Axiomatic Semantics

Renato Neves

Universidade do Minho

HASLab
HIGH-ASSURANCE SOFTWARE LABORATORY

Semantics for Every Season

Operational semantics	How a program operates
Denotational semantics	What a program is
Axiomatic semantics	Which logical properties it satisfies

Table of Contents

A Brief Warm-up

Solve the following exercises via your favorite semantics

- Calculate the output of $\mathtt{x} := 1 \,;\, \mathtt{x} := 2$

- Show that the following program outputs a state with $\mathtt{x} \geq 2$

$$\texttt{if } \mathtt{x} = 1 \texttt{ then } \mathtt{x} := 2 \texttt{ else } \mathtt{x} := 3$$

- Show that the following program is the factorial function

$$\texttt{while}\, \mathtt{x} > 0 \,\{\mathtt{y} := \mathtt{x} \times \mathtt{y} \,;\, \mathtt{x} := \mathtt{x} - 1\}$$

A Brief Warm-up

Solve the following exercises via your favorite semantics

- Calculate the output of $\mathrm{x} := 1 \,;\, \mathrm{x} := 2$

- Show that the following program outputs a state with $\mathrm{x} \geq 2$

$$\texttt{if } \mathrm{x} = 1 \texttt{ then } \mathrm{x} := 2 \texttt{ else } \mathrm{x} := 3$$

- Show that the following program is the factorial function

$$\texttt{while}\, \mathrm{x} > 0 \,\{\mathrm{y} := \mathrm{x} \times \mathrm{y} \,;\, \mathrm{x} := \mathrm{x} - 1\}$$

Hard ?

The Right Tools

Two last exercises were about post-conditions . . .

not exactly about determining output . . .

nor about program equivalence

The Right Tools

Two last exercises were about post-conditions ...

not exactly about determining output ...

nor about program equivalence

$\boxed{\text{Do we have the right semantics for solving them ?}}$

Table of Contents

Key Points

Focussed on output properties and less on outputs themselves

Centred around a logic (for reasoning about these properties)

Semantic rules are thus more logic oriented

Key Points

Focussed on output properties and less on outputs themselves

Centred around a logic (for reasoning about these properties)

Semantic rules are thus more logic oriented

Good for program correctness (recall ‘algorithms and complexity’)

Hoare Triples

Axiomatic semantics essentially about (dis)proving

$$\{\Phi\}\,\mathtt{p}\,\{\Psi\}$$

"If Φ holds at the input then Ψ holds at the output"

Examples

- $\{\mathtt{tt}\}\,\mathtt{p}\,\{\mathtt{x} \geq 2\}$
- $\{\mathtt{x} = \mathtt{n} \wedge \mathtt{y} = 1\}\,\mathtt{p}\,\{\mathtt{y} = \mathtt{n}!\}$
- ...

Meaning of Hoare Triples

Can we state mathematically what a Hoare triple really means ?

Meaning of Hoare Triples

Can we state mathematically what a Hoare triple really means ?

Question rooted on what a program means (recall our lectures)

... and of course on the choice of a logic for properties

Meaning of Hoare Triples

Can we state mathematically what a Hoare triple really means ?

Question rooted on what a program means (recall our lectures)

... and of course on the choice of a logic for properties

Right choice often not obvious ...

The Choice

Often varies depending on the problem at hand

... but typically the case that Φ corresponds to a subset

$$[\![\Phi]\!] \subseteq \mathrm{State}_\perp$$

('the elements of $\mathrm{State}_\perp$ at which Φ holds')

The Choice

Often varies depending on the problem at hand

... but typically the case that Φ corresponds to a subset

$$[\![\Phi]\!] \subseteq \mathrm{State}_\perp$$

('the elements of $\mathrm{State}_\perp$ at which Φ holds')

Scientists typically fix on the well-established first-order-logic

... which however brings its own set of problems

Meaning of Hoare Triples

$$\{\Phi\}\,\mathtt{p}\,\{\Psi\} \qquad \text{means} \qquad \Big(x \in [\![\Phi]\!] \implies [\![\mathtt{p}]\!](x) \in [\![\Psi]\!] \Big)$$

