

SNU 4541.664A
HW5 디자인 모범답안

조성근, 윤용호

2011년 5월 9일

1 대상 언어

$$\begin{aligned} C &\rightarrow \text{skip} \\ &| x := E \\ &| C ; C \\ &| \text{if } E C C \\ &| \text{while } E C \\ E &\rightarrow n \quad (n \in \mathbb{Z}) \\ &| E + E \\ &| -E \\ &| x \end{aligned}$$

2 모듬의미

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

$$\begin{aligned} \mathcal{C} C &\in 2^{\text{Memory}} \rightarrow 2^{\text{Memory}} \\ \mathcal{V} E &\in 2^{\text{Memory}} \rightarrow 2^{\text{Value}} \\ \mathcal{B} E &\in 2^{\text{Memory}} \rightarrow 2^{\text{Memory}} \\ \text{Memory} &= \text{Loc} \xrightarrow{\text{fin}} \text{Value} \\ \text{Value} &= \mathbb{Z} \\ \text{Loc} &= \text{Var} \\ m \in \text{Memory} \quad M &\in 2^{\text{Memory}} \end{aligned}$$

$$\begin{aligned}
\mathcal{C} \text{ skip } M &= M \\
\mathcal{C} x := E M &= \{m\{x \mapsto v\} \mid m \in M, v \in \mathcal{V} E M\} \\
\mathcal{C} C_1 ; C_2 M &= \mathcal{C} C_2 (\mathcal{C} C_1 M) \\
\mathcal{C} \text{ if } E C_1 C_2 M &= \mathcal{C} C_1 (\mathcal{B} E M) \cup \mathcal{C} C_2 (\neg \mathcal{B} E M) \\
\mathcal{C} \text{ while } E C M &= \neg \mathcal{B} E (fix \lambda X. M \cup \mathcal{C} C (\mathcal{B} E X)) \\
\mathcal{V} n M &= \{n\} \\
\mathcal{V} E_1 + E_2 M &= \{z_1 + z_2 \mid z_i \in \mathcal{V} E_i M\} \\
\mathcal{V} - E M &= \{-z \mid z \in \mathcal{V} E M\} \\
\mathcal{V} x M &= \{m x \mid m \in M\} \\
\mathcal{B} E M &= \{m \mid \mathcal{V} E \{m\} = \{n\}, n \neq 0, m \in M\} \\
\neg \mathcal{B} E M &= \{m \mid \mathcal{V} E \{m\} = \{0\}, m \in M\}
\end{aligned}$$

3 요약

3.1 갈로아 연결

갈로아 연결 된 요약공간

$$2^{Memory} \xleftrightarrow[\alpha_1]{\gamma_1} \hat{Memory} \quad 2^{Value} \xleftrightarrow[\alpha_2]{\gamma_2} \hat{Value}$$

3.1.1 \hat{Value}

$$\hat{Value} = \{\perp, odd, even, \top\}$$

$Value$ 에서의 부분적인 순서(partial order)는 집합의 포함관계이다. \hat{Value} 에서의 부분적인 순서는 다음과 같다.

$$\begin{aligned}
&\perp \sqsubseteq odd \sqsubseteq \top \quad \perp \sqsubseteq even \sqsubseteq \top \\
\alpha_2 V &= \begin{cases} \perp & \text{if } V = \{\}, \\ odd & \text{if } \forall v \in V : v \text{는 홀수,} \\ even & \text{if } \forall v \in V : v \text{는 짝수,} \\ \top & \text{otherwise.} \end{cases}
\end{aligned}$$

$$\gamma_2 \hat{v} = \begin{cases} \{\} & \text{if } \hat{v} = \perp, \\ \{2n + 1 \mid n \in \mathbb{Z}\} & \text{if } \hat{v} = \text{odd}, \\ \{2n \mid n \in \mathbb{Z}\} & \text{if } \hat{v} = \text{even}, \\ \mathbb{Z} & \text{if } \hat{v} = \top. \end{cases}$$

α_2, γ_2 은 갈로아 연결이다. 즉,

$$\forall V \in 2^{Value}, \hat{v} \in \hat{Value} : \alpha_2(V) \sqsubseteq \hat{v} \iff V \sqsubseteq \gamma_2(\hat{v}).$$

