SNU 4541.664A Program Analysis
Spring 2005
Note 9

Prof. Kwangkeun Yi

요약에 대한 사실과 예들

- 의미공간의 요약 예
- 의미구조의 요약 예

- "$\hat{D}$는 D를 요약한 것이다"는

$$D \underset{\alpha}{\overset{\gamma}{\rightleftarrows}} \hat{D}$$

인

$$\text{요약함수}(\textit{abstraction}) \quad \alpha : D \to \hat{D}$$

와

$$\text{구체함수}(\textit{concretization}) \quad \gamma : \hat{D} \to D$$

가 있을 때를 의미

- 필요하면 α와 γ의 정의구역을 첨자로:

$$\alpha_D, \quad \gamma_{\hat{D}}$$

갈로아 연결 예1

아래의 $\hat{A}$들은 $2^{\mathbb{Z}}$를 요약한 것이다:

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

각각의 α, γ를 알아보자:

- $\hat{A} = \{\perp\}$
- $\hat{A} = \{\perp, \texttt{+}, \texttt{-}, \texttt{0}, \top\}$
- $\hat{A} = \{\perp, \mathtt{p}, \mathtt{n}, \top\}$
- $\hat{A} = \mathbb{Z} \cup \{\perp, \top\}$
- $\hat{A} = \{\perp\} \cup \{\langle a, b\rangle \mid a \leq b,\ a, b \in \mathbb{Z} \cup \{\infty, -\infty\}\}$

(왜 $\top$은 맨 위에 있어야 할까?)

α와 γ는 대게 동전의 양면

- $\alpha : D \to \hat{D}$가 연속(*continuous*) 함수이고 D가 임의의 부분 집합의 최소 윗뚜껑(*least upper bound*)이 있으면($\sqcup$-*complete*), 갈로아 연결 짝 γ는

$$\gamma\,\hat{x} = \sqcup\{x \mid \alpha\,x \sqsubseteq \hat{x}\}.$$

- $\gamma : \hat{D} \to D$가 연속(*continuous*) 함수이고 $\hat{D}$가 임의의 부분 집합의 최대 밑뚜껑(*greatest lower bound*)이 있으면($\sqcap$-*complete*), 갈로아 연결 짝 α는

$$\alpha\,x = \sqcap\{\hat{x} \mid x \sqsubseteq \gamma\,\hat{x}\}.$$

갈로아 연결은 조립식

A를 요약한 것이 $\hat{A}$ 이고 B를 요약한 것이 $\hat{B}$이면,

- $A \times B$를 $\hat{A} \times \hat{B}$로 요약가능

$$\alpha_{A \times B} = \lambda \langle a, b \rangle . \langle \alpha_A a, \alpha_B b \rangle$$

- $A + B$를 $\hat{A} + \hat{B}$로 요약가능

$$\alpha_{A+B} = \lambda x . \alpha_A x \ \mathit{if} \ x \in A, \ \alpha_B x \ o.w.$$

- $A \rightarrow B$를 $\hat{A} \rightarrow \hat{B}$로 요약가능

$$\alpha_{A \rightarrow B} = \lambda f . \alpha_B \circ f \circ \gamma_{\hat{A}}$$

$2^A \leftrightarrows \hat{X}$ 이고 $2^B \leftrightarrows \hat{Y}$ 이면,

- $2^{A\times B} \leftrightarrows \hat{X} \times \hat{Y}$ 가능

$$\alpha = \lambda X.\langle \alpha_1\{a|\langle a,b\rangle \in X\}, \alpha_2\{b|\langle a,b\rangle \in X\}\rangle$$

- $2^{A\times B} \leftrightarrows A' \to \hat{Y}$ 가능 $(A' \subseteq A)$

$$\alpha = \lambda X.\{a \mapsto \alpha_2 S|\langle a,b\rangle \in X, S = \{b|\langle a,b\rangle \in X\}\}$$

- $2^{A+B} \leftrightarrows \hat{X} \times \hat{Y}$ 가능

$$\alpha = \lambda X.\langle \alpha_1\{a|a \in X, a \in A\}, \alpha_2\{b|b \in X, b \in B\}\rangle$$

- $2^A \to 2^B \leftrightarrows \hat{X} \to \hat{Y}$ 가능

$$\alpha = \lambda f.\alpha_2 \circ f \circ \gamma_1$$

의미함수의 요약

의미공간 A와 B 위에서 정의된 의미함수

$$f \in A \to B$$

를 요약된 의미공간

$$A \underset{\alpha_A}{\overset{\gamma_{\hat{A}}}{\leftrightarrows}} \hat{A} \quad \text{와} \quad B \underset{\alpha_B}{\overset{\gamma_{\hat{B}}}{\leftrightarrows}} \hat{B}$$

위의 함수

$$\hat{f} \in \hat{A} \to \hat{B}$$

로 정의하는 "최선의"(정확도를 최대로 유지하는) 방법은

$$\hat{f} = \alpha_B \circ f \circ \gamma_A$$

이다.

