



Semantics and Verification of Software

Winter Semester 2017/18

Lecture 10: Axiomatic Semantics of WHILE II (Soundness & Completeness)

Thomas Noll

Software Modeling and Verification Group

RWTH Aachen University

<http://moves.rwth-aachen.de/teaching/ws-1718/sv-sw/>

Recap: Axiomatic Semantics of WHILE

Outline of Lecture 10

Recap: Axiomatic Semantics of WHILE

Soundness of Hoare Logic

(In-)Completeness of Hoare Logic

Relative Completeness of Hoare Logic

Recap: Axiomatic Semantics of WHILE

Partial Correctness Properties

Validity of partial correctness property

$\{A\} c \{B\}$ is **valid** iff for all states $\sigma \in \Sigma$ which satisfy A :
if the execution of c in σ terminates in $\sigma' \in \Sigma$, then σ' satisfies B .

Recap: Axiomatic Semantics of WHILE

Syntax of Assertion Language

Definition (Syntax of assertions)

The **syntax of *Assn*** is defined by the following context-free grammar:

$$\begin{aligned} a &::= z \mid x \mid i \mid a_1 + a_2 \mid a_1 - a_2 \mid a_1 * a_2 \in LExp \\ A &::= t \mid a_1 = a_2 \mid a_1 > a_2 \mid \neg A \mid A_1 \wedge A_2 \mid A_1 \vee A_2 \mid \forall i. A \in Assn \end{aligned}$$

- Thus: $AExp \subsetneq LExp$, $BExp \subsetneq Assn$
- The following (and other) **abbreviations** will be employed:

$$\begin{aligned} A_1 \Rightarrow A_2 &:= \neg A_1 \vee A_2 \\ \exists i. A &:= \neg(\forall i. \neg A) \\ a_1 \geq a_2 &:= a_1 > a_2 \vee a_1 = a_2 \\ &\vdots \end{aligned}$$

Recap: Axiomatic Semantics of WHILE

Semantics of $LExp$

The semantics now additionally depends on values of logical variables:

Definition (Semantics of $LExp$)

An **interpretation** is an element of the set $Int := \{I \mid I : LVar \rightarrow \mathbb{Z}\}$. The **value of an arithmetic expressions with logical variables** is given by the functional

$$\mathcal{L}[\cdot] : LExp \rightarrow (Int \rightarrow (\Sigma \rightarrow \mathbb{Z}))$$

where

$$\begin{array}{ll} \mathcal{L}[z] l\sigma := z & \mathcal{L}[a_1 + a_2] l\sigma := \mathcal{L}[a_1] l\sigma + \mathcal{L}[a_2] l\sigma \\ \mathcal{L}[x] l\sigma := \sigma(x) & \mathcal{L}[a_1 - a_2] l\sigma := \mathcal{L}[a_1] l\sigma - \mathcal{L}[a_2] l\sigma \\ \mathcal{L}[i] l\sigma := I(i) & \mathcal{L}[a_1 * a_2] l\sigma := \mathcal{L}[a_1] l\sigma \cdot \mathcal{L}[a_2] l\sigma \end{array}$$

Definition 6.1 (denotational semantics of arithmetic expressions) implies:

Corollary

For every $a \in AExp$ (without logical variables), $I \in Int$, and $\sigma \in \Sigma$:

$$\mathcal{L}[a] l\sigma = \mathcal{U}[a] \sigma.$$

Recap: Axiomatic Semantics of WHILE

Semantics of Assertions

Reminder: $A ::= t \mid a_1 = a_2 \mid a_1 > a_2 \mid \neg A \mid A_1 \wedge A_2 \mid A_1 \vee A_2 \mid \forall i. A \in Assn$

Definition (Semantics of assertions)

Let $A \in Assn$, $\sigma \in \Sigma_{\perp}$, and $I \in Int$. The relation “ σ satisfies A in I ” (notation: $\sigma \models^I A$) is inductively defined by:

$$\begin{aligned} \sigma &\models^I \text{true} \\ \sigma &\models^I a_1 = a_2 && \text{if } \mathcal{L}[[a_1]]I\sigma = \mathcal{L}[[a_2]]I\sigma \\ \sigma &\models^I a_1 > a_2 && \text{if } \mathcal{L}[[a_1]]I\sigma > \mathcal{L}[[a_2]]I\sigma \\ \sigma &\models^I \neg A && \text{if not } \sigma \models^I A \\ \sigma &\models^I A_1 \wedge A_2 && \text{if } \sigma \models^I A_1 \text{ and } \sigma \models^I A_2 \\ \sigma &\models^I A_1 \vee A_2 && \text{if } \sigma \models^I A_1 \text{ or } \sigma \models^I A_2 \\ \sigma &\models^I \forall i. A && \text{if } \sigma \models^{[i \rightarrow z]} A \text{ for every } z \in \mathbb{Z} \\ \perp &\models^I A \end{aligned}$$

Furthermore σ satisfies A ($\sigma \models A$) if $\sigma \models^I A$ for every interpretation $I \in Int$, and A is called **valid** ($\models A$) if $\sigma \models A$ for every state $\sigma \in \Sigma$.

