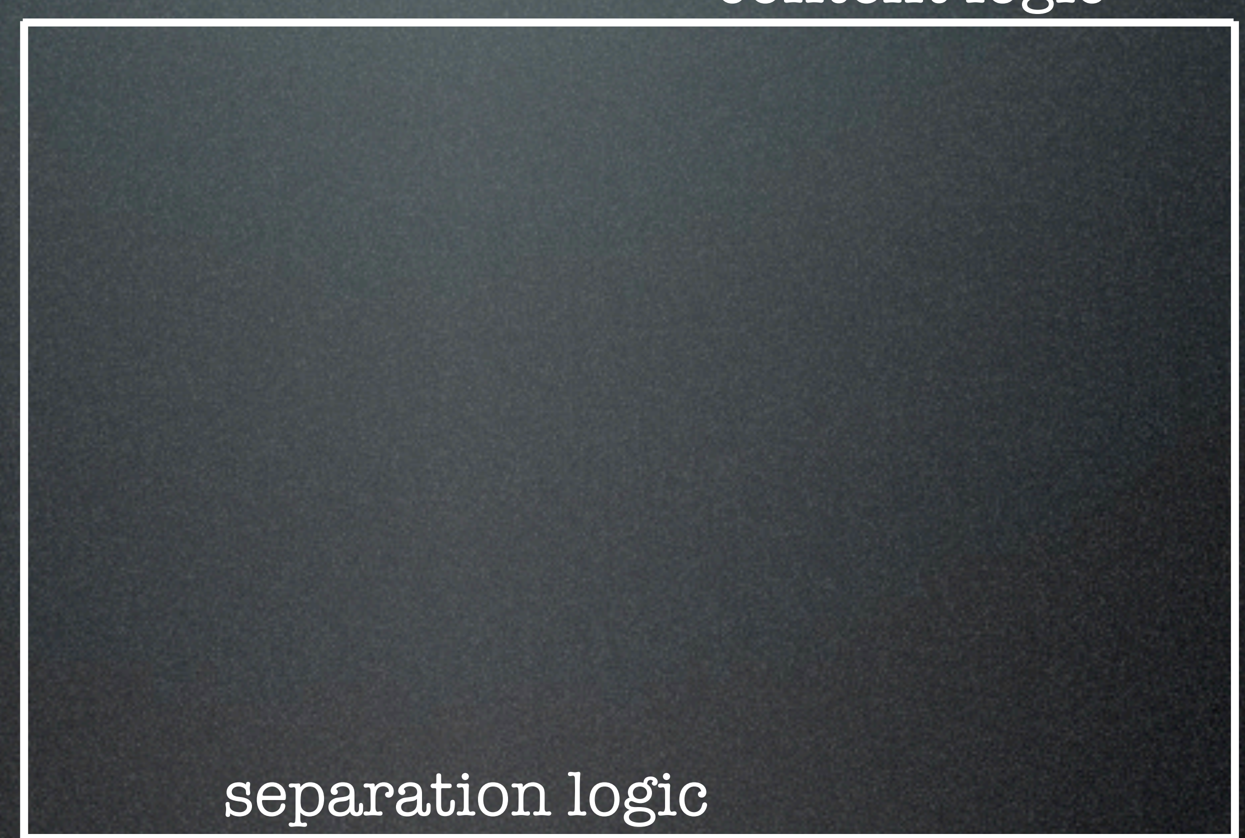
Concurrency at the Abstract Level

Mark Wheelhouse
James Kearney
Philippa Gardner

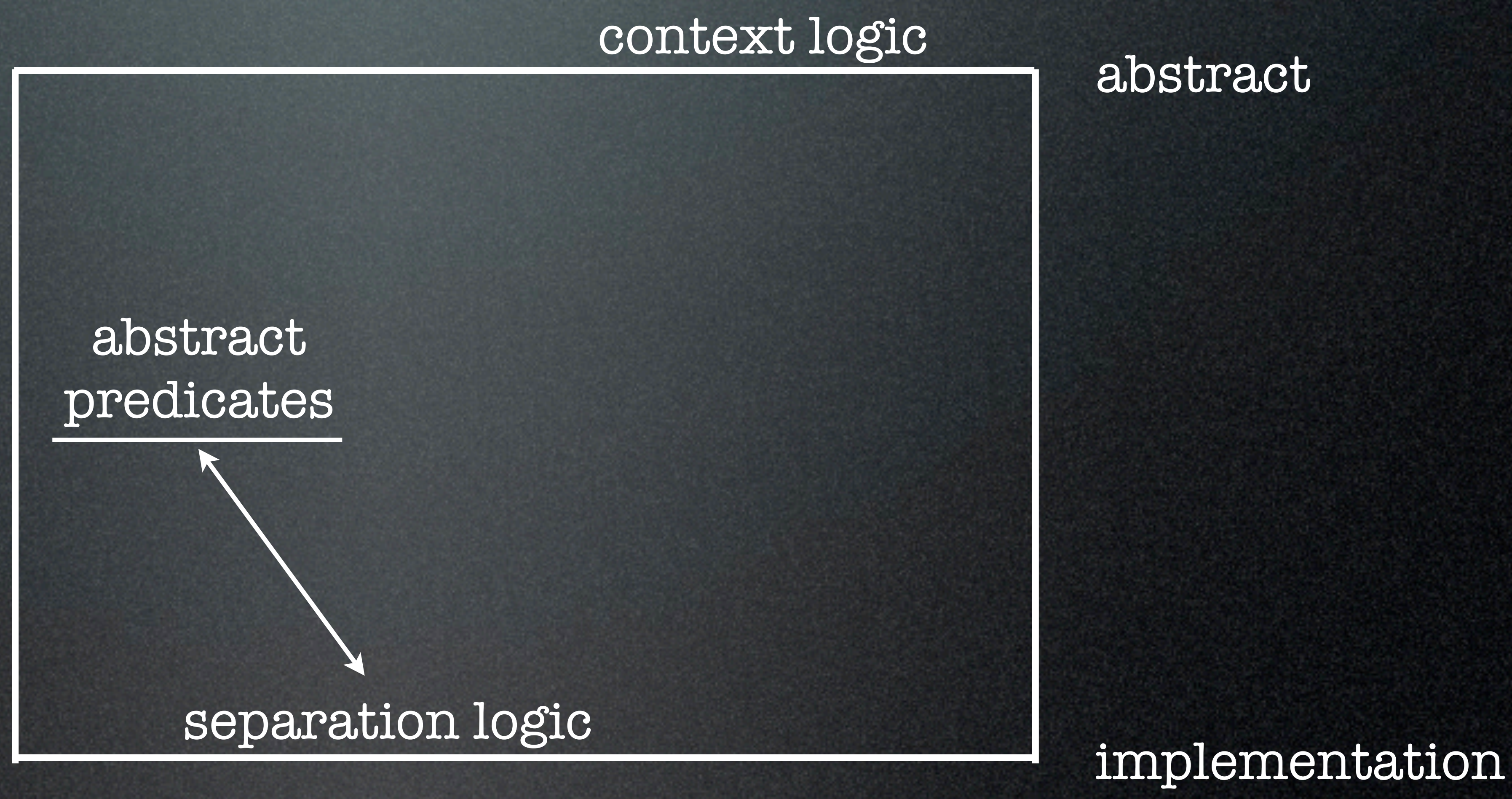
Imperial College London

Cambridge Concurrency Workshop - July 2010

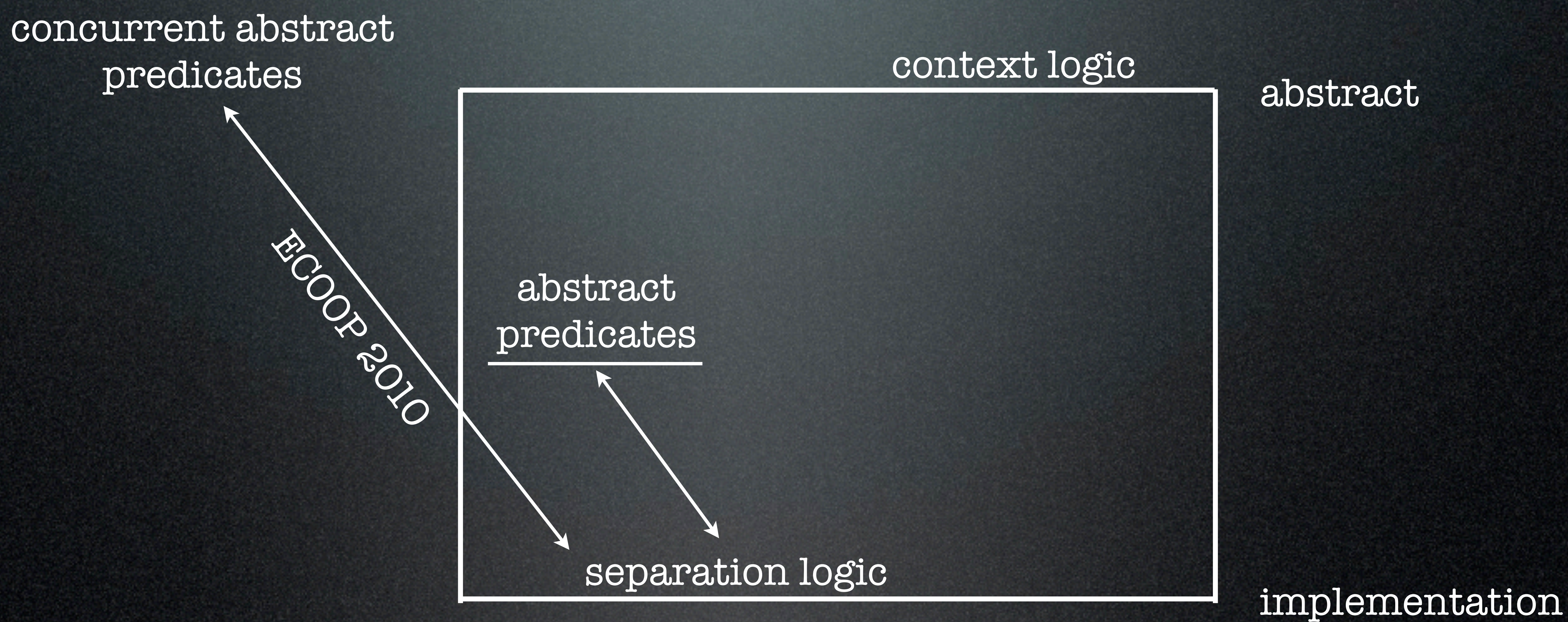
Abstraction Levels



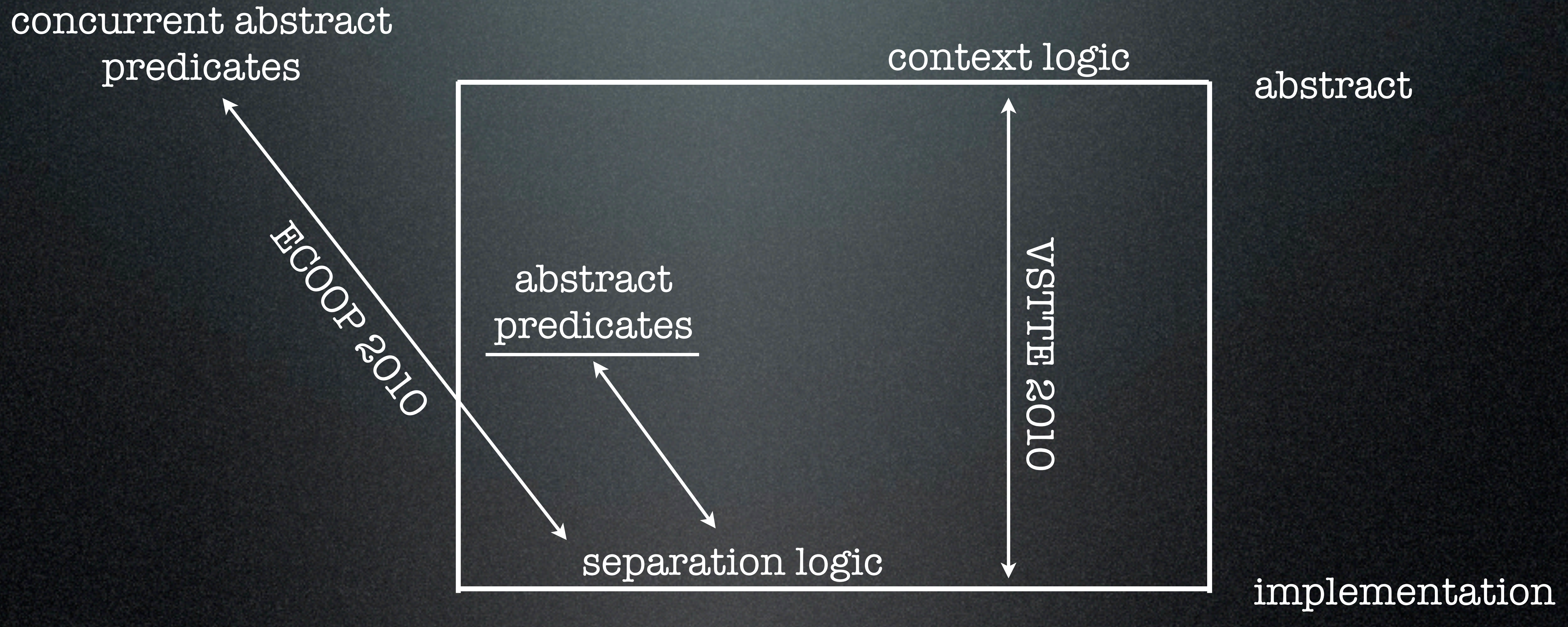
Abstraction Levels



Abstraction Levels



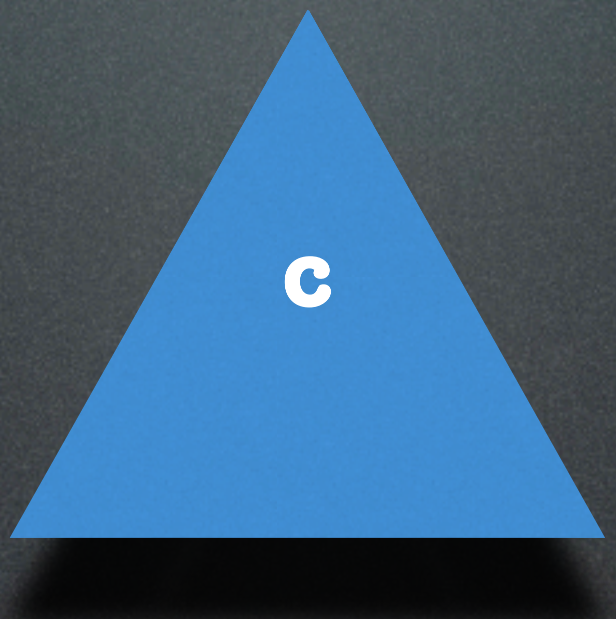
Abstraction Levels



Abstract Local Reasoning - Contexts

