AAA616: Program Analysis

Lecture 5 — Axiomatic Semantics (Hoare Logic)

Hakjoo Oh
2024 Fall

Review: **IMP**

n, m will range over numerals, **N**
t will range over truth values, **T**$= \{$ **true**, **false** $\}$
X, Y will range over locations, **Loc**
a will range over arithmetic expressions, **Aexp**
b will range over boolean expressions, **Bexp**
c will range over statements, **Com**

$$
\begin{array}{lcl}
a & ::= & n \mid X \mid a_0 + a_1 \mid a_0 \star a_1 \mid a_0 - a_1 \\
b & ::= & \texttt{true} \mid \texttt{false} \mid a_0 = a_1 \mid a_0 \leq a_1 \mid \neg b \mid b_0 \wedge b_1 \mid b_0 \vee b_1 \\
c & ::= & X := a \mid \texttt{skip} \mid c_0; c_1 \mid \texttt{if}\ b\ \texttt{then}\ c_0\ \texttt{else}\ c_1 \mid \texttt{while}\ b\ \texttt{do}\ c
\end{array}
$$

Review: States

- The meaning of a program depends on the values bound to the locations that occur in the program, e.g., $X + 3$.
- A state is a function from locations to values:

$$\sigma, s \in \Sigma = \mathbf{Loc} \to \mathbf{N}$$

- Let σ be a state. Let $m \in \mathbf{N}$. Let $X \in \mathbf{Loc}$. We write $\sigma[m/X]$ (or $\sigma[X \mapsto m]$) for the state obtained from σ by replacing its contents in X by m, i.e.,

$$\sigma[m/X](Y) = \sigma[X \mapsto m] = \begin{cases} m & \text{if } Y = X \\ \sigma(Y) & \text{if } Y \neq X \end{cases}$$

- $\Sigma_\perp = \Sigma \cup \{\perp\}$

Review: Denotational Semantics

$$
\begin{array}{rcl}
\mathcal{A}[\![a]\!] & : & \Sigma \to \mathbf{N} \\
\mathcal{A}[\![n]\!](s) & = & n \\
\mathcal{A}[\![x]\!](s) & = & s(x) \\
\mathcal{A}[\![a_1 + a_2]\!](s) & = & \mathcal{A}[\![a_1]\!](s) + \mathcal{A}[\![a_2]\!](s) \\
\mathcal{A}[\![a_1 \star a_2]\!](s) & = & \mathcal{A}[\![a_1]\!](s) \times \mathcal{A}[\![a_2]\!](s) \\
\mathcal{A}[\![a_1 - a_2]\!](s) & = & \mathcal{A}[\![a_1]\!](s) - \mathcal{A}[\![a_2]\!](s)
\end{array}
$$

$$
\begin{array}{rcl}
\mathcal{B}[\![b]\!] & : & \Sigma \to \mathbf{T} \\
\mathcal{B}[\![\mathtt{true}]\!](s) & = & \mathrm{true} \\
\mathcal{B}[\![\mathtt{false}]\!](s) & = & \mathrm{false} \\
\mathcal{B}[\![a_1 = a_2]\!](s) & = & \mathcal{A}[\![a_1]\!](s) = \mathcal{A}[\![a_2]\!](s) \\
\mathcal{B}[\![a_1 \leq a_2]\!](s) & = & \mathcal{A}[\![a_1]\!](s) \leq \mathcal{A}[\![a_2]\!](s) \\
\mathcal{B}[\![\neg b]\!](s) & = & \mathcal{B}[\![b]\!](s) = \mathrm{false} \\
\mathcal{B}[\![b_1 \wedge b_2]\!](s) & = & \mathcal{B}[\![b_1]\!](s) \wedge \mathcal{B}[\![b_2]\!](s) \\
\mathcal{B}[\![b_1 \vee b_2]\!](s) & = & \mathcal{B}[\![b_1]\!](s) \vee \mathcal{B}[\![b_2]\!](s)
\end{array}
$$

