

# Axiomatic semantics

CS 152 (Spring 2021)

Harvard University

Thursday, April 1, 2021

# Today, we will learn about

- ▶ Axiomatic Semantics
  - ▶ Pre- and Post-Conditions
  - ▶ Partial and Total Correctness
  - ▶ Validity of Assertions and Partial Correctness
  - ▶ Hoare Logic

# Meaning of Programs by

**operational model** how programs execute

**denotational model** what programs compute

**axiomatic model** logical formulas satisfied by the  
program

# Axiomatic Semantics

- ▶ give specifications for what programs are supposed to compute
- ▶ define the meaning of programs in terms of logical formulas satisfied by the program

# Pre- and Post-Conditions

$$\{Pre\} \ c \ \{Post\}$$

# Pre- and Post-Conditions

$$\{Pre\} \ c \ \{Post\}$$

“If *Pre* holds before *c*, and *c* terminates, then *Post* holds after *c*.”

# Partial Correctness and Total Correctness

$$\{Pre\} c \{Post\}$$

“If *Pre* holds before *c*, **and** *c* **terminates**, **then**  
*Post* holds after *c*.”

# Partial Correctness and Total Correctness

$$\{Pre\} c \{Post\}$$

“If *Pre* holds before *c*, **and** *c* **terminates**, **then**  
*Post* holds after *c*.”

$$[Pre] c [Post]$$

“If *Pre* holds before *c* **then** *c* **will terminate** and  
*Post* will hold after *c*.”



# Example

$\{\text{foo} = 0 \wedge \text{bar} = i\}$

$\text{baz} := 0;$

**while**  $\text{foo} \neq \text{bar}$  **do**

$(\text{baz} := \text{baz} - 2; \text{foo} := \text{foo} + 1)$

$\{\text{baz} = -2i\}$

# Total Correctness Example

```
[foo = 0 ∧ bar = i  
  ∧ i ≥ 0]  
  baz := 0;  
  while foo ≠ bar do  
    (baz := baz - 2; foo := foo + 1)  
[baz = -2i]
```

# Invalid Example

$\{\text{foo} = 0 \wedge \text{bar} = i\}$

baz := 0;

**while** foo  $\neq$  bar **do**

(baz := baz + foo; foo := foo + 1)

$\{\text{baz} = i\}$

## Invalid Example 2

$$\{a = i\}$$
$$x := 3;$$
$$y := a$$
$$\{y = i\}$$

Find  $a$  such that this triple is invalid.

# Formalization

- ▶ What logic do we use for writing assertions?  
That is, what can we express in pre- and post-condition?
- ▶ What does it mean that an assertion is valid?  
What does it mean that a partial correctness statement  $\{Pre\} c \{Post\}$  is valid?
- ▶ How can we prove that a partial correctness statement is valid?

# Language of Assertions

$P, Q \in \mathbf{Assn}$     $P ::=$  **true** | **false** |  $a_1 < a_2$  |  $a_1 = a_2$   
|  $P_1 \wedge P_2$  |  $P_1 \vee P_2$  |  $P_1 \Rightarrow P_2$   
|  $\neg P$  |  $\forall i. P$  |  $\exists i. P$

$a \in \mathbf{Aexp}$     $a ::=$   $n$  |  $x$  |  $a_1 + a_2$  |  $a_1 \times a_2$  |  $i$

$i, j \in \mathbf{LVar}$

# Validity of Assertions

# Validity of Assertions

- ▶ Interpretation  $I$ :

$$I : \mathbf{LVar} \rightarrow \mathbf{Int}$$

- ▶ “ $P$  is valid in store  $\sigma$  under interpretation  $I$ ”

$$\sigma \models_I P$$

- ▶ will write  $\sigma \not\models_I P$  whenever  $\sigma \models_I P$  doesn't hold



