Anytime, Anywhere
Modal Logics for Mobile Ambients

Luca Cardelli
Andy Gordon

Microsoft Research

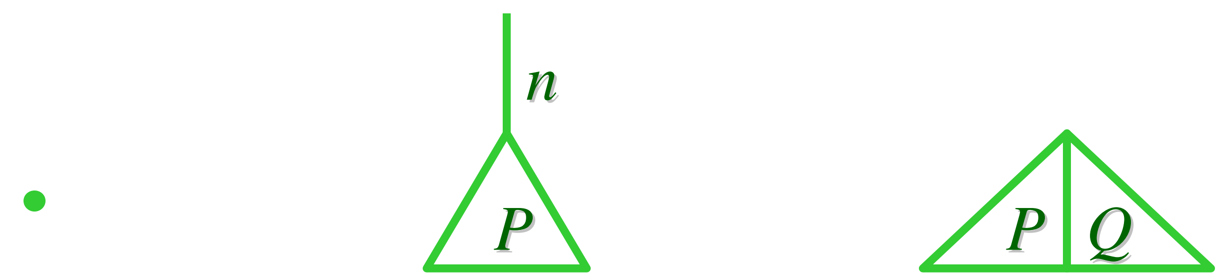
POPL 2000

Introduction

- We want to describe mobile behaviors. The *ambient calculus* provides an operational model, where spatial structures (agents, networks, etc.) are represented by nested locations.
- We also want to specify mobile behaviors. To this end, we devise an *ambient logic* that can talk about spatial structures.

Processes		*Formulas*	
$\mathbf{0}$	(void)	$\mathbf{0}$	(there is nothing here)
$n[P]$	(location)	$n[\mathcal{A}]$	(there is one thing here)
$P \mid Q$	(composition)	$\mathcal{A} \mid \mathcal{B}$	(there are two things here)

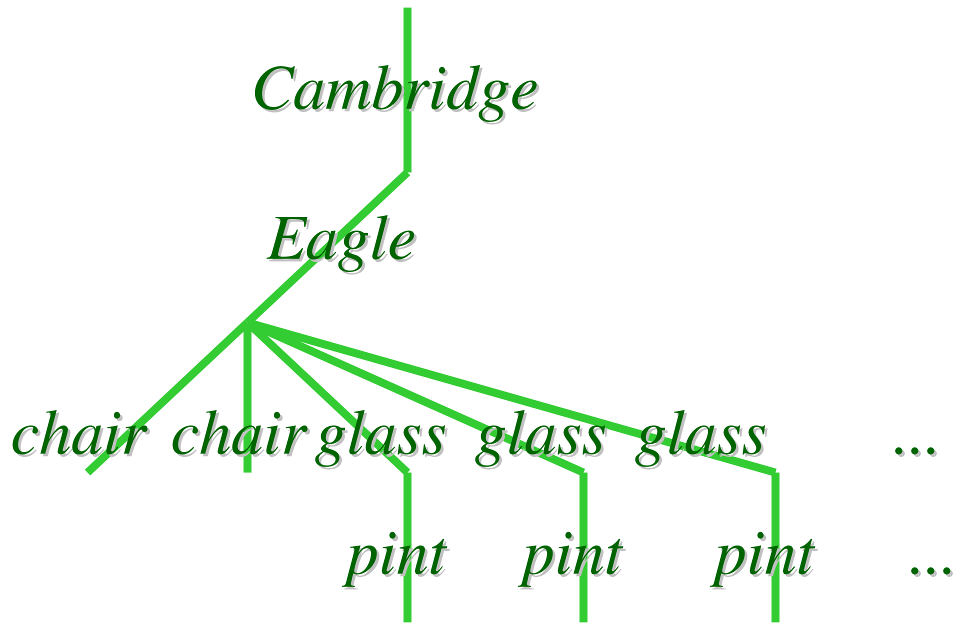
Trees



(void) (location) (composition)

Spatial Structures

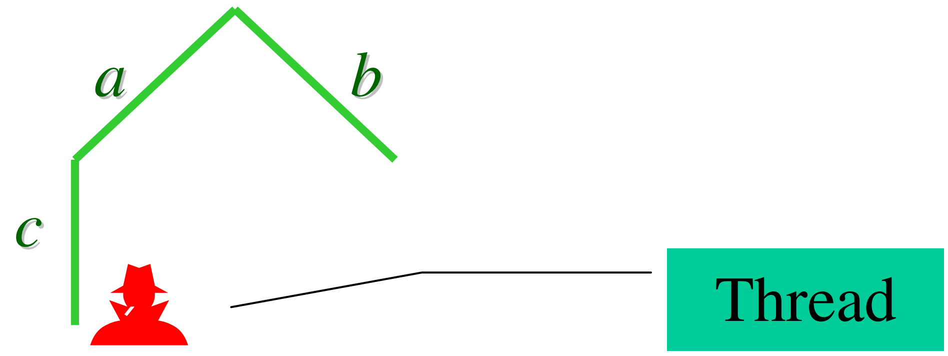
- Our basic model of space is going to be *finite-depth edge-labeled unordered trees*; for short: *spatial trees*, represented by a syntax of *spatial expressions*. Unbounded resources are represented by infinite branching:



$$Cambridge[Eagle[chair[\mathbf{0}] \mid chair[\mathbf{0}] \mid \mathbf{!}glass[pint[\mathbf{0}]]] \mid ...]$$

Ambient Structures

- Spatial expressions/trees are a subset of ambient expressions/trees, which can represent both the spatial and the dynamic aspects of mobile computation.

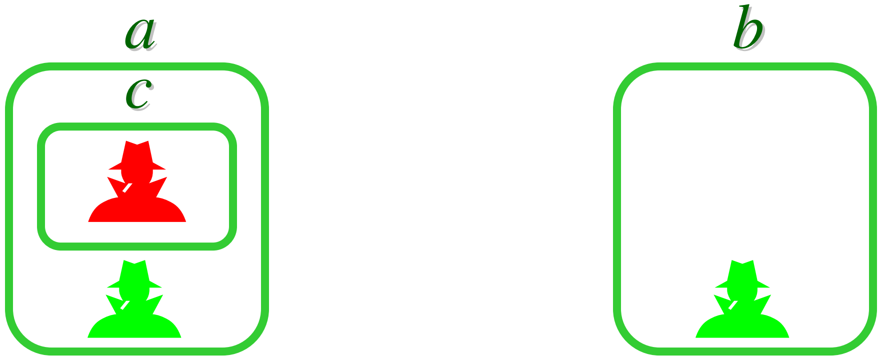


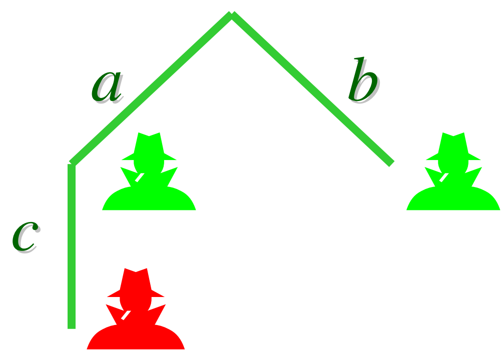
- An ambient tree is a spatial tree with, possibly, threads at each node that can locally change the shape of the tree.

$$a[c[\mathit{out}\ a.\ \mathit{in}\ b.\ P]]\ |\ b[\mathbf{0}]$$

Mobility

- *Mobility* is change of spatial structures over time.

