Anytime, Anywhere
Modal Logics for Mobile Ambients

Luca Cardelli
Andy Gordon

Microsoft Research

Edinburgh, June 15, 1999

Introduction

- We have been looking for ways to express properties of mobile computations, E.g.:
  - "Here today, gone tomorrow."
  - "Eventually the agent crosses the firewall."
  - "Every agent carries a suitcase."
  - "Somewhere there is a virus."
  - "There is always at most one ambient called *n* here."

- Options include equational reasoning, reasoning on traces, or...

Spatial Logic

- Devise a process logic that can talk about *space* as well as time.
- The ambient calculus has a spatial structure given by the nesting of ambients: we want a logic that can talk about that structure:

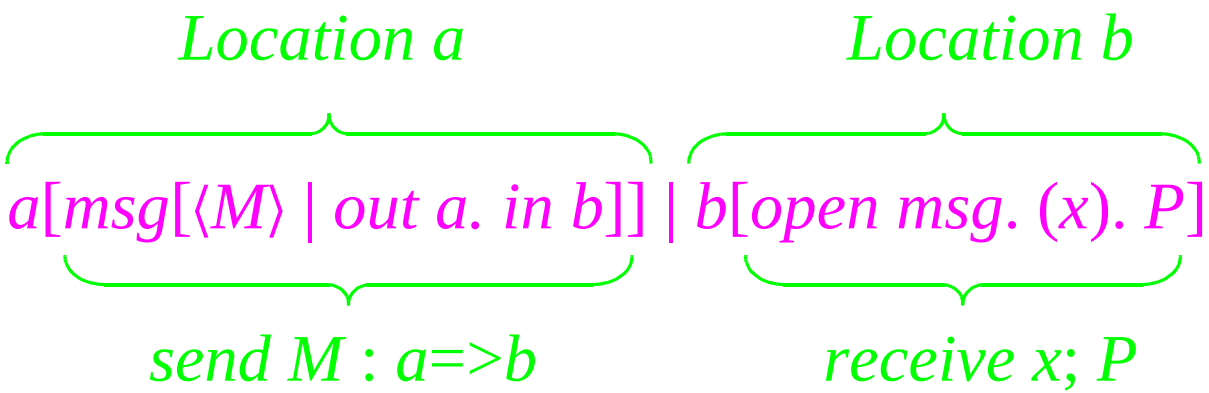
Process		*Formula*	
$\mathbf{0}$	(void)	$\mathbf{0}$	(there is nothing here)
$n[P]$	(location)	$n[\mathcal{A}]$	(there is one thing here)
$P \mid Q$	(composition)	$\mathcal{A} \mid \mathcal{B}$	(there are two things here)

- Could not find much of close relevance in the literature, except for Mads Dam's thesis and Urquhart's semantics, but we quickly diverge from both.

Ambients

- An *ambient* is a named, bounded place, where computation happens. (Can be hardware or software.) The boundary of an ambient is both a unit of mobility and a security perimeter.
- Ambients have a *name*, a collection of local *processes*, and a collection of *subambients*. That is, an ambient configuration is a tree of named locations with active processes inside.
- Ambients can move in an out of other ambients, subject to *capabilities* that are associated with ambient names. That is, the tree of location is dynamically reconfigurable (but only locally reconfigurable).
- Ambient names, and the capabilities extracted from them, are unforgeable (as in π and spi).

Example



$$a[msg[\langle M\rangle \mid out\ a.\ in\ b]] \mid b[open\ msg.\ (x).\ P]$$

(exit a) $\longrightarrow a[] \mid msg[\langle M\rangle \mid in\ b] \mid b[open\ msg.\ (x).\ P]$

(enter b) $\longrightarrow a[] \mid b[msg[\langle M\rangle] \mid open\ msg.\ (x).\ P]$

(open msg) $\longrightarrow a[] \mid b[\langle M\rangle \mid (x).\ P]$

(read M) $\longrightarrow a[] \mid b[P\{x \leftarrow M\}]$

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).

Restriction-free Ambient Calculus

$P,Q : \Pi ::=$	$M ::=$
$\mathbf{0}$	n
$P \mid Q$	$in\ M$
$!P$	$out\ M$
$M[P]$	$open\ M$
$M.P$	ε
$(n).P$	$M.M'$
$\langle M \rangle$	

$n[in\ m.\ P \mid Q] \mid m[R]$	$\longrightarrow$	$m[n[P \mid Q] \mid R]$	(enter reduction)
$m[n[out\ m.\ P \mid Q] \mid R]$	$\longrightarrow$	$n[P \mid Q] \mid m[R]$	(exit reduction)
$open\ m.\ P \mid m[Q]$	$\longrightarrow$	$P \mid Q$	(open reduction)
$(m).P \mid \langle M \rangle$	$\longrightarrow$	$P\{m \leftarrow M\}$	(read reduction)

Structural Congruence

$P \equiv P$	(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)
$P \equiv Q \Rightarrow (x).P \equiv (x).Q$	(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.