Review: Denotational Semantics

$$
\begin{array}{rcl}
\mathcal{C}[\![c]\!] & : & \Sigma \hookrightarrow \Sigma \\
\mathcal{C}[\![x := a]\!](s) & = & s[x \mapsto \mathcal{A}[\![a]\!](s)] \\
\mathcal{C}[\![\texttt{skip}]\!] & = & \textbf{id} \\
\mathcal{C}[\![c_1; c_2]\!] & = & \mathcal{C}[\![c_2]\!] \circ \mathcal{C}[\![c_1]\!] \\
\mathcal{C}[\![\texttt{if } b\ c_1\ c_2]\!] & = & \textbf{cond}(\mathcal{B}[\![b]\!], \mathcal{C}[\![c_1]\!], \mathcal{C}[\![c_2]\!]) \\
\mathcal{C}[\![\texttt{while } b\ c]\!] & = & fix F
\end{array}
$$

where

$$
\textbf{cond}(f, g, h) = \lambda s. \begin{cases} g(s) & \cdots f(s) = \text{true} \\ h(s) & \cdots f(s) = \text{false} \end{cases}
$$

$$
F(g) = \textbf{cond}(\mathcal{B}[\![b]\!], g \circ \mathcal{C}[\![c]\!], \textbf{id})
$$

cf) Relational Denotational Semantics

$$
\begin{array}{rcl}
\mathcal{C}[\![c]\!] & : & \Sigma \hookrightarrow \Sigma \\
\mathcal{C}[\![x := a]\!] & = & \{(s, s[x \mapsto \mathcal{A}[\![a]\!](s)]) \mid s \in \Sigma\} \\
\mathcal{C}[\![\texttt{skip}]\!] & = & \{(s, s) \mid s \in \Sigma\} \\
\mathcal{C}[\![c_1; c_2]\!] & = & \mathcal{C}[\![c_2]\!] \circ \mathcal{C}[\![c_1]\!] \\
\mathcal{C}[\![\texttt{if}\ b\ c_1\ c_2]\!] & = & \{(s, s') \mid \mathcal{B}[\![b]\!](s) = \text{true}, (s, s') \in \mathcal{C}[\![c_1]\!]\} cup \\
 & & \{(s, s') \mid \mathcal{B}[\![b]\!](s) = \text{false}, (s, s') \in \mathcal{C}[\![c_2]\!]\} \\
\mathcal{C}[\![\texttt{while}\ b\ c]\!] & = & \mathit{fix} F
\end{array}
$$

where

$$
\begin{array}{rcl}
F(g) & = & \{(s, s') \mid \mathcal{B}[\![b]\!](s) = \text{true}, (s, s') \in g \circ \mathcal{C}[\![c]\!]\} \cup \\
 & & \{(s, s) \mid \mathcal{B}[\![b]\!](s) = \text{false}\}
\end{array}
$$

Hoare Logic

- A formal proof system for proving properties of programs.
- Partial correctness assertions:

$$\{A\}c\{B\}$$

"For all states σ which satisfy A, if the execution c from σ terminates in state σ' then σ' satisfies B"

- Examples:
  - Sum of the first hundred numbers:

$$\{S = 0 \land N = 1\}$$
$$\texttt{while } (N \neq 101) \texttt{ do } S := S + N; N := N + 1$$
$$\{S = \textstyle\sum_{1 \leq m \leq 100} m\}$$

  - Non-terminating program:

$$\{\mathbf{true}\}\texttt{while true do skip}\{\mathbf{false}\}$$

The Assertion Language **Assn**

n will range over numerals, **N**
X will range over locations, **Loc**
i will range over integer variables, **Intvar**
a will range over arithmetic expressions, **Aexpv**

$$
\begin{array}{rcl}
a & ::= & n \mid X \mid i \mid a_0 + a_1 \mid a_0 \star a_1 \mid a_0 - a_1 \\
A & ::= & \texttt{true} \mid \texttt{false} \mid a_0 = a_1 \mid a_0 \leq a_1 \mid \\
 & & \neg A \mid A_0 \wedge A_1 \mid A_0 \vee A_1 \mid A_0 \Rightarrow A_1 \mid \forall i.A \mid \exists i.A
\end{array}
$$

