

Semantics and Verification of Software

Lecture 10: Axiomatic Semantics of WHILE II (Soundness of Hoare Logic)

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/svsw08/`

Winter semester 2008/09

Tag der Informatik
am 5. Dezember 2008

tdi2008

Program:

10:30–12:00 PhD Kolloquium (AH 5)

13:00–16:15 Opening and Talks (AH 5)

16:45–17:45 Software Award (AH 5)

18:00–19:15 Graduation Ceremony (Aula 2)

from 19:30 Party Time (AH 5)

- 1 Repetition: Hoare Logic
- 2 Soundness of Hoare Logic

Definition (Partial correctness properties)

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

- An expression of the form $\{A\} c \{B\}$ is called a **partial correctness property** with **precondition** A and **postcondition** B .
- Given $\sigma \in \Sigma_{\perp}$ and $I \in \text{Int}$, we let

$$\sigma \models^I \{A\} c \{B\}$$

if $\sigma \models^I A$ implies $\mathfrak{C}[\![c]\!]\sigma \models^I B$
(or equivalently: $\sigma \in A^I \implies \mathfrak{C}[\![c]\!]\sigma \in B^I$).

- $\{A\} c \{B\}$ is called **valid in I** (notation: $\models^I \{A\} c \{B\}$) if $\sigma \models^I \{A\} c \{B\}$ for every $\sigma \in \Sigma_{\perp}$ (or equivalently: $\mathfrak{C}[\![c]\!]A^I \subseteq B^I$).
- $\{A\} c \{B\}$ is called **valid** (notation: $\models \{A\} c \{B\}$) if $\models^I \{A\} c \{B\}$ for every $I \in \text{Int}$.

Hoare Logic I

Goal: syntactic derivation of valid partial correctness properties

Definition (Hoare Logic)

The **Hoare rules** are given by

$$\begin{array}{c} \text{(skip)} \frac{}{\{A\} \text{ skip } \{A\}} \qquad \text{(asgn)} \frac{}{\{A[x \mapsto a]\} x := a \{A\}} \\[10pt] \text{(seq)} \frac{\{A\} c_1 \{C\} \quad \{C\} c_2 \{B\}}{\{A\} c_1 ; c_2 \{B\}} \qquad \text{(if)} \frac{\{A \wedge b\} c_1 \{B\} \quad \{A \wedge \neg b\} c_2 \{B\}}{\{A\} \text{ if } b \text{ then } c_1 \text{ else } c_2 \{B\}} \\[10pt] \text{(while)} \frac{\{A \wedge b\} c \{A\}}{\{A\} \text{ while } b \text{ do } c \{A \wedge \neg b\}} \\[10pt] \text{(cons)} \frac{\models (A \implies A') \quad \{A'\} c \{B'\} \models (B' \implies B)}{\{A\} c \{B\}} \end{array}$$

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 .

Example

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

$c := (\text{while } \neg(x=1) \text{ do } (y:=y*x; x:=x-1))$

$A := (x = i)$

$B := (y = i!)$

(on the board)

Structure of the proof:

$$\begin{array}{c}
 \text{(seq)} \frac{\text{(cons)} \frac{\overline{4} \text{(asgn)} \overline{5} \overline{6}}{2} \text{(cons)} \overline{7} \text{(while)} \frac{\text{(cons)} \frac{\overline{11} \text{(seq)} \frac{\text{(asgn)} \overline{14} \text{(asgn)} \overline{15}}{12}}{10}}{8}}{9}}{1}
 \end{array}$$

Example (continued)

Here the single propositions are given by:

- ① $C := (x > 0 \implies y * x! = i! \wedge i \geq x)$
- ② $\{A\} y := 1; c \{B\}$
- ③ $\{A\} y := 1 \{C\}$
- ④ $\{C\} c \{B\}$
- ⑤ $\models (A \implies C[y \mapsto 1])$
- ⑥ $\{C[y \mapsto 1]\} y := 1 \{C\}$
- ⑦ $\models (C \implies C)$
- ⑧ $\models (C \implies C)$
- ⑨ $\{C\} c \{\neg(\neg(x = 1)) \wedge C\}$
- ⑩ $\models (\neg(\neg(x = 1)) \wedge C \implies B)$
- ⑪ $\{\neg(x = 1) \wedge C\} y := y * x; x := x - 1 \{C\}$
- ⑫ $\models (\neg(x = 1) \wedge C \implies C[x \mapsto x - 1, y \mapsto y * x])$
- ⑬ $\{C[x \mapsto x - 1, y \mapsto y * x]\} y := y * x; x := x - 1 \{C\}$
- ⑭ $\models (C \implies C)$
- ⑮ $\{C[x \mapsto x - 1, y \mapsto y * x]\} y := y * x \{C[x \mapsto x - 1]\}$
- ⑯ $\{C[x \mapsto x - 1]\} x := x - 1 \{C\}$

- 1 Repetition: Hoare Logic
- 2 Soundness of Hoare Logic

Soundness: no wrong propositions can be derived, i.e., every (syntactically) provable partial correctness property is also (semantically) valid

For the corresponding proof we use:

Lemma 10.1 (Substitution lemma)

For every $A \in Assn$, $x \in Var$, $a \in AExp$, $\sigma \in \Sigma$, and $I \in Int$:

$$\sigma \models^I A[x \mapsto a] \iff \sigma[x \mapsto \mathcal{A}[[a]]\sigma] \models^I A.$$

Proof.

by induction over $A \in Assn$ (omitted) □

Theorem 10.2 (Soundness of Hoare Logic)

For every partial correctness property $\{A\} c \{B\}$,
$$\vdash \{A\} c \{B\} \implies \models \{A\} c \{B\}.$$

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 $\sigma \models^I A$, $\mathfrak{C}[c]\sigma \models^I B$ (on the board).
(If $\sigma = \perp$, then $\mathfrak{C}[c]\sigma = \perp \models^I B$ holds trivially.) □