Semantics and Verification of Software

Summer Semester 2019

Lecture 12: Axiomatic Semantics of WHILE IV (Total Correctness & Axiomatic Equivalence)

Thomas Noll
Software Modeling and Verification Group
RWTH Aachen University

https://moves.rwth-aachen.de/teaching/ss-19/sv-sw/

Software Modeling and Verification Chair

RWTH AACHEN UNIVERSITY

Recap: Completeness & Total Correctness

Relative Completeness of Hoare Logic

Theorem (Cook's Completeness Theorem)

Hoare Logic is relatively complete, i.e., for every partial correctness property $\{A\}\, c\, \{B\}$*:*

$$\models \{A\}\, c\, \{B\} \quad \Rightarrow \quad \vdash \{A\}\, c\, \{B\}.$$

Stephen A. Cook (* 1939)

Thus: if we know that a partial correctness property is valid, then we know that there is a corresponding proof.

The proof uses the following concept: assume that, e.g., $\{A\}\, c_1 ; c_2\, \{B\}$ has to be derived. This requires an intermediate assertion $C \in \mathit{Assn}$ such that $\{A\}\, c_1\, \{C\}$ and $\{C\}\, c_2\, \{B\}$. How to find it?

Recap: Completeness & Total Correctness

Weakest Liberal Preconditions

Definition (Weakest liberal precondition)

Given $c \in \mathit{Cmd}$ and $S \subseteq \Sigma$, the weakest (liberal) precondition of S with respect to c collects all states σ such that running c in σ does not terminate or yields a state in S:

$$\mathit{wlp}[\![c]\!]S := \{\sigma \in \Sigma \mid \mathfrak{C}[\![c]\!]\sigma \in S \cup \{\bot\}\}.$$

Corollary

For every $c \in \mathit{Cmd}$, $A, B \in \mathit{Assn}$, and $I \in \mathit{Int}$:

1. $\models^I \{A\}\, c\, \{B\} \iff A^I \subseteq \mathit{wlp}[\![c]\!]B^I$
2. *If $A_0 \in \mathit{Assn}$ such that $A_0^I = \mathit{wlp}[\![c]\!]B^I$ for every $I \in \mathit{Int}$, then* $\models \{A\}\, c\, \{B\} \iff \models (A \Rightarrow A_0)$

Remarks:

- Corollary 11.5 justifies the notion of weakest precondition: it is entailed by every precondition A that makes $\{A\}\, c\, \{B\}$ valid.
- In the following, we do not distinguish between sets of program states (such as S or A^I) and predicates on program states (such as $\mathfrak{B}[\![b]\!]$).

Proving Total Correctness

Definition (Hoare Logic for total correctness)

The Hoare rules for total correctness are given by (where $i \in LVar$)

$$\text{(skip)}\ \frac{}{\{A\}\ \texttt{skip}\ \{\Downarrow A\}} \qquad \text{(asgn)}\ \frac{}{\{A[x \mapsto a]\}\ x := a\ \{\Downarrow A\}}$$

$$\text{(seq)}\ \frac{\{A\}\ c_1\ \{\Downarrow C\} \quad \{C\}\ c_2\ \{\Downarrow B\}}{\{A\}\ c_1 ; c_2\ \{\Downarrow B\}} \qquad \text{(if)}\ \frac{\{A \wedge b\}\ c_1\ \{\Downarrow B\} \quad \{A \wedge \neg b\}\ c_2\ \{\Downarrow B\}}{\{A\}\ \texttt{if}\ b\ \texttt{then}\ c_1\ \texttt{else}\ c_2\ \texttt{end}\ \{\Downarrow B\}}$$

$$\text{(while)}\ \frac{\models (i \geq 0 \wedge A(i+1) \Rightarrow b) \quad \{i \geq 0 \wedge A(i+1)\}\ c\ \{\Downarrow A(i)\} \quad \models (A(0) \Rightarrow \neg b)}{\{\exists i.\, i \geq 0 \wedge A(i)\}\ \texttt{while}\ b\ \texttt{do}\ c\ \texttt{end}\ \{\Downarrow A(0)\}}$$

$$\text{(cons)}\ \frac{\models (A \Rightarrow A') \quad \{A'\}\ c\ \{\Downarrow B'\} \quad \models (B' \Rightarrow B)}{\{A\}\ c\ \{\Downarrow B\}}$$

A total correctness property is provable (notation: $\vdash \{A\}\ c\ \{\Downarrow B\}$) if it is derivable by the Hoare rules. In case of (while), $A(i)$ is called a (loop) invariant.

