SNU 4541.664A

HW6 디자인 모범답안
기계 상태의 변환 스타일

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

프로그램 C의 모듬의미 $[\![C]\!]$ 를 C가 실행 중에 만드는 모든 기계상태들의 집합으

로 정의한다.

$$[\![C]\!] \in 2^{State}$$

물론, 다음 함수 $F \in 2^{State} \to 2^{State}$의 고정점으로 정의된다.

$$\mathit{fix}(F \stackrel{\text{let}}{=} \lambda T.T_0 \cup \mathit{Next}\ T)$$

2.1 의미 공간

$$\begin{array}{rcrcl} s & \in & \mathit{State} & = & \mathit{Memory} \times \mathit{Label} \\ m & \in & \mathit{Memory} & = & \mathit{Loc} \stackrel{\text{fin}}{\to} \mathit{Val} \\ v & \in & \mathit{Val} & = & \mathbb{Z} + \mathbb{B} + \mathit{Loc} \\ & & \mathit{Loc} & = & \mathit{Var} \\ x & \in & \mathit{Var} & = & \text{(Program Variables)} \\ l & \in & \mathit{Label} & = & \text{(Program Labels)} \end{array}$$

2.2 초기의 기계상태 집합 T_0

빈 메모리를 $m_0 \in \mathit{Memory}$라고 하면

$$T_0 = \{(m_0, l) \mid l \in \mathit{Label}\}$$

2.3 기계상태들을 받아 다음 기계상태들을 내놓는 함수

$\mathit{Next} \in 2^{State} \to 2^{State}$는 $\mathit{next} \in \mathit{State} \to \mathit{State}$로 정의된다.

$$Next = \wp\, next$$

2.3.1 next 함수의 정의

편의상 $s \in \mathit{State}$를 (m, C_l)로 표기한다. C_l에서 C는 $l \in \mathit{Label}$에 해당하는 명령어이다. $n \in \mathit{Label} \to (\mathit{Label} \cup \{l_{end}\})$은 프로그램의 레이블을 받아 그 다음에 실행될 레이블을 돌려주는 함수이다.

$$\frac{}{\mathit{next}(m, \texttt{skip}_l) = (m, n(l))}$$

$$\frac{\mathit{eval}(m, E) = v}{\mathit{next}(m, (x \texttt{ := } E)_l) = (m\{x \mapsto v\}, n(l))}$$

$$\frac{\mathit{eval}(m, E) = v}{\mathit{next}(m, (\texttt{*}x \texttt{ := } E)_l) = (m\{m(x) \mapsto v\}, n(l))}$$

$$\frac{}{next(m, (C_{l_1}\ ;\ C_{l_2})_l) = (m, C_{l_1})}$$

$$\frac{v = eval(m, E)}{next(m, (\texttt{if}\ E\ C_{l_1}\ C_{l_2})_l) = (m, C_{l_1})}\ v = true$$

$$\frac{v = eval(m, E)}{next(m, (\texttt{if}\ E\ C_{l_1}\ C_{l_2})_l) = (m, C_{l_2})}\ v = false$$

$$\frac{eval(m, E) = v}{next(m, (\texttt{while}\ E\ C_{l'})_l) = (m, C_{l'})}\ v = true$$

$$\frac{eval(m, E) = v}{next(m, (\texttt{while}\ E\ C_{l'})_l) = (m, n(l))}\ v = false$$

2.3.2 eval 함수의 정의

$eval \in Memory \times E \to Val$ 함수는 메모리와 식을 받아 그 값을 계산한다.

$$\frac{}{eval(m, n) = n}\ n \in \mathbb{Z}$$

$$\frac{}{eval(m, \texttt{true}) = true}$$

$$\frac{}{eval(m, \texttt{false}) = false}$$

$$\frac{}{eval(m, x) = m(x)}$$

$$\frac{}{eval(m, \texttt{*}x) = m(m(x))}$$

$$\frac{}{eval(m, \texttt{\&}x) = x}$$

$$\frac{eval(m, E_1) = v_1 \quad eval(m, E_2) = v_2}{eval(m, E_1\ \texttt{+}\ E_2) = v_1 + v_2}$$

$$\frac{eval(m, E) = v}{eval(m, \texttt{-}\ E) = -v}$$

$$\frac{eval(m, E_1) = v_1 \quad eval(m, E_2) = v_2}{eval(m, E_1\ \texttt{<}\ E_2) = true}\ v_1 < v_2$$

$$\frac{eval(m, E_1) = v_1 \quad eval(m, E_2) = v_2}{eval(m, E_1\ \texttt{<}\ E_2) = false}\ v_1 \geq v_2$$

3 요약

3.1 요약 공간

$$
\begin{aligned}
\hat{State} &= \hat{Memory} \times \hat{Label} \\
\hat{Memory} &= Loc \overset{\text{fin}}{\to} \hat{Val} \\
\hat{Val} &= \hat{\mathbb{Z}} + \hat{\mathbb{B}} + Loc + \{\bot, \top\} \\
Loc &= Var \\
Var &= Variable \\
\hat{Label} &= Label + \{\bot, \top\} \\
\hat{\mathbb{Z}} &= \{x \mid 0 \le x \le 10\} \times \{x \mid 0 \le x \le 10\} + \{\bot, \top\} \\
\hat{\mathbb{B}} &= \{\bot, \hat{false}, \hat{true}, \top\}
\end{aligned}
$$

3.2 갈로아 연결

3.2.1 $\hat{\mathbb{Z}}$

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

$\hat{\mathbb{Z}}$에서의 부분적인 순서는 다음과 같이 정의된다.