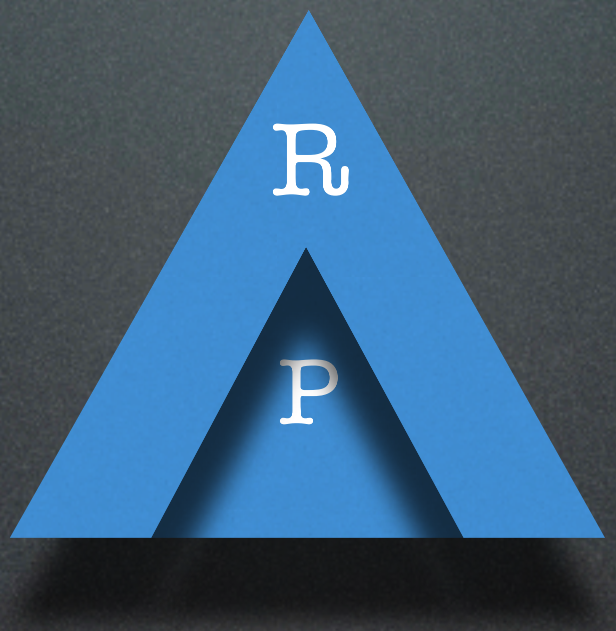
app not commutative

Abstract Local Reasoning - Contexts



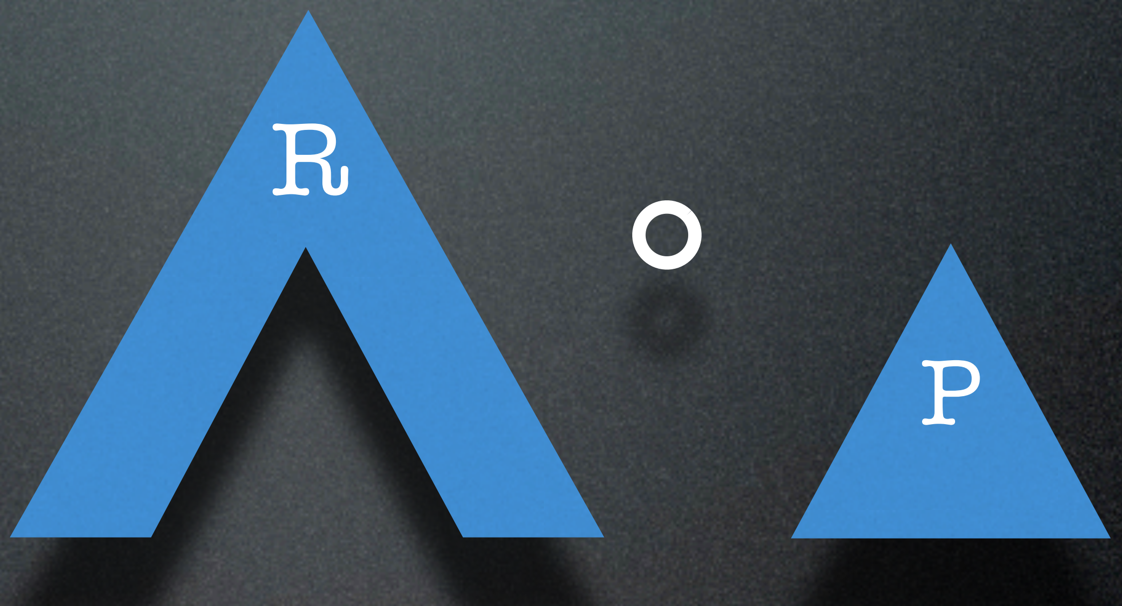
app not commutative

Abstract Local Reasoning - Contexts



app not commutative

Abstract Local Reasoning - Contexts



separating application

app not commutative

Abstract Local Reasoning - Contexts

separating application

app not commutative

Abstract Local Reasoning - Contexts

separating application

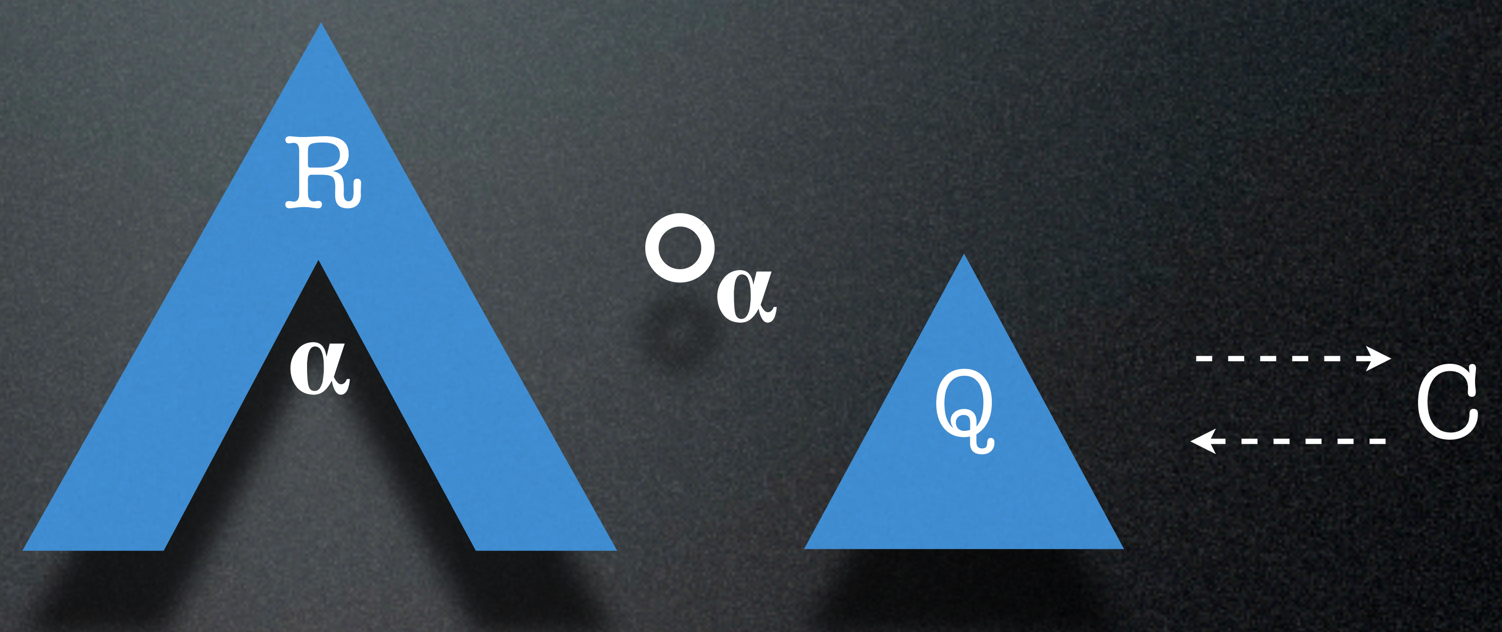
