Theorem Problem

SNU 4541.664A Program Analysis
Spring 2006
Note 10-1

Prof. Kwangkeun Yi

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*)

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

- 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.

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

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

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

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

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

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

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

모듬 의미(collecting semantics)

모듬 의미함수 $\mathcal{V}$는 아래와 같은 공간에서

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

조립식으로 정의된다:

$$\begin{array}{rcl} \mathcal{V}\, n\, \Sigma & = & \{n\} \\ \mathcal{V}\, x\, \Sigma & = & \{\sigma\, x \mid \sigma \in \Sigma\} \\ \mathcal{V}\, E_1 \texttt{+} E_2\, \Sigma & = & \{z_1 + z_2 \mid z_i \in \mathcal{V}\, E_i\, \Sigma\} \\ \mathcal{V}\, \texttt{-}\, E\, \Sigma & = & \{-z \mid z \in \mathcal{V}\, E\, \Sigma\} \\ \mathcal{V}\, \texttt{let}\, x\, E_1\, E_2\, \Sigma & = & \mathcal{V}\, E_2\, \{\sigma\{x \mapsto v\} \mid \sigma \in \Sigma,\ v \in \mathcal{V}\, E_1\, \Sigma\} \\ \mathcal{V}\, \texttt{if}\, E_1\, E_2\, E_3\, \Sigma & = & \mathcal{V}\, E_2\, (\mathcal{B}\, E_1\, \Sigma) \cup \mathcal{V}\, E_3\, (\neg\mathcal{B}\, E_1\, \Sigma) \\ \mathcal{B}\, E\, \Sigma & = & \cup\{\Sigma' \mid \mathcal{V}\, E\, \Sigma' \not\ni 0, \Sigma' \subseteq \Sigma\} \\ \neg\mathcal{B}\, E\, \Sigma & = & \cup\{\Sigma' \mid \mathcal{V}\, E\, \Sigma' = \{0\}, \Sigma' \subseteq \Sigma\} \end{array}$$

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 $\hat{\mathcal{V}}\,E$

최선의 요약 의미함수

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

의 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)

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

요약 의미함수 $\hat{\mathcal{V}}\, E$

또 다른 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)

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

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

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

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

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

요약

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

갈로아 연결 된 요약공간

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

$$
\begin{array}{rcl}
\hat{\mathcal{C}}\,\texttt{skip}\,\hat{m} & = & \hat{m} \\
\hat{\mathcal{C}}\,x\;\texttt{:=}\;E\,\hat{m} & = & \alpha_1\{m\{x \mapsto v\} \mid m \in \gamma_1\hat{m}, v \in \gamma_2(\hat{\mathcal{V}}\,E\,\hat{m})\} \\
\hat{\mathcal{C}}\,C_1\;;\;C_2\,\hat{m} & = & \hat{\mathcal{C}}\,C_2\,(\hat{\mathcal{C}}\,C_1\,\hat{m}) \\
\hat{\mathcal{C}}\,\texttt{if}\;B\,C_1\,C_2\,\hat{m} & = & \hat{\mathcal{C}}\,C_1\,(\hat{\mathcal{B}}\,B\,\hat{m}) \sqcup \hat{\mathcal{C}}\,C_1\,(\hat{\mathcal{B}}\,\neg B\,\hat{m}) \\
\hat{\mathcal{C}}\,\texttt{while}\;B\,C\,\hat{m} & = & \hat{\mathcal{B}}\,\neg B\,(\mathit{fix}\lambda\hat{x}.\hat{m} \sqcup \hat{\mathcal{C}}\,C\,(\hat{\mathcal{B}}\,B\,\hat{x})) \\
\hat{\mathcal{V}}\,n\,\hat{m} & = & \alpha_2\{n\} \\
\hat{\mathcal{V}}\,x\,\hat{m} & = & \hat{m}\,x \\
\hat{\mathcal{V}}\,E_1\;\texttt{+}\;E_2\,m & = & \alpha_2\{v_1 + v_2 \mid v_1 \in \gamma_2(\hat{\mathcal{V}}\,E_1\,\hat{m}), v_2 \in \gamma_2(\hat{\mathcal{V}}\,E_2\,\hat{m})\} \\
\hat{\mathcal{B}}\,B\,\hat{m} & = & \alpha_1(\cup\{M' \mid \mathcal{V}\,B\,M' = \{T\}, \hat{M}' \subseteq \gamma_1\hat{m}\})
\end{array}
$$

Lemma (Correctness)

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

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 $\mathit{fix}\hat{F} \in \widehat{Memory}$의 계산은

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

  으로.

