SNU 4541.664A Program Analysis
Note 9

Prof. Kwangkeun Yi

요약에 대한 사실과 예들

- 의미공간의 요약 예
- 의미구조의 요약 예

- "$\hat{D}$는 D를 요약한 것이다"는

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

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:

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

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 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 짝 α는

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

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 짝 γ는

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

  왜 갈로아 짝인가? $\alpha x \sqsubseteq \hat{x} \Leftrightarrow x \sqsubseteq \gamma \hat{x}$이다. ($\Rightarrow$)는 당연. ($\Leftarrow$)의 경우: 우변의 조건 $x \sqsubseteq \gamma \hat{x}$ 을 γ의 정의에 의해 다시 쓰면 $x \sqsubseteq \sqcup\{a \mid \alpha\, a \sqsubseteq \hat{x}\}$. 양쪽에 α를 취하면, 연속함수이므로, $\alpha\, x \sqsubseteq \sqcup\{\alpha\, a \mid \alpha\, a \sqsubseteq \hat{x}\}$이고 오른쪽은 다시 $\sqsubseteq \hat{x}$이므로 $\alpha\, x \sqsubseteq \hat{x}$.
- $\gamma : \hat{D} \to D$가 연속(*continuous*) 함수이고 $\hat{D}$가 임의의 부분 집합의 최대 밑뚜껑(*greatest lower bound*)이 있으면($\sqcap$-*complete*), 갈로아 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

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

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

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

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

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

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

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

과연 갈로아 연결인가? 그렇다. 갈로아 짝은
$\gamma_{\hat{A} \to \hat{B}} = \lambda \hat{f} . \gamma_{\hat{B}} \circ \hat{f} \circ \alpha_A$이다. 왜냐면: 임의의 f와 $\hat{f}$에 대해서
$\alpha_B \circ f \circ \gamma_{\hat{A}} \sqsubseteq \hat{f}$라고 하자. 즉(iff), $\gamma_{\hat{B}}$는 단조함수이므로,
$\gamma_{\hat{B}} \circ \alpha_B \circ f \circ \gamma_{\hat{A}} \sqsubseteq \gamma_{\hat{B}} \circ \hat{f}$이다. 즉, $id \sqsubseteq \gamma_{\hat{B}} \circ \alpha_B$이므로,
$f \circ \gamma_{\hat{A}} \sqsubseteq \gamma_{\hat{B}} \circ \hat{f}$. 즉, $f \circ \gamma_{\hat{A}} \circ \alpha_A \sqsubseteq \gamma_{\hat{B}} \circ \hat{f} \circ \alpha_A$. 즉, $id \sqsubseteq \gamma_{\hat{A}} \circ \alpha_A$이고
f는 단조함수 이므로, $f \sqsubseteq \gamma_{\hat{B}} \circ \hat{f} \circ \alpha_A$.

$2^A \underset{\alpha_1}{\overset{\gamma_1}{\leftrightarrows}} \hat{X}$ 이고 $2^B \underset{\alpha_2}{\overset{\gamma_2}{\leftrightarrows}} \hat{Y}$ 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

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

에서의 단조 함수

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

로 정의하는 "최선의"(정확도를 최대로 유지하는) 방법은

$$\hat{f} = \alpha_B \circ f \circ \gamma_{\hat{A}}$$

이다. 왜 최선인가? 두 가지를 보이면 된다.

- $\alpha \circ f \sqsubseteq \hat{f} \circ \alpha$ 인가?
- 만일 $\alpha \circ f \sqsubseteq \hat{g} \circ \alpha$이면 $\hat{f} \sqsubseteq \hat{g}$인가?

의미구조 요약 예1

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

궁극의 의미구조(*denotational semantics*) 스타일로:

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

확인할 것:

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

구현은:

- 임의의 프로그램 e에 대해서 $[\![\hat{e}]\!]$ 계산
- $[\![\hat{e}]\!]$ 계산은 유한 시간에 끝남

의미구조 요약 예2

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

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

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

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

- $[\![e]\!]$의 정의 1:

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

- $[\![e]\!]$의 정의 2:

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

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

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

요약 상태 전이는

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

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

$$\frac{}{\text{-}\hat{z} \rightarrow \hat{-}\hat{z}}$$

확인할 것:

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

구현은:

- 임의의 프로그램 e에 대해서 $[\![\hat{e}]\!]$ 계산
- $[\![\hat{e}]\!]$ 계산은 유한 시간에 끝남

언어의 확장1

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

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

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

확인할 것:

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

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 있슴.

언어의 확장2: $\top$의 사용

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

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

$$\begin{aligned} read &= \mathbb{Z} \\ \hat{read} &= \top \end{aligned}$$

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

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