SNU 4541.664A Program Analysis
Note 10-1

Prof. Kwangkeun Yi

요약해석 디자인과 구현의 예

- 변수가 있는 정수식 프로그램의 요약해석
- 명령형 언어 프로그램의 요약해석

변수가 있는 정수식 프로그램의 요약해석

$$
\begin{array}{rcll}
E & \to & n & (n \in \mathbb{Z}) \\
& | & x & \text{변수} \\
& | & E \texttt{ + } E & \\
& | & \texttt{-}\, E & \\
& | & \texttt{let}\ x\ E_1\ E_2 & \text{지역 변수} \\
& | & \texttt{if}\ E_1\ E_2\ E_3 &
\end{array}
$$

요약들

- 시작: 모듬의미(*collecting semantics*)

$$\begin{array}{rcl} \mathcal{V} & \in & Exp \to 2^{Env} \to 2^{\mathbb{Z}} \\ Env & = & Var \xrightarrow{\text{fin}} \mathbb{Z} \end{array}$$

요약들

- 시작: 모듬의미(*collecting semantics*)

$$
\begin{array}{rcl}
\mathcal{V} & \in & Exp \to 2^{Env} \to 2^{\mathbb{Z}} \\
Env & = & Var \xrightarrow{\text{fin}} \mathbb{Z}
\end{array}
$$

- 요약 일반:

$$
2^{Env} \to 2^{\mathbb{Z}} \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} \hat{Env} \to \hat{\mathbb{Z}}, \qquad 2^{Env} \underset{\alpha_1}{\overset{\gamma_1}{\leftrightarrows}} \hat{Env}, \qquad 2^{\mathbb{Z}} \underset{\alpha_2}{\overset{\gamma_2}{\leftrightarrows}} \hat{\mathbb{Z}}
$$

이고, 요약 의미 $\hat{\mathcal{V}}\, E$가

$$
\hat{\mathcal{V}}\, E \quad \sqsupseteq \quad \alpha(\mathcal{V}\, E) = \alpha_2 \circ \mathcal{V}\, E \circ \gamma_1
$$

이 되도록.

요약들

- 시작: 모듬의미(*collecting semantics*)

$$\begin{array}{rcl} \mathcal{V} & \in & Exp \rightarrow 2^{Env} \rightarrow 2^{\mathbb{Z}} \\ Env & = & Var \xrightarrow{\text{fin}} \mathbb{Z} \end{array}$$

- 요약 일반:

$$2^{Env} \rightarrow 2^{\mathbb{Z}} \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} \hat{Env} \rightarrow \hat{\mathbb{Z}}, \qquad 2^{Env} \underset{\alpha_1}{\overset{\gamma_1}{\leftrightarrows}} \hat{Env}, \qquad 2^{\mathbb{Z}} \underset{\alpha_2}{\overset{\gamma_2}{\leftrightarrows}} \hat{\mathbb{Z}}$$

  이고, 요약 의미 $\hat{\mathcal{V}}\, E$가

$$\hat{\mathcal{V}}\, E \quad \sqsupseteq \quad \alpha(\mathcal{V}\, E) = \alpha_2 \circ \mathcal{V}\, E \circ \gamma_1$$

  이 되도록.
- 요약 예

요약들

- 시작: 모듬의미(*collecting semantics*)

$$\begin{array}{rcl}\mathcal{V} & \in & Exp \rightarrow 2^{Env} \rightarrow 2^{\mathbb{Z}} \\ Env & = & Var \xrightarrow{\text{fin}} \mathbb{Z}\end{array}$$

- 요약 일반:

$$2^{Env} \rightarrow 2^{\mathbb{Z}} \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} \hat{Env} \rightarrow \hat{\mathbb{Z}}, \qquad 2^{Env} \underset{\alpha_1}{\overset{\gamma_1}{\leftrightarrows}} \hat{Env}, \qquad 2^{\mathbb{Z}} \underset{\alpha_2}{\overset{\gamma_2}{\leftrightarrows}} \hat{\mathbb{Z}}$$