app not commutative

Abstract Local Reasoning - Contexts

separating application

app not commutative

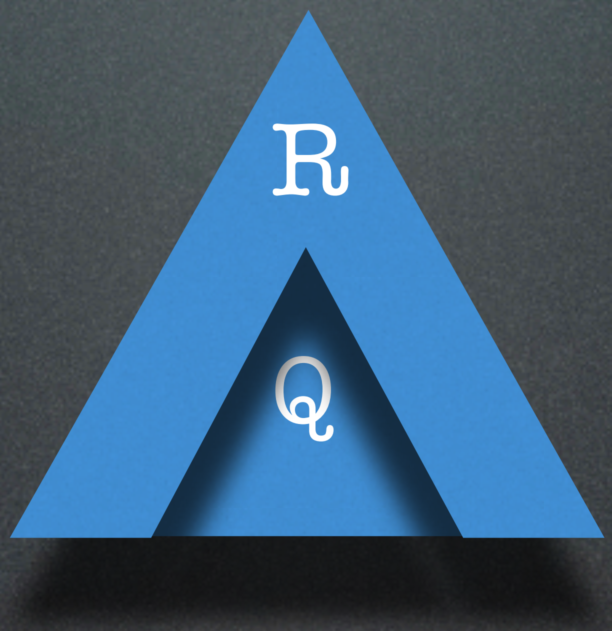
Abstract Local Reasoning - Contexts



separating application

app not commutative

Abstract Local Reasoning - Contexts



separating application

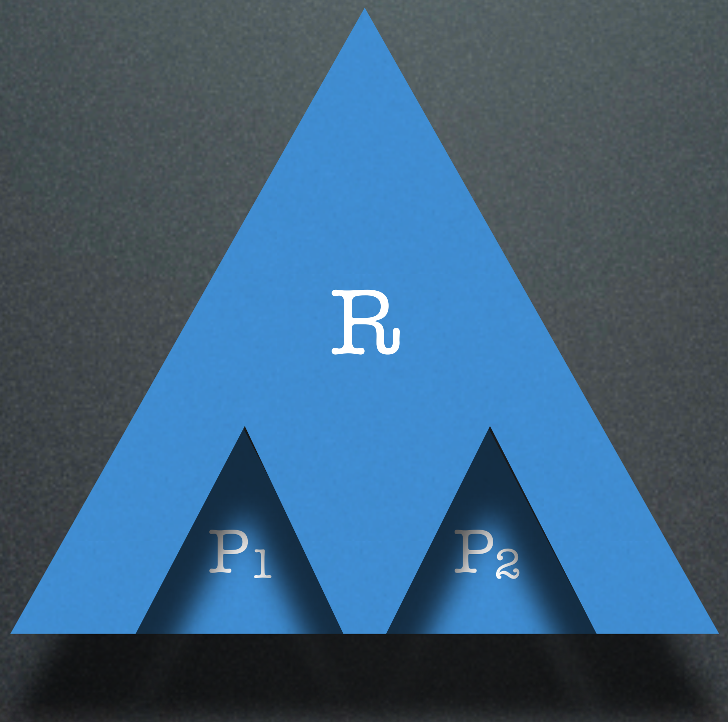
app not commutative

Reasoning About Concurrency

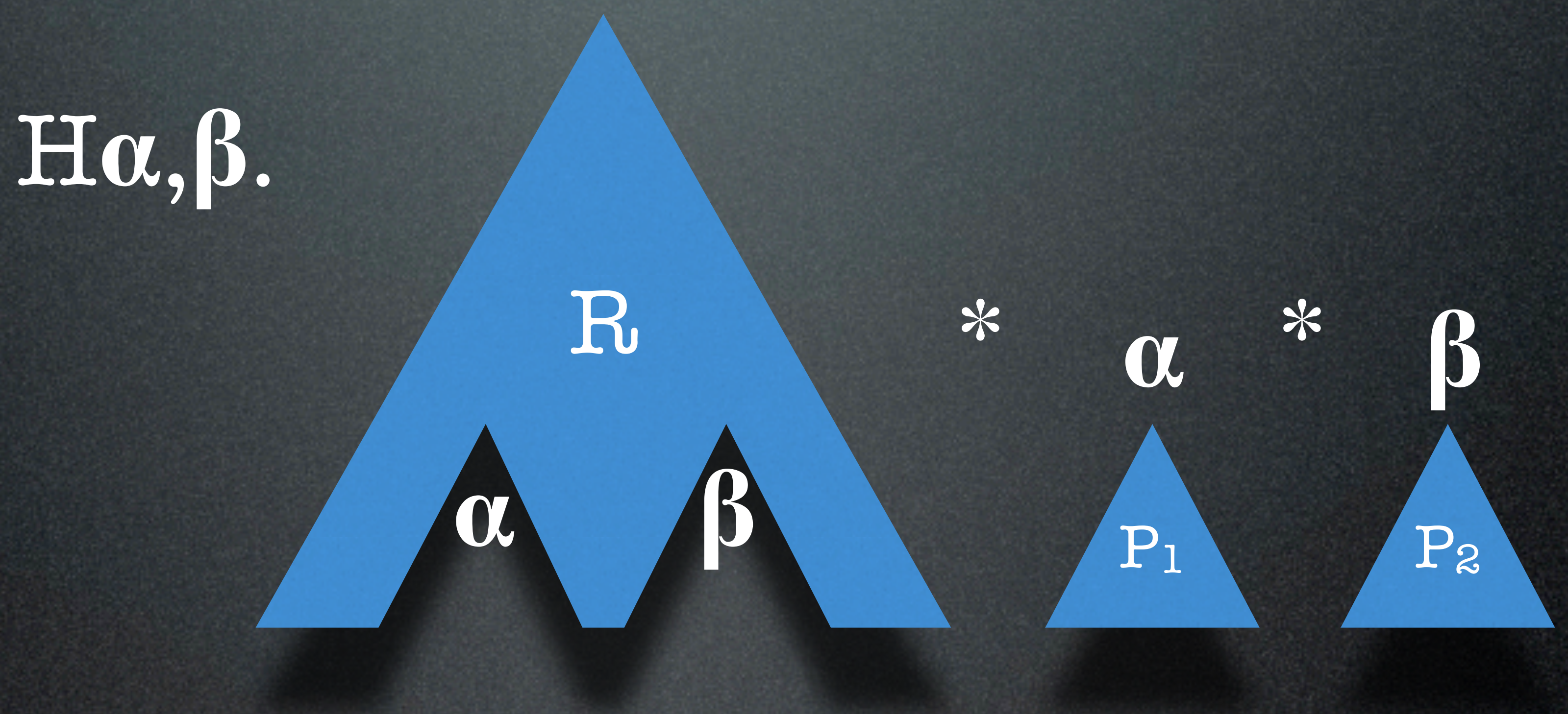
deleteTree(**n**) || deleteTree(**m**)