Reduction

$n[in\ m.\ P \mid Q] \mid m[R] \longrightarrow m[n[P \mid Q] \mid R]$ (Red In)

$m[n[out\ m.\ P \mid Q] \mid R] \longrightarrow n[P \mid Q] \mid m[R]$ (Red Out)

$open\ n.\ P \mid n[Q] \longrightarrow P \mid Q$ (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 ≡)

$\longrightarrow^*$ refl-tran closure of $\longrightarrow$

Syntactic Conventions

$!P \mid Q$	is read	$(!P) \mid Q$
$M.P \mid Q$	is read	$(M.P) \mid Q$
$(n).P \mid Q$	is read	$((n).P) \mid Q$

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

Why a Logic?

A recurring issue for us was how to state behavioral properties of ambients. E.g., protocol specifications.

We have formal tools for establishing equational properties. But many properties cannot easily be formulated as equations.

For example, type systems for ambients guarantee certain properties, such as that some ambients are immobile, some are persistent. It's hard to write down equations for immobility and persistence!

Our solution: use a (modal) logic tailored for ambients.

Modal Formulas

In a modal logic, the truth of a formula is relative to a state (world).

In our case, the truth of a *space-time* modal formula is relative to the *here and now* of a process. Each formula talks about the current time (before further evolution of the process) and the current place (the top-level of the process).

Therefore, 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

$\mathcal{A}, \mathcal{B} : \mathbf{\Phi} ::=$	
$\mathbf{T}$	true
$\neg\mathcal{A}$	negation (also $\mathcal{A}^{\neg}$)
$\mathcal{A} \vee \mathcal{B}$	disjunction
$\mathbf{0}$	void
$\eta[\mathcal{A}]$	location
$\mathcal{A} \mid \mathcal{B}$	composition
$\forall x.\mathcal{A}$	universal quantification over names
$\Diamond\mathcal{A}$	sometime modality (temporal)
$\varpropto\mathcal{A}$	somewhere modality (spatial)
$\mathcal{A}@\eta$	location adjunct
$\mathcal{A} \triangleright \mathcal{B}$	composition adjunct

where η is a name n or a (quantifiable) variable x.

Satisfaction Relation

$$
\begin{array}{lcl}
P \models \mathbf{T} & & \\
P \models \neg\mathcal{A} & \triangleq & \neg\, P \models \mathcal{A} \\
P \models \mathcal{A}\vee\mathcal{B} & \triangleq & P \models \mathcal{A} \vee P \models \mathcal{B} \\
P \models \mathbf{0} & \triangleq & P \equiv \mathbf{0} \\
P \models n[\mathcal{A}] & \triangleq & \exists P'{:}\Pi.\ P \equiv n[P'] \wedge P' \models \mathcal{A} \\
P \models \mathcal{A} \mid \mathcal{B} & \triangleq & \exists P', P''{:}\Pi.\ P \equiv P' \mid P'' \wedge P' \models \mathcal{A} \wedge P'' \models \mathcal{B} \\
P \models \forall x.\mathcal{A} & \triangleq & \forall m{:}\Lambda.\ P \models \mathcal{A}\{x \leftarrow m\} \\
P \models \Diamond\mathcal{A} & \triangleq & \exists P'{:}\Pi.\ P \rightarrow^{*} P' \wedge P' \models \mathcal{A} \\
P \models \mathrel{\diamond\!\!\!\!\cdot}\,\mathcal{A} & \triangleq & \exists P'{:}\Pi.\ P \downarrow^{*} P' \wedge P' \models \mathcal{A} \\
P \models \mathcal{A}@n & \triangleq & n[P] \models \mathcal{A} \\
P \models \mathcal{A} \triangleright \mathcal{B} & \triangleq & \forall P'{:}\Pi.\ P' \models \mathcal{A} \Rightarrow P \mid P' \models \mathcal{B}
\end{array}
$$

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

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

Basic Fact

Satisfaction is invariant under structural congruence:

$$(P \models \mathcal{A} \wedge P \equiv P') \Rightarrow P' \models \mathcal{A}$$

I.e.: $\{P{:}\Pi \parallel P \models \mathcal{A}\}$ is closed under $\equiv$.

Hence, formulas describe only congruence-invariant properties.