1. $\forall \hat{z} \in \hat{\mathbb{Z}} : \bot \sqsubseteq \hat{z} \sqsubseteq \top$
2. let $\hat{z_1} = (l_1, u_1), \hat{z_2} = (l_2, u_2)$
   then $(l_2 \le l_1 \wedge u_1 \le u_2) \Leftrightarrow \hat{z_1} \sqsubseteq \hat{z_2}$

α_z, γ_z는 다음과 같이 정의된다.

$$
\alpha_z(X) = \begin{cases} \bot & \text{if } X = \{\}, \\ (l, u) & \text{if } l = min\{v \bmod 11 \mid v \in X\} \\ & \text{and } r = max\{v \bmod 11 \mid v \in X\}, \\ \top & \text{otherwise.} \end{cases}
$$

$$
\gamma_z(Y) = \begin{cases} \{\} & \text{if } Y = \bot, \\ \{n \mid l \le n \bmod 11 \le u\} & \text{if } Y = (l, u), \\ \mathbb{Z} & \text{if } Y = \top. \end{cases}
$$

α_z, γ_z는 갈로아 연결이다. 즉,

$$\forall x \in 2^{\mathbb{Z}}, \hat{x} \in \hat{\mathbb{Z}} : \alpha_z(x) \sqsubseteq \hat{x} \Leftrightarrow x \sqsubseteq \gamma_z(\hat{x}).$$

3.2.2 $\hat{\mathbb{B}}$

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

α_b, γ_b는 다음과 같이 정의된다.

$$\alpha_b(X) = \begin{cases} \bot & \text{if } X = \{\}, \\ \hat{false} & \text{if } X = \{false\}, \\ \hat{true} & \text{if } X = \{true\}, \\ \top & \text{otherwise.} \end{cases}$$

$$\gamma_b(Y) = \begin{cases} \{\} & \text{if } Y = \bot, \\ \{true\} & \text{if } Y = \hat{true}, \\ \{false\} & \text{if } Y = \hat{false}, \\ \mathbb{B} & \text{if } Y = \top. \end{cases}$$

α_b, γ_b는 갈로아 연결이다. 즉,

$$\forall x \in 2^{\mathbb{B}}, \hat{x} \in \hat{\mathbb{B}} : \alpha_b(x) \sqsubseteq \hat{x} \Leftrightarrow x \sqsubseteq \gamma_b(\hat{x}).$$

3.2.3 $\hat{Label}$

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

α_l, γ_l는 다음과 같이 정의된다.

$$\alpha_l(X) = \begin{cases} \bot & \text{if } X = \{\}, \\ \hat{l} & \text{if } X = \{l\}, \\ \top & \text{otherwise.} \end{cases}$$

$$\gamma_l(Y) = \begin{cases} \{\} & \text{if } Y = \bot, \\ \{l\} & \text{if } Y = \hat{l}, \\ Label & \text{if } Y = \top. \end{cases}$$

$\hat{Label}$은 $Label$의 올려붙인 집합이므로 그 부분적인 순서와 갈로아 연결은 자명하다. γ_l은 그 정의에 의해 적용 결과가 $\{\}, Label, \{l\}$의 세 가지 경우 뿐이며, 요약분할함수로 인해 실제 계산에서는 $\{\}, Label$이 계산되지 않는다. 즉, 언제나 $\alpha_l\ l = \hat{l}$, $\gamma_l\ \hat{l} = \{l\}$의 계산만 일어난다. 따라서 앞으로는 편의상 $\hat{l}$을 l과 혼용하기로 한다.

3.2.4 $\hat{Value}$

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

α_v, γ_v는 다음과 같이 정의된다.

$$\alpha_v(X) = \begin{cases} \bot & \text{if } X = \{\}, \\ \alpha_z(X) & \text{if } X \subseteq \mathbb{Z}, \\ \alpha_b(X) & \text{if } X \subseteq \mathbb{B}, \\ x & \text{if } X = \{x\} \subseteq Loc, \\ \top & \text{otherwise.} \end{cases}$$

$$\gamma_v(Y) = \begin{cases} \{\} & \text{if } Y = \bot, \\ \gamma_z(Y) & \text{if } Y \in \hat{\mathbb{Z}}, \\ \gamma_b(Y) & \text{if } Y \in \hat{\mathbb{B}}, \\ \{Y\} & \text{if } Y \in Loc, \\ Val & \text{if } Y = \top. \end{cases}$$

α_v, γ_v는 갈로아 연결이다. 즉,

$$\forall x \in 2^{Value}, \hat{x} \in \hat{Value} : \alpha_v(x) \sqsubseteq \hat{x} \Leftrightarrow x \sqsubseteq \gamma_v(\hat{x}).$$

3.2.5 $\hat{Memory}$

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

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

α_m, γ_m은 갈로아 연결이다. 즉,

$$\forall M \in 2^{Memory}, \hat{m} \in \hat{Memory} : \alpha_m(M) \sqsubseteq \hat{m} \Longleftrightarrow M \sqsubseteq \gamma_m(\hat{m}).$$

3.2.6 $\hat{State}$

$$2^{State} \underset{\alpha_s}{\overset{\gamma_s}{\leftrightarrows}} \hat{State}$$

$$\alpha_s = \lambda X.(\alpha_m\{a \mid (a,b) \in X\}, \alpha_l\{b \mid (a,b) \in X\})$$

$$\gamma_s = \lambda \hat{X}.\{(m,l) \mid m \in \gamma_m(\hat{m}), l \in \gamma_l(\hat{l}), (\hat{m},\hat{l}) = \hat{X}\}$$

