

Preconditions

Using Z

Woodcock & Davies

Analysis

We may wish to show that

- the requirements are consistent: the constraint part of the state schema is satisfiable
- each operation is applied within its domain: the effect of the operation is properly defined whenever it is used

In each case, it is enough to consider **preconditions**.

Preconditions

The precondition of an operation is that constraint which is necessary and sufficient for the operation to be defined: that is, for an after state to exist.

The nature of the after state does not concern us; neither do the outputs of the operation. The precondition will take the form of a constraint upon the combination of the before state and the inputs.

Precondition schemas

A precondition schema is a schema that characterises the combinations of before states and inputs for which the effect of an operation is defined.

<i>State</i>
<i>inputs</i>
...

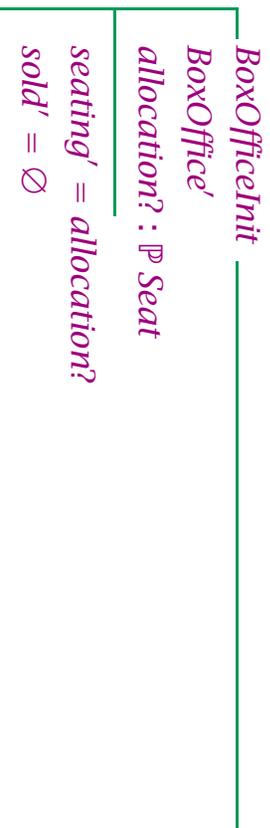
$$\begin{aligned}
 &= [\text{BoxOffice}; s? : \text{Seat}; && \text{[one-point rule, twice]} \\
 &\quad c? : \text{Customer} \mid \\
 &\quad \text{dom}(\text{sold} \cup \{s? \mapsto c?\}) \subseteq \text{seating} \wedge \\
 &\quad s? \in \text{seating} \setminus \text{dom sold}] \\
 &= [\text{BoxOffice}; s? : \text{Seat}; && \text{[property of 'dom']} \\
 &\quad c? : \text{Customer} \mid \\
 &\quad s? \in \text{seating} \setminus \text{dom sold}]
 \end{aligned}$$

Initialisation

The operation of initialisation is a special case; there is no before state, although there may be inputs:

The statement that initialisation is possible is sometimes called the [initialisation theorem](#):

$\exists \text{State}' \bullet \text{StateInit} \setminus \text{outputs}$

Example

$\exists \text{BoxOffice}' \bullet \text{BoxOfficeInit}$
 $\Leftrightarrow \exists \text{BoxOffice}' \bullet$ [definition of *BoxOfficeInit*]
 $[\text{BoxOffice}' ; \text{allocation?} : \mathbb{P} \text{ Seat} \mid$
 $\text{seating}' = \text{allocation?} \wedge$
 $\text{sold}' = \emptyset]$
 $\Leftrightarrow [\text{allocation?} : \mathbb{P} \text{ Seat} \mid$ [schema quantification]
 $\exists \text{BoxOffice}' \bullet$
 $\text{seating}' = \text{allocation?} \wedge$
 $\text{sold}' = \emptyset]$

\Leftrightarrow [allocation? : \mathbb{P} Seat | [definition of *BoxOffice'*]
 \exists seating' : \mathbb{P} Seat •
 \exists sold' : Seat \leftrightarrow Customer •
 $\text{dom sold}' \subseteq \text{seating}' \wedge$
 $\text{seating}' = \text{allocation?} \wedge$
 $\text{sold}' = \emptyset$]

\Leftrightarrow [allocation? : \mathbb{P} Seat | [one-point rule, twice]
 $\text{allocation?} \in \mathbb{P}$ Seat \wedge
 $\emptyset \in \text{Seat} \leftrightarrow \text{Customer} \wedge$
 $\emptyset \subseteq \text{allocation?}$]
 \Leftrightarrow [allocation? : \mathbb{P} Seat] [properties of sets]

Explicit vs implicit preconditions

There is a minor advantage to be gained by concentrating upon what an operation is supposed to do, and calculating its precondition later.

Even where an explicit precondition has been included, the calculation provides for a degree of cross-checking.

