숙제 2 예시답안

안중원

November 18, 2026

이번 숙제의 목적은, 특별한 방식의 정적분석을 이해하고 그것을 요약해석틀에서 정의될 수 있음을 확인하는 것이다.

- 강의 슬라이드 `10.pdf` 의 "Static Analysis by Monotonic Cloure"에서 예시로 보인 "point-to" 분석을 요약해석틀에서 정의하라.
- 요약공간이 무엇이고 요약의미함수가 무엇인지 정의하고, 올바름을 증명하라.

풀이 요약 한단계실행(transition relation)으로 도달가능한 상태의 집합으로 모듬실행의미를 정의하고, 이에 대한 요약공간과 요약의미함수로 point-to 분석을 정의하여 올바름을 보인다.

문법과 모듬실행의미 각 프로그램 P는 하나의 명령 C로 구성된다. 명령, 좌변, 우변의 문법은 다음과 같다.

$$\begin{array}{rcl} C \in \mathcal{C} & ::= & L \coloneqq R \mid C; C \mid \texttt{while}\ B\ C \\ L \in \mathcal{L} & ::= & x \mid *x \\ R \in \mathcal{R} & ::= & n \mid x \mid *x \mid \&x \end{array}$$

논리식, 변수, 상수 집합은 아래와 같이 주어져있다고 가정한다.

$$B \in \mathcal{B}, \qquad x \in \mathbb{X}, \qquad n \in \mathbb{N}.$$

프로그램 P에 등장하는 명령의 집합을 $\mathcal{C}_P \subseteq \mathcal{C} \cup \{\text{end}\}$라고 할 때, 실행공간은 다음과 같다.

$$\begin{aligned} \mathbb{V} &\triangleq \mathbb{N} + \mathbb{X} \\ \mathbb{M} &\triangleq \mathbb{X} \rightharpoonup \mathbb{V} \\ \mathbb{S} &\triangleq \mathcal{C}_P \times \mathbb{M} \end{aligned}$$

이때 $\rightharpoonup$는 부분함수(partial function)를 의미한다. 부분함수에서 정의되지 않은 입력에 대해서는 $\bot$을 반환하는 것으로 쓴다. 이를테면 메모리 $m \in \mathbb{M}$에 대해 x가 정의되지 않은 경우 $m\,x = \bot$이다. 상태 $(C, m) \in \mathbb{S}$는 명령 C 직전의 메모리 m를 의미하고, $(\text{end}, m) \in \mathbb{S}$는 프로그램이 종료되었을 때 메모리가 m임을 의미한다.

우변의 실행의미 $[\![R]\!] \in \mathbb{M} \rightharpoonup \mathbb{V}$는 각 경우에 대해 다음과 같이 정의된다.

$$\begin{aligned} [\![n]\!]\, m &\triangleq n \\ [\![x]\!]\, m &\triangleq m\,x \\ [\![*x]\!]\, m &\triangleq m\,(m\,x) \qquad m\,x \in \mathbb{X} \\ [\![\&x]\!]\, m &\triangleq x \end{aligned}$$

나머지 경우에는 $[\![R]\!]\, m = \bot$으로 정의한다. 논리식의 실행의미는 $[\![B]\!] \in \mathbb{M} \rightharpoonup \{\text{true}, \text{false}\}$로 주어졌다고 가정한다.

각 명령의 다음 명령을 구하는 함수는 $\text{next}, \text{nextTrue}, \text{nextFalse} \in \mathcal{C}_P \rightharpoonup \mathcal{C}_P$로 정의된다. 이들 명령어의 자세한 정의는 요약의미에서는 중요하지 않으므로 생략한다.

