COMP2111 Week 9
Term 1, 2024
Hoare Logic

Summary

- $\mathcal{L}$: A simple imperative programming language
- Hoare triples (SYNTAX)
- Hoare logic (PROOF)
- Semantics for Hoare logic
- Handling termination
- Adding non-determinism

Aims

We've seen how to use Hoare logic to verify programs.

But how do we know that Hoare logic *works*? Do we need to take the rules on faith? Or can we prove that it works?

Aims

We've seen how to use Hoare logic to verify programs.

But how do we know that Hoare logic *works*? Do we need to take the rules on faith? Or can we prove that it works?

We've already asked (and answered) a similar question about a different logic (natural deduction).

Informal semantics

Hoare logic gives a proof of $\{\varphi\}\,P\,\{\psi\}$, that is: $\vdash \{\varphi\}\,P\,\{\psi\}$ (axiomatic semantics)

What does it mean for $\{\varphi\}\,P\,\{\psi\}$ to be **valid**, that is: $\models \{\varphi\}\,P\,\{\psi\}$?

Informal semantics

Hoare logic gives a proof of $\{\varphi\}\, P\, \{\psi\}$, that is: $\vdash \{\varphi\}\, P\, \{\psi\}$ (axiomatic semantics)

What does it mean for $\{\varphi\}\, P\, \{\psi\}$ to be **valid**, that is: $\models \{\varphi\}\, P\, \{\psi\}$?

We need a *semantics* for $\mathcal{L}$.

Informal semantics

Hoare logic gives a proof of $\{\varphi\}\, P\, \{\psi\}$, that is: $\vdash \{\varphi\}\, P\, \{\psi\}$ (axiomatic semantics)

What does it mean for $\{\varphi\}\, P\, \{\psi\}$ to be **valid**, that is: $\models \{\varphi\}\, P\, \{\psi\}$?

We need a *semantics* for $\mathcal{L}$.

We *could* use the LTS semantics of $\mathcal{L}$ from Week 8. We will use a *denotational* style instead, similar to Assignment 1 Problem 1 but systematic.

Informal semantics: Programs

We know (from Assignment 1 Problem 1) that programs can be modelled as *relations* between initial and final states.

Informal semantics: States

What is a state?

Informal semantics: States

What is a state?

Two approaches:

- Concrete: from a physical perspective
- Abstract: from a mathematical perspective

Informal semantics: States

What is a state?

Two approaches:

- Concrete: from a physical perspective
  - States are memory configurations, register contents, etc.
  - Store of variables and the values associated with them
- Abstract: from a mathematical perspective

Informal semantics: States

What is a state?

Two approaches:

- Concrete: from a physical perspective
  - States are memory configurations, register contents, etc.
  - Store of variables and the values associated with them
- Abstract: from a mathematical perspective
  - The pre-/postcondition predicates *hold* in a state

  $\Rightarrow$ States are **logical interpretations** (Model + Environment)

Informal semantics: States

What is a state?

Two approaches:

- Concrete: from a physical perspective
  - States are memory configurations, register contents, etc.
  - Store of variables and the values associated with them
- Abstract: from a mathematical perspective
  - The pre-/postcondition predicates *hold* in a state

  $\Rightarrow$ States are **logical interpretations** (Model + Environment)
  - There is only one model of interest: standard interpretations of arithmetical symbols

Informal semantics: States

What is a state?

Two approaches:

- Concrete: from a physical perspective
  - States are memory configurations, register contents, etc.
  - Store of variables and the values associated with them
- Abstract: from a mathematical perspective
  - The pre-/postcondition predicates *hold* in a state

  $\Rightarrow$ States are **logical interpretations** (Model + Environment)
  - There is only one model of interest: standard interpretations of arithmetical symbols

  $\Rightarrow$ States are fully determined by **environments**

  $\Rightarrow$ States are functions that map variables to values

Informal semantics: States

State space ($\textsc{Env}$)

$x \leftarrow 0$
$y \leftarrow 0$
$z \leftarrow 0$

$x \leftarrow 3$
$y \leftarrow 2$
$z \leftarrow 1$

$x \leftarrow 1$
$y \leftarrow 1$
$z \leftarrow 1$

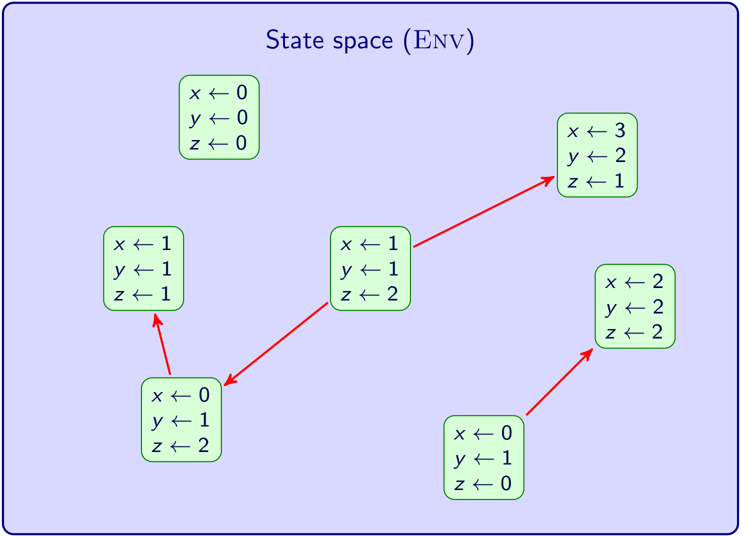
$x \leftarrow 1$
$y \leftarrow 1$
$z \leftarrow 2$

$x \leftarrow 2$
$y \leftarrow 2$
$z \leftarrow 2$

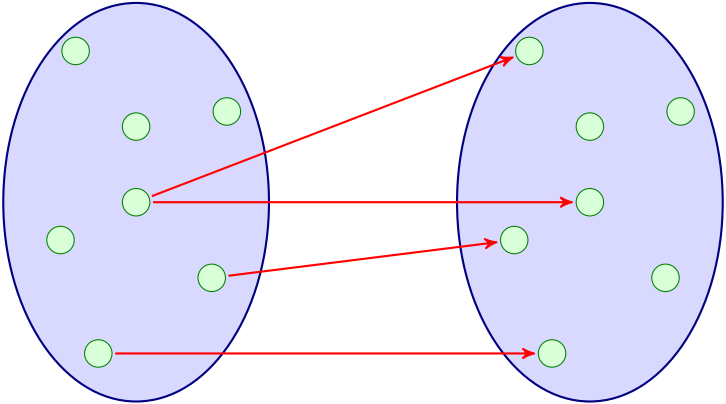
$x \leftarrow 0$
$y \leftarrow 1$
$z \leftarrow 2$

$x \leftarrow 0$
$y \leftarrow 1$
$z \leftarrow 0$

Informal semantics: States and Programs



Informal semantics: States and Programs



Semantics for $\mathcal{L}$

An **environment** or **state** is a function from variables to (numeric) values. We denote by $\textsc{Env}$ the set of all environments.

NB

An environment, η, assigns a numeric value $[\![e]\!]^\eta$ to all expressions e, and a boolean value $[\![b]\!]^\eta$ to all boolean expressions b.

Semantics for $\mathcal{L}$

An **environment** or **state** is a function from variables to (numeric) values. We denote by $\textsc{Env}$ the set of all environments.

NB

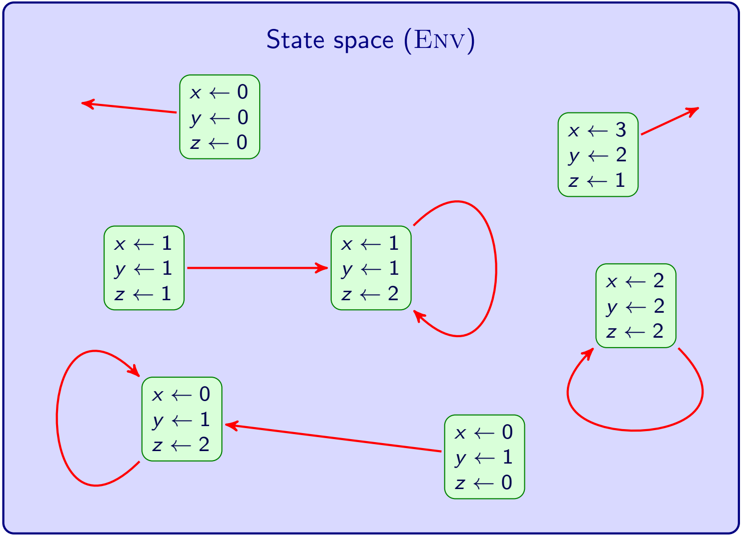
An environment, η, assigns a numeric value $[\![e]\!]^\eta$ to all expressions e, and a boolean value $[\![b]\!]^\eta$ to all boolean expressions b.

