Concurrent Separation Logic

Peter O'Hearn, HCSS Tutorial, 21 May 2009

References:

- **O'Hearn**: Resources, concurrency, and local reasoning. Reynolds Festschrift. Theor. Comput. Sci. 375(1-3): 271-307, 2007. Prelim version in CONCUR'04.
- **Brookes**: A semantics for concurrent separation logic. Reynolds Festschrift. Theor. Comput. Sci. 375(1-3): 227-270, 2007. Prelim version in CONCUR'04.
- **Hoare**: Towards a theory of parallel programming. Operating Systems Techniques. 1971

Dijkstra's Principle

- *We have stipulated that processes should be loosely connected; by this we mean that apart from the (rare) moments of explicit intercommunication, the individual processes are to be regarded as completely independent of each other.*
  (*Cooperating Sequential Processes, EW Dijkstra, 1965*)

Disjoint Concurrency

$$\frac{\{P_1\}\, C_1\, \{Q_1\} \quad \{P_2\}\, C_2\, \{Q_2\}}{\{P_1 * P_2\}\, C_1 \parallel C_2 \{Q_1 * Q_2\}}$$

where

C_i *does not alter variables free in* P_j, Q_j *when* $i \neq j$.

Disjoint Concurrency

$$\frac{\{P_1\}\,C_1\,\{Q_1\} \quad \{P_2\}\,C_2\,\{Q_2\}}{\{P_1 * P_2\}\,C_1 \parallel C_2\,\{Q_1 * Q_2\}}$$

We can't prove racy programs like

$$\{10 \mapsto -\}$$
$$[10] := 42 \;\parallel\; [10] := 6$$
$$\{??\}$$

We cannot send 10 to both processes in their preconditions, since

$$(10 \mapsto -) * (10 \mapsto -)$$

is false. But...

Well specified programs don't go wrong

$\{(x \mapsto -) * P\}\ [x]{:=}7\ \{(x \mapsto 7) * P\}$

$\{\texttt{true}\}\ [x]{:=}7\ \{??\}$

$\{P * (x \mapsto -)\}\ \texttt{dispose}(x)\ \{P\}$

$\{\texttt{true}\}\ \texttt{dispose}(x)\ \{??\}$

$\{P\}\ x = \texttt{cons}(a, b)\ \{P * (x \mapsto a, b)\}\quad (x \notin \mathit{free}(P))$

If $\{P\}C\{Q\}$ *holds then* P *describes all the resources that* C *needs (at the beginning) in order to run.*

Disjoint Concurrency

$$\frac{\{P_1\}\,C_1\,\{Q_1\} \quad \{P_2\}\,C_2\,\{Q_2\}}{\{P_1 * P_2\}\,C_1 \parallel C_2\,\{Q_1 * Q_2\}}$$

We can't prove racy programs like

$$\{10 \mapsto -\}$$
$$[10] := 42 \;\parallel\; [10] := 6$$
$$\{??\}$$

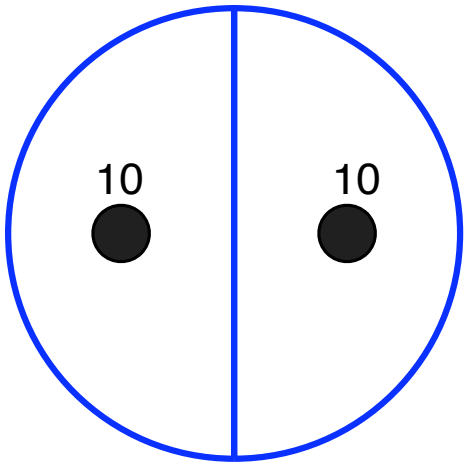
We cannot send 10 to both processes in their preconditions, since

$$(10 \mapsto -) * (10 \mapsto -)$$

is false. But...

An inconsistency: trying to be two places at once

10|->3 * 10|->3



Disjoint Concurrency

$$\frac{\{P_1\}\,C_1\,\{Q_1\} \quad \{P_2\}\,C_2\,\{Q_2\}}{\{P_1 * P_2\}\,C_1 \parallel C_2\,\{Q_1 * Q_2\}}$$

We can't prove racy programs like

$$\{10 \mapsto -\}$$
$$[10] := 42 \;\parallel\; [10] := 6$$
$$\{??\}$$

We cannot send 10 to both processes in their preconditions, since

$$(10 \mapsto -) * (10 \mapsto -)$$

is false. But...

Disjoint Concurrency

$$\frac{\{P_1\}\,C_1\,\{Q_1\} \quad \{P_2\}\,C_2\,\{Q_2\}}{\{P_1 * P_2\}\,C_1 \parallel C_2\,\{Q_1 * Q_2\}}$$

Preconditions can pick out race-free start-states, when they exist:

$$\begin{array}{ccc} & \{x \mapsto 3 * y \mapsto 3\} & \\ \{x \mapsto 3\} & & \{y \mapsto 3\} \\ [x] := 4 & \parallel & [y] := 5 \\ \{x \mapsto 4\} & & \{y \mapsto 5\} \\ & \{x \mapsto 4 * y \mapsto 5\} & \end{array}$$

Disjoint Concurrency

$$\frac{\{P_1\}\,C_1\,\{Q_1\} \quad \{P_2\}\,C_2\,\{Q_2\}}{\{P_1 * P_2\}\,C_1 \parallel C_2\,\{Q_1 * Q_2\}}$$

Preconditions can pick out race-free start-states, when they exist:

$$\begin{array}{c} \{x \mapsto 3 * y \mapsto 3\} \\ \{x \mapsto 3\} \qquad\qquad \{y \mapsto 3\} \\ [x]{:=}\,4 \qquad \parallel \qquad [y]{:=}\,5 \\ \{x \mapsto 4\} \qquad\qquad \{y \mapsto 5\} \\ \{x \mapsto 4 * y \mapsto 5\} \end{array}$$

That ‘proof figure” is an annotation form for

$$\frac{\{x \mapsto 3\}\,[x]{:=}\,4\,\{x \mapsto 4\} \qquad \{y \mapsto 3\}\,[y]{:=}\,5\,\{y \mapsto 5\}}{\{x \mapsto 3 * y \mapsto 3\}\,[x]{:=}\,4 \parallel [y]{:=}\,5\,\{x \mapsto 4 * y \mapsto 5\}}$$

Example: Parallel Mergesort

$\{array(a, i, j)\}$
procedure ms(a, i, j)
newvar $m := (i + j)/2$;
if $i < j$ then
$\big(\mathtt{ms}(a, i, m) \parallel \mathtt{ms}(a, m + 1, j)\big)$;
merge$(a, i, m + 1, j)$;
$\{sorted(a, i, j)\}$

Example: Parallel Mergesort

$\{array(a, i, j)\}$
`procedure` $\mathtt{ms}(a, i, j)$
`newvar` $m := (i + j)/2;$
`if` $i < j$ `then`
$\quad (\mathtt{ms}(a, i, m) \parallel \mathtt{ms}(a, m + 1, j));$
$\quad \mathtt{merge}(a, i, m + 1, j);$
$\{sorted(a, i, j)\}$

- Can't prove with disjoint concurrency rule

$$\frac{\{P\}C\{Q\} \quad \{P'\}C'\{Q'\}}{\{P \wedge P'\}C \parallel C'\{Q \wedge Q'\}}$$

where C does not modify any variables free in P', C', Q', and conversely. Because: Hoare logic treats an assignment to an array component as an assignment to the whole array.

Example: Parallel Mergesort

$\{array(a, i, j)\}$
`procedure` $\texttt{ms}(a, i, j)$
`newvar` $m := (i + j)/2;$
`if` $i < j$ `then`
$\quad (\texttt{ms}(a, i, m) \parallel \texttt{ms}(a, m + 1, j));$
$\quad \texttt{merge}(a, i, m + 1, j);$
$\{sorted(a, i, j)\}$

- To prove with invariants+preservation, you track many irrelevant interleavings
  - and... state complex recursion hypothesis

Example: Parallel Mergesort

$\{array(a, i, j)\}$
`procedure` $\mathtt{ms}(a, i, j)$
`newvar` $m := (i + j)/2;$
`if` $i < j$ `then`
$\quad (\mathtt{ms}(a, i, m) \parallel \mathtt{ms}(a, m + 1, j));$
$\quad \mathtt{merge}(a, i, m + 1, j);$
$\{sorted(a, i, j)\}$

- To prove with rely/guarantee, you complicate the spec (not just the reasoning)
  - Rely: no one else touches my segment
  - Guarantee: I only touch my own segment (frame axiom)

In Separation Logic[1]

- We just use the given pre/post spec.

$$\{array(a, i, m) * array(a, m+1, j)\}$$
$$\begin{array}{lcl} \{array(a, i, m)\} & & \{array(a, m+1, j)\} \\ \mathtt{ms}(a, i, m) & \| & \mathtt{ms}(a, m+1, j) \\ \{sorted(a, i, m)\} & & \{sorted(a, m+1, j)\} \end{array}$$
$$\{sorted(a, i, m) * sorted(a, m+1, j)\}$$

- Concurrency proof rule:

$$\frac{\{P_1\}C_1\{Q_1\} \quad \{P_2\}C_2\{Q_2\}}{\{P_1 * P_2\}C_1 \| C_2\{Q_1 * Q_2\}}$$

[1] $a[i]$ is sugar for $[a + i]$ in RAM model

Process Interaction:

Conditional Critical Regions (Hoare, 72)

Programs

init;
`resource` $r_1(\text{variable list}), \ldots, r_m(\text{variable list})$
$C_1 \parallel \cdots \parallel C_n$

CCRs

`with` r `when` B `do` C .