Recap: Axiomatic Semantics of WHILE

Partial Correctness Properties

Definition (Partial correctness properties)

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

- 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 $I \in Int$, we let

$$\sigma \models' \{A\} c \{B\}$$

if $\sigma \models' A$ implies $\mathcal{C}[[c]]\sigma \models' B$ (or equivalently: $\sigma \in A' \Rightarrow \mathcal{C}[[c]]\sigma \in B'$).

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

Recap: Axiomatic Semantics of WHILE

Hoare Logic

Goal: syntactic derivation of valid partial correctness properties.
Here $A[x \mapsto a]$ denotes the syntactic replacement of every occurrence of x by a in A .



Tony Hoare (* 1934)

Definition (Hoare Logic)

The **Hoare rules** are given by

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

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

Soundness of Hoare Logic

Outline of Lecture 10

Recap: Axiomatic Semantics of WHILE

Soundness of Hoare Logic

(In-)Completeness of Hoare Logic

Relative Completeness of Hoare Logic

Soundness of Hoare Logic

Soundness of Hoare Logic I

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

Soundness of Hoare Logic

Soundness of Hoare Logic I

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 $I \in Int$:

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

Soundness of Hoare Logic

Soundness of Hoare Logic I

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 $I \in Int$:

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

Proof.

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

Soundness of Hoare Logic

Soundness of Hoare Logic II

Theorem 10.2 (Soundness of Hoare Logic)

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

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

Soundness of Hoare Logic

Soundness of Hoare Logic II

Theorem 10.2 (Soundness of Hoare Logic)

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

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

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 $I \in \text{Int}$ such that $\sigma \models' A$, $\mathcal{C}[[c]]\sigma \models' B$ (on the board). (If $\sigma = \perp$, then $\mathcal{C}[[c]]\sigma = \perp \models' B$ holds trivially.) □

(In-)Completeness of Hoare Logic

Outline of Lecture 10

Recap: Axiomatic Semantics of WHILE

Soundness of Hoare Logic

(In-)Completeness of Hoare Logic

Relative Completeness of Hoare Logic

(In-)Completeness of Hoare Logic

Incompleteness of Hoare Logic I

Soundness: only valid partial correctness properties are provable ✓

Completeness: all valid partial correctness properties are systematically derivable ⚡

(In-)Completeness of Hoare Logic

Incompleteness of Hoare Logic I

Soundness: only valid partial correctness properties are provable ✓

Completeness: all valid partial correctness properties are systematically derivable ⚡

Theorem 10.3 (Gödel's Incompleteness Theorem)

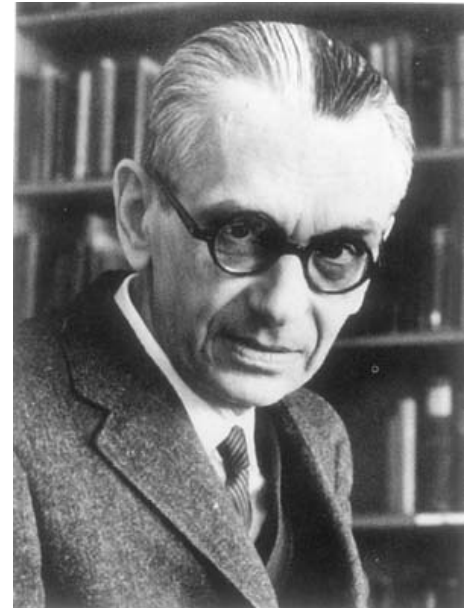
The set of all valid assertions

$$\{A \in Assn \mid \models A\}$$

is not recursively enumerable, i.e., there exists no proof system for $Assn$ in which all valid assertions are systematically derivable.

Proof.

see [Winskel 1996, p. 110 ff] □



Kurt Gödel
(1906–1978)

Incompleteness of Hoare Logic II

Corollary 10.4

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

(In-)Completeness of Hoare Logic

Incompleteness of Hoare Logic II

Corollary 10.4

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

Proof.

Given $A \in Assn$, $\models A$ is obviously equivalent to $\{\text{true}\} \text{skip} \{A\}$. Thus the enumerability of all valid partial correctness properties would imply the enumerability of all valid assertions. □

(In-)Completeness of Hoare Logic

Incompleteness of Hoare Logic II

Corollary 10.4

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

Proof.