Given a program P of $\mathcal{L}$, we define $[\![P]\!]$ to be a **binary relation** on $\textsc{Env}$ in the following manner...

Assignment

$$(\eta, \eta') \in [\![x := e]\!] \quad \text{if, and only if} \quad \eta' = \eta[x \mapsto [\![e]\!]^\eta]$$

Assignment: $[\![z := 2]\!]$



Recall

If R and S are binary relations, then the **relational composition** of R and S, $R;S$ is the relation:

$$R;S := \{(a,c) \ : \ \exists b \text{ such that } (a,b) \in R \text{ and } (b,c) \in S\}$$

If $R \subseteq A \times B$ is a relation, and $X \subseteq A$, then the **image of X under** R, $R(X)$ is the subset of B defined as:

$$R(X) := \{b \in B \ : \ \exists a \ \in X \text{ such that } (a,b) \in R\}.$$

Sequencing

$$[\![P; Q]\!] = [\![P]\!] ; [\![Q]\!]$$

where, on the RHS, ; is relational composition.

Conditional, first attempt

$$[\![\text{if } b \text{ then } P \text{ else } Q \text{ fi}]\!] = \begin{cases} [\![P]\!] & \text{if } [\![b]\!]^{\eta} = \texttt{true} \\ [\![Q]\!] & \text{otherwise.} \end{cases}$$

Conditional, first attempt

$$[\![\text{if } b \text{ then } P \text{ else } Q \text{ fi}]\!] = \begin{cases} [\![P]\!] & \text{if } [\![b]\!]^\eta = \mathtt{true} \\ [\![Q]\!] & \text{otherwise.} \end{cases}$$

We'd like to avoid mentioning η on the LHS, so this won't do.

Detour: Predicates as programs

A boolean expression b defines a subset (or unary relation) of $\textsc{Env}$:

$$\langle b \rangle = \{\eta \; : \; [\![b]\!]^{\eta} = \texttt{true}\}$$

This can be extended to a binary relation (i.e. a program):

$$[\![b]\!] = \{(\eta, \eta) \; : \; \eta \in \langle b \rangle\}$$

Detour: Predicates as programs

A boolean expression b defines a subset (or unary relation) of $\textsc{Env}$:

$$\langle b \rangle = \{\eta \ : \ [\![b]\!]^{\eta} = \texttt{true}\}$$

This can be extended to a binary relation (i.e. a program):

$$[\![b]\!] = \{(\eta, \eta) \ : \ \eta \in \langle b \rangle\}$$

Intuitively, b corresponds to the program

if b then skip else abort fi

Conditional, better attempt

$$[\![\text{if } b \text{ then } P \text{ else } Q \text{ fi}]\!] = [\![b; P]\!] \cup [\![\neg b; Q]\!]$$

While

while b do P od

- Do 0 or more executions of P while b holds
- Terminate when b does not hold

While

while b do P od

- Do 0 or more executions of $(b; P)$
- Terminate with an execution of $\neg b$

While

$$\text{while } b \text{ do } P \text{ od}$$

- Do 0 or more executions of $(b; P)$
- Terminate with an execution of $\neg b$

How to do "0 or more" executions of $(b; P)$?

Reflexive and transitive closure

Given a binary relation $R \subseteq E \times E$, the *transitive closure of* R, R^* is defined inductively by the following rules:

$$\frac{x \in E}{x \; R^* \; x} \qquad\qquad \frac{x \; R \; y \qquad y \; R^* \; z}{x \; R^* \; z}$$

NB

- $R; R^* \subseteq R^*$.

While

$$[\![\text{while } b \text{ do } P \text{ od}]\!] = [\![b; P]\!]^*; [\![\neg b]\!]$$

- Do 0 or more executions of $(b; P)$
- Conclude with an execution of $\neg b$

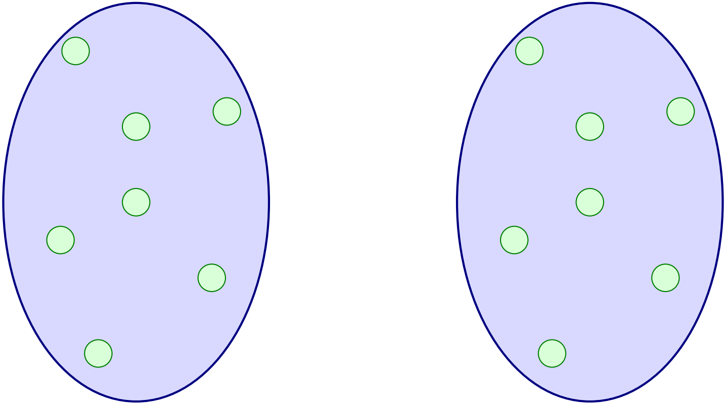
Validity

A Hoare triple is **valid**, written $\models \{\varphi\}\, P\, \{\psi\}$ if

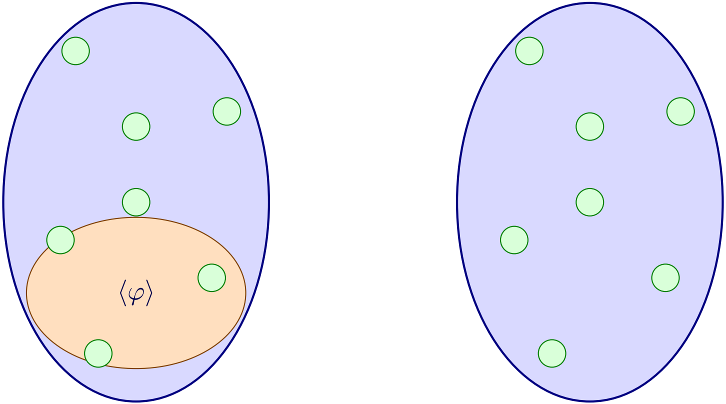
$$[\![P]\!](\langle\varphi\rangle) \subseteq \langle\psi\rangle.$$

That is, the relational image under $[\![P]\!]$ of the set of states where φ holds is contained in the set of states where ψ holds.

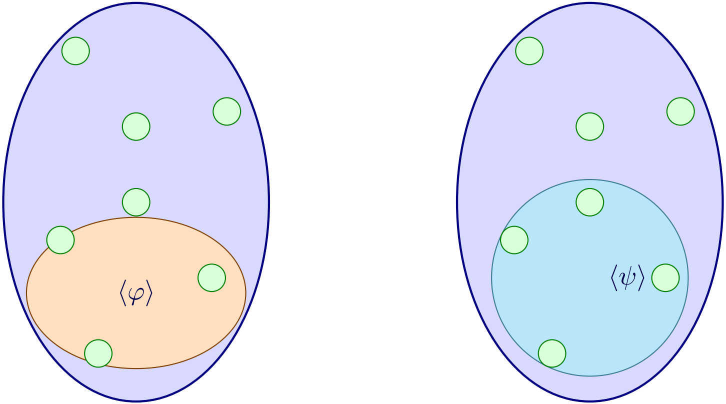
Validity



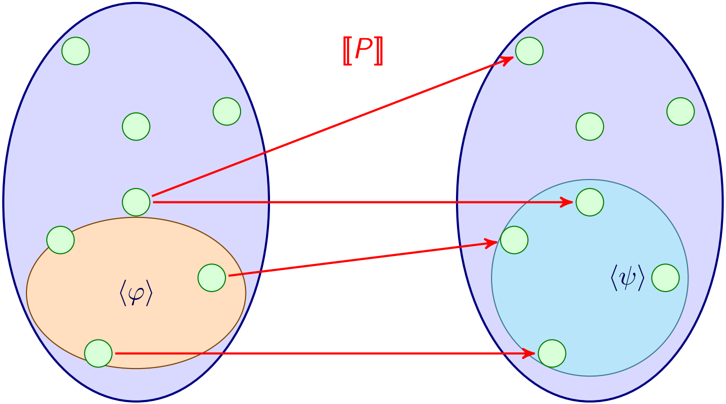
Validity



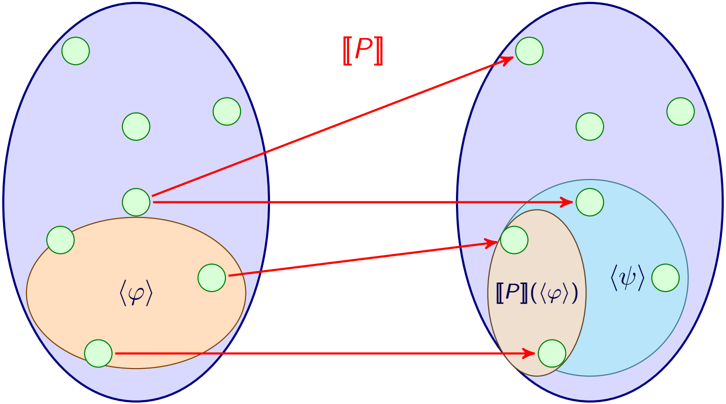
Validity



Validity



Validity



$[\![P]\!]$
$\langle\varphi\rangle$
$[\![P]\!](\langle\varphi\rangle)$
$\langle\psi\rangle$

Soundness of Hoare Logic

Theorem

If $\vdash \{\varphi\}\, P\, \{\psi\}$ *then* $\models \{\varphi\}\, P\, \{\psi\}$

Incompleteness

Theorem (Gödel's Incompleteness Theorem)

There is no proof system that can prove every valid first-order sentence about arithmetic over the natural numbers.