  이고, 요약 의미 $\hat{\mathcal{V}}\,E$가

$$\hat{\mathcal{V}}\,E \quad \sqsupseteq \quad \alpha(\mathcal{V}\,E) = \alpha_2 \circ \mathcal{V}\,E \circ \gamma_1$$

  이 되도록.
- 요약 예
  - 환경에서 변수간의 관계를 잊어버리기

$$\begin{array}{rcl}\hat{Env} & = & Var \xrightarrow{\text{fin}} 2^{\mathbb{Z}} \\ \hat{\mathbb{Z}} & = & 2^{\mathbb{Z}}\end{array} \qquad \begin{array}{rcl}\alpha_1 & = & \lambda\Sigma.\{x \mapsto \bigcup_{\sigma\in\Sigma}(\sigma x) \mid x \in Var\} \\ \alpha_2 & = & id\end{array}$$

요약들

- 시작: 모듬의미(*collecting semantics*)

$$\begin{array}{rcl} \mathcal{V} & \in & Exp \to 2^{Env} \to 2^{\mathbb{Z}} \\ Env & = & Var \xrightarrow{\text{fin}} \mathbb{Z} \end{array}$$

- 요약 일반:

$$2^{Env} \to 2^{\mathbb{Z}} \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} \hat{Env} \to \hat{\mathbb{Z}}, \qquad 2^{Env} \underset{\alpha_1}{\overset{\gamma_1}{\leftrightarrows}} \hat{Env}, \qquad 2^{\mathbb{Z}} \underset{\alpha_2}{\overset{\gamma_2}{\leftrightarrows}} \hat{\mathbb{Z}}$$

  이고, 요약 의미 $\hat{\mathcal{V}}\,E$가

$$\hat{\mathcal{V}}\,E \quad \sqsupseteq \quad \alpha(\mathcal{V}\,E) = \alpha_2 \circ \mathcal{V}\,E \circ \gamma_1$$

  이 되도록.
- 요약 예
  - 환경에서 변수간의 관계를 잊어버리기

$$\begin{array}{rcl} \hat{Env} & = & Var \xrightarrow{\text{fin}} 2^{\mathbb{Z}} \\ \hat{\mathbb{Z}} & = & 2^{\mathbb{Z}} \end{array} \qquad \begin{array}{rcl} \alpha_1 & = & \lambda\Sigma.\{x \mapsto \bigcup_{\sigma\in\Sigma}(\sigma x) \mid x \in Var\} \\ \alpha_2 & = & id \end{array}$$

  - 그리곤, 변수가 가지는 정수들을 요약하기 ($\alpha_2 \neq id$)

$$\hat{Env} \quad = \quad Var \xrightarrow{\text{fin}} \hat{\mathbb{Z}} \qquad \alpha_1 \quad = \quad \lambda\Sigma.\{x \mapsto \alpha_2(\bigcup_{\sigma\in\Sigma}(\sigma x)) \mid x \in Var\}$$

모듬 의미(collecting semantics)

모듬 의미함수 $\mathcal{V}$는 아래와 같은 공간에서

$$
\begin{array}{rcl}
\mathcal{V} & \in & Exp \rightarrow 2^{Env} \rightarrow 2^{\mathbb{Z}} \\
\Sigma & \in & 2^{Env} \\
\sigma & \in & Env = Var \xrightarrow{\text{fin}} \mathbb{Z}
\end{array}
$$

