# SNU 4541.664A Program Analysis
# Note 7

Prof. Kwangkeun Yi

## 요약해석 디자인과 구현의 예

- 변수가 있는 정수식 프로그램의 요약해석
- 명령형 언어 프로그램의 요약해석

# 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*)

$$\begin{array}{rcl} \underline{E} & \in & 2^{Env} \to 2^{\mathbb{Z}} \\ Env & = & Var \xrightarrow{\text{fin}} \mathbb{Z} \end{array}$$

# 요약들

- 시작: 모듬의미(*collecting semantics*)

$$\begin{array}{rcl} \underline{E} & \in & 2^{Env} \to 2^{\mathbb{Z}} \\ Env & = & Var \xrightarrow{\text{fin}} \mathbb{Z} \end{array}$$

- 요약 일반:

$$2^{Env} \to 2^{\mathbb{Z}} \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} Env^{\#} \to \mathbb{Z}^{\#}, \qquad 2^{Env} \underset{\alpha_1}{\overset{\gamma_1}{\leftrightarrows}} Env^{\#}, \qquad 2^{\mathbb{Z}} \underset{\alpha_2}{\overset{\gamma_2}{\leftrightarrows}} \mathbb{Z}^{\#}$$

이고, 요약 의미 $\underline{E}^{\#}$가

$\underline{E} \circ \gamma_1 \sqsubseteq \gamma_2 \circ \underline{E}^{\#}$ 같은 이야기로 $\alpha_2 \circ \underline{E} \circ \gamma_1 \sqsubseteq \underline{E}^{\#}$

이 되도록.

# 요약들

- 시작: 모듬의미(*collecting semantics*)

$$\begin{array}{rcl} \underline{E} & \in & 2^{Env} \to 2^{\mathbb{Z}} \\ Env & = & Var \stackrel{\text{fin}}{\to} \mathbb{Z} \end{array}$$

- 요약 일반:

$$2^{Env} \to 2^{\mathbb{Z}} \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} Env^{\#} \to \mathbb{Z}^{\#}, \qquad 2^{Env} \underset{\alpha_1}{\overset{\gamma_1}{\leftrightarrows}} Env^{\#}, \qquad 2^{\mathbb{Z}} \underset{\alpha_2}{\overset{\gamma_2}{\leftrightarrows}} \mathbb{Z}^{\#}$$

이고, 요약 의미 $\underline{E}^{\#}$가

$\underline{E} \circ \gamma_1 \sqsubseteq \gamma_2 \circ \underline{E}^{\#}$ 같은 이야기로 $\alpha_2 \circ \underline{E} \circ \gamma_1 \sqsubseteq \underline{E}^{\#}$

이 되도록.

- 요약 예

# 요약들

- 시작: 모듬의미(*collecting semantics*)

$$\begin{array}{rcl} \underline{E} & \in & 2^{Env} \to 2^{\mathbb{Z}} \\ Env & = & Var \stackrel{\text{fin}}{\to} \mathbb{Z} \end{array}$$

- 요약 일반:

$$2^{Env} \to 2^{\mathbb{Z}} \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} Env^{\#} \to \mathbb{Z}^{\#}, \qquad 2^{Env} \underset{\alpha_1}{\overset{\gamma_1}{\leftrightarrows}} Env^{\#}, \qquad 2^{\mathbb{Z}} \underset{\alpha_2}{\overset{\gamma_2}{\leftrightarrows}} \mathbb{Z}^{\#}$$

이고, 요약 의미 $\underline{E}^{\#}$가

$\underline{E} \circ \gamma_1 \sqsubseteq \gamma_2 \circ \underline{E}^{\#}$ 같은 이야기로 $\alpha_2 \circ \underline{E} \circ \gamma_1 \sqsubseteq \underline{E}^{\#}$

이 되도록.