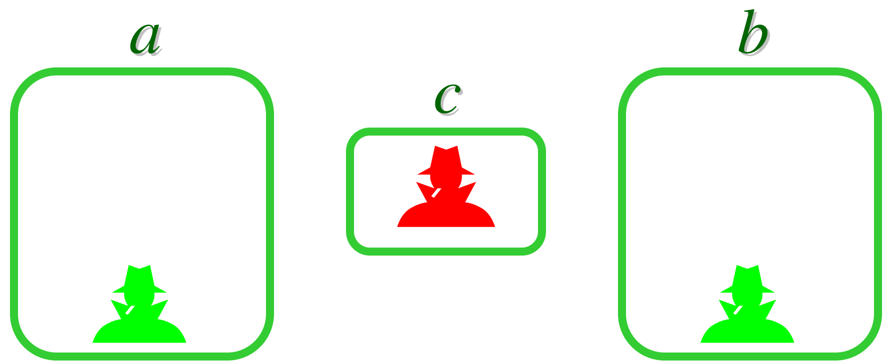


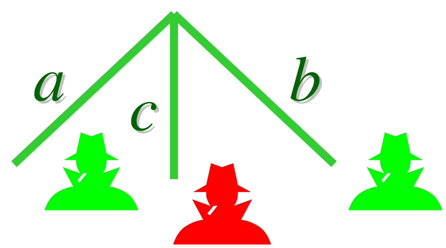


$a[Q \mid c[\mathit{out}\ a.\ \mathit{in}\ b.\ P]] \quad \mid b[R]$

Mobility

- *Mobility* is change of spatial structures over time.

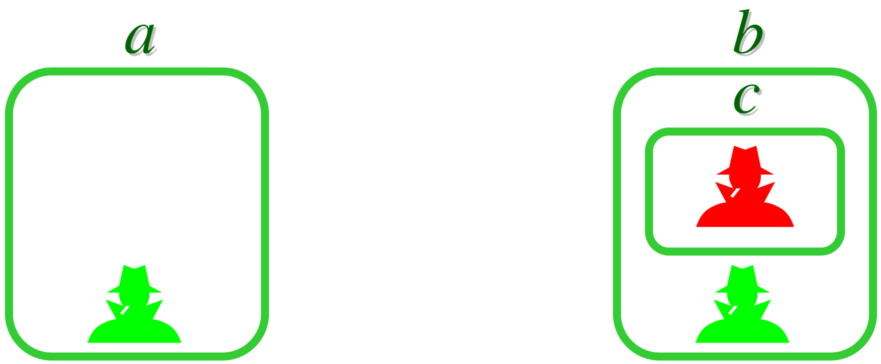


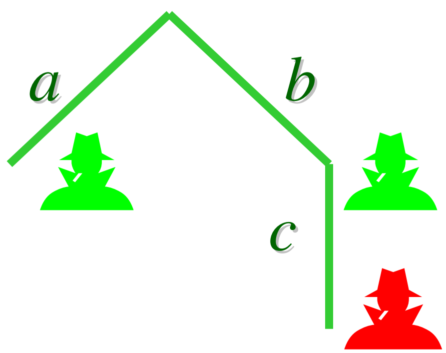


$a[Q] \quad | \; c[in\ b.\ P] \;\; | \; b[R]$

Mobility

- *Mobility* is change of spatial structures over time.





$$a[Q] \quad\quad\quad\quad\quad\quad \mid b[R \mid c[P]]$$

Restriction-Free Ambient Calculus

$P \in \Pi ::=$	Processes	$M ::=$	Messages
$\mathbf{0}$	inactivity	n	name
$P \mid P'$	parallel	$in\ M$	entry capability
$!P$	replication	$out\ M$	exit capability
$M[P]$	ambient	$open\ M$	open capability
$M.P$	exercise a capability	ε	empty path
$(n).P$	input locally, bind to n	$M.M'$	composite path
$\langle M \rangle$	output locally (async)		

$n[] \triangleq n[\mathbf{0}]$

$M \triangleq M.\mathbf{0}$ (where appropriate)

Reduction Semantics

- A structural congruence relation $P \equiv Q$:
  - On spatial expressions, $P \equiv Q$ iff P and Q denote the same tree.
  - On full ambient expressions, $P \equiv Q$ if in addition the respective threads are "trivially equivalent".
  - Prominent in the definition of the logic.

- A reduction relation $P \longrightarrow^* Q$:
  - Defining the meaning of mobility and communication actions.
  - Closed up to structural congruence:

$$P \equiv P', \; P' \longrightarrow^* Q', \; Q' \equiv Q \quad \Rightarrow \quad P \longrightarrow^* Q$$

Space-Time Modalities

- In a modal logic, the truth of a formula is relative to a state (called a *world*).
- In our case, the truth of a space-time modal formula is relative to the *here and now* of a process.
  - The formula $n[\mathbf{0}]$ is read:

    there is here and now an empty location called n
  - The operator $n[\mathcal{A}]$ is a single step in space (akin to the temporal next), which allows us talk about that place one step down into n.
  - Other modal operators can be used to talk about undetermined times (in the future) and undetermined places (in the location tree).

Logical Formulas

$\mathcal{A} \in \Phi ::=$	Formulas	(η is a name or a variable)
$\mathbf{T}$	true	
$\neg\mathcal{A}$	negation	
$\mathcal{A} \vee \mathcal{A}'$	disjunction	
$\mathbf{0}$	void	
$\eta[\mathcal{A}]$	location	
$\mathcal{A} \mid \mathcal{A}'$	composition	
$✧\mathcal{A}$	somewhere modality	
$\Diamond\mathcal{A}$	sometime modality	
$\mathcal{A}@\eta$	location adjunct	
$\mathcal{A} \triangleright \mathcal{A}'$	composition adjunct	
$\forall x.\mathcal{A}$	universal quantification over names	