조립식으로 정의된다:

$$
\begin{array}{rcl}
\mathcal{V}\, n\, \Sigma & = & \{n\} \\
\mathcal{V}\, x\, \Sigma & = & \{\sigma\, x \mid \sigma \in \Sigma\} \\
\mathcal{V}\, E_1 \texttt{+} E_2\, \Sigma & = & \{z_1 + z_2 \mid z_i \in \mathcal{V}\, E_i\, \Sigma\} \\
\mathcal{V}\, \texttt{-}\, E\, \Sigma & = & \{-z \mid z \in \mathcal{V}\, E\, \Sigma\} \\
\mathcal{V}\, \texttt{let}\, x\, E_1\, E_2\, \Sigma & = & \mathcal{V}\, E_2\, \{\sigma\{x \mapsto v\} \mid \sigma \in \Sigma,\ v \in \mathcal{V}\, E_1\, \Sigma\} \\
\mathcal{V}\, \texttt{if}\, E_1\, E_2\, E_3\, \Sigma & = & \mathcal{V}\, E_2\, (\mathcal{B}\, E_1\, \Sigma) \cup \mathcal{V}\, E_3\, (\neg\mathcal{B}\, E_1\, \Sigma) \\
\mathcal{B}\, E\, \Sigma & = & \{\sigma \mid \mathcal{V}\, E\, \{\sigma\} \neq \{0\}, \sigma \in \Sigma\} \\
\neg\mathcal{B}\, E\, \Sigma & = & \{\sigma \mid \mathcal{V}\, E\, \{\sigma\} = \{0\}, \sigma \in \Sigma\}
\end{array}
$$

의미공간 요약

요약된 의미함수 $\hat{\mathcal{V}}$는 다음의 공간에서

$$\hat{\mathcal{V}} \in Exp \to \hat{Env} \to \hat{\mathbb{Z}}$$

정의되고, 의미공간 사이의 갈로아 연결

$$2^{Env} \to 2^{Z} \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} \hat{Env} \to \hat{\mathbb{Z}}$$

은 각 부품의 갈로아 연결

$$2^{Env} \underset{\alpha_1}{\overset{\gamma_1}{\leftrightarrows}} \hat{Env} \quad \text{와} \quad 2^{\mathbb{Z}} \underset{\alpha_2}{\overset{\gamma_2}{\leftrightarrows}} \hat{\mathbb{Z}}$$

를 가지고 안전하게 정의될 수 있다.

요약 의미 함수 $\hat{\mathcal{V}}\ E$

최선

$$\hat{\mathcal{V}}\ E = \alpha_2 \circ \mathcal{V}\ E \circ \gamma_1$$

에 가까운(비 실용적인) 요약 의미함수의 정의:

$$\begin{array}{rcl}
\hat{\mathcal{V}}\ n\ \hat{\Sigma} & = & \alpha_2\ \{n\} \\
\hat{\mathcal{V}}\ E_1 \texttt{+} E_2\ \hat{\Sigma} & = & \alpha_2\{v_1 + v_2 \mid v_1 \in \gamma_2(\hat{\mathcal{V}}\ E_1\ \hat{\Sigma}), v_2 \in \gamma_2(\hat{\mathcal{V}}\ E_2\ \hat{\Sigma})\} \\
\hat{\mathcal{V}}\ \texttt{-}\ E\ \hat{\Sigma} & = & \alpha_2\{-v \mid v \in \gamma_2(\hat{\mathcal{V}}\ E\ \hat{\Sigma})\} \\
\hat{\mathcal{V}}\ \texttt{let}\ x\ E_1\ E_2\ \hat{\Sigma} & = & \hat{\mathcal{V}}\ E_2\ (\alpha_1\{\sigma\{x \mapsto v\} \mid \sigma \in \gamma_1(\hat{\Sigma}), v \in \gamma_2(\hat{\mathcal{V}}\ E_1\ \hat{\Sigma})\} \\
\hat{\mathcal{V}}\ \texttt{if}\ E_1\ E_2\ E_3\ \hat{\Sigma} & = & \hat{\mathcal{V}}\ E_2\ (\alpha_2(\mathcal{B}\ E_1\ (\gamma_1\hat{\Sigma}))) \sqcup \hat{\mathcal{V}}\ E_3\ (\alpha_2(\neg\mathcal{B}\ E_1\ (\gamma_1\hat{\Sigma}))
\end{array}$$

Lemma (Correctness)

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

표기법: $f \times g = \lambda\langle a,b\rangle.\langle f\,a, g\,b\rangle$, 남용해서도, $f \times g = \lambda a.\langle f\,a, g\,a\rangle$.