3.1.2 $Mem\hat{ory}$

$$\begin{array}{ccc} 2^{Memory} & \xleftrightarrow[\alpha_1]{\gamma_1} & Mem\hat{ory} \\ 2^{Loc} \xrightarrow{fin} Value & \xleftrightarrow[\alpha_1]{\gamma_1} & Loc \xrightarrow{fin} \hat{Value} \end{array}$$

$$\alpha_1 = \lambda M. \lambda l. \alpha_2(\{m \mid m \in M\})$$

$$\gamma_1 = \lambda \hat{m}. \{m \mid \forall l : m \in \gamma_2(\hat{m} \ l)\}$$

α_1, γ_1 은 갈로아 연결이다. 즉,

$$\forall M \in 2^{Memory}, \hat{m} \in Mem\hat{ory} : \alpha_1(M) \sqsubseteq \hat{m} \iff M \sqsubseteq \gamma_1(\hat{m}).$$

3.2 요약 의미함수

$$\hat{C} \ C \in Mem\hat{ory} \rightarrow Mem\hat{ory}$$

$$\hat{V} \ E \in Mem\hat{ory} \rightarrow \hat{Value}$$

$$\hat{B} \ E \in Mem\hat{ory} \rightarrow Mem\hat{ory}$$

$$\begin{aligned}
\hat{C} \text{ skip } \hat{m} &= \hat{m} \\
\hat{C} x := E \hat{m} &= \hat{m}\{x \mapsto \hat{V} E \hat{m}\} \\
\hat{C} C_1 ; C_2 \hat{m} &= \hat{C} C_2 (\hat{C} C_1 \hat{m}) \\
\hat{C} \text{ if } E C_1 C_2 \hat{m} &= \hat{C} C_1 (\hat{B} E \hat{m}) \sqcup \hat{C} C_2 (\neg \hat{B} E \hat{m}) \\
\hat{C} \text{ while } E C \hat{m} &= \neg \hat{B} E (fix \lambda \hat{x}. \hat{m} \sqcup \hat{C} C (\hat{B} E \hat{x})) \\
\hat{V} n \hat{m} &= \alpha_2\{n\} \\
\hat{V} E_1 + E_2 \hat{m} &= (\hat{V} E_1 \hat{m}) \hat{\dagger} (\hat{V} E_2 \hat{m}) \\
\hat{V} - E \hat{m} &= \hat{\smile} (\hat{V} E \hat{m}) \\
\hat{V} x \hat{m} &= \hat{m} \hat{a}t x \\
\hat{B} E \hat{m} &= \begin{cases} \perp_{Memory} & \text{if } E = 0, \\ \hat{m} & \text{otherwise.} \end{cases} \\
\neg \hat{B} E \hat{m} &= \begin{cases} \perp_{Memory} & \text{if } E = n \neq 0, \\ \hat{m}\{x \mapsto \text{even}\} & \text{if } E = x, \\ \hat{m} & \text{otherwise.} \end{cases}
\end{aligned}$$

여기서 $\hat{\dagger}$, $\hat{\smile}$, $\{x \mapsto \cdot\}$, $\hat{a}t$ 는 해당 연산들을 안전하게 요약한 것들임을 아래에서 보인다.

3.2.1 $\hat{\dagger}$, $\hat{\smile}$ 함수

$$\begin{aligned}
\hat{\dagger} &\in Val \times Val \rightarrow Val \\
\hat{\smile} &\in Val \rightarrow Val
\end{aligned}$$

$\hat{\dagger}$	\perp	<i>odd</i>	<i>even</i>	\top
\perp	\perp	\perp	\perp	\perp
<i>odd</i>	\perp	<i>even</i>	<i>odd</i>	\top
<i>even</i>	\perp	<i>odd</i>	<i>even</i>	\top
\top	\perp	\top	\top	\top

	\perp	<i>odd</i>	<i>even</i>	\top
$\hat{\smile}$	\perp	<i>odd</i>	<i>even</i>	\top

Lemma 1. $\hat{\dagger}$ 은 \dagger 을 안전하게 요약한 것이다.

$$\forall v_1, v_2 \in Value : (\alpha_2 \circ \dagger \circ (\gamma_2 \times \gamma_2))(v_1, v_2) \sqsubseteq \hat{\dagger}(v_1, v_2)$$

Proof.

