

## Theorem Problem

# SNU 4541.664A Program Analysis

Spring 2006

Note 9

Prof. Kwangkeun Yi

요약에 대한 사실과 예들  
의미공간의 요약 예  
의미구조의 요약 예

- “ $\hat{D}$ 는  $D$ 를 요약한 것이다”는

$$D \begin{array}{c} \xleftarrow{\gamma} \\ \xrightarrow{\alpha} \end{array} \hat{D}$$

인

요약함수(*abstraction*)  $\alpha : D \rightarrow \hat{D}$

와

구체함수(*concretization*)  $\gamma : \hat{D} \rightarrow D$

가 있을 때를 의미

- 필요하면  $\alpha$ 와  $\gamma$ 의 정의구역을 첨자로:

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

## 갈로아 연결 예1

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

$$2^{\mathbb{Z}} \begin{array}{c} \xleftarrow{\gamma} \\ \xrightarrow{\alpha} \end{array} \hat{A}$$

각각의  $\alpha, \gamma$ 를 알아보자:

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

(왜  $\top$ 은 맨 위에 있어야 할까?)

## $\alpha$ 와 $\gamma$ 는 대계 동전의 양면

- $\alpha : D \rightarrow \hat{D}$ 가 연속(*continuous*)<sup>1</sup> 함수이고  $D$ 가 임의의 부분 집합의 최소 윗뚜껑(*least upper bound*)이 있으면( $\sqcup$ -complete), 갈로아 연결 짝  $\gamma$ 는

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

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

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

<sup>1</sup>단조함수이고 방향성 있는 집합(*directed set*)의 최소 윗뚜껑을 보존

## 갈로아 연결은 조립식

$A$ 를 요약한 것이  $\hat{A}$  이고  $B$ 를 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

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

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

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

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

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

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

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

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

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

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

- $2^A \rightarrow 2^B \iff \hat{X} \rightarrow \hat{Y}$  가능

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

# 의미함수의 요약

의미공간  $A$ 와  $B$  위에서 정의된 의미함수

$$f \in A \rightarrow B$$

를 요약된 의미공간

$$A \begin{array}{c} \xleftarrow{\gamma_A} \\ \xrightarrow{\alpha_A} \end{array} \hat{A} \quad \text{와} \quad B \begin{array}{c} \xleftarrow{\gamma_B} \\ \xrightarrow{\alpha_B} \end{array} \hat{B}$$

위의 함수

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

로 정의하는 “최선의”(정확도를 최대로 유지하는) 방법은

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

이다.



# 의미구조 요약 예1

$$e \rightarrow z \mid e+e \mid -e$$

$$\llbracket e \rrbracket \in A = 2^Z$$

$$\llbracket \hat{e} \rrbracket \in \hat{A}$$

공극의 의미구조(*denotational semantics*) 스타일로:

$$\llbracket z \rrbracket = \{z\}$$

$$\llbracket \hat{z} \rrbracket = \alpha\{z\}$$

$$\llbracket e_1+e_2 \rrbracket = \llbracket e_1 \rrbracket \dot{+} \llbracket e_2 \rrbracket$$

$$\llbracket e_1+\hat{e}_2 \rrbracket = \llbracket \hat{e}_1 \rrbracket \hat{+} \llbracket \hat{e}_2 \rrbracket$$

$$\llbracket -e \rrbracket = \dot{-} \llbracket e \rrbracket$$

$$\llbracket \hat{-e} \rrbracket = \hat{-} \llbracket \hat{e} \rrbracket$$

$$a \dot{+} b = \{x + y \mid x \in a, y \in b\}$$

$$\hat{a} \hat{+} \hat{b} = ?$$

$$\dot{-} a = \{-x \mid x \in a\}$$

$$\hat{-} \hat{a} = ?$$

확인할 것:

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

$$\forall e. [e] \sqsubseteq \gamma[\hat{e}]$$

구현은:

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

## 의미구조 요약 예2

계산과정을 드러내는(*operational semantics*) 방식으로:

$\llbracket e \rrbracket$ 는 상태의 변환과정으로 정의됨

상태 변환 규칙은

$$\frac{e_1 \rightarrow e'_1}{e_1 + e_2 \rightarrow e'_1 + e_2}$$

$$\frac{e \rightarrow e'}{z + e \rightarrow z + e'}$$

$$\frac{e \rightarrow e'}{-e \rightarrow -e'}$$

$$\frac{}{z_1 + z_2 \rightarrow z_1 + z_2}$$

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

- $\llbracket e \rrbracket$ 의 정의 1:

$$\llbracket e \rrbracket \in 2^{(S^*)}, \quad S = \text{Exp}$$

$$\llbracket e \rrbracket = \text{fix} \lambda T. \{e\} \sqcup \{t \rightarrow e'' \mid t \in T \wedge t = \dots \rightarrow e' \wedge e' \rightarrow e''\}$$

where  $T_1 \sqsubseteq T_2$  iff  $\forall t_1 \in T_1. \exists t_2 \in T_2. t_2 = t_1 \rightarrow \dots$