Some Derived Formulas

$\mathbf{F}$	$\triangleq \neg\mathbf{T}$	
$\mathcal{A} \Rightarrow \mathcal{B}$	$\triangleq \neg\mathcal{A} \vee \mathcal{B}$	$P \models \text{-}$ iff $P \models \mathcal{A} \Rightarrow P \models \mathcal{B}$
$\mathcal{A} \wedge \mathcal{B}$	$\triangleq \neg(\neg\mathcal{A} \vee \neg\mathcal{B})$	$P \models \text{-}$ iff $P \models \mathcal{A} \wedge P \models \mathcal{B}$
$\exists x.\mathcal{A}$	$\triangleq \neg\forall x.\neg\mathcal{A}$	$P \models \text{-}$ iff $\exists m{:}\Lambda.\ P \models \mathcal{A}\{x \leftarrow m\}$
$\Box\!\!\!\!-\mathcal{A}$	$\triangleq \neg\diamond\neg\mathcal{A}$	$P \models \text{-}$ iff $\forall P'{:}\Pi.\ P{\downarrow^*}P' \Rightarrow P' \models \mathcal{A}$
$\Box\mathcal{A}$	$\triangleq \neg\diamond\neg\mathcal{A}$	$P \models \text{-}$ iff $\forall P'{:}\Pi.\ P{\rightarrow^*}P' \Rightarrow P' \models \mathcal{A}$
$\mathcal{A}^{\mathbf{F}}$	$\triangleq \mathcal{A} \triangleright \mathbf{F}$	$P \models \text{-}$ iff $\forall P'{:}\Pi.\ P' \models \mathcal{A} \Rightarrow P \mid P' \models \mathbf{F}$
		iff $\forall P'{:}\Pi.\ \neg\ P' \models \mathcal{A}$
$\mathcal{A}^{\neg\mathbf{F}}$	$\mathcal{A}$ *valid*	$P \models \text{-}$ iff $\forall P'{:}\Pi.\ P' \models \mathcal{A}$
$\mathcal{A}^{\mathbf{F}\neg}$	$\mathcal{A}$ *satisfiable*	$P \models \text{-}$ iff $\exists P'{:}\Pi.\ P' \models \mathcal{A}$

Simple Examples

(1) $p[\mathbf{T}] \mid \mathbf{T}$

there is a *p* here (and possibly something else)

(2) $\diamond(1)$

somewhere there is a *p*

(3) $(2) \Rightarrow \Box(2)$

if there is a *p* somewhere, then forever there is a *p* somewhere

(4) $p[q[\mathbf{T}] \mid \mathbf{T}] \mid \mathbf{T}$

there is a *p* with a child *q* here

(5) $\diamond(4)$

somewhere there is a *p* with a child *q*

Claims

- The satisfaction relation is "utterly natural" (to us):
  - The definitions of $\mathbf{0}$, $\mathcal{A}|\mathcal{B}$, and $n[\mathcal{A}]$ seem inevitable, once we accept that formulas should be able to talk about the tree structure of locations, and that they should not distinguish processes that are surely indistinguishable (up to $\equiv$).
  - The connectives $\mathcal{A}@n$ and $\mathcal{A}\triangleright\mathcal{B}$ have security motivations.
  - The modalities $\Diamond\mathcal{A}$ and $\Cdot\mathcal{A}$ 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 Logic

Propositional validity

$$\mathbf{vld}\ \mathcal{A} \quad \triangleq \quad \forall P{:}\Pi.\ P \models \mathcal{A} \qquad\qquad \mathcal{A}\ \text{(closed) is valid}$$

Sequents

$$\mathcal{A} \vdash \mathcal{B} \quad \triangleq \quad \mathbf{vld}\ (\mathcal{A} \Rightarrow \mathcal{B})$$

Rules

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

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

N.B.: All the rules shown later are validated accordingly.

Conventions:

$\dashv\vdash$ means $\vdash$ in both directions

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

"Neutral" Sequents

- The logic is formulated as a sequent calculus 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, all the standard rules of sequent and natural deduction systems with multiple premises/conclusions can be derived.
  - By taking $|$ on the left of $\vdash$ as a structural operator, all the rules of intuitionistic linear logic can be derived (by appropriate mappings of the ILL connectives).
  - By taking nestings of $\wedge$ and $|$ on the left of $\vdash$ as structural "bunches", we obtain a bunched logic, with its two associated implications, $\Rightarrow$ and $\rhd$.
- This is convenient. We do not know much, however, about the metatheory of this presentation style.