Soundness and Completeness of Hoare Logic for Total Correctness

Soundness

In analogy to Theorem 10.4 we can show that the Hoare Logic for total correctness properties is also sound:

Theorem 12.1 (Soundness)

For every total correctness property $\{A\}\, c\, \{\Downarrow B\}$,

$$\vdash \{A\}\, c\, \{\Downarrow B\} \quad \Rightarrow \quad \models \{A\}\, c\, \{\Downarrow B\}.$$

Proof.

Again by structural induction over the derivation tree of $\vdash \{A\}\, c\, \{\Downarrow B\}$. Here we only consider the (while) case:

$$\text{(while)}\ \frac{\models (i \geq 0 \wedge A(i+1) \Rightarrow b) \quad \{i \geq 0 \wedge A(i+1)\}\, c\, \{\Downarrow A(i)\} \quad \models (A(0) \Rightarrow \neg b)}{\{\exists i.\, i \geq 0 \wedge A(i)\}\ \texttt{while}\ b\ \texttt{do}\ c\ \texttt{end}\ \{\Downarrow A(0)\}}$$

(on the board) □

Relative Completeness

Also the counterpart to Cook's Completeness Theorem 12.1 applies:

Theorem 12.2 (Completeness)

The Hoare Logic for total correctness properties is relatively complete, i.e., for every $\{A\}\, c\, \{\Downarrow B\}$*:*

$$\models \{A\}\, c\, \{\Downarrow B\} \quad \Rightarrow \quad \vdash \{A\}\, c\, \{\Downarrow B\}.$$

Proof.

again using weakest preconditions (see following slides) □

Weakest Preconditions I

Definition 12.3 (Weakest precondition)

Given $c \in \mathit{Cmd}$ and $S \subseteq \Sigma$, the weakest precondition of S with respect to c collects all states σ such that executing c in σ terminates and yields a state in S:

$$wp[\![c]\!]S := \{\sigma \in \Sigma \mid \mathfrak{C}[\![c]\!]\sigma \in S\}.$$

Corollary 12.4

For every $c \in \mathit{Cmd}$, $A, B \in \mathit{Assn}$, and $I \in \mathit{Int}$:

1. $\models^I \{A\}\, c\, \{\Downarrow B\} \iff A^I \subseteq wp[\![c]\!]B^I$
2. *If $A_0 \in \mathit{Assn}$ such that $A_0^I = wp[\![c]\!]B^I$ for every $I \in \mathit{Int}$, then*

$$\models \{A\}\, c\, \{\Downarrow B\} \iff \models (A \Rightarrow A_0)$$

Weakest Preconditions II

Lemma 12.5 (Weakest precondition transformer)

Weakest preconditions $wp[\![.]\!]. : Cmd \times 2^{\Sigma} \to 2^{\Sigma}$ *can be computed as follows:*

$$\begin{aligned} wp[\![\texttt{skip}]\!]S &= S \\ wp[\![x := a]\!]S &= \{\sigma \in \Sigma \mid \sigma[x \mapsto \mathfrak{A}[\![a]\!]\sigma] \in S\} \\ wp[\![c_1 ; c_2]\!]S &= wp[\![c_1]\!](wp[\![c_2]\!]S) \\ wp[\![\texttt{if } b \texttt{ then } c_1 \texttt{ else } c_2 \texttt{ end}]\!]S &= (\mathfrak{B}[\![b]\!] \cap wp[\![c_1]\!]S) \cup (\mathfrak{B}[\![\neg b]\!] \cap wp[\![c_2]\!]S) \\ wp[\![\texttt{while } b \texttt{ do } c \texttt{ end}]\!]S &= \mathrm{fix}(\Psi) \end{aligned}$$

where $\mathrm{fix}(\Psi)$ *denotes the least fixpoint (w.r.t.* $(2^{\Sigma}, \subseteq)$*) of*

$$\Psi : 2^{\Sigma} \to 2^{\Sigma} : T \mapsto (\mathfrak{B}[\![b]\!] \cap wlp[\![c]\!]T) \cup (\mathfrak{B}[\![\neg b]\!] \cap S)$$

Proof.

omitted □

Weakest Preconditions III

Example 12.6 (cf. Example 11.7)

Using Lemma 12.5, we want to determine the weakest precondition for

$$\{?\}\ \underbrace{\texttt{while x} \neq 0 \wedge \texttt{x} \neq 1 \texttt{ do } \overbrace{\texttt{x := x-2}}^{c_0} \texttt{ end}}_{c}\ \{\texttt{x} = 1\}$$

i.e., $wp[\![c]\!]S$ for $S := \mathfrak{B}[\![\texttt{x} = 1]\!] = \{\sigma \in \Sigma \mid \sigma(\texttt{x}) = 1\}$.