Proof. 증명전에 상기하자: $\alpha f \sqsubseteq \hat{f}$ 는 곧 $\alpha \circ f \circ \gamma \sqsubseteq \hat{f}$ 곧 $\alpha \circ f \sqsubseteq \hat{f} \circ \alpha$ 곧 $f \circ \gamma \sqsubseteq \gamma \circ \hat{f}$.

- E_1 + E_2이 경우. 잘 보면,

$$\begin{aligned}
\hat{\mathcal{V}}\, E_1 + E_2 &= \alpha_2 \circ \dot{+} \circ \gamma_2 \times \gamma_2 \circ \hat{\mathcal{V}}\, E_1 \times \hat{\mathcal{V}}\, E_2 \\
&= \alpha_2 \circ \dot{+} \circ (\gamma_2 \circ \hat{\mathcal{V}}\, E_1) \times (\gamma_2 \circ \hat{\mathcal{V}}\, E_2) \\
\alpha(\mathcal{V}\, E_1 + E_2) &= \alpha_2 \circ \mathcal{V}\, E_1 + E_2 \circ \gamma_1 \\
&= \alpha_2 \circ \dot{+} \circ \mathcal{V}\, E_1 \times \mathcal{V}\, E_2 \circ \gamma_1 \\
&= \alpha_2 \circ \dot{+} \circ (\mathcal{V}\, E_1 \circ \gamma_1) \times (\mathcal{V}\, E_2 \circ \gamma_1)
\end{aligned}$$

  이다. 귀납 가정에 의해 $\mathcal{V}\, E_i \circ \gamma_1 \sqsubseteq \gamma_2 \circ \hat{\mathcal{V}}\, E_i$ 이므로 쉽게 확인할 수 있다, $\alpha(\mathcal{V}\, E_1 + E_2) \sqsubseteq \hat{\mathcal{V}}\, E_1 + E_2$ 임을.

- 다른 경우들도 마찬가지다. 잘 보면,

$$\begin{aligned}
\hat{\mathcal{V}}\, \texttt{let}\; x\; E_1\; E_2 &= \hat{\mathcal{V}}\, E_2 \circ \alpha_1 \circ \cdot\{x \mapsto \cdot\} \circ \gamma_1 \times (\gamma_2 \circ \hat{\mathcal{V}}\, E_1) \\
\alpha(\mathcal{V}\, \texttt{let}\; x\; E_1\; E_2) &= \alpha_2 \circ \mathcal{V}\, \texttt{let}\; x\; E_1\; E_2) \circ \gamma_1 \\
&= \alpha_2 \circ \mathcal{V}\, E_2 \circ \cdot\{x \mapsto \cdot\} \circ id \times \mathcal{V}\, E_1 \circ \gamma_1 \\
&= \alpha_2 \circ \mathcal{V}\, E_2 \circ \cdot\{x \mapsto \cdot\} \circ \gamma_1 \times (\mathcal{V}\, E_1 \circ \gamma_1)
\end{aligned}$$

  이고

$$\begin{aligned}
\hat{\mathcal{V}}\, \texttt{if}\; E_1\; E_2\; E_3 &= \sqcup \circ \\
&\quad (\hat{\mathcal{V}}\, E_2 \circ \alpha_2 \circ \mathcal{B}\, E_1 \circ \gamma_1) \times \\
&\quad (\hat{\mathcal{V}}\, E_3 \circ \alpha_2 \circ \neg\mathcal{B}\, E_1 \circ \gamma_1) \\
\alpha(\mathcal{V}\, \texttt{if}\; E_1\; E_2\; E_3) &= \alpha_2 \circ \mathcal{V}\, \texttt{if}\; E_1\; E_2\; E_3 \circ \gamma_1 \\
&= \alpha_2 \circ \cup \circ \\
&\quad (\mathcal{V}\, E_2 \circ \mathcal{B}\, E_1 \circ \gamma_1) \times (\mathcal{V}\, E_3 \circ \neg\mathcal{B}\, E_1 \circ \gamma_1)
\end{aligned}$$