Step 1: Propositional Rules

(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**) $\mathcal{A}\vdash\mathbf{F}\vee\mathcal{B}$ $\}$ $\mathcal{A}\vdash\mathcal{B}$

($\neg$-L) $\mathcal{A}\vdash\mathcal{C}\vee\mathcal{B}$ $\}$ $\mathcal{A}\wedge\neg\mathcal{C}\vdash\mathcal{B}$

($\neg$-R) $\mathcal{A}\wedge\mathcal{C}\vdash\mathcal{B}$ $\}$ $\mathcal{A}\vdash\neg\mathcal{C}\vee\mathcal{B}$

Step 2: Concurrency Rules

- Apart from our interest in mobility and nested locations, a fragment of our logic makes sense just for ordinary concurrency (i.e., for a CCS-like process calculus with **0** and |). We examine this fragment first.
- (Small caveat. To get things off the ground, one needs some process that is definitely $\neg$**0**. In our full logic, locations have this property, otherwise something must be introduced for this purpose.)

Concurrency Rules

(| **0**)	$\mathcal{A} \mid \mathbf{0} \dashv\vdash \mathcal{A}$	**0** is nothing
(| ¬**0**)	$\mathcal{A} \mid \neg\mathbf{0} \vdash \neg\mathbf{0}$	if a part is non-**0**, so is the whole
(A |)	$\mathcal{A} \mid (\mathcal{B} \mid \mathcal{C}) \dashv\vdash (\mathcal{A} \mid \mathcal{B}) \mid \mathcal{C}$	| associativity
(X |)	$\mathcal{A} \mid \mathcal{B} \vdash \mathcal{B} \mid \mathcal{A}$	| commutativity
(| ⊢)	$\mathcal{A}' \vdash \mathcal{B}';\ \mathcal{A}'' \vdash \mathcal{B}'' \ \} \ \mathcal{A}' \mid \mathcal{A}'' \vdash \mathcal{B}' \mid \mathcal{B}''$	| congruence
(| ∨)	$(\mathcal{A} \vee \mathcal{B}) \mid \mathcal{C} \vdash \mathcal{A} \mid \mathcal{C} \vee \mathcal{B} \mid \mathcal{C}$	|-∨ distribution
(| ||)	$\mathcal{A}' \mid \mathcal{A}'' \vdash \mathcal{A}' \mid \mathcal{B}'' \vee \mathcal{B}' \mid \mathcal{A}'' \vee \neg\mathcal{B}' \mid \neg\mathcal{B}''$	decomposition
(| ▷)	$\mathcal{A} \mid \mathcal{C} \vdash \mathcal{B} \ \{\ \} \ \mathcal{A} \vdash \mathcal{C} \triangleright \mathcal{B}$	|-▷ adjunction

N.B., neutral sequents make the rule (| ⊢) (and others) particularly simple, even though | does not distribute with ∧ in the "useful" direction.

The Decomposition Operator

Consider the De Morgan dual of $|$:

$\mathcal{A} \,||\, \mathcal{B} \;\triangleq\; \neg(\neg\mathcal{A} \,|\, \neg\mathcal{B})$ $\quad P \vDash$ - iff $\forall P', P'' : \Pi.\ P \equiv P' | P'' \Rightarrow P' \vDash \mathcal{A} \vee P'' \vDash \mathcal{B}$

$\mathcal{A}^{\forall} \;\triangleq\; \mathcal{A} \,||\, \mathbf{F}$ $\quad P \vDash$ - iff $\forall P', P'' : \Pi.\ P \equiv P' | P'' \Rightarrow P' \vDash \mathcal{A}$

$\mathcal{A}^{\exists} \;\triangleq\; \mathcal{A} \,|\, \mathbf{T}$ $\quad P \vDash$ - iff $\exists P', P'' : \Pi.\ P \equiv P' | P'' \wedge P' \vDash \mathcal{A}$

$\mathcal{A} \,||\, \mathcal{B}$ — 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

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

The Decomposition Axiom

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

Alternative formulations and special cases:

$\vdash (\mathcal{A}' \mid \mathcal{A}'') \wedge (\mathcal{B}' \parallel \mathcal{B}'') \vdash (\mathcal{A}' \mid \mathcal{B}'') \vee (\mathcal{B}' \mid \mathcal{A}'')$

"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 $\mathcal{A}''$."

$\vdash \neg(\mathcal{A} \mid \mathcal{B}) \vdash (\mathcal{A} \mid \mathbf{T}) \Rightarrow (\mathbf{T} \mid \neg\mathcal{B})$

"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 $\mathcal{B}$."

