A Problematic Program

John C. Reynolds
Carnegie Mellon University
and
Microsoft Research Cambridge

5 February 2008 — Dagstuhl
(Joint work with Josh Berdine)

(Research partially supported by National Science Foundation Grant CCF-054102l.)

A Problematic Program

It is widely believed that two concurrent processes that both mutate the same location may cause a potential race condition unless all mutations occur within critical regions associated with the same resource.

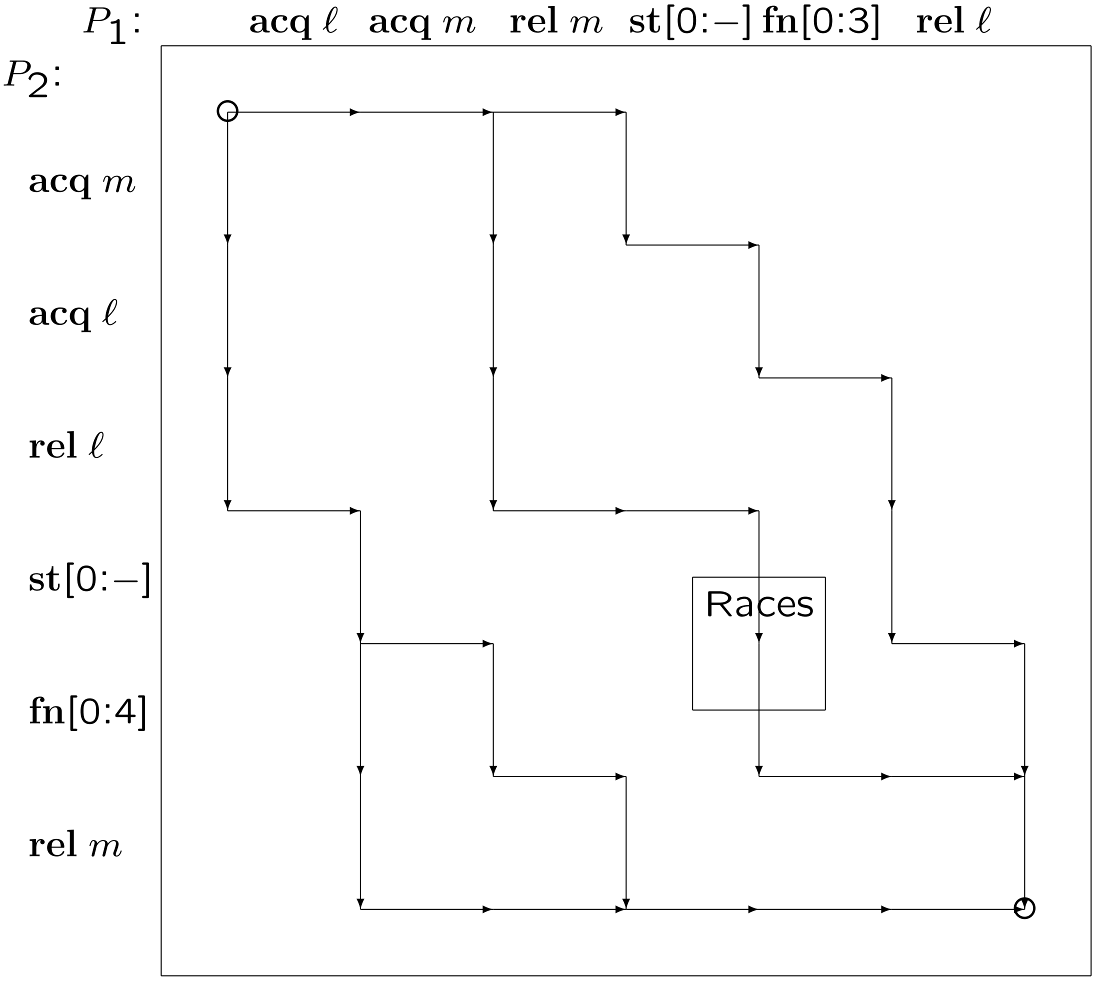
In fact, the following program cannot cause a race condition:

$$\begin{array}{l}\textbf{resource}\ \ell\ \textbf{in}\ \textbf{resource}\ m\ \textbf{in}\\ \qquad (\textbf{with}\ \ell\ \textbf{do}\ ((\textbf{with}\ m\ \textbf{do}\ \textbf{skip}); [0] := 3))\\ \qquad \parallel (\textbf{with}\ m\ \textbf{do}\ ((\textbf{with}\ \ell\ \textbf{do}\ \textbf{skip}); [0] := 4)).\end{array}$$

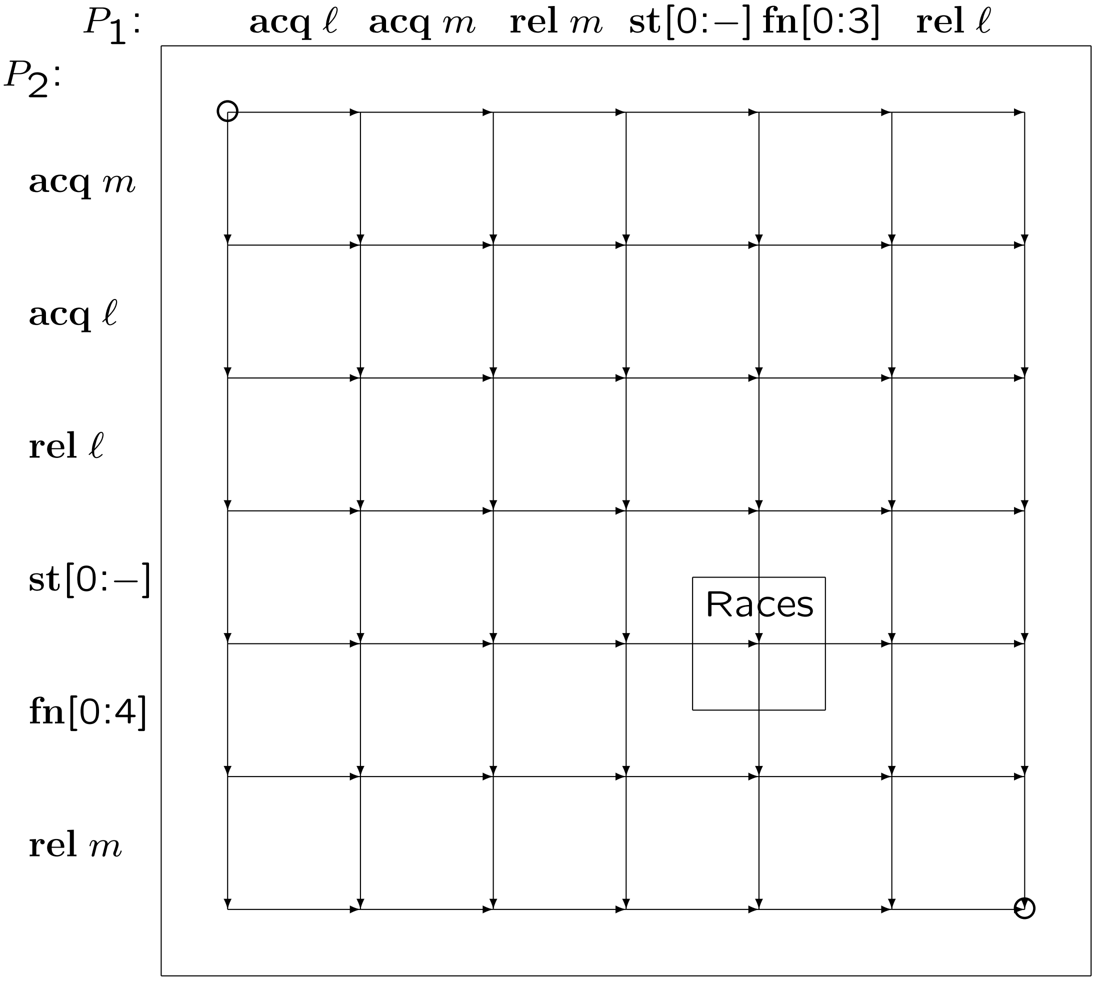
(although it can deadlock).

