Promotion

Using Z

Woodcock & Davies

Promotion

Promotion is a structuring technique that may be used whenever the state of a system contains multiple, indexed instances of the same component.

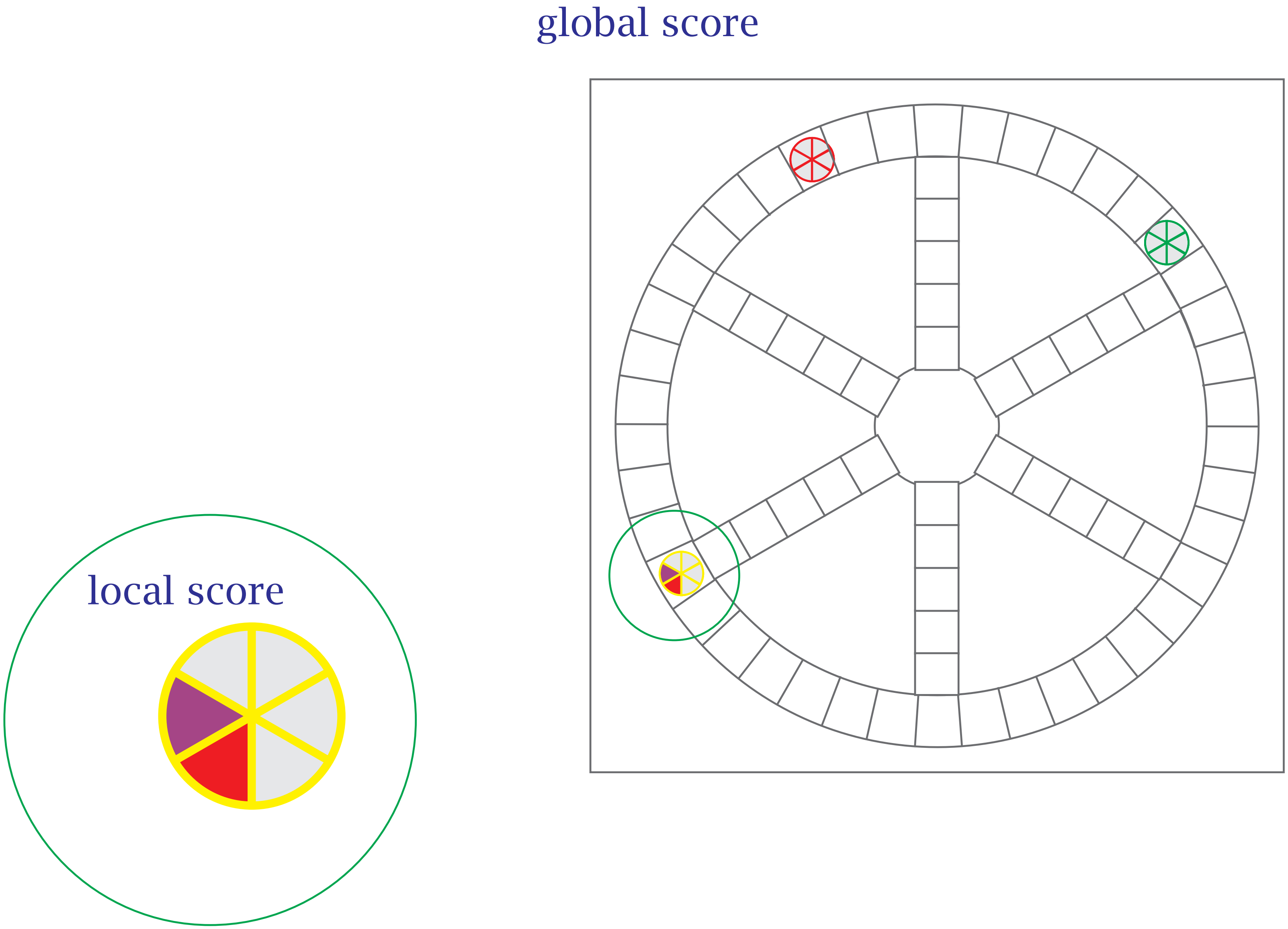
It is most useful when several operations are possible upon the component, and their effect is independent of the index: that is, their effect is the same for each instance.