$\vdash \neg(\mathbf{T} \mid \mathcal{B}) \vdash \mathbf{T} \mid \neg\mathcal{B}$

The Composition Adjunct

$(|\triangleright)$ $\quad \mathcal{A} \,|\, C \vdash \mathcal{B} \;\{\!|\}\; \mathcal{A} \vdash C \triangleright \mathcal{B}$

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

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

"If anything that satisfies $\mathcal{D}$ satisfies $\mathcal{A}$, and anything that satisfies $\mathcal{B}$ satisfies 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) C."

Proof:

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

$\mathcal{A}' \vdash \mathcal{A};\ \mathcal{B} \vdash \mathcal{B}' \vdash \mathcal{A} \triangleright \mathcal{B} \vdash \mathcal{A}' \triangleright \mathcal{B}'$	$\triangleright$ 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

Step 3: Location Rules

$(n[]\ \neg\mathbf{0})$	$\}\ n[\mathcal{A}] \vdash \neg\mathbf{0}$	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
$(n[]\ \mathbf{F})$	$\}\ n[\mathbf{F}] \vdash \mathbf{F}$	can't hold absurdity
$(n[]\ @)$	$n[\mathcal{A}] \vdash \mathcal{B}\ \{\}\ \mathcal{A} \vdash \mathcal{B}@n$	$n[]$-@ adjunction

Some Derived Rules

Consequences:

$\mathcal{A} \vdash \mathcal{B} \;\}\; \mathcal{A}@n \vdash \mathcal{B}@n$ @ 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 $\mathcal{A}$
$\Box((n[\mathbf{T}] \Rightarrow n[\mathcal{A}])^{\forall})$	every *n* everywhere satisfies $\mathcal{A}$

Step 4: Time and Space Modalities

$(\Diamond)$ $\quad \} \ \Diamond\mathcal{A} \dashv\vdash \neg\Box\neg\mathcal{A}$

$(\Box\ \mathrm{K})$ $\quad \} \ \Box(\mathcal{A} \Rightarrow \mathcal{B}) \vdash \Box\mathcal{A} \Rightarrow \Box\mathcal{B}$

$(\Box\ \mathrm{T})$ $\quad \} \ \Box\mathcal{A} \vdash \mathcal{A}$

$(\Box\ 4)$ $\quad \} \ \Box\mathcal{A} \vdash \Box\Box\mathcal{A}$

$(\Box \vdash)$ $\quad \mathcal{A} \vdash \mathcal{B} \ \} \ \Box\mathcal{A} \vdash \Box\mathcal{B}$

$(\Diamond)$ $\quad \} \ \Diamond\mathcal{A} \dashv\vdash \neg\, \Box\, \neg\mathcal{A}$

$(\Box\ \mathrm{K})$ $\quad \} \ \Box(\mathcal{A} \Rightarrow \mathcal{B}) \vdash \Box\mathcal{A} \Rightarrow \Box\mathcal{B}$

$(\Box\ \mathrm{T})$ $\quad \} \ \Box\mathcal{A} \vdash \mathcal{A}$

$(\Box\ 4)$ $\quad \} \ \Box\mathcal{A} \vdash \Box\,\Box\mathcal{A}$

$(\Box \vdash)$ $\quad \mathcal{A} \vdash \mathcal{B} \ \} \ \Box\mathcal{A} \vdash \Box\mathcal{B}$

S4, but not S5:

$\neg$ ***vld*** $\Diamond\mathcal{A} \vdash \Box\Diamond\mathcal{A}$

$\neg$ ***vld*** $\Diamond\mathcal{A} \vdash \Box\,\Diamond\mathcal{A}$

Additional Modality Rules

$(\Diamond\ n[])$ $\quad\}\ n[\Diamond\mathcal{A}] \vdash \Diamond n[\mathcal{A}]$

$(\Diamond \mid)$ $\quad\}\ (\Diamond\mathcal{A}) \mid (\Diamond\mathcal{B}) \vdash \Diamond(\mathcal{A} \mid \mathcal{B})$

$(\Diamond\!\!\!\!-\ n[])$ $\quad\}\ n[\Diamond\!\!\!\!-\mathcal{A}] \vdash \Diamond\!\!\!\!-\mathcal{A}$

$(\Diamond\!\!\!\!- \mid)$ $\quad\}\ (\Diamond\!\!\!\!-\mathcal{A}) \mid \mathcal{B} \vdash \Diamond\!\!\!\!-(\mathcal{A} \mid \mathbf{T})$