α_s, γ_s은 갈로아 연결이다. 즉,

$$\forall x \in 2^{State}, \hat{x} \in \hat{State} : \alpha_s(x) \sqsubseteq \hat{x} \Longleftrightarrow x \sqsubseteq \gamma_s(\hat{x}).$$

3.3 요약 의미함수

$\hat{Next} \in \dot{2}^{\hat{State}} \to \dot{2}^{\hat{State}}$는 $\hat{next} \in \hat{State} \to 2^{\hat{State}}$와 $\hat{\pi} \in \dot{2}^{\hat{State}} \to \dot{2}^{\dot{2}^{\hat{State}}}$로 정의된다.

$$\hat{Next} = \wp\sqcup \circ \hat{\pi} \circ \wp\cup \hat{next}$$

3.3.1 $\hat{\pi}$ 함수의 정의

$$\pi X = \wp(\lambda l.\{(m,l) \mid (m,l) \in X\})Label$$

$$\hat{\pi} X = \wp(\lambda l.\{(\hat{m},l) \mid (\hat{m},l) \in X\})Label$$

3.3.2 $\hat{next}$ 함수의 정의

편의상 $\hat{s} \in \hat{State}$를 $(\hat{m}, C_l)$로 표기한다. C_l에서 C는 $l \in Label$에 해당하는 명령어이다.

$$\frac{}{\hat{next}(\hat{m}, \texttt{skip}_l) = \{(\hat{m}, n(l))\}}$$

$$\frac{\hat{eval}(\hat{m}, E) = \hat{v}}{\hat{next}(\hat{m}, (x \texttt{ := } E)_l) = \{(\hat{m}\{x \mapsto \hat{v}\}, n(l))\}}$$

$$\frac{\hat{eval}(\hat{m}, E) = \hat{v}}{\hat{next}(\hat{m}, (\texttt{*}x \texttt{ := } E)_l) = \{(\hat{m}\{\hat{m}(x) \mapsto \hat{v}\}, n(l))\}} \ \hat{m}(x) \in Loc$$

$$\frac{\hat{eval}(\hat{m}, E) = \hat{v}}{\hat{next}(\hat{m}, (\texttt{*}x \texttt{ := } E)_l) = \{(\hat{m}\{y \hat{\mapsto} \hat{v}\}, n(l)) \mid y \in Loc\}} \ \hat{m}(x) = \top$$

$$\frac{}{\hat{next}(\hat{m}, (C_{l_1} \ ; \ C_{l_2})_l) = \{(\hat{m}, C_{l_1})\}}$$

$$\frac{\hat{eval}(\hat{m}, E) = \hat{v}}{\hat{next}(\hat{m}, (\texttt{if}\ E\ C_{l_1}\ C_{l_2})_l) = \{(\hat{m}, C_{l_1})\}}\ \hat{v} = \hat{true}$$

$$\frac{\hat{eval}(\hat{m}, E) = \hat{v}}{\hat{next}(\hat{m}, (\texttt{if}\ E\ C_{l_1}\ C_{l_2})_l) = \{(\hat{m}, C_{l_2})\}}\ \hat{v} = \hat{false}$$

$$\frac{\hat{eval}(\hat{m}, E) = \hat{v}}{\hat{next}(\hat{m}, (\texttt{if}\ E\ C_{l_1}\ C_{l_2})_l) = \{(\hat{m}, C_{l_1}), (\hat{m}, C_{l_2})\}}\ \hat{v} = \top$$

$$\frac{\hat{eval}(\hat{m}, E) = \hat{v}}{\hat{next}(\hat{m}, (\texttt{while}\ E\ C_{l'})_l) = \{(\hat{m}, C_{l'})\}}\ \hat{v} = \hat{true}$$

$$\frac{\hat{eval}(\hat{m}, E) = \hat{v}}{\hat{next}(\hat{m}, (\texttt{while}\ E\ C_{l'})_l) = \{(\hat{m}, n(l))\}}\ \hat{v} = \hat{false}$$

$$\frac{\hat{eval}(\hat{m}, E) = \hat{v}}{\hat{next}(\hat{m}, (\texttt{while}\ E\ C_{l'})_l) = \{(\hat{m}, n(l)), (\hat{m}, C_{l'})\}}\ \hat{v} = \top$$

3.3.3 $\hat{eval}$ 함수의 정의

$\hat{eval} \in \hat{Memory} \times E \to \hat{Val}$ 함수는 요약된 메모리와 식을 받아 그 값을 계산한다.

$$\frac{}{\hat{eval}(\hat{m}, n) = [n \bmod 11, n \bmod 11]}\ n \in \mathbb{Z}$$

$$\frac{}{\hat{eval}(\hat{m}, \texttt{true}) = \hat{true}}$$

$$\frac{}{\hat{eval}(\hat{m}, \texttt{false}) = \hat{false}}$$

$$\frac{}{\hat{eval}(\hat{m}, x) = \hat{m}(x)}$$

$$\frac{}{\hat{eval}(\hat{m}, \texttt{*}x) = \hat{m}(\hat{m}(x))}$$

$$\frac{}{\hat{eval}(\hat{m}, \texttt{\&}x) = x}$$

$$\frac{\hat{eval}(\hat{m}, E_1) = \hat{v}_1 \quad \hat{eval}(\hat{m}, E_2) = \hat{v}_2}{\hat{eval}(\hat{m}, E_1 \texttt{ + } E_2) = \hat{v}_1 \hat{+} \hat{v}_2}$$

$$\frac{\hat{eval}(\hat{m}, E) = \hat{v}}{\hat{eval}(\hat{m}, \texttt{-}\ E) = \hat{-}\hat{v}}$$

$$\frac{}{\hat{eval}(\hat{m}, E_1 \texttt{ < } E_2) = \top}$$

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

3.3.4 $\hat{+}$, $\hat{-}$ 함수

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

$\hat{+}$	$\bot$	(l_1, u_1)	$\top$
$\bot$	$\bot$	$\bot$	$\bot$
(l_2, u_2)	$\bot$	$\hat{add}(l_1, u_1, l_2, u_2)$	$\top$
$\top$	$\bot$	$\top$	$\top$