한단계실행 $\hookrightarrow \subseteq \mathbb{S} \times \mathbb{S}$는 다음과 같이 정의된다. 각 규칙에서 C는 이전 명령을 의미한다.

$$\begin{array}{rcll} (x \coloneqq R, m) & \hookrightarrow & (\text{next}(C), m[x \mapsto [\![R]\!]\, m]) & \text{if } [\![R]\!]\, m \neq \bot \\ (*x \coloneqq R, m) & \hookrightarrow & (\text{next}(C), m[m\,x \mapsto [\![R]\!]\, m]) & \text{if } m\,x \in \mathbb{X}, [\![R]\!]\, m \neq \bot \\ (C_1; C_2, m) & \hookrightarrow & (\text{next}(C), m) & \\ (\texttt{while}\ B\ C_0, m) & \hookrightarrow & (\text{nextTrue}(C), m) & \text{if } [\![B]\!]\, m = \text{true} \\ (\texttt{while}\ B\ C_0, m) & \hookrightarrow & (\text{nextFalse}(C), m) & \text{if } [\![B]\!]\, m = \text{false} \end{array}$$

프로그램 P의 모음실행의미 $[\![P]\!] \in \wp(\mathbb{S})$는 다음과 같이 정의된다.

$$
\begin{aligned}
I &\triangleq \{(P, \bot)\} \\
\mathit{Step}(S) &\triangleq \{s' \mid s \in S, s \hookrightarrow s'\} \\
F(S) &\triangleq I \cup \mathit{Step}(S) \\
[\![P]\!] &\triangleq \mathrm{lfp}\, F
\end{aligned}
$$

이때 $(P, \bot)$은 프로그램 P의 시작 상태에 빈 메모리 $\bot$가 주어졌음을 의미한다.

요약공간 요약공간 $\mathbb{S}^\#$과 복원함수(concretization) γ는 다음과 같이 정의된다.

$$
\begin{aligned}
\mathbb{S}^\# &\triangleq \wp(\mathbb{X} \times \mathbb{X}) \qquad \gamma \in \mathbb{S}^\# \to \wp(\mathbb{S}) \\
\gamma(s^\#) &\triangleq \{(C, m) \in \mathbb{S} \mid \forall x, y \in \mathbb{X} : \; m\, x = y \implies (x \to y) \in s^\#\}
\end{aligned}
$$

Point-to 분석에서 모아가는 $x \to y$ 관계는 요약상태 $s^\# \in \mathbb{S}^\#$의 원소로 표현된다. γ의 단조성은 자명하다: $s_1^\# \subseteq s_2^\#$일 때,

$$
\begin{aligned}
(C, m) \in \gamma(s_1^\#) &\implies \forall x, y \in \mathbb{X} : \; m\, x = y \implies (x \to y) \in s_1^\# \\
&\qquad\qquad\qquad\qquad\qquad\qquad \subseteq s_2^\# \\
&\implies (C, m) \in \gamma(s_2^\#)
\end{aligned}
$$

요약의미함수 각 우변식 $R \in \mathcal{R}$에 대해 요약의미함수 $[\![R]\!]^\# \in \mathbb{S}^\# \to \wp(\mathbb{X})$는 다음과 같이 정의된다.

$$
\begin{aligned}
[\![n]\!]^\# \, s^\# &\triangleq \emptyset & [\![x]\!]^\# \, s^\# &\triangleq \{y \mid (x \to y) \in s^\#\} \\
[\![{*x}]\!]^\# \, s^\# &\triangleq \{z \mid (x \to y), (y \to z) \in s^\#\} & [\![\&x]\!]^\# \, s^\# &\triangleq \{x\}
\end{aligned}
$$

각 명령 $C \in \mathcal{C}_P$에 대해 요약의미함수 $[\![C]\!]^\# \in \mathbb{S}^\# \to \mathbb{S}^\#$는 다음과 같이 정의된다.

$$
\begin{aligned}
[\![x \coloneqq R]\!]^\# \, s^\# &\triangleq s^\# \cup \{(x \to y) \mid y \in [\![R]\!]^\# \, s^\#\} \\
[\![{*x} \coloneqq R]\!]^\# \, s^\# &\triangleq s^\# \cup \{(y \to z) \mid (x \to y) \in s^\#, z \in [\![R]\!]^\# \, s^\#\} \\
[\![C]\!]^\# \, s^\# &\triangleq s^\# \qquad \text{otherwise}
\end{aligned}
$$

이 정의가 강의자료의 point-to 정의와 동일함은 자명하다.

