

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)



noll@cs.rwth-aachen.de

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

Winter Semester 2011/12

- 1 Repetition: Hoare Logic
- 2 Total Correctness
- 3 Soundness and Completeness of Total Correctness

Hoare Logic

Goal: syntactic derivation of valid partial correctness properties

Definition (Hoare Logic)

The **Hoare rules** are given by

$$\begin{array}{c} \text{(skip)} \frac{}{\{A\} \text{ skip } \{A\}} \qquad \text{(asgn)} \frac{}{\{A[x \mapsto a]\} x := a \{A\}} \\ \text{(seq)} \frac{\{A\} c_1 \{C\} \quad \{C\} c_2 \{B\}}{\{A\} c_1 ; c_2 \{B\}} \qquad \text{(if)} \frac{\{A \wedge b\} c_1 \{B\} \quad \{A \wedge \neg b\} c_2 \{B\}}{\{A\} \text{ if } b \text{ then } c_1 \text{ else } c_2 \{B\}} \\ \text{(while)} \frac{\{A \wedge b\} c \{A\}}{\{A\} \text{ while } b \text{ do } c \{A \wedge \neg b\}} \\ \text{(cons)} \frac{\models (A \Rightarrow A') \quad \{A'\} c \{B'\} \quad \models (B' \Rightarrow B)}{\{A\} c \{B\}} \end{array}$$

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 .

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 $I \in Int$ such that $\sigma \models^I A$, $\mathcal{C}[[c]]\sigma \models^I B$ (on the board).

(If $\sigma = \perp$, then $\mathcal{C}[[c]]\sigma = \perp \models^I B$ holds trivially.)



(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 $\{A\} c \{B\}$:

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



Stephen A. Cook
(* 1939)

- 1 Repetition: Hoare Logic
- 2 Total Correctness
- 3 Soundness and Completeness of 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 $c \in \text{Cmd}$ and $A, B \in \text{Assn}$

- 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 .

Definition 12.1 (Semantics of total correctness properties)

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

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

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

$$\begin{array}{l} \text{(skip)} \frac{}{\{A\} \text{ skip } \{\Downarrow A\}} \qquad \text{(asgn)} \frac{}{\{A[x \mapsto a]\} x := a \{\Downarrow A\}} \\ \text{(seq)} \frac{\{A\} c_1 \{\Downarrow C\} \quad \{C\} c_2 \{\Downarrow B\}}{\{A\} c_1; c_2 \{\Downarrow B\}} \qquad \text{(if)} \frac{\{A \wedge b\} c_1 \{\Downarrow B\} \quad \{A \wedge \neg b\} c_2 \{\Downarrow B\}}{\{A\} \text{ if } b \text{ then } c_1 \text{ else } c_2 \{\Downarrow B\}} \\ \text{(while)} \frac{\vdash (i \geq 0 \wedge A(i+1) \Rightarrow b) \quad \{i \geq 0 \wedge A(i+1)\} c \{\Downarrow A(i)\} \quad \vdash (A(0) \Rightarrow \neg b)}{\{\exists i. i \geq 0 \wedge A(i)\} \text{ while } b \text{ do } c \{\Downarrow A(0)\}} \\ \text{(cons)} \frac{\vdash (A \Rightarrow A') \quad \{A'\} c \{\Downarrow B'\} \quad \vdash (B' \Rightarrow B)}{\{A\} c \{\Downarrow B\}} \end{array}$$

where $i \in LVar$.

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

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

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

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

Example 12.3

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

```
A := (x > 0 ∧ x = i)
c := while ¬(x=1) do (y:=y*x; x:=x-1)
B := (y = i!)
```

(on the board)

- 1 Repetition: Hoare Logic
- 2 Total Correctness
- 3 Soundness and Completeness of Total Correctness

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) □

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