Incompleteness

Theorem (Gödel's Incompleteness Theorem)

There is no proof system that can prove every valid first-order sentence about arithmetic over the natural numbers.

$\Rightarrow$ There are true statements that do not have a proof.

Incompleteness

Theorem (Gödel's Incompleteness Theorem)

There is no proof system that can prove every valid first-order sentence about arithmetic over the natural numbers.

$\Rightarrow$ There are true statements that do not have a proof.

$\Rightarrow$ Because of (cons) there are valid triples that result from valid, but unprovable, consequences.

Incompleteness

Theorem (Gödel's Incompleteness Theorem)

There is no proof system that can prove every valid first-order sentence about arithmetic over the natural numbers.

- $\Rightarrow$ There are true statements that do not have a proof.
- $\Rightarrow$ Because of (cons) there are valid triples that result from valid, but unprovable, consequences.
- $\Rightarrow$ Hoare Logic is not complete.

Relative completeness of Hoare Logic

Theorem (Relative completeness of Hoare Logic)

With an oracle that decides the validity of predicates,

$$\textit{if } \models \{\varphi\}\, P\, \{\psi\} \;\textit{ then } \vdash \{\varphi\}\, P\, \{\psi\}\,.$$

Intuitively: Hoare logic is no more incomplete than the logic used to express the pre- and postconditions.

Summary

- $\mathcal{L}$: A simple imperative programming language
- Hoare triples (SYNTAX)
- Hoare logic (PROOF)
- Semantics for Hoare logic
- Handling termination
- Adding non-determinism

Termination

Hoare triples for partial correctness:

$$\{\varphi\}\, P\, \{\psi\}$$

Asserts ψ holds *if* P terminates.

That's just a safety property. Let's add liveness!

Termination

Hoare triples for partial correctness:

$$\{\varphi\}\, P\, \{\psi\}$$

Asserts ψ holds *if* P terminates.

That's just a safety property. Let's add liveness!

Hoare triples for total correctness:

$$[\varphi]\, P\, [\psi]$$

Asserts:
If φ holds at a starting state, and P is executed;
then P will terminate and ψ will hold in the resulting state.

Warning

Termination is hard!

- Algorithmic limitations (e.g. Halting problem)

Warning

Termination is hard!

- Algorithmic limitations (e.g. Halting problem)
- Mathematical limitations

Example

COLLATZ

while $n > 1$ do
    if $n\%2 = 0$
    then
        $n := n/2$
    else
        $n := 3 * n + 1$
    fi
od

Total correctness

How can we show:

$$[(m \geq 0) \wedge (n > 0)]\ \mathrm{P{\scriptsize OW}}\ [r = n^m]?$$

Total correctness

How can we show:

$$[(m \geq 0) \wedge (n > 0)]\ \textsc{Pow}\ [r = n^m]?$$

Use **Hoare Logic for total correctness**:

- (ass), (seq), (cond), and (cons) rules all the same
- Modified (loop) rule

Rules for total correctness

$$\frac{}{[\varphi[e/x]]\ x := e\ [\varphi]} \quad \text{(ass)}$$

$$\frac{[\varphi]\ P\ [\psi] \qquad [\psi]\ Q\ [\rho]}{[\varphi]\ P; Q\ [\rho]} \quad \text{(seq)}$$

$$\frac{[\varphi \wedge g]\ P\ [\psi] \qquad [\varphi \wedge \neg g]\ Q\ [\psi]}{[\varphi]\ \text{if } g \text{ then } P \text{ else } Q \text{ fi}\ [\psi]} \quad \text{(if)}$$

$$\frac{\varphi' \to \varphi \qquad [\varphi]\ P\ [\psi] \qquad \psi \to \psi'}{[\varphi']\ P\ [\psi']} \quad \text{(cons)}$$

Terminating while loops

$$\{\varphi\}\,\text{while } b \text{ do } P \text{ od}\,\{\psi\}$$

Partial correctness:
Find an invariant I such that:

- $\varphi \to I$ (establish)
- $\{I \wedge b\}\, P\, \{I\}$ (maintain)
- $(I \wedge \neg b) \to \psi$ (conclude)

Terminating while loops

$$[\varphi]\ \text{while } b \text{ do } P \text{ od } [\psi]$$

Partial correctness:
Find an invariant I such that:

- $\varphi \to I$ (establish)
- $[I \wedge b]\ P\ [I]$ (maintain)
- $(I \wedge \neg b) \to \psi$ (conclude)

Show termination:
Find a **variant** v such that:

- $(I \wedge b) \to v > 0$ (positivity)
- $[I \wedge b \wedge v = N]\ P\ [v < N]$ (progress)

Loop rule for total correctness

$$\frac{[\varphi \wedge g \wedge (v = N)]\ P\ [\varphi \wedge (v < N)] \qquad (\varphi \wedge g) \rightarrow (v > 0)}{[\varphi]\ \text{while } g \text{ do } P \text{ od}\ [\varphi \wedge \neg g]} \quad \text{(loop)}$$

Termination for Pow

Pow

$$\{\text{init: } (m \geq 0) \wedge (n > 0)\}$$
$$\{(1 = n^0) \wedge (0 \leq m) \wedge \text{init}\}$$

$r := 1;$ $\quad \{(r = n^0) \wedge (0 \leq m) \wedge \text{init}\}$

$i := 0;$

$$\{\text{Inv}\}$$

while $i < m$ do $\quad \{\text{Inv} \wedge (i < m) \}$

$\quad\quad \{(r * n = n^{i+1}) \wedge (i + 1 \leq m) \wedge \text{init} \}$

$\quad r := r * n;$ $\quad \{(r = n^{i+1}) \wedge (i + 1 \leq m) \wedge \text{init} \}$

$\quad i := i + 1$ $\quad \{\text{Inv} \}$

od $\quad \{\text{Inv} \wedge (i \geq m)\}$

$$\{r = n^m\}$$

What is a suitable variant?

Termination for Pow

Pow

$$\{\text{init}: (m \geq 0) \wedge (n > 0)\}$$
$$\{(1 = n^0) \wedge (0 \leq m) \wedge \text{init}\}$$

$r := 1;$ $\quad \{(r = n^0) \wedge (0 \leq m) \wedge \text{init}\}$

$i := 0;$

$$\{\text{Inv}\}$$

while $i < m$ do $\quad \{\text{Inv} \wedge (i < m)\}$

$$\{(r * n = n^{i+1}) \wedge (i + 1 \leq m) \wedge \text{init}\}$$

$\quad r := r * n;$ $\quad \{(r = n^{i+1}) \wedge (i + 1 \leq m) \wedge \text{init}\}$

$\quad i := i + 1$ $\quad \{\text{Inv}\}$

od $\quad \{\text{Inv} \wedge (i \geq m)\}$

$$\{r = n^m\}$$

What is a suitable variant? $v := (m - i)$

Termination for Pow

Pow	
	$\{\text{init}: (m \geq 0) \wedge (n > 0)\}$
	$\{(1 = n^0) \wedge (0 \leq m) \wedge \text{init}\}$
$r := 1;$	$\{(r = n^0) \wedge (0 \leq m) \wedge \text{init}\}$
$i := 0;$	
	$\{\text{Inv}\}$
while $i < m$ do	$\{\text{Inv} \wedge (i < m) \wedge (v = N)\}$
	$\{(r * n = n^{i+1}) \wedge (i + 1 \leq m) \wedge \text{init}\}$
$r := r * n;$	$\{(r = n^{i+1}) \wedge (i + 1 \leq m) \wedge \text{init}\}$
$i := i + 1$	$\{\text{Inv}\}$
od	$\{\text{Inv} \wedge (i \geq m)\}$
	$\{r = n^m\}$

What is a suitable variant? $v := (m - i)$

Termination for Pow

POW	
	$\{\text{init}: (m \geq 0) \wedge (n > 0)\}$
	$\{(1 = n^0) \wedge (0 \leq m) \wedge \text{init}\}$
$r := 1;$	$\{(r = n^0) \wedge (0 \leq m) \wedge \text{init}\}$
$i := 0;$	
	$\{\text{Inv}\}$
while $i < m$ do	$\{\text{Inv} \wedge (i < m) \wedge (v = N)\}$
	$\{(r * n = n^{i+1}) \wedge (i + 1 \leq m) \wedge \text{init}\}$
$r := r * n;$	$\{(r = n^{i+1}) \wedge (i + 1 \leq m) \wedge \text{init}\}$
$i := i + 1$	$\{\text{Inv} \wedge (v < N)\}$
od	$\{\text{Inv} \wedge (i \geq m)\}$
	$\{r = n^m\}$

