SNU 4541.664A Program Analysis Note 10-1b

Prof. Kwangkeun Yi

요약해석 디자인과 구현의 예

계산 실행과정(trace)의 요약해석

계산실행과정(trace)으로 표현된 의미구조를 요약하는 방안들

프로그램 C의 의미 $[\![C]\!]$는 C가 실행되면서 가질 수 있는 기계상태들의 (유한 혹은 무한한) 모든 족적들

$$
\begin{array}{rcll}
[\![C]\!] & \in & 2^{Trace} & \\
\tau, \tau_0\tau_1\cdots\tau_n & \in & Trace & = & State^{\omega} \\
 & & State & = & Command \times Memory \times \cdots
\end{array}
$$

참고:

$Trace$	$=$	$State^{\omega}$	v.s.	$State^{*}$
		liveness analysis		safety analysis
		prop. after infinite traces		prop. within finite traces

$$2^{Trace} \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} \hat{Trace}$$

$\overset{\alpha_0}{\longrightarrow}$ Trace of set of states: sequence of set of states appearing at a given time along at least one of the traces

$$\alpha_0(X) = \lambda i.\{\tau_i \mid \tau \in X, 0 \leq i < |\tau|\} \quad \in \hat{Trace} = \mathbb{N} \xrightarrow{\text{fin}} 2^{State}$$

$\overset{\alpha_1 \circ \alpha_0}{\longrightarrow}$ Set of reachable states (global invariant): set of states appearing at least once along a trace

$$\alpha_1(Y) = \bigcup\{Y(i) \mid i \in \mathsf{Dom}\ Y\} \quad \in \hat{Trace} = 2^{State}$$

$\overset{\alpha_2 \circ \alpha_1 \circ \alpha_0}{\longrightarrow}$ Partitioned set of reachable states (local invariant): e.g., project along each control point $\in \Delta$ (a finite set)

$$\alpha_2(Z) = \lambda c.\{s_i \mid \langle c_i, s_i\rangle \in Z, c_i = c \in \Delta\} \quad \in \hat{Trace} = \Delta \to 2^{State}$$

$\overset{\alpha_3 \circ \alpha_2 \circ \alpha_1 \circ \alpha_0}{\longrightarrow}$ Abstracting the partitioned set of reachable states

$$\alpha_3(\Phi) = \lambda c.\alpha(\Phi\ c) \quad \in \hat{Trace} = \Delta \to \hat{State}$$

where

$$2^{State} \leftrightarrows \hat{State}$$

실행과정(trace) 요약해석의 안전성 증명

$$\mathit{fix}(F \stackrel{\text{let}}{=} \lambda T.T_0 \cup \mathit{Next}\ T) \quad \text{and} \quad \mathit{fix}(\hat{F} \stackrel{\text{let}}{=} \lambda \hat{T}.\alpha(T_0) \sqcup \hat{\mathit{Next}}\ \hat{T})$$

여기서

$$F \in 2^{\mathit{Trace}} \to 2^{\mathit{Trace}} \quad \text{and} \quad \hat{F} \in \hat{\mathit{Trace}} \to \hat{\mathit{Trace}}.$$

보일 것은 $\alpha(\mathit{fix} F) \sqsubseteq \mathit{fix} \hat{F}$ 즉, $\alpha \circ F \sqsubseteq \hat{F} \circ \alpha$. 이 조건을 추적하면, $\hat{\mathit{Trace}}$가 $\sqcup$에 닫혀있다면, 다음 조건을 증명하면 된다:

$$\alpha \circ \mathit{Next} \sqsubseteq \hat{\mathit{Next}} \circ \alpha.$$

실행과정(trace) 요약해석의 안전성 증명(0/6)

증명과정에 사용할 표기법

- $\uparrow \in X \to 2^X$는 $\uparrow x = \{x\}$.
- $f \in A \to B$ 일때 $\wp f \in 2^A \to 2^B$는 $(\wp f)X = \{fx \mid x \in X\}$.
- $f \in A \to 2^B$일때 $\wp_\cup f = \cup \circ \wp f$.

사용할 간단한 사실들

- $\wp_\cup (f \circ g) = (\wp_\cup f) \circ (\wp g)$.
- $\wp_\cup (\wp_\cup f) \circ (\wp g) = (\wp_\cup f) \circ (\wp_\cup g)$.
- $x \in A, X \in 2^A$일때, $fx \in gx$ 이면 $(\wp f)X \subseteq (\wp_\cup g)X$.

실행과정(trace) 요약해석의 안전성 증명(1/6)

다음의 최종 단계의 요약에 촛점:

$$2^{State} \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} (\Delta \to \hat{State})$$

즉,

- 프로그램의 모듬의미 = 그 프로그램이 실행중에 만드는 모든 기계상태들의 모음

$$[\![C]\!] \in 2^{State}$$

- 프로그램의 요약의미 = 모든 기계상태들의 모음을 몇개의 조각으로 분할해서 요약:

$$[\![\hat{C}]\!] \in \Delta \to \hat{State}$$

  - Δ: 복수의 요약 기계상태들의 분할 기준으로 작용하는 집합(set of partinitiong indices).
  - 예: Δ = 프로그램 지점들의 집합.

