퀴즈 3 예시답안

안중원

October 30, 2026

Exercise 1 요약해석 디자인의 올바름 증명을 완성하라. (강의슬라이드 7, 16-17쪽 (명령형 언어 요약해석))

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

모듬의미 공간은

$$\begin{array}{rcl} \underline{C} & \in & 2^{Memory} \to 2^{Memory} \\ \underline{E} & \in & 2^{Memory} \to 2^{Value} \\ \underline{B} & \in & 2^{Memory} \to 2^{Memory} \end{array}$$

$$\begin{array}{rcl} Memory & = & Loc \xrightarrow{\text{fin}} Value \\ Value & = & \mathbb{Z} + \mathbb{B} \\ Loc & = & Var \\ \mathbb{B} & = & \{T, F\} \end{array}$$

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

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

요약의미 공간은

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

갈로아 연결 된 요약공간

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

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

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

요약의미의 올바름은:

Theorem (Correctness)**.**

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

Proof. $\underline{E}^{\#}$의 안전성을 먼저 증명하고, 이를 활용하여 $\underline{C}^{\#}$의 안전성을 증명한다.

$\underline{E}^{\#}$의 안전성은 다음과 같이 표현되며:

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

이는 E의 구조에 대한 귀납법으로 증명할 수 있다.

- $E = n$.

$$\begin{aligned}(\underline{n} \circ \gamma_1)\ m^{\#} &= \{n\} \\ &\subseteq (\gamma_2 \circ \alpha_2)\ \{n\} \\ &= (\gamma_2 \circ \underline{n}^{\#})\ m^{\#}.\end{aligned}$$

- $E = x$.

$$\begin{aligned}(\underline{x} \circ \gamma_1)\ m^{\#} &= \{m\, x \mid m \in \gamma_1(m^{\#})\} \\ &\subseteq \gamma_2(m^{\#}\ at^{\#}\ x) \qquad (at^{\#}\text{의 안전성}) \\ &= (\gamma_2 \circ \underline{x}^{\#})\ m^{\#}.\end{aligned}$$

- $E = B$.
  $\underline{B}^{\#}$의 안전성에 의해 곧바로

$$\underline{B} \circ \gamma_1 \sqsubseteq \gamma_2 \circ \underline{B}^{\#}.$$

- $E = E_1 \texttt{ + } E_2$.
  ${\underline{E_1}}^{\#}$와 ${\underline{E_2}}^{\#}$의 안전성을 가정하면,

$$\begin{aligned}(\underline{E_1 \texttt{ + } E_2} \circ \gamma_1)\ m^{\#} &= \{v_1 + v_2 \mid v_1 \in \underline{E_1}\,\gamma_1(m^{\#}), v_2 \in \underline{E_2}\,\gamma_1(m^{\#})\} \\ &\subseteq \{v_1 + v_2 \mid v_1 \in \gamma_2({\underline{E_1}}^{\#}\ m^{\#}), v_2 \in \gamma_2({\underline{E_2}}^{\#}\ m^{\#})\} \qquad ({\underline{E_1}}^{\#}\text{ 및 }{\underline{E_2}}^{\#}\text{의 안전성}) \\ &\subseteq \gamma_2(({\underline{E_1}}^{\#}\ m^{\#}) +^{\#} ({\underline{E_2}}^{\#}\ m^{\#})) \qquad (+^{\#}\text{의 안전성}) \\ &= (\gamma_2 \circ \underline{E_1 \texttt{ + } E_2}^{\#})\ m^{\#}.\end{aligned}$$

귀납법에 의해 모든 E에 대해 $\underline{E}^{\#}$은 안전하다.

이어서 $\underline{C}^{\#}$의 안전성도 C의 구조에 대한 귀납법으로 증명한다.

- $C = \texttt{skip}$.

$$\begin{aligned}\underline{\texttt{skip}} \circ \gamma_1 &= \gamma_1 \\ &= \gamma_1 \circ \underline{\texttt{skip}}^{\#}.\end{aligned}$$

- $C = x \texttt{ := } E$.

$$\begin{aligned}(\underline{x \texttt{ := } E} \circ \gamma_1)\ m^{\#} &= \{m\{x \mapsto v\} \mid m \in \gamma_1(m^{\#}), v \in \underline{E}\,\gamma_1(m^{\#})\} \\ &\subseteq \{m\{x \mapsto v\} \mid m \in \gamma_1(m^{\#}), v \in \gamma_2(\underline{E}^{\#}\ m^{\#})\} \qquad (\underline{E}^{\#}\text{의 안전성}) \\ &\subseteq \gamma_1(m^{\#}\{x \mapsto^{\#} \underline{E}^{\#}\ m^{\#}\}) \qquad (\cdot\{x \mapsto^{\#} \cdot\}\text{의 안전성}) \\ &= (\gamma_1 \circ \underline{x \texttt{ := } E}^{\#})\ m^{\#}.\end{aligned}$$

- $C = C_1 \,;\, C_2$.
  ${\underline{C_1}}^{\#}$와 ${\underline{C_2}}^{\#}$의 안전성을 가정하면,

$$\begin{aligned}\underline{C_1 \,;\, C_2} \circ \gamma_1 &= \underline{C_2} \circ \underline{C_1} \circ \gamma_1 \\ &\sqsubseteq \underline{C_2} \circ \gamma_1 \circ {\underline{C_1}}^{\#} \qquad (\underline{C_2}\text{의 단조성과 }{\underline{C_1}}^{\#}\text{의 안전성}) \\ &\sqsubseteq \gamma_1 \circ {\underline{C_2}}^{\#} \circ {\underline{C_1}}^{\#} \qquad ({\underline{C_2}}^{\#}\text{의 안전성}) \\ &= \gamma_1 \circ \underline{C_1 \,;\, C_2}^{\#}.\end{aligned}$$