의미구조 요약 예1

$$e \ \rightarrow \ z \mid e\texttt{+}e \mid \texttt{-}e$$

$$\begin{array}{rcl} [\![e]\!] & \in & A = 2^{\mathbb{Z}} \\ \hat{[\![e]\!]} & \in & \hat{A} \end{array}$$

궁극의 의미구조(*denotational semantics*) 스타일로:

$$\begin{array}{rcl} [\![z]\!] & = & \{z\} \\ [\![e_1\texttt{+}e_2]\!] & = & [\![e_1]\!]\dot{+}[\![e_2]\!] \\ [\![\texttt{-}e]\!] & = & \dot{-}[\![e]\!] \\ a\dot{+}b & = & \{x+y \mid x \in a, y \in b\} \\ \dot{-}a & = & \{-x \mid x \in a\} \end{array}$$

$$\begin{array}{rcl} \hat{[\![z]\!]} & = & \alpha\{z\} \\ \hat{[\![e_1\texttt{+}e_2]\!]} & = & \hat{[\![e_1]\!]}\hat{+}\hat{[\![e_2]\!]} \\ \hat{[\![\texttt{-}e]\!]} & = & \hat{-}\hat{[\![e]\!]} \\ \hat{a}\hat{+}\hat{b} & = & ? \\ \hat{-}\hat{a} & = & ? \end{array}$$

확인할 것:

$$\forall e.\alpha(\llbracket e \rrbracket) \sqsubseteq \hat{\llbracket e \rrbracket} \quad \text{또는 같은 이야기로}$$
$$\forall e.\llbracket e \rrbracket \sqsubseteq \gamma \hat{\llbracket e \rrbracket}$$

구현은:

- 임의의 프로그램 e에 대해서 $\hat{\llbracket e \rrbracket}$ 계산
- $\hat{\llbracket e \rrbracket}$ 계산은 유한 시간에 끝남

의미구조 요약 예2

계산과정을 드러내는(*operational semantics*) 방식으로:
$[\![e]\!]$는 상태의 변환과정으로 정의됨
상태 변환 규칙은

$$\frac{e_1 \longrightarrow e_1'}{e_1 + e_2 \longrightarrow e_1' + e_2} \qquad \frac{e \longrightarrow e'}{z\text{+}e \longrightarrow z\text{+}e'}$$

$$\frac{e \longrightarrow e'}{\text{-}e \longrightarrow \text{-}e'} \qquad \frac{}{z_1\text{+}z_2 \longrightarrow z_1 + z_2}$$

$$\frac{}{\text{-}z \longrightarrow -z}$$

- $[\![e]\!]$의 정의 1:

$$
\begin{array}{rcl}
[\![e]\!] & \in & 2^{(S^*)}, \quad S = Exp \\
[\![e]\!] & = & fix \lambda T.\{e\} \sqcup \{t \to e'' \mid t \in T \ \wedge t = \cdots \to e' \ \wedge \ e' \to e''\} \\
 & & where\ T_1 \sqsubseteq T_2\ iff\ \forall t_1 \in T_1 . \exists t_2 \in T_2 . t_2 = t1 \to \cdots
\end{array}
$$

- $[\![e]\!]$의 정의 2:

$$
\begin{array}{rcl}
[\![e]\!] & \in & S^*, \quad S = 2^{Exp} \\
[\![e]\!] & = & fix \lambda t.\{e\} \sqcup (t \to X) \\
 & & where\ X = \{e'' \mid t = \cdots \to E \ \wedge \ e' \in E \ \wedge \ e' \to e''\}
\end{array}
$$

요약본 $[\![\hat{e}]\!]$는 요약상태의 전환과정으로 정의됨

$$
\begin{array}{rcl}
[\![\hat{e}]\!] & \in & (\hat{S})^*, \quad \hat{S} \underset{\gamma_{\hat{S}}}{\overset{\alpha_S}{\leftrightarrows}} 2^{Exp} \\
[\![\hat{e}]\!] & = & \mathit{fix}\lambda\hat{t}.\alpha_S\{e\} \sqcup (\hat{t} \to \hat{e}') \\
 & & \textit{where } \hat{t} = \cdots \to \hat{e}_n \wedge \hat{e}_n \to \hat{e}'
\end{array}
$$