- $wp[\![c]\!]S = \text{fix}(\Psi)$ for $\Psi(T) = (\mathfrak{B}[\![\texttt{x} \neq 0 \wedge \texttt{x} \neq 1]\!] \cap wp[\![c_0]\!]T) \cup \underbrace{(\mathfrak{B}[\![\texttt{x} \in \{0,1\}]\!] \cap S)}_{=s}$
- $wp[\![c_0]\!]T = \{\sigma \in \Sigma \mid \sigma[\texttt{x} \mapsto \sigma(\texttt{x}) - 2] \in T\}$
- Fixpoint iteration (with initial value $\bigsqcup \emptyset = \emptyset$):

$$\begin{aligned}
\Psi(\emptyset) &= (\mathfrak{B}[\![\texttt{x} \neq 0 \wedge \texttt{x} \neq 1]\!] \cap wp[\![c_0]\!]\emptyset) \cup S = \mathfrak{B}[\![\texttt{x} = 1]\!] \\
\Psi^2(\emptyset) &= (\mathfrak{B}[\![\texttt{x} \neq 0 \wedge \texttt{x} \neq 1]\!] \cap wp[\![c_0]\!](\mathfrak{B}[\![\texttt{x} = 1]\!])) \cup S = \mathfrak{B}[\![\texttt{x} \in \{1,3\}]\!] \\
\Psi^3(\emptyset) &= (\mathfrak{B}[\![\texttt{x} \neq 0 \wedge \texttt{x} \neq 1]\!] \cap wp[\![c_0]\!](\mathfrak{B}[\![\texttt{x} \in \{1,3\}]\!])) \cup S = \mathfrak{B}[\![\texttt{x} \in \{1,3,5\}]\!] \\
&\vdots
\end{aligned}$$

$$\Rightarrow \text{fix}(\Psi) = \bigcup_{n \in \mathbb{N}} \Psi^n(\emptyset) = \{\sigma \in \Sigma \mid \sigma(\texttt{x}) \in \{1,3,5,\ldots\}\}$$

Operational and Denotational Equivalence

Definition 4.1: $\mathfrak{O}[\![.]\!] : \mathit{Cmd} \to (\Sigma \dashrightarrow \Sigma)$ given by

$$\mathfrak{O}[\![c]\!]\sigma = \sigma' \iff \langle c, \sigma \rangle \to \sigma'$$

Definition 4.2: Two statements $c_1, c_2 \in \mathit{Cmd}$ are operationally equivalent (notation: $c_1 \sim c_2$) if

$$\mathfrak{O}[\![c_1]\!] = \mathfrak{O}[\![c_2]\!]$$

Theorem 8.5: For every $c \in \mathit{Cmd}$,

$$\mathfrak{O}[\![c]\!] = \mathfrak{C}[\![c]\!]$$

(and thus operational and denotational equivalence coincide)

Axiomatic Equivalence I

In the axiomatic semantics, two statements have to be considered equivalent if they are indistinguishable w.r.t. (partial) correctness properties:

Definition 12.7 (Axiomatic equivalence)

Two statements $c_1, c_2 \in \mathit{Cmd}$ are called axiomatically equivalent (notation: $c_1 \approx c_2$) if, for all assertions $A, B \in \mathit{Assn}$,

$$\models \{A\}\, c_1\, \{B\} \quad \Longleftrightarrow \quad \models \{A\}\, c_2\, \{B\}.$$

(later: total correctness yields same notion of equivalence)

Axiomatic Equivalence II

Example 12.8

We show that $\texttt{while}\ b\ \texttt{do}\ c\ \texttt{end} \approx \texttt{if}\ b\ \texttt{then}\ c\texttt{;while}\ b\ \texttt{do}\ c\ \texttt{end else skip end}$ (cf. Lemma 4.3). Let $A, B \in \mathit{Assn}$:

