퀴즈 4 예시답안

안중원

2026년 11월 3일

Exercise 1 요약해석 디자인의 올바름 증명을 완성하라. (강의슬라이드 8-1, 8쪽, fixpoint induction)

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

모둠의미는 아래 방정식 $\mathcal{F}$의 최소해 $lfp\mathcal{F}$로 정의된다.

$$\begin{array}{rl} & \mathcal{F} \in (Cmd \to 2^{Mem} \to 2^{Mem}) \to (Cmd \to 2^{Mem} \to 2^{Mem}) \\ \mathcal{F}(f) = & \lambda C.\,\lambda M. \\ & \quad \texttt{case}\ C\ \texttt{of} \\ & \qquad \begin{array}{ll} \texttt{skip} & \Rightarrow M \\ x \texttt{ := } E & \Rightarrow update_x(M, \mathcal{E}\ E\ M) \\ C_1;C_2 & \Rightarrow f\ C_2\ (f\ C_1\ M) \\ \texttt{if } B\ C_1\ C_2 & \Rightarrow f\ C_1\ (trim_B M) \cup f\ C_2\ (trim_{\neg B} M) \\ \texttt{while } B\ C_0 & \Rightarrow trim_{\neg B}\big(M \cup f\ (\texttt{while } B\ C_0)\ (f\ C_0\ (trim_B M))\big) \end{array} \end{array}$$

여기서 $update_x, \mathcal{E}, trim_B$은 연속함수로 정의된 연산자다.

$$update_x : 2^{Mem} \times 2^{Val} \to 2^{Mem} \qquad \mathcal{E} : Exp \to 2^{Mem} \to 2^{Val} \qquad trim_B : 2^{Mem} \to 2^{Mem}$$

요약공간의 갈로아 연결은

$$2^{Mem} \underset{\alpha_M}{\overset{\gamma_M}{\leftrightarrows}} Mem^\# \qquad 2^{Val} \underset{\alpha_V}{\overset{\gamma_V}{\leftrightarrows}} Val^\#$$

요약의미는 $\mathcal{F}$의 요약 버전 $\mathcal{F}^\#$의 최소고정점 $lfp\mathcal{F}^\#$로 정의된다.

$$\begin{array}{rl} & \mathcal{F}^\# \in (Cmd \to Mem^\# \to Mem^\#) \to (Cmd \to Mem^\# \to Mem^\#) \\ \mathcal{F}^\#(f^\#) = & \lambda C.\,\lambda M^\#. \\ & \quad \texttt{case}\ C\ \texttt{of} \\ & \qquad \begin{array}{ll} \texttt{skip} & \Rightarrow M^\# \\ x \texttt{ := } E & \Rightarrow update_x^\#(M^\#, \mathcal{E}^\# E\ M^\#) \\ C_1;C_2 & \Rightarrow f^\#\ C_2\ (f^\#\ C_1\ M^\#) \\ \texttt{if } B\ C_1\ C_2 & \Rightarrow f^\#\ C_1\ (trim_B^\# M^\#) \cup^\# f^\#\ C_2\ (trim_{\neg B}^\#\ M^\#) \\ \texttt{while } B\ C_0 & \Rightarrow trim_{\neg B}^\#\big(M^\# \cup^\# f^\#(\texttt{while } B\ C_0)\ (f^\#\ C_0\ (trim_B^\#\ M^\#))\big). \end{array} \end{array}$$

여기서 $\cup^\#, update_x^\#, \mathcal{E}^\#, trim_B^\#$은 해당 연산들을 안전하게 요약한 것들이다.

$$\cup \circ (\gamma_M \times \gamma_M) \sqsubseteq \gamma_M \circ \cup^\# \qquad update_x \circ (\gamma_M \times \gamma_V) \sqsubseteq \gamma_M \circ update_x^\#$$
$$\mathcal{E}\ E \circ \gamma_M \sqsubseteq \gamma_V \circ \mathcal{E}^\#\ E \qquad trim_B \circ \gamma_M \sqsubseteq \gamma_M \circ trim_B^\#.$$

이때 $\langle f, g\rangle = \lambda x.\langle f(x), g(x)\rangle$ 그리고 $f \times g = \lambda\langle x, y\rangle.\langle f(x), g(y)\rangle$.