Example

The state of a game of trivial pursuit might be described using the following pair of schemas:

$$\begin{array}{l}\text{\_\_ } \mathit{LocalScore} \text{ \_\_\_\_\_\_\_\_\_\_\_\_} \\ s : \mathbb{P}\, \mathit{Colour} \\ \text{\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_}\end{array}$$

$$\begin{array}{l}\text{\_\_ } \mathit{GlobalScore} \text{ \_\_\_\_\_\_\_\_\_\_\_\_} \\ \mathit{score} : \mathit{Players} \nrightarrow \mathit{LocalScore} \\ \text{\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_}\end{array}$$


global score
local score

The change in state associated with a single player answering a scoring question correctly could be described by:

$$
\begin{array}{|l}
\hline
\textit{AnswerGlobal} \\
\Delta \textit{GlobalScore} \\
p? : \textit{Player} \\
c? : \textit{Colour} \\
\hline
p? \in \operatorname{dom} \textit{score} \\
\{p?\} \ntriangleleft \textit{score}' = \{p?\} \ntriangleleft \textit{score} \\
(\textit{score}'\ p?).s = (\textit{score}\ p?).s \cup \{c?\} \\
\hline
\end{array}
$$

The change in local state—in the individual player's score—could be described by

$$\begin{array}{|l}
\hline
\textit{AnswerLocal} \\
\Delta \textit{LocalScore} \\
c? : \textit{Colour} \\
\hline
s' = s \cup \{c?\} \\
\hline
\end{array}$$

The following mixed operation identifies a particular local score; one of the copies indexed by *score*:

$$
\begin{array}{|l}
\multicolumn{1}{l}{\textit{Mixed}} \\
\hline
\Delta GlobalScore \\
\Delta LocalScore \\
p? : Player \\
\hline
p? \in \operatorname{dom} score \\
\theta LocalScore = score\ p? \\
score' = score \oplus \{p? \mapsto \theta LocalScore'\} \\
\hline
\end{array}
$$

The following operation describes the change in global state that accompanies such a correct answer:

$$AnswerLocal \land Mixed$$

Removing the extra names from the declaration, we obtain a global operation schema:

$$\exists\, \Delta LocalScore \bullet AnswerLocal \land Mixed$$

Promotion schemas

If *Local* describes a copy of the local state and *Global* describes a copy of the global state, then a promotion schema *Promote* will contain decorated and undecorated copies of both *Local* and *Global*.

