Axiomatic Semantics

Renato Neves

Universidade do Minho

HASLab
HIGH-ASSURANCE SOFTWARE LABORATORY

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 $\mathtt{x} := 1 \,;\, \mathtt{x} := 2$
- 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

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

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

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

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

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

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

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 $\perp \in [\![\Phi]\!]$

Entails that we are working only with partial correctness

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

Exercises

Argue informally whether the triples below hold

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

Table of Contents

What and Why

Focus is on deriving the weakest condition Φ such that

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

What and Why

Focus is on deriving the weakest condition Φ such that

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

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

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

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

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

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

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

$$\mathrm{wp}\,(\mathtt{while}\ \mathtt{b}\ \mathtt{do}\ \{\ \mathtt{p}\ \}, \Phi) = \ \ldots$$

Exercises

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

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

The Semantics

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

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

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

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

The Semantics

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

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

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

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

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

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

Unfolding While-loops

$$\mathrm{wp}\left(\texttt{while}\ \mathrm{b}\ \texttt{do}\ \{\ \mathrm{p}\ \}, \Phi\right)$$

$$= \Psi_0 \qquad \text{(trivial)}^{*}$$

$$\wedge\ \neg \mathsf{b} \wedge \Phi\ \vee\ \mathsf{b} \wedge \mathrm{wp}\left(\mathrm{p}, \Psi_0\right) \qquad \text{(\underline{terminates} with } \Phi \text{ \underline{or iterates once} and then \underline{*})}^{**}$$

$$\wedge\ \neg \mathsf{b} \wedge \Phi\ \vee\ \mathsf{b} \wedge \mathrm{wp}\left(\mathrm{p}, \Psi_1\right) \qquad \text{(\underline{terminates} with } \Phi \text{ \underline{or iterates once} and then \underline{**})}$$

$$\wedge\ \ldots$$

Unfolding While-loops

$$
\begin{aligned}
&\mathrm{wp}\big(\texttt{while}\,\mathrm{b}\,\texttt{do}\,\{\,\mathrm{p}\,\},\Phi\big)\\
&= \Psi_0 && \text{(trivial)}^{*}\\
&\ \wedge \neg \mathtt{b} \wedge \Phi \ \vee\ \mathtt{b} \wedge \mathrm{wp}\big(\mathrm{p},\Psi_0\big) && \text{(terminates with } \Phi \text{ or iterates once and then } \underline{*}\text{)}^{**}\\
&\ \wedge \neg \mathtt{b} \wedge \Phi \ \vee\ \mathtt{b} \wedge \mathrm{wp}\big(\mathrm{p},\Psi_1\big) && \text{(terminates with } \Phi \text{ or iterates once and then } \underline{**}\text{)}\\
&\ \wedge \ \ldots
\end{aligned}
$$

Infinitary formula tracks when the loop terminates

... in which case it enforces Φ

Each conjunct Ψ_{n+1} tracks up to n iterations

Unfolding While-loops (The Case of Divergence)

$$
\begin{aligned}
&\mathrm{wp}\,(\texttt{while}\,\texttt{tt}\,\texttt{do}\,\{\,\mathrm{p}\,\}, \Phi) \\
&= \Psi_0 \qquad (= \texttt{tt}) \\
&\;\wedge \neg\texttt{tt} \wedge \Phi \;\vee\; \texttt{tt} \wedge \mathrm{wp}\,(\mathrm{p}, \texttt{tt}) \qquad (= \texttt{tt}) \\
&\;\wedge \neg\texttt{tt} \wedge \Phi \;\vee\; \texttt{tt} \wedge \mathrm{wp}\,(\mathrm{p}, \texttt{tt}) \qquad (= \texttt{tt}) \\
&\;\wedge \;\ldots \\
&\;= \texttt{tt}
\end{aligned}
$$

Exercises

Prove that the following equations hold

- $\mathrm{wp}\,(\mathtt{p}, \mathtt{tt}) = \mathtt{tt}$
- $\mathrm{wp}\,(\mathtt{p}, \Phi \wedge \Psi) = \mathrm{wp}\,(\mathtt{p}, \Phi) \wedge \mathrm{wp}\,(\mathtt{p}, \Psi)$
- $\mathrm{wp}\,(\mathtt{p}, \bigwedge_{i \in I} \Phi_i) = \bigwedge_{i \in I} \mathrm{wp}\,(\mathtt{p}, \Phi_i)$

Pre-condition and Denotational Semantics

Theorem

$[\![\mathrm{wp}\,(\mathrm{p}, \Phi)]\!] = [\![\mathrm{p}]\!]^{-1}([\![\Phi]\!])$

Proof.