Semantics of **Assn**

- Interpretation $I : \mathbf{Intvar} \to \mathbf{N}$
- Semantics of expressions:

$$\begin{array}{rcl} \mathcal{A}v[\![n]\!]I\sigma & = & n \\ \mathcal{A}v[\![X]\!]I\sigma & = & \sigma(X) \\ \mathcal{A}v[\![i]\!]I\sigma & = & I(i) \\ \mathcal{A}v[\![a_0 + a_1]\!]I\sigma & = & \mathcal{A}v[\![a_0]\!]I\sigma + \mathcal{A}v[\![a_1]\!]I\sigma \end{array}$$

- Semantics of assertions ($\sigma \models^I A$ means σ satisfies A in interpretation I):

$$\begin{array}{l} \sigma \models^I \mathbf{true} \\ \sigma \models^I a_0 = a_1 \text{ if } \mathcal{A}v[\![a_0]\!]I\sigma = \mathcal{A}v[\![a_1]\!]I\sigma \\ \sigma \models^I A \land B \text{ if } \sigma \models^I A \text{ and } \sigma \models^I B \\ \sigma \models^I A \Rightarrow B \text{ if } \sigma \not\models^I A \text{ or } \sigma \models^I B \\ \sigma \models^I \forall i.A \text{ if } \sigma \models^{I[n/i]} A \text{ for all } n \\ \sigma \models^I \exists i.A \text{ if } \sigma \models^{I[n/i]} A \text{ for some } n \\ \bot \models^I A \end{array}$$

- An assertion denotes a set of states:

$$A^I = \{\sigma \in \Sigma_\bot \mid \sigma \models^I A\}$$

Properties

- For all $\boldsymbol{a} \in \mathbf{Aexp}$, states $\boldsymbol{\sigma}$, and interpretations $\boldsymbol{I}$,

$$\mathcal{A}[\![a]\!]\sigma = \mathcal{A}v[\![a]\!]I\sigma$$

- For $\boldsymbol{b} \in \mathbf{Bexp}, \boldsymbol{\sigma} \in \boldsymbol{\Sigma}$,

$$\begin{array}{rcl} \mathcal{B}[\![b]\!]\sigma = \mathbf{true} & \iff & \sigma \models^I b \\ \mathcal{B}[\![b]\!]\sigma = \mathbf{false} & \iff & \sigma \not\models^I b \end{array}$$

  for any interpretation $\boldsymbol{I}$.

- For $\boldsymbol{a} \in \mathbf{Aexpv}$,

$$\mathcal{A}v[\![a]\!]I[n/i]\sigma = \mathcal{A}v[\![a[n/i]]\!]I\sigma$$

Partial Correctness Assertions

- A partial correctness assertion has the form

$$\{A\}c\{B\}$$

where $A, B \in \mathbf{Assn}$ and $c \in \mathbf{Com}$.

- Let I be an interpretation. Let $\sigma \in \Sigma_\perp$. We define the satisfaction relation between states and partial correctness assertions, with respect to I, by

$$\sigma \models^I \{A\}c\{B\} \text{ iff } \sigma \models^I A \Rightarrow \mathcal{C}[\![c]\!]\sigma \models^I B$$

- A partial correctness assertion $\{A\}c\{B\}$ is *valid*

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

if $\sigma \models^I \{A\}c\{B\}$ holds for all states $\sigma \in \Sigma_\perp$ and interpretations $I \in \mathbf{Intvar} \to \mathrm{N}$.

- An assertion A is *valid*

$$\models A$$

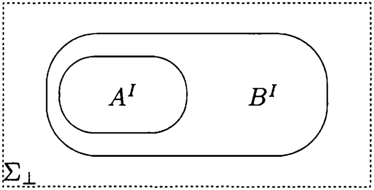
iff for all interpretations I and states σ, $\sigma \models^I A$.

Example

Suppose $\models (A \Rightarrow B)$. Then for any interpretation I,

$$\forall \sigma \in \Sigma. ((\sigma \models^I A) \Rightarrow (\sigma \models^I B))$$

i.e., $A^I \subseteq B^I$.