	$\bot$	(l, u)	$\top$
$\hat{-}$	$\bot$	$\hat{minus}(l, u)$	$\top$

$$\hat{add}(l_1, u_1, l_2, u_2) = \begin{cases} (l_1 + l_2, u_1 + u_2) & \text{if } l_1 + l_2 < 11, u_1 + u_2 < 11, \\ (l_1 + l_2 - 11, u_1 + u_2 - 11) & \text{if } l_1 + l_2 \geq 11, u_1 + u_2 \geq 11, \\ \top & \text{otherwise.} \end{cases}$$

$$\hat{minus}(l, u) = \begin{cases} (11 - u, 11 - l) & \text{if } l \neq 0, \\ \top & \text{otherwise.} \end{cases}$$

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.

- **$\hat{v_1}$ 또는 $\hat{v_2}$가 $\bot$일 때**

$$\begin{aligned} \left(\alpha_v \circ \dot{+} \circ (\gamma_v \times \gamma_v)\right)(\hat{v_1}, \hat{v_2}) &= \alpha_v\{\} \\ &= \bot \\ \hat{+}(\hat{v_1}, \hat{v_2}) &= \bot \end{aligned}$$

- **$\hat{v_1}$ 또는 $\hat{v_2}$가 $\top$일 때**

$$\begin{aligned} \hat{+}(\hat{v_1}, \hat{v_2}) &= \top \\ \left(\alpha_v \circ \dot{+} \circ (\gamma_v \times \gamma_v)\right)(\hat{v_1}, \hat{v_2}) &\sqsubseteq \top \end{aligned}$$

- **$\hat{v_1} = (l_1, u_1)$, $\hat{v_2} = (l_2, u_2)$일 때**

- $l_1 + l_2 < 11$**이고** $u_1 + u_2 < 11$**일 때**

  $\gamma_v(\hat{v_1}) = \{11q_1 + r_1 \mid q_1 \in \mathbb{Z} \wedge l_1 \leq r_1 \leq u_1\}$ 이고
  $\gamma_v(\hat{v_2}) = \{11q_2 + r_2 \mid q \in \mathbb{Z} \wedge l_2 \leq r_2 \leq u_2\}$ 이므로

$$\begin{aligned}
\left(\alpha_v \circ \dot{+} \circ (\gamma_v \times \gamma_v)\right)(\hat{v_1}, \hat{v_2}) &= \alpha_v\{11q + (r_1 + r_2) \mid q \in \mathbb{Z} \wedge l_1 + l_2 \leq r_1 + r_2 \leq u_1 + u_2\} \\
&= (l_1 + l_2, u_1 + u_2) \\
\hat{+}(\hat{v_1}, \hat{v_2}) &= (l_1 + l_2, u_1 + u_2)
\end{aligned}$$

- $l_1 + l_2 \geq 11$**이고** $u_1 + u_2 \geq 11$**일 때**

  $\gamma_v(\hat{v_1}) = \{11q_1 + r_1 \mid q_1 \in \mathbb{Z} \wedge l_1 \leq r_1 \leq u_1\}$ 이고
  $\gamma_v(\hat{v_2}) = \{11q_2 + r_2 \mid q \in \mathbb{Z} \wedge l_2 \leq r_2 \leq u_2\}$ 이므로

$$\begin{aligned}
\left(\alpha_v \circ \dot{+} \circ (\gamma_v \times \gamma_v)\right)(\hat{v_1}, \hat{v_2}) &= \alpha_v\{11(q+1) + (r_1 + r_2 - 11) \mid q \in \mathbb{Z}, \\
&\quad\ l_1 + l_2 \leq r_1 + r_2 \leq u_1 + u_2\} \\
&= (l_1 + l_2 - 11, u_1 + u_2 - 11) \\
\hat{+}(\hat{v_1}, \hat{v_2}) &= (l_1 + l_2 - 11, u_1 + u_2 - 11)
\end{aligned}$$

- $l_1 + l_2 < 11$**이고** $u_1 + u_2 \geq 11$**일 때**

$$\begin{aligned}
\hat{+}(\hat{v_1}, \hat{v_2}) &= \top \\
\left(\alpha_v \circ \dot{+} \circ (\gamma_v \times \gamma_v)\right)(\hat{v_1}, \hat{v_2}) &\sqsubseteq \top
\end{aligned}$$

□

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.

- $\hat{v}$**가** $\bot$**이거나** $\top$**일 때**

  증명이 간단하므로 생략한다.