Satisfaction Relation

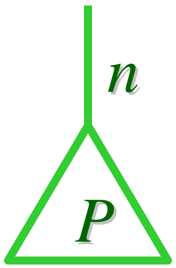
$P \vDash \mathbf{T}$		
$P \vDash \neg\mathcal{A}$	$\triangleq$	$\neg\, P \vDash \mathcal{A}$
$P \vDash \mathcal{A} \vee \mathcal{B}$	$\triangleq$	$P \vDash \mathcal{A} \vee P \vDash \mathcal{B}$
$P \vDash \mathbf{0}$	$\triangleq$	$P \equiv \mathbf{0}$
$P \vDash n[\mathcal{A}]$	$\triangleq$	$\exists P' \in \Pi.\ P \equiv n[P'] \wedge P' \vDash \mathcal{A}$
$P \vDash \mathcal{A} \mid \mathcal{B}$	$\triangleq$	$\exists P', P'' \in \Pi.\ P \equiv P' \mid P'' \wedge P' \vDash \mathcal{A} \wedge P'' \vDash \mathcal{B}$
$P \vDash ✧\mathcal{A}$	$\triangleq$	$\exists P' \in \Pi.\ P \downarrow^{*} P' \wedge P' \vDash \mathcal{A}$
$P \vDash \Diamond\mathcal{A}$	$\triangleq$	$\exists P' \in \Pi.\ P \longrightarrow^{*} P' \wedge P' \vDash \mathcal{A}$
$P \vDash \mathcal{A}@n$	$\triangleq$	$n[P] \vDash \mathcal{A}$
$P \vDash \mathcal{A} \triangleright \mathcal{B}$	$\triangleq$	$\forall P' \in \Pi.\ P' \vDash \mathcal{A} \Rightarrow P \mid P' \vDash \mathcal{B}$
$P \vDash \forall x.\mathcal{A}$	$\triangleq$	$\forall m \in \Lambda.\ P \vDash \mathcal{A}\{x \leftarrow m\}$

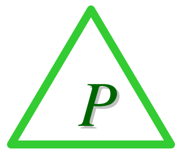
$P \downarrow P'$ iff $\exists n, P''.\ P \equiv n[P'] \mid P''$

$\downarrow^{*}$ is the reflexive and transitive closure of $\downarrow$

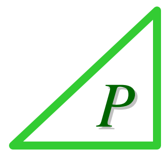
Satisfaction Relation for Trees

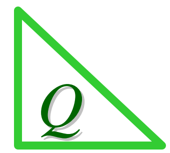
- $\models \mathbf{0}$



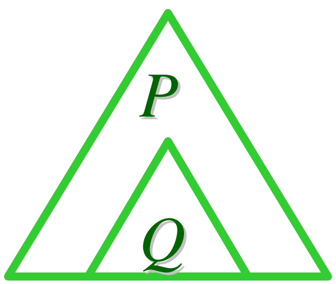
$\models n[\mathcal{A}]$ if 

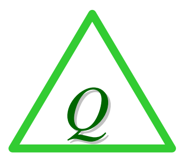
$\models \mathcal{A}$

$\models \mathcal{A} \mid \mathcal{B}$ if 

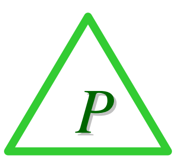
$\models \mathcal{A}$ and 

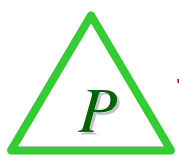
$\models \mathcal{B}$

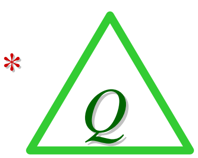


$\models \diamond\mathcal{A}$ if 

$\models \mathcal{A}$

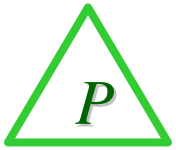


$\models \Diamond\mathcal{A}$ if 

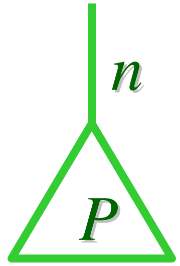
$\longrightarrow^*$ 

and 

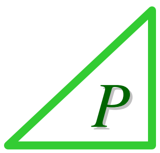
$\models \mathcal{A}$



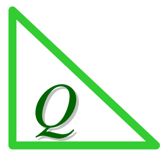
$\vDash \mathcal{A}@n$ if



$\vDash \mathcal{A}$



$\vDash \mathcal{A} \triangleright \mathcal{B}$ if for all



$\vDash \mathcal{A}$ we have

$\vDash \mathcal{B}$

- Basic Fact: satisfaction is invariant under structural congruence:

$$P \vDash \mathcal{A},\ P \equiv P' \ \Rightarrow\ P' \vDash \mathcal{A}$$

I.e.: $\{P \in \Pi \mid P \vDash \mathcal{A}\}$ is closed under $\equiv$.

Hence, formulas describe only congruence-invariant properties.

Some Derived Connectives

$\mathbf{F}$	$\triangleq \neg\mathbf{T}$	false
$\mathcal{A} \wedge \mathcal{B}$	$\triangleq \neg(\neg\mathcal{A} \vee \neg\mathcal{B})$	conjunction
$\mathcal{A} \Rightarrow \mathcal{B}$	$\triangleq \neg\mathcal{A} \vee \mathcal{B}$	implication
$\Box\mathcal{A}$	$\triangleq \neg\Diamond\neg\mathcal{A}$	everytime modality
$✧\mathcal{A}$	$\triangleq \neg✧\neg\mathcal{A}$	everywhere modality
$\exists x.\mathcal{A}$	$\triangleq \neg\forall x.\neg\mathcal{A}$	existential quantification
$\mathcal{A} \propto \mathcal{B}$	$\triangleq \neg(\mathcal{B} \triangleright \neg\mathcal{A})$	fusion
$\mathcal{A} \mid\Rightarrow \mathcal{B}$	$\triangleq \neg(\mathcal{A} \mid \neg\mathcal{B})$	fusion adjunct
$\mathcal{A} \parallel \mathcal{B}$	$\triangleq \neg(\neg\mathcal{A} \mid \neg\mathcal{B})$	decomposition
$\mathcal{A}^{\forall}$	$\triangleq \mathcal{A} \parallel \mathbf{F}$	every component satisfies $\mathcal{A}$
$\mathcal{A}^{\exists}$	$\triangleq \mathcal{A} \mid \mathbf{T}$	some component satisfies $\mathcal{A}$
$\mathcal{A}^{\mathbf{F}}$	$\triangleq \mathcal{A} \triangleright \mathbf{F}$	$\mathcal{A}$ is unsatisfiable

Claims

- The satisfaction relation looks natural (to us):
  - The definitions of $\mathbf{0}$, $n[\mathcal{A}]$, and $\mathcal{A} \mid \mathcal{B}$ seem inevitable, once we accept that formulas should be able to talk about the tree structure of locations (up to $\equiv$).
  - The connectives $\mathcal{A}@n$ and $\mathcal{A} \triangleright \mathcal{B}$ have security motivations.
  - The modalities $\Diamond\mathcal{A}$ and $✧\mathcal{A}$ talk about process evolution and structure in an undetermined way (good for specs).
  - The fragment $\mathbf{T}$, $\neg\mathcal{A}$, $\mathcal{A}\vee\mathcal{B}$, $\forall x.\mathcal{A}$, is classical: why not?
- The logic is induced by the satisfaction relation.
  - We did not have any preconceptions about what kind of logic this ought to be. We didn't invent this logic, we discovered it!