–if a variable belongs to a resource, it cannot appear in a parallel process except in a critical section for that resource

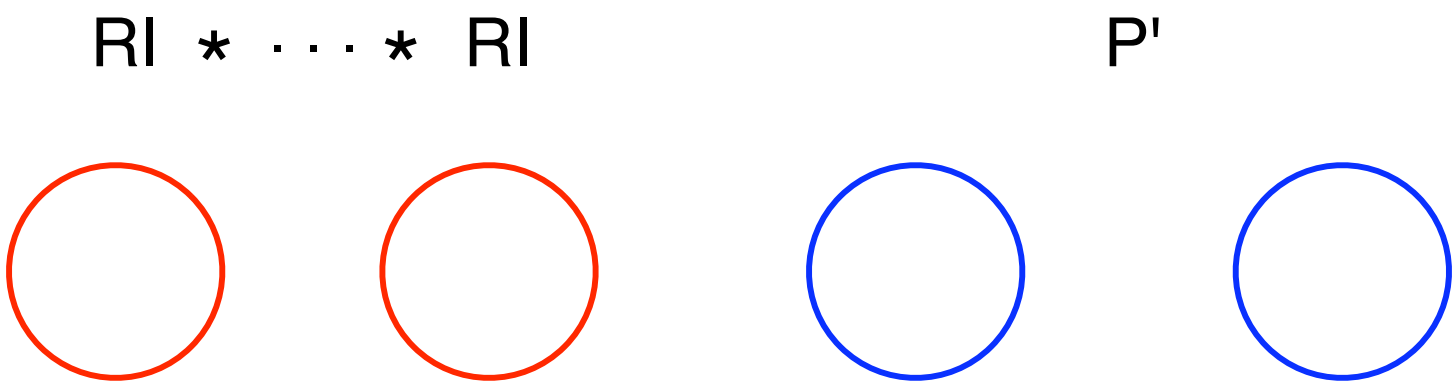
–if a variable is changed in one process, it cannot appear in another unless it belongs to a resource.

The Sequential Processes

$$
\begin{array}{rcl}
C & ::= & x{:=}\,E \mid x{:=}\,[E] \mid [E]{:=}\,F \\
& \mid & x{:=}\,\texttt{cons}(E_1, \ldots, E_n) \mid \texttt{dispose}(E) \\
& \mid & \texttt{skip} \mid C; C \mid \texttt{if } B \texttt{ then } C \texttt{ else } C \\
& \mid & \texttt{while } B \texttt{ do } C \\
& \mid & \texttt{with } r \texttt{ when } B \texttt{ do } C
\end{array}
$$

Some sugar: $x.i{:=}\,E$ for $[x + i - 1]{:=}\,E$

$$\frac{\{P\}\,init\,\{RI_{r_1} * \cdots * RI_{r_m} * P'\} \qquad \{P'\}\,C_1 \parallel \cdots \parallel C_n\,\{Q\}}{\begin{array}{l}\{P\}\\ init;\\ \texttt{resource}\ r_1(\text{variable list}), \ldots, r_m(\text{variable list})\\ C_1 \parallel \cdots \parallel C_n\\ \{RI_{r_1} * \cdots * RI_{r_m} * Q\}\end{array}}$$



$$\frac{\{P\}\,init\,\{RI_{r_1} * \cdots * RI_{r_m} * P'\} \qquad \{P'\}\,C_1 \parallel \cdots \parallel C_n\{Q\}}{}$$

$\{P\}$

init;

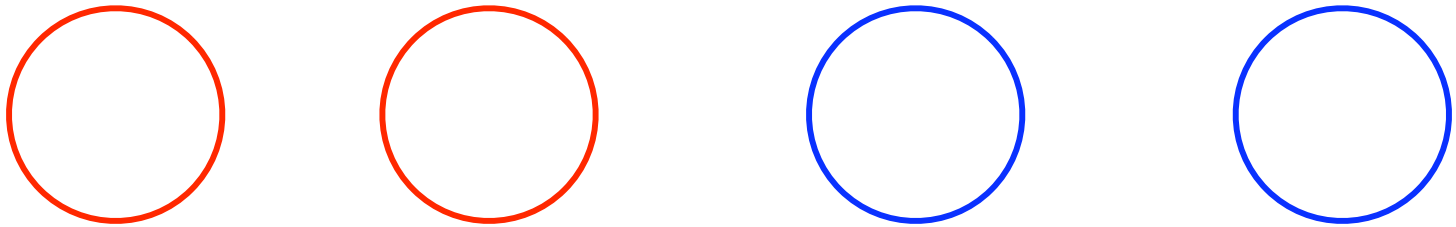
`resource` r_1(variable list), ..., r_m(variable list)

$C_1 \parallel \cdots \parallel C_n$

$\{RI_{r_1} * \cdots * RI_{r_m} * Q\}$

RI * · · · * RI

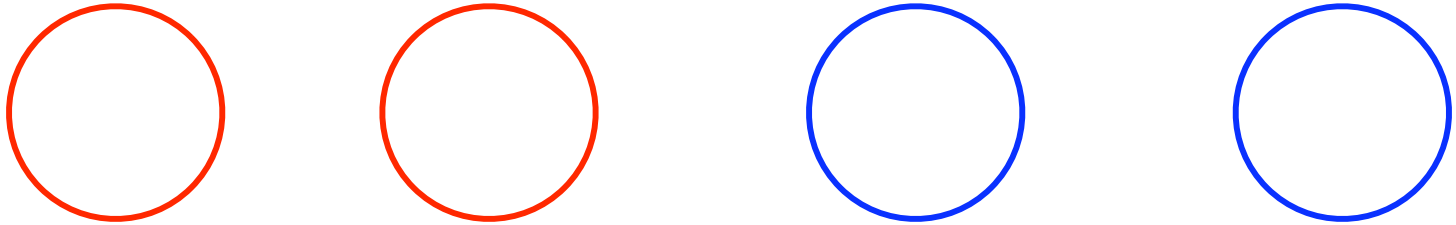
P1 * · · · * Pn



$$\frac{\{P_1\}\, C_1\, \{Q_1\} \;\cdots\; \{P_n\}\, C_n\, \{Q_n\}}{\{P_1 * \cdots * P_n\}\, C_1 \parallel \cdots \parallel C_n\, \{Q_1 * \cdots * Q_n\}}$$

RI $*$ $\cdots$ $*$ RI

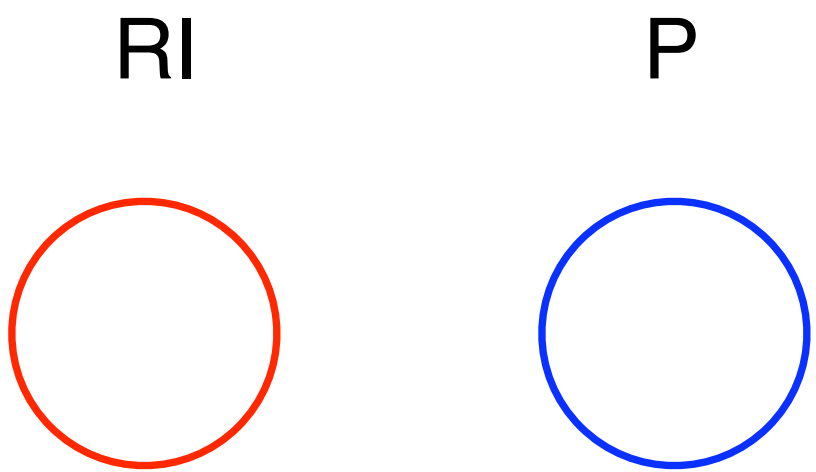
P1 $*$ $\cdots$ $*$ Pn



– no variable free in P_i or Q_i is changed in C_j when $j \neq i$.

– any modified variable free in RI_r must occur only within a critical region for r.

$$\frac{\{(P * RI_r) \wedge B\}\ C\ \{Q * RI_r\}}{\{P\}\ \texttt{with}\ r\ \texttt{when}\ B\ \texttt{do}\ C\ \{Q\}}$$