- 요약 예
  - 환경에서 변수간의 관계를 잊어버리기

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

# 요약들

- 시작: 모듬의미(*collecting semantics*)

$$\begin{array}{rcl} \underline{E} & \in & 2^{Env} \to 2^{\mathbb{Z}} \\ Env & = & Var \xrightarrow{\text{fin}} \mathbb{Z} \end{array}$$

- 요약 일반:

$$2^{Env} \to 2^{\mathbb{Z}} \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} Env^{\#} \to \mathbb{Z}^{\#}, \qquad 2^{Env} \underset{\alpha_1}{\overset{\gamma_1}{\leftrightarrows}} Env^{\#}, \qquad 2^{\mathbb{Z}} \underset{\alpha_2}{\overset{\gamma_2}{\leftrightarrows}} \mathbb{Z}^{\#}$$

이고, 요약 의미 $\underline{E}^{\#}$가

$\underline{E} \circ \gamma_1 \sqsubseteq \gamma_2 \circ \underline{E}^{\#}$ 같은 이야기로 $\alpha_2 \circ \underline{E} \circ \gamma_1 \sqsubseteq \underline{E}^{\#}$

이 되도록.

- 요약 예
  - 환경에서 변수간의 관계를 잊어버리기

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

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

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

# 모듬 의미(collecting semantics)

모듬 의미 $\underline{E}$는 아래와 같은 공간에서

$$\begin{array}{rcl} \underline{E} & \in & 2^{Env} \to 2^{\mathbb{Z}} \\ \Sigma & \in & 2^{Env} \\ \sigma & \in & Env = Var \xrightarrow{\text{fin}} \mathbb{Z} \end{array}$$

조립식으로 정의된다:

$$\begin{array}{rcl} \underline{n}\,\Sigma & = & \{n\} \\ \underline{x}\,\Sigma & = & \{\sigma\,x \mid \sigma \in \Sigma\} \\ \underline{E_1 \texttt{ + } E_2}\,\Sigma & = & \{z_1 + z_2 \mid z_i \in \underline{E_i}\,\Sigma\} \\ \underline{\texttt{- } E}\,\Sigma & = & \{-z \mid z \in \underline{E}\,\Sigma\} \\ \underline{\texttt{let}\ x\ E_1\ E_2}\,\Sigma & = & \underline{E_2}\,\{\sigma\{x \mapsto v\} \mid \sigma \in \Sigma,\ v \in \underline{E_1}\,\Sigma\} \\ \underline{\texttt{if}\ E_1\ E_2\ E_3}\,\Sigma & = & \underline{E_2}\,(\mathcal{B}\,E_1\,\Sigma) \cup \underline{E_3}\,(\neg\mathcal{B}\,E_1\,\Sigma) \\ \mathcal{B}\,E\,\Sigma & = & \{\sigma \mid \underline{E}\,\{\sigma\} \neq \{0\}, \sigma \in \Sigma\} \\ \neg\mathcal{B}\,E\,\Sigma & = & \{\sigma \mid \underline{E}\,\{\sigma\} = \{0\}, \sigma \in \Sigma\} \end{array}$$

# 의미공간 요약

요약된 의미 $\underline{E}^{\#}$는 다음의 공간에서

$$\underline{E}^{\#} \in Env^{\#} \to \mathbb{Z}^{\#}$$

정의되고, 의미공간 사이의 갈로아 연결

$$2^{Env} \to 2^{Z} \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} Env^{\#} \to \mathbb{Z}^{\#}$$

은 각 부품의 갈로아 연결

$$2^{Env} \underset{\alpha_1}{\overset{\gamma_1}{\leftrightarrows}} Env^{\#} \quad \text{와} \quad 2^{\mathbb{Z}} \underset{\alpha_2}{\overset{\gamma_2}{\leftrightarrows}} \mathbb{Z}^{\#}$$

를 가지고 안전하게 정의될 수 있다.