So $\models (A \Rightarrow B)$ iff for all interpretations I, all states which satisfy A also satisfy B.

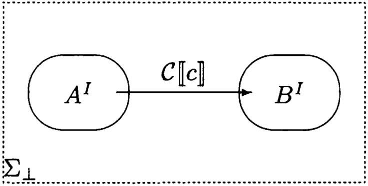
Over-Approximation of Program Semantics

Suppose $\models \{A\}c\{B\}$. Then for any interpretation I and state σ

$$\sigma \models^{I} A \Rightarrow \mathcal{C}[\![c]\!]\sigma \models^{I} B$$

i.e., the image of A under $\mathcal{C}[\![c]\!]$ is included in B:

$$\mathcal{C}[\![c]\!]A^{I} \subseteq B^{I}$$



- B: correctness specification ("no errors")
- A: a sufficient condition to ensure B after execution

Proof Rules (Hoare Logic)

We write $\vdash \{A\}c\{B\}$ when $\{A\}c\{B\}$ is derivable by the following rules.

- Rule for skip:

$$\{A\}\texttt{skip}\{A\}$$

- Rule for assignment:

$$\{B[a/X]\}X := a\{B\}$$

- Rule for sequencing:

$$\frac{\{A\}c_0\{C\} \quad \{C\}c_1\{B\}}{\{A\}c_0; c_1\{B\}}$$

- Rule for conditionals:

$$\frac{\{A \land b\}c_0\{B\} \quad \{A \land \neg b\}c_1\{B\}}{\{A\}\texttt{if } b \texttt{ then } c_0 \texttt{ else } c_1\{B\}}$$

- Rule for while loops:

$$\frac{\{A \land b\}c\{A\}}{\{A\}\texttt{while } b \texttt{ do } c\{A \land \neg b\}}$$

- Rule of consequence:

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

Examples

$$\{\textsf{true}\}X := n\{X = n\}$$

$$\frac{\{\textsf{true}\}X := n\{X = n\} \quad \{X = n\}Y := 1\{X = n \land Y = 1\}}{\{\textsf{true}\}X := n; Y := 1\{X = n \land Y = 1\}}$$

$$\frac{\models (X = 1) \Rightarrow \textsf{true} \quad \{\textsf{true}\}X := n\{x = n\} \quad \models (X = n) \Rightarrow (X \leq n)}{\{X = 1\}X := n\{X \leq n\}}$$

$$\frac{\dfrac{\models (X > 0) \Rightarrow \textsf{true} \quad \{\textsf{true}\}Y := 1\{Y > 0\}}{\{X > 0\}Y := 1\{Y > 0\}} \quad \dfrac{\models (X \leq 0) \Rightarrow \textsf{true} \quad \{\textsf{true}\}Y := 2\{Y > 0\}}{\{X \leq 0\}Y := 2\{Y > 0\}}}{\{\textsf{true}\}\texttt{if } (X > 0) \texttt{ then } Y := 1 \texttt{ else } Y := 2\{Y > 0\}}$$

Example: Factorial

$$\{n \geq 0 \wedge x = n \wedge y = 1\} \mathit{while}\ (x > 0)\ (y := x \times y; x := x - 1)\{y = n!\}$$

Let $w = \mathit{while}\ (x > 0)\ (y := x \times y; x := x - 1)$.

1. Take a loop invariant

$$p = (y \times x! = n! \wedge x \geq 0)$$

2. Show that p is indeed a loop invariant:

$$\frac{\{p \wedge x > 0\}y := x \times y\{q\} \quad \{q\}x := x - 1\{p\}}{\{p \wedge x > 0\}y := x \times y; x := x - 1\{p\}}$$

   where $q = (y \times (x - 1)! = n! \wedge x \geq 1)$.

3. By the Hoare rule,

$$\{p\}w\{p \wedge x \leq 0\}$$

4. Show that

$$(n \geq 0 \wedge x = n \wedge y = 1) \Rightarrow p \quad \text{and} \quad p \wedge x \leq 0 \Rightarrow y = n!$$

Example: Multiplication

$$\{x = 0 \land y = b\} while\ (y \neq 0)\ (x := x + a; y := y - 1)\{x = a \times b\}$$

Let w be the loop.