  이므로 귀납가정과 $\hat{\mathbb{Z}}$이 $\sqcup$에 닫혀있다는 가정하에 $\alpha_2 \circ \cup = \sqcup \circ \alpha_2 \times \alpha_2$을 이용해서 쉽게 안전함을 보일 수 있다.

요약 의미함수 $\hat{\mathcal{V}}\ E$

실용적인 요약 의미함수의 정의:

$$
\begin{array}{rcl}
\hat{\mathcal{V}}\ n\ \hat{\Sigma} & = & \alpha_2\ \{n\} \\
\hat{\mathcal{V}}\ E_1\ \texttt{+}\ E_2\ \hat{\Sigma} & = & (\hat{\mathcal{V}}\ E_1\ \hat{\Sigma}) \hat{+} (\hat{\mathcal{V}}\ E_2\ \hat{\Sigma}) \\
\hat{\mathcal{V}}\ \texttt{-}\ E\ \hat{\Sigma} & = & \hat{-}(\hat{\mathcal{V}}\ E\ \hat{\Sigma}) \\
\hat{\mathcal{V}}\ \texttt{let}\ x\ E_1\ E_2\ \hat{\Sigma} & = & \hat{\mathcal{V}}\ E_2\ (\hat{\Sigma}\{x \hat{\mapsto} \hat{\mathcal{V}}\ E_1\ \hat{\Sigma}\}) \\
\hat{\mathcal{V}}\ \texttt{if}\ E_1\ E_2\ E_3\ \hat{\Sigma} & = & (\hat{\mathcal{V}}\ E_2\ (\hat{\mathcal{B}}\ E_1\ \hat{\Sigma})) \sqcup (\hat{\mathcal{V}}\ E_3\ (\hat{\neg\mathcal{B}}\ E_1\ \hat{\Sigma}))
\end{array}
$$

여기서 $\hat{+}$, $\hat{-}$, $\cdot\{x \hat{\mapsto} \cdot\}$, $\hat{\mathcal{B}}$, $\hat{\neg\mathcal{B}}$는 해당 연산들을 안전하게 요약한 것들이어야.

Lemma (Correctness)

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

표기법: $f \times g = \lambda\langle a, b\rangle.\langle f\ a, g\ b\rangle$, 남용해서도,
$f \times g = \lambda a.\langle f\ a, g\ a\rangle$.
Proof. 증명전에 상기하자: $\alpha f \sqsubseteq \hat{f}$ 는 곧 $\alpha \circ f \circ \gamma \sqsubseteq \hat{f}$ 곧
$\alpha \circ f \sqsubseteq \hat{f} \circ \alpha$ 곧 $f \circ \gamma \sqsubseteq \gamma \circ \hat{f}$.
증명하자. 경우마다 잘 보면,

$$
\begin{aligned}
\hat{\mathcal{V}}\ E_1 + E_2 &= \hat{+} \circ \hat{\mathcal{V}}\ E_1 \times \hat{\mathcal{V}}\ E_2 \\
\alpha(\mathcal{V}\ E_1 + E_2) &= \alpha_2 \circ \mathcal{V}\ E_1 + E_2 \circ \gamma_1 \\
&= \alpha_2 \circ \dot{+} \circ \mathcal{V}\ E_1 \times \mathcal{V}\ E_2 \circ \gamma_1 \\
&= \alpha_2 \circ \dot{+} \circ (\mathcal{V}\ E_1 \circ \gamma_1) \times (\mathcal{V}\ E_2 \circ \gamma_1)
\end{aligned}
$$