From Satisfaction to (Propositional) Logic

- Propositional validity

$$\boldsymbol{vld}\,\mathcal{A} \;\triangleq\; \forall P\in\Pi.\ P \vDash \mathcal{A} \qquad\qquad \mathcal{A}\text{ (closed) is valid}$$

- Sequents

$$\mathcal{A} \vdash \mathcal{B} \;\triangleq\; \forall P\in\Pi.\ P \vDash \mathcal{A} \Rightarrow P \vDash \mathcal{B}$$

- Rules

$$\mathcal{A}_1 \vdash \mathcal{B}_1; \ldots; \mathcal{A}_n \vdash \mathcal{B}_n \;\}\; \mathcal{A} \vdash \mathcal{B} \;\triangleq \qquad (n\geq 0)$$

$$\mathcal{A}_1 \vdash \mathcal{B}_1 \wedge \ldots \wedge \mathcal{A}_n \vdash \mathcal{B}_n \Rightarrow \mathcal{A} \vdash \mathcal{B}$$

(N.B.: all the rules shown later are validated accordingly.)

- Conventions:
  - $\dashv\vdash$ means $\vdash$ in both directions

    $\{\}$ means $\}$ in both directions

Logical Adjunctions

- This is a logic with multiple logical adjunctions (3 of them!):

  $\wedge$ / $\Rightarrow$ (classical)

  $\mathcal{A} \wedge \mathcal{C} \vdash \mathcal{B}$ iff $\mathcal{A} \vdash \mathcal{C} \Rightarrow \mathcal{B}$

  - $|$ / $\triangleright$ (linear, $\otimes$ / $\multimap$)

    $\mathcal{A} \mid \mathcal{C} \vdash \mathcal{B}$ iff $\mathcal{A} \vdash \mathcal{C} \triangleright \mathcal{B}$

  - $n[\text{-}]$ / $\text{-}@n$

    $n[\mathcal{A}] \vdash \mathcal{B}$ iff $\mathcal{A} \vdash \mathcal{B}@n$

- Which one should be taken as *the* logical adjunction for sequents? I.e., what should "," mean in a sequent?

"Neutral" Sequents

- Our logic is formulated with single-premise, single-conclusion sequents. We don't pre-judge ",".
  - By taking $\wedge$ on the left and $\vee$ on the right of $\vdash$ as structural operators, we can derive all the standard rules of sequent and natural deduction systems with multiple premises/conclusions.
  - By taking $\mid$ on the left of $\vdash$ as a structural operator, we can derive all the rules of intuitionistic linear logic (by appropriate mappings of the ILL connectives).
  - By taking nestings of $\wedge$ and $\mid$ on the left of $\vdash$ as structural "bunches", we obtain a bunched logic, with its two associated implications, $\Rightarrow$ and $\triangleright$.
- This is convenient. We do not know much, however, about the meta-theory of this presentation style.

Rules: Propositional Calculus

(A-L)	$\mathcal{A}\wedge(\mathcal{C}\wedge\mathcal{D}) \vdash \mathcal{B}\ \{\}\ (\mathcal{A}\wedge\mathcal{C})\wedge\mathcal{D} \vdash \mathcal{B}$
(A-R)	$\mathcal{A} \vdash (\mathcal{C}\vee\mathcal{D})\vee\mathcal{B}\ \{\}\ \mathcal{A} \vdash \mathcal{C}\vee(\mathcal{D}\vee\mathcal{B})$
(X-L)	$\mathcal{A}\wedge\mathcal{C} \vdash \mathcal{B}\ \}\ \mathcal{C}\wedge\mathcal{A} \vdash \mathcal{B}$
(X-R)	$\mathcal{A} \vdash \mathcal{C}\vee\mathcal{B}\ \}\ \mathcal{A} \vdash \mathcal{B}\vee\mathcal{C}$
(C-L)	$\mathcal{A}\wedge\mathcal{A} \vdash \mathcal{B}\ \}\ \mathcal{A} \vdash \mathcal{B}$
(C-R)	$\mathcal{A} \vdash \mathcal{B}\vee\mathcal{B}\ \}\ \mathcal{A} \vdash \mathcal{B}$
(W-L)	$\mathcal{A} \vdash \mathcal{B}\ \}\ \mathcal{A}\wedge\mathcal{C} \vdash \mathcal{B}$
(W-R)	$\mathcal{A} \vdash \mathcal{B}\ \}\ \mathcal{A} \vdash \mathcal{C}\vee\mathcal{B}$
(Id)	$\}\ \mathcal{A} \vdash \mathcal{A}$
(Cut)	$\mathcal{A} \vdash \mathcal{C}\vee\mathcal{B};\ \mathcal{A}'\wedge\mathcal{C} \vdash \mathcal{B}'\ \}\ \mathcal{A}\wedge\mathcal{A}' \vdash \mathcal{B}\vee\mathcal{B}'$
(**T**)	$\mathcal{A}\wedge\mathbf{T} \vdash \mathcal{B}\ \}\ \mathcal{A} \vdash \mathcal{B}$
(**F**)	$\mathcal{A} \vdash \mathbf{F}\vee\mathcal{B}\ \}\ \mathcal{A} \vdash \mathcal{B}$
(¬-L)	$\mathcal{A} \vdash \mathcal{C}\vee\mathcal{B}\ \}\ \mathcal{A}\wedge\neg\mathcal{C} \vdash \mathcal{B}$
(¬-R)	$\mathcal{A}\wedge\mathcal{C} \vdash \mathcal{B}\ \}\ \mathcal{A} \vdash \neg\mathcal{C}\vee\mathcal{B}$

