SNU 4541.664A Program Analysis
Note 8-1

Prof. Kwangkeun Yi

요약해석 틀: 스타일 별로

- 프로그램의 의미를 조립식으로 (최소고정점) “compositional semantics”
- 프로그램의 의미를 기계상태의 전이과정으로 (최소고정점) “transitional semantics”
- 프로그램의 의미를 실행기 함수로 (최소고정점) “definitional-intrprtr semantics”

예) 의미를 실행기 함수로

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

예) 의미를 실행기 함수로

$$
\begin{array}{rcl}
\text{실행기 함수} \quad \mathcal{I} & \in & Cmd \to 2^{Mem} \to 2^{Mem} \\
\text{실행기 함수} \quad \mathcal{E} & \in & Exp \to 2^{Mem} \to 2^{Val}
\end{array}
$$

$$
\begin{array}{rcl}
\mathcal{I}\,\texttt{skip} & = & \lambda M.M \\
\mathcal{I}\,(x\ \texttt{:=}\ E) & = & \lambda M.update_x(M, \mathcal{E}\ E\ M) \\
\mathcal{I}\,(C_1\ ;\ C_2) & = & \lambda M.\mathcal{I}\,C_2\,(\mathcal{I}\,C_1\,M) \\
\mathcal{I}\,(\texttt{if}\ B\ C_1\ C_2) & = & \lambda M.\mathcal{I}\,C_1\,(trim_B\,M)\ \cup\ \mathcal{I}\,C_2\,(trim_{\neg B}\,M) \\
\mathcal{I}\,(\texttt{while}\ B\ C) & = & \lambda M.trim_{\neg B} \\
 & & \quad (M\ \cup\ (\mathcal{I}\,(\texttt{while}\ B\ C)\,(\mathcal{I}\,C\,(trim_B\,M)))) \\
\mathcal{E}\,n & = & \lambda M.\{n\} \\
\mathcal{E}\,x & = & \lambda M.read_x M \\
\mathcal{E}\,(E_1\ \texttt{+}\ E_2) & = & \lambda M.add(\mathcal{E}\,E_1\,M, \mathcal{E}\,E_2\,M) \\
trim_B & = & \lambda M.\cup\{M' \mid \mathcal{E}\,B\,M' = \{T\}, M' \subseteq M\}
\end{array}
$$

정의 vs 방정식

프로그램 C의 의미는 $\mathcal{I}(C)$로 정의되는가?

- No. $\mathcal{I}$가 뭔가요? 위의 $=$ 은 $\mathcal{I}$에 대한 방정식일 뿐.
- 그런 $\mathcal{I}$는 그 방정식의 해.
- 방정식의 해 $=$ 최소고정점! (해당하는 연속함수의)

$\mathcal{I}$의 방정식

$$\mathcal{I} = \mathcal{F}(\mathcal{I})$$

- $\mathcal{F}$는 실행기함수 $\mathcal{I}$의 몸통 모습 그대로

$$\mathcal{F}(\mathcal{I}) = \lambda C.\mathsf{case}\ C\ \mathsf{of} \cdots \mathcal{I} \cdots\ .$$

$$\mathcal{F} : (Cmd \to 2^{Mem} \to 2^{Mem}) \to (Cmd \to 2^{Mem} \to 2^{Mem})$$

- $\mathcal{I}$는 위 방정식의 최소해로 정의됨:

$$\mathcal{I} \stackrel{\mathsf{def}}{=} fix\mathcal{F}$$

- 프로그램 C의 의미는:

$$fix\mathcal{F}(C).$$

올바르게 요약하기: $\mathcal{F}^\sharp$

- $\mathcal{F}$ 요약버전 $\mathcal{F}^\sharp$ 을 정의

$$\begin{array}{rcl} \mathcal{F} & \in & (Cmd \to 2^{Mem} \to 2^{Mem}) \to (Cmd \to 2^{Mem} \to 2^{Mem}) \\ \mathcal{F}^\sharp & \in & (Cmd \to Mem^\sharp \to Mem^\sharp) \to (Cmd \to Mem^\sharp \to Mem^\sharp) \end{array}$$