# 요약 의미함수 $\underline{E}^{\#}$

요약 의미함수의 정의:

$$
\begin{array}{rcl}
\underline{n}^{\#}\ \Sigma^{\#} & = & \alpha_2\,\{n\} \\
\underline{E_1 \texttt{ + } E_2}^{\#}\ \Sigma^{\#} & = & (\underline{E_1}^{\#}\ \Sigma^{\#}) +^{\#} (\underline{E_2}^{\#}\ \Sigma^{\#}) \\
\underline{\texttt{- } E}^{\#}\ \Sigma^{\#} & = & -^{\#}(\underline{E}^{\#}\ \Sigma^{\#}) \\
\underline{\texttt{let } x\ E_1\ E_2}^{\#}\ \Sigma^{\#} & = & \underline{E_2}^{\#}\ (\Sigma^{\#}\{x \mapsto^{\#} \underline{E_1}^{\#}\ \Sigma^{\#}\}) \\
\underline{\texttt{if } E_1\ E_2\ E_3}^{\#}\ \Sigma^{\#} & = & (\underline{E_2}^{\#}\ (\mathcal{B}^{\#}\ E_1\ \Sigma^{\#})) \cup^{\#} (\underline{E_3}^{\#}\ (\neg\mathcal{B}^{\#}\ E_1\ \Sigma^{\#}))
\end{array}
$$

여기서 $+^{\#}$, $-^{\#}$, $\cdot\{x \mapsto^{\#} \cdot\}$, $\mathcal{B}^{\#}$, $\neg\mathcal{B}^{\#}$, $\cup^{\#}$는 해당 연산들을 안전하게 요약한 것들이어야.

## Theorem (Correctness)

$\forall E : \underline{E} \circ \gamma_1 \sqsubseteq \gamma_2 \circ \underline{E}^{\#}$

표기법: $f \times g = \lambda\langle a, b\rangle.\langle f\ a, g\ b\rangle$, 남용해서도,
$f \times g = \lambda a.\langle f\ a, g\ a\rangle$.

**Proof.** 식 $E$에 대한 귀납법으로 증명한다.

$$
\begin{array}{rcl}
\underline{E_1 \texttt{ + } E_2} & = & \dot{+} \circ \underline{E_1} \times \underline{E_2} \\
\underline{E_1 \texttt{ + } E_2}^{\#} & = & +^{\#} \circ \underline{E_1}^{\#} \times \underline{E_2}^{\#} \\
\underline{\texttt{let}\ x\ E_1\ E_2}^{\#} & = & \underline{E_2}^{\#} \circ \cdot\{x \mapsto^{\#} \cdot\} \circ id \times \underline{E_1}^{\#} \\
\underline{\texttt{if}\ E_1\ E_2\ E_3}^{\#} & = & \cup^{\#} \circ (\underline{E_2}^{\#} \circ \mathcal{B}^{\#}\ E_1) \times (\underline{E_3}^{\#} \circ \neg\mathcal{B}^{\#}\ E_1)
\end{array}
$$

이므로 귀납가정과 안전한 연산자 조건($f \circ \gamma \sqsubset \gamma \circ f^{\#}$)을 이용해서 쉽게 안전함을 보일 수 있다.

# 명령형 언어 프로그램의 요약해석

$$
\begin{array}{rcl}
C & \to & \texttt{skip} \mid x \texttt{ := } E \mid C \texttt{ ; } C \\
 & \mid & \texttt{if } B\ C\ C \\
 & \mid & \texttt{while } B\ C \\
E & \to & n \quad (n \in \mathbb{Z}) \mid x \\
 & \mid & E \texttt{ + } E \mid B \quad \text{(boolean expr)}
\end{array}
$$