프로그램의 요약의미 $[\![P]\!]^\# \in \mathbb{S}^\#$는 다음과 같이 정의된다.

$$
\begin{aligned}
I^\# &\triangleq \emptyset & \mathit{Step}^\#(s^\#) &\triangleq \bigcup_{C \in \mathcal{C}_P} [\![C]\!]^\# \, s^\# \\
F^\#(s^\#) &\triangleq I^\# \cup \mathit{Step}^\#(s^\#) & [\![P]\!]^\# &\triangleq \mathrm{lfp}\, F^\#
\end{aligned}
$$

올바름 증명 요약의미의 올바름(soundness)은 각 우변식과 명령 요약의미의 올바름으로부터 증명할 수 있다.

Lemma 1. *각 우변식의 요약의미함수 $[\![R]\!]^\#$는 올바르다: 요약상태 $s^\# \in \mathbb{S}^\#$에 대해, 다음이 성립한다.*

$$
\forall (C, m) \in \gamma(s^\#) : \; [\![R]\!]\, m \in \mathbb{X} \implies [\![R]\!]\, m \in [\![R]\!]^\# \, s^\#
$$

Proof. 복원 조건 $(C, m) \in \gamma(s^\#)$를 풀어쓰면 다음과 같다.

$$
\forall a, b \in \mathbb{X} : \; m\, a = b \implies (a \to b) \in s^\# \tag{1}
$$

조건 (1)이 주어졌을 때, 우변식의 각 경우에 대해 증명한다.

- $R = n$. 이 경우 $[\![R]\!]\, m = n$이고, $n \notin \mathbb{X}$이므로 전제가 성립하지 않는다.
- $R = x$. 이 경우 $[\![R]\!]\, m = m\, x \in \mathbb{X}$이다. (1)에 의해 $(x \to m\, x) \in s^\#$이므로,

$$
[\![R]\!]\, m = m\, x \in \{y \mid (x \to y) \in s^\#\} = [\![R]\!]^\# \, s^\#.
$$

- $R = *x$. 이 경우 $[\![R]\!]\, m = m\,(m\,x)$이고 $m\,x, m\,(m\,x) \in \mathbb{X}$이다. (1)에 의해 $(x \to m\,x), (m\,x \to m\,(m\,x)) \in s^\#$이므로,

$$[\![R]\!]\, m = m\,(m\,x) \in \{z \mid (x \to y), (y \to z) \in s^\#\} = [\![R]\!]^\#\, s^\#.$$

- $R = \&x$. 이 경우 $[\![R]\!]\, m = x$이다. 따라서,

$$[\![R]\!]\, m = x \in \{x\} = [\![R]\!]^\#\, s^\#. \qquad \square$$

Lemma 2. *각 명령의 요약의미함수 $[\![C]\!]^\#$ 는 올바르다: 요약상태 $s^\# \in \mathbb{S}^\#$ 와 상태 $(C, m) \in \gamma(s^\#)$ 에 대해, 다음이 성립한다.*

$$\forall (C', m') \in \mathbb{S} :\ (C, m) \hookrightarrow (C', m') \implies (C', m') \in \gamma([\![C]\!]^\#\, s^\#)$$

Proof. 복원 조건 $(C, m) \in \gamma(s^\#)$을 (1)에서와 같이 풀어쓸 수 있다:

$$\forall a, b \in \mathbb{X} :\ m\,a = b \implies (a \to b) \in s^\#.$$

이 조건이 주어졌을 때, $m'\,a = b$인 모든 $a, b \in \mathbb{X}$에 대해 다음을 보여야 한다.

$$(a \to b) \in [\![C]\!]^\#\, s^\#$$

이를 C의 각 경우에 대해 증명한다.