- No other process modifies variables in P or Q

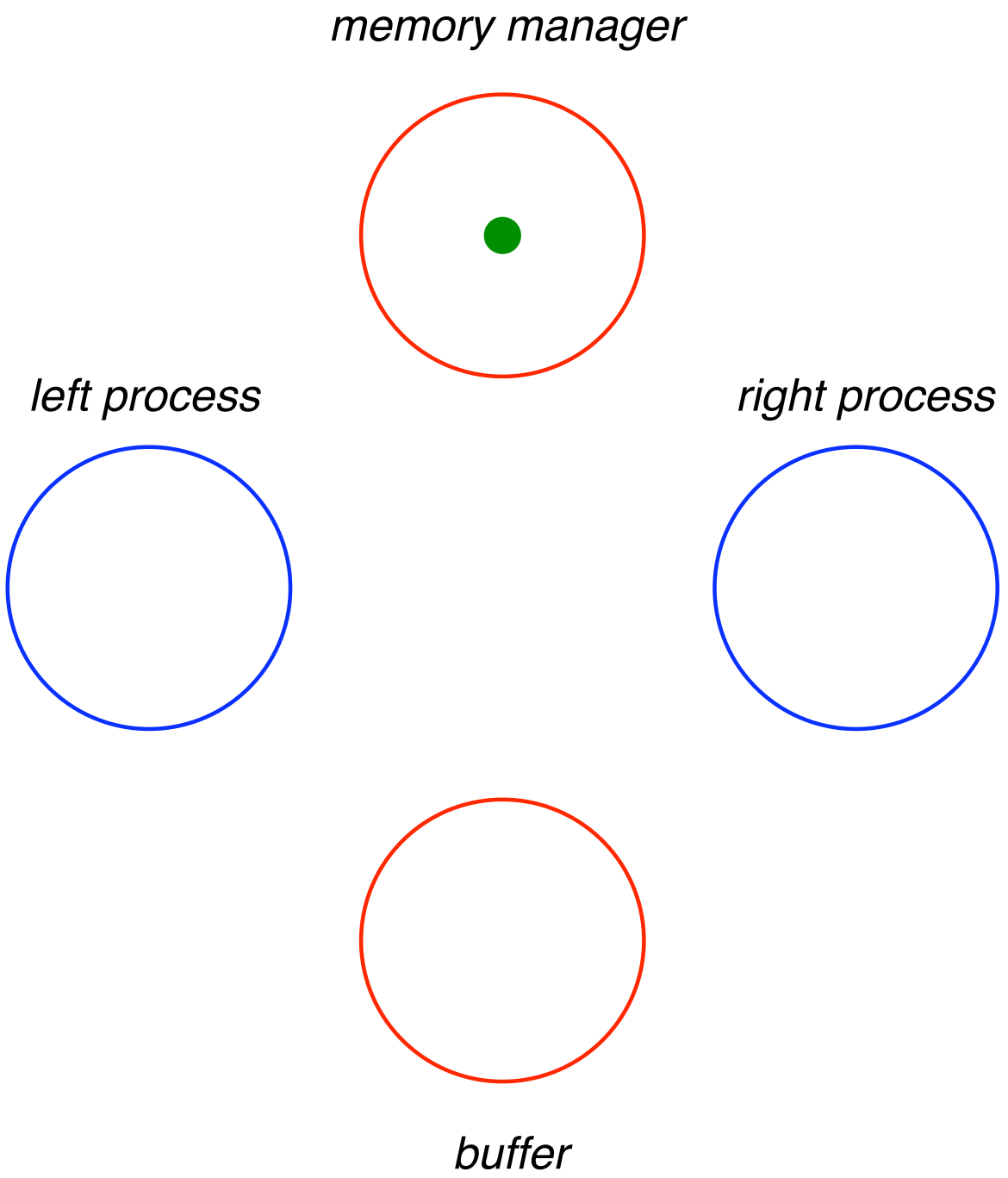
Example: Pointer Transfer

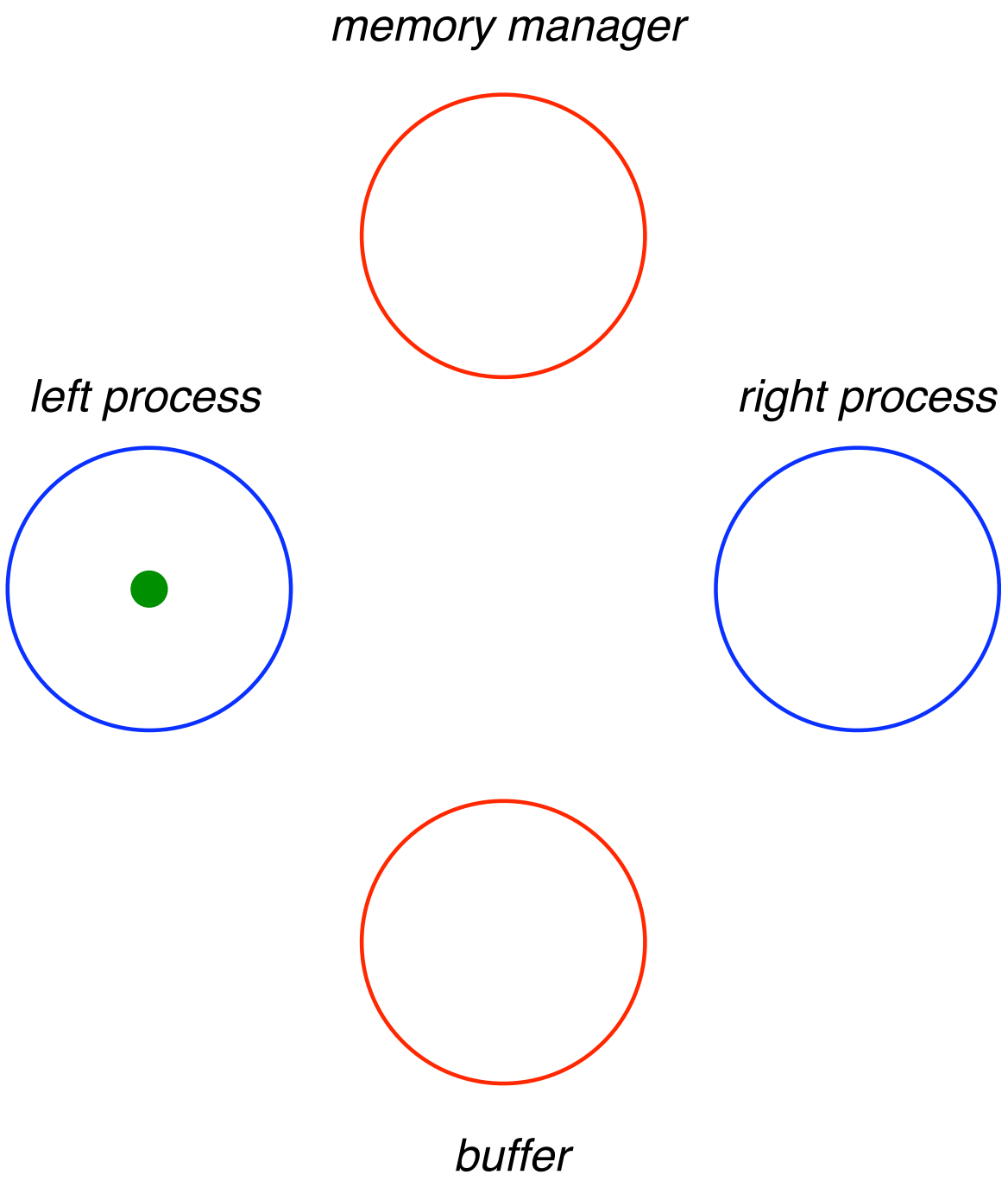
$$\texttt{resource}\ \mathit{buf}(c, \mathit{full} := \texttt{false});$$

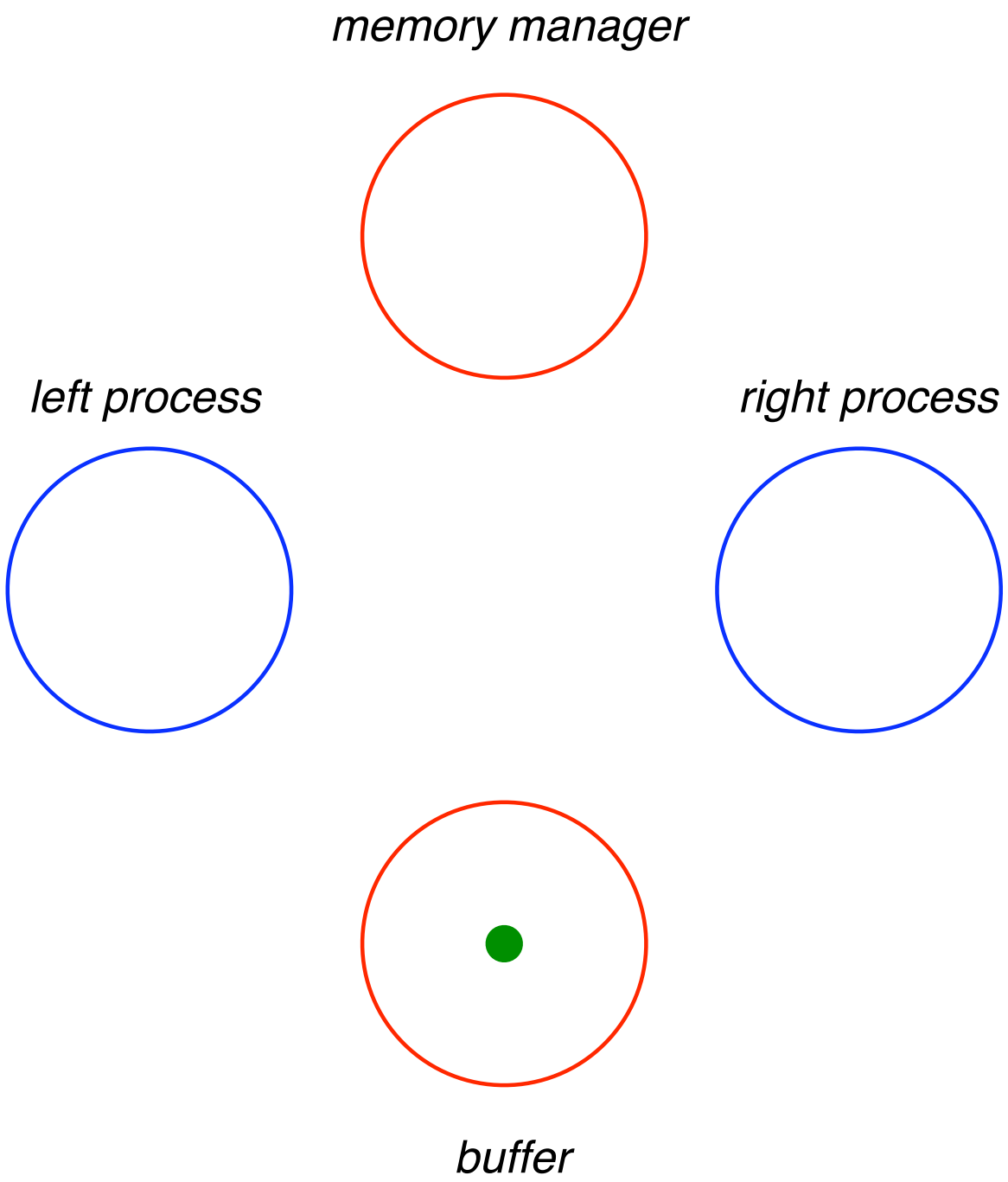
$$\begin{array}{l} x := \texttt{cons}(-); \\ \texttt{with}\ \mathit{buf}\ \texttt{when}\ \neg \mathit{full}\ \texttt{do} \\ \quad (c := x;\ \mathit{full} := \texttt{true};) \end{array} \quad \| \quad \begin{array}{l} \texttt{with}\ \mathit{buf}\ \texttt{when}\ \mathit{full}\ \texttt{do} \\ \quad (y := c;\ \mathit{full} := \texttt{false};) \\ \texttt{dispose}(y); \end{array}$$