Rules: Composition

$(\mid \mathbf{0})$	$\} \ \mathcal{A} \mid \mathbf{0} \dashv\vdash \mathcal{A}$	$\mathbf{0}$ is nothing
$(\mid \neg\mathbf{0})$	$\} \ \mathcal{A} \mid \neg\mathbf{0} \vdash \neg\mathbf{0}$	if a part is non-$\mathbf{0}$, so is the whole
$(\mathrm{A} \mid)$	$\} \ \mathcal{A} \mid (\mathcal{B} \mid \mathcal{C}) \dashv\vdash (\mathcal{A} \mid \mathcal{B}) \mid \mathcal{C}$	$\mid$ associativity
$(\mathrm{X} \mid)$	$\} \ \mathcal{A} \mid \mathcal{B} \vdash \mathcal{B} \mid \mathcal{A}$	$\mid$ commutativity
$(\mid \vdash)$	$\mathcal{A}' \vdash \mathcal{B}'; \ \mathcal{A}'' \vdash \mathcal{B}'' \ \} \ \mathcal{A}' \mid \mathcal{A}'' \vdash \mathcal{B}' \mid \mathcal{B}''$	$\mid$ congruence
$(\mid \vee)$	$\} \ (\mathcal{A} \vee \mathcal{B}) \mid \mathcal{C} \vdash \mathcal{A} \mid \mathcal{C} \vee \mathcal{B} \mid \mathcal{C}$	$\mid$-$\vee$ distribution
$(\mid \| \,)$	$\} \ \mathcal{A}' \mid \mathcal{A}'' \vdash \mathcal{A}' \mid \mathcal{B}'' \vee \mathcal{B}' \mid \mathcal{A}'' \vee \neg\mathcal{B}' \mid \neg\mathcal{B}''$	decomposition
$(\mid \triangleright)$	$\mathcal{A} \mid \mathcal{C} \vdash \mathcal{B} \ \{\} \ \mathcal{A} \vdash \mathcal{C} \triangleright \mathcal{B}$	$\mid$-$\triangleright$ adjunction
$(\triangleright\mathbf{F} \neg)$	$\} \ \mathcal{A}^{\mathbf{F}} \vdash \mathcal{A}^{\neg}$	if $\mathcal{A}$ is unsatisfiable then $\mathcal{A}$ is false
$(\neg \triangleright\mathbf{F})$	$\} \ \mathcal{A}^{\mathbf{F}\neg} \vdash \mathcal{A}^{\mathbf{FF}}$	if $\mathcal{A}$ is satisfiable then $\mathcal{A}^{\mathbf{F}}$ is unsatisfiable

where $\mathcal{A}^{\neg} \triangleq \neg\mathcal{A}$ and $\mathcal{A}^{\mathbf{F}} \triangleq \mathcal{A} \triangleright \mathbf{F}$

The Decomposition Operator

- Consider the De Morgan dual of | :

$\mathcal{A} \parallel \mathcal{B}$	$\triangleq \neg(\neg\mathcal{A} \mid \neg\mathcal{B})$	$P \vDash$ - iff $\forall P', P'' \in \Pi.\ P \equiv P' \mid P'' \Rightarrow P' \vDash \mathcal{A} \vee P'' \vDash \mathcal{B}$
$\mathcal{A}^{\forall}$	$\triangleq \mathcal{A} \parallel \mathbf{F}$	$P \vDash$ - iff $\forall P', P'' \in \Pi.\ P \equiv P' \mid P'' \Rightarrow P' \vDash \mathcal{A}$
$\mathcal{A}^{\exists}$	$\triangleq \mathcal{A} \mid \mathbf{T}$	$P \vDash$ - iff $\exists P', P'' \in \Pi.\ P \equiv P' \mid P'' \wedge P' \vDash \mathcal{A}$

$\mathcal{A} \parallel \mathcal{B}$ — for every partition, one piece satisfies $\mathcal{A}$ or the other piece satisfies $\mathcal{B}$

$\mathcal{A}^{\forall} \Leftrightarrow \neg((\neg\mathcal{A})^{\exists})$ — every component satisfies $\mathcal{A}$

$\mathcal{A}^{\exists} \Leftrightarrow \neg((\neg\mathcal{A})^{\forall})$ — some component satisfies $\mathcal{A}$

Examples:

$(p[\mathbf{T}] \Rightarrow p[q[\mathbf{T}]^{\exists}])^{\forall}$ — every p has a q child

$(p[\mathbf{T}] \Rightarrow p[q[\mathbf{T}] \mid (\neg q[\mathbf{T}])^{\forall}])^{\forall}$ — every p has a unique q child

The Decomposition Axiom

$(\,|\,\|\,)$ } $(\mathcal{A}' \mid \mathcal{A}'') \vdash (\mathcal{A}' \mid \mathcal{B}'') \vee (\mathcal{B}' \mid \mathcal{A}'') \vee (\neg\mathcal{B}' \mid \neg\mathcal{B}'')$

- Alternative formulations and special cases:
  - $(\mathcal{A}' \mid \mathcal{A}'') \wedge (\mathcal{B}' \,\|\, \mathcal{B}'') \vdash (\mathcal{A}' \mid \mathcal{B}'') \vee (\mathcal{B}' \mid \mathcal{A}'')$

    "If P has a partition into pieces that satisfy $\mathcal{A}'$ and $\mathcal{A}''$, and every partition has one piece that satisfies $\mathcal{B}'$ or the other that satisfies $\mathcal{B}''$, then either P has a partition into pieces that satisfy $\mathcal{A}'$ and $\mathcal{B}''$, or it has a partition into pieces that satisfy $\mathcal{B}'$ and $\mathcal{A}''$."
  - $\neg(\mathcal{A} \mid \mathcal{B}) \vdash (\mathcal{A} \mid \mathbf{T}) \Rightarrow (\mathbf{T} \mid \neg\mathcal{B})$

    "If P has no partition into pieces that satisfy $\mathcal{A}$ and $\mathcal{B}$, but P has a piece that satisfies $\mathcal{A}$, then P has a piece that does not satisfy $\mathcal{B}$."
  - $\neg(\mathbf{T} \mid \mathcal{B}) \vdash \mathbf{T} \mid \neg\mathcal{B}$
  - $\neg(\mathcal{A} \mid \mathcal{B}) \vdash (\neg\mathcal{A} \mid \mathbf{T}) \vee (\mathbf{T} \mid \neg\mathcal{B})$

The Composition Adjunct

$(\mid\triangleright)\quad \mathcal{A} \mid \mathcal{C} \vdash \mathcal{B} \;\}\{\; \mathcal{A} \vdash \mathcal{C} \triangleright \mathcal{B}$

"Assume that every process that has a partition into pieces that satisfy $\mathcal{A}$ and $\mathcal{C}$, also satisfies $\mathcal{B}$. Then, every process that satisfies $\mathcal{A}$, together with any process that satisfies $\mathcal{C}$, satisfies $\mathcal{B}$. (And vice versa.)" (*c.f.* $(\multimap \mathrm{R})$)

- Interpretations of $\mathcal{A} \triangleright \mathcal{B}$:
  - P provides $\mathcal{B}$ in any context that provides $\mathcal{A}$
  - P ensures $\mathcal{B}$ under any attack that ensures $\mathcal{A}$

That is, $P \vDash \mathcal{A} \triangleright \mathcal{B}$ is a context-system spec (a concurrent version of a pre-post spec).

Moreover $\mathcal{A} \triangleright \mathcal{B}$ is, in a precise sense, linear implication: the context that satisfies $\mathcal{A}$ is used exactly once in the system that satisfies $\mathcal{B}$.

Some Derived Rules

$\} \ (\mathcal{A} \triangleright \mathcal{B}) \mid \mathcal{A} \vdash \mathcal{B}$

"If P provides $\mathcal{B}$ in any context that provides $\mathcal{A}$, and Q provides $\mathcal{A}$, then P and Q together provide $\mathcal{B}$."