# Validity of Assertions

$\sigma \models_I \mathbf{true}$	(always)
$\sigma \models_I a_1 < a_2$	if $\mathcal{A}_{\text{Interp}}[[a_1]](\sigma, I) < \mathcal{A}_{\text{Interp}}[[a_2]](\sigma, I)$
$\sigma \models_I a_1 = a_2$	if $\mathcal{A}_{\text{Interp}}[[a_1]](\sigma, I) = \mathcal{A}_{\text{Interp}}[[a_2]](\sigma, I)$
$\sigma \models_I P_1 \wedge P_2$	if $\sigma \models_I P_1$ and $\sigma \models_I P_2$
$\sigma \models_I P_1 \vee P_2$	if $\sigma \models_I P_1$ or $\sigma \models_I P_2$
$\sigma \models_I P_1 \Rightarrow P_2$	if $\sigma \not\models_I P_1$ or $\sigma \models_I P_2$
$\sigma \models_I \neg P$	if $\sigma \not\models_I P$
$\sigma \models_I \forall i. P$	if $\forall k \in \text{Int}. \sigma \models_{I[i \rightarrow k]} P$
$\sigma \models_I \exists i. P$	if $\exists k \in \text{Int}. \sigma \models_{I[i \rightarrow k]} P$

$$\mathcal{A}_{\text{Interp}}[[n]](\sigma, I) = n$$

$$\mathcal{A}_{\text{Interp}}[[x]](\sigma, I) = \sigma(x)$$

$$\mathcal{A}_{\text{Interp}}[[i]](\sigma, I) = I(i)$$

$$\mathcal{A}_{\text{Interp}}[[a_1 + a_2]](\sigma, I) = \mathcal{A}_{\text{Interp}}[[a_1]](\sigma, I) + \mathcal{A}_{\text{Interp}}[[a_2]](\sigma, I)$$

# Validity of Partial Correctness

# Validity of Partial Correctness

$\{P\} c \{Q\}$  is valid in store  $\sigma$  and interpretation  $I$ ,  
written  $\sigma \models_I \{P\} c \{Q\}$ , if:

$\forall \sigma'. \text{ if } \sigma \models_I P \text{ and } \mathcal{C}[[c]]\sigma = \sigma' \text{ then } \sigma' \models_I Q$

# Validity of Partial Correctness

$\{P\} c \{Q\}$  is valid in store  $\sigma$  and interpretation  $I$ , written  $\sigma \models_I \{P\} c \{Q\}$ , if:

$\forall \sigma'. \text{ if } \sigma \models_I P \text{ and } \mathcal{C}[[c]]\sigma = \sigma' \text{ then } \sigma' \models_I Q$

A partial correctness triple is valid (written  $\models \{P\} c \{Q\}$ ), if it is valid in any store and interpretation:

$\forall \sigma, I. \sigma \models_I \{P\} c \{Q\}$ .

# Outlook

Now we know what we mean when we say  
“assertion  $P$  holds” or “partial correctness  
statement  $\{P\} c \{Q\}$  is valid.”

# Hoare logic

# Hoare logic

How do we show that a partial correctness statement  $\{P\} c \{Q\}$  holds?

# Hoare logic

How do we show that a partial correctness statement  $\{P\} c \{Q\}$  holds?

We know that  $\{P\} c \{Q\}$  is valid if it holds for all stores and interpretations:  $\forall \sigma, I. \sigma \models_I \{P\} c \{Q\}$ .

Furthermore, showing that  $\sigma \models_I \{P\} c \{Q\}$  requires reasoning about the execution of command  $c$  (that is,  $\mathcal{C}[[c]]$ ), as indicated by the definition of validity.

It turns out that there is an elegant way of deriving valid partial correctness statements, without having to reason about stores, interpretations, and the execution of  $c$ . We can use a set of inference rules and axioms, called *Hoare* rules, to directly derive valid partial correctness statements. The set of rules forms a proof system known as Hoare logic.



# Hoare logic rules

# Hoare logic rules

These set of Hoare rules represent an inductive definition for a set of partial correctness statements  $\{P\} c \{Q\}$ . We will say that  $\{P\} c \{Q\}$  is a theorem in Hoare logic, written  $\vdash \{P\} c \{Q\}$ , if we can build a finite proof tree for it.

# Hoare logic rules (Skip)

$$\text{SKIP} \frac{}{\vdash \{P\} \mathbf{skip} \{P\}}$$

# Hoare logic rules (Assign)

$$\text{ASSIGN} \frac{}{\vdash \{P[a/x]\} x := a \{P\}}$$

# Puzzler: Why is this rule wrong?

WRONG-ASSIGN  $\frac{}{\vdash \{\mathbf{true}\} x := a \{x = a\}}$

# Hoare logic rules (Seq)

$$\text{SEQ} \frac{\vdash \{P\} c_1 \{R\} \quad \vdash \{R\} c_2 \{Q\}}{\vdash \{P\} c_1; c_2 \{Q\}}$$