What is a suitable variant? $v := (m - i)$

Termination for Pow

Pow

	$\{\text{init}: (m \geq 0) \wedge (n > 0)\}$
	$\{(1 = n^0) \wedge (0 \leq m) \wedge \text{init}\}$
$r := 1;$	$\{(r = n^0) \wedge (0 \leq m) \wedge \text{init}\}$
$i := 0;$	
	$\{\text{Inv}\}$
while $i < m$ do	$\{\text{Inv} \wedge (i < m) \wedge (v = N)\}$
	$\{(r * n = n^{i+1}) \wedge (i + 1 \leq m) \wedge \text{init}\}$
$\quad r := r * n;$	$\{(r = n^{i+1}) \wedge (i + 1 \leq m) \wedge \text{init} \wedge (v = N)\}$
$\quad i := i + 1$	$\{\text{Inv} \wedge (v < N)\}$
od	$\{\text{Inv} \wedge (i \geq m)\}$
	$\{r = n^m\}$

What is a suitable variant? $v := (m - i)$

Termination for Pow

Pow

	$\{\text{init: } (m \geq 0) \wedge (n > 0)\}$
	$\{(1 = n^0) \wedge (0 \leq m) \wedge \text{init}\}$
$r := 1;$	$\{(r = n^0) \wedge (0 \leq m) \wedge \text{init}\}$
$i := 0;$	
	$\{\text{Inv}\}$
while $i < m$ do	$\{\text{Inv} \wedge (i < m) \wedge (v = N)\}$
	$\{(r * n = n^{i+1}) \wedge (i + 1 \leq m) \wedge \text{init} \wedge (v = N)\}$
$\quad r := r * n;$	$\{(r = n^{i+1}) \wedge (i + 1 \leq m) \wedge \text{init} \wedge (v = N)\}$
$\quad i := i + 1$	$\{\text{Inv} \wedge (v < N)\}$
od	$\{\text{Inv} \wedge (i \geq m)\}$
	$\{r = n^m\}$

What is a suitable variant? $v := (m - i)$

Additional proof obligations

$$
\begin{aligned}
\text{init:} \quad & (m \geq 0) \wedge (n > 0) \\
\text{Inv:} \quad & (r = n^i) \wedge (i \leq m) \wedge \text{init} \\
v: \quad & m - i
\end{aligned}
$$

- $\text{Inv} \wedge (i < m) \quad \rightarrow \quad (v > 0)$
- $[v = N]\, i := i + 1\, [v < N]$

Additional proof obligations

Total correctness Hoare logic is designed to prove partial correctness and termination at the same time.

You can also do them separately:

1. Prove a partial correctness Hoare triple.
2. Find a variant for every loop.

Doing it completely separate isn't always possible: sometimes, termination depends on the invariant.

Summary

- $\mathcal{L}$: A simple imperative programming language
- Hoare triples (SYNTAX)
- Hoare logic (PROOF)
- Semantics for Hoare logic
- Handling termination
- Adding non-determinism

Non-determinism

Non-determinism involves the computational model branching into one of several directions.

Any branch can happen (decision is not under our control).

Non-determinism

Why add non-determinism?

- More general than deterministic behaviour
- Sometimes useful for modelling interaction (c.f. coffee machines).
- Useful for abstraction (abstracted code is easier to reason about)

$\mathcal{L}^+$: a simple language with non-determinism

We relax the Conditional and Loop commands in $\mathcal{L}$ to give us non-deterministic behaviour.

The programs of $\mathcal{L}^+$ are defined as:

Assign: $x := e$, where x is a variable and e is an expression

Predicate: φ, where φ is a predicate

Sequence: $P; Q$, where P and Q are programs

$\mathcal{L}^+$: a simple language with non-determinism

We relax the Conditional and Loop commands in $\mathcal{L}$ to give us non-deterministic behaviour.

The programs of $\mathcal{L}^+$ are defined as:

Assign: $x := e$, where x is a variable and e is an expression

Predicate: φ, where φ is a predicate

Sequence: $P; Q$, where P and Q are programs

Choice: $P + Q$, where P and Q are programs; intuitively, make a non-deterministic choice between P and Q

$\mathcal{L}^+$: a simple language with non-determinism

We relax the Conditional and Loop commands in $\mathcal{L}$ to give us non-deterministic behaviour.

The programs of $\mathcal{L}^+$ are defined as:

Assign: $x := e$, where x is a variable and e is an expression

Predicate: φ, where φ is a predicate

Sequence: $P; Q$, where P and Q are programs

Choice: $P + Q$, where P and Q are programs; intuitively, make a non-deterministic choice between P and Q

Loop: P^*, where P is a program; intuitively, loop for a non-deterministic number of iterations

$\mathcal{L}^+$: a simple language with non-determinism

We relax the Conditional and Loop commands in $\mathcal{L}$ to give us non-deterministic behaviour.

The programs of $\mathcal{L}^+$ are defined as:

Assign: $x := e$, where x is a variable and e is an expression

Predicate: φ, where φ is a predicate

Sequence: $P; Q$, where P and Q are programs

Choice: $P + Q$, where P and Q are programs; intuitively, make a non-deterministic choice between P and Q

Loop: P^*, where P is a program; intuitively, loop for a non-deterministic number of iterations

$$P :: (x := e) \mid \varphi \mid P_1; P_2 \mid P_1 + P_2 \mid P_1^*$$

$\mathcal{L}^+$: a simple language with non-determinism

$$P :: (x := e) \mid \varphi \mid P_1; P_2 \mid P_1 + P_2 \mid P_1^*$$

NB

$\mathcal{L}$ can be defined in $\mathcal{L}^+$ by defining:

- if b then P else Q od $= (b; P) + (\neg b; Q)$
- while b do P od $= (b; P)^*; \neg b$

Example

Example

A program in $\mathcal{L}^+$ that non-deterministically checks if $(x \vee y) \wedge (\neg x \vee \neg z) \wedge (\neg y \vee z)$ is satisfiable:

SAT
$(x := 0) + (x := 1);$ $(y := 0) + (y := 1);$ $(z := 0) + (z := 1);$

Example

Example

A program in $\mathcal{L}^+$ that non-deterministically checks if $(x \vee y) \wedge (\neg x \vee \neg z) \wedge (\neg y \vee z)$ is satisfiable:

SAT
$(x := 0) + (x := 1);$ $(y := 0) + (y := 1);$ $(z := 0) + (z := 1);$ $\text{if}((x = 1) \vee (y = 1)) \wedge$ $\quad ((x = 0) \vee (z = 0)) \wedge$ $\quad ((y = 0) \vee (z = 1))$

Example

Example

A program in $\mathcal{L}^+$ that non-deterministically checks if $(x \vee y) \wedge (\neg x \vee \neg z) \wedge (\neg y \vee z)$ is satisfiable:

SAT
$(x := 0) + (x := 1);$ $(y := 0) + (y := 1);$ $(z := 0) + (z := 1);$ if$((x = 1) \vee (y = 1)) \wedge$ $\quad ((x = 0) \vee (z = 0)) \wedge$ $\quad ((y = 0) \vee (z = 1))$ then $r := 1$ else $r := 0$ fi

The formula is satisfiable if SAT *could* set r to 1.

Proof rules

Hoare logic rules are cleaner:

$$\frac{\{\varphi\}\, P\, \{\psi\} \qquad \{\varphi\}\, Q\, \{\psi\}}{\{\varphi\}\, P + Q\, \{\psi\}} \quad \text{(choice)}$$

$$\frac{\{\varphi\}\, P\, \{\varphi\}}{\{\varphi\}\, P^{*}\, \{\varphi\}} \quad \text{(loop)}$$

Semantics

Semantics is as for $\mathcal{L}$, except:

$$[\![P + Q]\!] = [\![P]\!] \cup [\![Q]\!] \qquad\qquad [\![P^*]\!] = [\![P]\!]^*$$

Bonus slides

What follows is a proof that Hoare logic is sound.

We most likely won't have time to do any of this in the lectures.