DOM IDs n & m

Abstract Local Reasoning - Segments



Abstract Local Reasoning - Segments



separating conjunction
abstract heap addresses
abstract wiring

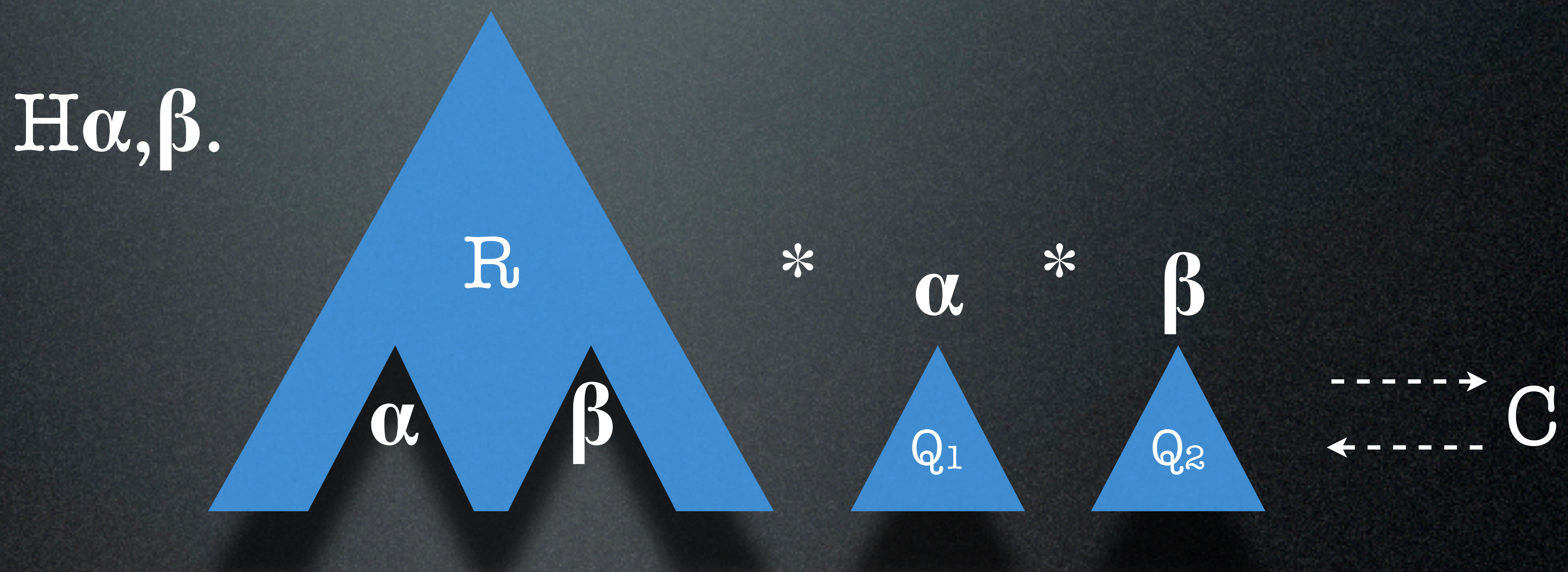
Abstract Local Reasoning - Segments

separating conjunction
abstract heap addresses
abstract wiring

Abstract Local Reasoning - Segments

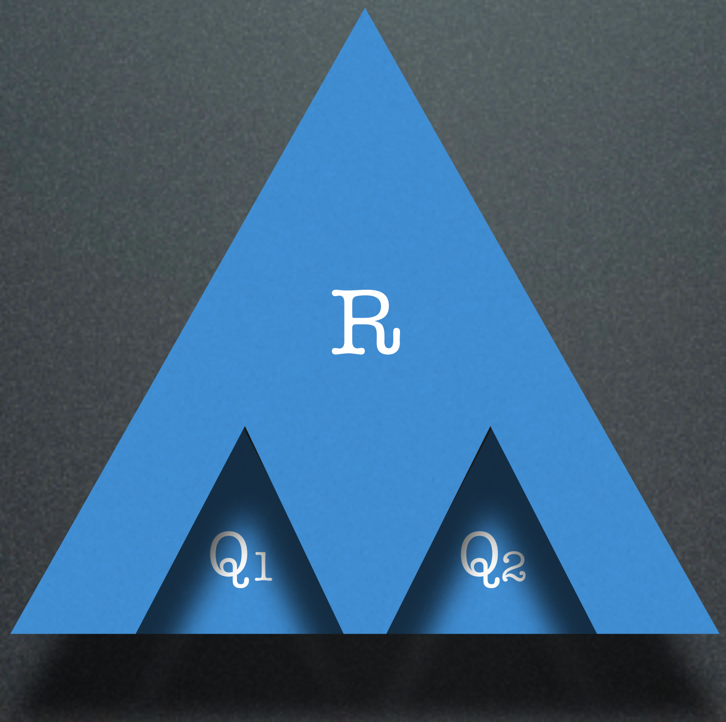
separating conjunction
abstract heap addresses
abstract wiring

Abstract Local Reasoning - Segments



separating conjunction
abstract heap addresses
abstract wiring

Abstract Local Reasoning - Segments



separating conjunction
abstract heap addresses
abstract wiring

Concurrent Update Language

skip

x := Exp

C_{Basic}

C ; C

if B then C else C

while B do C

C || C

res r in C

with r when B do C

Tree Segments

tree context $\mathbf{c} ::= \mathbf{0} \mid \mathbf{x} \mid \mathbf{n}[\mathbf{c}] \mid \mathbf{c} \otimes \mathbf{c}$

tree segment $\mathbf{s} ::= \emptyset \mid \mathbf{x} \leftarrow \mathbf{c} \mid \mathbf{s} + \mathbf{s} \mid (\mathbf{x})(\mathbf{s})$

Unique node identifiers **n**

Unique free hole addresses **x**

Unique free hole labels **x**

$+$ associative & commutative with unit $\emptyset$

$\otimes$ associative with unit $\emptyset$

restriction familar
from pi calculus

Tree Segments

tree context $\mathbf{c} ::= \mathbf{0} \mid \mathbf{x} \mid \mathbf{n}[\mathbf{c}] \mid \mathbf{c} \otimes \mathbf{c}$

tree segment $\mathbf{s} ::= \emptyset \mid \mathbf{x} \leftarrow \mathbf{c} \mid \mathbf{s} + \mathbf{s} \mid (\mathbf{x})(\mathbf{s})$

Unique node identifiers **n**

Unique free hole addresses **x**

Unique free hole labels **x**

+ associative & commutative with unit $\emptyset$

$\otimes$ associative with unit $\emptyset$

& no cycles!

restriction familar
from pi calculus

Tree Segment Formulae

emp	no segments.
$\alpha \leftarrow T$	tree segment satisfying T at address α.
$P * Q$	separating conjunction. disjoint segments P and Q.
$H\alpha.P$	hiding quanti… α restricted i…

standard pi-calc hiding
restriction + freshness
(existence not enough)

Sequential Abstract Local Reasoning

Fault Avoiding
Partial Correctness: $\{ P \}\ C\ \{ Q \}$

Small Axioms

$$\{ \alpha \leftarrow \mathbf{n}[\mathbf{t}] \}$$
$$\text{deleteTree}(\mathbf{n})$$
$$\{ \alpha \leftarrow \mathbf{0} \}$$

$$\{ \alpha \leftarrow \mathbf{n}[\gamma] \ * \ \beta \leftarrow \mathbf{m}[\mathbf{t}] \}$$
$$\text{append}(\mathbf{n}, \mathbf{m})$$
$$\{ \alpha \leftarrow \mathbf{n}[\ \gamma \otimes \mathbf{m}[\mathbf{t}]\ ] \ * \ \beta \leftarrow \mathbf{0} \}$$

Frame Rules

Separation Frame

$$\frac{\{\, P \,\}\ C\ \{\, Q \,\}}{\{\, R * P \,\}\ C\ \{\, R * Q \,\}}$$

Hiding Introduction

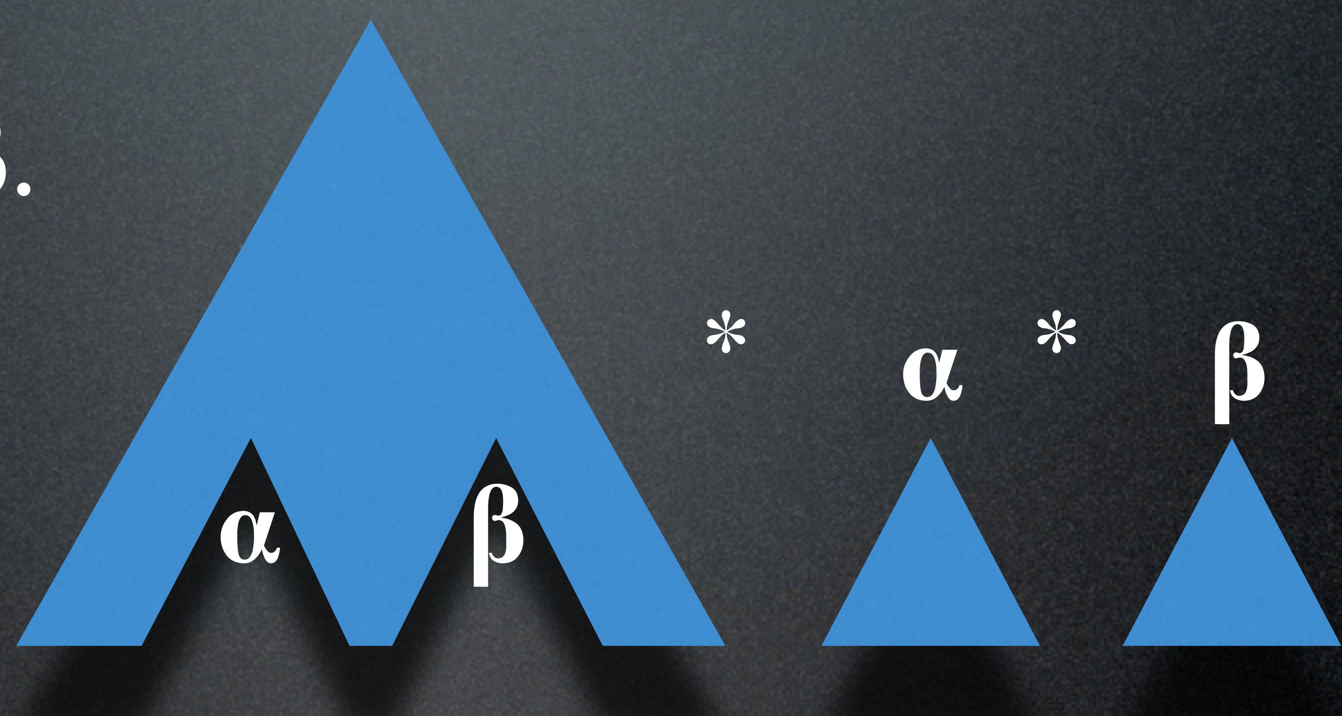
$$\frac{\{\, P \,\}\ C\ \{\, Q \,\}}{\{\, H\alpha.P \,\}\ C\ \{\, H\alpha.Q \,\}}$$

(Derived)

Local Reasoning

Local Reasoning

Hα,β.