- 위의 계산이 끝나지 않거나 시간이 너무 오래걸릴 수 있으면 축지법($\triangledown$)과 좁히기($\triangle$)를 이용

$$
\begin{array}{rcl}
\hat{\mathcal{C}}\ \texttt{skip}\ \hat{m} & = & \hat{m} \\
\hat{\mathcal{C}}\ x\ \texttt{:=}\ E\ \hat{m} & = & \alpha_1\{m\{x \mapsto v\} \mid m \in \gamma_1 \hat{m}, v \in \gamma_2(\hat{\mathcal{V}}\ E\ \hat{m})\} \\
\hat{\mathcal{C}}\ C_1\ \texttt{;}\ C_2\ \hat{m} & = & \hat{\mathcal{C}}\ C_2\ (\hat{\mathcal{C}}\ C_1\ \hat{m}) \\
\hat{\mathcal{C}}\ \texttt{if}\ B\ C_1\ C_2\ \hat{m} & = & \hat{\mathcal{C}}\ C_1\ (\hat{\mathcal{B}}\ B\ \hat{m})\ \sqcup\ \hat{\mathcal{C}}\ C_1\ (\hat{\mathcal{B}}\ \neg B\ \hat{m}) \\
\hat{\mathcal{C}}\ \texttt{while}\ B\ C\ \hat{m} & = & \hat{\mathcal{B}}\ \neg B\ (Narrow(Widen\ (\lambda \hat{x}.\hat{m}\ \sqcup\ \hat{\mathcal{C}}\ C\ (\hat{\mathcal{B}}\ B\ \hat{x})))) \\
\hat{\mathcal{V}}\ n\ \hat{m} & = & \alpha_2\{n\} \\
\hat{\mathcal{V}}\ x\ \hat{m} & = & \hat{m}\ x \\
\hat{\mathcal{V}}\ E_1\ \texttt{+}\ E_2\ m & = & \alpha_2\{v_1 + v_2 \mid v_1 \in \gamma_2(\hat{\mathcal{V}}\ E_1\ \hat{m}), v_2 \in \gamma_2(\hat{\mathcal{V}}\ E_2\ \hat{m})\} \\
\hat{\mathcal{B}}\ B\ \hat{m} & = & \alpha_1(\cup\{M' \mid \mathcal{V}\ B\ M' = \{T\}, \hat{M}' \subseteq \gamma_1 \hat{m}\})
\end{array}
$$

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

$$Narrow(\hat{m}) = \lim_{i \in \mathbb{N}} \begin{cases} \hat{Z}_0 = \hat{m} \\ \hat{Z}_{i+1} = \hat{Z}_i \bigtriangleup \hat{F}(\hat{Z}_i) \end{cases}$$

계산 실행과정을 요약하는 방안들

프로그램 C의 의미 $[\![C]\!]$는 C가 실행되면서 가질 수 있는 기계상태들의 (유한 혹은 무한한) 모든 족적들

$$
\begin{array}{rcccl}
[\![C]\!] & \in & 2^{Trace} & & \\
\tau, \tau_0\tau_1\cdots\tau_n & \in & Trace & = & State^{\omega} \\
 & & State & = & Command \times Memory \times \cdots
\end{array}
$$

$$2^{Trace} \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} \hat{Trace}$$

$\xrightarrow{\alpha_0}$ Trace of set of states: sequence of set of states appearing at a given time along at least one of the traces

$$\alpha_0(X) = \lambda i.\{\tau_i \mid \tau \in X, 0 \leq i < |\tau|\}$$

$\xrightarrow{\alpha_1}$ Set of reachable states (global invariant): set of states appearing at least once along a trace

$$\alpha_1(Y) = \bigcup\{Y(i) \mid 0 \leq i < |Y|\}$$

$\xrightarrow{\alpha_2}$ Partitioned set of reachable states (local invariant): project along each control point $\in \Delta$

$$\alpha_2(\{\langle c_i, s_i\rangle \mid i \in \Delta\}) = \lambda c.\{s_i \mid i \in \Delta, c = c_i\}$$