- Proof: $\mathcal{A} \triangleright \mathcal{B} \vdash \mathcal{A} \triangleright \mathcal{B} \ \} \ (\mathcal{A} \triangleright \mathcal{B}) \mid \mathcal{A} \vdash \mathcal{B}$ by (Id), (| ▷)

$\mathcal{D} \vdash \mathcal{A}; \ \mathcal{B} \vdash \mathcal{C} \ \} \ \mathcal{D} \mid (\mathcal{A} \triangleright \mathcal{B}) \vdash \mathcal{C}$ (*c.f.* ($\multimap$ L))

"If anything that satisfies $\mathcal{D}$ satisfies $\mathcal{A}$, and anything that satisfies $\mathcal{B}$ satisfies $\mathcal{C}$, then: anything that has a partition into a piece satisfying $\mathcal{D}$ (and hence $\mathcal{A}$), and another piece satisfying $\mathcal{B}$ in a context that satisfies $\mathcal{A}$, it satisfies ($\mathcal{B}$ and hence) $\mathcal{C}$."

- Proof:

$\mathcal{D} \vdash \mathcal{A}; \ \mathcal{A} \triangleright \mathcal{B} \vdash \mathcal{A} \triangleright \mathcal{B} \ \} \ \mathcal{D} \mid \mathcal{A} \triangleright \mathcal{B} \vdash \mathcal{A} \mid \mathcal{A} \triangleright \mathcal{B}$	assumption, (Id), (| ⊢)
$\mathcal{A} \mid \mathcal{A} \triangleright \mathcal{B} \vdash \mathcal{B}$	above
$\mathcal{B} \vdash \mathcal{C}$	assumption

More Derived Rules

$\} \ \mathcal{A} \vdash \mathbf{T} \mid \mathcal{A}$	you can always add more pieces (if they are **0**)
$\} \ \mathbf{F} \mid \mathcal{A} \vdash \mathbf{F}$	if a piece is absurd, so is the whole
$\} \ \mathbf{0} \vdash \neg(\neg\mathbf{0} \mid \neg\mathbf{0})$	**0** is single-threaded
$\} \ \mathcal{A} \mid \mathcal{B} \wedge \mathbf{0} \vdash \mathcal{A}$	you can split **0** (but you get **0**). Proof uses (| ||)
$\mathcal{A}' \vdash \mathcal{A};\ \mathcal{B} \vdash \mathcal{B}' \ \} \ \mathcal{A} \triangleright \mathcal{B} \vdash \mathcal{A}' \triangleright \mathcal{B}'$	$\triangleright$ is contravariant on the left
$\} \ \mathcal{A} \triangleright \mathcal{B} \mid \mathcal{B} \triangleright \mathcal{C} \vdash \mathcal{A} \triangleright \mathcal{C}$	$\triangleright$ is transitive
$\} \ (\mathcal{A} \mid \mathcal{B}) \triangleright \mathcal{C} \dashv\vdash \mathcal{A} \triangleright (\mathcal{B} \triangleright \mathcal{C})$	$\triangleright$ curry/uncurry
$\} \ \mathcal{A} \triangleright (\mathcal{B} \triangleright \mathcal{C}) \vdash \mathcal{B} \triangleright (\mathcal{A} \triangleright \mathcal{C})$	contexts commute
$\} \ \mathbf{T} \dashv\vdash \mathbf{T} \triangleright \mathbf{T}$	truth can withstand any attack
$\} \ \mathbf{T} \vdash \mathbf{F} \triangleright \mathcal{A}$	anything goes if you can find an absurd partner
$\} \ \mathbf{T} \triangleright \mathcal{A} \vdash \mathcal{A}$	if $\mathcal{A}$ resists any attack, then it holds

Rules: Location

$(n[]\ \neg\mathbf{0})$	$\}\ n[\mathcal{A}] \vdash \neg\mathbf{0}$	locations exist
$(n[]\ \neg\mid)$	$\}\ n[\mathcal{A}] \vdash \neg(\neg\mathbf{0} \mid \neg\mathbf{0})$	are not decomposable
$(n[]\vdash)$	$\mathcal{A} \vdash \mathcal{B}\ \{\}\ n[\mathcal{A}] \vdash n[\mathcal{B}]$	$n[]$ congruence
$(n[]\ \wedge)$	$\}\ n[\mathcal{A}] \wedge n[\mathcal{C}] \vdash n[\mathcal{A} \wedge \mathcal{C}]$	$n[]$-$\wedge$ distribution
$(n[]\ \vee)$	$\}\ n[\mathcal{C} \vee \mathcal{B}] \vdash n[\mathcal{C}] \vee n[\mathcal{B}]$	$n[]$-$\vee$ distribution
$(n[]\ @)$	$n[\mathcal{A}] \vdash \mathcal{B}\ \{\}\ \mathcal{A} \vdash \mathcal{B}@n$	$n[]$-@ adjunction
$(\neg\ @)$	$\}\ \mathcal{A}@n \dashv\vdash \neg((\neg\mathcal{A})@n)$	@ is self-dual

Rules: Time and Space Modalities

$(\Diamond)$	$\}\ \Diamond\mathcal{A} \dashv\vdash \neg\Box\neg\mathcal{A}$	(✧)	$\}$ ✧$\mathcal{A} \dashv\vdash \neg$¤$\neg\mathcal{A}$
$(\Box\ \mathbf{K})$	$\}\ \Box(\mathcal{A}\Rightarrow\mathcal{B}) \vdash \Box\mathcal{A}\Rightarrow\Box\mathcal{B}$	(¤ **K**)	$\}$ ¤$(\mathcal{A}\Rightarrow\mathcal{B}) \vdash$ ¤$\mathcal{A}\Rightarrow$ ¤$\mathcal{B}$
$(\Box\ \mathrm{T})$	$\}\ \Box\mathcal{A} \vdash \mathcal{A}$	(¤ T)	$\}$ ¤$\mathcal{A} \vdash \mathcal{A}$
$(\Box\ 4)$	$\}\ \Box\mathcal{A} \vdash \Box\Box\mathcal{A}$	(¤ 4)	$\}$ ¤$\mathcal{A} \vdash$ ¤ ¤$\mathcal{A}$
$(\Box\ \mathbf{T})$	$\}\ \mathbf{T} \vdash \Box\mathbf{T}$	(¤ **T**)	$\}\ \mathbf{T} \vdash$ ¤$\mathbf{T}$
$(\Box\ \vdash)$	$\mathcal{A} \vdash \mathcal{B}\ \}\ \Box\mathcal{A} \vdash \Box\mathcal{B}$	(¤ $\vdash$)	$\mathcal{A} \vdash \mathcal{B}\ \}$ ¤$\mathcal{A} \vdash$ ¤$\mathcal{B}$
$(\Diamond n[])$	$\}\ n[\Diamond\mathcal{A}] \vdash \Diamond n[\mathcal{A}]$	(✧n[])	$\}\ n[$✧$\mathcal{A}] \vdash$ ✧$\mathcal{A}$
$(\Diamond \mid)$	$\}\ \Diamond\mathcal{A} \mid \Diamond\mathcal{B} \vdash \Diamond(\mathcal{A} \mid \mathcal{B})$	(✧ $\mid$)	$\}$ ✧$\mathcal{A} \mid \mathcal{B} \vdash$ ✧$(\mathcal{A} \mid \mathbf{T})$
(✧$\Diamond$)	$\}$ ✧$\Diamond\mathcal{A} \vdash \Diamond$✧$\mathcal{A}$		