Summary

- Set theory revisited
- Soundness of Hoare Logic
- Completeness of Hoare Logic

Summary

- Set theory revisited
- Soundness of Hoare Logic
- Completeness of Hoare Logic

Some results on relational images

Lemma

For any binary relations $R, S \subseteq X \times Y$ *and subsets* $A, B \subseteq X$*:*

(a) *If* $A \subseteq B$ *then* $R(A) \subseteq R(B)$

(b) $R(A) \cup S(A) = (R \cup S)(A)$

(c) $R(S(A)) = (S; R)(A)$

Some results on relational images

Lemma

For any binary relations $R, S \subseteq X \times Y$ *and subsets* $A, B \subseteq X$:

(a) *If* $A \subseteq B$ *then* $R(A) \subseteq R(B)$

(b) $R(A) \cup S(A) = (R \cup S)(A)$

(c) $R(S(A)) = (S; R)(A)$

Proof (a):

Some results on relational images

Lemma

For any binary relations $R, S \subseteq X \times Y$ and subsets $A, B \subseteq X$:

(a) *If $A \subseteq B$ then $R(A) \subseteq R(B)$*
(b) $R(A) \cup S(A) = (R \cup S)(A)$
(c) $R(S(A)) = (S; R)(A)$

Proof (a):

$$\begin{aligned} y \in R(A) &\Leftrightarrow \exists x \in A \text{ such that } (x, y) \in R \\ &\Rightarrow \exists x \in B \text{ such that } (x, y) \in R \\ &\Leftrightarrow y \in R(B) \end{aligned}$$

Some results on relational images

Lemma

For any binary relations $R, S \subseteq X \times Y$ and subsets $A, B \subseteq X$:

(a) *If $A \subseteq B$ then $R(A) \subseteq R(B)$*

(b) $R(A) \cup S(A) = (R \cup S)(A)$

(c) $R(S(A)) = (S; R)(A)$

Proof (b):

Some results on relational images

Lemma

For any binary relations $R, S \subseteq X \times Y$ and subsets $A, B \subseteq X$:

(a) *If $A \subseteq B$ then $R(A) \subseteq R(B)$*

(b) $R(A) \cup S(A) = (R \cup S)(A)$

(c) $R(S(A)) = (S; R)(A)$

Proof (b):

$$
\begin{aligned}
y \in R(A) \cup S(A) \quad &\Leftrightarrow \quad y \in R(A) \text{ or } y \in S(A) \\
&\Leftrightarrow \quad \exists x \in A \text{ s.t. } (x, y) \in R \text{ or } \exists x \in A \text{ s.t. } (x, y) \in S \\
&\Leftrightarrow \quad \exists x \in A \text{ s.t. } (x, y) \in R \text{ or } (x, y) \in S \\
&\Leftrightarrow \quad \exists x \in A \text{ s.t. } (x, y) \in (R \cup S) \\
&\Leftrightarrow \quad y \in (R \cup S)(A)
\end{aligned}
$$

Some results on relational images

Lemma

For any binary relations $R, S \subseteq X \times Y$ and subsets $A, B \subseteq X$:

(a) *If* $A \subseteq B$ *then* $R(A) \subseteq R(B)$

(b) $R(A) \cup S(A) = (R \cup S)(A)$

(c) $R(S(A)) = (S; R)(A)$

Proof (c):

Some results on relational images

Lemma

For any binary relations $R, S \subseteq X \times Y$ and subsets $A, B \subseteq X$:

(a) *If $A \subseteq B$ then $R(A) \subseteq R(B)$*
(b) $R(A) \cup S(A) = (R \cup S)(A)$
(c) $R(S(A)) = (S;R)(A)$

Proof (c):

$$
\begin{aligned}
z \in R(S(A)) \quad &\Leftrightarrow \quad \exists y \in S(A) \text{ s.t. } (y,z) \in R \\
&\Leftrightarrow \quad \exists x \in A,\ y \in S(A) \text{ s.t. } (x,y) \in S \text{ and } (y,z) \in R \\
&\Leftrightarrow \quad \exists x \in A \text{ s.t. } (x,z) \in (S;R) \\
&\Leftrightarrow \quad z \in (S;R)(A)
\end{aligned}
$$

Some results on relational images

Corollary

If $R(A) \subseteq A$ *then* $R^*(A) \subseteq A$

Reformulated: assuming $R(A) \subseteq A$, $x \in A$, and $x \; R^* \; y$, prove $y \in A$.

Proof is by induction on the derivation of $x \; R^* \; y$.

(B) Trivial when $x = y$.

(I) We know that $x \in A$, $x \; R \; y$ and $y \; R^* \; z$. Because $R(A) \subseteq A$, we have $y \in A$. By the induction hypothesis, $z \in A$.

Summary

- Set theory revisited
- Soundness of Hoare Logic
- Completeness of Hoare Logic

Soundness of Hoare Logic

Theorem

If $\vdash \{\varphi\}\, P\, \{\psi\}$ *then* $\models \{\varphi\}\, P\, \{\psi\}$

Soundness of Hoare Logic

Theorem

If $\vdash \{\varphi\}\, P\, \{\psi\}$ *then* $\models \{\varphi\}\, P\, \{\psi\}$

Proof:

Soundness of Hoare Logic

Theorem

If $\vdash \{\varphi\}\, P\, \{\psi\}$ *then* $\models \{\varphi\}\, P\, \{\psi\}$

Proof:
By induction on the structure of the proof.

Base case: Assignment rule

$$\frac{}{\{\varphi[e/x]\}\ x := e\ \{\varphi\}} \quad \text{(ass)}$$

Base case: Assignment rule

$$\frac{}{\{\varphi[e/x]\}\, x := e\, \{\varphi\}} \quad \text{(ass)}$$

Need to show $\{\varphi[e/x]\}\, x := e\, \{\varphi\}$ is always valid. That is,

$$[\![x := e]\!](\langle \varphi[e/x] \rangle) \subseteq \langle \varphi \rangle.$$

Base case: Assignment rule

$$\frac{}{\{\varphi[e/x]\}\, x := e\, \{\varphi\}} \quad (\text{ass})$$

Need to show $\{\varphi[e/x]\}\, x := e\, \{\varphi\}$ is always valid. That is,

$$[\![x := e]\!](\langle \varphi[e/x] \rangle) \subseteq \langle \varphi \rangle.$$

Observation: $[\![\varphi[e/x]]\!]^{\eta} = [\![\varphi]\!]^{\eta'}$ where $\eta' = \eta[x \mapsto [\![e]\!]^{\eta}]$

Base case: Assignment rule

$$\frac{}{\{\varphi[e/x]\}\, x := e\, \{\varphi\}} \quad \text{(ass)}$$

Need to show $\{\varphi[e/x]\}\, x := e\, \{\varphi\}$ is always valid. That is,

$$[\![x := e]\!](\langle\varphi[e/x]\rangle) \subseteq \langle\varphi\rangle.$$

Observation: $[\![\varphi[e/x]]\!]^\eta = [\![\varphi]\!]^{\eta'}$ where $\eta' = \eta[x \mapsto [\![e]\!]^\eta]$

So if $\eta \in \langle\varphi[e/x]\rangle$ then $\eta' \in \langle\varphi\rangle$

Base case: Assignment rule

$$\frac{}{\{\varphi[e/x]\}\, x := e\, \{\varphi\}} \quad \text{(ass)}$$

Need to show $\{\varphi[e/x]\}\, x := e\, \{\varphi\}$ is always valid. That is,

$$[\![x := e]\!](\langle\varphi[e/x]\rangle) \subseteq \langle\varphi\rangle.$$

Observation: $[\![\varphi[e/x]]\!]^{\eta} = [\![\varphi]\!]^{\eta'}$ where $\eta' = \eta[x \mapsto [\![e]\!]^{\eta}]$

So if $\eta \in \langle\varphi[e/x]\rangle$ then $\eta' \in \langle\varphi\rangle$

Recall: $(\eta, \eta'') \in [\![x := e]\!]$ if and only if $\eta'' = \eta[x \mapsto [\![e]\!]^{\eta}]$,

Base case: Assignment rule

$$\frac{}{\{\varphi[e/x]\}\, x := e\, \{\varphi\}} \quad \text{(ass)}$$

Need to show $\{\varphi[e/x]\}\, x := e\, \{\varphi\}$ is always valid. That is,

$$[\![x := e]\!](\langle\varphi[e/x]\rangle) \subseteq \langle\varphi\rangle.$$

Observation: $[\![\varphi[e/x]]\!]^{\eta} = [\![\varphi]\!]^{\eta'}$ where $\eta' = \eta[x \mapsto [\![e]\!]^{\eta}]$

So if $\eta \in \langle\varphi[e/x]\rangle$ then $\eta' \in \langle\varphi\rangle$

Recall: $(\eta, \eta'') \in [\![x := e]\!]$ if and only if $\eta'' = \eta[x \mapsto [\![e]\!]^{\eta}]$,

So $[\![x := e]\!](\eta) \in \langle\varphi\rangle$ for all $\eta \in \langle\varphi[e/x]\rangle$

