

# Logics for Mobility

*Luca Cardelli*  
*Andy Gordon*

Microsoft Research

Tokyo 2000-08-21

# 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."
  
- As with properties of ordinary concurrent computations, options include equational reasoning (hard), reasoning on traces (ugly), and reasoning via modal (e.g. temporal) logics.

# Spatial Logics

- 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

$\mathbf{0}$	(void)
$n[P]$	(location)
$P \mid Q$	(composition)

## Formulas

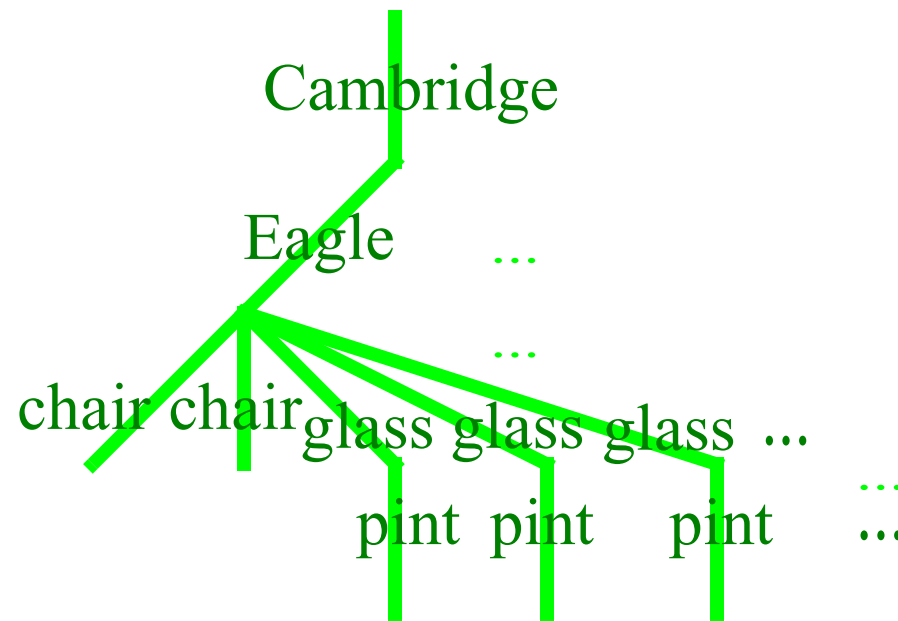
$\mathbf{0}$	(there is nothing here)
$n[\mathcal{A}]$	(there is one thing here)
$\mathcal{A} \mid \mathcal{B}$	(there are two things here)

## Trees



# Spatial Structures

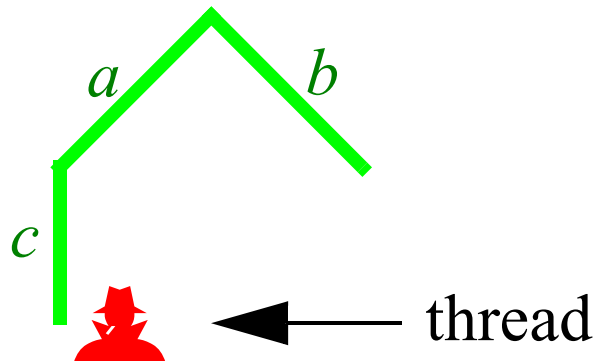
- Our basic model of space is going to be *finite-depth edge-labeled unordered trees*; for short: *spatial trees*, represented by a syntax of *spatial expressions*. Unbounded resources are represented by infinite branching:



Cambridge[Eagle[chair[0] | chair[0] | !glass[pint[0]]] | ...]

# Ambient Structures

- Spatial expressions/trees are a subset of *ambient expressions/trees*, where we can represent not only the spatial aspects, but also the dynamic aspects of mobile computation.