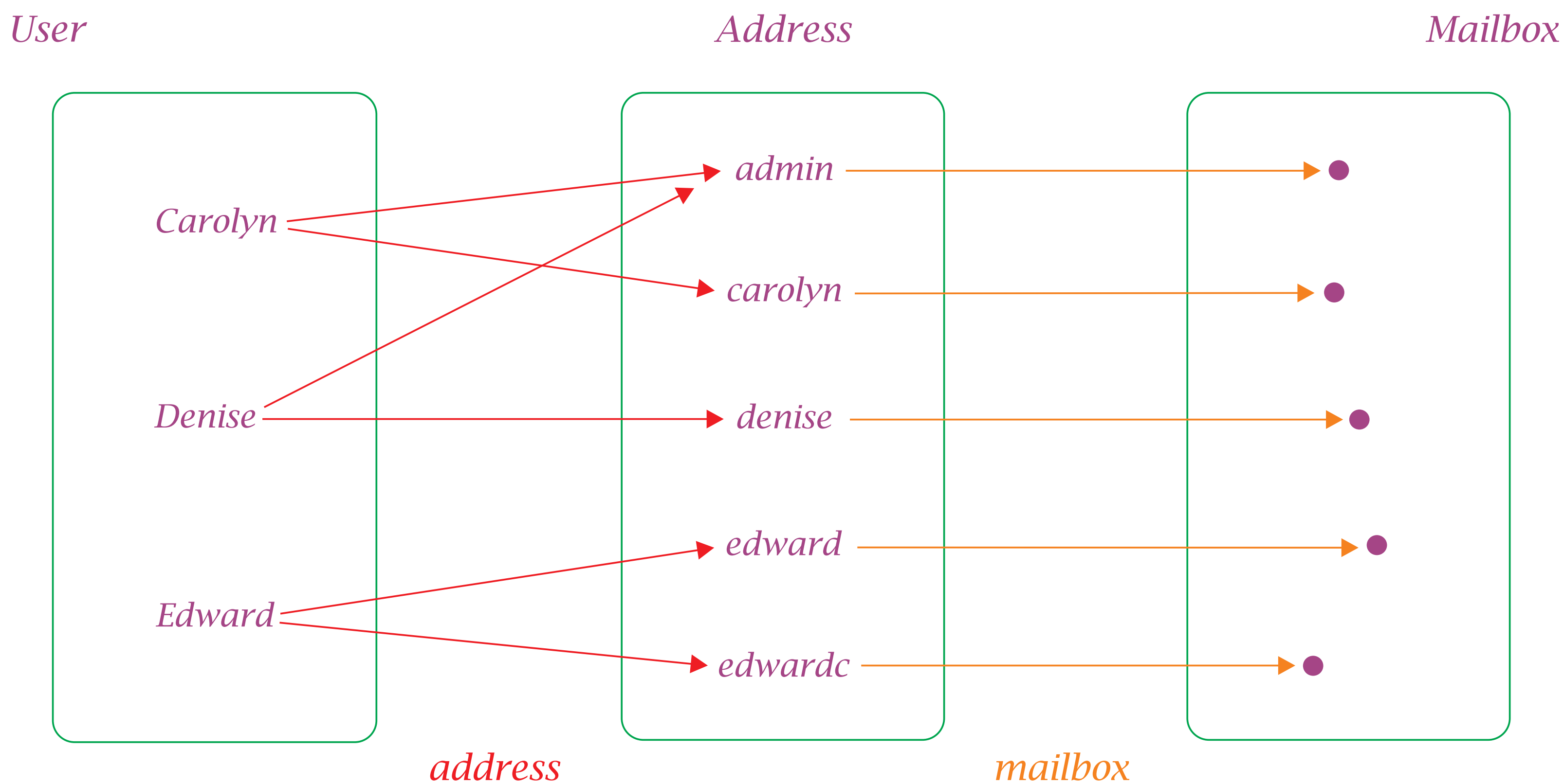
If *LocalOperation* contains decorated and undecorated copies of *Local*, then we may promote *LocalOperation* to the global operation

$$\exists \Delta Local \bullet Promote \wedge LocalOperation$$

Example

$$
\begin{array}{|l}
\hline
\textit{MailSystem} \\
\hline
address : Person \leftrightarrow Address \\
mailbox : Address \pfun MailBox \\
\hline
\end{array}
$$

$$
\begin{array}{|l}
\hline
\textit{MailBox} \\
\hline
mail : \mathrm{seq}\ Message \\
new\_mail, last\_read : TimeStamp \\
\hline
\end{array}
$$


User
Address
Mailbox
Carolyn
Denise
Edward
admin
carolyn
denise
edward
edwardc
address
mailbox

Each mailbox is a binding:

$$\langle\!| \; mail \leadsto \langle m_1, m_2, m_3 \rangle,$$
$$new\_mail \leadsto \text{Tue 14 Feb, 11.00 a.m.},$$
$$last\_read \leadsto \text{Sun 12 Feb, 12.30 p.m.} \; |\!\rangle$$

A local operation:

$$
\begin{array}{l}
\textit{ReceiveBox} \\
\hline
\Delta \textit{MailBox} \\
m? : \textit{Message} \\
t? : \textit{TimeStamp} \\
\hline
\textit{mail}' = \textit{mail} \frown \langle m? \rangle \\
\textit{new\_mail}' = t? \\
\textit{last\_read}' = \textit{last\_read} \\
\hline
\end{array}
$$

A promotion schema:

$$
\begin{array}{|l}
\multicolumn{1}{l}{\textit{Promote}} \\
\hline
\Delta MailSystem \\
\Delta MailBox \\
u? : User \\
a! : Address \\
\hline
u? \mapsto a! \in address \\
address' = address \\
a! \in \operatorname{dom} mailbox \\
\theta MailBox = mailbox\ a! \\
mailbox' = mailbox \oplus \{a! \mapsto \theta MailBox'\} \\
\hline
\end{array}
$$