Base case: Assignment rule

$$\frac{}{\{\varphi[e/x]\}\, x := e\, \{\varphi\}} \quad \text{(ass)}$$

Need to show $\{\varphi[e/x]\}\, x := e\, \{\varphi\}$ is always valid. That is,

$$[\![x := e]\!](\langle\varphi[e/x]\rangle) \subseteq \langle\varphi\rangle.$$

Observation: $[\![\varphi[e/x]]\!]^{\eta} = [\![\varphi]\!]^{\eta'}$ where $\eta' = \eta[x \mapsto [\![e]\!]^{\eta}]$

So if $\eta \in \langle\varphi[e/x]\rangle$ then $\eta' \in \langle\varphi\rangle$

Recall: $(\eta, \eta'') \in [\![x := e]\!]$ if and only if $\eta'' = \eta[x \mapsto [\![e]\!]^{\eta}]$,

So $[\![x := e]\!](\eta) \in \langle\varphi\rangle$ for all $\eta \in \langle\varphi[e/x]\rangle$

So $[\![x := e]\!](\langle\varphi[e/x]\rangle) \subseteq \langle\varphi\rangle$

Inductive case 1: Sequence rule

$$\frac{\{\varphi\}\ P\ \{\psi\} \qquad \{\psi\}\ Q\ \{\rho\}}{\{\varphi\}\ P; Q\ \{\rho\}} \quad (\text{seq})$$

Inductive case 1: Sequence rule

$$\frac{\{\varphi\}\ P\ \{\psi\} \qquad \{\psi\}\ Q\ \{\rho\}}{\{\varphi\}\ P; Q\ \{\rho\}} \quad \text{(seq)}$$

Assume $\{\varphi\}\ P\ \{\psi\}$ and $\{\psi\}\ Q\ \{\rho\}$ are valid. Need to show that $\{\varphi\}\ P; Q\ \{\rho\}$ is valid.

Inductive case 1: Sequence rule

$$\frac{\{\varphi\}\, P\, \{\psi\} \qquad \{\psi\}\, Q\, \{\rho\}}{\{\varphi\}\, P; Q\, \{\rho\}} \quad \text{(seq)}$$

Assume $\{\varphi\}\, P\, \{\psi\}$ and $\{\psi\}\, Q\, \{\rho\}$ are valid. Need to show that $\{\varphi\}\, P; Q\, \{\rho\}$ is valid.

Recall: $[\![P; Q]\!] = [\![P]\!]; [\![Q]\!]$

Inductive case 1: Sequence rule

$$\frac{\{\varphi\}\, P\, \{\psi\} \qquad \{\psi\}\, Q\, \{\rho\}}{\{\varphi\}\, P; Q\, \{\rho\}} \quad \text{(seq)}$$

Assume $\{\varphi\}\, P\, \{\psi\}$ and $\{\psi\}\, Q\, \{\rho\}$ are valid. Need to show that $\{\varphi\}\, P; Q\, \{\rho\}$ is valid.

Recall: $[\![P; Q]\!] = [\![P]\!]; [\![Q]\!]$

So: $[\![P; Q]\!](\langle\varphi\rangle) = [\![Q]\!]\big([\![P]\!](\langle\varphi\rangle)\big)$ (see Lemma 1(c))

Inductive case 1: Sequence rule

$$\frac{\{\varphi\}\, P\, \{\psi\} \qquad \{\psi\}\, Q\, \{\rho\}}{\{\varphi\}\, P; Q\, \{\rho\}} \quad (\text{seq})$$

Assume $\{\varphi\}\, P\, \{\psi\}$ and $\{\psi\}\, Q\, \{\rho\}$ are valid. Need to show that $\{\varphi\}\, P; Q\, \{\rho\}$ is valid.

Recall: $[\![P; Q]\!] = [\![P]\!]; [\![Q]\!]$

So: $[\![P; Q]\!](\langle\varphi\rangle) = [\![Q]\!]\big([\![P]\!](\langle\varphi\rangle)\big)$ (see Lemma 1(c))

By IH: $[\![P]\!](\langle\varphi\rangle) \subseteq \langle\psi\rangle$ and $[\![Q]\!](\langle\psi\rangle) \subseteq \langle\rho\rangle$

Inductive case 1: Sequence rule

$$\frac{\{\varphi\}\,P\,\{\psi\} \qquad \{\psi\}\,Q\,\{\rho\}}{\{\varphi\}\,P;Q\,\{\rho\}} \quad \text{(seq)}$$

Assume $\{\varphi\}\,P\,\{\psi\}$ and $\{\psi\}\,Q\,\{\rho\}$ are valid. Need to show that $\{\varphi\}\,P;Q\,\{\rho\}$ is valid.

Recall: $[\![P;Q]\!] = [\![P]\!];[\![Q]\!]$

So: $[\![P;Q]\!](\langle\varphi\rangle) = [\![Q]\!]\big([\![P]\!](\langle\varphi\rangle)\big)$ (see Lemma 1(c))

By IH: $[\![P]\!](\langle\varphi\rangle) \subseteq \langle\psi\rangle$ and $[\![Q]\!](\langle\psi\rangle) \subseteq \langle\rho\rangle$

So: $[\![Q]\!]\big([\![P]\!](\langle\varphi\rangle)\big) \subseteq [\![Q]\!]\big(\langle\psi\rangle\big) \subseteq \langle\rho\rangle$ (see Lemma 1(a))

Two more useful results

Lemma

For $R \subseteq \textsc{Env} \times \textsc{Env}$*, predicates* φ *and* ψ*, and* $X \subseteq \textsc{Env}$*:*

(a) $[\![\varphi]\!](X) = \langle\varphi\rangle \cap X$

(b) $R(\langle\varphi \wedge \psi\rangle) = ([\![\varphi]\!]; R)(\langle\psi\rangle)$

Two more useful results

Lemma

For $R \subseteq \textsc{Env} \times \textsc{Env}$, *predicates* φ *and* ψ, *and* $X \subseteq \textsc{Env}$*:*

(a) $[\![\varphi]\!](X) = \langle\varphi\rangle \cap X$

(b) $R(\langle\varphi \wedge \psi\rangle) = ([\![\varphi]\!]; R)(\langle\psi\rangle)$

Proof (a):

Two more useful results

Lemma

For $R \subseteq \textsc{Env} \times \textsc{Env}$, predicates φ and ψ, and $X \subseteq \textsc{Env}$:

1. (a) $[\![\varphi]\!](X) = \langle\varphi\rangle \cap X$
2. (b) $R(\langle\varphi \wedge \psi\rangle) = ([\![\varphi]\!]; R)(\langle\psi\rangle))$

Proof (a):

$$
\begin{aligned}
\eta' \in [\![\varphi]\!](X) \quad & \Leftrightarrow \quad \exists \eta \in X \text{ s.t. } (\eta, \eta') \in [\![\varphi]\!] \\
& \Leftrightarrow \quad \exists \eta \in X \text{ s.t. } \eta = \eta' \text{ and } \eta \in \langle\varphi\rangle \\
& \Leftrightarrow \quad \eta' \in X \cap \langle\varphi\rangle
\end{aligned}
$$

Two more useful results

Lemma

For $R \subseteq \textsc{Env} \times \textsc{Env}$, *predicates* φ *and* ψ, *and* $X \subseteq \textsc{Env}$*:*

(a) $[\![\varphi]\!](X) = \langle\varphi\rangle \cap X$

(b) $R(\langle\varphi \wedge \psi\rangle) = ([\![\varphi]\!]; R)(\langle\psi\rangle)$

Proof (b):

$$\begin{array}{rcl} \langle\varphi \wedge \psi\rangle & = & \langle\varphi\rangle \cap \langle\psi\rangle = [\![\varphi]\!](\langle\psi\rangle) \\ \text{So } R(\langle\varphi \wedge \psi\rangle) & = & R\big([\![\varphi]\!](\langle\psi\rangle)\big) \\ & = & ([\![\varphi]\!]; R)(\langle\psi\rangle) \qquad \text{(see Lemma 1(b))} \end{array}$$

Inductive case 2: Conditional rule

$$\frac{\{\varphi \wedge g\}\ P\ \{\psi\} \qquad \{\varphi \wedge \neg g\}\ Q\ \{\psi\}}{\{\varphi\}\ \text{if } g \text{ then } P \text{ else } Q \text{ fi}\ \{\psi\}} \quad \text{(if)}$$

Inductive case 2: Conditional rule

$$\frac{\{\varphi \wedge g\}\ P\ \{\psi\} \qquad \{\varphi \wedge \neg g\}\ Q\ \{\psi\}}{\{\varphi\}\ \textsf{if}\ g\ \textsf{then}\ P\ \textsf{else}\ Q\ \textsf{fi}\ \{\psi\}} \quad \text{(if)}$$

Assume $\{\varphi \wedge g\}\ P\ \{\psi\}$ and $\{\varphi \wedge \neg g\}\ Q\ \{\psi\}$ are valid. Need to show that $\{\varphi\}\ \textsf{if}\ g\ \textsf{then}\ P\ \textsf{else}\ Q\ \textsf{fi}\ \{\psi\}$ is valid.