이고

$$
\begin{aligned}
\hat{\mathcal{V}}\, \texttt{let}\ x\ E_1\ E_2 &= \hat{\mathcal{V}}\ E_2 \circ \cdot\{x \hat{\mapsto} \cdot\} \circ id \times \hat{\mathcal{V}}\ E_1 \\
\alpha(\mathcal{V}\, \texttt{let}\ x\ E_1\ E_2) &= \alpha_2 \circ \mathcal{V}\, \texttt{let}\ x\ E_1\ E_2 \circ \gamma_1 \\
&= \alpha_2 \circ \mathcal{V}\ E_2 \circ \cdot\{x \mapsto \cdot\} \circ id \times \mathcal{V}\ E_1 \circ \gamma_1
\end{aligned}
$$

이고

$$
\begin{aligned}
\hat{\mathcal{V}}\, \texttt{if}\ E_1\ E_2\ E_3 &= \sqcup \circ (\hat{\mathcal{V}}\ E_2 \circ \hat{\mathcal{B}}\ E_1) \times (\hat{\mathcal{V}}\ E_3 \circ \widehat{\neg\mathcal{B}}\ E_1) \\
\alpha(\mathcal{V}\, \texttt{if}\ E_1\ E_2\ E_3) &= \alpha_2 \circ \mathcal{V}\, \texttt{if}\ E_1\ E_2\ E_3 \circ \gamma_1 \\
&= \alpha_2 \circ \cup \circ \\
&\quad (\mathcal{V}\ E_2 \circ \mathcal{B}\ E_1 \circ \gamma_1) \times (\mathcal{V}\ E_3 \circ \neg\mathcal{B}\ E_1) \circ \gamma_1)
\end{aligned}
$$

이므로 귀납가정과 $\hat{\mathbb{Z}}$이 $\sqcup$에 닫혀있다는 가정하에
$\alpha_2 \circ \cup = \sqcup \circ \alpha_2 \times \alpha_2$을 이용해서 쉽게 안전함을 보일 수 있다.

명령형 언어 프로그램의 요약해석

$$
\begin{array}{rcl}
C & \rightarrow & \texttt{skip} \mid x \texttt{ := } E \mid C \texttt{ ; } C \\
 & \mid & \texttt{if } B\ C\ C \\
 & \mid & \texttt{while } B\ C \\
E & \rightarrow & n \quad (n \in \mathbb{Z}) \mid x \\
 & \mid & E \texttt{ + } E \mid B \quad (\text{boolean expr})
\end{array}
$$

의미공간은

$$
\begin{array}{rcl}
\mathcal{C}\ C & \in & 2^{Memory} \rightarrow 2^{Memory} \\
\mathcal{V}\ E & \in & 2^{Memory} \rightarrow 2^{Value} \\
\mathcal{B}\ B & \in & 2^{Memory} \rightarrow 2^{Memory} \\
Memory & = & Loc \xrightarrow{\text{fin}} Value \\
Value & = & \mathbb{Z} + \mathbb{B} \\
Loc & = & Var \\
\mathbb{B} & = & \{T, F\}
\end{array}
$$