- 갈로아연결 & 사용하는 모든 함수 f들을 안전하게 요약

$$2^{Mem} \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} Mem^{\#}$$
$$f \circ \gamma \sqsubseteq \gamma \circ f^\sharp$$

- 그리고 확인

$$\forall C. fix\mathcal{F}(C) \circ \gamma \sqsubseteq \gamma \circ fix\mathcal{F}^\sharp(C)$$

증명방법: “fixpoint induction”

증명할 것, C의 각 경우마다

$$fix\mathcal{F}(C) \circ \gamma \sqsubseteq \gamma \circ fix\mathcal{F}^{\sharp}(C)$$

증명방법: “포함되는(inclusive) 성질” $\mathcal{Q}$에 대해서

- 보이고 $\mathcal{Q}(\bot)$,
- 보이면 $\mathcal{Q}(x) \implies \mathcal{Q}(F(x))$,
- 그러면 $\mathcal{Q}(fixF)$ 이 사실임.

(“포함되는 성질”? $\forall$ + 단순성질(first-order predicate) + $\sqsubseteq$ + 연속함수.)

초보적인 분석 알고리즘: 프로그램 의미$\in A^\sharp \to B^\sharp$

$Tabulate(\mathcal{F}^\sharp\colon (Code \to A^\sharp \to B^\sharp) \to Code \to A^\sharp \to B^\sharp,\ C\colon Code,\ {a_0}^\sharp\colon A^\sharp)$
$T_A\colon Code \to A^\sharp$;
$T_B\colon Code \to B^\sharp$;

$f\ (c\colon Code)\ (a\colon A^\sharp) \quad : B^\sharp$
begin
    $T_A(c) := T_A(c) \sqcup a$;
    return $T_B(c)$
end

begin
    $\forall C_i$ of $C : T_A(C_i) := \bot_{A^\sharp}, \quad T_B(C_i) := \bot_{B^\sharp}$;
    $T_A(C) = a_0^\sharp$;
    repeat
        $\forall C_i \in C : T_B(C_i) := \mathcal{F}^\sharp(\ f,\ C_i,\ T_A(C_i))$;
    until (T_A and T_B are stable)
end

할일만 하기 방식의 분석 알고리즘: 프로그램 의미$\in A^\sharp \to B^\sharp$

$Tabulate(\mathcal{F}^\sharp\colon (Code \to A^\sharp \to B^\sharp) \to (Code \to A^\sharp \to B^\sharp),\ C\colon Code,\ a_0^\sharp\colon A^\sharp)$
$T_A\colon Code \to A^\sharp, \quad T_B\colon Code \to B^\sharp, \quad W\colon 2^{Code}, \quad w\colon Code, \quad y\colon B^\sharp$

$f\ (c\colon Code)\ (a\colon A^\sharp) \quad : B^\sharp$
`begin`
  record that evaluation of w requires that of c;
  `if` $(a \not\sqsubseteq T_A(c))$ `then`
    $T_A(c) := T_A(c) \sqcup a$;
    $W := \mathbf{Add}(W, c)$;
  `return` $T_B(c)$
`end`
`begin`
  $\forall C_i \in C : T_A(C_i) := \bot_{A^\sharp}, T_B(C_i) := \bot_{B^\sharp}$;
  $T_A(C) := a_0^\sharp; \quad W := \{C_i \mid C_i \in C\}$
  `repeat`
    $w := \mathbf{Select}(W); \quad y := \mathcal{F}^\sharp(\ f,\ w\ , T_A(w))$
    `if` $y \not\sqsubseteq T_B(w)$ `then`
      $T_B(w) := y$;
      $\forall w'$ whose evaluation needs that of w :
        $W := \mathbf{Add}(W, w')$
  `until` $W = \{\}$
`end`