Inductive case 2: Conditional rule

$$\frac{\{\varphi \wedge g\}\, P\, \{\psi\} \qquad \{\varphi \wedge \neg g\}\, Q\, \{\psi\}}{\{\varphi\}\, \text{if } g \text{ then } P \text{ else } Q \text{ fi}\, \{\psi\}} \quad \text{(if)}$$

Assume $\{\varphi \wedge g\}\, P\, \{\psi\}$ and $\{\varphi \wedge \neg g\}\, Q\, \{\psi\}$ are valid. Need to show that $\{\varphi\}$ if g then P else Q fi $\{\psi\}$ is valid.

Recall: $[\![\text{if } g \text{ then } P \text{ else } Q \text{ fi}]\!] = [\![g; P]\!] \cup [\![\neg g; Q]\!]$

Inductive case 2: Conditional rule

$$\frac{\{\varphi \wedge g\}\, P\, \{\psi\} \qquad \{\varphi \wedge \neg g\}\, Q\, \{\psi\}}{\{\varphi\}\ \mathsf{if}\ g\ \mathsf{then}\ P\ \mathsf{else}\ Q\ \mathsf{fi}\ \{\psi\}} \quad (\mathsf{if})$$

Assume $\{\varphi \wedge g\}\, P\, \{\psi\}$ and $\{\varphi \wedge \neg g\}\, Q\, \{\psi\}$ are valid. Need to show that $\{\varphi\}\ \mathsf{if}\ g\ \mathsf{then}\ P\ \mathsf{else}\ Q\ \mathsf{fi}\ \{\psi\}$ is valid.

Recall: $[\![\mathsf{if}\ g\ \mathsf{then}\ P\ \mathsf{else}\ Q\ \mathsf{fi}]\!] = [\![g; P]\!] \cup [\![\neg g; Q]\!]$

$$[\![\mathsf{if}\ g\ \mathsf{then}\ P\ \mathsf{else}\ Q\ \mathsf{fi}]\!](\langle\varphi\rangle)$$

Inductive case 2: Conditional rule

$$\frac{\{\varphi \wedge g\}\ P\ \{\psi\} \qquad \{\varphi \wedge \neg g\}\ Q\ \{\psi\}}{\{\varphi\}\ \text{if } g \text{ then } P \text{ else } Q \text{ fi}\ \{\psi\}} \quad \text{(if)}$$

Assume $\{\varphi \wedge g\}\ P\ \{\psi\}$ and $\{\varphi \wedge \neg g\}\ Q\ \{\psi\}$ are valid. Need to show that $\{\varphi\}$ if g then P else Q fi $\{\psi\}$ is valid.

Recall: $[\![\text{if } g \text{ then } P \text{ else } Q \text{ fi}]\!] = [\![g; P]\!] \cup [\![\neg g; Q]\!]$

$$[\![\text{if } g \text{ then } P \text{ else } Q \text{ fi}]\!](\langle\varphi\rangle)$$

$$= [\![g; P]\!](\langle\varphi\rangle) \cup [\![\neg g; Q]\!](\langle\varphi\rangle) \qquad \text{(see Lemma 1(b))}$$

Inductive case 2: Conditional rule

$$\frac{\{\varphi \wedge g\}\ P\ \{\psi\} \qquad \{\varphi \wedge \neg g\}\ Q\ \{\psi\}}{\{\varphi\}\ \text{if } g \text{ then } P \text{ else } Q \text{ fi}\ \{\psi\}} \quad \text{(if)}$$

Assume $\{\varphi \wedge g\}\ P\ \{\psi\}$ and $\{\varphi \wedge \neg g\}\ Q\ \{\psi\}$ are valid. Need to show that $\{\varphi\}$ if g then P else Q fi $\{\psi\}$ is valid.

Recall: $[\![\text{if } g \text{ then } P \text{ else } Q \text{ fi}]\!] = [\![g; P]\!] \cup [\![\neg g; Q]\!]$

$$\begin{aligned}
&[\![\text{if } g \text{ then } P \text{ else } Q \text{ fi}]\!](\langle\varphi\rangle) \\
&= [\![g; P]\!](\langle\varphi\rangle) \cup [\![\neg g; Q]\!](\langle\varphi\rangle) && \text{(see Lemma 1(b))} \\
&= [\![P]\!](\langle g \wedge \varphi\rangle) \cup [\![Q]\!](\langle \neg g \wedge \varphi\rangle) && \text{(see Lemma 2(b))}
\end{aligned}$$

Inductive case 2: Conditional rule

$$\frac{\{\varphi \wedge g\}\ P\ \{\psi\} \qquad \{\varphi \wedge \neg g\}\ Q\ \{\psi\}}{\{\varphi\}\ \text{if } g \text{ then } P \text{ else } Q \text{ fi}\ \{\psi\}} \quad \text{(if)}$$

Assume $\{\varphi \wedge g\}\ P\ \{\psi\}$ and $\{\varphi \wedge \neg g\}\ Q\ \{\psi\}$ are valid. Need to show that $\{\varphi\}\ \text{if } g \text{ then } P \text{ else } Q \text{ fi}\ \{\psi\}$ is valid.

Recall: $[\![\text{if } g \text{ then } P \text{ else } Q \text{ fi}]\!] = [\![g; P]\!] \cup [\![\neg g; Q]\!]$

$$\begin{aligned}
&[\![\text{if } g \text{ then } P \text{ else } Q \text{ fi}]\!](\langle\varphi\rangle) \\
&\quad = [\![g; P]\!](\langle\varphi\rangle) \cup [\![\neg g; Q]\!](\langle\varphi\rangle) && \text{(see Lemma 1(b))} \\
&\quad = [\![P]\!](\langle g \wedge \varphi\rangle) \cup [\![Q]\!](\langle \neg g \wedge \varphi\rangle) && \text{(see Lemma 2(b))} \\
&\quad \subseteq \langle\psi\rangle && \text{(by IH)}
\end{aligned}$$

Inductive case 3: While rule

$$\frac{\{\varphi \wedge g\}\ P\ \{\varphi\}}{\{\varphi\}\ \text{while}\ g\ \text{do}\ P\ \text{od}\ \{\varphi \wedge \neg g\}} \quad \text{(loop)}$$

Inductive case 3: While rule

$$\frac{\{\varphi \wedge g\}\ P\ \{\varphi\}}{\{\varphi\}\ \text{while}\ g\ \text{do}\ P\ \text{od}\ \{\varphi \wedge \neg g\}}\quad \text{(loop)}$$

Assume $\{\varphi \wedge g\}\ P\ \{\varphi\}$ is valid. Need to show that $\{\varphi\}\ \text{while}\ g\ \text{do}\ P\ \text{od}\ \{\varphi \wedge \neg g\}$ is valid.

Inductive case 3: While rule

$$\frac{\{\varphi \wedge g\}\ P\ \{\varphi\}}{\{\varphi\}\ \text{while } g \text{ do } P \text{ od}\ \{\varphi \wedge \neg g\}} \quad \text{(loop)}$$

Assume $\{\varphi \wedge g\}\ P\ \{\varphi\}$ is valid. Need to show that $\{\varphi\}\ \text{while } g \text{ do } P \text{ od}\ \{\varphi \wedge \neg g\}$ is valid.

Recall: $[\![\text{while } g \text{ do } P \text{ od}]\!] = [\![g; P]\!]^*; [\![\neg g]\!]$

Inductive case 3: While rule

$$\frac{\{\varphi \wedge g\}\ P\ \{\varphi\}}{\{\varphi\}\ \text{while } g \text{ do } P \text{ od}\ \{\varphi \wedge \neg g\}} \quad \text{(loop)}$$

Assume $\{\varphi \wedge g\}\ P\ \{\varphi\}$ is valid. Need to show that $\{\varphi\}$ while g do P od $\{\varphi \wedge \neg g\}$is valid.

Recall: $[\![\text{while } g \text{ do } P \text{ od}]\!] = [\![g; P]\!]^*; [\![\neg g]\!]$

$$[\![g; P]\!](\langle\varphi\rangle) \quad = [\![P]\!](\langle g \wedge \varphi\rangle) \qquad \text{(see Lemma 2(b))}$$

Inductive case 3: While rule

$$\frac{\{\varphi \wedge g\}\, P\, \{\varphi\}}{\{\varphi\}\, \text{while } g \text{ do } P \text{ od}\, \{\varphi \wedge \neg g\}} \quad \text{(loop)}$$

Assume $\{\varphi \wedge g\}\, P\, \{\varphi\}$ is valid. Need to show that $\{\varphi\}\, \text{while } g \text{ do } P \text{ od}\, \{\varphi \wedge \neg g\}$ is valid.