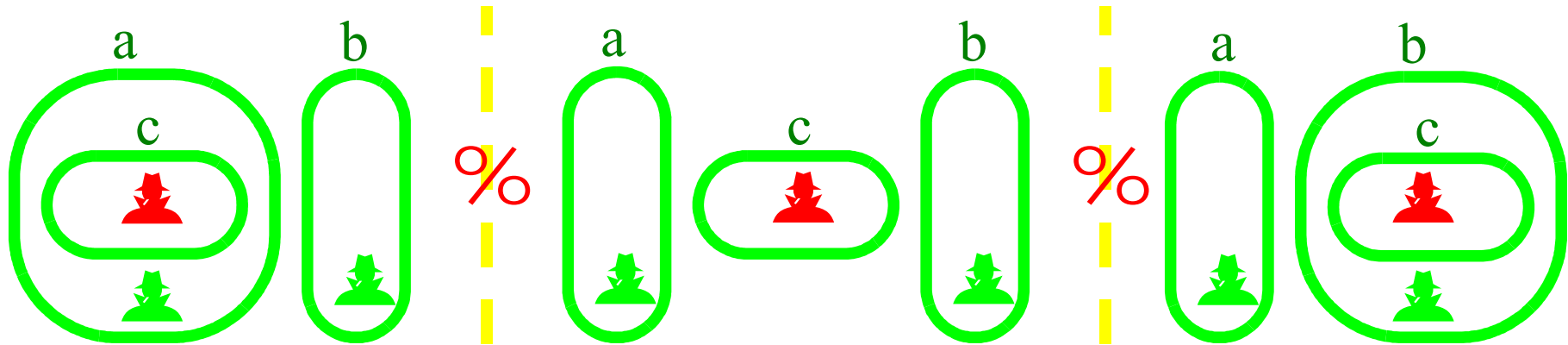
- An ambient tree is a spatial tree with, possibly, threads at each node that can locally change the shape of the tree.

$$a[c[out\ a.\ in\ b.P] \mid b[0]]$$

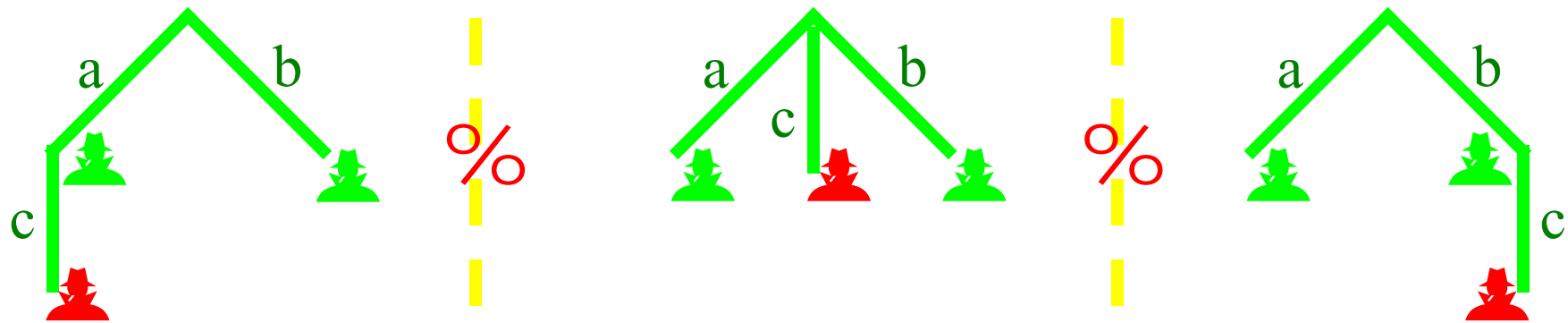
# Mobility

*Mobility* is change of spatial structures over time.