실행과정(trace) 요약해석의 안전성 증명(2/6)

셋팅

- $\Delta \rightarrow \hat{State}$는 편의를 위해서 멱집합(powerset)

$$\dot{2}^{\hat{State}} = 2^{\hat{State}} \setminus \{\emptyset\}$$

으로하고 증명을 진행. 원소들 순서는:

$$\hat{X} \sqsubseteq \hat{Y} \quad \text{iff} \quad \forall \hat{x} \in \hat{X}, \exists \hat{y} \in \hat{Y} : \hat{x} \sqsubseteq \hat{y}.$$

- π와 $\hat{\pi}$는 분할(partitioning)함수들:

$$\begin{array}{rcl} \pi & \in & 2^{State} \rightarrow 2^{2^{State}} \\ \hat{\pi} & \in & \dot{2}^{\hat{State}} \rightarrow \dot{2}^{\dot{2}^{\hat{State}}} \end{array}$$

실행과정(trace) 요약해석의 안전성 증명(3/6)

그러면

- 갈로아연결

$$2^{State} \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} \dot{2}^{\hat{State}} \quad (\Delta \rightarrow \hat{State})$$

은

$$\alpha = (\wp\alpha_1) \circ \pi.$$

- 위에서 α_1은 $\hat{State}$를 만드는 요약:

$$2^{State} \underset{\alpha_1}{\overset{\gamma_1}{\leftrightarrows}} \hat{State}.$$

실행과정(trace) 요약해석의 안전성 증명(4/6)

$Next$와 $\hat{Next}$가 사용할 전이함수들

- 실제 전이함수 $next$:

$$next \in State \to State$$

  (종료 기계상태에서는 제자리 맴맴)
- 요약 전이함수 $\hat{next}$:

$$\hat{next} \in \hat{State} \to 2^{\hat{State}}$$

  (하나의 요약기계상태에서 복수의 요약기계상태들로 전이가능)

실행과정(trace) 요약해석의 안전성 증명(5/6)

Theorem (Correctness)

Next와 $\hat{Next}$의 정의를:

$$\begin{array}{rcll} Next & = & \wp next & \in 2^{State} \to 2^{State} \\ \hat{Next} & = & (\wp\sqcup) \circ \hat{\pi} \circ (\wp_\cup \hat{next}) & \in \dot{2}^{\hat{State}} \to \dot{2}^{\hat{State}} \end{array}$$

로 하고, 아래 두 조건을 만족하면 $\alpha \circ Next \sqsubseteq \hat{Next} \circ \alpha$가 성립:

1. *요약 분할($\hat{\pi}$)의 조건:*

$$(\wp\alpha_1) \circ \pi \circ (\wp_\cup \gamma) \sqsubseteq (\wp\sqcup) \circ \hat{\pi} \tag{1}$$

2. *요약 전이함수($\hat{next}$)의 조건:*

$$next\ x \in ((\wp_\cup \gamma) \circ \hat{next} \circ \alpha_1 \circ \uparrow)\ x \tag{2}$$

실행과정(trace) 요약해석의 안전성 증명(6/6)

Proof. 우선, 조건 (2) 이면 다음이 사실이다:

$$\wp next \sqsubseteq (\wp_\cup \gamma) \circ (\wp_\cup \hat{next}) \circ \alpha \qquad (3)$$

왜냐면,

$$\begin{array}{rcll} \wp next & \sqsubseteq & \wp_\cup((\wp_\cup\gamma) \circ \hat{next} \circ \alpha_1 \circ \uparrow) & (\text{조건 (2)}, (fx \in gx \text{ 이면 } (\wp f)X \subseteq (\wp_\cup g)X)) \\ & = & \wp_\cup(\wp_\cup\gamma) \circ \wp(\hat{next} \circ \alpha_1 \circ \uparrow) & (\wp_\cup(f \circ g) = (\wp_\cup f) \circ (\wp g)) \\ & = & (\wp_\cup\gamma) \circ (\wp_\cup \hat{next}) \circ (\wp\alpha_1) \circ (\wp \uparrow) & (\wp_\cup(\wp_\cup f) \circ (\wp g) = (\wp_\cup f) \circ (\wp_\cup g)) \\ & \sqsubseteq & (\wp_\cup\gamma) \circ (\wp_\cup \hat{next}) \circ (\wp\alpha_1) \circ \pi & (\gamma, \hat{next}, \alpha_1\text{는 모두 단조함수}) \\ & = & (\wp_\cup\gamma) \circ (\wp_\cup \hat{next}) \circ \alpha. & \end{array}$$

따라서,

$$\begin{array}{rcll} \alpha \circ Next & = & (\wp\alpha_1) \circ \pi \circ (\wp next) & \\ & \sqsubseteq & (\wp\alpha_1) \circ \pi \circ (\wp_\cup\gamma) \circ (\wp_\cup \hat{next}) \circ \alpha & (\text{조건 (3)}) \\ & \sqsubseteq & (\wp\sqcup) \circ \hat{\pi} \circ (\wp_\cup \hat{next}) \circ \alpha & (\text{조건 (1)}) \\ & = & \hat{Next} \circ \alpha. & \end{array}$$

즉, 조건 (1)와 조건 (2)이면 $\alpha \circ Next \sqsubseteq \hat{Next} \circ \alpha$ 이고, 이는 곧(Fixpoint Transfer Theorem)

$$\alpha(\mathit{fix}(\lambda T.T_0 \cup Next\ T)) \sqsubseteq \mathit{fix}(\lambda \hat{T}.\alpha(T_0) \sqcup \hat{Next}\ \hat{T}).$$

□