Recall: $[\![\text{while } g \text{ do } P \text{ od}]\!] = [\![g; P]\!]^*; [\![\neg g]\!]$

$$\begin{aligned}[\![g; P]\!](\langle\varphi\rangle) &= [\![P]\!](\langle g \wedge \varphi\rangle) && \text{(see Lemma 2(b))}\\ &\subseteq \langle\varphi\rangle && \text{(IH)}\end{aligned}$$

Inductive case 3: While rule

$$\frac{\{\varphi \wedge g\}\ P\ \{\varphi\}}{\{\varphi\}\ \text{while } g \text{ do } P \text{ od}\ \{\varphi \wedge \neg g\}} \quad \text{(loop)}$$

Assume $\{\varphi \wedge g\}\ P\ \{\varphi\}$ is valid. Need to show that $\{\varphi\}\ \text{while } g \text{ do } P \text{ od}\ \{\varphi \wedge \neg g\}$is valid.

Recall: $[\![\text{while } g \text{ do } P \text{ od}]\!] = [\![g; P]\!]^*; [\![\neg g]\!]$

$$\begin{aligned} [\![g;P]\!](\langle\varphi\rangle) &= [\![P]\!](\langle g \wedge \varphi\rangle) && \text{(see Lemma 2(b))} \\ &\subseteq \langle\varphi\rangle && \text{(IH)} \\ \text{So } [\![g;P]\!]^*(\langle\varphi\rangle) &\subseteq \langle\varphi\rangle && \text{(see Corollary)} \end{aligned}$$

Inductive case 3: While rule

$$\frac{\{\varphi \wedge g\}\ P\ \{\varphi\}}{\{\varphi\}\ \text{while } g \text{ do } P \text{ od}\ \{\varphi \wedge \neg g\}} \quad \text{(loop)}$$

Assume $\{\varphi \wedge g\}\ P\ \{\varphi\}$ is valid. Need to show that $\{\varphi\}$ while g do P od $\{\varphi \wedge \neg g\}$is valid.

Recall: $[\![\text{while } g \text{ do } P \text{ od}]\!] = [\![g; P]\!]^*; [\![\neg g]\!]$

$$\begin{aligned}
[\![g; P]\!](\langle\varphi\rangle) &= [\![P]\!](\langle g \wedge \varphi\rangle) && \text{(see Lemma 2(b))} \\
&\subseteq \langle\varphi\rangle && \text{(IH)} \\
\text{So } [\![g; P]\!]^*(\langle\varphi\rangle) &\subseteq \langle\varphi\rangle && \text{(see Corollary)} \\
\text{So } [\![g; P]\!]^*; [\![\neg g]\!](\langle\varphi\rangle) &= [\![\neg g]\!]\big([\![g; P]\!]^*(\langle\varphi\rangle)\big) && \text{(see Lemma 1(c))}
\end{aligned}$$

Inductive case 3: While rule

$$\frac{\{\varphi \wedge g\}\ P\ \{\varphi\}}{\{\varphi\}\ \text{while } g \text{ do } P \text{ od}\ \{\varphi \wedge \neg g\}} \quad \text{(loop)}$$

Assume $\{\varphi \wedge g\}\ P\ \{\varphi\}$ is valid. Need to show that $\{\varphi\}$ while g do P od $\{\varphi \wedge \neg g\}$is valid.

Recall: $[\![\text{while } g \text{ do } P \text{ od}]\!] = [\![g; P]\!]^*; [\![\neg g]\!]$

$$\begin{aligned}
[\![g; P]\!](\langle\varphi\rangle) &= [\![P]\!](\langle g \wedge \varphi\rangle) && \text{(see Lemma 2(b))}\\
&\subseteq \langle\varphi\rangle && \text{(IH)}\\
\text{So } [\![g; P]\!]^*(\langle\varphi\rangle) &\subseteq \langle\varphi\rangle && \text{(see Corollary)}\\
\text{So } [\![g; P]\!]^*; [\![\neg g]\!](\langle\varphi\rangle) &= [\![\neg g]\!]\big([\![g; P]\!]^*(\langle\varphi\rangle)\big) && \text{(see Lemma 1(c))}\\
&\subseteq [\![\neg g]\!](\langle\varphi\rangle) && \text{(see Lemma 1(a))}
\end{aligned}$$

Inductive case 3: While rule

$$\frac{\{\varphi \wedge g\}\ P\ \{\varphi\}}{\{\varphi\}\ \text{while}\ g\ \text{do}\ P\ \text{od}\ \{\varphi \wedge \neg g\}}\quad \text{(loop)}$$

Assume $\{\varphi \wedge g\}\ P\ \{\varphi\}$ is valid. Need to show that $\{\varphi\}\ \text{while}\ g\ \text{do}\ P\ \text{od}\ \{\varphi \wedge \neg g\}$is valid.

Recall: $[\![\text{while}\ g\ \text{do}\ P\ \text{od}]\!] = [\![g; P]\!]^*; [\![\neg g]\!]$

$$\begin{aligned}
[\![g; P]\!](\langle\varphi\rangle) &= [\![P]\!](\langle g \wedge \varphi\rangle) && \text{(see Lemma 2(b))}\\
&\subseteq \langle\varphi\rangle && \text{(IH)}\\
\text{So } [\![g; P]\!]^*(\langle\varphi\rangle) &\subseteq \langle\varphi\rangle && \text{(see Corollary)}\\
\text{So } [\![g; P]\!]^*; [\![\neg g]\!](\langle\varphi\rangle) &= [\![\neg g]\!]\big([\![g; P]\!]^*(\langle\varphi\rangle)\big) && \text{(see Lemma 1(c))}\\
&\subseteq [\![\neg g]\!](\langle\varphi\rangle) && \text{(see Lemma 1(a))}\\
&= \langle\neg g \wedge \varphi\rangle && \text{(see Lemma 2(a))}
\end{aligned}$$

Inductive case 4: Consequence rule

$$\frac{\varphi' \to \varphi \qquad \{\varphi\}\, P\, \{\psi\} \qquad \psi \to \psi'}{\{\varphi'\}\, P\, \{\psi'\}} \quad \text{(cons)}$$

Inductive case 4: Consequence rule

$$\frac{\varphi' \to \varphi \qquad \{\varphi\}\, P\, \{\psi\} \qquad \psi \to \psi'}{\{\varphi'\}\, P\, \{\psi'\}} \quad \text{(cons)}$$

Assume $\{\varphi\}\, P\, \{\psi\}$ is valid and $\varphi' \to \varphi$ and $\psi \to \psi'$. Need to show that $\{\varphi'\}\, P\, \{\psi'\}$ is valid.

Inductive case 4: Consequence rule

$$\frac{\varphi' \to \varphi \qquad \{\varphi\}\, P\, \{\psi\} \qquad \psi \to \psi'}{\{\varphi'\}\, P\, \{\psi'\}} \quad \text{(cons)}$$

Assume $\{\varphi\}\, P\, \{\psi\}$ is valid and $\varphi' \to \varphi$ and $\psi \to \psi'$. Need to show that $\{\varphi'\}\, P\, \{\psi'\}$ is valid.

Observe: If $\varphi' \to \varphi$ then $\langle \varphi' \rangle \subseteq \langle \varphi \rangle$

Inductive case 4: Consequence rule

$$\frac{\varphi' \to \varphi \qquad \{\varphi\}\, P\, \{\psi\} \qquad \psi \to \psi'}{\{\varphi'\}\, P\, \{\psi'\}} \quad \text{(cons)}$$

Assume $\{\varphi\}\, P\, \{\psi\}$ is valid and $\varphi' \to \varphi$ and $\psi \to \psi'$. Need to show that $\{\varphi'\}\, P\, \{\psi'\}$ is valid.

Observe: If $\varphi' \to \varphi$ then $\langle \varphi' \rangle \subseteq \langle \varphi \rangle$

$$[\![P]\!](\langle \varphi' \rangle) \quad \subseteq \quad [\![P]\!](\langle \varphi \rangle) \quad \text{(see Lemma 1(a))}$$

Inductive case 4: Consequence rule

$$\frac{\varphi' \to \varphi \qquad \{\varphi\}\, P\, \{\psi\} \qquad \psi \to \psi'}{\{\varphi'\}\, P\, \{\psi'\}} \quad \text{(cons)}$$

Assume $\{\varphi\}\, P\, \{\psi\}$ is valid and $\varphi' \to \varphi$ and $\psi \to \psi'$. Need to show that $\{\varphi'\}\, P\, \{\psi'\}$ is valid.

Observe: If $\varphi' \to \varphi$ then $\langle \varphi' \rangle \subseteq \langle \varphi \rangle$

$$\begin{aligned} [\![P]\!](\langle \varphi' \rangle) &\subseteq [\![P]\!](\langle \varphi \rangle) && \text{(see Lemma 1(a))} \\ &\subseteq \langle \psi \rangle && \text{(IH)} \\ &\subseteq \langle \psi' \rangle \end{aligned}$$