Intuition



Semantics



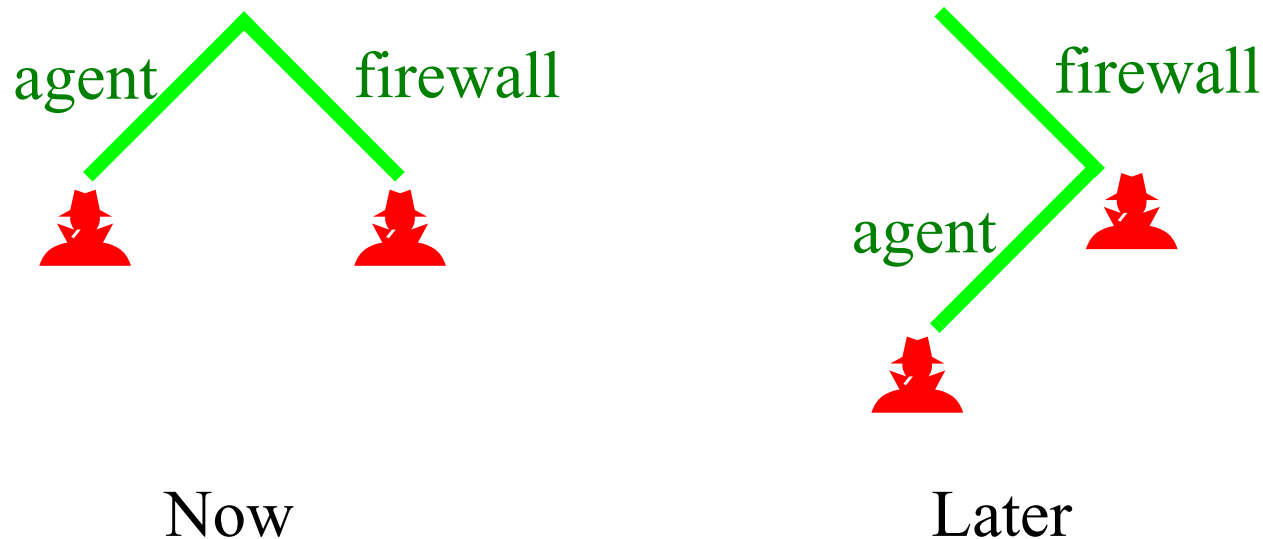
Syntax

$a[c[R] \mid P] \mid b[Q]$     %     $a[P] \mid c[R'] \mid b[Q]$     %     $a[P] \mid b[c[R'']] \mid Q$

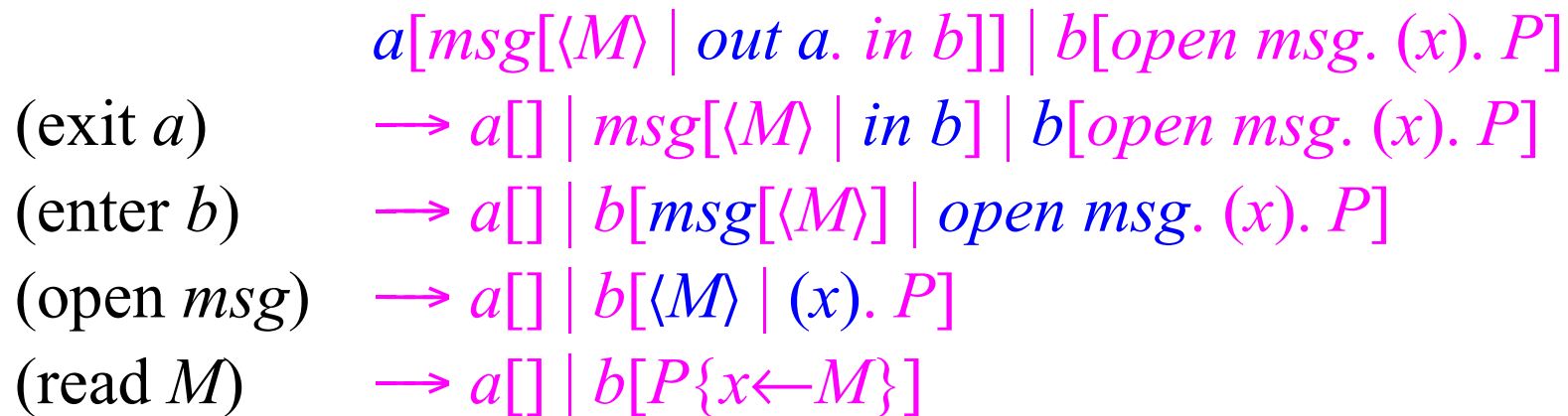
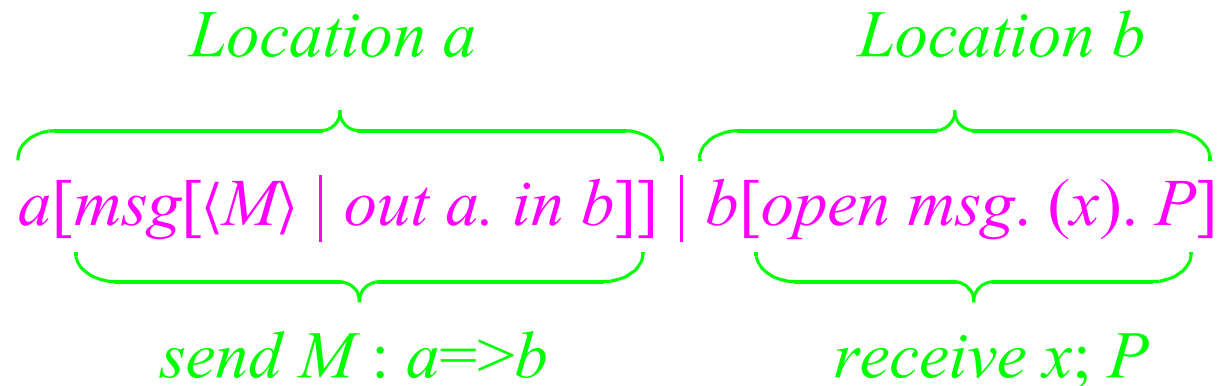
# Properties of Mobile Computation