- $\hat{v} = (l, u)$**이고** $l \neq 0$**일 때**

$$\begin{aligned}
\left(\alpha_v \circ \dot{-} \circ \gamma_v\right)(\hat{v}) &= \alpha_v\{-(11q + r) \mid q \in \mathbb{Z} \wedge l \leq r \leq u\} \\
&= \alpha_v\{-11(q+1) + (11 - r) \mid q \in \mathbb{Z} \wedge l \leq r \leq u\} \\
&= (11 - u, 11 - l) \\
\hat{-}(\hat{v}) &= (11 - u, 11 - l)
\end{aligned}$$

- $\hat{v} = (l, u)$**이고** $l = 0$**일 때**

$$\begin{aligned}
\hat{-}(\hat{v}) &= \top \\
\left(\alpha_v \circ \dot{+} \circ \gamma_v\right)(\hat{v}) &\sqsubseteq \top
\end{aligned}$$

□

3.3.5 $\cdot\{x \hat{\mapsto} \cdot\}$ 함수

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

Lemma 3. $\cdot\{x \hat{\mapsto} \cdot\}$*은* $\cdot\{x \dot{\mapsto} \cdot\}$*를 안전하게 요약한 것이다.*

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

Proof.

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

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

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

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

$$\begin{aligned}
\alpha_v(\{m\ l \mid m \in M\}) &\sqsubseteq \alpha_v(\gamma_v\ (\hat{m}\ l)) \quad (\text{if } l \neq x) \\
\alpha_v(\{m\ l \mid m \in M\}) &\sqsubseteq \alpha_v(\gamma_v\ \hat{v}) \quad (\text{if } l = x)
\end{aligned}$$

그러므로

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

□

3.3.6 $\hat{at}$ 함수

$$\hat{at} \in (\hat{Memory} \times Loc) \to \hat{Value}$$

Lemma 4. *$\hat{at}$은 at을 안전하게 요약한 것이다.*

$$\forall \hat{m} \in \hat{Memory}, x \in Loc : (\alpha_v \circ at \circ (\gamma_m \times id))\,(\hat{m}, x) \sqsubseteq \hat{at}(\hat{m}, x)$$

Proof.

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

□

3.4 안전성 증명

Lemma 5. $(\wp\alpha_s) \circ \pi \circ (\wp\cup\gamma_s) \sqsubseteq (\wp\sqcup) \circ \hat{\pi}$ *(요약 분할의 조건)*

Proof.

$$\begin{aligned}
\text{(lhs) } (\wp\alpha_s) \circ \pi \circ (\wp\cup\gamma_s) &= (\wp\alpha_s) \circ \pi \circ \left(\lambda X. \bigcup\{\gamma_s(\hat{m}, l) \mid (\hat{m}, l) \in X\}\right) \\
&= (\wp\alpha_s) \circ \pi \circ (\lambda X.\{(m, l) \mid (\hat{m}, l) \in X \wedge m \in \gamma_m(\hat{m})\}) \\
&= (\wp\alpha_s) \circ (\lambda X.\wp\,(\lambda x.\{(m, l) \mid (\hat{m}, l) \in X \wedge m \in \gamma_m(\hat{m}) \wedge x = l\})\,Label) \\
&= \lambda X.\wp\,(\lambda x.\alpha_s\{(m, l) \mid (\hat{m}, l) \in X \wedge m \in \gamma_m(\hat{m}) \wedge x = l\})\,Label \\
&= \lambda X.\wp\,(\lambda x.(\alpha_m\{m \mid (\hat{m}, x) \in X \wedge m \in \gamma_m(\hat{m})\}, x))\,Label \\
&= \lambda X.\wp\left(\lambda x.(\alpha_m \circ \bigcup \circ \wp\gamma_m\{\hat{m} \mid (\hat{m}, x) \in X\}, x)\right)\,Label
\end{aligned}$$

$$
\begin{aligned}
\text{(rhs) } (\wp\sqcup) \circ \hat{\pi} &= (\wp\sqcup) \circ (\lambda X.\wp\,(\lambda x.\{(\hat{m}, l) \mid (\hat{m}, l) \in X \wedge x = l\})\, Label) \\
&= \lambda X.\wp\left(\lambda x.\bigsqcup\{(\hat{m}, l) \mid (\hat{m}, l) \in X \wedge x = l\}\right) Label \\
&= \lambda X.\wp\left(\lambda x.\left(\bigsqcup\{\hat{m} \mid (\hat{m}, x) \in X\}, x\right)\right) Label
\end{aligned}
$$

이 때, $\alpha_m \circ \bigcup \circ \wp\gamma_m \sqsubseteq \bigsqcup$이므로
$\alpha_m \circ \bigcup \circ \wp\gamma_m\{m \mid (\hat{m}, x) \in X\} \sqsubseteq \bigsqcup\{\hat{m} \mid (\hat{m}, x) \in X\}$ 이다.

Lemma 6. *$eval(m, E) \in (\gamma_v \circ \hat{eval})\ (\alpha_m\ \{m\}, E)$ (eval 함수의 안전성)*

Proof. E에 대한 귀납법으로 증명한다. $\hat{m} = \alpha_m\{m\}$이라 하자.