1. Take a loop invariant

$$p = (x = (b - y) \times a)$$

2. Show that p is indeed a loop invariant:

$$\frac{\{p \land y \neq 0\}x := x + 1\{q\} \quad \{q\}y := y - 1\{p\}}{\{p \land y \neq 0\}x := x + 1; y := y - 1\{p\}}$$

where $q = (x = (b - y + 1) \times a)$.

3. By the Hoare rule,

$$\{p\}w\{p \land y = 0\}$$

4. Show that

$$(x = 0 \land y = b) \Rightarrow p \quad \text{and} \quad p \land y = 0 \Rightarrow x = a \times b$$

Soundness and Completeness

- Soundness: Every partial correctness assertion obtained from the proof system of Hoare rules is valid.

$$\vdash \{A\}c\{B\} \implies \models \{A\}c\{B\}$$

- Completeness: All valid partial correctness assertions can be obtained from the proof system.

$$\models \{A\}c\{B\} \implies \vdash \{A\}c\{B\}$$

Soundness Proof

Lemma (1)

Let $a, a_0 \in \mathbf{Aexpv}$ *and* $X \in \mathbf{Loc}$. *Then for all* I *and* σ

$$\mathcal{A}v[\![a_0[a/X]]\!]I\sigma = \mathcal{A}v[\![a_0]\!]I\sigma[\mathcal{A}v[\![a]\!]I\sigma/X]$$

E.g., when $a_0 = X + 1, a = Y, \sigma(Y) = 2$

$$\mathcal{A}v[\![Y + 1]\!]I\sigma = 3 = \mathcal{A}v[\![X + 1]\!]I\sigma[2/X]$$

Lemma (2)

Let I *be an interpretation. Let* $B \in \mathbf{Assn}$, $X \in \mathbf{Loc}$, *and* $a \in \mathbf{Aexp}$. *Then for all* σ

$$\sigma \models^I B[a/X] \iff \sigma[\mathcal{A}[\![a]\!]\sigma/X] \models^I B$$

E.g., when $a = 1, B = X < 2$

$$\sigma \models^I 1 < 2 \iff \sigma[1/X] \models^I X < 2$$

We prove each rule is sound; each rule preserves validity.

- Skip: Clearly $\models \{A\}\texttt{skip}\{A\}$.
- Assignment: Let I be an interpretation.

$$\begin{aligned} \sigma \models^I B[a/X] &\Rightarrow \sigma[\mathcal{A}[\![a]\!]\sigma/X] \models^I B && \text{Lemma (2)} \\ &\Rightarrow \mathcal{C}[\![X := a]\!]\sigma \models^I B && \text{def. of } \mathcal{C}[\![-]\!] \end{aligned}$$

  Hence $\models \{B[a/X]\}X := a\{B\}$.

- Sequencing: Assume $\models \{A\}c_0\{C\}$ and $\models \{C\}c_1\{B\}$. Let I be an interpretation and σ a state.

$$\begin{aligned} \sigma \models^I A &\Rightarrow \mathcal{C}[\![c_0]\!]\sigma \models^I C && \models \{A\}c_0\{C\} \\ &\Rightarrow \mathcal{C}[\![c_1]\!](\mathcal{C}[\![c_0]\!]\sigma) \models^I B && \models \{C\}c_1\{B\} \\ &\Rightarrow \mathcal{C}[\![c_0; c_1]\!]\sigma \models^I B && \text{def. of } \mathcal{C}[\![-]\!] \end{aligned}$$

  Hence $\models \{A\}c_0; c_1\{B\}$.