A global operation:

$$\exists\, \Delta \mathit{MailBox} \bullet \mathit{ReceiveBox} \wedge \mathit{Promote}$$

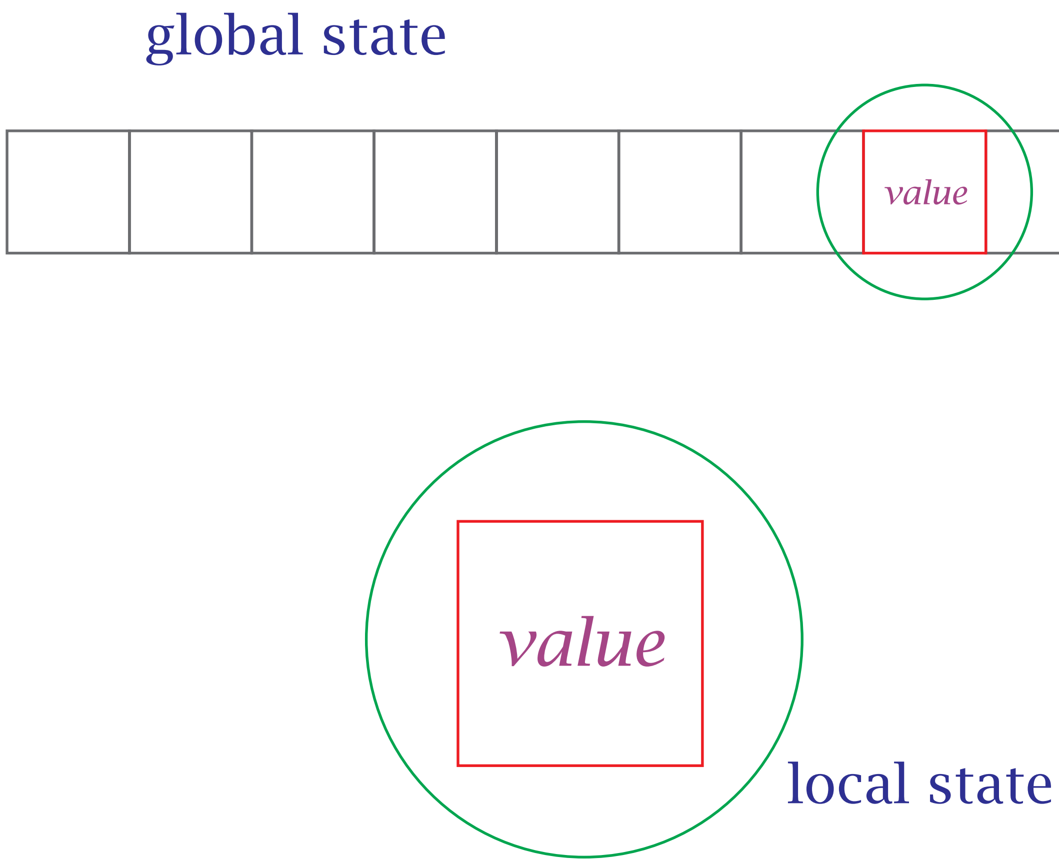
A global operation (without promotion):

$$
\begin{array}{|l}
\hline
\Delta MailSystem \\
u? : User; \; m? : Message \\
t? : TimeStamp; \; a! : Address \\
\hline
u? \mapsto a! \in address \\
address' = address \\
a! \in \operatorname{dom} mailbox \\
\{a?\} \ntriangleleft mailbox' = \{a?\} \ntriangleleft mailbox \\
(mailbox' \; a!).mail = (mailbox \; a!).mail \frown \langle m? \rangle \\
(mailbox' \; a!).new\_mail = t? \\
(mailbox' \; a!).last\_read = (mailbox \; a!).last\_read \\
\hline
\end{array}
$$

Example

$$
\begin{array}{|l}
\multicolumn{1}{l}{\textit{Array}} \\
\hline
array : \mathrm{seq}\ Data \\
\hline
\end{array}
$$

$$
\begin{array}{|l}
\multicolumn{1}{l}{\textit{Data}} \\
\hline
value : Value \\
\hline
\end{array}
$$


global state
value
value
local state

A local operation:

$$
\begin{array}{|l}
\multicolumn{1}{l}{\textit{AssignData}} \\
\hline
\Delta Data \\
new? : Value \\
\hline
value' = new? \\
\hline
\end{array}
$$

Question

How should we complete the following definition?

$$
\begin{array}{|l}
\textit{Promote} \\
\hline
\Delta \textit{Array} \\
\Delta \textit{Data} \\
\textit{index}? : \mathbb{N} \\
\hline
\\
\hline
\end{array}
$$

Question

How can we obtain a global operation from *AssignData* and *Promote*?