Example

$capacity : \mathbb{N}$
$capacity > 0$

<i>CarPark</i>
$count : \mathbb{N}$
$count \leq capacity$

$Enter_0$
$\Delta CarPark$
$count' = count + 1$
$Exit_0$
$\Delta CarPark$
$count' = count - 1$

$$\begin{aligned}
 & \text{pre } Exit_0 \\
 &= \exists CarPark' \bullet Exit_0 \quad \text{[definition of } Exit_0] \\
 &= [CarPark \mid \quad \text{[definition of } CarPark']] \\
 & \quad \exists count' : \mathbb{N} \mid \\
 & \quad \quad count' \leq capacity \bullet \\
 & \quad \quad count' = count - 1] \\
 &= [CarPark \mid count - 1 \in \mathbb{N}] \quad \text{[one-point rule]}
 \end{aligned}$$

Informed design:

<i>ExtraCar</i>
$\exists \text{CarPark}$
<i>r!</i> : Report
<i>count</i> = 0
<i>r!</i> = <i>extra_car</i>

$\text{Exit} \hat{=} \text{Exit}_0 \vee \text{ExtraCar}$

A recipe for preconditions

Suppose that we wish to calculate the precondition of

<i>Operation</i>
<i>Declaration</i>
<i>Predicate</i>

Step One

Take the various clauses of *Declaration* and assemble them to make three new declarations:

- *Before* introducing only inputs and before components (unprimed state components);
- *After* introducing only outputs and after components (primed state components);
- *Mixed* consisting of the remaining clauses.

Step Two

If *Mixed* is not an empty declaration, expand every schema mentioned in *Mixed*; add all input and before components to *Before*; add all output and after components to *After*.

As there may be several levels of schema inclusion, repeat this step until there are no clauses left in *Mixed*.

Step Three

The precondition of *Operation* is then

<i>Before</i>
\exists <i>After</i> •
<i>Predicate</i>

Question

Given the following schema definitions,

<i>S</i>
$a : \mathbb{N}$
$b : \mathbb{N}$
$a \neq b$

<i>T</i>
<i>S</i>
$c : \mathbb{N}$
$b \neq c$

what is the precondition of the following operation?

Increment

ΔT

$in? : \mathbb{N}$

$out! : \mathbb{N}$

$a' = a + in?$

$b' = b$

$c' = c$

$out! = c$

Simplification

Suppose that we wished to simplify the precondition schema

Before

\exists *After* •

Predicate

Step Four

Expand any schemas in *After* that contain equations identifying outputs or after components.

Step Five

Expand any schemas in *After* that refer to outputs or after components for which we already have equations.

Step Six

If *Predicate* contains an equation identifying a component declared in *After*, then use the one-point rule to eliminate that component.

Repeat this step as many times as possible.

Step Seven

If *After*₁ and *Predicate*₁ are what remains of *After* and *Predicate*, then the precondition is now

<i>Before</i>
$\exists \textit{After}_1 \bullet$
<i>Predicate</i> ₁

Question

How may we simplify the predicate part of *pre Increment*?

$\exists out! : \mathbb{N}; T' \bullet$

$$a' = a + in? \wedge$$

$$b' = b \wedge$$

$$c' = c \wedge$$

$$out! = c$$

Disjunction

If

$$Op \hat{=} Op_1 \vee Op_2$$

then

$$\text{pre } Op = \text{pre } Op_1 \vee \text{pre } Op_2$$

Conjunction

In general, if

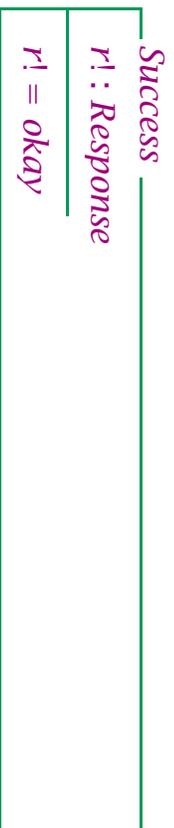
$$Op \hat{=} Op_1 \wedge Op_2$$

then

$$\text{pre } Op \neq \text{pre } Op_1 \wedge \text{pre } Op_2$$

However, it may be that the declarations introduce disjoint sets of variables...