- Conditionals: Assume $\models \{A \wedge b\} c_0 \{B\}$ and $\models \{A \wedge \neg b\} c_1 \{B\}$.
  - $\sigma \models^I b$:

$$\begin{aligned} \sigma \models^I A \wedge b \Rightarrow \mathcal{C}[\![c_0]\!]\sigma \models^I B & \quad \models \{A \wedge b\} c_0 \{B\} \\ \Rightarrow \mathcal{C}[\![\texttt{if}\ b\ c_0\ c_1]\!]\sigma \models^I B & \quad \text{def. of } \mathcal{C}[\![-]\!] \end{aligned}$$

    Hence $\models \{A \wedge b\}\texttt{if}\ b\ c_0\ c_1\{B\}$. Thus, $\models \{A\}\texttt{if}\ b\ c_0\ c_1\{B\}$.
  - $\sigma \models^I \neg b$:

$$\begin{aligned} \sigma \models^I A \wedge \neg b \Rightarrow \mathcal{C}[\![c_1]\!]\sigma \models^I B & \quad \models \{A \wedge \neg b\} c_1 \{B\} \\ \Rightarrow \mathcal{C}[\![\texttt{if}\ b\ c_0\ c_1]\!]\sigma \models^I B & \quad \text{def. of } \mathcal{C}[\![-]\!] \end{aligned}$$

    Hence $\models \{A \wedge \neg b\}\texttt{if}\ b\ c_0\ c_1\{B\}$. Thus, $\models \{A\}\texttt{if}\ b\ c_0\ c_1\{B\}$.
- Consequence: Assume $\models A \Rightarrow A'$, $\models \{A'\}c\{B'\}$, $\models B' \Rightarrow B$.

$$\begin{aligned} \sigma \models^I A \Rightarrow \sigma \models^I A' & \quad \models A \Rightarrow A' \\ \Rightarrow \mathcal{C}[\![c]\!]\sigma \models^I B' & \quad \models \{A'\}c\{B'\} \\ \Rightarrow \mathcal{C}[\![c]\!]\sigma \models^I B & \quad \models B' \Rightarrow B \end{aligned}$$

  Hence $\models \{A\}c\{B\}$.

- Loops: Assume $\models \{A \wedge b\}c\{A\}$, i.e., A is an invariant of

$$w \equiv \texttt{while}\ b\ \texttt{do}\ c$$

Recall that $\mathcal{C}[\![w]\!] = \bigcup_{n \in \omega} \theta_n$ where

$$\begin{array}{rcl} \theta_0 & = & \emptyset \\ \theta_{n+1} & = & \{(\sigma, \sigma') \mid \mathcal{B}[\![b]\!]\sigma = \mathbf{true}\ \&\ (\sigma, \sigma') \in \theta_n \circ \mathcal{C}[\![c]\!]\} \\ & \cup & \{(\sigma, \sigma) \mid \mathcal{B}[\![b]\!]\sigma = \mathbf{false}\} \end{array}$$

We show by mathematical induction that $P(n)$ holds for all $n \in \omega$:

$$P(n) \iff \forall \sigma, \sigma'.(\sigma, \sigma') \in \theta_n\ \&\ \sigma \models^I A \Rightarrow \sigma' \models^I A \wedge \neg b$$

It then follows that

$$\sigma \models^I A \Rightarrow \mathcal{C}[\![w]\!]\sigma \models^I A \wedge \neg b$$

for all states σ, and hence we have $\models \{A\}w\{A \wedge \neg b\}$.

Weakest Precondition

- Let $c \in \mathbf{Com}$ and $B \in \mathbf{Assn}$. The weakest (liberal) precondition $wp^I(c, B)$ of B w.r.t. c in I:

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

- If $\models^I \{A\}c\{B\}$ then $A^I \subseteq wp^I(c, B)$.
- Suppose there is an assertion A_0 such that in all interpretations I,

$$A_0^I = wp^I(c, B)$$

  Then

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

  for any interpretation I, i.e.,

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

Weakest Precondition

- We say $\mathbf{Assn}$ is expressive iff for every command c and assertion B there is an assertion A_0 such that $A_0^I = wp^I(c, B)$ for any interpretation I.
- $\mathbf{Assn}$ is expressive. For all assertions B there is an assertion $w(c, B)$ such that for all interpretations I

$$wp^I(c, B) = w(c, B)^I$$

  for all command. (Proof defines wp in terms of $\mathbf{Assn}$).
- Note that

$$\sigma \models^I w(c, B) \iff \mathcal{C}[\![c]\!]\sigma \models^I B$$