Local Reasoning

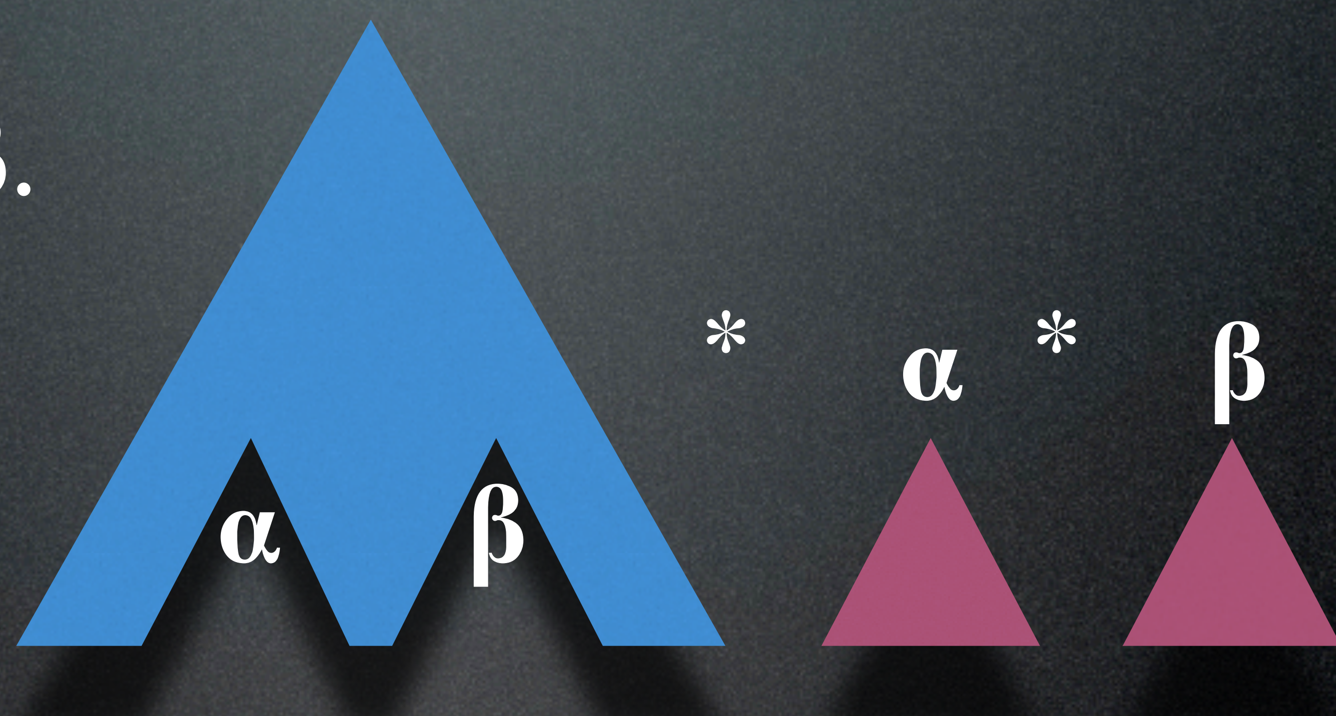
Local Reasoning

Local Reasoning

Local Reasoning

Local Reasoning

Hα,β.



Local Reasoning

Concurrent Abstract Local Reasoning

Disjoint Concurrency

$$\frac{\Gamma \vdash \{\ P_1\ \}\ C_1\ \{\ Q_1\ \} \qquad \Gamma \vdash \{\ P_2\ \}\ C_2\ \{\ Q_2\ \}}{\Gamma \vdash \{\ P_1 * P_2\ \}\ C_1 || C_2\ \{\ Q_1 * Q_2\ \}}\ \text{PAR}$$

Disjoint Concurrency Example

deleteTree(**n**) || deleteTree(**m**)

Disjoint Concurrency Example

$$\{\ \alpha \leftarrow \mathbf{n}[\mathbf{t}]\ * \ \beta \leftarrow \mathbf{m}[\mathbf{t'}]\ \}$$

deleteTree(**n**)	‖	deleteTree(**m**)

Disjoint Concurrency Example

$$\{\ \alpha \leftarrow \mathbf{n}[\mathbf{t}]\ \ast\ \beta \leftarrow \mathbf{m}[\mathbf{t'}]\ \}$$

$\{\ \alpha \leftarrow \mathbf{n}[\mathbf{t}]\ \}$ $\quad\|\quad$ $\{\ \beta \leftarrow \mathbf{m}[\mathbf{t'}]\ \}$

deleteTree(**n**) $\quad\|\quad$ deleteTree(**m**)

Disjoint Concurrency Example

$$\{\ \alpha \leftarrow \mathbf{n}[\mathbf{t}]\ *\ \beta \leftarrow \mathbf{m}[\mathbf{t'}]\ \}$$

$\{\ \alpha \leftarrow \mathbf{n}[\mathbf{t}]\ \}$	$\|\|$	$\{\ \beta \leftarrow \mathbf{m}[\mathbf{t'}]\ \}$
deleteTree(**n**)		deleteTree(**m**)
$\{\ \alpha \leftarrow \mathbf{0}\ \}$		$\{\ \beta \leftarrow \mathbf{0}\ \}$

Disjoint Concurrency Example

$$\{\ \alpha \leftarrow \mathbf{n}[\mathbf{t}]\ *\ \beta \leftarrow \mathbf{m}[\mathbf{t'}]\ \}$$

$\{\ \alpha \leftarrow \mathbf{n}[\mathbf{t}]\ \}$	$\parallel$	$\{\ \beta \leftarrow \mathbf{m}[\mathbf{t'}]\ \}$
deleteTree(**n**)	$\parallel$	deleteTree(**m**)
$\{\ \alpha \leftarrow \mathbf{0}\ \}$	$\parallel$	$\{\ \beta \leftarrow \mathbf{0}\ \}$

$$\{\ \alpha \leftarrow \mathbf{0}\ *\ \beta \leftarrow \mathbf{0}\ \}$$

Concurrent Abstract Local Reasoning

Sharing Program State

$$\frac{\Gamma(r \rightarrow \Pi, RI) \vdash \{\ P\ \}\ \ C\ \ \{\ Q\ \}}{\Gamma \vdash \{\ H\Pi.(RI * P)\ \}\ \ \text{res}\ \ r\ \ \text{in}\ \ C\ \{\ H\Pi.(RI * Q)\ \}}\ \text{RES}$$

$$\frac{\Gamma \vdash \{\ H\Pi.(RI * P\ ) \wedge B\ \}\ C\ \ \{H\Pi.(RI * Q)\ \}}{\Gamma(r \rightarrow \Pi, RI) \vdash \{\ P\ \}\ \ \text{with}\ \ r\ \ \text{when}\ \ B\ \ \text{do}\ \ C\ \{\ Q\ \}}\ \text{CCR}$$

Shared State Example

```
                 res r in

with r do ⟨                ||   with r do ⟨
    a:= getLeft(n)         ||       b:= getRight(n)
⟩                          ||   ⟩
deleteTree(a)              ||   deleteTree(b)
```

Shared State Example

$$\{\ \alpha \leftarrow \mathbf{p}[\mathbf{t}] \otimes \mathbf{n}[\gamma] \otimes \mathbf{q}[\mathbf{t'}]\ \}$$

res r in

with r do ⟨	‖	with r do ⟨
a := getLeft(**n**)	‖	b := getRight(**n**)
⟩	‖	⟩
deleteTree(a)	‖	deleteTree(b)

$$\{\ \alpha \leftarrow \mathbf{n}[\gamma]\ \}$$

Shared State Example

$\{ \alpha \leftarrow \mathbf{p}[\mathbf{t}] \otimes \mathbf{n}[\gamma] \otimes \mathbf{q}[\mathbf{t'}] \}$

res r in $\langle$

$$\vdots \quad \| \quad \vdots$$

$\rangle$

Shared State Example

$\{\ \alpha \leftarrow \mathbf{p}[\mathbf{t}] \otimes \mathbf{n}[\gamma] \otimes \mathbf{q}[\mathbf{t'}]\ \}$

$\{\ \mathrm{H}\ \boldsymbol{\beta},\boldsymbol{\delta}.(\ \alpha \leftarrow \boldsymbol{\beta} \otimes \mathbf{n}[\gamma] \otimes \boldsymbol{\delta}\ *\ \boldsymbol{\beta} \leftarrow \mathbf{p}[\mathbf{t}]\ *\ \boldsymbol{\delta} \leftarrow \mathbf{q}[\mathbf{t'}]\ )\ \}$

res r in $\langle$

$$\vdots \quad \Big\| \quad \vdots$$

$\rangle$

Shared State Example

$\{\ \alpha \leftarrow \mathbf{p}[\mathbf{t}] \otimes \mathbf{n}[\gamma] \otimes \mathbf{q}[\mathbf{t'}]\ \}$

$\{\ \mathrm{H}\ \beta,\delta.(\ \alpha \leftarrow \beta \otimes \mathbf{n}[\gamma] \otimes \delta\ *\ \beta \leftarrow \mathbf{p}[\mathbf{t}]\ *\ \delta \leftarrow \mathbf{q}[\mathbf{t'}]\ )\ \}$

res r in $\langle$

$\mathrm{RI} = \alpha \leftarrow \beta \otimes \mathbf{n}[\gamma] \otimes \delta$

$\Pi = \beta,\delta$

$\vdots \quad \| \quad \vdots$

$\rangle$

Shared State Example

$\{\ \alpha \leftarrow \mathbf{p}[\mathbf{t}] \otimes \mathbf{n}[\gamma] \otimes \mathbf{q}[\mathbf{t'}]\ \}$