- v_1 또는 v_2 가 \perp 일 때

$$\begin{aligned} (\alpha_2 \circ \dot{\vdash} \circ (\gamma_2 \times \gamma_2))(v_1, v_2) &= \alpha_2\{\} \\ &= \perp \\ \hat{\vdash}(v_1, v_2) &= \perp \end{aligned}$$

- v_1 또는 v_2 가 \top 일 때

$$\begin{aligned} \hat{\vdash}(v_1, v_2) &= \top \\ (\alpha_2 \circ \dot{\vdash} \circ (\gamma_2 \times \gamma_2))(v_1, v_2) &\sqsubseteq \top \end{aligned}$$

- v_1 또는 v_2 가 모두 *odd*이거나 모두 *even*일 때

$$\begin{aligned} (\alpha_2 \circ \dot{\vdash} \circ (\gamma_2 \times \gamma_2))(v_1, v_2) &= \alpha_2\{2n \mid n \in \mathbb{Z}\} \\ &= \text{even} \\ \hat{\vdash}(v_1, v_2) &= \text{even} \end{aligned}$$

- v_1 와 v_2 중 하나는 *odd*이고 다른 하나는 *even*일 때

$$\begin{aligned} (\alpha_2 \circ \dot{\vdash} \circ (\gamma_2 \times \gamma_2))(v_1, v_2) &= \alpha_2\{2n + 1 \mid n \in \mathbb{Z}\} \\ &= \text{odd} \\ \hat{\vdash}(v_1, v_2) &= \text{odd} \end{aligned}$$

□

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

증명이 간단하므로 생략한다.

3.2.2 $\cdot\{x \mapsto \cdot\}$ 함수

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

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

$$\forall \hat{m} \in \hat{Memory}, \hat{v} \in \hat{Value} : (\alpha_1 \circ \dot{\cdot}\{x \mapsto \cdot\} \circ (\gamma_1 \times \gamma_2))(\hat{m}, \hat{v}) \sqsubseteq \cdot\{x \mapsto \cdot\}(\hat{m}, \hat{v})$$

Proof.

$$\begin{aligned}
\cdot\{x \mapsto \cdot\}(\hat{m}, \hat{v}) &= \hat{m}\{x \mapsto \hat{v}\} \\
(\alpha_1 \circ \cdot\{x \mapsto \cdot\} \circ (\gamma_1 \times \gamma_2))(\hat{m}, \hat{v}) &= (\alpha_1 \circ \cdot\{x \mapsto \cdot\})(\gamma_1 \hat{m}, \gamma_2 \hat{v}) \\
&= \alpha_1((\gamma_1 \hat{m})\{x \mapsto \gamma_2 \hat{v}\}) \\
&= \alpha_1(\{m \mid \forall l : m l \in \gamma_2(\hat{m} l)\}\{x \mapsto \gamma_2 \hat{v}\})
\end{aligned}$$

여기서 $\{m \mid \forall l : m l \in \gamma_2(\hat{m} l)\}\{x \mapsto \gamma_2 \hat{v}\}$ 을 M 이라고 하면, $m \in M$ 인 모든 m 이 다음을 만족한다.

$$\begin{aligned}
m l &\in \gamma_2(\hat{m} l) \quad (\text{if } l \neq x) \\
m l &\in \gamma_2 \hat{v} \quad (\text{if } l = x)
\end{aligned}$$

$(\alpha_1 M) l$ 은 α_1 의 정의에 따라서 $\alpha_2(\{m l \mid m \in M\})$ 이고 다음을 만족한다.

$$\begin{aligned}
\alpha_2(\{m l \mid m \in M\}) &\sqsubseteq \alpha_2(\gamma_2(\hat{m} l)) \quad (\text{if } l \neq x) \\
\alpha_2(\{m l \mid m \in M\}) &\sqsubseteq \alpha_2(\gamma_2 \hat{v}) \quad (\text{if } l = x)
\end{aligned}$$