$(\Diamond\!\!\!\!-\Diamond)$ $\quad\}\ \Diamond\!\!\!\!-\Diamond\mathcal{A} \vdash \Diamond\Diamond\!\!\!\!-\mathcal{A}$

if somewhere sometime $\mathcal{A}$, then sometime somewhere $\mathcal{A}$

Step 5: Validity and Satisfiability

$P \models \mathcal{A}^{\mathbf{F}}$ iff $\forall P' {:}\Pi.\ P' \models \mathcal{A} \Rightarrow P \mid P' \models \mathbf{F}$

iff $\forall P' {:}\Pi.\ \neg P' \models \mathcal{A}$ iff $\mathcal{A}$ is unsatisfiable

$(\triangleright\mathbf{F}\ \neg)$ $\quad \} \ \mathcal{A}^{\mathbf{F}} \vdash \mathcal{A}^{\neg}$ if $\mathcal{A}$ is unsatisfiable then $\mathcal{A}$ is false

$(\neg\ \triangleright\mathbf{F})$ $\quad \} \ \mathcal{A}^{\mathbf{F}\neg} \vdash \mathcal{A}^{\mathbf{FF}}$ if $\mathcal{A}$ is satisfiable then $\mathcal{A}^{\mathbf{F}}$ is unsatisfiable

We can reflect validity and satisfiability within the logic:

$Vld\ \mathcal{A} \triangleq \mathcal{A}^{\neg\mathbf{F}}$ $\qquad P \models Vld\ \mathcal{A}$ iff $\forall P' {:}\Pi.\ P' \models \mathcal{A}$

$Sat\ \mathcal{A} \triangleq \mathcal{A}^{\mathbf{F}\neg}$ $\qquad P \models Sat\ \mathcal{A}$ iff $\exists P' {:}\Pi.\ P' \models \mathcal{A}$

Then, as derived rules we have that *Vld*,*Sat* are S5 modalities.
(That is, S4 plus: $\} \ Sat\ \mathcal{A} \vdash Vld\ Sat\ \mathcal{A}$.)

Reflecting Name Equality

Name equality can be defined within the logic:

$$\eta = \mu \triangleq \eta[\mathbf{T}]@\mu$$

Since (for any substitution applied to η,μ):

$$P \models \eta[\mathbf{T}]@\mu$$
$$\text{iff } \mu[P] \models \eta[\mathbf{T}]$$
$$\text{iff } \eta = \mu \wedge P \models \mathbf{T}$$
$$\text{iff } \eta = \mu$$

Example: "Any two ambients here have different names":

$$\forall x.\forall y.\ x[\mathbf{T}] \mid y[\mathbf{T}] \mid \mathbf{T} \Rightarrow \neg\, x{=}y$$

What Kind of Logic is This?

- Not sure where we stand in the Big Picture:
  - A relevant logic without contraction? (Heresy!)
  - A linear logic with distribution? (Anathema!)
  - Two implications, one classical and additive, $\Rightarrow$, one intuitionistic and multiplicative, $\triangleright$? (Confusion!)
- Admittedly, this is intentionally ad-hoc: we are motivated by capturing truths about the ambient calculus.
- Still, there are interesting and unusual sublogics that seem applicable to other contexts and, in particular, to other process calculi.

Urquhart Decontracted

- (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 $\mathcal{A}|\mathcal{B}$ is defined just like *intesional 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 $\sqsubseteq$ as in Urquhart's general case. (We may have a need for a partial order in more sophisticated versions of our logic.)

Girard Redistributed

- (Noted after the fact [Winskel, O'Hearn].) In an appropriate sense, $\mathcal{A}|\mathcal{B}$ is *linear tensor*, and $\mathcal{A}\triangleright\mathcal{B}$ is *linear implication*. A precise connection can be made with full intuitionistic linear logic.
- Except:
  - The additives, $\oplus_{\mathrm{ILL}}$ and $\&_{\mathrm{ILL}}$, distribute (a derived rule).
  - $\bot_{\mathrm{ILL}}$ collapses with $\mathbf{0}_{\mathrm{ILL}}$.
  - $!_{\mathrm{ILL}}$ is rather degenerate. $(!_{\mathrm{ILL}}\mathcal{A}) \multimap_{\mathrm{ILL}} \mathcal{B}$ does not seem to have an interesting interpretation.
- Still, the multiplicative fragment seems faithful.