Given $A \in \text{Assn}$, $\models A$ is obviously equivalent to $\{\text{true}\} \text{skip} \{A\}$. Thus the enumerability of all valid partial correctness properties would imply the enumerability of all valid assertions. □

Remark: alternative proof (using computability theory):

$\{\text{true}\} c \{\text{false}\}$ is valid iff c does not terminate on any input state. But the set of all non-terminating WHILE statements is not enumerable.

Relative Completeness of Hoare Logic

Outline of Lecture 10

Recap: Axiomatic Semantics of WHILE

Soundness of Hoare Logic

(In-)Completeness of Hoare Logic

Relative Completeness of Hoare Logic

Relative Completeness of Hoare Logic

Relative Completeness of Hoare Logic I

- We will see: actual reason of incompleteness is rule

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

since it is based on the **validity of implications** within *Assn*

Relative Completeness of Hoare Logic

Relative Completeness of Hoare Logic I

- We will see: actual reason of incompleteness is rule

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

since it is based on the **validity of implications** within *Assn*

- The other language constructs are “enumerable”

Relative Completeness of Hoare Logic

Relative Completeness of Hoare Logic I

- We will see: actual reason of incompleteness is rule

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

since it is based on the **validity of implications** within *Assn*

- The other language constructs are “enumerable”
- Therefore: **separation** of proof system (Hoare Logic) and assertion language (*Assn*)

Relative Completeness of Hoare Logic

Relative Completeness of Hoare Logic I

- We will see: actual reason of incompleteness is rule

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

since it is based on the **validity of implications** within *Assn*

- The other language constructs are “enumerable”
- Therefore: **separation** of proof system (Hoare Logic) and assertion language (*Assn*)
- One can show: if an “oracle” is available which decides whether a given assertion is valid, then all valid partial correctness properties can be systematically derived

Relative Completeness of Hoare Logic

Relative Completeness of Hoare Logic I

- We will see: actual reason of incompleteness is rule

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

since it is based on the **validity of implications** within *Assn*

- The other language constructs are “enumerable”
 - Therefore: **separation** of proof system (Hoare Logic) and assertion language (*Assn*)
 - One can show: if an “oracle” is available which decides whether a given assertion is valid, then all valid partial correctness properties can be systematically derived
- ⇒ **“Relative completeness”**

Relative Completeness of Hoare Logic

Relative Completeness of Hoare Logic II

Theorem 10.5 (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)

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

Relative Completeness of Hoare Logic

Relative Completeness of Hoare Logic II

Theorem 10.5 (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)

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

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* $C \in \text{Assn}$ such that $\{A\} c_1 \{C\}$ and $\{C\} c_2 \{B\}$. How to find it?

Relative Completeness of Hoare Logic

Weakest Preconditions I

Definition 10.6 (Weakest precondition)

Given $c \in \text{Cmd}$, $B \in \text{Assn}$ and $I \in \text{Int}$, the **weakest (liberal) precondition** of B with respect to c under I is defined by:

$$wp'[[c, B]] := \{\sigma \in \Sigma_{\perp} \mid \mathcal{C}[[c]]\sigma \models' B\}.$$

Relative Completeness of Hoare Logic

Weakest Preconditions I

Definition 10.6 (Weakest precondition)

Given $c \in \text{Cmd}$, $B \in \text{Assn}$ and $I \in \text{Int}$, the **weakest (liberal) precondition** of B with respect to c under I is defined by:

$$wp^I[[c, B]] := \{\sigma \in \Sigma_{\perp} \mid \mathcal{C}[[c]]\sigma \models^I B\}.$$

Corollary 10.7

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

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

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

Relative Completeness of Hoare Logic

Weakest Preconditions I

Definition 10.6 (Weakest precondition)

Given $c \in \text{Cmd}$, $B \in \text{Assn}$ and $I \in \text{Int}$, the **weakest (liberal) precondition** of B with respect to c under I is defined by:

$$wp^I[[c, B]] := \{\sigma \in \Sigma_{\perp} \mid \mathcal{C}[[c]]\sigma \models^I B\}.$$

Corollary 10.7

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

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

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

Remark: (2) justifies the notion of **weakest** precondition: it is implied by every precondition A that makes $\{A\} c \{B\}$ valid

Relative Completeness of Hoare Logic

Weakest Preconditions II

Definition 10.8 (Expressivity of assertion languages)

An assertion language $Assn$ is called **expressive** if, for every $c \in Cmd$ and $B \in Assn$, there exists $A_{c,B} \in Assn$ such that $A'_{c,B} = wp'[[c, B]]$ for every $I \in Int$.