그러므로

$$\begin{aligned}
\alpha_1 M &\sqsubseteq \alpha_2 \circ \gamma_2 \circ (\hat{m}\{x \mapsto \hat{v}\}) \\
&\sqsubseteq \hat{m}\{x \mapsto \hat{v}\}. \quad (\alpha_2 \circ \gamma_2 \sqsubseteq id \text{이므로})
\end{aligned}$$

□

3.2.3 \hat{at} 함수

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

Lemma 4. \hat{at} 은 at 을 안전하게 요약한 것이다.

$$\forall \hat{m} \in Memory, x \in Loc : (\alpha_2 \circ at \circ (\gamma_1 \times id))(\hat{m}, x) \sqsubseteq \hat{at}(\hat{m}, x)$$

Proof.

$$\begin{aligned}
\hat{at}(\hat{m}, x) &= \hat{m} x \\
(\alpha_2 \circ at \circ (\gamma_1 \times id))(\hat{m}, x) &= (\alpha_2 \circ at)(\gamma_1 \hat{m}, x) \\
&= \alpha_2\{m x \mid m \in \gamma_1 \hat{m}\} \\
&= \alpha_2\{m x \mid \forall l : m l \in \gamma_2(\hat{m} l)\} \quad (\gamma_1 \text{의 정의에 의해서}) \\
&\sqsubseteq \alpha_2(\gamma_2(\hat{m} x)) \\
&\sqsubseteq \hat{m} x \quad (\alpha_2 \circ \gamma_2 \sqsubseteq id \text{이므로})
\end{aligned}$$

□

3.3 안전성 증명

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

Proof. E 에 대한 귀납법으로 증명한다.

- $E = n$ 일 때

$$\begin{aligned}\hat{\mathcal{V}} n \hat{m} &= \alpha_2\{n\} \\ (\alpha(\mathcal{V} n))\hat{m} &= (\alpha_2 \circ (\mathcal{V} n) \circ \gamma_1)\hat{m} \\ &= \alpha_2\{n\}\end{aligned}$$

- $E = E_1 + E_2$ 일 때

$$\begin{aligned}\hat{\mathcal{V}} E_1 + E_2 &= \hat{\dagger} \circ (\hat{\mathcal{V}} E_1 \times \hat{\mathcal{V}} E_2) \\ \alpha(\mathcal{V} E_1 + E_2) &= \alpha_2 \circ \mathcal{V} E_1 + E_2 \circ \gamma_1 \\ &= \alpha_2 \circ \dot{\dagger} \circ (\mathcal{V} E_1 \times \mathcal{V} E_2) \circ \gamma_1 \\ &= \alpha_2 \circ \dot{\dagger} \circ ((\mathcal{V} E_1 \circ \gamma_1) \times (\mathcal{V} E_2 \circ \gamma_1)) \\ &\sqsubseteq \alpha_2 \circ \dot{\dagger} \circ ((\gamma_2 \circ \hat{\mathcal{V}} E_1) \times (\gamma_2 \circ \hat{\mathcal{V}} E_2)) \quad (\text{귀납가정에 의해서}) \\ &= \alpha_2 \circ \dot{\dagger} \circ (\gamma_2 \times \gamma_2) \circ (\hat{\mathcal{V}} E_1 \times \hat{\mathcal{V}} E_2) \\ &\sqsubseteq \hat{\dagger} \circ (\hat{\mathcal{V}} E_1 \times \hat{\mathcal{V}} E_2) \quad (\hat{\dagger} \text{는 안전한 요약이므로})\end{aligned}$$

- $E = - E'$ 일 때

$$\begin{aligned}\hat{\mathcal{V}} - E' &= \hat{\smile} \circ (\hat{\mathcal{V}} E') \\ \alpha(\mathcal{V} - E') &= \alpha_2 \circ (\mathcal{V} - E') \circ \gamma_1 \\ &= \alpha_2 \circ \dot{\smile} \circ (\mathcal{V} E') \circ \gamma_1 \\ &\sqsubseteq \alpha_2 \circ \dot{\smile} \circ \gamma_2 \circ (\hat{\mathcal{V}} E') \quad (\text{귀납가정에 의해서}) \\ &\sqsubseteq \hat{\smile} \circ (\hat{\mathcal{V}} E') \quad (\hat{\smile} \text{는 안전한 요약이므로})\end{aligned}$$