Example



$$\text{pre } (\text{Purchase}_0 \wedge \text{Success}) = \text{pre } \text{Purchase}_0$$

Free promotion

$$\begin{aligned} \exists \text{Local}' \bullet & \quad \Leftrightarrow \forall \text{Local}' \bullet \\ \exists \text{Global}' \bullet \text{Promote} & \quad \exists \text{Global}' \bullet \text{Promote} \end{aligned}$$

A useful result

$$\begin{aligned} \text{pre } \text{GOP} & \quad \Leftrightarrow \exists \text{Global}' \bullet && \text{[definition of 'pre']} \\ & \quad \text{GOP} && \\ & \quad \Leftrightarrow \exists \text{Global}' \bullet && \text{[definition of GOP]} \\ & \quad \exists \Delta \text{Local} \bullet \text{Promote} \wedge \text{LOP} && \\ & \quad \Leftrightarrow \exists \Delta \text{Local} \bullet && \text{[property of } \exists \text{]} \\ & \quad \exists \text{Global}' \bullet \text{Promote} \wedge \text{LOP} && \end{aligned}$$

$$\begin{aligned}
 &\Leftrightarrow \exists \textit{Local} \bullet && \text{[definition of } \Delta \text{]} \\
 &\quad \exists \textit{Local}' \bullet \exists \textit{Global}' \bullet \textit{Promote} \wedge \textit{LOp} \\
 &\Leftrightarrow \exists \textit{Local} \bullet && \text{[lemma]} \\
 &\quad (\exists \textit{Local}' \bullet \exists \textit{Global}' \bullet \textit{Promote}) \wedge (\exists \textit{Local}' \bullet \textit{LOp}) \\
 &\Leftrightarrow \exists \textit{Local} \bullet && \text{[definition of 'pre', twice]} \\
 &\quad \textit{pre Promote} \wedge \textit{pre LOp}
 \end{aligned}$$

Lemma

The equivalence labelled 'lemma' is easily proved in the forward direction. A proof in the other direction (\Leftarrow) requires the free promotion property.

We abbreviate *Local'*, *Global'*, and *Promote* to *L'*, *G'*, and *P*, respectively.

$$\begin{array}{c}
 \frac{\exists L' \bullet \exists G' \bullet P}{\forall L' \bullet \exists G' \bullet P} \text{ [free promotion]} \\
 \frac{[\exists L' \in L]^{[1]}}{\frac{\frac{\frac{\exists G' \bullet P}{\exists G' \bullet P \wedge LOP} \text{ [V-elim]}}{[\exists L' \in L]^{[1]}} \text{ [LOp]}^{[1]}}{[\exists L' \bullet \exists G' \bullet P \wedge LOP]} \text{ [G' not free in LOP]}} \text{ [L-elim]} \\
 \frac{[\exists L' \bullet \exists G' \bullet P \wedge LOP]}{\exists L' \bullet \exists G' \bullet P \wedge LOP} \text{ [L-intro]} \\
 \frac{\exists L' \bullet LOP}{\exists L' \bullet \exists G' \bullet P \wedge LOP} \text{ [L-elim]}
 \end{array}$$

Example

$$\begin{array}{l}
 \text{AssignIndex} \hat{=} \exists \Delta \text{Data} \bullet \text{AssignData} \wedge \text{Promote} \\
 \text{pre AssignIndex} = \\
 \exists \text{Data} \bullet \text{pre AssignData} \wedge \text{pre Promote}
 \end{array}$$

Question

What is the precondition of *AssignData*?

AssignData
 $\Delta Data$
new? : *Value*
value' = *new?*

Question

What is the precondition of *Promote*?

Promote
 $\Delta Array$
 $\Delta Data$
index? : \mathbb{N}
index? \in dom *array*
 $\{index?\} \triangleleft array = \{index?\} \triangleleft array'$
array *index?* = $\theta Data$
array' *index?* = $\theta Data'$

Question

What is the precondition of

$\exists \Delta Data \bullet Promote \wedge AssignData$?

Results

It is often useful to tabulate the results of our analysis; against each operation, we record the predicate that characterises its precondition.

We should check that the predicates are a correct reflection of our expectations: that each operation schema is exactly as prescriptive as it should be.

Example

<i>IritBoxOffice</i>	<i>true</i>
<i>Purchase₀</i>	$s? \in \text{seating} \setminus \text{dom sold}$
<i>NotAvailable</i>	$s? \notin \text{seating} \setminus \text{dom sold}$
<i>Purchase</i>	<i>true</i>
<i>Return₀</i>	$s? \mapsto c? \in \text{sold}$
<i>NotPossible</i>	$s? \mapsto c? \notin \text{sold}$
<i>Return</i>	<i>true</i>

Summary

- preconditions
- pre *Schema*
- initialisation
- calculation and simplification
- disjunction
- promotion