- $C = (x \coloneqq R) \wedge x \neq a$. 이 경우 $b = m'\,a = m\,a$이므로

$$(a \to b) \in s^\# \subseteq [\![C]\!]^\#\, s^\#.$$

- $C = (x \coloneqq R) \wedge x = a$. 이 경우 $b = m'\,a = [\![R]\!]\, m$이고, Lemma 1에 의해 $[\![R]\!]\, m \in [\![R]\!]^\#\, s^\#$이므로

$$(a \to b) = (x \to [\![R]\!]\, m) \in \{(x \to y) \mid y \in [\![R]\!]^\#\, s^\#\} \subseteq [\![C]\!]^\#\, s^\#.$$

- $C = (*x \coloneqq R) \wedge m\,x \neq a$. 이 경우 $b = m'\,a = m\,a$이므로

$$(a \to b) \in s^\# \subseteq [\![C]\!]^\#\, s^\#.$$

- $C = (*x \coloneqq R) \wedge m\,x = a$. 이 경우 $b = m'\,a = [\![R]\!]\, m$이고, Lemma 1에 의해 $[\![R]\!]\, m \in [\![R]\!]^\#\, s^\#$이다. 또한, (1)에 의해 $(x \to m\,x) \in s^\#$이므로

$$(a \to b) = (m\,x \to [\![R]\!]\, m) \in \{(y \to z) \mid (x \to y) \in s^\#, z \in [\![R]\!]^\#\, s^\#\} \subseteq [\![C]\!]^\#\, s^\#.$$

- 나머지 경우에는 $m' = m$ 즉 $b = m'\,a = m\,a$이고 $[\![C]\!]^\#\, s^\# = s^\#$이므로

$$(a \to b) \in s^\# = [\![C]\!]^\#\, s^\#. \qquad \square$$

Theorem 1. *프로그램의 요약의미 $[\![P]\!]^\#$ 는 올바르다.*

$$[\![P]\!] \subseteq \gamma([\![P]\!]^\#)$$

Proof. 우선 $\mathit{Step}^\#$이 올바름을 다음과 같이 보일 수 있다: 요약상태 $s^\# \in \mathbb{S}^\#$가 주어졌을 때 상태 (C', m')에 대해 $(C', m') \in \mathit{Step}(\gamma(s^\#))$이면,

$$\begin{aligned}
(C', m') \in \mathit{Step}(\gamma(s^\#)) &\implies \exists (C, m) \in \gamma(s^\#) : (C, m) \hookrightarrow (C', m') \\
&\implies \exists C \in \mathcal{C}_P : (C', m') \in \gamma([\![C]\!]^\#\, s^\#) \qquad \text{(Lemma 2)} \\
&\implies (C', m') \in \bigcup_{C \in \mathcal{C}_P} \gamma([\![C]\!]^\#\, s^\#) \\
&\qquad \subseteq \gamma\Big(\bigcup_{C \in \mathcal{C}_P} [\![C]\!]^\#\, s^\#\Big) \qquad (\gamma\text{의 단조성}) \\
&\qquad = \gamma(\mathit{Step}^\#(s^\#))
\end{aligned}$$

즉, $\mathit{Step} \circ \gamma \sqsubseteq \gamma \circ \mathit{Step}^\#$이다. 또한, $I \subseteq \gamma(I^\#)$이므로 $F \circ \gamma \sqsubseteq \gamma \circ F^\#$이다. 고정점 전달 정리(fixpoint transfer theorem)에 의해 $\mathrm{lfp}\, F \sqsubseteq \gamma(\mathrm{lfp}\, F^\#)$이 성립하므로, $[\![P]\!] \subseteq \gamma([\![P]\!]^\#)$이다. $\square$