Semantics and Verification of Software

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

Thomas Noll

Lehrstuhl für Informatik 2
(Software Modeling and Verification)

RWTH AACHEN UNIVERSITY

noll@cs.rwth-aachen.de

http://www-i2.informatik.rwth-aachen.de/i2/svsw11/

Winter Semester 2011/12

Outline

Hoare Logic

Goal: syntactic derivation of valid partial correctness properties

Definition (Hoare Logic)

The Hoare rules are given by

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

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

$$\text{(while)}\ \frac{\{A \wedge b\}\,c\,\{A\}}{\{A\}\,\texttt{while}\ b\ \texttt{do}\ c\,\{A \wedge \neg b\}}$$

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

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

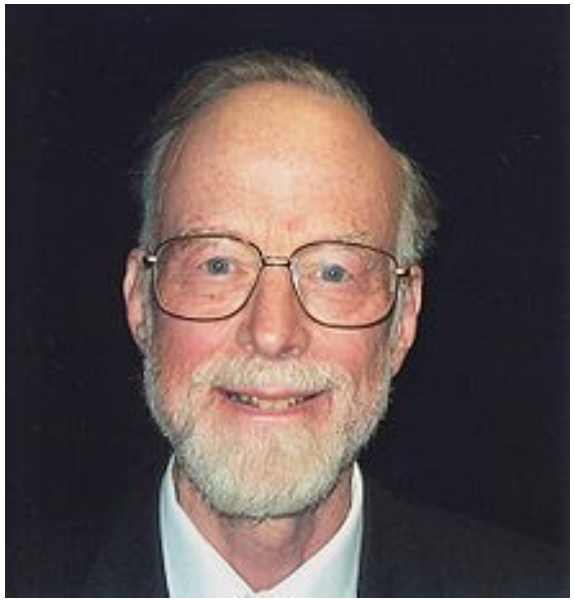
Here $A[x \mapsto a]$ denotes the syntactic replacement of every occurrence of x by a in A.

Soundness of Hoare Logic

Theorem (Soundness of Hoare Logic)

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

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



Tony Hoare (* 1934)

Proof.

Let $\vdash \{A\}\, c\, \{B\}$. By induction over the structure of the corresponding proof tree we show that, for every $\sigma \in \Sigma$ and $I \in \mathit{Int}$ such that $\sigma \models^I A$, $\mathfrak{C}[\![c]\!]\sigma \models^I B$ (on the board).
(If $\sigma = \bot$, then $\mathfrak{C}[\![c]\!]\sigma = \bot \models^I B$ holds trivially.) $\square$

(Relative) Completeness of Hoare Logic

Corollary

There is no proof system in which all valid partial correctness properties can be enumerated.

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)

Outline

Total Correctness

- **Observation:** partial correctness properties only speak about terminating computations of a given program

Total Correctness

- **Observation:** partial correctness properties only speak about terminating computations of a given program
- Total correctness additionally requires the proof that the program indeed stops (on the input states admitted by the precondition)

Total Correctness

- **Observation:** partial correctness properties only speak about terminating computations of a given program
- Total correctness additionally requires the proof that the program indeed stops (on the input states admitted by the precondition)
- Consider total correctness properties of the form

$$\{A\}\, c\, \{\Downarrow B\}$$

where $c \in \mathit{Cmd}$ and $A, B \in \mathit{Assn}$

Total Correctness

- **Observation:** partial correctness properties only speak about terminating computations of a given program
- Total correctness additionally requires the proof that the program indeed stops (on the input states admitted by the precondition)
- Consider total correctness properties of the form

$$\{A\}\, c\, \{\Downarrow B\}$$

  where $c \in \mathit{Cmd}$ and $A, B \in \mathit{Assn}$
- Interpretation:

Validity of property $\{A\}\, c\, \{\Downarrow B\}$

For all states $\sigma \in \Sigma$ which satisfy A:
the execution of c in σ terminates and yields a state which satisfies B.

Semantics of Total Correctness Properties

Definition 12.1 (Semantics of total correctness properties)

Let $A, B \in \mathit{Assn}$ and $c \in \mathit{Cmd}$.

- $\{A\}\, c\, \{\Downarrow B\}$ is called valid in $\sigma \in \Sigma$ and $I \in \mathit{Int}$ (notation: $\sigma \models^I \{A\}\, c\, \{\Downarrow B\}$) if $\sigma \models^I A$ implies that $\mathfrak{C}[\![c]\!]\sigma \neq \bot$ and $\mathfrak{C}[\![c]\!]\sigma \models^I B$.

Semantics of Total Correctness Properties

Definition 12.1 (Semantics of total correctness properties)

Let $A, B \in \mathit{Assn}$ and $c \in \mathit{Cmd}$.