- $E = n$**일 때**

$$
\begin{aligned}
eval(m, n) &= n \\
(\gamma_v \circ \hat{eval})(\hat{m}, n) &= \gamma_v(n \bmod 11, n \bmod 11) \\
&= \{x \mid x \in \mathbb{Z} \wedge x \bmod 11 = n \bmod 11\} \\
&\ni n
\end{aligned}
$$

- $E = \texttt{true}$**일 때**

$$
\begin{aligned}
eval(m, \texttt{true}) &= true \\
(\gamma_v \circ \hat{eval})(\hat{m}, true) &= \gamma_v\ \hat{true} \\
&= \{true\} \\
&\ni true
\end{aligned}
$$

- $E = \texttt{false}$**일 때**

$$
\begin{aligned}
eval(m, \texttt{false}) &= false \\
(\gamma_v \circ \hat{eval})(\hat{m}, false) &= \gamma_v\ \hat{false} \\
&= \{false\} \\
&\ni false
\end{aligned}
$$

- $E = x$일 때

$$\begin{aligned}
eval(m, x) &= m(x) \\
(\gamma_v \circ \hat{eval})(\hat{m}, x) &= \gamma_v\ \hat{m}(x) \\
&= (\gamma_v \circ \lambda l.\alpha_v\{m\ l\})x \\
&= \gamma_v \circ \alpha_v\{m(x)\} \\
&\sqsupseteq \{m(x)\}
\end{aligned}$$

- $E = *x$일 때

$$\text{let } x' = (m\ x) \in Loc$$

$$\begin{aligned}
eval(m, *x) &= m(m(x)) \\
&= m(x') \\
(\gamma_v \circ \hat{eval})(\hat{m}, *x) &= \gamma_v\ \hat{m}(\hat{m}(x)) \\
&= (\gamma_v \circ \hat{m} \circ \lambda l.\alpha_v\{m\ l\})x \\
&= \gamma_v \circ \hat{m} \circ \alpha_v\{m(x)\} \\
&= \gamma_v \circ \hat{m} \circ \alpha_v\{x'\} \\
&= \gamma_v \hat{m}(\hat{x'}) \\
&\sqsupseteq \{m(x')\}
\end{aligned}$$

- $E = \&x$일 때

$$\begin{aligned}
eval(m, \&x) &= x \\
(\gamma_v \circ \hat{eval})(\hat{m}, \&x) &= \gamma_v\ x \\
&= \{x\}
\end{aligned}$$

- $E = E_1 + E_2$일 때

$$\begin{aligned}
eval(m, E_1 + E_2) &= eval(m, E_1) + eval(m, E_2) \\
(\gamma_v \circ \hat{eval})(\hat{m}, E_1 + E_2) &= \gamma_v(\hat{eval}(\hat{m}, E_1) \hat{+} \hat{eval}(\hat{m}, E_2)) \\
&\sqsupseteq \gamma_v \circ \alpha_v\{v_1 + v_2 \mid v_1 \in \gamma_v \hat{eval}(\hat{m}, E_1) \wedge v_2 \in \gamma_v \hat{eval}(\hat{m}, E_2)\} \\
&\sqsupseteq \gamma_v \circ \alpha_v\{eval(m, E_1) + eval(m, E_2)\} \\
&\sqsupseteq \{eval(m, E_1) + eval(m, E_2)\}
\end{aligned}$$

- $E = \texttt{-}\,E'$일 때

$$\begin{aligned}
eval(m, \texttt{-}\,E') &= -eval(m, E') \\
(\gamma_v \circ \hat{eval})(\hat{m}, \texttt{-}\,E') &= \gamma_v(\hat{-}\hat{eval}(\hat{m}, E')) \\
&\sqsupseteq \gamma_v \circ \alpha_v\{-v \mid v \in \gamma_v \hat{eval}(\hat{m}, E')\} \\
&\sqsupseteq \gamma_v \circ \alpha_v\{eval(m, E')\} \\
&\sqsupseteq \{eval(m, E')\}
\end{aligned}$$

- $E = E_1 \texttt{<} E_2$일 때

$$\begin{aligned}
\hat{eval}(\hat{m}, E_1 \texttt{<} E_2) &= \top \\
&\sqsupseteq \{eval(m, E_1 \texttt{<} E_2)\}
\end{aligned}$$

□

Lemma 7. *next* $(m, C_l) \in ((\wp_{\cup}\gamma_s) \circ \hat{next} \circ \alpha_s)\{(m, C_l)\}$ *(요약 전이함수의 조건)*

$\alpha_m\{m\}$을 $\hat{m}$이라 하자.

- $C_l = \texttt{skip}_l$일 때

$$\begin{aligned}
next(m, \texttt{skip}_l) &= (m, n(l)) \\
((\wp_{\cup}\gamma_s) \circ \hat{next} \circ \alpha_s)\{(m, \texttt{skip}_l)\} &= (\wp_{\cup}\gamma_s)\{(\hat{m}, n(\hat{l}))\} \\
&= \gamma_s(\hat{m}, n(\hat{l})) \\
&= \{(a, n(l)) \mid a \in \gamma_m(\alpha_m\{m\})\}
\end{aligned}$$

보일 것은$m \in \gamma_m(\alpha_m\{m\})$이다.
α_m, γ_m이 갈로아 연결이므로$\{m\} \subseteq \gamma_m(\alpha_m\{m\})$임을 쉽게 알 수 있다.

- $C_l = (x \texttt{ := } E)_l$일 때

$$\text{let } v = eval(m, E), \hat{v} = \hat{eval}(\hat{m}, E)$$

$$\begin{aligned}
next(m, (x \texttt{ := } E)_l) &= (m\{x \mapsto v\}, n(l)) \\
((\wp_{\cup}\gamma_s) \circ \hat{next} \circ \alpha_s)\{(m, (x \texttt{ := } E)_l)\} &= (\wp_{\cup}\gamma_s)\{(\hat{m}\{x \hat{\mapsto} \hat{v}\}, n(l))\} \\
&= \gamma_s(\hat{m}\{x \hat{\mapsto} \hat{v}\}, n(l)) \\
&= \{(a, n(l)) \mid a \in \gamma_m(\hat{m}\{x \hat{\mapsto} \hat{v}\})\}
\end{aligned}$$