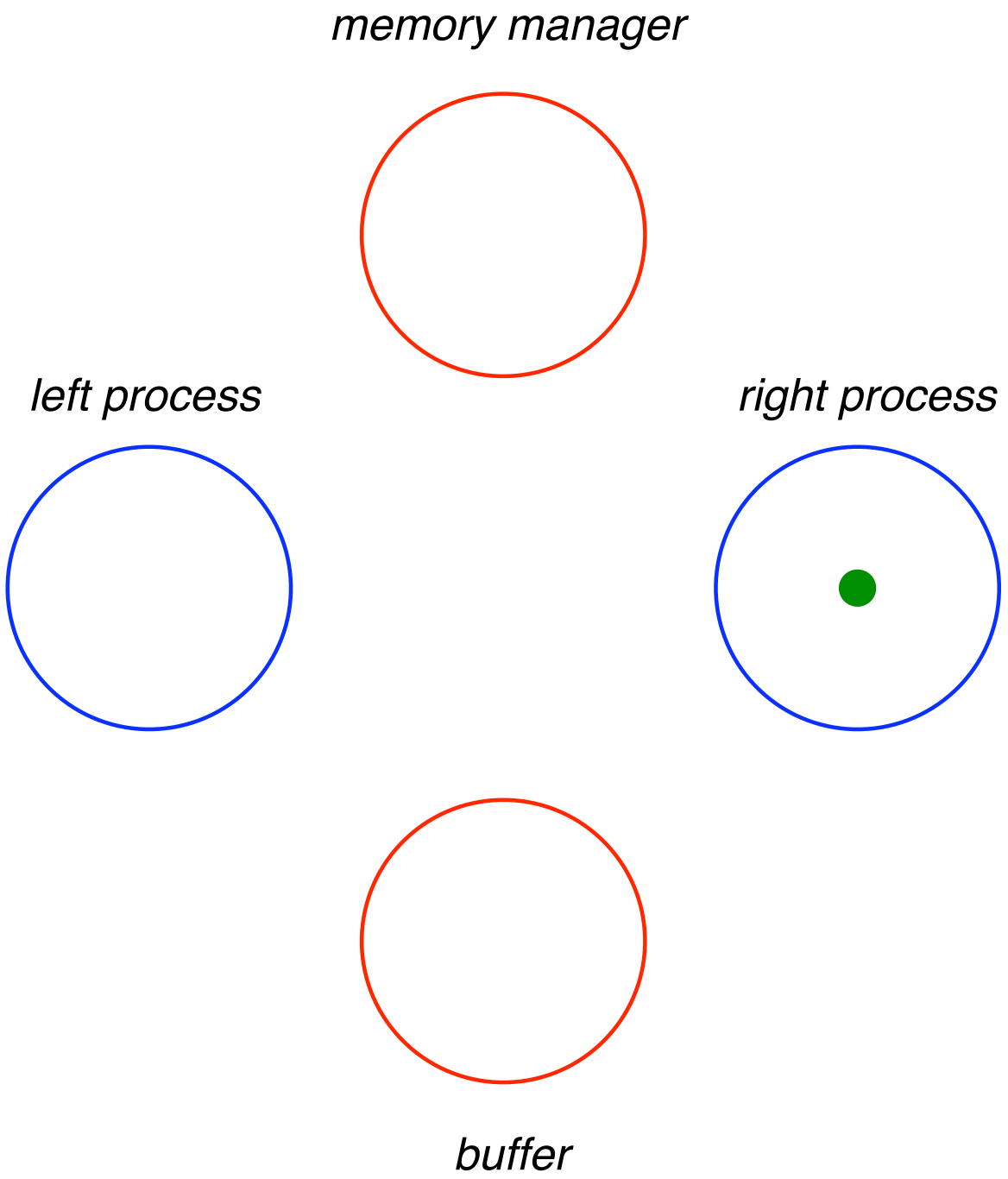
$$\frac{\{(P * \mathit{RI}_r) \wedge B\}\ C\ \{Q * \mathit{RI}_r\}}{\{P\}\ \texttt{with}\ r\ \texttt{when}\ B\ \texttt{do}\ C\ \{Q\}}$$

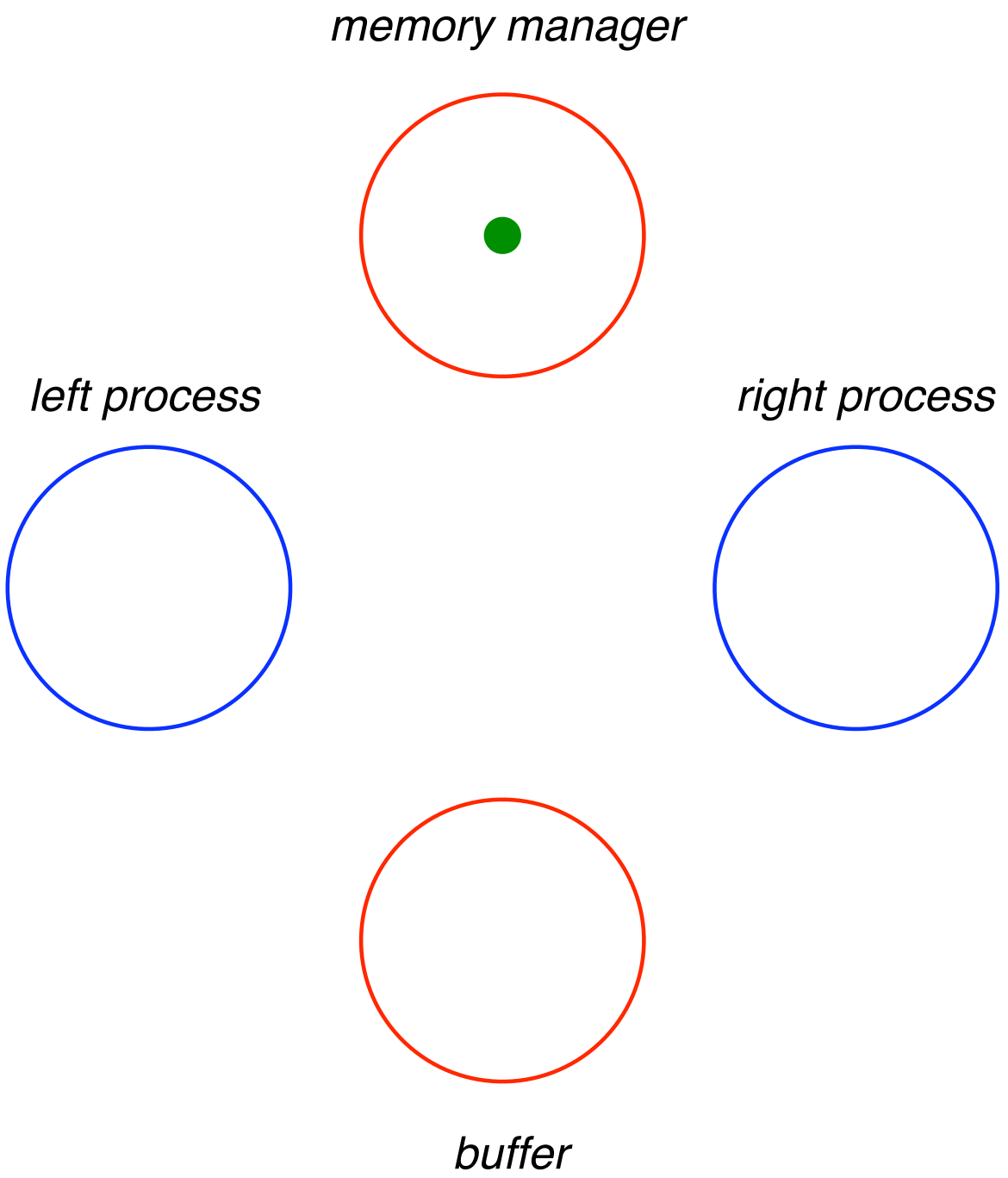
$$\mathit{RI} \triangleq (\texttt{emp} \wedge \neg \mathit{full}) \vee (c \mapsto - \wedge \mathit{full})$$


memory manager
left process
right process
buffer


memory manager
left process
right process
buffer


memory manager
left process
right process
buffer


memory manager
left process
right process
buffer


memory manager
left process
right process
buffer

Example: Pointer Transfer

$$\texttt{resource}\ \mathit{buf}(c, \mathit{full} := \texttt{false});$$

$$\begin{array}{l} x := \texttt{cons}(-); \\ \texttt{with}\ \mathit{buf}\ \texttt{when}\ \neg \mathit{full}\ \texttt{do} \\ \quad (c := x;\ \mathit{full} := \texttt{true};) \end{array} \quad \| \quad \begin{array}{l} \texttt{with}\ \mathit{buf}\ \texttt{when}\ \mathit{full}\ \texttt{do} \\ \quad (y := c;\ \mathit{full} := \texttt{false};) \\ \texttt{dispose}(y); \end{array}$$

$$\frac{\{(P * \mathit{RI}_r) \wedge B\}\ C\ \{Q * \mathit{RI}_r\}}{\{P\}\ \texttt{with}\ r\ \texttt{when}\ B\ \texttt{do}\ C\ \{Q\}}$$

$$\mathit{RI} \triangleq (\texttt{emp} \wedge \neg \mathit{full}) \vee (c \mapsto - \wedge \mathit{full})$$

Example: Pointer Transfer

$$\texttt{resource}\ \mathit{buf}(c, \mathit{full} := \texttt{false});$$

$$\begin{array}{l} x := \texttt{cons}(-); \\ \texttt{with}\ \mathit{buf}\ \texttt{when}\ \neg \mathit{full}\ \texttt{do} \\ \quad (c := x;\ \mathit{full} := \texttt{true};) \end{array} \quad \| \quad \begin{array}{l} \texttt{with}\ \mathit{buf}\ \texttt{when}\ \mathit{full}\ \texttt{do} \\ \quad (y := c;\ \mathit{full} := \texttt{false};) \\ \texttt{dispose}(y); \end{array}$$

$$\frac{\{(P * \mathit{RI}_r) \wedge B\}\ C\ \{Q * \mathit{RI}_r\}}{\{P\}\ \texttt{with}\ r\ \texttt{when}\ B\ \texttt{do}\ C\ \{Q\}}$$

$$\mathit{RI} \triangleq (\texttt{emp} \wedge \neg \mathit{full}) \vee (c \mapsto - \wedge \mathit{full})$$

