Axiomatic semantics

CS 152 (Spring 2024)

Harvard University

Tuesday, April 2, 2024

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

$$\{\mathsf{foo} = 0 \land \mathsf{bar} = i\}$$

```
baz := 0;
while foo ≠ bar do
    (baz := baz − 2; foo := foo + 1)
```

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

Total Correctness Example

```
[$\mathsf{foo} = 0 \land \mathsf{bar} = i$
          $\land i \geq 0$]
               $\mathsf{baz} := 0;$
               while $\mathsf{foo} \neq \mathsf{bar}$ do
                  $(\mathsf{baz} := \mathsf{baz} - 2; \mathsf{foo} := \mathsf{foo} + 1)$
      [$\mathsf{baz} = -2i$]
```

Invalid Example

$$\{\mathsf{foo} = 0 \land \mathsf{bar} = i\}$$

```
$\mathsf{baz} := 0;$
$\textbf{while}\ \mathsf{foo} \neq \mathsf{bar}\ \textbf{do}$
$(\mathsf{baz} := \mathsf{baz} + \mathsf{foo}; \mathsf{foo} := \mathsf{foo} + 1)$
```

$$\{\mathsf{baz} = i\}$$

Invalid Example 2

$$\{a = i\}$$

$$\text{x} := 3;$$

$$\text{y} := a$$

$$\{y = i\}$$

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

$$\begin{array}{lrl}
P, Q \in \textbf{Assn} & P ::= & \textbf{true} \mid \textbf{false} \mid a_1 < a_2 \mid a_1 = a_2 \\
 & & \mid P_1 \wedge P_2 \mid P_1 \vee P_2 \mid P_1 \Rightarrow P_2 \\
 & & \mid \neg P \mid \forall i.\ P \mid \exists i.\ P \\
a \in \textbf{Aexp} & a ::= & n \mid x \mid a_1 + a_2 \mid a_1 \times a_2 \mid i \\
i, j \in \textbf{LVar} & &
\end{array}$$

Validity of Assertions

Validity of Assertions

- Interpretation I:

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

- "P is valid in store σ 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

$\sigma \vDash_I \textbf{true}$	(always)
$\sigma \vDash_I a_1 < a_2$	if $\mathcal{A}_{\text{Interp}}[\![a_1]\!](\sigma, I) < \mathcal{A}_{\text{Interp}}[\![a_2]\!](\sigma, I)$
$\sigma \vDash_I a_1 = a_2$	if $\mathcal{A}_{\text{Interp}}[\![a_1]\!](\sigma, I) = \mathcal{A}_{\text{Interp}}[\![a_2]\!](\sigma, I)$
$\sigma \vDash_I P_1 \wedge P_2$	if $\sigma \vDash_I P_1$ and $\sigma \vDash_I P_2$
$\sigma \vDash_I P_1 \vee P_2$	if $\sigma \vDash_I P_1$ or $\sigma \vDash_I P_2$
$\sigma \vDash_I P_1 \Rightarrow P_2$	if $\sigma \nvDash_I P_1$ or $\sigma \vDash_I P_2$
$\sigma \vDash_I \neg P$	if $\sigma \nvDash_I P$
$\sigma \vDash_I \forall i.\ P$	if $\forall k \in Int.\ \sigma \vDash_{I[i \mapsto k]} P$
$\sigma \vDash_I \exists i.\ P$	if $\exists k \in Int.\ \sigma \vDash_{I[i \mapsto k]} P$

$$\begin{aligned}
\mathcal{A}_{\text{Interp}}[\![n]\!](\sigma, I) &= n \\
\mathcal{A}_{\text{Interp}}[\![x]\!](\sigma, I) &= \sigma(x) \\
\mathcal{A}_{\text{Interp}}[\![i]\!](\sigma, I) &= I(i) \\
\mathcal{A}_{\text{Interp}}[\![a_1 + a_2]\!](\sigma, I) &= \mathcal{A}_{\text{Interp}}[\![a_1]\!](\sigma, I) + \mathcal{A}_{\text{Interp}}[\![a_2]\!](\sigma, I)
\end{aligned}$$

Validity of Partial Correctness

Validity of Partial Correctness

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

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

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

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

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

Furthermore, showing that $\sigma \vDash_I \{P\}\ c\ \{Q\}$ 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)

$$\textsc{Skip}\ \frac{}{\vdash \{P\}\ \textbf{skip}\ \{P\}}$$

Hoare logic rules (Assign)

$$\textsc{Assign}\ \frac{}{\vdash \{P[a/x]\}\ x := a\ \{P\}}$$

Puzzler: Why is this rule wrong?

$$\textsc{Wrong-Assign}\ \frac{}{\vdash \{\textbf{true}\}\ x := a\ \{x = a\}}$$

Hoare logic rules (Seq)

$$\textsc{Seq}\ \frac{\vdash \{P\}\ c_1\ \{R\} \qquad \vdash \{R\}\ c_2\ \{Q\}}{\vdash \{P\}\ c_1; c_2\ \{Q\}}$$