By induction. Case of while-loops proved neatly via domain theory $\square$

Corollary

$[\![\mathrm{p}]\!] = [\![\mathrm{q}]\!] \implies \forall \Phi.\, \mathrm{wp}\,(\mathrm{p}, \Phi) \equiv \mathrm{wp}\,(\mathrm{q}, \Phi)$

Expressivity Matters

Is it true that $\Big(\forall \Phi.\, \mathrm{wp}(\mathsf{p}, \Phi) \equiv \mathrm{wp}\,(\mathsf{q}, \Phi)\Big) \implies [\![\mathsf{p}]\!] = [\![\mathsf{q}]\!]$?

Expressivity Matters

Is it true that $\Big(\forall \Phi.\, \mathrm{wp}(\mathrm{p}, \Phi) \equiv \mathrm{wp}\,(\mathrm{q}, \Phi)\Big) \implies [\![\mathrm{p}]\!] = [\![\mathrm{q}]\!]$?

Well . . .

$$
\begin{aligned}
&\forall \Phi.\, \mathrm{wp}\,(\mathrm{p}, \Phi) \equiv \mathrm{wp}\,(\mathrm{q}, \Phi) \\
&\implies \forall \Phi.\, [\![\mathrm{wp}\,(\mathrm{p}, \Phi)]\!] = [\![\mathrm{wp}\,(\mathrm{q}, \Phi)]\!] \\
&\implies \forall \Phi.\, [\![\mathrm{p}]\!]^{-1}([\![\Phi]\!]) = [\![\mathrm{q}]\!]^{-1}([\![\Phi]\!]) \\
&\implies [\![\mathrm{p}]\!] = [\![\mathrm{q}]\!]
\end{aligned}
$$

Expressivity Matters

Is it true that $\Big(\forall \Phi.\, \mathrm{wp}(\mathrm{p}, \Phi) \equiv \mathrm{wp}\,(\mathrm{q}, \Phi)\Big) \implies [\![\mathrm{p}]\!] = [\![\mathrm{q}]\!]$?

Well ...

$$\begin{aligned}
&\forall \Phi.\, \mathrm{wp}\,(\mathrm{p}, \Phi) \equiv \mathrm{wp}\,(\mathrm{q}, \Phi) \\
&\implies \forall \Phi.\, [\![\mathrm{wp}\,(\mathrm{p}, \Phi)]\!] = [\![\mathrm{wp}\,(\mathrm{q}, \Phi)]\!] \\
&\implies \forall \Phi.\, [\![\mathrm{p}]\!]^{-1}([\![\Phi]\!]) = [\![\mathrm{q}]\!]^{-1}([\![\Phi]\!]) \\
&\implies [\![\mathrm{p}]\!] = [\![\mathrm{q}]\!]
\end{aligned}$$

A counter-example (the simplest grammar of propositions)

$$\mathtt{b} ::= \mathtt{tt} \mid \neg \mathtt{b} \mid \mathtt{b} \vee \mathtt{b} \mid \bigwedge \mathtt{b}$$

Calculate all possible interpretations $[\![\mathtt{b}]\!]$

From Weakest Pre-conditions to Hoare Triples

We wish to prove the validity of Hoare triples

... like in 'algorithms and complexity'

For this we use a simple calculus from the semantics

... with merely one rule

$$\frac{\vdash \Phi \to \mathrm{wp}\,(\mathrm{p}, \Psi)}{\vdash \{\Phi\}\, \mathrm{p}\, \{\Psi\}}$$

Soundness

Is our calculus correct ?

... *i.e.* $\vdash \{\Phi\}\,\mathtt{p}\,\{\Psi\} \implies [\![\Phi]\!] \subseteq [\![\mathtt{p}]\!]^{-1}([\![\Psi]\!])$

Soundness

Is our calculus correct ?

$\ldots$ *i.e.* $\vdash \{\Phi\}\,\mathtt{p}\,\{\Psi\} \Longrightarrow [\![\Phi]\!] \subseteq [\![\mathtt{p}]\!]^{-1}([\![\Psi]\!])$

Yes, and the proof is easy !!

Completeness

Is our calculus complete ?

. . . *i.e.* $[\![\Phi]\!] \subseteq [\![\mathtt{p}]\!]^{-1}([\![\Psi]\!]) \Longrightarrow \vdash \{\Phi\}\,\mathtt{p}\,\{\Psi\}$

Completeness

Is our calculus complete ?

... *i.e.* $[\![\Phi]\!] \subseteq [\![\mathtt{p}]\!]^{-1}([\![\Psi]\!]) \Longrightarrow \vdash \{\Phi\}\,\mathtt{p}\,\{\Psi\}$

It depends on whether the logic is complete

... *i.e.* $[\![\Phi_1]\!] \subseteq [\![\Phi_2]\!] \Longrightarrow \vdash \Phi_1 \to \Phi_2$ for all formulae Φ_1, Φ_2

Table of Contents