- $E = x$ 일 때

$$\begin{aligned}\hat{\mathcal{V}} x \hat{m} &= \hat{at}(\hat{m}, x) \\ (\alpha(\mathcal{V} x))\hat{m} &= (\alpha_2 \circ (\mathcal{V} x) \circ \gamma_1)\hat{m} \\ &= (\alpha_2 \circ at \circ (\gamma_1 \times id))(\hat{m}, x) \\ &\sqsubseteq \hat{at}(\hat{m}, x) \quad (\hat{at} \text{는 안전한 요약이므로})\end{aligned}$$

□

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

Proof. E 에 대한 귀납법으로 증명한다.

- $E = 0$ 일 때

$$\begin{aligned}\hat{\mathcal{B}} 0 \hat{m} &= \perp_{Memory} \\ (\alpha(\mathcal{B} 0)) \hat{m} &= \alpha_1(\{\}) \\ &= \perp_{Memory}\end{aligned}$$

- 그 밖의 경우

$$\begin{aligned}\hat{\mathcal{B}} E \hat{m} &= \hat{m} \\ (\alpha(\mathcal{B} E)) \hat{m} &= (\alpha_1 \circ (\mathcal{B} E) \circ \gamma_1) \hat{m} \\ &= \alpha_1(\{m \mid \mathcal{V} E \{m\} = \{n\}, n \neq 0, m \in \gamma_1 \hat{m}\}) \\ &\sqsubseteq \alpha_1(\gamma_1 \hat{m}) \\ &\sqsubseteq \hat{m} \qquad (\alpha_1 \circ \gamma_1 \sqsubseteq id \text{이므로})\end{aligned}$$

□

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

Proof. E 에 대한 귀납법으로 증명한다.

- $E = n \neq 0$ 일 때

$$\begin{aligned}\neg \hat{\mathcal{B}} n \hat{m} &= \perp_{Memory} \\ (\alpha(\neg \mathcal{B} n)) \hat{m} &= \alpha_1(\{\}) \\ &= \perp_{Memory}\end{aligned}$$

- $E = x$ 일 때

$$\begin{aligned}\neg \hat{\mathcal{B}} x \hat{m} &= \hat{m}\{x \mapsto even\} \\ (\alpha(\neg \mathcal{B} x)) \hat{m} &= \alpha_1(\{m \mid \mathcal{V} x \{m\} = \{0\}, m \in \gamma_1 \hat{m}\}) \\ &\sqsubseteq \alpha_1((\gamma_1 \hat{m})\{x \mapsto \{0\}\}) \\ &\sqsubseteq (\alpha_1 \circ \cdot\{x \mapsto \cdot\} \circ (\gamma_1 \times \gamma_2)) (\hat{m}, \alpha_2(\{0\})) \quad (\gamma_2 \circ \alpha_2 \sqsubseteq id \text{이므로}) \\ &\sqsubseteq \cdot\{x \mapsto \cdot\} (\hat{m}, \alpha_2(\{0\})) \quad (\cdot\{x \mapsto \cdot\} \text{은 안전한 요약이므로}) \\ &= \hat{m}\{x \mapsto even\}\end{aligned}$$

- 그 밖의 경우

$$\begin{aligned}\neg \hat{\mathcal{B}} E \hat{m} &= \hat{m} \\ (\alpha(\neg \mathcal{B} E)) \hat{m} &= \alpha_1(\{m \mid \mathcal{V} E \{m\} = \{0\}, m \in \gamma_1 \hat{m}\}) \\ &\sqsubseteq \alpha_1(\gamma_1 \hat{m}) \\ &\sqsubseteq \hat{m} \qquad (\alpha_1 \circ \gamma_1 \sqsubseteq id \text{이므로})\end{aligned}$$

□

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

Proof. C 에 대한 귀납법으로 증명한다.