증명할 요약의미의 안전성은

$$\forall C : \quad lfp\mathcal{F}\ C \circ \gamma_M \ \sqsubseteq\ \gamma_M \circ lfp\mathcal{F}^\#\ C.$$

예시답안

Proof. 아래의 Q에 고정점 귀납법(fixpoint induction)을 적용하여 요약의미의 안전성을 증명한다.

$$Q\langle f, f^{\#}\rangle \quad \Longleftrightarrow \quad \forall C: \quad f\ C\ \circ \gamma_M \sqsubseteq \gamma_M \circ f^{\#}\ C.$$

이때 Q는 포함성질(inclusive)이다: 체인 $\{\langle f_i, f_i^{\#}\rangle\}_i$가 Q를 만족하면 그 최소윗뚜껑(least upper bound)도 Q를 만족한다:

$$\begin{aligned}
\left(\bigsqcup_i f_i\right)\ C\ \circ \gamma_M &= \bigsqcup_i (f_i\ C\ \circ \gamma_M) \\
&\sqsubseteq \bigsqcup_i (\gamma_M \circ f_i^{\#}\ C) && (\text{각 } i\text{에서 } Q\text{를 만족}) \\
&\sqsubseteq \gamma_M \circ \left(\bigsqcup_i f_i^{\#}\right)\ C. && (\gamma_M\text{의 단조성})
\end{aligned}$$

Base. 바닥 원소는 $\langle \lambda C.\lambda M.\emptyset,\ \lambda C.\lambda M^{\#}.\bot^{\#}\rangle$이다.

$$\begin{aligned}
(\lambda C.\lambda M.\emptyset)\ C\ \gamma_M(M^{\#}) &= \emptyset \\
&\sqsubseteq \gamma_M(\bot^{\#}) \\
&= \gamma_M\ ((\lambda C.\lambda M^{\#}.\bot^{\#})\ C\ M^{\#}).
\end{aligned}$$

따라서 $Q\langle \lambda C.\lambda M.\emptyset,\ \lambda C.\lambda M^{\#}.\bot^{\#}\rangle$이다.

Induction. 귀납가정 $Q\langle f, f^{\#}\rangle$를 가정하고:

$$\forall C: \quad f\ C\ \circ \gamma_M \sqsubseteq \gamma_M \circ f^{\#}\ C,$$

$Q\langle \mathcal{F}(f), \mathcal{F}^{\#}(f^{\#})\rangle$를 보이자:

$$\forall C: \quad \mathcal{F}(f)\ C\ \circ \gamma_M \sqsubseteq \gamma_M \circ \mathcal{F}^{\#}(f^{\#})\ C.$$

증명은 C의 각 경우를 나누어 진행한다.

- $C = \texttt{skip}$.

$$\begin{aligned}
\mathcal{F}(f)\ \texttt{skip} \circ \gamma_M &= \gamma_M \\
&= \gamma_M \circ \mathcal{F}^{\#}(f^{\#})\ \texttt{skip}.
\end{aligned}$$

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

$$\begin{aligned}
&\mathcal{F}(f)\ (x\ \texttt{:=}\ E) \circ \gamma_M \\
&= \mathit{update}_x \circ \langle \gamma_M, \mathcal{E}\ E \circ \gamma_M\rangle \\
&\sqsubseteq \mathit{update}_x \circ \langle \gamma_M, \gamma_V \circ \mathcal{E}^{\#} E\rangle && (\mathcal{E}^{\#}\text{의 안전성}, \mathit{update}_x\text{의 단조성}) \\
&= \mathit{update}_x \circ (\gamma_M \times \gamma_V) \circ \langle \mathit{id}, \mathcal{E}^{\#} E\rangle \\
&\sqsubseteq \gamma_M \circ \mathit{update}_x^{\#} \circ \langle \mathit{id}, \mathcal{E}^{\#} E\rangle && (\mathit{update}_x^{\#}\text{의 안전성}) \\
&= \gamma_M \circ \mathcal{F}^{\#}(f^{\#})\ (x\ \texttt{:=}\ E).
\end{aligned}$$

- $C = C_1; C_2$.

$$\begin{aligned}
\mathcal{F}(f)\ (C_1; C_2) \circ \gamma_M &= f\ C_2 \circ f\ C_1 \circ \gamma_M \\
&\sqsubseteq f\ C_2 \circ \gamma_M \circ f^{\#}\ C_1 && (\text{귀납가정}, f\ C_2\text{의 단조성}) \\
&\sqsubseteq \gamma_M \circ f^{\#}\ C_2 \circ f^{\#}\ C_1 && (\text{귀납가정}) \\
&= \gamma_M \circ \mathcal{F}^{\#}(f^{\#})\ (C_1; C_2).
\end{aligned}$$

- $C = \texttt{if}\ B\ C_1\ C_2$.