의미공간은

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

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

$$\begin{array}{rcl}
\underline{\texttt{skip}}\, M & = & M \\
\underline{x \texttt{ := } E}\, M & = & \{m\{x \mapsto v\} \mid m \in M, v \in \underline{E}\, M\} \\
\underline{C_1 \texttt{ ; } C_2}\, M & = & \underline{C_2}\, (\underline{C_1}\, M) \\
\underline{\texttt{if } B\ C_1\ C_2}\, M & = & \underline{C_1}\, (\underline{B}\, M) \cup \underline{C_2}\, (\underline{\neg B}\, M) \\
\underline{\texttt{while } B\ C}\, M & = & \underline{\neg B}\, (lfp \lambda X.M \cup \underline{C}\, (\underline{B}\, X)) \\
\underline{n}\, M & = & \{n\} \\
\underline{x}\, M & = & \{m\, x \mid m \in M\} \\
\underline{E_1 \texttt{ + } E_2}\, M & = & \{v_1 + v_2 \mid v_1 \in \underline{E_1}\, M, v_2 \in \underline{E_2}\, M\} \\
\underline{B}\, M & = & \{m \mid \underline{B}\, m = T, m \in M\}
\end{array}$$

# 요약

$$\begin{array}{lcl} \underline{C}^{\#} & \in & Memory^{\#} \to Memory^{\#} \\ \underline{E}^{\#} & \in & Memory^{\#} \to Value^{\#} \\ \underline{B}^{\#} & \in & Memory^{\#} \to Memory^{\#} \end{array}$$

갈로아 연결 된 요약공간

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

$$
\begin{array}{rcl}
\underline{\texttt{skip}}^{\#}\ m^{\#} & = & m^{\#} \\
\underline{x\ \texttt{:=}\ E}^{\#}\ m^{\#} & = & m^{\#}\{x \mapsto^{\#} \underline{E}^{\#}\ m^{\#}\} \\
\underline{C_1\ ;\ C_2}^{\#}\ m^{\#} & = & \underline{C_2}^{\#}\ (\underline{C_1}^{\#}\ m^{\#}) \\
\underline{\texttt{if}\ B\ C_1\ C_2}^{\#}\ m^{\#} & = & \underline{C_1}^{\#}\ (\underline{B}^{\#}\ m^{\#})\ \cup^{\#}\ \underline{C_1}^{\#}\ (\underline{\neg B}^{\#}\ m^{\#}) \\
\underline{\texttt{while}\ B\ C}^{\#}\ m^{\#} & = & \underline{\neg B}^{\#}\ (lfp\lambda x^{\#}.m^{\#}\ \cup^{\#}\ \underline{C}^{\#}\ (\underline{B}^{\#}\ x^{\#})) \\
\underline{n}^{\#}\ m^{\#} & = & \alpha_2\{n\} \\
\underline{x}^{\#}\ m^{\#} & = & m^{\#}\ at^{\#}\ x \\
\underline{E_1\ \texttt{+}\ E_2}^{\#}\ m^{\#} & = & (\underline{E_1}^{\#}\ m^{\#})\ +^{\#}\ (\underline{E_2}^{\#}\ m^{\#})
\end{array}
$$

여기서 $+^{\#}$, $\cdot\{x \mapsto^{\#} \cdot\}$, $at^{\#}$, $\cup^{\#}$, $\underline{B}^{\#}$, $\underline{\neg B}^{\#}$는 해당 연산들을 안전하게 요약한 것들이어야.

**Theorem (Correctness)**

$\forall C : \underline{C} \circ \gamma_1 \sqsubseteq \gamma_2 \circ \underline{C}^{\#}$

**Proof.** 경우마다 잘 보면, 이전 증명들과 비슷하게 쉽게 진행된다. 특이한 경우는

$$\begin{aligned} \underline{\texttt{while}\ B\ C}^{\#}\ m^{\#} &= \underline{\neg B}^{\#} \\ & \quad (lfp(F^{\#} \overset{\text{let}}{=} \lambda x^{\#}.m^{\#} \cup^{\#} \underline{C}^{\#}(\underline{B}^{\#} x^{\#}))) \\ \underline{\texttt{while}\ B\ C}(\gamma_1\ m^{\#}) &= \underline{\neg B} \\ & \quad (lfp(F \overset{\text{let}}{=} \lambda X.\gamma_1 m^{\#} \cup \underline{C}\ (\underline{B} X))) \end{aligned}$$