Interleavings as Paths

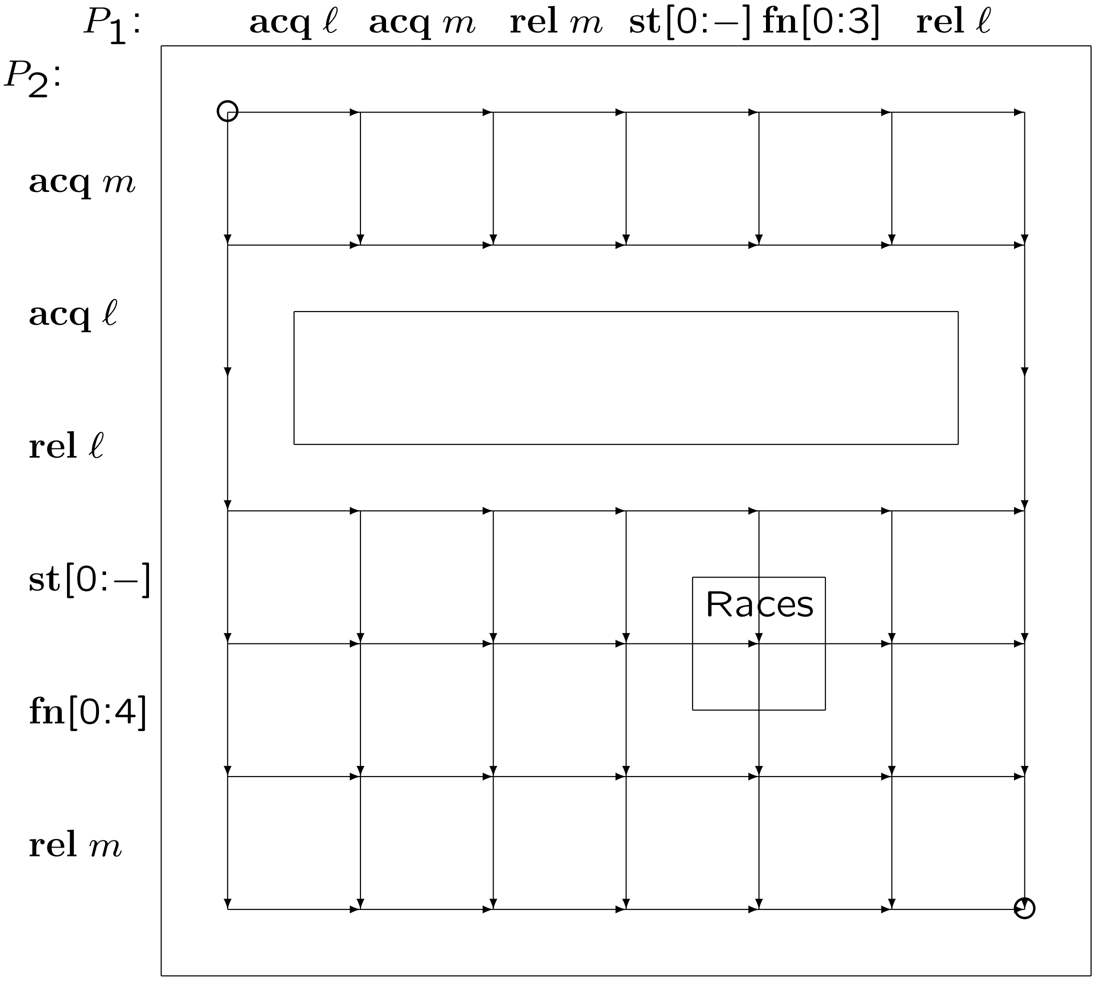
$$(\textbf{with}\ \ell\ \textbf{do}\ ((\textbf{with}\ m\ \textbf{do skip}); [0] := 3))$$
$$\parallel (\textbf{with}\ m\ \textbf{do}\ ((\textbf{with}\ \ell\ \textbf{do skip}); [0] := 4)).$$