Warning

- There are weird resource invariants, like

$$\texttt{true} \qquad\qquad 10 \mapsto - \vee 42 \mapsto \vee$$

  which are unclear about which storage is "owned"
- Soundness broken by this weirdness (cf, Reynolds counterexample)

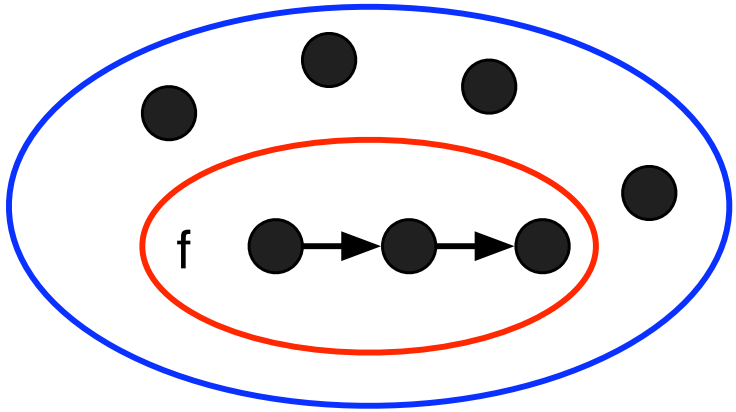
$$\frac{\{(P * \mathit{weird}) \wedge B\}\ C\ \{Q * \mathit{weird}\}}{\{P\}\ \texttt{with}\ r\ \texttt{when}\ B\ \texttt{do}\ C\ \texttt{endwith}\ \{Q\}}$$

- A class of precise predicates, rule out weirdness.
- **Brookes's Soundness Theorem**: The proof rules are sound if we restrict the proof rule to be

$$\frac{\{(P * \mathit{precise}) \wedge B\}\ C\ \{Q * \mathit{precise}\}}{\{P\}\ \texttt{with}\ r\ \texttt{when}\ B\ \texttt{do}\ C\ \texttt{endwith}\ \{Q\}}$$

Precise Predicates

- A predicate is **precise** if, for every state, there is at most one substate that satisfies it.



- For all s, h, exists at most one $h' \sqsubseteq h$ where $s, h' \models P$.

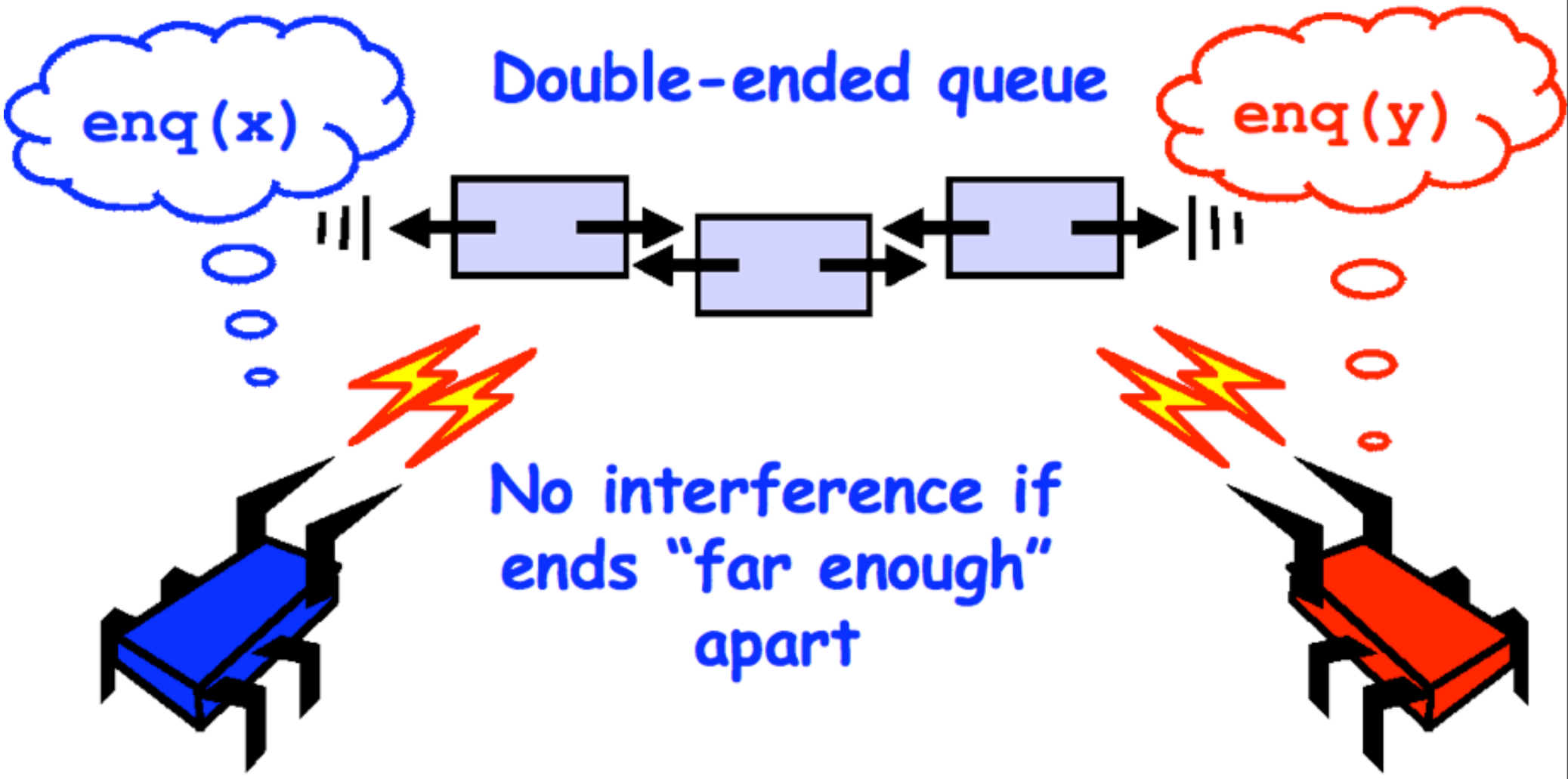
Further Work

- For more concurrency today, see the talks of **Zhong Shao** and **Alexey Gotsman** this afternoon.