$\{\ \exists\ \beta,\delta.(\ \alpha \leftarrow \beta \otimes \mathbf{n}[\gamma] \otimes \delta\ *\ \beta \leftarrow \mathbf{p}[\mathbf{t}]\ *\ \delta \leftarrow \mathbf{q}[\mathbf{t'}]\ )\ \}$

res r in $\langle$

$\{\ \beta \leftarrow \mathbf{p}[\mathbf{t}]\ *\ \delta \leftarrow \mathbf{q}[\mathbf{t'}]\ \}$

$\vdots \quad \| \quad \vdots$

$\rangle$

$RI = \alpha \leftarrow \beta \otimes \mathbf{n}[\gamma] \otimes \delta$

$\Pi = \beta,\delta$

Shared State Example

$\{\ \alpha \leftarrow \mathbf{p}[\mathbf{t}] \otimes \mathbf{n}[\gamma] \otimes \mathbf{q}[\mathbf{t'}]\ \}$

$\{\ \exists\, \beta,\delta.(\ \alpha \leftarrow \beta \otimes \mathbf{n}[\gamma] \otimes \delta\ *\ \beta \leftarrow \mathbf{p}[\mathbf{t}]\ *\ \delta \leftarrow \mathbf{q}[\mathbf{t'}]\ )\ \}$

res r in $\langle$

$\{\ \beta \leftarrow \mathbf{p}[\mathbf{t}]\ *\ \delta \leftarrow \mathbf{q}[\mathbf{t'}]\ \}$

$$\begin{array}{c|c} \{\ \beta \leftarrow \mathbf{p}[\mathbf{t}]\ \} & \{\ \delta \leftarrow \mathbf{q}[\mathbf{t'}]\ \} \\ \vdots & \vdots \\ \{\ \beta \leftarrow \mathbf{0}\ \} & \{\ \delta \leftarrow \mathbf{0}\ \} \end{array}$$

$\rangle$

$\mathrm{RI} = \alpha \leftarrow \beta \otimes \mathbf{n}[\gamma] \otimes \delta$

$\Pi = \beta,\delta$

Shared State Example

$\{\ \alpha \leftarrow \mathbf{p}[\mathbf{t}] \otimes \mathbf{n}[\gamma] \otimes \mathbf{q}[\mathbf{t'}]\ \}$

$\{\ \exists\ \beta,\delta.(\ \alpha \leftarrow \beta \otimes \mathbf{n}[\gamma] \otimes \delta\ *\ \beta \leftarrow \mathbf{p}[\mathbf{t}]\ *\ \delta \leftarrow \mathbf{q}[\mathbf{t'}]\ )\ \}$

res r in $\langle$

$\{\ \beta \leftarrow \mathbf{p}[\mathbf{t}]\ *\ \delta \leftarrow \mathbf{q}[\mathbf{t'}]\ \}$

$\{\ \beta \leftarrow \mathbf{p}[\mathbf{t}]\ \}$	$\|$	$\{\ \delta \leftarrow \mathbf{q}[\mathbf{t'}]\ \}$
$\vdots$	$\|$	$\vdots$
$\{\ \beta \leftarrow \mathbf{0}\ \}$	$\|$	$\{\ \delta \leftarrow \mathbf{0}\ \}$

$\{\ \beta \leftarrow \mathbf{0}\ *\ \delta \leftarrow \mathbf{0}\ \}$

$\rangle$

RI $= \alpha \leftarrow \beta \otimes \mathbf{n}[\gamma] \otimes \delta$

$\Pi = \beta,\delta$

Shared State Example

$\{\ \alpha \leftarrow \mathbf{p}[\mathbf{t}] \otimes \mathbf{n}[\gamma] \otimes \mathbf{q}[\mathbf{t'}]\ \}$

$\{\ \text{Ħ}\, \beta,\delta.(\ \alpha \leftarrow \beta \otimes \mathbf{n}[\gamma] \otimes \delta\ *\ \beta \leftarrow \mathbf{p}[\mathbf{t}]\ *\ \delta \leftarrow \mathbf{q}[\mathbf{t'}]\ )\ \}$

res r in $\langle$

$\{\ \beta \leftarrow \mathbf{p}[\mathbf{t}]\ *\ \delta \leftarrow \mathbf{q}[\mathbf{t'}]\ \}$

$$\begin{array}{c|c} \{\ \beta \leftarrow \mathbf{p}[\mathbf{t}]\ \} & \{\ \delta \leftarrow \mathbf{q}[\mathbf{t'}]\ \} \\ \vdots & \vdots \\ \{\ \beta \leftarrow \mathbf{0}\ \} & \{\ \delta \leftarrow \mathbf{0}\ \} \end{array}$$

$\{\ \beta \leftarrow \mathbf{0}\ *\ \delta \leftarrow \mathbf{0}\ \}$

$\rangle$

$\{\ \text{Ħ}\, \beta,\delta.(\ \alpha \leftarrow \beta \otimes \mathbf{n}[\gamma] \otimes \delta\ *\ \beta \leftarrow \mathbf{0}\ *\ \delta \leftarrow \mathbf{0}\ )\ \}$

$RI = \alpha \leftarrow \beta \otimes \mathbf{n}[\gamma] \otimes \delta$

$\Pi = \beta,\delta$

Shared State Example

$\{\ \alpha \leftarrow \mathbf{p}[\mathbf{t}] \otimes \mathbf{n}[\gamma] \otimes \mathbf{q}[\mathbf{t'}]\ \}$

$\{\ \exists\ \beta,\delta.(\ \alpha \leftarrow \beta \otimes \mathbf{n}[\gamma] \otimes \delta \ * \ \beta \leftarrow \mathbf{p}[\mathbf{t}] \ * \ \delta \leftarrow \mathbf{q}[\mathbf{t'}]\ )\ \}$

res r in $\langle$

$\{\ \beta \leftarrow \mathbf{p}[\mathbf{t}] \ * \ \delta \leftarrow \mathbf{q}[\mathbf{t'}]\ \}$

$\{\ \beta \leftarrow \mathbf{p}[\mathbf{t}]\ \} \quad \| \quad \{\ \delta \leftarrow \mathbf{q}[\mathbf{t'}]\ \}$

$\vdots \qquad \vdots$

$\{\ \beta \leftarrow \mathbf{0}\ \} \quad \| \quad \{\ \delta \leftarrow \mathbf{0}\ \}$

$\{\ \beta \leftarrow \mathbf{0} \ * \ \delta \leftarrow \mathbf{0}\ \}$

$\rangle$

$\{\ \exists\ \beta,\delta.(\ \alpha \leftarrow \beta \otimes \mathbf{n}[\gamma] \otimes \delta \ * \ \beta \leftarrow \mathbf{0} \ * \ \delta \leftarrow \mathbf{0}\ )\ \}$

$\{\ \alpha \leftarrow \mathbf{0} \otimes \mathbf{n}[\gamma] \otimes \mathbf{0}\ \}$

RI $= \alpha \leftarrow \beta \otimes \mathbf{n}[\gamma] \otimes \delta$

$\Pi = \beta,\delta$

Shared State Example

$\{\ \alpha \leftarrow \mathbf{p}[\mathbf{t}] \otimes \mathbf{n}[\gamma] \otimes \mathbf{q}[\mathbf{t'}]\ \}$

$\{\ \exists\ \beta,\delta.(\ \alpha \leftarrow \beta \otimes \mathbf{n}[\gamma] \otimes \delta\ *\ \beta \leftarrow \mathbf{p}[\mathbf{t}]\ *\ \delta \leftarrow \mathbf{q}[\mathbf{t'}]\ )\ \}$

res r in $\langle$

$\{\ \beta \leftarrow \mathbf{p}[\mathbf{t}]\ *\ \delta \leftarrow \mathbf{q}[\mathbf{t'}]\ \}$

$\{\ \beta \leftarrow \mathbf{p}[\mathbf{t}]\ \}\ \ \Vert\ \ \{\ \delta \leftarrow \mathbf{q}[\mathbf{t'}]\ \}$

$\vdots \qquad\qquad \vdots$

$\{\ \beta \leftarrow \mathbf{0}\ \}\ \ \Vert\ \ \{\ \delta \leftarrow \mathbf{0}\ \}$

$\{\ \beta \leftarrow \mathbf{0}\ *\ \delta \leftarrow \mathbf{0}\ \}$

$\rangle$

$\{\ \exists\ \beta,\delta.(\ \alpha \leftarrow \beta \otimes \mathbf{n}[\gamma] \otimes \delta\ *\ \beta \leftarrow \mathbf{0}\ *\ \delta \leftarrow \mathbf{0}\ )\ \}$

$\{\ \alpha \leftarrow \mathbf{0} \otimes \mathbf{n}[\gamma] \otimes \mathbf{0}\ \}$

$\{\ \alpha \leftarrow \mathbf{n}[\gamma]\ \}$

RI $= \alpha \leftarrow \beta \otimes \mathbf{n}[\gamma] \otimes \delta$

$\Pi = \beta,\delta$

Shared State Example

$\{\ \beta \leftarrow \mathbf{p}[\mathbf{t}]\ \}$
with r do $\langle$

a := getLeft($\mathbf{n}$)

$\rangle$

deleteTree(a)
$\{\ \beta \leftarrow \mathbf{0}\ \}$

$RI = \alpha \leftarrow \beta \otimes \mathbf{n}[\gamma] \otimes \delta$
$\Pi = \beta, \delta$

Shared State Example

$\{\ \beta \leftarrow \mathbf{p}[\mathbf{t}]\ \}$
with r do $\langle$
$\quad \{\ \mathrm{H}\Pi.(\mathrm{RI} * \beta \leftarrow \mathbf{p}[\mathbf{t}])\ \}$

$\quad$ a := getLeft($\mathbf{n}$)

$\rangle$

deleteTree(a)
$\{\ \beta \leftarrow \mathbf{0}\ \}$

$\mathrm{RI} = \alpha \leftarrow \beta \otimes \mathbf{n}[\gamma] \otimes \delta$
$\Pi = \beta, \delta$