- $C = \texttt{if}\ B\ C_1\ C_2$.
  $\underline{C_1}^{\#}$, $\underline{C_2}^{\#}$의 안전성을 가정하면,

$$\begin{aligned}
(\underline{\texttt{if}\ B\ C_1\ C_2} \circ \gamma_1)\ m^{\#} &= \underline{C_1}\,(\underline{B}\,\gamma_1(m^{\#})) \cup \underline{C_2}\,(\underline{\neg B}\,\gamma_1(m^{\#})) \\
&\subseteq \underline{C_1}\,\gamma_1(\underline{B}^{\#}\ m^{\#}) \cup \underline{C_2}\,\gamma_1(\underline{\neg B}^{\#}\ m^{\#}) \qquad (\underline{C_1}\text{ 및 }\underline{C_2}\text{의 단조성과 }\underline{B}^{\#}\text{ 및 }\underline{\neg B}^{\#}\text{의 안전성}) \\
&\subseteq \gamma_1(\underline{C_1}^{\#}\ (\underline{B}^{\#}\ m^{\#})) \cup \gamma_1(\underline{C_2}^{\#}\ (\underline{\neg B}^{\#}\ m^{\#})) \qquad (\underline{C_1}^{\#}\text{ 및 }\underline{C_2}^{\#}\text{의 안전성}) \\
&\subseteq \gamma_1(\underline{C_1}^{\#}\ (\underline{B}^{\#}\ m^{\#}) \cup^{\#}\ \underline{C_2}^{\#}\ (\underline{\neg B}^{\#}\ m^{\#})) \qquad (\cup^{\#}\text{의 안전성}) \\
&= (\gamma_1 \circ \underline{\texttt{if}\ B\ C_1\ C_2}^{\#})\ m^{\#}.
\end{aligned}$$

- $C = \texttt{while}\ B\ C'$.
  $\underline{C'}^{\#}$의 안전성을 가정한다. 좌변과 우변을 풀어쓰면:

$$(\underline{\texttt{while}\ B\ C'} \circ \gamma_1)\ m^{\#} = \underline{\neg B}\,(\mathit{lfp}\ \lambda X.\gamma_1(m^{\#}) \cup \underline{C'}\,(\underline{B}\,X)),$$
$$(\gamma_1 \circ \underline{\texttt{while}\ B\ C'}^{\#})\ m^{\#} = \gamma_1(\underline{\neg B}^{\#}\ (\mathit{lfp}\ \lambda x^{\#}.m^{\#} \cup^{\#} \underline{C'}^{\#}\ (\underline{B}^{\#}\ x^{\#}))).$$

  F와 $F^{\#}$를 다음과 같이 정의하면:

$$F(X) = \gamma_1(m^{\#}) \cup \underline{C'}\,(\underline{B}\,X), \qquad F^{\#}(x^{\#}) = m^{\#} \cup^{\#} \underline{C'}^{\#}\ (\underline{B}^{\#}\ x^{\#}),$$

  $F \circ \gamma_1 \sqsubseteq \gamma_1 \circ F^{\#}$를 보인 다음 고정점 전달 정리(fixpoint transfer theorem)을 적용할 수 있다.

$$\begin{aligned}
(F \circ \gamma_1)\ x^{\#} &= \gamma_1(m^{\#}) \cup \underline{C'}\,(\underline{B}\,\gamma_1(x^{\#})) \\
&\subseteq \gamma_1(m^{\#}) \cup \underline{C'}(\gamma_1(\underline{B}^{\#}\ x^{\#})) \qquad (\underline{C'}\text{의 단조성과 }\underline{B}^{\#}\text{의 안전성}) \\
&\subseteq \gamma_1(m^{\#}) \cup \gamma_1(\underline{C'}^{\#}\ (\underline{B}^{\#}\ x^{\#})) \qquad (\underline{C'}^{\#}\text{의 안전성}) \\
&\subseteq \gamma_1(m^{\#} \cup^{\#} \underline{C'}^{\#}\ (\underline{B}^{\#}\ x^{\#})) \qquad (\cup^{\#}\text{의 안전성}) \\
&= (\gamma_1 \circ F^{\#})\ x^{\#}.
\end{aligned}$$

  따라서,

$$\begin{aligned}
(\underline{\texttt{while}\ B\ C'} \circ \gamma_1)\ m^{\#} &= \underline{\neg B}\,(\mathit{lfp}\ F) \\
&\subseteq \underline{\neg B}\,\gamma_1(\mathit{lfp}\ F^{\#}) \qquad (\text{고정점 전달 정리와 }\underline{\neg B}\text{의 단조성}) \\
&\subseteq \gamma_1(\underline{\neg B}^{\#}\ (\mathit{lfp}\ F^{\#})) \qquad (\underline{\neg B}^{\#}\text{의 안전성}) \\
&= (\gamma_1 \circ \underline{\texttt{while}\ B\ C'}^{\#})\ m^{\#}.
\end{aligned}$$

귀납법에 의해 모든 C에 대해 $\underline{C}^{\#}$은 안전하다. □