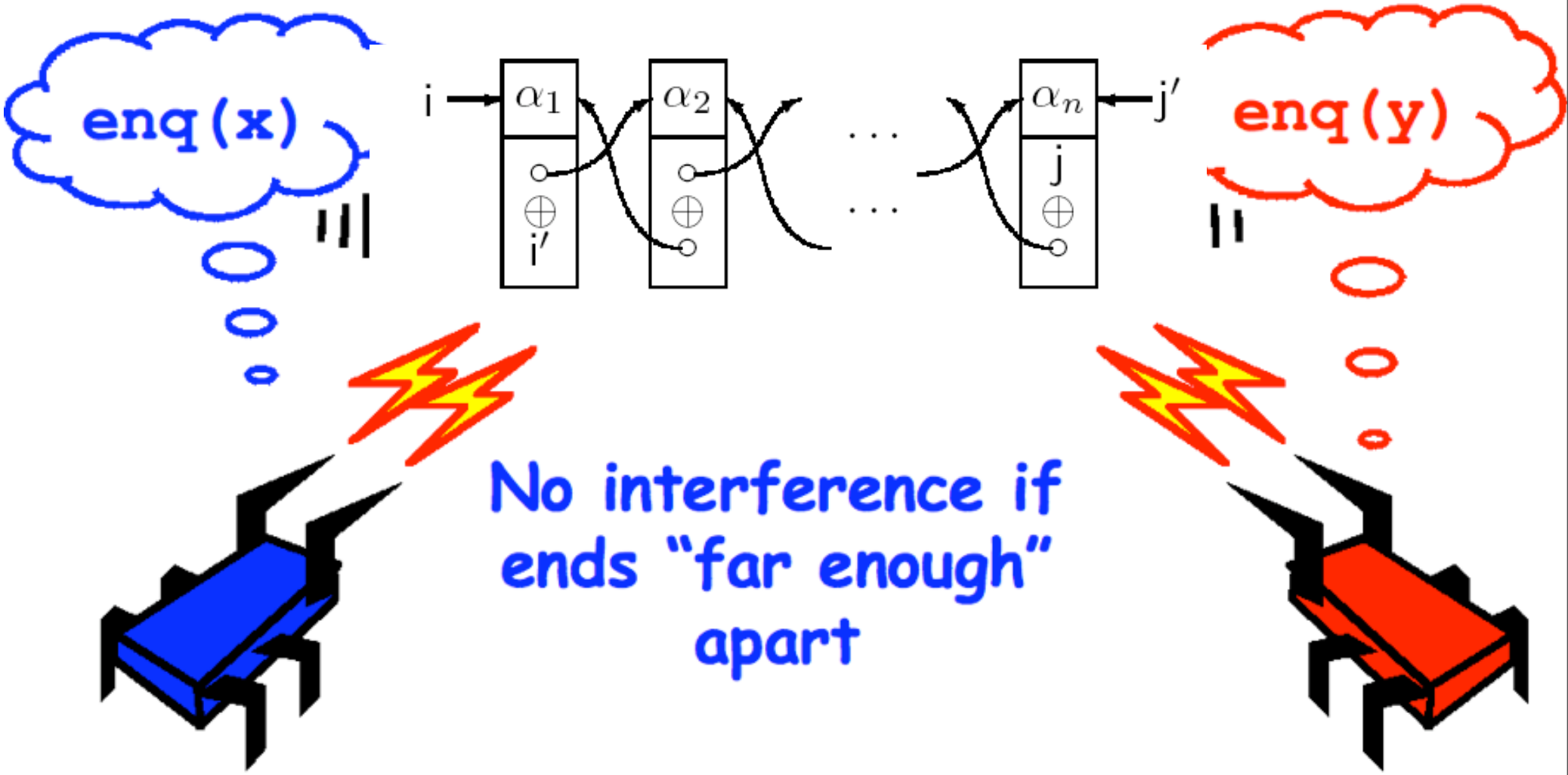
Further Work

- For more concurrency today, see the talks of **Zhong Shao** and **Alexey Gotsman** this afternoon.
- There is also much further work on **fine-grained concurrency** and **separation logic meets rely guarantee**.
  - Xinyu Feng, Rodrigo Ferreira, Zhong Shao: On the Relationship Between Concurrent Separation Logic and Assume-Guarantee Reasoning. ESOP 2007: 173-188
  - Viktor Vafeiadis, Matthew J. Parkinson: A Marriage of Rely/Guarantee and Separation Logic. CONCUR 2007: 256-271
  - Cristiano Calcagno, Matthew J. Parkinson, Viktor Vafeiadis: Modular Safety Checking for Fine-Grained Concurrency. SAS 2007: 233-248
  - Xinyu Feng: Local rely-guarantee reasoning. POPL 2009: 315-327
  - Viktor Vafeiadis: Shape-Value Abstraction for Verifying Linearizability. VMCAI 2009: 335-34
  - Mike Dodds, Xinyu Feng, Matthew J. Parkinson, Viktor Vafeiadis: Deny-Guarantee Reasoning. ESOP 2009: 363-377

Sadistic Homework Assignment



Sadistic Homework Assignment



No interference if ends "far enough" apart

Additional Slides

$\{\mathtt{emp}\}$

$\mathtt{resource}\ \mathit{buf}(c, \mathit{full} := \mathtt{false});$

$\{\mathtt{emp} \wedge \neg \mathit{full}\}$

$x := \mathtt{cons}(-);$		$\mathtt{with}\ \mathit{buf}\ \mathtt{when}\ \mathit{full}\ \mathtt{do}$
$\mathtt{with}\ \mathit{buf}\ \mathtt{when}\ \neg \mathit{full}\ \mathtt{do}$	$\|\|$	$y := c;\ \mathit{full} := \mathtt{false}$
$c := x;\ \mathit{full} := \mathtt{true};$		$\mathtt{endwith};$
		$\mathtt{dispose}(y);$
$\mathtt{endwith};$		

$$\frac{\{(P * RI_r) \wedge B\}\ C\ \{Q * RI_r\}}{\{P\}\ \mathtt{with}\ r\ \mathtt{when}\ B\ \mathtt{do}\ C\ \{Q\}}$$

$$RI \quad \triangleq \quad (\mathtt{emp} \wedge \neg \mathit{full}) \vee (c \mapsto - \wedge \mathit{full})$$

$\{\mathtt{emp}\}$

$\mathtt{resource}\ \mathit{buf}(c, \mathit{full} := \mathtt{false});$

$\{\mathtt{emp} * \mathtt{emp} * (\mathtt{emp} \wedge \neg \mathit{full})\}$

$x := \mathtt{cons}(-);$	$\mathtt{with}\ \mathit{buf}\ \mathtt{when}\ \mathit{full}\ \mathtt{do}$
$\mathtt{with}\ \mathit{buf}\ \mathtt{when}\ \neg \mathit{full}\ \mathtt{do}$	$y := c;\ \mathit{full} := \mathtt{false}$
$c := x;\ \mathit{full} := \mathtt{true};$	$\mathtt{endwith};$
	$\mathtt{dispose}(y);$
$\mathtt{endwith};$	

$$\frac{\{(P * RI_r) \wedge B\}\ C\ \{Q * RI_r\}}{\{P\}\ \mathtt{with}\ r\ \mathtt{when}\ B\ \mathtt{do}\ C\ \{Q\}}$$

$$RI \quad \triangleq \quad (\mathtt{emp} \wedge \neg \mathit{full}) \vee (c \mapsto - \wedge \mathit{full})$$

$\{\mathtt{emp}\}$

$\mathtt{resource}\ \mathit{buf}(c, \mathit{full} := \mathtt{false});$

$\{\mathtt{emp} * \mathtt{emp} * \mathit{RI}\}$

$x := \mathtt{cons}(-);$

$\mathtt{with}\ \mathit{buf}\ \mathtt{when}\ \neg \mathit{full}\ \mathtt{do}$

$\quad c := x;\ \mathit{full} := \mathtt{true};$

$\mathtt{endwith};$

$\|$

$\mathtt{with}\ \mathit{buf}\ \mathtt{when}\ \mathit{full}\ \mathtt{do}$

$\quad y := c;\ \mathit{full} := \mathtt{false}$

$\mathtt{endwith};$

$\mathtt{dispose}(y);$

$$\frac{\{(P * \mathit{RI}_r) \wedge B\}\ C\ \{Q * \mathit{RI}_r\}}{\{P\}\ \mathtt{with}\ r\ \mathtt{when}\ B\ \mathtt{do}\ C\ \{Q\}}$$

$$\mathit{RI} \quad \triangleq \quad (\mathtt{emp} \wedge \neg \mathit{full}) \vee (c \mapsto - \wedge \mathit{full})$$

$\{\mathtt{emp}\}$

$\mathtt{resource}\ \mathit{buf}(c, \mathit{full} := \mathtt{false});$

$\{\mathtt{emp} * \mathtt{emp} * \mathit{RI}\}$

$\{\mathtt{emp}\}$

$x := \mathtt{cons}(-);$

$\mathtt{with}\ \mathit{buf}\ \mathtt{when}\ \neg \mathit{full}\ \mathtt{do}$

$\quad c := x;\ \mathit{full} := \mathtt{true};$

$\mathtt{endwith};$

$\|$

$\{\mathtt{emp}\}$

$\mathtt{with}\ \mathit{buf}\ \mathtt{when}\ \mathit{full}\ \mathtt{do}$

$\quad y := c;\ \mathit{full} := \mathtt{false}$

$\mathtt{endwith};$

$\mathtt{dispose}(y);$

$$\frac{\{(P * \mathit{RI}_r) \wedge B\}\ C\ \{Q * \mathit{RI}_r\}}{\{P\}\ \mathtt{with}\ r\ \mathtt{when}\ B\ \mathtt{do}\ C\ \{Q\}}$$

$$\mathit{RI} \triangleq (\mathtt{emp} \wedge \neg \mathit{full}) \vee (c \mapsto - \wedge \mathit{full})$$

$\{\mathtt{emp}\}$

$\mathtt{resource}\ \mathit{buf}(c, \mathit{full} := \mathtt{false});$

$\{\mathtt{emp} * \mathtt{emp} * \mathit{RI}\}$

$\{\mathtt{emp}\}$

$x := \mathtt{cons}(-);$

$\{x \mapsto -\}$

$\mathtt{with}\ \mathit{buf}\ \mathtt{when}\ \neg \mathit{full}\ \mathtt{do}$

$c := x;\ \mathit{full} := \mathtt{true};$

$\mathtt{endwith};$

$\|$

$\{\mathtt{emp}\}$

$\mathtt{with}\ \mathit{buf}\ \mathtt{when}\ \mathit{full}\ \mathtt{do}$

$y := c;\ \mathit{full} := \mathtt{false}$

$\mathtt{endwith};$

$\mathtt{dispose}(y);$

$$\frac{\{(P * \mathit{RI}_r) \wedge B\}\ C\ \{Q * \mathit{RI}_r\}}{\{P\}\ \mathtt{with}\ r\ \mathtt{when}\ B\ \mathtt{do}\ C\ \{Q\}}$$

$$\mathit{RI} \quad \triangleq \quad (\mathtt{emp} \wedge \neg \mathit{full}) \vee (c \mapsto - \wedge \mathit{full})$$

$\{\mathtt{emp}\}$

$\mathtt{resource}\ \mathit{buf}(c, \mathit{full} := \mathtt{false});$

$\{\mathtt{emp} * \mathtt{emp} * \mathit{RI}\}$

$\{\mathtt{emp}\}$

$x := \mathtt{cons}(-);$

$\{x \mapsto -\}$

$\mathtt{with}\ \mathit{buf}\ \mathtt{when}\ \neg \mathit{full}\ \mathtt{do}$

$\{(x \mapsto -) * (\mathtt{emp} \wedge \neg \mathit{full})\}$

$c := x;\ \mathit{full} := \mathtt{true};$

$\mathtt{endwith};$

$\|$

$\{\mathtt{emp}\}$

$\mathtt{with}\ \mathit{buf}\ \mathtt{when}\ \mathit{full}\ \mathtt{do}$

$y := c;\ \mathit{full} := \mathtt{false}$

$\mathtt{endwith};$

$\mathtt{dispose}(y);$

$$\frac{\{(P * \mathit{RI}_r) \wedge B\}\ C\ \{Q * \mathit{RI}_r\}}{\{P\}\ \mathtt{with}\ r\ \mathtt{when}\ B\ \mathtt{do}\ C\ \{Q\}}$$

$$\mathit{RI} \triangleq (\mathtt{emp} \wedge \neg \mathit{full}) \vee (c \mapsto - \wedge \mathit{full})$$