$$m \in Memory \qquad M \in 2^{Memory}$$

$$\begin{array}{rcl}
\mathcal{C}\ \texttt{skip}\ M & = & M \\
\mathcal{C}\ x\ \texttt{:=}\ E\ M & = & \{m\{x \mapsto v\} \mid m \in M, v \in \mathcal{V}\ E\ M\} \\
\mathcal{C}\ C_1\ \texttt{;}\ C_2\ M & = & \mathcal{C}\ C_2\ (\mathcal{C}\ C_1\ M) \\
\mathcal{C}\ \texttt{if}\ B\ C_1\ C_2\ M & = & \mathcal{C}\ C_1\ (\mathcal{B}\ B\ M)\ \cup\ \mathcal{C}\ C_2\ (\mathcal{B}\ \neg B\ M) \\
\mathcal{C}\ \texttt{while}\ B\ C\ M & = & \mathcal{B}\ \neg B\ (\mathit{fix}\,\lambda X.M \cup \mathcal{C}\ C\ (\mathcal{B}\ B\ X)) \\
\mathcal{V}\ n\ M & = & \{n\} \\
\mathcal{V}\ x\ M & = & \{m\ x \mid m \in M\} \\
\mathcal{V}\ E_1\ \texttt{+}\ E_2\ M & = & \{v_1 + v_2 \mid v_1 \in \mathcal{V}\ E_1\ M, v_2 \in \mathcal{V}\ E_2\ M\} \\
\mathcal{B}\ B\ M & = & \cup\{M' \mid \mathcal{V}\ B\ M' = \{T\}, M' \subseteq M\}
\end{array}$$

요약

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

갈로아 연결 된 요약공간

$$
2^{Memory} \underset{\alpha_1}{\overset{\gamma_1}{\leftrightarrows}} \widehat{Memory} \qquad 2^{Value} \underset{\alpha_2}{\overset{\gamma_2}{\leftrightarrows}} \widehat{Value}
$$

$$
\begin{array}{rcl}
\hat{\mathcal{C}}\ \texttt{skip}\ \hat{m} & = & \hat{m} \\
\hat{\mathcal{C}}\ x\ \texttt{:=}\ E\ \hat{m} & = & \hat{m}\{x \hat{\mapsto} \hat{\mathcal{V}}\ E\ \hat{m}\} \\
\hat{\mathcal{C}}\ C_1\ \texttt{;}\ C_2\ \hat{m} & = & \hat{\mathcal{C}}\ C_2\ (\hat{\mathcal{C}}\ C_1\ \hat{m}) \\
\hat{\mathcal{C}}\ \texttt{if}\ B\ C_1\ C_2\ \hat{m} & = & \hat{\mathcal{C}}\ C_1\ (\hat{\mathcal{B}}\ B\ \hat{m})\ \sqcup\ \hat{\mathcal{C}}\ C_1\ (\hat{\mathcal{B}}\ \neg B\ \hat{m}) \\
\hat{\mathcal{C}}\ \texttt{while}\ B\ C\ \hat{m} & = & \hat{\mathcal{B}}\ \neg B\ (\mathit{fix} \lambda \hat{x}.\hat{m}\ \sqcup\ \hat{\mathcal{C}}\ C\ (\hat{\mathcal{B}}\ B\ \hat{x})) \\
\hat{\mathcal{V}}\ n\ \hat{m} & = & \alpha_2\{n\} \\
\hat{\mathcal{V}}\ x\ \hat{m} & = & \hat{m}\ \hat{at}\ x \\
\hat{\mathcal{V}}\ E_1\ \texttt{+}\ E_2\ \hat{m} & = & (\hat{\mathcal{V}}\ E_1\ \hat{m})\ \hat{+}\ (\hat{\mathcal{V}}\ E_2\ \hat{m})
\end{array}
$$

여기서 $\hat{+}$, $\cdot\{x \hat{\mapsto} \cdot\}$, $\hat{\mathcal{B}}$, $\hat{at}$는 해당 연산들을 안전하게 요약한 것들이어야.

Lemma (Correctness)

$\forall C : \alpha(\mathcal{C}\ C) \sqsubseteq \hat{\mathcal{C}}\ C$

Proof. 경우마다 잘 보면, 이전 증명들과 비슷하게 쉽게 진행된다. 특이한 경우는

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

여기서 $\alpha_1 \circ F \sqsubseteq \hat{F} \circ \alpha_1$을 쉽게 보일 수 있고, 이는 “Fixpoint Transfer Theorem”에 의해 $\alpha_1(\mathit{fix} F) \sqsubseteq \mathit{fix}\hat{F}$ 즉,
$\mathit{fix} F \sqsubseteq \gamma_1\,(\mathit{fix}\hat{F})$이고, $\hat{\mathcal{B}}\,B$와 $\hat{\mathcal{B}}\,\neg B$가 안전하다는 가정하에, 쉽게 위의 두 개 사이의 올바른 관계

$$(\alpha_1 \circ \mathcal{B}\,\neg B)\ \mathit{fix} F \sqsubseteq \hat{\mathcal{B}}\,\neg B\ \mathit{fix}\hat{F}$$

을 확인 할 수 있다.