여기서 $F \circ \gamma_1 \sqsubseteq \gamma_1 \circ F^{\#}$을 쉽게 보일 수 있고, 이는 "Fixpoint Transfer Theorem"에 의해 $lfpF \sqsubseteq \gamma_1(lfpF^{\#})$ 이고, $\underline{B}^{\#}$와 $\underline{\neg B}^{\#}$가 안전하다는 가정하에, 쉽게 위의 두 개 사이의 올바른 관계

$$\underline{\neg B}\ lfpF \sqsubseteq \gamma_1(\underline{\neg B}^{\#}\ lfpF^{\#})$$

을 확인 할 수 있다.

# 구현

주어진 프로그램 $C$와, 관심있는 초기 메모리 $m_0^\#$에 대해서 조립식으로 정의된

$$\underline{C}^\# \, m_0^\#$$

를 계산.

- 이때 $C$안에 있는 `while` $E \; C'$에 대해서 $lfpF^\# \in Memory^\#$의 계산은

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

  으로.

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

$$
\begin{array}{rcl}
\underline{\texttt{skip}}^{\#}\ m^{\#} & = & m^{\#} \\
\underline{x\ \texttt{:=}\ E}^{\#}\ m^{\#} & = & m^{\#}\{x \mapsto^{\#} \underline{E}^{\#}\ m^{\#})\} \\
\underline{C_1\ ;\ C_2}^{\#}\ m^{\#} & = & \underline{C_2}^{\#}\ (\underline{C_1}^{\#}\ m^{\#}) \\
\underline{\texttt{if}\ B\ C_1\ C_2}^{\#}\ m^{\#} & = & \underline{C_1}^{\#}\ (\underline{B}^{\#}\ m^{\#})\ \cup^{\#}\ \underline{C_1}^{\#}\ (\underline{\neg B}^{\#}\ m^{\#}) \\
\underline{\texttt{while}\ B\ C}^{\#}\ m^{\#} & = & \underline{\neg B}^{\#} \\
 & & (Narrow(\ Widen\ (\lambda x^{\#}.m^{\#} \cup^{\#}\ \underline{C}^{\#}\ (\underline{B}^{\#}\ x^{\#})))) \\
\underline{n}^{\#}\ m^{\#} & = & \alpha_2\{n\} \\
\underline{x}^{\#}\ m^{\#} & = & m^{\#}\ at^{\#}\ x \\
\underline{E_1\ \texttt{+}\ E_2}^{\#}\ m^{\#} & = & (\underline{E_1}^{\#}\ m^{\#})\ +^{\#}\ (\underline{E_2}^{\#}\ m^{\#})
\end{array}
$$

$$
\begin{aligned}
Widen(F^{\#}) &= \lim_{i\in\mathbb{N}} \begin{cases} Y_0^{\#} &= \bot_{Memory^{\#}} \\ Y_{i+1}^{\#} &= \begin{cases} Y_i^{\#} & \text{if } F^{\#}(Y_i^{\#}) \sqsubseteq Y_i^{\#} \\ Y_i^{\#} \bigtriangledown F^{\#}(Y_i^{\#}) & \text{o.w.} \end{cases} \end{cases} \\
Narrow(m^{\#}) &= \lim_{i\in\mathbb{N}} \begin{cases} Z_0^{\#} &= m^{\#} \\ Z_{i+1}^{\#} &= Z_i^{\#} \bigtriangleup F^{\#}(Z_i^{\#}) \end{cases}
\end{aligned}
$$