Meaning of Hoare Triples

$$\{\Phi\}\,\mathrm{p}\,\{\Psi\} \qquad \text{means} \qquad \Big(x \in [\![\Phi]\!] \Longrightarrow [\![\mathrm{p}]\!](x) \in [\![\Psi]\!] \Big)$$

Remarkably note the following equivalence

$$\Big(x \in [\![\Phi]\!] \Longrightarrow [\![\mathrm{p}]\!](x) \in [\![\Psi]\!] \Big) \quad \text{iff} \quad [\![\Phi]\!] \subseteq [\![\mathrm{p}]\!]^{-1}([\![\psi]\!])$$

It is at the root of a rich theory of

‘backward transformations’ known as predicate transformers

Liberals vs. Conservatives

In the sequel we will consider only liberal conditions

... *i.e.* every predicate Φ will have $\bot \in [\![\Phi]\!]$

Entails that we are working only with partial correctness

... *i.e.* no predicate enforces termination

Exercises

Argue informally whether the triples below hold

- $\{\mathtt{tt}\}$ $\mathtt{while}$ $\mathtt{tt}$ $\mathtt{skip}$ $\{\mathtt{ff}\}$
- $\{\mathtt{tt}\}$ $\mathtt{if}\ \mathrm{b}\ \mathtt{then}\ \mathtt{x} := 2\ \mathtt{else}\ \mathtt{x} := 3$ $\{\mathtt{x} \geq 2\}$
- $\{\mathtt{x} = \mathtt{a} \wedge \mathtt{y} = \mathtt{b}\}$ $\mathtt{x} := \mathtt{y} \,;\, \mathtt{y} := \mathtt{x}$ $\{\mathtt{x} = \mathtt{b} \wedge \mathtt{y} = \mathtt{a}\}$
- $\{\mathtt{x} = \mathtt{a} \wedge \mathtt{y} = \mathtt{b}\}$ $\mathtt{x} := \mathtt{aux} \,;\, \mathtt{x} := \mathtt{y} \,;\, \mathtt{y} := \mathtt{aux}$ $\{\mathtt{x} = \mathtt{b} \wedge \mathtt{y} = \mathtt{a}\}$
- $\{\mathtt{x} = \mathtt{n} \wedge \mathtt{y} = 1\}$ $\mathtt{fact}$ $\{\mathtt{y} = \mathtt{n}!\}$

Table of Contents

What and Why

Focus is on deriving the weakest condition Φ such that

$$\{\Phi\}\, \mathrm{p}\, \{\Psi\} \qquad \Big(\text{iff } [\![\Phi]\!] \subseteq [\![\mathrm{p}]\!]^{-1}([\![\Psi]\!])\Big)$$

What and Why

Focus is on deriving the weakest condition Φ such that

$$\{\Phi\}\,\mathtt{p}\,\{\Psi\} \qquad \Big(\text{iff } [\![\Phi]\!] \subseteq [\![\mathtt{p}]\!]^{-1}([\![\Psi]\!])\Big)$$

Φ 'weaker' (*i.e.* less restrictive) than Φ' means $[\![\Phi]\!] \supseteq [\![\Phi']\!]$

What and Why

Focus is on deriving the weakest condition Φ such that

$$\{\Phi\}\, p\, \{\Psi\} \qquad \Big(\text{iff } [\![\Phi]\!] \subseteq [\![p]\!]^{-1}([\![\Psi]\!])\Big)$$

Φ 'weaker' (*i.e.* less restrictive) than Φ' means $[\![\Phi]\!] \supseteq [\![\Phi']\!]$

To understand a program amounts to knowing the weakest precondition that ensures a given postcondition