Shared State Example

$\{\ \beta \leftarrow \mathbf{p}[\mathbf{t}]\ \}$

with r do $\langle$

$\{\ H\Pi.(RI * \beta \leftarrow \mathbf{p}[\mathbf{t}])\ \}$

$\{\ H\beta,\delta.(\alpha \leftarrow \beta \otimes \mathbf{n}[\gamma] \otimes \delta\ *\ \beta \leftarrow \mathbf{p}[\mathbf{t}])\ \}$

a := getLeft($\mathbf{n}$)

$\rangle$

deleteTree(a)

$\{\ \beta \leftarrow \mathbf{0}\ \}$

$RI = \alpha \leftarrow \beta \otimes \mathbf{n}[\gamma] \otimes \delta$

$\Pi = \beta,\delta$

Shared State Example

$RI = \alpha \leftarrow \beta \otimes \mathbf{n}[\gamma] \otimes \delta$
$\Pi = \beta,\delta$

$\{ \beta \leftarrow \mathbf{p}[\mathbf{t}] \}$
with r do $\langle$

$\{ H\Pi.(RI * \beta \leftarrow \mathbf{p}[\mathbf{t}]) \}$

$\{ H\beta,\delta.(\alpha \leftarrow \beta \otimes \mathbf{n}[\gamma] \otimes \delta \; * \; \beta \leftarrow \mathbf{p}[\mathbf{t}]) \}$

$\{ H\delta.(\alpha \leftarrow \mathbf{p}[\mathbf{t}] \otimes \mathbf{n}[\gamma] \otimes \delta) \}$

a := getLeft($\mathbf{n}$)

$\rangle$

deleteTree(a)
$\{ \beta \leftarrow \mathbf{0} \}$

Shared State Example

$RI = \alpha \leftarrow \beta \otimes \mathbf{n}[\gamma] \otimes \delta$

$\Pi = \beta,\delta$

$\{ \beta \leftarrow \mathbf{p}[\mathbf{t}] \}$

with r do $\langle$

$\{ H\Pi.(RI * \beta \leftarrow \mathbf{p}[\mathbf{t}]) \}$

$\{ H\beta,\delta.(\alpha \leftarrow \beta \otimes \mathbf{n}[\gamma] \otimes \delta \; * \; \beta \leftarrow \mathbf{p}[\mathbf{t}]) \}$

$\{ H\delta.(\alpha \leftarrow \mathbf{p}[\mathbf{t}] \otimes \mathbf{n}[\gamma] \otimes \delta) \}$

a := getLeft($\mathbf{n}$)

$\{ H\delta.(\alpha \leftarrow \mathbf{p}[\mathbf{t}] \otimes \mathbf{n}[\gamma] \otimes \delta \wedge (a=\mathbf{p})) \}$

$\rangle$

deleteTree(a)

$\{ \beta \leftarrow \mathbf{0} \}$

Shared State Example

$\{\ \beta \leftarrow \mathbf{p}[\mathbf{t}]\ \}$

with r do $\langle$

$\{\ H\Pi.(RI * \beta \leftarrow \mathbf{p}[\mathbf{t}])\ \}$

$\{\ H\beta,\delta.(\alpha \leftarrow \beta \otimes \mathbf{n}[\gamma] \otimes \delta\ *\ \beta \leftarrow \mathbf{p}[\mathbf{t}])\ \}$

$\{\ H\delta.(\alpha \leftarrow \mathbf{p}[\mathbf{t}] \otimes \mathbf{n}[\gamma] \otimes \delta)\ \}$

a := getLeft(**n**)

$\{\ H\delta.(\alpha \leftarrow \mathbf{p}[\mathbf{t}] \otimes \mathbf{n}[\gamma] \otimes \delta \wedge (a=\mathbf{p}))\ \}$

$\{\ H\beta,\delta.(\alpha \leftarrow \beta \otimes \mathbf{n}[\gamma] \otimes \delta\ *\ \beta \leftarrow \mathbf{p}[\mathbf{t}] \wedge (a=\mathbf{p}))\ \}$

$\rangle$

deleteTree(a)

$\{\ \beta \leftarrow \mathbf{0}\ \}$

$RI = \alpha \leftarrow \beta \otimes \mathbf{n}[\gamma] \otimes \delta$

$\Pi = \beta,\delta$

Shared State Example

$\{ \beta \leftarrow \mathbf{p}[\mathbf{t}] \}$

with r do $\langle$

$\{ H\Pi.(RI * \beta \leftarrow \mathbf{p}[\mathbf{t}]) \}$

$\{ H\beta,\delta.(\alpha \leftarrow \beta \otimes \mathbf{n}[\gamma] \otimes \delta \; * \; \beta \leftarrow \mathbf{p}[\mathbf{t}]) \}$

$\{ H\delta.(\alpha \leftarrow \mathbf{p}[\mathbf{t}] \otimes \mathbf{n}[\gamma] \otimes \delta) \}$

a := getLeft($\mathbf{n}$)

$\{ H\delta.(\alpha \leftarrow \mathbf{p}[\mathbf{t}] \otimes \mathbf{n}[\gamma] \otimes \delta \wedge (a=\mathbf{p})) \}$

$\{ H\beta,\delta.(\alpha \leftarrow \beta \otimes \mathbf{n}[\gamma] \otimes \delta \; * \; \beta \leftarrow \mathbf{p}[\mathbf{t}] \wedge (a=\mathbf{p})) \}$

$\{ H\Pi.(RI * \beta \leftarrow \mathbf{p}[\mathbf{t}] \wedge (a=\mathbf{p})) \}$

$\rangle$

deleteTree(a)

$\{ \beta \leftarrow \mathbf{0} \}$

$RI = \alpha \leftarrow \beta \otimes \mathbf{n}[\gamma] \otimes \delta$

$\Pi = \beta,\delta$

Shared State Example

$RI = \alpha \leftarrow \beta \otimes \mathbf{n}[\gamma] \otimes \delta$

$\Pi = \beta,\delta$

$\{ \beta \leftarrow \mathbf{p}[\mathbf{t}] \}$

with r do $\langle$

$\{ H\Pi.(RI * \beta \leftarrow \mathbf{p}[\mathbf{t}]) \}$

$\{ H\beta,\delta.(\alpha \leftarrow \beta \otimes \mathbf{n}[\gamma] \otimes \delta \; * \; \beta \leftarrow \mathbf{p}[\mathbf{t}]) \}$

$\{ H\delta.(\alpha \leftarrow \mathbf{p}[\mathbf{t}] \otimes \mathbf{n}[\gamma] \otimes \delta) \}$

a := getLeft(**n**)

$\{ H\delta.(\alpha \leftarrow \mathbf{p}[\mathbf{t}] \otimes \mathbf{n}[\gamma] \otimes \delta \wedge (a=\mathbf{p})) \}$

$\{ H\beta,\delta.(\alpha \leftarrow \beta \otimes \mathbf{n}[\gamma] \otimes \delta \; * \; \beta \leftarrow \mathbf{p}[\mathbf{t}] \wedge (a=\mathbf{p})) \}$

$\{ H\Pi.(RI * \beta \leftarrow \mathbf{p}[\mathbf{t}] \wedge (a=\mathbf{p})) \}$

$\rangle$

$\{ \beta \leftarrow \mathbf{p}[\mathbf{t}] \wedge (a=\mathbf{p}) \}$

deleteTree(a)

$\{ \beta \leftarrow \mathbf{0} \}$

Shared State Example

$RI = \alpha \leftarrow \beta \otimes \mathbf{n}[\gamma] \otimes \delta$

$\Pi = \beta,\delta$

$\{\ \beta \leftarrow \mathbf{p}[\mathbf{t}]\ \}$

with r do $\langle$

$\{\ H\Pi.(RI * \beta \leftarrow \mathbf{p}[\mathbf{t}])\ \}$

$\{\ H\beta,\delta.(\alpha \leftarrow \beta \otimes \mathbf{n}[\gamma] \otimes \delta\ *\ \beta \leftarrow \mathbf{p}[\mathbf{t}])\ \}$

$\{\ H\delta.(\alpha \leftarrow \mathbf{p}[\mathbf{t}] \otimes \mathbf{n}[\gamma] \otimes \delta)\ \}$

a := getLeft($\mathbf{n}$)

$\{\ H\delta.(\alpha \leftarrow \mathbf{p}[\mathbf{t}] \otimes \mathbf{n}[\gamma] \otimes \delta \wedge (a{=}\mathbf{p}))\ \}$

$\{\ H\beta,\delta.(\alpha \leftarrow \beta \otimes \mathbf{n}[\gamma] \otimes \delta\ *\ \beta \leftarrow \mathbf{p}[\mathbf{t}] \wedge (a{=}\mathbf{p}))\ \}$

$\{\ H\Pi.(RI * \beta \leftarrow \mathbf{p}[\mathbf{t}] \wedge (a{=}\mathbf{p}))\ \}$

$\rangle$

$\{\ \beta \leftarrow \mathbf{p}[\mathbf{t}] \wedge (a{=}\mathbf{p})\}$

deleteTree(a)

$\{\ \beta \leftarrow \mathbf{0}\ \}$

More Shared State

```
                    res r in

with r do ⟨                  ‖   with r do ⟨
    a := getLeft(n)          ‖       b := getRight(n)
    append(n, a)             ‖       append(n, b)
⟩                            ‖   ⟩
```

More Shared State

$$\{\ \alpha \leftarrow \mathbf{p}[\mathbf{t}] \otimes \mathbf{n}[\gamma] \otimes \mathbf{q}[\mathbf{t'}]\ \}$$

res r in

with r do ⟨
    a := getLeft(**n**)
    append(**n**, a)
⟩

$\|$

with r do ⟨
    b := getRight(**n**)
    append(**n**, b)
⟩

$$\left\{ \begin{array}{c} \alpha \leftarrow \mathbf{n}[\gamma \otimes \mathbf{p}[\mathbf{t}] \otimes \mathbf{q}[\mathbf{t'}]] \\ \vee \\ \alpha \leftarrow \mathbf{n}[\gamma \otimes \mathbf{q}[\mathbf{t'}] \otimes \mathbf{p}[\mathbf{t}]] \end{array} \right\}$$