구현

주어진 프로그램 C와, 관심있는 초기 메모리 $\hat{m}_0$에 대해서 조립식으로 정의된

$$\hat{\mathcal{C}}\ C\ \hat{m}_0$$

를 계산.

- 이때 C안에 있는 `while` $E\ C'$에 대해서 $\mathit{fix}\hat{F} \in \hat{Memory}$의 계산은

$$\bigsqcup_{i \in \mathbb{N}} \hat{F}^i(\bot_{\hat{Memory}})$$

  으로.
- 위의 계산이 끝나지 않거나 시간이 너무 오래걸릴 수 있으면 축지법($\bigtriangledown$)과 좁히기($\bigtriangleup$)를 이용

$$
\begin{array}{rcl}
\hat{\mathcal{C}}\ \texttt{skip}\ \hat{m} & = & \hat{m} \\
\hat{\mathcal{C}}\ x\ \texttt{:=}\ E\ \hat{m} & = & \hat{m}\{x \hat{\mapsto} \hat{\mathcal{V}}\ E\ \hat{m})\} \\
\hat{\mathcal{C}}\ C_1\ \texttt{;}\ C_2\ \hat{m} & = & \hat{\mathcal{C}}\ C_2\ (\hat{\mathcal{C}}\ C_1\ \hat{m}) \\
\hat{\mathcal{C}}\ \texttt{if}\ B\ C_1\ C_2\ \hat{m} & = & \hat{\mathcal{C}}\ C_1\ (\hat{\mathcal{B}}\ B\ \hat{m})\ \sqcup\ \hat{\mathcal{C}}\ C_1\ (\hat{\mathcal{B}}\ \neg B\ \hat{m}) \\
\hat{\mathcal{C}}\ \texttt{while}\ B\ C\ \hat{m} & = & \hat{\mathcal{B}}\ \neg B\ (\mathit{Narrow}(\mathit{Widen}\ (\lambda \hat{x}.\hat{m}\ \sqcup\ \hat{\mathcal{C}}\ C\ (\hat{\mathcal{B}}\ B\ \hat{x})))) \\
\hat{\mathcal{V}}\ n\ \hat{m} & = & \alpha_2\{n\} \\
\hat{\mathcal{V}}\ x\ \hat{m} & = & \hat{m}\ \hat{at}\ x \\
\hat{\mathcal{V}}\ E_1\ \texttt{+}\ E_2\ m & = & (\hat{\mathcal{V}}\ E_1\ \hat{m})\ \hat{+}\ (\hat{\mathcal{V}}\ E_2\ \hat{m})
\end{array}
$$

$$
Widen(\hat{F}) = \lim_{i \in \mathbb{N}} \left\{ \begin{array}{lcl} \hat{Y}_0 & = & \bot_{\hat{Memory}} \\ \hat{Y}_{i+1} & = & \left\{ \begin{array}{ll} \hat{Y}_i & \text{if } \hat{F}(\hat{Y}_i) \sqsubseteq \hat{Y}_i \\ \hat{Y}_i \bigtriangledown \hat{F}(\hat{Y}_i) & \text{o.w.} \end{array} \right. \end{array} \right.
$$

$$
Narrow(\hat{m}) = \lim_{i \in \mathbb{N}} \left\{ \begin{array}{lcl} \hat{Z}_0 & = & \hat{m} \\ \hat{Z}_{i+1} & = & \hat{Z}_i \bigtriangleup \hat{F}(\hat{Z}_i) \end{array} \right.
$$