Syntactic Connections with Linear Logic

- Intuitionistic linear logic (ILL) can be embedded in our logic:

$$\begin{array}{lcl} \mathbf{1}_{\mathrm{ILL}} & \triangleq & \mathbf{0} \\ \bot_{\mathrm{ILL}} & \triangleq & \mathbf{F} \\ \top_{\mathrm{ILL}} & \triangleq & \mathbf{T} \\ \mathbf{0}_{\mathrm{ILL}} & \triangleq & \mathbf{F} \end{array} \qquad \begin{array}{lcl} \mathcal{A} \oplus \mathcal{B} & \triangleq & \mathcal{A} \vee \mathcal{B} \\ \mathcal{A} \,\&\, \mathcal{B} & \triangleq & \mathcal{A} \wedge \mathcal{B} \\ \mathcal{A} \otimes \mathcal{B} & \triangleq & \mathcal{A} \mid \mathcal{B} \\ \mathcal{A} \multimap \mathcal{B} & \triangleq & \mathcal{A} \rhd \mathcal{B} \\ !\mathcal{A} & \triangleq & \mathbf{0} \wedge (\mathbf{0} \Rightarrow \mathcal{A})^{\neg \mathbf{F}} \end{array}$$

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

Semantic Connections with Linear Logic

- A (commutative) quantale $\mathcal{Q}$ is a structure
  $\langle S : \mathrm{Set}, \leq : S^2 \to \mathrm{Bool}, \otimes : S^2 \to S, 1 : S, \bigvee : \mathcal{P}(S) \to S \rangle$ such that:

  $\leq, \bigvee$: a complete join semilattice

  $\otimes, 1$: a commutative monoid

  $p \otimes \bigvee Q = \bigvee \{p \otimes q \parallel q \in Q\}$

- They are complete models of Intuitionistic Linear Logic (ILL):

$$[\![\mathcal{A} \oplus \mathcal{B}]\!] \triangleq \bigvee \{[\![\mathcal{A}]\!], [\![\mathcal{B}]\!]\} \qquad [\![\mathbf{1}_{\mathrm{ILL}}]\!] \triangleq 1$$
$$[\![\mathcal{A} \,\&\, \mathcal{B}]\!] \triangleq \bigvee \{C \parallel C \leq [\![\mathcal{A}]\!] \wedge C \leq [\![\mathcal{B}]\!]\} \qquad [\![\bot_{\mathrm{ILL}}]\!] \triangleq \text{any element of } S$$
$$[\![\mathcal{A} \otimes \mathcal{B}]\!] \triangleq [\![\mathcal{A}]\!] \otimes [\![\mathcal{B}]\!] \qquad [\![\top_{\mathrm{ILL}}]\!] \triangleq \bigvee S$$
$$[\![\mathcal{A} \multimap \mathcal{B}]\!] \triangleq \bigvee \{C \parallel C \otimes [\![\mathcal{A}]\!] \leq [\![\mathcal{B}]\!]\} \qquad [\![\mathbf{0}_{\mathrm{ILL}}]\!] \triangleq \bigvee \emptyset$$
$$[\![!\mathcal{A}]\!] \triangleq \upsilon X.\, [\![\mathbf{1} \,\&\, \mathcal{A} \,\&\, X \otimes X]\!] \quad \text{where} \quad \upsilon X.\, A\{X\} \triangleq \bigvee \{C \parallel C \leq A\{C\}\}$$

$$\mathbf{vld}_{\mathrm{ILL}}(\mathcal{A}_1, \ldots, \mathcal{A}_n \vdash_{\mathrm{ILL}} \mathcal{B})_{\mathcal{Q}} \triangleq [\![\mathcal{A}_1]\!]_{\mathcal{Q}} \otimes_{\mathcal{Q}} \ldots \otimes_{\mathcal{Q}} [\![\mathcal{A}_n]\!]_{\mathcal{Q}} \leq_{\mathcal{Q}} [\![\mathcal{B}]\!]_{\mathcal{Q}}$$

The Process Quantale

- The sets of processes closed under $\equiv$ and ordered by inclusion form a quantale (let $A^{\equiv} \triangleq \{P \parallel P \equiv Q \wedge Q \in A\}$):

  $\mathbf{\Phi} \triangleq \langle \Phi, \subseteq, \otimes, \mathbf{1}, \bigcup \rangle$ where, for $A,B \subseteq \Pi$:

  $\Phi \triangleq \{A^{\equiv} \parallel A \subseteq \Pi\}$

  $1_{\mathbf{\Phi}} \triangleq \{\mathbf{0}\}^{\equiv}$, $A \otimes_{\mathbf{\Phi}} B \triangleq \{P \mid Q \parallel P \in A \wedge Q \in B\}^{\equiv}$

- Our syntactic definitions of ILL operators match their quantale interpretation. (E.g.: $[\![\mathcal{A} \otimes \mathcal{B}]\!]_{\mathbf{\Phi}} = [\![\mathcal{A}]\!]_{\mathbf{\Phi}} \otimes_{\mathbf{\Phi}} [\![\mathcal{B}]\!]_{\mathbf{\Phi}}$, $[\![!\mathcal{A}]\!]_{\mathbf{\Phi}} = !_{\mathbf{\Phi}}[\![\mathcal{A}]\!]_{\mathbf{\Phi}}$.)