보일 것은 $m\{x \mapsto v\} \in \gamma_m \hat{m}\{x \hat{\mapsto} \hat{v}\}$이다.

$$\begin{array}{rcl}
\gamma_m \hat{m}\{x \hat{\mapsto} \hat{v}\} & \sqsupseteq & \gamma_m(\alpha_m((\gamma_m \hat{m})\{x \dot{\mapsto} \gamma_v \hat{v}\})) \\
& \sqsupseteq & (\gamma_m \hat{m})\{x \dot{\mapsto} \gamma_v \hat{v}\} \\
& = & \{m'\{x \mapsto v'\} \mid m' \in \gamma_m \hat{m} \wedge v' \in \gamma_v \hat{v}\} \\
& \supseteq & \{m\{x \mapsto v\}\} \\
& \ni & m\{x \mapsto v\}
\end{array}$$

- $C_l = (*x := E)_l$ **일 때**

$$\text{let } v = eval(m, E), \hat{v} = \hat{eval}(\hat{m}, E)$$

  - $\hat{m}(x) \in Loc$ **일 때**

$$\begin{array}{rcl}
next(m, (*x := E)_l) & = & (m\{m(x) \mapsto v\}, n(l)) \\
((\wp \cup \gamma_s) \circ \hat{next} \circ \alpha_s)\{(m, *x := E_l)\} & = & (\wp \cup \gamma_s)\{(\hat{m}\{\hat{m}(x) \hat{\mapsto} \hat{v}\}, n(l))\} \\
& = & \gamma_s(\hat{m}\{\hat{m}(x) \hat{\mapsto} \hat{v}\}, n(l)) \\
& = & (\gamma_m(\hat{m}\{\hat{m}(x) \hat{\mapsto} \hat{v}\}), n(l))
\end{array}$$

보일 것은 $m\{m(x) \mapsto v\} \in \gamma_m \hat{m}\{\hat{m}(x) \hat{\mapsto} \hat{v}\}$ 이다.

$$\begin{array}{rcl}
\gamma_m \hat{m}\{\hat{m}(x) \hat{\mapsto} \hat{v}\} & \sqsupseteq & \gamma_m(\alpha_m((\gamma_m \hat{m})\{\hat{m}(x) \dot{\mapsto} \gamma_v \hat{v}\})) \\
& \sqsupseteq & (\gamma_m \hat{m})\{\hat{m}(x) \dot{\mapsto} \gamma_v \hat{v}\} \\
& = & \{m'\{\hat{m}(x) \mapsto v\} \mid m' \in \gamma_m \hat{m} \wedge v' \in \gamma_v \hat{v}\} \\
& \ni & m\{\hat{m}(x) \mapsto v\}
\end{array}$$

여기서 다시 보일 것은 $\hat{m}(x) = m(x)$ 이다.

$$\begin{array}{rcl}
\hat{m}(x) & = & (\alpha_m \{m\})(x) \\
& = & (\lambda l.\alpha_v\{m(l)\})x \\
& = & \alpha_v\{m(x)\} \\
& = & m(x) \quad (\alpha_v\text{의 정의와 } \hat{m}(x) \in Loc)
\end{array}$$

- $\hat{m}(x) = \top$ **일 때**

$$
\begin{aligned}
next(m, (*x \texttt{ := } E)_l) &= (m\{m(x) \mapsto v\}, n(l)) \\
((\wp \cup \gamma_s) \circ \hat{next} \circ \alpha_s)\{(m, *x \texttt{ := } E_l)\} &= (\wp \cup \gamma_s)\{(\hat{m}\{y \hat{\mapsto} \hat{v}\}, n(l)) \mid y \in Loc\} \\
&= \bigcup\{\gamma_s(\hat{m}\{y \hat{\mapsto} \hat{v}\}, n(l)) \mid y \in Loc\} \\
&\supseteq \gamma_s(\hat{m}\{m(x) \hat{\mapsto} \hat{v}\}, n(l)) \\
&= (\gamma_m \hat{m}\{m(x) \hat{\mapsto} \hat{v}\}, n(l))
\end{aligned}
$$

보일 것은 $m\{m(x) \mapsto v\} \in \gamma_m \hat{m}\{m(x) \hat{\mapsto} \hat{v}\}$ 이다. 이것의 증명 과정은 $m\{m(x) \mapsto v\} \in \gamma_m \hat{m}\{\hat{m}(x) \hat{\mapsto} \hat{v}\}$의 증명과 같다.

- $C_l = (C_{l_1} \texttt{ ; } C_{l_2})_l$**일 때**

$$
\begin{aligned}
next(m, (C_{l_1} \texttt{ ; } C_{l_2})_l) &= (m, C_{l_1}) \\
((\wp \cup \gamma_s) \circ \hat{next} \circ \alpha_s)\{(m, (C_{l_1} \texttt{ ; } C_{l_2})_l)\} &= (\wp \cup \gamma_s)\{(\hat{m}, C_{l_1})\} \\
&= \gamma_s(\hat{m}, C_{l_1}) \\
&\ni (m, C_{l_1})
\end{aligned}
$$

- $C_l = (\texttt{if } E\ C_{l_1}\ C_{l_2})_l$**일 때**

$$\text{let } v = eval(m, E), \hat{v} = \hat{eval}(\hat{m}, E)$$

  - $v = true$**일 때**

$$next(m, (\texttt{if } E\ C_{l_1}\ C_{l_2})_l) = (m, C_{l_1})$$

$v \in \gamma_v\ \hat{v}$이므로 $\hat{v} = \top$ 또는 $\hat{v} = \hat{true}$이다.