S4, but not S5: $\neg$ ***vld*** $\Diamond\mathcal{A} \vdash \Box\Diamond\mathcal{A}$ $\neg$ ***vld*** ✧$\mathcal{A} \vdash$ ¤ ✧$\mathcal{A}$

(✧$\Diamond$): if somewhere sometime $\mathcal{A}$, then sometime somewhere $\mathcal{A}$

Some Derived Rules

$\mathcal{A} \vdash \mathcal{B} \ \} \ \mathcal{A}@n \vdash \mathcal{B}@n$ **@ congruence**

$\} \ n[\mathcal{A}@n] \vdash \mathcal{A}$

$\} \ \mathcal{A} \dashv\vdash n[\mathcal{A}]@n$

$\} \ n[\neg\mathcal{A}] \vdash \neg n[\mathcal{A}]$

$\} \ \neg n[\mathcal{A}] \dashv\vdash \neg n[\mathbf{T}] \vee n[\neg\mathcal{A}]$

Examples

- $an\ n \triangleq n[\mathbf{T}] \mid \mathbf{T}$ — there is now an n here
- $no\ n \triangleq \neg an\ n$ — there is now no n here
- $one\ n \triangleq n[\mathbf{T}] \mid no\ n$ — there is now exactly one n here
- $\mathcal{A}^{\forall} \triangleq \neg(\neg\mathcal{A} \mid \mathbf{T})$ — everybody here satisfies $\mathcal{A}$
- $(n[\mathbf{T}] \Rightarrow n[\mathcal{A}])^{\forall}$ — every n here satisfies $\mathcal{A}$
- $\boxtimes((n[\mathbf{T}] \Rightarrow n[\mathcal{A}])^{\forall})$ — every n everywhere satisfies $\mathcal{A}$

Ex: Immovable Object vs. Irresistible Force

$$Im \triangleq \mathbf{T} \triangleright \Box(obj[\mathbf{0}] \mid \mathbf{T})$$

$$Ir \triangleq \mathbf{T} \triangleright \Box\Diamond\neg(obj[\mathbf{0}] \mid \mathbf{T})$$

$Im \mid Ir \;=\; (\mathbf{T} \triangleright \Box(obj[\mathbf{0}] \mid \mathbf{T})) \mid Ir$	$\mathcal{A} \vdash \mathbf{T}$
$\quad\vdash\; \Box(obj[\mathbf{0}] \mid \mathbf{T})$	$(\mathcal{A} \triangleright \mathcal{B}) \mid \mathcal{A} \vdash \mathcal{B}$
$\quad\vdash\; \Diamond\mathrm{P}(obj[\mathbf{0}] \mid \mathbf{T})$	$\mathcal{A} \vdash \Diamond\mathcal{A}$
$Im \mid Ir \;=\; Im \mid (\mathbf{T} \triangleright \Box\Diamond\neg(obj[\mathbf{0}] \mid \mathbf{T}))$	
$\quad\vdash\; \Box\mathrm{N}\neg(obj[\mathbf{0}] \mid \mathbf{T})$	$\Diamond\neg\mathcal{A} \vdash \neg\Box\mathcal{A}$
$\quad\vdash\; \neg\Diamond\mathrm{P}(obj[\mathbf{0}] \mid \mathbf{T})$	$\Box\neg\mathcal{A} \vdash \neg\Diamond\mathcal{A}$
Hence: $Im \mid Ir \vdash \mathbf{F}$	$\mathcal{A} \wedge \neg\mathcal{A} \vdash \mathbf{F}$

Model Checking

- If P is $!$-free and $\mathscr{A}$ is $\triangleright$-free, then $P \vDash \mathscr{A}$ is decidable.
- This provides a way of mechanically checking (certain) assertions about (certain) mobile processes.
- Potential application: checking (the bytecode of) mobile agents against the internal mobility policies of receiving sites. (I.e.: conferring more flexibility than just sandboxing the agent.)

Connections with Intuitionistic Linear Logic

- Weakening and contraction are not valid rules: principle of *conservation of space*.
- Semantic connection: sets of processes closed under $\equiv$ and ordered by inclusion form a quantale (a model of ILL).
- Multiplicative intuitionistic linear logic (MILL) can be faithfully embedded in our logic:

$$\begin{array}{lll} \mathbf{1}_{\mathrm{MILL}} & \triangleq & \mathbf{0} \\ \mathcal{A} \otimes_{\mathrm{MILL}} \mathcal{B} & \triangleq & \mathcal{A} \mid \mathcal{B} \\ \mathcal{A} \multimap_{\mathrm{MILL}} \mathcal{B} & \triangleq & \mathcal{A} \triangleright \mathcal{B} \end{array}$$

MILL rules and our rules are interderivable ("our rules" means the rules involving only $\mathbf{0}$, $\mid$, $\triangleright$, plus a derivable cut rule for $\mid$).

- Full intuitionistic linear logic (ILL) can be embedded:

$\mathbf{1}_{ILL}$	$\triangleq$	$\mathbf{0}$	$\mathcal{A} \oplus \mathcal{B}$	$\triangleq$	$\mathcal{A} \vee \mathcal{B}$
$\bot_{ILL}$	$\triangleq$	$\mathbf{F}$	$\mathcal{A} \,\&\, \mathcal{B}$	$\triangleq$	$\mathcal{A} \wedge \mathcal{B}$
$\top_{ILL}$	$\triangleq$	$\mathbf{T}$	$\mathcal{A} \otimes \mathcal{B}$	$\triangleq$	$\mathcal{A} \mid \mathcal{B}$
$\mathbf{0}_{ILL}$	$\triangleq$	$\mathbf{F}$	$\mathcal{A} \multimap \mathcal{B}$	$\triangleq$	$\mathcal{A} \triangleright \mathcal{B}$
			$!\mathcal{A}$	$\triangleq$	$\mathbf{0} \wedge (\mathbf{0} \Rightarrow \mathcal{A})^{\neg\mathbf{F}}$

- The rules of ILL can be logically derived from these definitions. (E.g.: the proof of $!\mathcal{A} \vdash\ !\mathcal{A} \otimes\ !\mathcal{A}$ uses the decomposition axiom.)