Question

What about the following local operation schema?

$$
\begin{array}{|l}
\hline
\textit{ReadData} \\
\Xi \textit{Data} \\
\textit{out}! : \textit{Value} \\
\hline
\textit{out}! = \textit{value} \\
\hline
\end{array}
$$

Free promotion

A promotion is said to be free if and only if

$$(\exists \mathit{Local}' \bullet \exists \mathit{Global}' \bullet \mathit{Promote})$$
$$\Rightarrow$$
$$(\forall \mathit{Local}' \bullet \exists \mathit{Global}' \bullet \mathit{Promote})$$

Example

We can show that

$$
\begin{array}{l}
(\exists\, Data' \bullet \exists\, Array' \bullet Promote) \\
\quad \Rightarrow \\
\qquad (\forall\, Data' \bullet \exists\, Array' \bullet Promote)
\end{array}
$$

$$
\begin{aligned}
&\exists\, Array' \bullet Promote \\
&\quad \Leftrightarrow [\, Array;\ \Delta Data;\ index? : \mathbb{N} \mid \\
&\qquad\quad \exists\, array' : \mathrm{seq}\, Data \bullet \\
&\qquad\qquad index? \in \mathrm{dom}\, array \land \\
&\qquad\qquad array\ index? = \theta Data \land \\
&\qquad\qquad array' = array \oplus \{ index? \mapsto \theta Data' \} \,]
\end{aligned}
$$

$$
\begin{aligned}
\Leftrightarrow [&Array;\ \Delta Data;\ index? : \mathbb{N} \mid \\
&\quad index? \in \operatorname{dom} array \land \\
&\quad array\ index? = \theta Data \land \\
&\quad array \oplus \{index? \mapsto \theta Data'\} \in \operatorname{seq} Data]
\end{aligned}
$$

$$
\begin{aligned}
\Leftrightarrow [\,& Array;\ \Delta Data;\ index? : \mathbb{N} \mid \\
& \quad index? \in \operatorname{dom} array \land \\
& \quad array\ index? = \theta Data \land \\
& \quad \theta Data' \in Data]
\end{aligned}
$$

Method

To decide whether a given promotion is free (or not):

- expand $\exists \mathit{Global}' \bullet \mathit{Promote}$
- if necessary, rewrite the constraint to obtain an equation for each decorated component of the global state
- use the one-point rule to eliminate each of these components
- apply set theory and logic

Constrained promotion

Any promotion which is not free is said to be constrained.

This may be the case if the promotion schema—or the global state invariant—refers to some variable within the local state.

Example

$$
\begin{array}{|l}
\hline
\multicolumn{1}{l}{\mathit{Item}} \\
\mathit{pri} : \mathbb{N} \\
d : \mathit{Data} \\
\hline
\end{array}
$$

$$
\begin{array}{|l}
\hline
\multicolumn{1}{l}{\mathit{Stack}} \\
\mathit{stack} : \mathrm{seq}\ \mathit{Item} \\
\hline
\forall\, i, j : \mathrm{dom}\, \mathit{stack} \mid i < j \bullet \\
\qquad (\mathit{stack}\ i).\mathit{pri} \geq (\mathit{stack}\ j).\mathit{pri} \\
\hline
\end{array}
$$

$$
\begin{array}{|l}
\hline
\textit{Promote} \\
\Delta \textit{Stack} \\
\Delta \textit{Item} \\
\hline
\textit{stack} \neq \langle\, \rangle \\
\theta \textit{Item} = \textit{head stack} \\
\textit{stack}' = \langle \theta \textit{Item}' \rangle \frown \textit{tail stack} \\
\hline
\end{array}
$$