# Hoare logic rules (If)

$$\text{IF} \frac{\vdash \{P \wedge b\} c_1 \{Q\} \quad \vdash \{P \wedge \neg b\} c_2 \{Q\}}{\vdash \{P\} \text{if } b \text{ then } c_1 \text{ else } c_2 \{Q\}}$$

# Hoare logic rules (While)

$$\text{WHILE} \frac{\vdash \{P \wedge b\} c \{P\}}{\vdash \{P\} \mathbf{while} \ b \ \mathbf{do} \ c \ \{P \wedge \neg b\}}$$



# Hoare logic rules (Consequence)

$$\text{CONSEQUENCE} \frac{\begin{array}{l} \models (P \Rightarrow P') \\ \models (Q' \Rightarrow Q) \\ \vdash \{P'\} c \{Q'\} \end{array}}{\vdash \{P\} c \{Q\}}$$

# Two kinds of partial correctness assertions

- a) valid partial correctness statements  
 $\models \{P\} c \{Q\}$ , which hold for all stores and interpretations, according to the semantics of  $c$ ; and
- b) Hoare logic theorems  $\vdash \{P\} c \{Q\}$ , that is, a partial correctness statement that can be derived using Hoare rules.

# Soundness and (Relative) Completeness of Hoare Logic

▶ soundness:

does  $\vdash \{P\} c \{Q\}$  imply  $\models \{P\} c \{Q\}$ ?

# Soundness and (Relative) Completeness of Hoare Logic

▶ soundness:

does  $\vdash \{P\} c \{Q\}$  imply  $\models \{P\} c \{Q\}$ ?

yes

# Soundness and (Relative) Completeness of Hoare Logic

- ▶ soundness:

does  $\vdash \{P\} c \{Q\}$  imply  $\models \{P\} c \{Q\}$ ?

yes

- ▶ completeness:

does  $\models \{P\} c \{Q\}$  imply  $\vdash \{P\} c \{Q\}$ ?

# Soundness and (Relative) Completeness of Hoare Logic

- ▶ soundness:

does  $\vdash \{P\} c \{Q\}$  imply  $\models \{P\} c \{Q\}$ ?

yes

- ▶ completeness:

does  $\models \{P\} c \{Q\}$  imply  $\vdash \{P\} c \{Q\}$ ?

qualified yes: if  $\models \{P\} c \{Q\}$  then there is a proof of  $\{P\} c \{Q\}$  using the rules of Hoare logic, provided there are proofs for the validity of assertions that occur in the rule of consequence  $\models (P \Rightarrow P')$  and  $\models (Q' \Rightarrow Q)$ .

# Proof of Soundness (Overview)

By induction on the derivation  $\vdash \{P\} c \{Q\}$ .  
It suffices to show, for each inference rule, that if each hypothesis holds semantically, then the conclusion holds semantically.

## Soundness Proof Case (If)

$$\text{IF} \frac{\vdash \{P \wedge b\} c_1 \{Q\} \quad \vdash \{P \wedge \neg b\} c_2 \{Q\}}{\vdash \{P\} \text{if } b \text{ then } c_1 \text{ else } c_2 \{Q\}}$$

Assume  $\models \{P \wedge b\} c_1 \{Q\}$  and  $\models \{P \wedge \neg b\} c_2 \{Q\}$ .

Let  $I$  be an interpretation.

Suppose  $\sigma \models_I P$ . Either  $\sigma \models_I b$  or  $\sigma \models_I \neg b$ .

If  $\sigma \models_I b$ , then  $\sigma \models P \wedge b$  so  $\mathcal{C}[[c_1]]\sigma \models_I Q$ .

Similarly for  $\sigma \models_I \neg b$ .

Thus,  $\models \{P\} \text{if } b \text{ then } c_1 \text{ else } c_2 \{Q\}$ .



# Factorial example using Hoare Logic

```
{X = x && X >= 0 && Y = 1}
{Y * X! = x! && X >= 0}
while X != 0 do
  ({Y * X! = x! && X >= 0 && X != 0}
  {(Y * X) * (X - 1)! = x! && (X - 1) >= 0}
  Y := Y * X;
  {Y * (X - 1)! = x! && (X - 1) >= 0}
  X := X - 1
  {Y * X! = x! && X >= 0})
{Y * X! = x! && X >= 0 && ¬(X != 0)}
{Y = x!}
```