요약 상태 전이는

$$
\frac{\hat{e_1} \to \hat{e_1'}}{\hat{e_1} + \hat{e_2} \to \hat{e_1'} + \hat{e_2}} \qquad \frac{\hat{e} \to \hat{e'}}{\hat{z}\texttt{+}\hat{e} \to \hat{z}\texttt{+}\hat{e'}}
$$

$$
\frac{\hat{e} \to \hat{e'}}{\texttt{-}\hat{e} \to \texttt{-}\hat{e'}} \qquad \frac{}{\hat{z_1}\texttt{+}\hat{z_2} \to \hat{z_1}\hat{+}\hat{z_2}}
$$

$$
\frac{}{\texttt{-}\hat{z} \to \hat{-}\hat{z}}
$$

확인할 것:

$$\forall e.\alpha(\llbracket e \rrbracket) \sqsubseteq \llbracket \hat{e} \rrbracket \quad \text{또는 같은 이야기로}$$
$$\forall e.\llbracket e \rrbracket \sqsubseteq \gamma\llbracket \hat{e} \rrbracket$$

구현은:

- 임의의 프로그램 e에 대해서 $\llbracket \hat{e} \rrbracket$ 계산
- $\llbracket \hat{e} \rrbracket$ 계산은 유한 시간에 끝남

언어의 확장1

$$e \;\rightarrow\; \cdots \;\mid\; \texttt{if}\; e\; e\; e$$

$$[\![\texttt{if}\; e_1\; e_2\; e_3]\!] \;=\; \mathit{if}\; [\![e_1]\!]\; [\![e_2]\!]\; [\![e_3]\!]$$

$$\widehat{[\![\texttt{if}\; e_1\; e_2\; e_3]\!]} \;=\; \hat{\mathit{if}}\; \widehat{[\![e_1]\!]}\; \widehat{[\![e_2]\!]}\; \widehat{[\![e_3]\!]}$$

확인할 것:

$\forall e.\alpha([\![e]\!]) \sqsubseteq \widehat{[\![e]\!]}$ 또는 같은 이야기로
$\forall e.[\![e]\!] \sqsubseteq \gamma\widehat{[\![e]\!]}$

요약공간 $\hat{A}$에서 $\sqcup$의 두가지 용도

1. $\sqcup$은 $\hat{A}$의 체인에 대해서 정의되 있기만 하면 됨 (요약해석틀)
2. $\sqcup$이 $\hat{A}$의 임의의 두 원소에 대해서 정의되 있다면, 의미함수 정의에 유용하게 쓰임:

$$\begin{array}{rcl} \mathit{if}\ [\![e_1]\!]\ [\![e_2]\!]\ [\![e_3]\!] & = & \{z \in [\![e_2]\!] \mid 0 \neq n \in [\![e_1]\!]\} \\ & \cup & \{z \in [\![e_3]\!] \mid 0 \in [\![e_1]\!]\} \\ \hat{\mathit{if}}\ [\![\hat{e_1}]\!]\ [\![\hat{e_2}]\!]\ [\![\hat{e_3}]\!] & = & ? \end{array}$$

만일 $A \underset{\gamma}{\overset{\alpha}{\leftrightarrows}} \hat{A}$ 인 CPO A와 $\hat{A}$가 $\sqcup$에 대해서 닫혀있으면(semi-lattices),

$$\forall x, y \in A. \alpha(x \sqcup_A y) = \alpha(x) \sqcup_{\hat{A}} \alpha(y)$$

이므로 $\hat{\mathit{if}}$를 $\sqcup_{\hat{A}}$가지고 정의할 수 있음.

언어의 확장2: ⊤의 사용

$$e \;\rightarrow\; \cdots \mid \texttt{readin}$$

$$\begin{aligned}[\![\texttt{readin}]\!] &= \mathit{read}\\ \hat{[\![\texttt{readin}]\!]} &= \hat{\mathit{read}}\end{aligned}$$

$$\mathit{read} = \mathbb{Z}$$
$$\hat{\mathit{read}} = \top$$

안전한 의미 함수들의 조립은 안전

$$
\begin{array}{ccc}
A & \underset{\alpha_A}{\overset{\gamma_A}{\leftrightarrows}} & \hat{A} \\
f \downarrow & & \downarrow \hat{f} \\
B & \underset{\alpha_B}{\overset{\gamma_B}{\leftrightarrows}} & \hat{B} \\
g \downarrow & & \downarrow \hat{g} \\
C & \underset{\alpha_C}{\overset{\gamma_C}{\leftrightarrows}} & \hat{C}
\end{array}
$$

이고 단조(*monotonic*)인 의미함수들 $f, g, \hat{f}, \hat{g}$가

$$\alpha_B \circ f \sqsubseteq \hat{f} \circ \alpha_A \quad \text{이고} \quad \alpha_C \circ g \sqsubseteq \hat{g} \circ \alpha_B$$

이면

$$\alpha_C \circ (g \circ f) \sqsubseteq (\hat{g} \circ \hat{f}) \circ \alpha_A.$$