$$
\begin{array}{l}
\exists\, Stack' \bullet Promote \\
\quad \Leftrightarrow [\, Stack;\ \Delta Item \mid \\
\qquad\qquad \exists\, stack' : \mathrm{seq}\, Item \bullet \\
\qquad\qquad\quad stack \neq \langle\rangle \wedge \\
\qquad\qquad\quad \theta Item = head\ stack \wedge \\
\qquad\qquad\quad stack' = \langle \theta Item' \rangle \frown tail\ stack \wedge \\
\qquad\qquad\quad \forall\, i, j : \mathrm{dom}\, stack' \mid i < j \bullet \\
\qquad\qquad\qquad (stack'\ i).pri \geq (stack'\ j).pri \,]
\end{array}
$$

$$
\begin{array}{l}
\Leftrightarrow [\, Stack;\ \Delta Item \mid \\
\qquad \exists\, stack' : \mathrm{seq}\, Item \bullet \\
\qquad\quad stack \neq \langle\rangle \land \\
\qquad\quad \theta Item = head\ stack \land \\
\qquad\quad \forall\, i, j : \mathrm{dom}(\langle \theta Item' \rangle \frown tail\ stack) \mid i < j \bullet \\
\qquad\qquad ((\langle \theta Item' \rangle \frown tail\ stack)\ i).pri \\
\qquad\qquad \geq \\
\qquad\qquad ((\langle \theta Item' \rangle \frown tail\ stack)\ j).pri \,]
\end{array}
$$

$$
\begin{aligned}
\Leftrightarrow [\, & Stack;\ \Delta Item \mid \\
& \quad \exists\, stack' : \mathrm{seq}\, Item \bullet \\
& \qquad stack \neq \langle\rangle \land \\
& \qquad \theta Item = head\ stack \land \\
& \qquad \forall\, i, j : \mathrm{dom}\, stack \mid i < j \bullet \\
& \qquad\quad ((\langle \theta Item' \rangle \frown tail\ stack)\ i).pri \\
& \qquad\quad \geq \\
& \qquad\quad ((\langle \theta Item' \rangle \frown tail\ stack)\ j).pri\ ]
\end{aligned}
$$

$$
\begin{aligned}
\Leftrightarrow [\,& Stack;\ \Delta Item \mid \\
&\quad \exists\, stack' : \mathrm{seq}\, Item \bullet \\
&\qquad stack \neq \langle\rangle \land \\
&\qquad \theta Item = head\ stack \land \\
&\qquad \forall\, i, j : \mathrm{dom}\, tail\ stack \mid i < j \bullet \\
&\qquad\quad (tail\ stack)\ i.pri \geq (tail\ stack)\ j.pri \land \\
&\qquad \forall\, j : \mathrm{dom}\, tail\ stack \bullet \\
&\qquad\quad \theta Item'.pri \geq (tail\ stack)\ j.pri\,]
\end{aligned}
$$

Multiple promotion

Even if a global operation involves two or more indexed components, it is still possible to use promotion.

We express the global change in state as a sequential composition: the local states are updated one after the other.

Each component of the sequential composition can then be defined using promotion and renaming.

Example

Suppose that

- *Global* involves indexed instances of *Local*
- *LOpA* and *LOpB* are operations on *Local*
- the promotion of a single change is described by the schema *Promote*
- the indexing variable in *Promote* is $i?$

If we promote each of the local operations:

$$GOpA \mathrel{\widehat=} \exists \Delta Local \bullet LOpA \land Promote$$

$$GOpB \mathrel{\widehat=} \exists \Delta Local \bullet LOpB \land Promote$$

then the operation

$$GOp \mathrel{\widehat=} GOpA[a?/i?] \mathbin{;} GOpB[b?/i?]$$

describes an operation in which only components $a?$ and $b?$ are changed. The effect upon these components is described by $LOpA$ and $LOpB$, respectively.

Question

In the composition $GOpA[a?/i?] \mathbin{;} GOpB[b?/i?]$, does the intermediate state need to satisfy the global state invariant?

Summary

- indexed instances of the same component
- promotion schemas
- free promotion
- constrained promotion
- multiple promotion