■ These often have the form:

- *Right now*, we have a spatial configuration, and *later*, we have another spatial configuration.
- E.g.: Right now, the agent is outside the firewall, and later (after running an authentication protocol), the agent is inside the firewall.



# Ambient Calculus: Example



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).



# Ambient Calculus

$P, Q : \Pi ::=$	<i>(processes)</i>	$M ::=$	<i>(messages)</i>
$(\nu n)P$		$n$	
$\mathbf{0}$		$in\ M$	
$P \mid Q$		$out\ M$	
$!P$		$open\ M$	
$M[P]$		$\varepsilon$	
$M.P$		$M.M'$	
$(n).P$			
$\langle M \rangle$			

$$\begin{aligned} n[] &\triangleq n[\mathbf{0}] \\ M &\triangleq M.\mathbf{0} \end{aligned} \quad (\text{where appropriate})$$

# 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  $P \rightarrow^* Q$ :
  - Defining the mobility and communication actions.
  - Up to structural congruence:

$$P \equiv P', P' \rightarrow Q', Q' \equiv Q \quad \Rightarrow \quad P \rightarrow Q$$

# Reduction

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

$$\begin{aligned} n[in\ m.\ P \mid Q] \mid m[R] &\longrightarrow m[n[P \mid Q] \mid R] && \text{(Red In)} \\ m[n[out\ m.\ P \mid Q] \mid R] &\longrightarrow n[P \mid Q] \mid m[R] && \text{(Red Out)} \\ open\ n.\ P \mid n[Q] &\longrightarrow P \mid Q && \text{(Red Open)} \\ (n).\ P \mid \langle M \rangle &\longrightarrow P\{n \leftarrow M\} && \text{(Red Comm)} \end{aligned}$$

$$\begin{aligned} P \longrightarrow Q &\Rightarrow (\nu n)P \longrightarrow (\nu n)Q && \text{(Red Res)} \\ P \longrightarrow Q &\Rightarrow n[P] \longrightarrow n[Q] && \text{(Red Amb)} \\ P \longrightarrow Q &\Rightarrow P \mid R \longrightarrow Q \mid R && \text{(Red Par)} \\ P' \equiv P, P \longrightarrow Q, Q \equiv Q' &\Rightarrow P' \longrightarrow Q' && \text{(Red } \equiv) \end{aligned}$$

$\longrightarrow^*$

refl-tran closure of  $\longrightarrow$

# Structural Congruence

■ Routine, but used heavily in the logic and in the 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)
$P \equiv Q \Rightarrow (\nu n)P \equiv (\nu n)Q$	(Struct Res)
$P \equiv Q \Rightarrow P \mid R \equiv Q \mid R$	(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 $\varepsilon$ )
$(M.M').P \equiv M.M'.P$	(Struct .)