$\{\mathtt{emp}\}$

$\mathtt{resource}\ \mathit{buf}(c, \mathit{full} := \mathtt{false});$

$\{\mathtt{emp} * \mathtt{emp} * \mathit{RI}\}$

$\{\mathtt{emp}\}$

$x := \mathtt{cons}(-);$

$\{x \mapsto -\}$

$\mathtt{with}\ \mathit{buf}\ \mathtt{when}\ \neg \mathit{full}\ \mathtt{do}$

$\{(x \mapsto -) * (\mathtt{emp} \wedge \neg \mathit{full})\}$

$c := x;\ \mathit{full} := \mathtt{true};$

$\{(c \mapsto -) * (\mathtt{emp} \wedge \mathit{full})\}$

$\mathtt{endwith};$

$\|$

$\{\mathtt{emp}\}$

$\mathtt{with}\ \mathit{buf}\ \mathtt{when}\ \mathit{full}\ \mathtt{do}$

$y := c;\ \mathit{full} := \mathtt{false}$

$\mathtt{endwith};$

$\mathtt{dispose}(y);$

$$\frac{\{(P * \mathit{RI}_r) \wedge B\}\ C\ \{Q * \mathit{RI}_r\}}{\{P\}\ \mathtt{with}\ r\ \mathtt{when}\ B\ \mathtt{do}\ C\ \{Q\}}$$

$$\mathit{RI} \triangleq (\mathtt{emp} \wedge \neg \mathit{full}) \vee (c \mapsto - \wedge \mathit{full})$$

$\{\mathtt{emp}\}$

$\mathtt{resource}\ \mathit{buf}(c, \mathit{full} := \mathtt{false});$

$\{\mathtt{emp} * \mathtt{emp} * \mathit{RI}\}$

$\{\mathtt{emp}\}$

$x := \mathtt{cons}(-);$

$\{x \mapsto -\}$

$\mathtt{with}\ \mathit{buf}\ \mathtt{when}\ \neg \mathit{full}\ \mathtt{do}$

$\{(x \mapsto -) * (\mathtt{emp} \wedge \neg \mathit{full})\}$

$c := x;\ \mathit{full} := \mathtt{true};$

$\{(c \mapsto -) * (\mathtt{emp} \wedge \mathit{full})\}$

$\{(c \mapsto - \wedge \mathit{full}\}$

$\mathtt{endwith};$

$\|$

$\{\mathtt{emp}\}$

$\mathtt{with}\ \mathit{buf}\ \mathtt{when}\ \mathit{full}\ \mathtt{do}$

$y := c;\ \mathit{full} := \mathtt{false}$

$\mathtt{endwith};$

$\mathtt{dispose}(y);$

$$\frac{\{(P * \mathit{RI}_r) \wedge B\}\ C\ \{Q * \mathit{RI}_r\}}{\{P\}\ \mathtt{with}\ r\ \mathtt{when}\ B\ \mathtt{do}\ C\ \{Q\}}$$

$$\mathit{RI} \triangleq (\mathtt{emp} \wedge \neg \mathit{full}) \vee (c \mapsto - \wedge \mathit{full})$$

$\{\mathtt{emp}\}$

$\mathtt{resource}\ \mathit{buf}(c, \mathit{full} := \mathtt{false});$

$\{\mathtt{emp} * \mathtt{emp} * \mathit{RI}\}$

$\{\mathtt{emp}\}$

$x := \mathtt{cons}(-);$

$\{x \mapsto -\}$

$\mathtt{with}\ \mathit{buf}\ \mathtt{when}\ \neg \mathit{full}\ \mathtt{do}$

$\{(x \mapsto -) * (\mathtt{emp} \wedge \neg \mathit{full})\}$

$c := x;\ \mathit{full} := \mathtt{true};$

$\{(c \mapsto -) * (\mathtt{emp} \wedge \mathit{full})\}$

$\{\mathit{RI}\}$

$\mathtt{endwith};$

$\|$

$\{\mathtt{emp}\}$

$\mathtt{with}\ \mathit{buf}\ \mathtt{when}\ \mathit{full}\ \mathtt{do}$

$y := c;\ \mathit{full} := \mathtt{false}$

$\mathtt{endwith};$

$\mathtt{dispose}(y);$

$$\frac{\{(P * \mathit{RI}_r) \wedge B\}\ C\ \{Q * \mathit{RI}_r\}}{\{P\}\ \mathtt{with}\ r\ \mathtt{when}\ B\ \mathtt{do}\ C\ \{Q\}}$$

$$\mathit{RI} \triangleq (\mathtt{emp} \wedge \neg \mathit{full}) \vee (c \mapsto - \wedge \mathit{full})$$

$\{\mathtt{emp}\}$

$\mathtt{resource}\ \mathit{buf}(c, \mathit{full} := \mathtt{false});$

$\{\mathtt{emp} * \mathtt{emp} * \mathit{RI}\}$

$\{\mathtt{emp}\}$

$x := \mathtt{cons}(-);$

$\{x \mapsto -\}$

$\mathtt{with}\ \mathit{buf}\ \mathtt{when}\ \neg \mathit{full}\ \mathtt{do}$

$\{(x \mapsto -) * (\mathtt{emp} \wedge \neg \mathit{full})\}$

$c := x;\ \mathit{full} := \mathtt{true};$

$\{(c \mapsto -) * (\mathtt{emp} \wedge \mathit{full})\}$

$\{\mathtt{emp} * \mathit{RI}\}$

$\mathtt{endwith};$

$\|$

$\{\mathtt{emp}\}$

$\mathtt{with}\ \mathit{buf}\ \mathtt{when}\ \mathit{full}\ \mathtt{do}$

$y := c;\ \mathit{full} := \mathtt{false}$

$\mathtt{endwith};$

$\mathtt{dispose}(y);$

$$\frac{\{(P * \mathit{RI}_r) \wedge B\}\ C\ \{Q * \mathit{RI}_r\}}{\{P\}\ \mathtt{with}\ r\ \mathtt{when}\ B\ \mathtt{do}\ C\ \{Q\}}$$

$$\mathit{RI} \triangleq (\mathtt{emp} \wedge \neg \mathit{full}) \vee (c \mapsto - \wedge \mathit{full})$$

$\{\mathtt{emp}\}$

$\mathtt{resource}\ \mathit{buf}(c, \mathit{full} := \mathtt{false});$

$\{\mathtt{emp} * \mathtt{emp} * \mathit{RI}\}$

$\{\mathtt{emp}\}$

$x := \mathtt{cons}(-);$

$\{x \mapsto -\}$

$\mathtt{with}\ \mathit{buf}\ \mathtt{when}\ \neg \mathit{full}\ \mathtt{do}$

$\{(x \mapsto -) * (\mathtt{emp} \wedge \neg \mathit{full})\}$

$c := x;\ \mathit{full} := \mathtt{true};$

$\{(c \mapsto -) * (\mathtt{emp} \wedge \mathit{full})\}$

$\{\mathtt{emp} * \mathit{RI}\}$

$\mathtt{endwith};$

$\{\mathtt{emp}\}$

$\|$

$\{\mathtt{emp}\}$

$\mathtt{with}\ \mathit{buf}\ \mathtt{when}\ \mathit{full}\ \mathtt{do}$

$y := c;\ \mathit{full} := \mathtt{false}$

$\mathtt{endwith};$

$\mathtt{dispose}(y);$

$$\frac{\{(P * \mathit{RI}_r) \wedge B\}\ C\ \{Q * \mathit{RI}_r\}}{\{P\}\ \mathtt{with}\ r\ \mathtt{when}\ B\ \mathtt{do}\ C\ \{Q\}}$$

$$\mathit{RI} \triangleq (\mathtt{emp} \wedge \neg \mathit{full}) \vee (c \mapsto - \wedge \mathit{full})$$

$\{\mathtt{emp}\}$

$\mathtt{resource}\ \mathit{buf}(c, \mathit{full} := \mathtt{false});$

$\{\mathtt{emp} * \mathtt{emp} * \mathit{RI}\}$

$\{\mathtt{emp}\}$
$x := \mathtt{cons}(-);$
$\{x \mapsto -\}$
$\mathtt{with}\ \mathit{buf}\ \mathtt{when}\ \neg \mathit{full}\ \mathtt{do}$
$\{(x \mapsto -) * (\mathtt{emp} \wedge \neg \mathit{full})\}$
$c := x;\ \mathit{full} := \mathtt{true};$
$\{(c \mapsto -) * (\mathtt{emp} \wedge \mathit{full})\}$
$\{\mathtt{emp} * \mathit{RI}\}$
$\mathtt{endwith};$
$\{\mathtt{emp}\}$

$\|$

$\{\mathtt{emp}\}$
$\mathtt{with}\ \mathit{buf}\ \mathtt{when}\ \mathit{full}\ \mathtt{do}$
$\{\mathtt{emp} * ((c \mapsto -) \wedge \mathit{full})\}$
$y := c;\ \mathit{full} := \mathtt{false}$
$\{(y \mapsto -) * (\mathtt{emp} \wedge \neg \mathit{full})\}$
$\mathtt{endwith};$

$\mathtt{dispose}(y);$

$$\frac{\{(P * \mathit{RI}_r) \wedge B\}\ C\ \{Q * \mathit{RI}_r\}}{\{P\}\ \mathtt{with}\ r\ \mathtt{when}\ B\ \mathtt{do}\ C\ \{Q\}}$$

$$\mathit{RI} \triangleq (\mathtt{emp} \wedge \neg \mathit{full}) \vee (c \mapsto - \wedge \mathit{full})$$

$\{\mathsf{emp}\}$

$\texttt{resource}\ \mathit{buf}(c, \mathit{full} := \texttt{false});$

$\{\mathsf{emp} * \mathsf{emp} * \mathit{RI}\}$

$\{\mathsf{emp}\}$

$x := \texttt{cons}(-);$

$\{x \mapsto -\}$

$\texttt{with}\ \mathit{buf}\ \texttt{when}\ \neg \mathit{full}\ \texttt{do}$

$\{(x \mapsto -) * (\mathsf{emp} \wedge \neg \mathit{full})\}$

$c := x;\ \mathit{full} := \texttt{true};$

$\{(c \mapsto -) * (\mathsf{emp} \wedge \mathit{full})\}$

$\{\mathsf{emp} * \mathit{RI}\}$

$\texttt{endwith};$

$\{\mathsf{emp}\}$

$\|$

$\{\mathsf{emp}\}$

$\texttt{with}\ \mathit{buf}\ \texttt{when}\ \mathit{full}\ \texttt{do}$

$\{\mathsf{emp} * ((c \mapsto -) \wedge \mathit{full})\}$

$y := c;\ \mathit{full} := \texttt{false}$

$\{(y \mapsto -) * (\mathsf{emp} \wedge \neg \mathit{full})\}$

$\texttt{endwith};$

$\{y \mapsto -\}$

$\texttt{dispose}(y);$

$$\frac{\{(P * \mathit{RI}_r) \wedge B\}\ C\ \{Q * \mathit{RI}_r\}}{\{P\}\ \texttt{with}\ r\ \texttt{when}\ B\ \texttt{do}\ C\ \{Q\}}$$

$$\mathit{RI} \triangleq (\mathsf{emp} \wedge \neg \mathit{full}) \vee (c \mapsto - \wedge \mathit{full})$$

