이의 올바른 관계

$$(\alpha_m \circ \neg\mathcal{B}\ E)\mathit{fix}F \sqsubseteq \neg\hat{\mathcal{B}}\ E\ \mathit{fix}\hat{F}$$

을 확인할 수 있다.

□