The Semantics

$$
\begin{aligned}
\mathrm{wp}\,(\mathtt{x} := \mathtt{e}, \Phi) &= \Phi[\mathtt{e}/\mathtt{x}] \\
\mathrm{wp}\,(\mathtt{p}\,;\,\mathtt{q}, \Phi) &= \mathrm{wp}\,(\mathtt{q}, \mathrm{wp}\,(\mathtt{p}, \Phi)) \\
\mathrm{wp}\,(\mathtt{if}\;\mathtt{b}\;\mathtt{then}\;\mathtt{p}\;\mathtt{else}\;\mathtt{q}, \Phi) &= \mathtt{b} \wedge \mathrm{wp}\,(\mathtt{p}, \Phi) \;\vee\; \neg\mathtt{b} \wedge \mathrm{wp}\,(\mathtt{q}, \Phi) \\
\mathrm{wp}\,(\mathtt{while}\;\mathtt{b}\;\mathtt{do}\;\{\,\mathtt{p}\,\}, \Phi) &= \;\ldots
\end{aligned}
$$

Exercises

Calculate the weakest preconditions w.r.t. the following pairs

- $(\mathtt{x} := \mathtt{y},\ \mathtt{x} \geq 1)$
- $(\mathtt{if}\ \mathtt{b}\ \mathtt{then}\ \mathtt{x} := 2\ \mathtt{else}\ \mathtt{x} := 3,\ \mathtt{x} \geq 2)$
- $(\mathtt{x} := \mathtt{y}\ ;\ \mathtt{y} := \mathtt{x},\ \mathtt{x} = \mathtt{b} \wedge \mathtt{y} = \mathtt{a})$
- $(\mathtt{x} := \mathtt{aux}\ ;\ \mathtt{x} := \mathtt{y}\ ;\ \mathtt{y} := \mathtt{aux},\ \mathtt{x} = \mathtt{b} \wedge \mathtt{y} = \mathtt{a})$

The Semantics

$$\begin{aligned}
\mathrm{wp}\left(\mathtt{x} := \mathtt{e}, \Phi\right) &= \Phi[\mathtt{e}/\mathtt{x}] \\
\mathrm{wp}\left(\mathtt{p} \,;\, \mathtt{q}, \Phi\right) &= \mathrm{wp}\left(\mathtt{q}, \mathrm{wp}\left(\mathtt{p}, \Phi\right)\right) \\
\mathrm{wp}\left(\mathtt{if}\ \mathtt{b}\ \mathtt{then}\ \mathtt{p}\ \mathtt{else}\ \mathtt{q}, \Phi\right) &= \mathtt{b} \wedge \mathrm{wp}\left(\mathtt{p}, \Phi\right) \vee \neg\mathtt{b} \wedge \mathrm{wp}\left(\mathtt{q}, \Phi\right) \\
\mathrm{wp}\left(\mathtt{while}\ \mathtt{b}\ \mathtt{do}\ \{\, \mathtt{p}\, \}, \Phi\right) &= \bigwedge_{n \in \mathbb{N}} \Psi_n
\end{aligned}$$

The Semantics

$$\mathrm{wp}\left(\mathtt{x} := \mathtt{e}, \Phi\right) = \Phi[\mathtt{e}/\mathtt{x}]$$

$$\mathrm{wp}\left(\mathtt{p} \,;\, \mathtt{q}, \Phi\right) = \mathrm{wp}\left(\mathtt{q}, \mathrm{wp}\left(\mathtt{p}, \Phi\right)\right)$$

$$\mathrm{wp}\left(\mathtt{if}\ \mathtt{b}\ \mathtt{then}\ \mathtt{p}\ \mathtt{else}\ \mathtt{q}, \Phi\right) = \mathtt{b} \wedge \mathrm{wp}\left(\mathtt{p}, \Phi\right) \vee \neg\mathtt{b} \wedge \mathrm{wp}\left(\mathtt{q}, \Phi\right)$$

$$\mathrm{wp}\left(\mathtt{while}\ \mathtt{b}\ \mathtt{do}\ \{\ \mathtt{p}\ \}, \Phi\right) = \bigwedge_{n \in \mathbb{N}} \Psi_n$$

$$\Psi_0 = \mathtt{tt}$$

$$\Psi_{n+1} = \neg\mathtt{b} \wedge \Phi \vee \mathtt{b} \wedge \mathrm{wp}\left(\mathtt{p}, \Psi_n\right)$$

Table of Contents