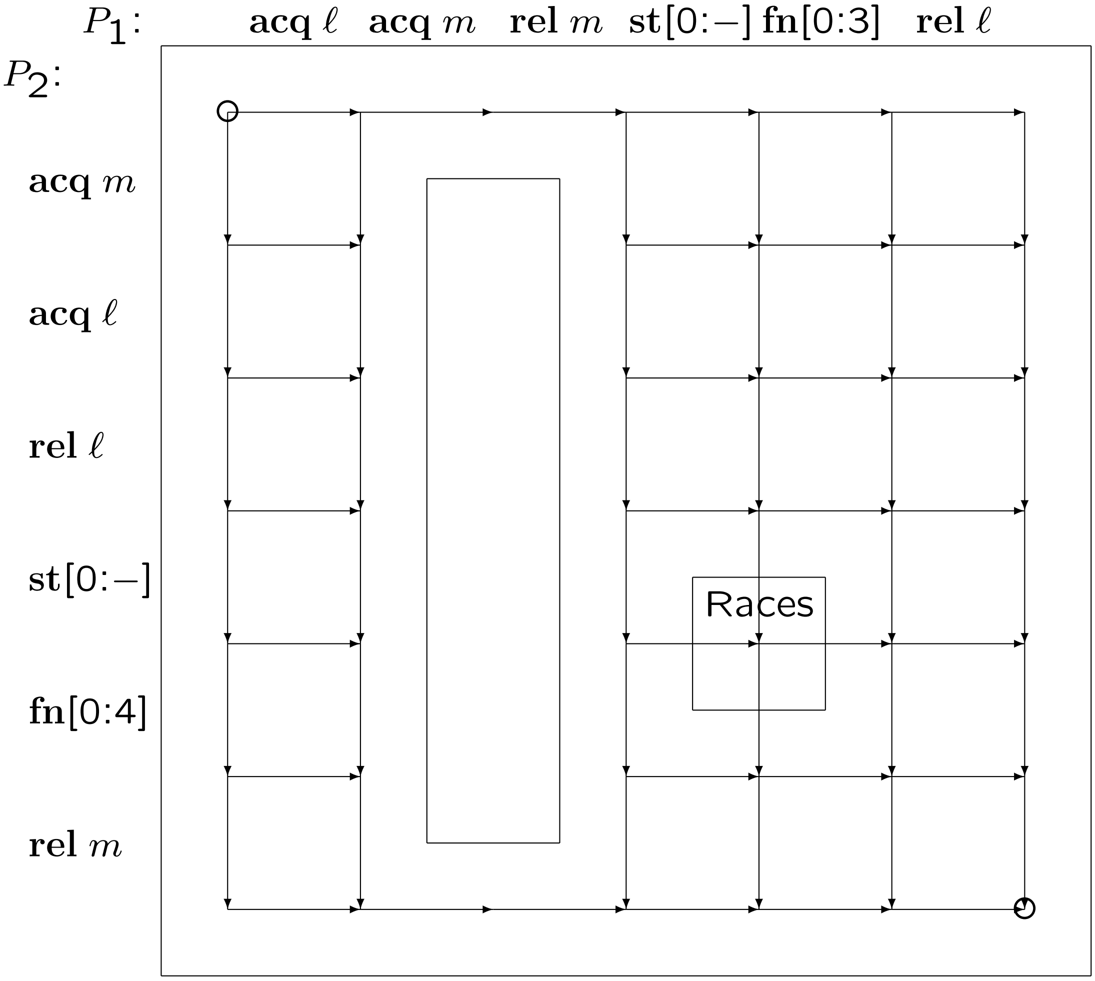
All Possible Interleavings



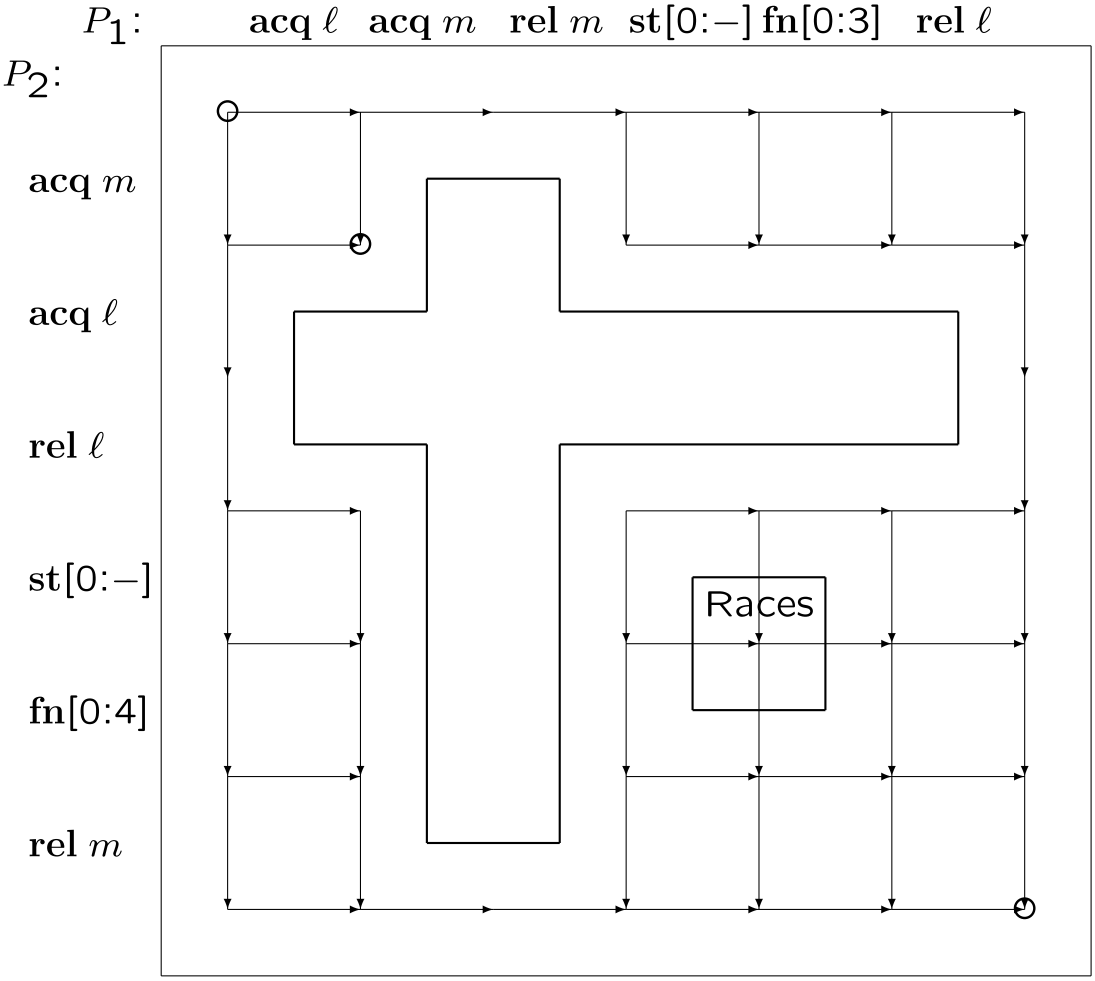
Exclusion by ℓ



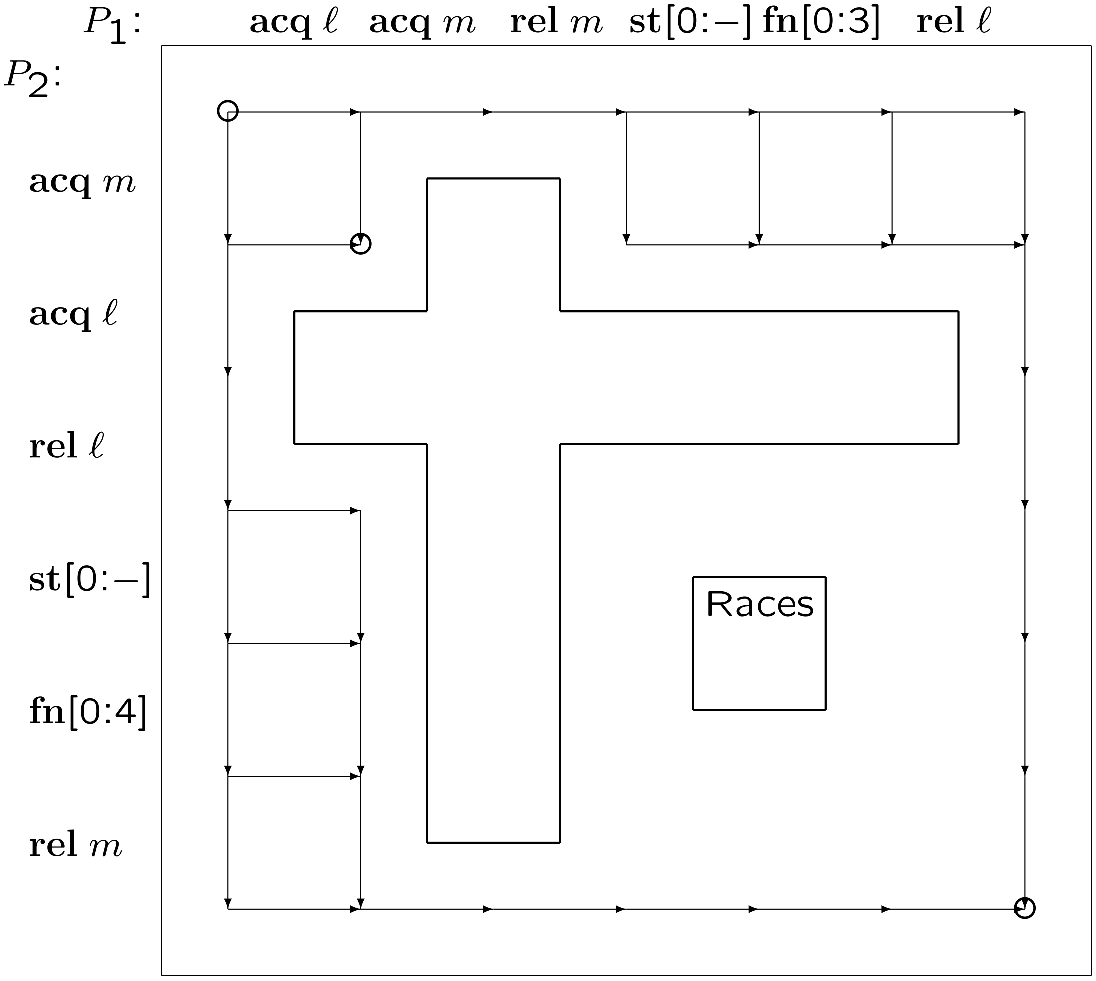
Exclusion by m



The Combined Exclusion



Excluding Unreachable Nodes



How to Prove it: Use an Auxiliary Variable

```
$\{0 \mapsto -\}$
$\textbf{resource}\ \ell\ \textbf{in resource}\ m\ \textbf{in}$
    $(\textbf{with}\ \ell\ \textbf{do}\ ((\textbf{with}\ m\ \textbf{do}\ p := 0); [0] := 3))$
    $\parallel (\textbf{with}\ m\ \textbf{do}\ ((\textbf{with}\ \ell\ \textbf{do}\ p := 1); [0] := 4))$
$\{0 \mapsto -\}$
```