- $\llbracket e \rrbracket$ 의 정의 2:

$$\llbracket e \rrbracket \in S^*, \quad S = 2^{\text{Exp}}$$

$$\llbracket e \rrbracket = \text{fix} \lambda t. \{e\} \sqcup (t \rightarrow X)$$

where  $X = \{e'' \mid t = \dots \rightarrow E \wedge e' \in E \wedge e' \rightarrow e''\}$

요약본  $[[\hat{e}]]$ 는 요약상태의 전환과정으로 정의됨

$$[[\hat{e}]] \in (\hat{S})^*, \quad \hat{S} \xrightleftharpoons[\gamma_{\hat{S}}]{\alpha_S} 2^{Exp}$$

$$[[\hat{e}]] = \text{fix } \lambda \hat{t}. \alpha_S \{e\} \sqcup (\hat{t} \rightarrow \hat{e}')$$

$$\text{where } \hat{t} = \dots \rightarrow \hat{e}_n \wedge \hat{e}_n \rightarrow \hat{e}'$$

요약 상태 전이는

$$\frac{\hat{e}_1 \rightarrow \hat{e}'_1}{\hat{e}_1 + \hat{e}_2 \rightarrow \hat{e}'_1 + \hat{e}_2}$$

$$\frac{\hat{e} \rightarrow \hat{e}'}{\hat{z} + \hat{e} \rightarrow \hat{z} + \hat{e}'}$$

$$\frac{\hat{e} \rightarrow \hat{e}'}{-\hat{e} \rightarrow -\hat{e}'}$$

$$\frac{}{\hat{z}_1 + \hat{z}_2 \rightarrow \hat{z}_1 + \hat{z}_2}$$

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

확인할 것:

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

$$\forall e. [e] \sqsubseteq \gamma[\hat{e}]$$

구현은:

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

## 언어의 확장1

$$e \rightarrow \dots \mid \text{if } e \ e \ e$$

$$\llbracket \text{if } e_1 \ e_2 \ e_3 \rrbracket = \text{if } \llbracket e_1 \rrbracket \llbracket e_2 \rrbracket \llbracket e_3 \rrbracket$$

$$\llbracket \text{if } e_1 \ \hat{e}_2 \ e_3 \rrbracket = \hat{\text{if}} \llbracket \hat{e}_1 \rrbracket \llbracket \hat{e}_2 \rrbracket \llbracket \hat{e}_3 \rrbracket$$

확인할 것:

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

$$\forall e. \llbracket e \rrbracket \sqsubseteq \gamma \llbracket \hat{e} \rrbracket$$

# 요약공간 $\hat{A}$ 에서 $\sqcup$ 의 두가지 용도

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

$$\begin{aligned} \text{if } \llbracket e_1 \rrbracket \llbracket e_2 \rrbracket \llbracket e_3 \rrbracket &= \{z \in \llbracket e_2 \rrbracket \mid 0 \neq n \in \llbracket e_1 \rrbracket\} \\ &\cup \{z \in \llbracket e_3 \rrbracket \mid 0 \in \llbracket e_1 \rrbracket\} \\ \hat{\text{if}} \llbracket \hat{e}_1 \rrbracket \llbracket \hat{e}_2 \rrbracket \llbracket \hat{e}_3 \rrbracket &= ? \end{aligned}$$

만일  $A \xrightleftharpoons[\gamma]{\alpha} \hat{A}$  인 CPO  $A$ 와  $\hat{A}$ 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  $\hat{\text{if}}$ 를  $\sqcup_{\hat{A}}$ 가지고 정의할 수 있음.



언어의 확장2:  $\top$ 의 사용
$$e \rightarrow \dots \mid \text{readin}$$

$$\llbracket \text{readin} \rrbracket = \text{read}$$

$$\llbracket \hat{\text{readin}} \rrbracket = \hat{\text{read}}$$

$$\text{read} = \mathbb{Z}$$

$$\hat{\text{read}} = \top$$

## 안전한 의미 함수들의 조립은 안전

$$\begin{array}{ccc}
 A & \begin{array}{c} \xleftarrow{\gamma_A} \\ \xrightarrow{\alpha_A} \end{array} & \hat{A} \\
 f \downarrow & & \downarrow \hat{f} \\
 B & \begin{array}{c} \xleftarrow{\gamma_B} \\ \xrightarrow{\alpha_B} \end{array} & \hat{B} \\
 g \downarrow & & \downarrow \hat{g} \\
 C & \begin{array}{c} \xleftarrow{\gamma_C} \\ \xrightarrow{\alpha_C} \end{array} & \hat{C}
 \end{array}$$

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

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