$(\nu n)\mathbf{0} \equiv \mathbf{0}$  (Struct Res Zero)

$(\nu n)(\nu m)P \equiv (\nu m)(\nu n)P$  (Struct Res Res)

$(\nu n)(P \mid Q) \equiv P \mid (\nu n)Q$  if  $n \notin fn(P)$  (Struct Res Par)

$(\nu n)(m[P]) \equiv m[(\nu n)P]$  if  $n \neq m$  (Struct Res Amb)

$P \mid \mathbf{0} \equiv P$  (Struct Par Zero)

$P \mid Q \equiv Q \mid P$  (Struct Par Comm)

$(P \mid Q) \mid R \equiv P \mid (Q \mid R)$  (Struct Par Assoc)

$!(P \mid Q) \equiv !P \mid !Q$  (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 (N.B.: !) 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.

## Space-Time Modalities

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. The formula  $n[0]$  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

$A, B : \Phi ::=$

( $\eta$  is a name  $n$  or a variable  $x$ )

$\mathbf{T}$

true

$\neg A$

negation

$A \vee B$

disjunction

$\mathbf{0}$

void

$A | B$

composition

$A \triangleright B$

composition adjunct

$\eta[A]$

location

$A @ \eta$

location adjunct

$\eta \textcircled{R} A$

revelation

$A \textcircled{O} \eta$

revelation adjunct

$" A$

somewhere modality

$\diamond A$

sometime modality

$\forall x. A$

universal quantification over names

# Satisfaction Relation

$$P \models \mathbf{T}$$

$$P \models \neg \mathcal{A} \quad \triangleq \quad \neg P \models \mathcal{A}$$

$$P \models \mathcal{A} \vee \mathcal{B} \quad \triangleq \quad P \models \mathcal{A} \vee P \models \mathcal{B}$$

$$P \models \mathbf{0} \quad \triangleq \quad P \equiv \mathbf{0}$$

$$P \models \mathcal{A} \mid \mathcal{B} \quad \triangleq \quad \exists P', P'': \Pi. P \equiv P' \mid P'' \wedge P' \models \mathcal{A} \wedge P'' \models \mathcal{B}$$

$$P \models \mathcal{A} \triangleright \mathcal{B} \quad \triangleq \quad \forall P': \Pi. P' \models \mathcal{A} \Rightarrow P \mid P' \models \mathcal{B}$$

$$P \models n[\mathcal{A}] \quad \triangleq \quad \exists P': \Pi. P \equiv n[P'] \wedge P' \models \mathcal{A}$$

$$P \models \mathcal{A} @ n \quad \triangleq \quad n[P] \models \mathcal{A}$$

$$P \models n \textcircled{\mathcal{A}} \quad \triangleq \quad \exists P': \Pi. P \equiv (\nu n)P' \wedge P' \models \mathcal{A}$$

$$P \models \mathcal{A} \textcircled{n} \quad \triangleq \quad (\nu n)P \models \mathcal{A}$$

$$P \models \text{"} \mathcal{A} \quad \triangleq \quad \exists P': \Pi. P \downarrow^* P' \wedge P' \models \mathcal{A}$$

$$P \models \diamond \mathcal{A} \quad \triangleq \quad \exists P': \Pi. P \rightarrow^* P' \wedge P' \models \mathcal{A}$$

$$P \models \forall x. \mathcal{A} \quad \triangleq \quad \forall m: \Lambda. P \models \mathcal{A}\{x \leftarrow m\}$$

$P \downarrow P'$  iff  $\exists n, P''. P \equiv n[P'] \mid P''$ .  $\downarrow^*$  is the refl-trans closure of  $\downarrow$



