# SNU 4541.664A Program Analysis Note 6

Prof. Kwangkeun Yi

요약에 대한 사실과 예들

- 의미공간의 요약 예
- 의미구조의 요약 예

- "$D^\sharp$는 $D$를 요약한 것이다"는

$$D \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} D^\sharp$$

인

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

와

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

가 있을 때를 의미

- 필요하면 $\alpha$와 $\gamma$의 정의구역을 첨자로:

$$\alpha_D, \quad \gamma_{D^\sharp}$$

# 갈로아 연결 예1

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

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

각각의 $\alpha, \gamma$를 알아보자:

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

# $\alpha$와 $\gamma$는 대게 동전의 양면

- $\alpha : D \to D^\sharp$가 연속(*continuous*) 함수이고 $D$가 임의의 부분 집합의 최소 윗뚜껑(*least upper bound*)이 있으면($\sqcup$-*complete*), 갈로아 짝 $\gamma$는

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

- $\gamma : D^\sharp \to D$가 연속(*continuous*) 함수이고 $D^\sharp$가 임의의 부분 집합의 최대 밑뚜껑(*greatest lower bound*)이 있으면($\sqcap$-*complete*), 갈로아 짝 $\alpha$는

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

# $\alpha$와 $\gamma$는 대게 동전의 양면

- $\alpha : D \to D^\sharp$가 연속(*continuous*) 함수이고 $D$가 임의의 부분 집합의 최소 윗뚜껑(*least upper bound*)이 있으면($\sqcup$-*complete*), 갈로아 짝 $\gamma$는

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

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

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

# 갈로아 연결은 조립식

$A$를 요약한 것이 $A^\sharp$ 이고 $B$를 요약한 것이 $B^\sharp$이면,

- $A \times B$를 $A^\sharp \times B^\sharp$로 요약가능

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

- $A + B$를 $A^\sharp + B^\sharp$로 요약가능

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

- $A \to B$를 $A^\sharp \to B^\sharp$로 요약가능

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

# 갈로아 연결은 조립식

$A$를 요약한 것이 $A^\sharp$ 이고 $B$를 요약한 것이 $B^\sharp$이면,

- $A \times B$를 $A^\sharp \times B^\sharp$로 요약가능

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

- $A + B$를 $A^\sharp + B^\sharp$로 요약가능

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

- $A \to B$를 $A^\sharp \to B^\sharp$로 요약가능

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

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

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

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

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

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

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

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

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

- $2^A \to 2^B \leftrightarrows X^\sharp \to Y^\sharp$ 가능

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

# 의미함수의 요약

의미공간 $A$와 $B$ 위에서 정의된 의미함수

$$f \in A \to B$$

를 요약된 의미공간

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

에서의 단조 함수

$$f^\sharp \in A^\sharp \to B^\sharp$$

로 정의하는 "최선의"(정확도를 최대로 유지하는) 방법은

$$f^\sharp = \alpha_B \circ f \circ \gamma_{A^\sharp}$$

이다. 왜 최선인가? 두 가지를 보이면 된다.

- $f \circ \gamma \sqsubseteq \gamma \circ f^\sharp$ 인가?
- 만일 $f \circ \gamma \sqsubseteq \gamma \circ g^\sharp$이면 $f^\sharp \sqsubseteq g^\sharp$인가?

# 의미구조 요약 예1

$$e \;\to\; z \mid e\mathtt{+}e \mid \mathtt{-}e$$

$$\begin{aligned} [\![e]\!] &\in A = 2^{\mathbb{Z}} \\ [\![e]\!]^\sharp &\in A^\sharp \end{aligned}$$

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

$$\begin{aligned} [\![z]\!]^\sharp &= \alpha\{z\} \\ [\![e_1\mathtt{+}e_2]\!]^\sharp &= [\![e_1]\!]^\sharp +^\sharp [\![e_2]\!] \\ [\![\mathtt{-}e]\!]^\sharp &= -^\sharp [\![e]\!]^\sharp \\ a^\sharp +^\sharp b^\sharp &= ? \\ -^\sharp a^\sharp &= ? \end{aligned}$$

확인할 것:

$$\forall e.\alpha(\llbracket e \rrbracket) \sqsubseteq \llbracket e \rrbracket^\sharp \quad \text{또는} \quad \forall e.\llbracket e \rrbracket \sqsubseteq \gamma \llbracket e \rrbracket^\sharp$$

구현은:

- 임의의 프로그램 $e$에 대해서 $\llbracket e \rrbracket^\sharp$ 계산
- $\llbracket e \rrbracket^\sharp$ 계산은 유한 시간에 끝남

# 언어의 확장1

$$
\begin{aligned}
e &\rightarrow \cdots \mid \texttt{if}\ e\ e\ e \\
[\![\texttt{if}\ e_1\ e_2\ e_3]\!] &= \mathit{if}\ [\![e_1]\!]\ [\![e_2]\!]\ [\![e_3]\!] \\
[\![\texttt{if}\ e_1\ e_2\ e_3]\!]^\sharp &= \mathit{if}^\sharp\ [\![e_1]\!]^\sharp\ [\![e_2]\!]^\sharp\ [\![e_3]\!]^\sharp
\end{aligned}
$$

확인할 것:

$$\forall e.\alpha([\![e]\!]) \sqsubseteq [\![e]\!]^\sharp \quad \text{또는} \quad \forall e.[\![e]\!] \sqsubseteq \gamma[\![e]\!]^\sharp$$

# 요약공간 $A^\sharp$에서 $\sqcup$의 두가지 용도

1. $\sqcup$은 $A^\sharp$의 체인에 대해서 정의되 있기만 하면 됨 (요약해석 틀)
2. $\sqcup$이 $A^\sharp$의 임의의 두 원소에 대해서 정의되 있다면, 의미함수 정의에 유용하게 쓰임:

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

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

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

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

# 언어의 확장2: ⊤의 사용

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

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

$$\begin{aligned} \mathit{read} &= \mathbb{Z} \\ \mathit{read}^\sharp &= \top \end{aligned}$$

# 안전한 의미 함수들의 조립은 안전

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

이고 단조(*monotonic*)인 의미함수들 $f, g$가

$$f \circ \gamma_A \sqsubseteq \gamma_B \circ f^\sharp \quad \text{이고} \quad g \circ \gamma_B \sqsubseteq \gamma_C \circ g^\sharp$$

이면

$$(g \circ f) \circ \gamma_A \sqsubseteq \gamma_C \circ (g^\sharp \circ f^\sharp).$$