- So, $\mathcal{A}_1, ..., \mathcal{A}_n \vdash_{ILL} \mathcal{B}$ implies $\mathcal{A}_1 \mid ... \mid \mathcal{A}_n \vdash \mathcal{B}$.

- Some discrepancies: $\bot_{ILL} = \mathbf{0}_{ILL}$; the additives distribute; $!\mathcal{A}$ is not "replication"; $!\mathcal{A} \multimap \mathcal{B}$ is not so interesting; $\mathcal{A}^{\bot}/\mathcal{A}^{\mathbf{0}}$ is unusually interesting.

Connection with Relevant Logic

- (Noted after the fact [O'Hearn, Pym].) The definition of the satisfaction relation is very similar to Urquhart's semantics of relevant logic. In particular $\mathcal{A} \mid \mathcal{B}$ is defined just like *intensional conjunction*, and $\mathcal{A} \triangleright \mathcal{B}$ is defined just like *relevant implication* in that semantics.

- Except:
  - We do not have contraction. This does not make sense in process calculi, because $P \mid P \neq P$. Urquhart semantics without contraction does not seem to have been studied.
  - We use an equivalence $\equiv$, instead of a Kripke-style partial order $\not\!\!\supset$ as in Urquhart's general case. (We may have a need for a partial order in more sophisticated versions of our logic.)

Connections with Bunched Logic

- Peter O'Hearn and David Pym study *bunched logics*, where sequents have two structural combinators, instead of the standard single "," combinator (usually meaning $\wedge$ or $\otimes$ on the left) found in most presentations of logic. Thus, sequents are *bunches* of formulas, instead of lists of formulas. Correspondingly, there are two implications that arise as the adjuncts of the two structural combinators.

- The situation is very similar to our combinators $|$ and $\wedge$, which can combine to irreducible bunches of formulas in sequents, and to our two implications $\Rightarrow$ and $\triangleright$. However, we have a classical and a linear implication, while bunched logics have so far had an intuitionistic and a linear implication.

Conclusions

- The novel aspects of our logic lie in its explicit treatment of *space* and of the evolution of space over time (*mobility*). The logic has a linear flavor in the sense that space cannot be instantly created or deleted, although it can be transformed over time.
- These ideas can be applied to any process calculus that embodies a distinction between topological and dynamic operators.
- Our logical rules arise from a particular model. This approach makes the logic very concrete, but raises questions of logical completeness, which are being investigated.
- We are now working on generalizing the logic to the full ambient calculus (including restriction), in order to talk about properties of hidden/secret locations.

Ambient Calculus: Example

$$\overbrace{a[\underbrace{msg[\langle M\rangle \mid out\ a.\ in\ b.\ P]]}_{\textit{send } M \textit{ from } a \textit{ to } b}}^{\textit{location } a} \mid \overbrace{b[\underbrace{open\ msg.\ (n).\ P]}_{\textit{receive } n;\ \textit{do } P}}^{\textit{location } b}$$

The packet *msg* moves from *a* to *b*, mediated by the capabilities *out a* (to exit *a*), *in b* (to enter *b*), and *open msg* (to open the *msg* envelope).

$$\begin{array}{lllll}
 & & a[msg[\langle M\rangle \mid out\ a.\ in\ b.\ P]] & & \mid b[open\ msg.\ (n).\ P] \\
\text{(exit)} & \longrightarrow & a[] & \mid msg[\langle M\rangle \mid in\ b.\ P] & \mid b[open\ msg.\ (n).\ P] \\
\text{(enter)} & \longrightarrow & a[] & & \mid b[msg[\langle M\rangle] \mid open\ msg.\ (n).\ P] \\
\text{(open)} & \longrightarrow & a[] & & \mid b[\langle M\rangle \mid (n).\ P] \\
\text{(read)} & \longrightarrow & a[] & & \mid b[P\{n\leftarrow M\}]
\end{array}$$

Reduction

- Four basic reductions plus propagation, rearrangement (composition with structural congruence), and transitivity.

$n[in\ m.\ P \mid Q] \mid m[R]$	$\longrightarrow m[n[P \mid Q] \mid R]$	(Red In)
$m[n[out\ m.\ P \mid Q] \mid R]$	$\longrightarrow n[P \mid Q] \mid m[R]$	(Red Out)
$open\ m.\ P \mid m[Q]$	$\longrightarrow P \mid Q$	(Red Open)
$(n).P \mid \langle M \rangle$	$\longrightarrow P\{n \leftarrow M\}$	(Red Comm)
$P \longrightarrow Q \;\Rightarrow\; n[P] \longrightarrow n[Q]$		(Red Amb)
$P \longrightarrow Q \;\Rightarrow\; P \mid R \longrightarrow Q \mid R$		(Red Par)
$P' \equiv P,\ P \longrightarrow Q,\ Q \equiv Q' \;\Rightarrow\; P' \longrightarrow Q'$		(Red $\equiv$)

$\longrightarrow^*$ is the reflexive-transitive closure of $\longrightarrow$

Structural Congruence

- Routine definition, but used heavily in the logic and semantics.

$P \equiv P$	(Struct Refl)
$P \equiv Q \;\Rightarrow\; Q \equiv P$	(Struct Symm)
$P \equiv Q, Q \equiv R \;\Rightarrow\; P \equiv R$	(Struct Trans)
$P \equiv Q \;\Rightarrow\; P \mid R \equiv Q \mid R$	(Struct Par)
$P \equiv Q \;\Rightarrow\; !P \equiv !Q$	(Struct Repl)
$P \equiv Q \;\Rightarrow\; M[P] \equiv M[Q]$	(Struct Amb)
$P \equiv Q \;\Rightarrow\; M.P \equiv M.Q$	(Struct Action)
$P \equiv Q \;\Rightarrow\; (n).P \equiv (n).Q$	(Struct Input)
$\varepsilon.P \equiv P$	(Struct ε)
$(M.M').P \equiv M.M'.P$	(Struct .)

$P \mid Q \equiv Q \mid P$	(Struct Par Comm)
$(P \mid Q) \mid R \equiv P \mid (Q \mid R)$	(Struct Par Assoc)
$P \mid \mathbf{0} \equiv P$	(Struct Par Zero)
$!(P \mid Q) \equiv\ !P \mid\ !Q$	(Struct Repl Par)
$!\mathbf{0} \equiv \mathbf{0}$	(Struct Repl Zero)
$!P \equiv P \mid\ !P$	(Struct Repl Copy)
$!P \equiv\ !!P$	(Struct Repl Repl)

- These axioms (particularly the ones for !) are sound and complete with respect to equality of spatial trees: edge-labeled finite-depth unordered trees, with infinite-branching but finitely many distinct labels under each node.