- $C = \text{skip}$ 일 때

$$\begin{aligned} \hat{\mathcal{C}} \text{ skip} &= \hat{id} \\ \alpha(\mathcal{C} \text{ skip}) &= \alpha_1 \circ (\mathcal{C} \text{ skip}) \circ \gamma_1 \\ &= \alpha_1 \circ id \circ \gamma_1 \\ &\sqsubseteq \hat{id} \quad (\alpha_1 \circ \gamma_1 \sqsubseteq id \text{이므로}) \end{aligned}$$

- $C = x := E$ 일 때

$$\begin{aligned} \hat{\mathcal{C}} x := E &= \cdot\{x \mapsto \cdot\} \circ (\hat{id} \times \hat{\mathcal{V}} E) \\ \alpha(\mathcal{C} x := E) &= \alpha_1 \circ (\mathcal{C} x := E) \circ \gamma_1 \\ &= \alpha_1 \circ \cdot\{x \mapsto \cdot\} \circ (id \times \mathcal{V} E) \circ \gamma_1 \\ &\sqsubseteq \alpha_1 \circ \cdot\{x \mapsto \cdot\} \circ (\gamma_1 \times \gamma_2) \circ (\hat{id} \times \hat{\mathcal{V}} E) \quad (\text{Lemma 5에 의해서}) \\ &\sqsubseteq \cdot\{x \mapsto \cdot\} \circ (\hat{id} \times \hat{\mathcal{V}} E) \quad (\cdot\{x \mapsto \cdot\} \text{은 안전한 요약이므로}) \end{aligned}$$

- $C = C_1 ; C_2$ 일 때

$$\begin{aligned} \hat{\mathcal{C}} C_1 ; C_2 &= (\hat{\mathcal{C}} C_2) \circ (\hat{\mathcal{C}} C_1) \\ \alpha(\mathcal{C} C_1 ; C_2) &= \alpha_1 \circ (\mathcal{C} C_1 ; C_2) \circ \gamma_1 \\ &= \alpha_1 \circ (\mathcal{C} C_2) \circ (\mathcal{C} C_1) \circ \gamma_1 \\ &\sqsubseteq \alpha_1 \circ (\mathcal{C} C_2) \circ \gamma_1 \circ (\hat{\mathcal{C}} C_1) \quad (\text{귀납가정에 의해서}) \\ &\sqsubseteq (\hat{\mathcal{C}} C_2) \circ (\hat{\mathcal{C}} C_1) \quad (\text{귀납가정에 의해서}) \end{aligned}$$

- $C = \text{if } E C_1 C_2$ 일 때

$$\begin{aligned} \hat{\mathcal{C}} \text{if } E C_1 C_2 &= \sqcup \circ \left((\hat{\mathcal{C}} C_1 \circ \alpha_1 \circ \mathcal{B} E \circ \gamma_1) \times (\hat{\mathcal{C}} C_2 \circ \alpha_1 \circ \neg \mathcal{B} E \circ \gamma_1) \right) \\ \alpha(\mathcal{C} \text{if } E C_1 C_2) &= \alpha_1 \circ \mathcal{C} \text{if } E C_1 C_2 \circ \gamma_1 \\ &= \alpha_1 \circ \sqcup \circ ((\mathcal{C} C_1 \circ \mathcal{B} E \circ \gamma_1) \times (\mathcal{C} C_2 \circ \neg \mathcal{B} E \circ \gamma_1)) \\ &= \sqcup \circ (\alpha_1 \times \alpha_1) \circ ((\mathcal{C} C_1 \circ \mathcal{B} E \circ \gamma_1) \times (\mathcal{C} C_2 \circ \neg \mathcal{B} E \circ \gamma_1)) \\ &= \sqcup \circ ((\alpha_1 \circ \mathcal{C} C_1 \circ \mathcal{B} E \circ \gamma_1) \times (\alpha_1 \circ \mathcal{C} C_2 \circ \neg \mathcal{B} E \circ \gamma_1)) \\ &\sqsubseteq \sqcup \circ ((\alpha_1 \circ \mathcal{C} C_1 \circ \gamma_1 \circ \alpha_1 \circ \mathcal{B} E \circ \gamma_1) \times (\alpha_1 \circ \mathcal{C} C_2 \circ \gamma_1 \circ \alpha_1 \circ \neg \mathcal{B} E \circ \gamma_1)) \\ &\quad (\gamma_1 \circ \alpha_1 \sqsupseteq id \text{이므로}) \\ &\sqsubseteq \sqcup \circ \left((\hat{\mathcal{C}} C_1 \circ \alpha_1 \circ \mathcal{B} E \circ \gamma_1) \times (\hat{\mathcal{C}} C_2 \circ \alpha_1 \circ \neg \mathcal{B} E \circ \gamma_1) \right) \\ &\quad (\text{귀납가정에 의해서}) \end{aligned}$$