Hoare logic rules (If)

$$\textsc{If}\ \frac{\vdash \{P \land b\}\ c_1\ \{Q\} \qquad \vdash \{P \land \neg b\}\ c_2\ \{Q\}}{\vdash \{P\}\ \textbf{if}\ b\ \textbf{then}\ c_1\ \textbf{else}\ c_2\ \{Q\}}$$

Hoare logic rules (While)

$$\textsc{While}\,\frac{\vdash \{P \land b\}\ c\ \{P\}}{\vdash \{P\}\ \textbf{while}\ b\ \textbf{do}\ c\ \{P \land \neg b\}}$$

Hoare logic rules (Consequence)

$$\textsc{Consequence}\ \frac{\begin{array}{c}\models (P \Rightarrow P') \\ \models (Q' \Rightarrow Q) \\ \vdash \{P'\}\ c\ \{Q'\}\end{array}}{\vdash \{P\}\ c\ \{Q\}}$$

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 $\quad \vdash \{P\}\ c\ \{Q\} \quad$ imply $\quad \vDash \{P\}\ c\ \{Q\}$?

Soundness and (Relative) Completeness of Hoare Logic

- soundness:

  does $\quad \vdash \{P\}\ c\ \{Q\} \quad$ imply $\quad \vDash \{P\}\ c\ \{Q\}$?

  yes

Soundness and (Relative) Completeness of Hoare Logic

- soundness:

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

  yes

- completeness:

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

Soundness and (Relative) Completeness of Hoare Logic

- soundness:

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

  yes

- completeness:

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

  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)

$$\textsc{If}\ \frac{\vdash \{P \land b\}\ c_1\ \{Q\} \qquad \vdash \{P \land \neg b\}\ c_2\ \{Q\}}{\vdash \{P\}\ \textbf{if}\ b\ \textbf{then}\ c_1\ \textbf{else}\ c_2\ \{Q\}}$$

Assume $\vDash \{P \land b\}\ c_1\ \{Q\}$ and $\vDash \{P \land \neg b\}\ c_2\ \{Q\}$.
Let I be an interpretation.
Suppose $\sigma \vDash_I P$. Either $\sigma \vDash_i b$ or $\sigma \vDash_i \neg b$.
If $\sigma \vDash_i b$, then $\sigma \vDash P \land b$ so $\mathcal{C}[\![c_1]\!]\sigma \vDash_I Q$.
Similarly for $\sigma \vDash_i \neg b$.
Thus, $\vDash \{P\}\ \textbf{if}\ b\ \textbf{then}\ c_1\ \textbf{else}\ c_2\ \{Q\}$.

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!}
```

Weakest Preconditions and Verification Conditions

The weakest precondition $wpc(c, Q)$ is a precondition such that the Hoare triple $\{wpc(c, Q)\}\ c\ \{Q\}$ is valid and any other valid precondition P is stronger, i.e. $\vDash \{P\}\ c\ \{Q\}$ valid iff $P \Rightarrow wpc(c, Q)$.

Verification Conditions

The verification condition $\mathit{vc}(c, Q)$ is a valid precondition, so $\{\mathit{vc}(c, Q)\}\ c\ \{Q\}$ is guaranteed to be valid. However, it is not guaranteed to be the weakest precondition. This means that if $P \Rightarrow \mathit{vc}(c, Q)$, then we can be sure that $\vDash \{P\}\ c\ \{Q\}$, just from the rule of consequence. However, if $P \Rightarrow \mathit{vc}(c, Q)$ does not hold, then have no way of knowing whether it was because the Hoare triple $\{P\}\ c\ \{Q\}$ is not valid, or whether the triple is valid, but $\mathit{vc}(c, Q)$ was just not good enough to prove it.

Weakest Preconditions and Verification Conditions

- $wpc(\textbf{skip}, Q) = Q$
- $wpc(x := a, Q) = Q[a/x]$
- $wpc(c_1; c_2, Q) = wpc(c_1, wpc(c_2, Q))$
- $wpc(\textbf{if } b \textbf{ then } c_1 \textbf{ else } c_2, Q) =$
  $(b \wedge wpc(c_1, Q)) \vee (\neg b \wedge wpc(c_2, Q))$

Weakest Precondition While-Loop

Let $W = wpc(\textbf{while } b \textbf{ do } c, Q)$. Then,

$$W = b \Rightarrow wpc(c, W) \wedge \neg b \Rightarrow Q$$

Verification Condition While-Loop

$$vc(\textbf{while } b \textbf{ do } c, Q) =$$

$$I \wedge \forall x_1, \ldots x_n \; I \Rightarrow (b \Rightarrow vc(c, I) \wedge \neg b \Rightarrow Q)$$

where x_i are variables modified by c.