Resource Invariant

$$\alpha \leftarrow \mathbf{p}[\mathbf{t}] \otimes \mathbf{n}[\gamma] \otimes \mathbf{q}[\mathbf{t'}]$$

$$\vee$$

$$\alpha \leftarrow \mathbf{n}[\gamma \otimes \mathbf{p}[\mathbf{t}]] \otimes \mathbf{q}[\mathbf{t'}]$$

$$\vee$$

$$\alpha \leftarrow \mathbf{p}[\mathbf{t}] \otimes \mathbf{n}[\gamma \otimes \mathbf{q}[\mathbf{t'}]]$$

$$\vee$$

$$\alpha \leftarrow \mathbf{n}[\gamma \otimes \mathbf{p}[\mathbf{t}] \otimes \mathbf{q}[\mathbf{t'}]]$$

$$\vee$$

$$\alpha \leftarrow \mathbf{n}[\gamma \otimes \mathbf{q}[\mathbf{t'}] \otimes \mathbf{p}[\mathbf{t}]]$$

Adding Tokens

$\alpha \leftarrow \mathbf{p}[\mathbf{t}] \otimes \mathbf{n}[\gamma] \otimes \mathbf{q}[\mathbf{t'}] * \text{t1} * \text{t2}$

$\vee$

$\alpha \leftarrow \mathbf{n}[\gamma \otimes \mathbf{p}[\mathbf{t}]] \otimes \mathbf{q}[\mathbf{t'}] * \text{t1} * \text{t2}$

$\vee$

$\alpha \leftarrow \mathbf{p}[\mathbf{t}] \otimes \mathbf{n}[\gamma \otimes \mathbf{q}[\mathbf{t'}]] * \text{t1} * \text{t2}$

$\vee$

$\alpha \leftarrow \mathbf{n}[\gamma \otimes \mathbf{p}[\mathbf{t}] \otimes \mathbf{q}[\mathbf{t'}]] * \text{t1} * \text{t2}$

$\vee$

$\alpha \leftarrow \mathbf{n}[\gamma \otimes \mathbf{q}[\mathbf{t'}] \otimes \mathbf{p}[\mathbf{t}]] * \text{t1} * \text{t2}$

Adding Tokens

$\alpha \leftarrow \mathbf{p}[\mathbf{t}] \otimes \mathbf{n}[\gamma] \otimes \mathbf{q}[\mathbf{t'}]$ * t1 * t2

V

$\alpha \leftarrow \mathbf{n}[\gamma \otimes \mathbf{p}[\mathbf{t}]] \otimes \mathbf{q}[\mathbf{t'}]$ * t1 * t2

V

$\alpha \leftarrow \mathbf{p}[\mathbf{t}] \otimes \mathbf{n}[\gamma \otimes \mathbf{q}[\mathbf{t'}]]$ * t1 * t2

V

$\alpha \leftarrow \mathbf{n}[\gamma \otimes \mathbf{p}[\mathbf{t}] \otimes \mathbf{q}[\mathbf{t'}]]$ * t1 * t2

V

$\alpha \leftarrow \mathbf{n}[\gamma \otimes \mathbf{q}[\mathbf{t'}] \otimes \mathbf{p}[\mathbf{t}]]$ * t1 * t2

<u>thread 1</u>

t1

Adding Tokens

$\alpha \leftarrow \mathbf{p}[\mathbf{t}] \otimes \mathbf{n}[\gamma] \otimes \mathbf{q}[\mathbf{t'}] * \text{t1} * \text{t2}$

V

~~$\alpha \leftarrow \mathbf{n}[\gamma \otimes \mathbf{p}[\mathbf{t}]] \otimes \mathbf{q}[\mathbf{t'}] * \text{t1} * \text{t2}$~~

V

$\alpha \leftarrow \mathbf{p}[\mathbf{t}] \otimes \mathbf{n}[\gamma \otimes \mathbf{q}[\mathbf{t'}]] * \text{t1} * \text{t2}$

V

~~$\alpha \leftarrow \mathbf{n}[\gamma \otimes \mathbf{p}[\mathbf{t}] \otimes \mathbf{q}[\mathbf{t'}]] * \text{t1} * \text{t2}$~~

V

~~$\alpha \leftarrow \mathbf{n}[\gamma \otimes \mathbf{q}[\mathbf{t'}] \otimes \mathbf{p}[\mathbf{t}]] * \text{t1} * \text{t2}$~~

<u>thread 1</u>

t1

Adding Tokens

$$\alpha \leftarrow \mathbf{p}[\mathbf{t}] \otimes \mathbf{n}[\gamma] \otimes \mathbf{q}[\mathbf{t'}] * t1 * t2$$

$$\vee$$

$$\alpha \leftarrow \mathbf{n}[\gamma \otimes \mathbf{p}[\mathbf{t}]] \otimes \mathbf{q}[\mathbf{t'}] * t1 * t2$$

$$\vee$$

$$\alpha \leftarrow \mathbf{p}[\mathbf{t}] \otimes \mathbf{n}[\gamma \otimes \mathbf{q}[\mathbf{t'}]] * t1 * t2$$

$$\vee$$

$$\alpha \leftarrow \mathbf{n}[\gamma \otimes \mathbf{p}[\mathbf{t}] \otimes \mathbf{q}[\mathbf{t'}]] * t1 * t2$$

$$\vee$$

$$\alpha \leftarrow \mathbf{n}[\gamma \otimes \mathbf{q}[\mathbf{t'}] \otimes \mathbf{p}[\mathbf{t}]] * t1 * t2$$

<u>thread 1</u>

t1

<u>end</u>

t1 * t2

Adding Tokens

~~$\alpha \leftarrow \mathbf{p}[\mathbf{t}] \otimes \mathbf{n}[\gamma] \otimes \mathbf{q}[\mathbf{t'}]$ * t1 * t2~~

V

~~$\alpha \leftarrow \mathbf{n}[\gamma \otimes \mathbf{p}[\mathbf{t}]] \otimes \mathbf{q}[\mathbf{t'}]$ * t1 * t2~~

V

~~$\alpha \leftarrow \mathbf{p}[\mathbf{t}] \otimes \mathbf{n}[\gamma \otimes \mathbf{q}[\mathbf{t'}]]$ * t1 * t2~~

V

$\alpha \leftarrow \mathbf{n}[\gamma \otimes \mathbf{p}[\mathbf{t}] \otimes \mathbf{q}[\mathbf{t'}]]$ * t1 * t2

V

$\alpha \leftarrow \mathbf{n}[\gamma \otimes \mathbf{q}[\mathbf{t'}] \otimes \mathbf{p}[\mathbf{t}]]$ * t1 * t2

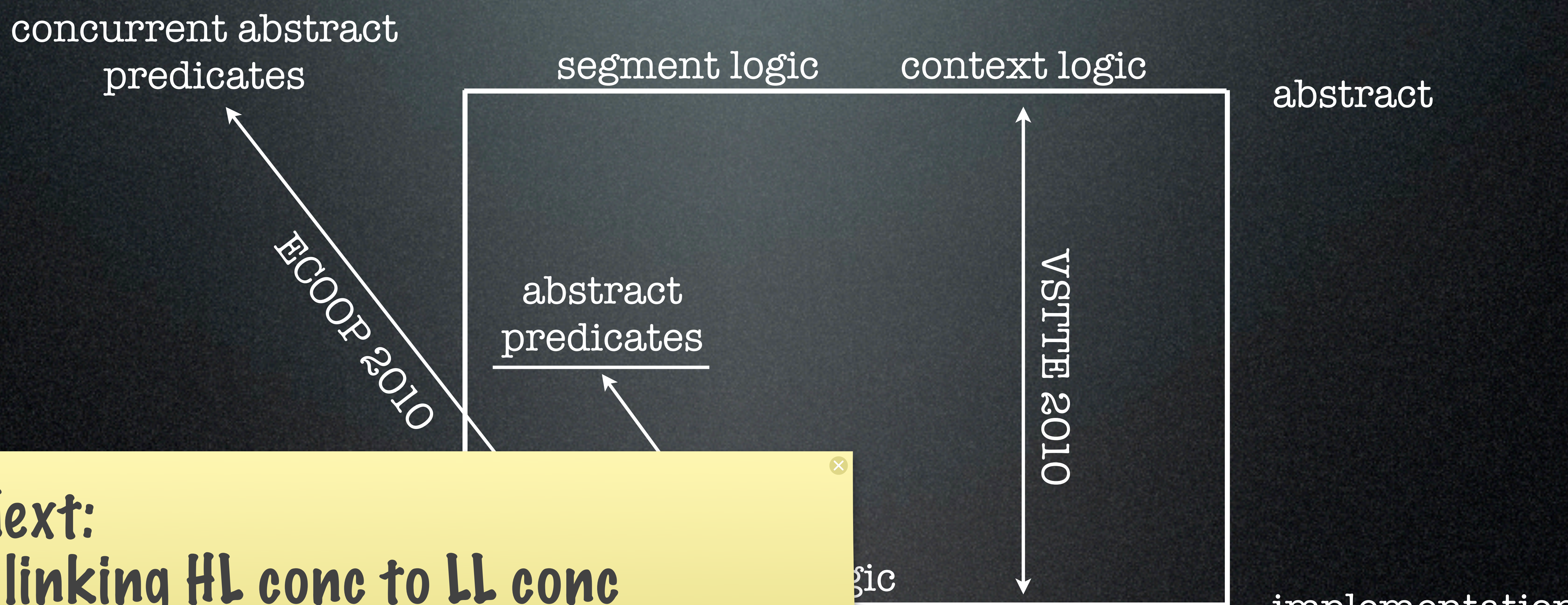
thread 1

t1

end

t1 * t2

Abstraction Levels



Next:
- linking HL conc to LL conc
- look at CAP in more detail
- Dynamic Lock Creation
- Automated Invariant Generation