    * $\hat{v} = \hat{true}$**일 때**

$$
\begin{aligned}
((\wp \cup \gamma_s) \circ \hat{next} \circ \alpha_s)\{(m, (\texttt{if } E\ C_{l_1}\ C_{l_2})_l)\} &= (\wp \cup \gamma_s)\{(\hat{m}, C_{l_1})\} \\
&= \gamma_s(\hat{m}, C_{l_1}) \\
&\ni (m, C_{l_1})
\end{aligned}
$$

* $\hat{v} = \top$일 때

$$\begin{aligned}((\wp_{\cup}\gamma_s) \circ \hat{next} \circ \alpha_s)\{(m, (\texttt{if}\ E\ C_{l_1}\ C_{l_2})_l)\} &= (\wp_{\cup}\gamma_s)\{(\hat{m}, C_{l_1}), (\hat{m}, C_{l_2})\} \\ &= \gamma_s(\hat{m}, C_{l_1}) \cup \gamma_s(\hat{m}, C_{l_2}) \\ &\supseteq \gamma_s(\hat{m}, C_{l_1}) \\ &\ni (m, C_{l_1})\end{aligned}$$

- $v = false$일 때

$$next(m, (\texttt{if}\ E\ C_{l_1}\ C_{l_2})_l) = (m, C_{l_2})$$

$v \in \gamma_v\ \hat{v}$이므로 $\hat{v} = \top$ 또는 $\hat{v} = \hat{false}$이다.

* $\hat{v} = \hat{false}$일 때

$$\begin{aligned}((\wp_{\cup}\gamma_s) \circ \hat{next} \circ \alpha_s)\{(m, (\texttt{if}\ E\ C_{l_1}\ C_{l_2})_l)\} &= (\wp_{\cup}\gamma_s)\{(\hat{m}, C_{l_2})\} \\ &= \gamma_s(\hat{m}, C_{l_2}) \\ &\ni (m, C_{l_2})\end{aligned}$$

* $\hat{v} = \top$일 때

$$\begin{aligned}((\wp_{\cup}\gamma_s) \circ \hat{next} \circ \alpha_s)\{(m, (\texttt{if}\ E\ C_{l_1}\ C_{l_2})_l)\} &= (\wp_{\cup}\gamma_s)\{(\hat{m}, C_{l_1}), (\hat{m}, C_{l_2})\} \\ &= \gamma_s(\hat{m}, C_{l_1}) \cup \gamma_s(\hat{m}, C_{l_2}) \\ &\supseteq \gamma_s(\hat{m}, C_{l_2}) \\ &\ni (m, C_{l_2})\end{aligned}$$

- $C_l = (\texttt{while}\ E\ C_{l'})_l$일 때

$$\text{let } v = eval(m, E), \hat{v} = \hat{eval}(\hat{m}, E)$$

- $v = true$일 때

$$next(m, (\texttt{while}\ E\ C_{l'})_l) = (m, C_{l'})$$

$v \in \gamma_v\ \hat{v}$이므로 $\hat{v} = \top$ 또는 $\hat{v} = \hat{true}$이다.

* $\hat{v} = \hat{true}$일 때

$$\begin{aligned}((\wp_{\cup}\gamma_s) \circ \hat{next} \circ \alpha_s)\{(m, (\texttt{while}\ E\ C_{l'})_l)\} &= (\wp_{\cup}\gamma_s)\{(\hat{m}, C_{l'})\} \\ &= \gamma_s(\hat{m}, C_{l'}) \\ &\ni (m, C_{l'})\end{aligned}$$

* $\hat{v} = \top$일 때

$$
\begin{array}{rcl}
((\wp_{\cup}\gamma_s) \circ \hat{next} \circ \alpha_s)\{(m, (\texttt{while}\ E\ C_{l'})_l)\} & = & (\wp_{\cup}\gamma_s)\{(\hat{m}, C_{l'}), (\hat{m}, n(l))\} \\
& = & \gamma_s(\hat{m}, C_{l'}) \cup \gamma_s(\hat{m}, n(l)) \\
& \supseteq & \gamma_s(\hat{m}, C_{l'}) \\
& \ni & (m, C_{l'})
\end{array}
$$

- $v = false$일 때

$$
next(m, (\texttt{while}\ E\ C_{l'})_l) \quad = \quad (m, n(l))
$$

$v \in \gamma_v\ \hat{v}$이므로 $\hat{v} = \top$ 또는 $\hat{v} = \hat{false}$이다.

* $\hat{v} = \hat{false}$일 때

$$
\begin{array}{rcl}
((\wp_{\cup}\gamma_s) \circ \hat{next} \circ \alpha_s)\{(m, (\texttt{while}\ E\ C_{l'})_l)\} & = & (\wp_{\cup}\gamma_s)\{(\hat{m}, n(l))\} \\
& = & \gamma_s(\hat{m}, n(l)) \\
& \ni & (m, n(l))
\end{array}
$$

* $\hat{v} = \top$일 때

$$
\begin{array}{rcl}
((\wp_{\cup}\gamma_s) \circ \hat{next} \circ \alpha_s)\{(m, (\texttt{while}\ E\ C_{l'})_l)\} & = & (\wp_{\cup}\gamma_s)\{(\hat{m}, C_{l'}), (\hat{m}, n(l))\} \\
& = & \gamma_s(\hat{m}, C_{l'}) \cup \gamma_s(\hat{m}, n(l)) \\
& \supseteq & \gamma_s(\hat{m}, n(l)) \\
& \ni & (m, n(l))
\end{array}
$$

$\square$