- $\{A\}\, c\, \{\Downarrow B\}$ is called valid in $\sigma \in \Sigma$ and $I \in \mathit{Int}$ (notation: $\sigma \models^I \{A\}\, c\, \{\Downarrow B\}$) if $\sigma \models^I A$ implies that $\mathfrak{C}[\![c]\!]\sigma \neq \bot$ and $\mathfrak{C}[\![c]\!]\sigma \models^I B$.
- $\{A\}\, c\, \{\Downarrow B\}$ is called valid in $I \in \mathit{Int}$ (notation: $\models^I \{A\}\, c\, \{\Downarrow B\}$) if $\sigma \models^I \{A\}\, c\, \{\Downarrow B\}$ for every $\sigma \in \Sigma$.

Semantics of Total Correctness Properties

Definition 12.1 (Semantics of total correctness properties)

Let $A, B \in \mathit{Assn}$ and $c \in \mathit{Cmd}$.

- $\{A\}\, c\, \{\Downarrow B\}$ is called valid in $\sigma \in \Sigma$ and $I \in \mathit{Int}$ (notation: $\sigma \models^I \{A\}\, c\, \{\Downarrow B\}$) if $\sigma \models^I A$ implies that $\mathfrak{C}[\![c]\!]\sigma \neq \bot$ and $\mathfrak{C}[\![c]\!]\sigma \models^I B$.
- $\{A\}\, c\, \{\Downarrow B\}$ is called valid in $I \in \mathit{Int}$ (notation: $\models^I \{A\}\, c\, \{\Downarrow B\}$) if $\sigma \models^I \{A\}\, c\, \{\Downarrow B\}$ for every $\sigma \in \Sigma$.
- $\{A\}\, c\, \{\Downarrow B\}$ is called valid (notation: $\models \{A\}\, c\, \{B\}$) if $\models^I \{A\}\, c\, \{\Downarrow B\}$ for every $I \in \mathit{Int}$.

Proving Total Correctness I

Goal: syntactic derivation of valid total correctness properties

Definition 12.2 (Hoare Logic for total correctness)

The Hoare rules for total correctness are given by

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

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

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

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

where $i \in \mathit{LVar}$.

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.

Proving Total Correctness II

- In rule

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

  the notation $A(i)$ indicates that assertion A parametrically depends on the value of the logical variable $i \in \mathit{LVar}$.

Proving Total Correctness II

- In rule

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

  the notation $A(i)$ indicates that assertion A parametrically depends on the value of the logical variable $i \in \mathit{LVar}$.

- Idea: i represents the remaining number of loop iterations

Proving Total Correctness II

- In rule

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

  the notation $A(i)$ indicates that assertion A parametrically depends on the value of the logical variable $i \in \mathit{LVar}$.

- Idea: i represents the remaining number of loop iterations
- Loop to be traversed $i+1$ times ($i \geq 0$)
  $\Rightarrow A(i+1)$ holds
  $\Rightarrow$ execution condition b satisfied

  Thus: $\models (i \geq 0 \wedge A(i+1) \Rightarrow b)$, and $i+1$ decreased to i after execution of c

Proving Total Correctness II

- In rule

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

  the notation $A(i)$ indicates that assertion A parametrically depends on the value of the logical variable $i \in \mathit{LVar}$.

- Idea: i represents the remaining number of loop iterations
- Loop to be traversed $i+1$ times ($i \geq 0$)
  $\Rightarrow A(i+1)$ holds
  $\Rightarrow$ execution condition b satisfied

  Thus: $\models (i \geq 0 \wedge A(i+1) \Rightarrow b)$, and $i+1$ decreased to i after execution of c
- Execution terminated
  $\Rightarrow A(0)$ holds
  $\Rightarrow$ execution condition b violated

  Thus: $\models (A(0) \Rightarrow \neg b)$

Total Correctness of Factorial Program

Example 12.3

Proof of $\{A\}\,\texttt{y:=1;}c\,\{\Downarrow B\}$ where

$$
\begin{aligned}
A &:= (\texttt{x} > 0 \wedge \texttt{x} = i) \\
c &:= \texttt{while } \neg\texttt{(x=1) do (y:=y*x; x:=x-1)} \\
B &:= (\texttt{y} = i!)
\end{aligned}
$$

(on the board)

Outline

Soundness

In analogy to Theorem 11.2 we can show that the Hoare Logic for total correctness properties is also sound:

Theorem 12.4 (Soundness)

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

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

Soundness

In analogy to Theorem 11.2 we can show that the Hoare Logic for total correctness properties is also sound:

Theorem 12.4 (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 $\vdash \{A\}\, c\, \{\Downarrow B\}$ (only (while) case; on the board) □

Relative Completeness

Also the counterpart to Cook's Completeness Theorem 11.5 applies:

Theorem 12.5 (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.

omitted □