Relative Completeness of Hoare Logic

Weakest Preconditions II

Definition 10.8 (Expressivity of assertion languages)

An assertion language $Assn$ is called **expressive** if, for every $c \in Cmd$ and $B \in Assn$, there exists $A_{c,B} \in Assn$ such that $A'_{c,B} = wp'[[c, B]]$ for every $I \in Int$.

Theorem 10.9 (Expressivity of $Assn$)

$Assn$ is expressive.

Relative Completeness of Hoare Logic

Weakest Preconditions II

Definition 10.8 (Expressivity of assertion languages)

An assertion language $Assn$ is called **expressive** if, for every $c \in Cmd$ and $B \in Assn$, there exists $A_{c,B} \in Assn$ such that $A'_{c,B} = wp'[c, B]$ for every $I \in Int$.

Theorem 10.9 (Expressivity of $Assn$)

$Assn$ is expressive.

Proof.

(idea; see [Winskel 1996, p. 103 ff for details])

Given $c \in Cmd$ and $B \in Assn$, construct $A_{c,B} \in Assn$ with

$\sigma \models' A_{c,B} \iff \mathcal{C}[c]\sigma \models' B$ (for every $\sigma \in \Sigma_{\perp}$, $I \in Int$). For example:

$$\begin{aligned} A_{\text{skip},B} &:= B & A_{x:=a,B} &:= B[x \mapsto a] \\ A_{c_1;c_2,B} &:= A_{c_1,A_{c_2,B}} & \dots & \end{aligned}$$

(for **while**: “Gödelization” of sequences of intermediate states) □

Relative Completeness of Hoare Logic

Relative Completeness of Hoare Logic III

The following lemma shows that weakest preconditions are “provable”:

Lemma 10.10

For every $c \in \text{Cmd}$ and $B \in \text{Assn}$: $\vdash \{A_{c,B}\} c \{B\}$

Relative Completeness of Hoare Logic

Relative Completeness of Hoare Logic III

The following lemma shows that weakest preconditions are “provable”:

Lemma 10.10

For every $c \in \text{Cmd}$ and $B \in \text{Assn}$: $\vdash \{A_{c,B}\} c \{B\}$

Proof.

by structural induction over c (omitted) □

Relative Completeness of Hoare Logic

Relative Completeness of Hoare Logic III

The following lemma shows that weakest preconditions are “provable”:

Lemma 10.10

For every $c \in \text{Cmd}$ and $B \in \text{Assn}$: $\vdash \{A_{c,B}\} c \{B\}$

Proof.

by structural induction over c (omitted) □

Proof (Cook’s Completeness Theorem 10.5).

We have to show that Hoare Logic is relatively complete, i.e., that

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

Relative Completeness of Hoare Logic

Relative Completeness of Hoare Logic III

The following lemma shows that weakest preconditions are “provable”:

Lemma 10.10

For every $c \in \text{Cmd}$ and $B \in \text{Assn}$: $\vdash \{A_{c,B}\} c \{B\}$

Proof.

by structural induction over c (omitted) □

Proof (Cook’s Completeness Theorem 10.5).

We have to show that Hoare Logic is relatively complete, i.e., that

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

- Lemma 10.10: $\vdash \{A_{c,B}\} c \{B\}$

Relative Completeness of Hoare Logic

Relative Completeness of Hoare Logic III

The following lemma shows that weakest preconditions are “provable”:

Lemma 10.10

For every $c \in \text{Cmd}$ and $B \in \text{Assn}$: $\vdash \{A_{c,B}\} c \{B\}$

Proof.

by structural induction over c (omitted) □

Proof (Cook’s Completeness Theorem 10.5).

We have to show that Hoare Logic is relatively complete, i.e., that

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

- Lemma 10.10: $\vdash \{A_{c,B}\} c \{B\}$
- Corollary 10.7: $\models \{A\} c \{B\} \Rightarrow \models (A \Rightarrow A_{c,B})$

Relative Completeness of Hoare Logic

Relative Completeness of Hoare Logic III

The following lemma shows that weakest preconditions are “provable”:

Lemma 10.10

For every $c \in \text{Cmd}$ and $B \in \text{Assn}$: $\vdash \{A_{c,B}\} c \{B\}$

Proof.

by structural induction over c (omitted) □

Proof (Cook’s Completeness Theorem 10.5).

We have to show that Hoare Logic is relatively complete, i.e., that

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

- Lemma 10.10: $\vdash \{A_{c,B}\} c \{B\}$
- Corollary 10.7: $\models \{A\} c \{B\} \Rightarrow \models (A \Rightarrow A_{c,B})$
- $\frac{\models (A \Rightarrow A_{c,B}) \quad \vdash \{A_{c,B}\} c \{B\} \quad \models (B \Rightarrow B)}{\vdash \{A\} c \{B\}}$ (cons) □