$$
\begin{aligned}
&\mathcal{F}(f)\ (\texttt{if}\ B\ C_1\ C_2) \circ \gamma_M \\
&= \cup \circ \langle f\ C_1 \circ \mathit{trim}_B \circ \gamma_M, f\ C_2 \circ \mathit{trim}_{\neg B} \circ \gamma_M \rangle \\
&\sqsubseteq \cup \circ \langle f\ C_1 \circ \gamma_M \circ \mathit{trim}^{\#}_B, f\ C_2 \circ \gamma_M \circ \mathit{trim}^{\#}_{\neg B} \rangle && (\mathit{trim}^{\#}_B, \mathit{trim}^{\#}_{\neg B}\text{의 안전성} \\
&&& f\ C_1, f\ C_2, \cup\text{의 단조성}) \\
&\sqsubseteq \cup \circ \langle \gamma_M \circ f^{\#}\ C_1 \circ \mathit{trim}^{\#}_B, \gamma_M \circ f^{\#}\ C_2 \circ \mathit{trim}^{\#}_{\neg B} \rangle && (\text{귀납가정}, \cup\text{의 단조성}) \\
&= \cup \circ (\gamma_M \times \gamma_M) \circ \langle f^{\#}\ C_1 \circ \mathit{trim}^{\#}_B, f^{\#}\ C_2 \circ \mathit{trim}^{\#}_{\neg B} \rangle \\
&\sqsubseteq \gamma_M \circ \cup^{\#} \circ \langle f^{\#}\ C_1 \circ \mathit{trim}^{\#}_B, f^{\#}\ C_2 \circ \mathit{trim}^{\#}_{\neg B} \rangle && (\cup^{\#}\text{의 안전성}) \\
&= \gamma_M \circ \mathcal{F}^{\#}(f^{\#})\ (\texttt{if}\ B\ C_1\ C_2).
\end{aligned}
$$

- $C = \texttt{while}\ B\ C_0$.

$$
\begin{aligned}
&\mathcal{F}(f)\ C \circ \gamma_M \\
&= \mathit{trim}_{\neg B} \circ \cup \circ \langle \gamma_M, f\ C \circ f\ C_0 \circ \mathit{trim}_B \circ \gamma_M \rangle \\
&\sqsubseteq \mathit{trim}_{\neg B} \circ \cup \circ \langle \gamma_M, f\ C \circ f\ C_0 \circ \gamma_M \circ \mathit{trim}^{\#}_B \rangle && (\mathit{trim}^{\#}_B\text{의 안전성}, \\
&&& f\ C_0, f\ C, \cup, \mathit{trim}_{\neg B}\text{의 단조성}) \\
&\sqsubseteq \mathit{trim}_{\neg B} \circ \cup \circ \langle \gamma_M, f\ C \circ \gamma_M \circ f^{\#}\ C_0 \circ \mathit{trim}^{\#}_B \rangle && (\text{귀납가정}, f\ C, \cup, \mathit{trim}_{\neg B}\text{의 단조성}) \\
&\sqsubseteq \mathit{trim}_{\neg B} \circ \cup \circ \langle \gamma_M, \gamma_M \circ f^{\#}\ C \circ f^{\#}\ C_0 \circ \mathit{trim}^{\#}_B \rangle && (\text{귀납가정}, \cup, \mathit{trim}_{\neg B}\text{의 단조성}) \\
&= \mathit{trim}_{\neg B} \circ \cup \circ (\gamma_M \times \gamma_M) \circ \langle \mathit{id}, f^{\#}\ C \circ f^{\#}\ C_0 \circ \mathit{trim}^{\#}_B \rangle \\
&\sqsubseteq \mathit{trim}_{\neg B} \circ \gamma_M \circ \cup^{\#} \circ \langle \mathit{id}, f^{\#}\ C \circ f^{\#}\ C_0 \circ \mathit{trim}^{\#}_B \rangle && (\cup^{\#}\text{의 안전성}, \mathit{trim}_{\neg B}\text{의 단조성}) \\
&\sqsubseteq \gamma_M \circ \mathit{trim}^{\#}_{\neg B} \circ \cup^{\#} \circ \langle \mathit{id}, f^{\#}\ C \circ f^{\#}\ C_0 \circ \mathit{trim}^{\#}_B \rangle && (\mathit{trim}^{\#}_{\neg B}\text{의 안전성}) \\
&= \gamma_M \circ \mathcal{F}^{\#}(f^{\#})\ C.
\end{aligned}
$$

고정점 귀납법에 의해 $Q\langle \mathit{lfp}\mathcal{F}, \mathit{lfp}\mathcal{F}^{\#} \rangle$가 성립하며, 따라서 요약의미의 안전성이 증명된다:

$$\forall C: \quad \mathit{lfp}\mathcal{F}\ C \circ \gamma_M\ \sqsubseteq\ \gamma_M \circ \mathit{lfp}\mathcal{F}^{\#}\ C.$$

□