The Resource Invariants

Let

$$\begin{aligned} R_\ell &= \mathbf{if}\ p = 0\ \mathbf{then}\ 0 \mapsto -\ \mathbf{else}\ \mathbf{emp} \\ R_m &= \mathbf{if}\ p = 0\ \mathbf{then}\ \mathbf{emp}\ \mathbf{else}\ 0 \mapsto - \end{aligned}$$

Then

$$\begin{aligned} & R_\ell * R_m \\ & \quad \text{iff } \mathbf{if}\ p = 0\ \mathbf{then}\ 0 \mapsto - * \mathbf{emp}\ \mathbf{else}\ \mathbf{emp} * 0 \mapsto - \\ & \quad \text{iff } \mathbf{if}\ p = 0\ \mathbf{then}\ 0 \mapsto -\ \mathbf{else}\ 0 \mapsto - \\ & \quad \text{iff } 0 \mapsto - \end{aligned}$$

and

$$\begin{aligned} R_\ell * (p = 0 \wedge \mathbf{emp}) &\text{ iff } 0 \mapsto - * (p = 0 \wedge \mathbf{emp}) \\ R_m * (p \neq 0 \wedge \mathbf{emp}) &\text{ iff } 0 \mapsto - * (p \neq 0 \wedge \mathbf{emp}) \end{aligned}$$

Thus

$\{R_\ell * R_m\}$

$\{0 \mapsto -\}$

$p := 0$

$\{0 \mapsto - * (p = 0 \wedge \mathbf{emp})\}$

$\{R_\ell * R_m * (p = 0 \wedge \mathbf{emp})\}$

$\{R_\ell\}$

$\mathbf{with}\ m\ \mathbf{do}\ p := 0;$

$\{R_\ell * (p = 0 \wedge \mathbf{emp})\}$

$\{0 \mapsto - * (p = 0 \wedge \mathbf{emp})\}$

$[0] := 3$

$\{0 \mapsto - * (p = 0 \wedge \mathbf{emp})\}$

$\{R_\ell * (p = 0 \wedge \mathbf{emp})\}$

$\{R_\ell\}$

$$\begin{array}{l}\{\mathbf{emp}\}\\ \mathbf{with}\ \ell\ \mathbf{do}\ ((\mathbf{with}\ m\ \mathbf{do}\ p := \mathsf{0})\ ;\ [\mathsf{0}] := \mathsf{3})\\ \{\mathbf{emp}\}\end{array}$$

and similarly

$$\begin{array}{l}\{\mathbf{emp}\}\\ \mathbf{with}\ m\ \mathbf{do}\ ((\mathbf{with}\ \ell\ \mathbf{do}\ p := \mathsf{1})\ ;\ [\mathsf{0}] := \mathsf{4})\\ \{\mathbf{emp}\}\end{array}$$

So

$$\begin{array}{l}\{\mathbf{emp} * \mathbf{emp}\}\\ \mathbf{with}\ \ell\ \mathbf{do}\ ((\mathbf{with}\ m\ \mathbf{do}\ p := \mathsf{0})\ ;\ [\mathsf{0}] := \mathsf{3})\\ \ \| \ \mathbf{with}\ m\ \mathbf{do}\ ((\mathbf{with}\ \ell\ \mathbf{do}\ p := \mathsf{1})\ ;\ [\mathsf{0}] := \mathsf{4})\\ \{\mathbf{emp} * \mathbf{emp}\}\end{array}$$

and finally

```
    $\{0 \mapsto -\}$
    $\{R_\ell * R_m\}$
    $\textbf{resource}\ \ell\ \textbf{in}\ \textbf{resource}\ m\ \textbf{in}$
        $(\textbf{with}\ \ell\ \textbf{do}\ ((\textbf{with}\ m\ \textbf{do}\ p := 0); [0] := 3))$
        $\parallel (\textbf{with}\ m\ \textbf{do}\ ((\textbf{with}\ \ell\ \textbf{do}\ p := 1); [0] := 4))$
    $\{R_\ell * R_m\}$
    $\{0 \mapsto -\}$
```

Note that the resources ℓ and m each have half permission for the variable p (in the sense of Bornat).