$$
\begin{aligned}
& \models \{A\}\ \texttt{while}\ b\ \texttt{do}\ c\ \texttt{end}\ \{B\} \\
\iff & \vdash \{A\}\ \texttt{while}\ b\ \texttt{do}\ c\ \texttt{end}\ \{B\} && \text{(Theorem 10.4, 12.1)} \\
\iff & \text{ex. } C \in \mathit{Assn} \text{ such that } \models (A \Rightarrow C), \models (C \wedge \neg b \Rightarrow B), && \text{(rule (cons))} \\
& \vdash \{C\}\ \texttt{while}\ b\ \texttt{do}\ c\ \texttt{end}\ \{C \wedge \neg b\} \\
\iff & \text{ex. } C \in \mathit{Assn} \text{ such that } \models (A \Rightarrow C), \models (C \wedge \neg b \Rightarrow B), && \text{(rule (while))} \\
& \vdash \{C \wedge b\}\ c\ \{C\} \\
\iff & \text{ex. } C \in \mathit{Assn} \text{ such that } \models (A \Rightarrow C), \models (C \wedge \neg b \Rightarrow B), && \text{(rule (seq), (skip))} \\
& \vdash \{C \wedge b\}\ c\texttt{;while}\ b\ \texttt{do}\ c\ \texttt{end}\ \{C \wedge \neg b\} \\
& \vdash \{C \wedge \neg b\}\ \texttt{skip}\ \{C \wedge \neg b\} \\
\iff & \text{ex. } C \in \mathit{Assn} \text{ such that } \models (A \Rightarrow C), \models (C \wedge \neg b \Rightarrow B), && \text{(rule (if))} \\
& \vdash \{C\}\ \texttt{if}\ b\ \texttt{then}\ c\texttt{;while}\ b\ \texttt{do}\ c\ \texttt{end else skip end}\ \{C \wedge \neg b\} \\
\iff & \vdash \{A\}\ \texttt{if}\ b\ \texttt{then}\ c\texttt{;while}\ b\ \texttt{do}\ c\ \texttt{end else skip end}\ \{B\} && \text{(rule (cons))} \\
\iff & \models \{A\}\ \texttt{if}\ b\ \texttt{then}\ c\texttt{;while}\ b\ \texttt{do}\ c\ \texttt{end else skip end}\ \{B\} && \text{(Theorem 10.4, 12.1)}
\end{aligned}
$$

Characteristic Assertions I

The following results are based of the following encoding of states by assertions:

Definition 12.9

Given a state $\sigma \in \Sigma$ and a finite subset of program variables $X \subseteq \mathit{Var}$, the characteristic assertion of σ w.r.t. X is given by

$$\mathit{state}(\sigma, X) := \bigwedge_{x \in X} (x = \underbrace{\sigma(x)}_{\in \mathbb{Z}}) \in \mathit{Assn}$$

(where $\mathit{state}(\sigma, \emptyset) := \text{true}$). Moreover, we let $\mathit{state}(\bot, X) := \text{false}$.

Corollary 12.10

For all finite $X \subseteq \mathit{Var}$ and $\sigma \in \Sigma$,

$$\sigma \models \mathit{state}(\sigma, X)$$

Characteristic Assertions II

Programs and characteristic state assertions are obviously related as follows:

Corollary 12.11

Let $c \in Cmd$, and let $FV(c) \subseteq Var$ denote the set of all variables occurring in c. Then, for every finite $X \supseteq FV(c)$ and $\sigma \in \Sigma$, $\models \{state(\sigma, X)\}\, c\, \{state(\mathfrak{C}[\![c]\!]\sigma, X)\}$. If moreover $\mathfrak{C}[\![c]\!]\sigma \neq \bot$, then $\models \{state(\sigma, X)\}\, c\, \{\Downarrow state(\mathfrak{C}[\![c]\!]\sigma, X)\}$.

Example 12.12 (Factorial program)

For $c := (\texttt{y:=1; while } \neg(\texttt{x=1}) \texttt{ do y:=y*x; x:=x-1 end})$, $X = \{\texttt{x}, \texttt{y}, \texttt{z}\} \supseteq FV(c) = \{\texttt{x}, \texttt{y}\}$, $\sigma(\texttt{x}) = 3$, $\sigma(\texttt{y}) = 0$, and $\sigma(\texttt{z}) = 1$, we obtain

$$state(\sigma, X) = (\texttt{x=3} \wedge \texttt{y=0} \wedge \texttt{z=1}) \quad \text{and} \quad state(\mathfrak{C}[\![c]\!]\sigma, X) = (\texttt{x=1} \wedge \texttt{y=6} \wedge \texttt{z=1})$$

and thus $\models \{state(\sigma, X)\}\, c\, \{state(\mathfrak{C}[\![c]\!]\sigma, X)\}$.

If $X \not\supseteq FV(c)$, then the claim does not hold: e.g., $\not\models \{\texttt{y=0}\}\, c\, \{\texttt{y=6}\}$!

Partial vs. Total Equivalence

Using characteristic state assertions, we can show that considering total rather than partial correctness properties yields the same notion of equivalence:

Theorem 12.13

Let $c_1, c_2 \in Cmd$. The following propositions are equivalent:

1. $\forall A, B \in Assn: \quad \models \{A\}\, c_1\, \{B\} \iff \models \{A\}\, c_2\, \{B\}$
2. $\forall A, B \in Assn: \quad \models \{A\}\, c_1\, \{\Downarrow B\} \iff \models \{A\}\, c_2\, \{\Downarrow B\}$

Proof.

on the board □