- Interpretation of formulas:

  $[\![\mathcal{A}]\!] \triangleq \{P{:}\Pi \parallel P \vDash \mathcal{A}\}$ where $[\![\mathcal{A}]\!] = [\![\mathcal{A}]\!]^{\equiv}$

- Our validity matches ILL validity for ILL sequents:

  $\mathbf{vld}_{\mathrm{ILL}}(\mathcal{A}_1, \ldots, \mathcal{A}_n \vdash_{\mathrm{ILL}} \mathcal{B})_{\mathbf{\Phi}} \Leftrightarrow \mathbf{vld}(\mathcal{A}_1 \mid \ldots \mid \mathcal{A}_n \vdash \mathcal{B})$

Applications

- Model Checking
  - We have an algorithm for deciding the $\models$ relation for **!**-free processes and $\triangleright$-free formulas.
- Expressing Locking
  - If $E, n{:}Amb^{\bullet}[S] \vdash P : T$ (a typing judgment asserting that no ambient called n can ever be opened in P), then:

    $$P \models \Box(\Diamond an\ n \Rightarrow \Box\Diamond an\ n)$$
- Expressing Immobility
  - If $E, p{:}Amb^{\bullet}[S], q{:}Amb^{\bullet}[\overset{\vee}{-}S'] \vdash P : T$ (a typing judgment asserting that no ambient called q can ever move within P), then:

    $$P \models \Box(\Diamond(p\ parents\ q) \Rightarrow \Box\Diamond(p\ parents\ q))$$

    where $p\ parents\ q \triangleq p[q[\mathbf{T}] \mid \mathbf{T}] \mid \mathbf{T}$

Future Directions: Fixpoints

- Abadi, Lamport, and Plotkin and have described *reactive* specifications such that:

$$\mathcal{A} \rightarrow \mathcal{B} \mid \mathcal{B} \rightarrow \mathcal{A} \;\Rightarrow\; \mathcal{A} \wedge \mathcal{B}$$

  Define: $\mathcal{Y} \rightarrow \mathcal{Z} \;\triangleq\; \mu\mathcal{X}.\, (\mathcal{X} \triangleright \mathcal{Y}) \triangleright \mathcal{Z}$. Then:

$$\mathcal{A} \rightarrow \mathcal{B} \;=\; ((\mathcal{A} \rightarrow \mathcal{B}) \triangleright \mathcal{A}) \triangleright \mathcal{B} \;\Rightarrow\; (\mathcal{B} \rightarrow \mathcal{A}) \triangleright \mathcal{B}$$
$$\mathcal{B} \rightarrow \mathcal{A} \;=\; ((\mathcal{B} \rightarrow \mathcal{A}) \triangleright \mathcal{B}) \triangleright \mathcal{A} \;\Rightarrow\; (\mathcal{A} \rightarrow \mathcal{B}) \triangleright \mathcal{A}$$

$$\mathcal{A} \rightarrow \mathcal{B} \mid \mathcal{B} \rightarrow \mathcal{A} \;\Rightarrow\; (\mathcal{B} \rightarrow \mathcal{A}) \triangleright \mathcal{B} \mid \mathcal{B} \rightarrow \mathcal{A} \;\Rightarrow\; \mathcal{B}$$
$$\mathcal{A} \rightarrow \mathcal{B} \mid \mathcal{B} \rightarrow \mathcal{A} \;\Rightarrow\; \mathcal{A} \rightarrow \mathcal{B} \mid (\mathcal{A} \rightarrow \mathcal{B}) \triangleright \mathcal{A} \;\Rightarrow\; \mathcal{A}$$

- Modalities and their variations can be defined from fixpoints. Moreover, we can express new useful predicates:

$$\not{n} \;\triangleq\; \neg\Diamond(n[\mathbf{T}] \mid \mathbf{T})$$
$$\mathit{unique}\ n \;\triangleq\; \mu\mathcal{X}.\, \not{n} \mid (n[\not{n}] \vee \exists y{\neq}n.\, y[\mathcal{X}])$$

Conclusions

- The novel aspects of our logic lie in its treatment of *space* (spatial structures) and of the evolution of space over time (mobility).
- The logic has a strong intensional flavor, reflecting the fact that space has intensional properties. The logic has a linear flavor in the sense that space cannot be instantly created or deleted.
- These principles can be applied to any process calculus that embodies a distinction between topological and dynamic operators.
- The logic is based on strong computational intuitions, so we are not too timid about our choice of connectives. However, from a purely logical point of view, it seems to have unusual properties (perhaps accidental to our presentation).