- $C = \text{while } E \ C'$ 일 때

$$\begin{aligned}
\hat{C} \text{ while } E \ C' \ \hat{m} &= \neg \hat{\mathcal{B}} \ E \ (\text{fix}(\hat{F} \stackrel{\text{let}}{=} \lambda \hat{x}. \hat{m} \sqcup \hat{C} \ C' \ (\hat{\mathcal{B}} \ E \ \hat{x}))) \\
(\alpha(\mathcal{C} \text{ while } E \ C')) \ \hat{m} &= (\alpha_1 \circ \mathcal{C} \ \text{while } E \ C' \circ \gamma_1) \ \hat{m} \\
&= (\alpha_1 \circ \neg \mathcal{B} \ E) \ (\text{fix}(F \stackrel{\text{let}}{=} \lambda X. \gamma_1 \ \hat{m} \cup \mathcal{C} \ C' \ (\mathcal{B} \ E \ X)))
\end{aligned}$$

여기서 $\alpha_1 \circ F \sqsubseteq \hat{F} \circ \alpha_1$ 을 다음과 같이 보일 수 있다.

$$\begin{aligned}
\alpha_1 \circ F &= \alpha_1 \circ (\lambda X. \gamma_1 \ \hat{m} \cup \mathcal{C} \ C' \ (\mathcal{B} \ E \ X)) \\
&= \lambda X. \alpha_1(\gamma_1 \ \hat{m}) \sqcup \alpha_1(\mathcal{C} \ C' \ (\mathcal{B} \ E \ X)) \\
\hat{F} \circ \alpha_1 &= (\lambda \hat{x}. \hat{m} \sqcup \hat{C} \ C' \ (\hat{\mathcal{B}} \ E \ \hat{x})) \circ \alpha_1 \\
&= \lambda X. \hat{m} \sqcup \hat{C} \ C' \ (\hat{\mathcal{B}} \ E \ (\alpha_1 X))
\end{aligned}$$

$$\begin{aligned}
\alpha_1(\gamma_1 \ \hat{m}) &\sqsubseteq \hat{m} && (\alpha_1 \circ \gamma_1 \sqsubseteq id \text{이므로}) \\
\alpha_1 \circ (\mathcal{C} \ C') \circ (\mathcal{B} \ E) &\sqsubseteq \alpha_1 \circ (\mathcal{C} \ C') \circ \gamma_1 \circ \alpha_1 \circ (\mathcal{B} \ E) && (\gamma_1 \circ \alpha_1 \sqsupseteq id \text{이므로}) \\
&\sqsubseteq (\hat{C} \ C') \circ \alpha_1 \circ (\mathcal{B} \ E) && (\text{귀납가정에 의해서}) \\
&\sqsubseteq (\hat{C} \ C') \circ \alpha_1 \circ (\mathcal{B} \ E) \circ \gamma_1 \circ \alpha_1 && (\gamma_1 \circ \alpha_1 \sqsupseteq id \text{이므로}) \\
&\sqsubseteq (\hat{C} \ C') \circ (\hat{\mathcal{B}} \ E) \circ \alpha_1 && (\text{Lemma 6에 의해서})
\end{aligned}$$

그러므로 $\alpha_1 \circ F \sqsubseteq \hat{F} \circ \alpha_1$ 이다.

“Fixpoint Transfer Theorem”에 의해 $\alpha_1(\text{fix} F) \sqsubseteq \text{fix} \hat{F}$ 이고, $\hat{\mathcal{B}} \ E$ 와 $\neg \hat{\mathcal{B}} \ E$ 가 안전하므로 위의 두 개 사이의 올바른 관계

$$(\alpha_1 \circ \neg \mathcal{B} \ E) \text{fix} F \sqsubseteq \neg \hat{\mathcal{B}} \ E \ \text{fix} \hat{F}$$

을 확인할 수 있다.

□