$\{\mathsf{emp}\}$

$\texttt{resource}\ \mathit{buf}(c, \mathit{full} := \texttt{false});$

$\{\mathsf{emp} * \mathsf{emp} * \mathit{RI}\}$

$\{\mathsf{emp}\}$	$\{\mathsf{emp}\}$
$x := \texttt{cons}(-);$	$\texttt{with}\ \mathit{buf}\ \texttt{when}\ \mathit{full}\ \texttt{do}$
$\{x \mapsto -\}$	$\quad \{\mathsf{emp} * ((c \mapsto -) \wedge \mathit{full})\}$
$\texttt{with}\ \mathit{buf}\ \texttt{when}\ \neg \mathit{full}\ \texttt{do}$	$\quad y := c;\ \mathit{full} := \texttt{false}$
$\quad \{(x \mapsto -) * (\mathsf{emp} \wedge \neg \mathit{full})\}$	$\quad \{(y \mapsto -) * (\mathsf{emp} \wedge \neg \mathit{full})\}$
$\quad c := x;\ \mathit{full} := \texttt{true};$	$\texttt{endwith};$
$\quad \{(c \mapsto -) * (\mathsf{emp} \wedge \mathit{full})\}$	$\{y \mapsto -\}$
$\quad \{\mathsf{emp} * \mathit{RI}\}$	$\texttt{dispose}(y);$
$\texttt{endwith};$	$\{\mathsf{emp}\}$
$\{\mathsf{emp}\}$	

$$\frac{\{(P * \mathit{RI}_r) \wedge B\}\ C\ \{Q * \mathit{RI}_r\}}{\{P\}\ \texttt{with}\ r\ \texttt{when}\ B\ \texttt{do}\ C\ \{Q\}}$$

$$\mathit{RI} \triangleq (\mathsf{emp} \wedge \neg \mathit{full}) \vee (c \mapsto - \wedge \mathit{full})$$

$\{\mathsf{emp}\}$

$\mathtt{resource}\ \mathit{buf}(c, \mathit{full} := \mathtt{false});$

$\{\mathsf{emp} * \mathsf{emp} * \mathit{RI}\}$

$\{\mathsf{emp}\}$

$x := \mathtt{cons}(-);$

$\{x \mapsto -\}$

$\mathtt{with}\ \mathit{buf}\ \mathtt{when}\ \neg \mathit{full}\ \mathtt{do}$

$\{(x \mapsto -) * (\mathsf{emp} \wedge \neg \mathit{full})\}$

$c := x;\ \mathit{full} := \mathtt{true};$

$\{(c \mapsto -) * (\mathsf{emp} \wedge \mathit{full})\}$

$\{\mathsf{emp} * \mathit{RI}\}$

$\mathtt{endwith};$

$\{\mathsf{emp}\}$

$\mathtt{dispose}(x);$

$\|$

$\{\mathsf{emp}\}$

$\mathtt{with}\ \mathit{buf}\ \mathtt{when}\ \mathit{full}\ \mathtt{do}$

$\{\mathsf{emp} * ((c \mapsto -) \wedge \mathit{full})\}$

$y := c;\ \mathit{full} := \mathtt{false}$

$\{(y \mapsto -) * (\mathsf{emp} \wedge \neg \mathit{full})\}$

$\mathtt{endwith};$

$\{y \mapsto -\}$

$\mathtt{dispose}(y);$

$\{\mathsf{emp}\}$

$$\frac{\{(P * \mathit{RI}_r) \wedge B\}\ C\ \{Q * \mathit{RI}_r\}}{\{P\}\ \mathtt{with}\ r\ \mathtt{when}\ B\ \mathtt{do}\ C\ \{Q\}}$$

$$\mathit{RI} \triangleq (\mathsf{emp} \wedge \neg \mathit{full}) \vee (c \mapsto - \wedge \mathit{full})$$

$\{\mathsf{emp}\}$

$\texttt{resource}\ \mathit{buf}(c, \mathit{full} := \texttt{false});$

$\{\mathsf{emp} * \mathsf{emp} * \mathit{RI}\}$

$\{\mathsf{emp}\}$

$x := \texttt{cons}(-);$

$\{x \mapsto -\}$

$\texttt{with}\ \mathit{buf}\ \texttt{when}\ \neg \mathit{full}\ \texttt{do}$

$\{(x \mapsto -) * (\mathsf{emp} \wedge \neg \mathit{full})\}$

$c := x;\ \mathit{full} := \texttt{true};$

$\{(c \mapsto -) * (\mathsf{emp} \wedge \mathit{full})\}$

$\{\mathsf{emp} * \mathit{RI}\}$

$\texttt{endwith};$

$\{\mathsf{emp}\}$

$\texttt{dispose}(x);$

$\{???\}$

$\|$

$\{\mathsf{emp}\}$

$\texttt{with}\ \mathit{buf}\ \texttt{when}\ \mathit{full}\ \texttt{do}$

$\{\mathsf{emp} * ((c \mapsto -) \wedge \mathit{full})\}$

$y := c;\ \mathit{full} := \texttt{false}$

$\{(y \mapsto -) * (\mathsf{emp} \wedge \neg \mathit{full})\}$

$\texttt{endwith};$

$\{y \mapsto -\}$

$\texttt{dispose}(y);$

$\{\mathsf{emp}\}$

$$\frac{\{(P * \mathit{RI}_r) \wedge B\}\ C\ \{Q * \mathit{RI}_r\}}{\{P\}\ \texttt{with}\ r\ \texttt{when}\ B\ \texttt{do}\ C\ \{Q\}}$$

$$\mathit{RI} \triangleq (\mathsf{emp} \wedge \neg \mathit{full}) \vee (c \mapsto - \wedge \mathit{full})$$

$\{\mathtt{emp}\}$

$\mathtt{resource}\ \mathit{buf}(c, \mathit{full} := \mathtt{false});$

$\{\mathtt{emp} * \mathtt{emp} * \mathit{RI}\}$

$\{\mathtt{emp}\}$	$\{\mathtt{emp}\}$
$x := \mathtt{cons}(-);$	$\mathtt{with}\ \mathit{buf}\ \mathtt{when}\ \mathit{full}\ \mathtt{do}$
$\{x \mapsto -\}$	$\quad\{\mathtt{emp} * ((c \mapsto -) \wedge \mathit{full})\}$
$\mathtt{with}\ \mathit{buf}\ \mathtt{when}\ \neg \mathit{full}\ \mathtt{do}$	$\quad y := c;\ \mathit{full} := \mathtt{false}$
$\quad\{(x \mapsto -) * (\mathtt{emp} \wedge \neg \mathit{full})\}$	$\quad\{(y \mapsto -) * (\mathtt{emp} \wedge \neg \mathit{full})\}$
$\quad c := x;\ \mathit{full} := \mathtt{true};$	$\mathtt{endwith};$
$\quad\{(c \mapsto -) * (\mathtt{emp} \wedge \mathit{full})\}$	$\{y \mapsto -\}$
$\quad\{\mathtt{emp} * \mathit{RI}\}$	$\mathtt{dispose}(y);$
$\mathtt{endwith};$	$\{\mathtt{emp}\}$
$\{\mathtt{emp}\}$	

$\{RI\}$

$$\frac{\{(P * RI_r) \wedge B\}\ C\ \{Q * RI_r\}}{\{P\}\ \mathtt{with}\ r\ \mathtt{when}\ B\ \mathtt{do}\ C\ \{Q\}}$$

$$RI \quad \triangleq \quad (\mathtt{emp} \wedge \neg \mathit{full}) \vee (c \mapsto - \wedge \mathit{full})$$

The Reynolds Counterexample

$\texttt{resource}\ r()$ $\quad$ *invariant* $RI_r = \texttt{true}$

From

$$\dfrac{\dfrac{\{\texttt{true}\}\texttt{skip}\{\texttt{true}\}}{\{(\texttt{emp} \vee \texttt{one}) * \texttt{true}\}\texttt{skip}\{\texttt{emp} * \texttt{true}\}}}{\{\texttt{emp} \vee \texttt{one}\}\texttt{with}\ r\ \texttt{when true do skip}\ \{\texttt{emp}\}}$$

We obtain an inconsistency

$$\dfrac{\dfrac{\dfrac{\dfrac{\{\texttt{emp} \vee \texttt{one}\}\texttt{with} \cdots\ \{\texttt{emp}\}}{\{\texttt{emp}\}\texttt{with} \cdots\ \{\texttt{emp}\}}}{\{\texttt{emp} * \texttt{one}\}\texttt{with} \cdots\ \{\texttt{emp} * \texttt{one}\}}}{\{\texttt{one}\}\texttt{with} \cdots \{\texttt{one}\}} \qquad \dfrac{\{\texttt{emp} \vee \texttt{one}\}\texttt{with} \cdots\ \{\texttt{emp}\}}{\{\texttt{one}\}\texttt{with} \cdots \{\texttt{emp}\}}}{\{\texttt{one} \wedge \texttt{one}\}\texttt{with}\ r\ \texttt{when true do skip}\ \{\texttt{emp} \wedge \texttt{one}\}}}{\{\texttt{one}\}\texttt{with}\ r\ \texttt{when true do skip}\ \{\texttt{false}\}}$$