# Satisfaction Relation for Trees

- $\models 0$

$$\begin{array}{c} | \\ \triangle \\ P \end{array} \overset{n}{\models} n[\mathcal{A}] \text{ if } \triangle_P \models \mathcal{A}$$

$$\triangle_{P|Q} \models \mathcal{A} | \mathcal{B} \text{ if } \triangle_P \models \mathcal{A} \text{ and } \triangle_Q \models \mathcal{B}$$

$$\triangle_{\triangle_P \triangle_Q} \models " \mathcal{A} \text{ if } \triangle_Q \models \mathcal{A}$$

$$\triangle_P \models \diamond \mathcal{A} \text{ if } \triangle_P \%^* \triangle_Q \text{ and } \triangle_Q \models \mathcal{A}$$

$$\triangle P \models C@n \text{ if } \begin{array}{c} | \\ \triangle P \end{array} \models C$$

$$\triangleleft P \models \mathcal{A} \triangleright \mathcal{B} \text{ if for all } \triangleleft Q \models \mathcal{A}, \text{ we have } \triangleleft P \mid Q \models \mathcal{B}$$

**Basic Fact:** Satisfaction is invariant under structural congruence:

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

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

Hence, formulas describe only congruence-invariant properties.

## Simple Examples

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

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

(2)  $\Box (1)$

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)  $\Box (4)$

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

# Revelation

$$P \vDash n^{\circledast} \mathcal{A} \quad \triangleq \quad \exists P':\Pi. P \equiv (\nu n)P' \wedge P' \vDash \mathcal{A}$$

■  $n^{\circledast} \mathcal{A}$  is read, informally:

- *Reveal* a private name as  $n$  and check that the revealed process satisfies  $\mathcal{A}$ .
- Pull (by  $\equiv$ ) a  $(\nu n)$  binder at the top and check that the stripped process satisfies  $\mathcal{A}$ .

■ Ex.:  $n^{\circledast} n[0]$ : reveal a private name (say,  $p$ ) as  $n$  and check the presence of an empty  $n$  ambient in the revealed process.

$$(\nu p)p[0] \vDash n^{\circledast} n[0]$$

$$\text{since } (\nu p)p[0] \equiv (\nu n)n[0] \text{ and } n[0] \vDash n[0]$$

■ More examples of revelation:

$0 \models n^{\circledast}0$       since  $0 \equiv (vn)0$  and  $0 \models 0$

$m[0] \models n^{\circledast}T$       since  $m[0] \equiv (vn)m[0]$  and  $m[0] \models T$

$n[0] \not\models n^{\circledast}T$       since:  $n[0] \not\equiv (vn)...$

■ Therefore, the set of processes satisfying  $n^{\circledast}A$  is

- closed under  $\alpha$ -variants
- closed under  $\equiv$ -variants
- not closed under changes in the set of free names
- not closed under reduction (free names may disappear)
- not closed under any equivalence that includes reduction
- still ok for temporal reasoning:  $\neg n^{\circledast}A \wedge \diamond n^{\circledast}A$

# Some Derived Formulas

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

# Revelation Derived Formulas

$\odot n$	$\triangleq \neg n \textcircled{\mathbf{T}}$	$P \models -$ iff $\neg \exists P' \in \Pi. P \equiv (\nu n)P'$ iff $n \in fn(P)$
<i>closed</i>	$\triangleq \neg \exists x. \odot x$	$P \models -$ iff $\neg \exists n:\Lambda. n \in fn(P)$
<i>separate</i>	$\triangleq \neg \exists x. \odot x \mid \odot x$	$P \models -$ iff $\neg \exists n:\Lambda, P' \in \Pi, P'' \in \Pi.$ $P \equiv P' \mid P'' \wedge n \in fn(P') \wedge n \in fn(P'')$

## ■ Examples :

$$n[] \models \odot n$$

$$(\nu m)m[] \models (\nu x)x[]$$

$$(\nu m)m[] \models (\nu x)n[]$$

$$(\nu n)n[] \mid (\nu n)n[] \not\models (\nu x)(x[] \mid x[])$$

$$(\nu n)(n[] \mid n[]) \not\models (\nu x)x[] \mid (\nu x)x[]$$

# Name Equality

Name equality can be defined within the logic:

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

Since (for any substitution applied to  $\eta, \mu$ ):

$$P \vDash \eta[\mathbf{T}]@ \mu$$

$$\text{iff } \mu[P] \vDash \eta[\mathbf{T}]$$

$$\text{iff } \eta = \mu \wedge P \vDash \mathbf{T}$$

$$\text{iff } \eta = \mu$$

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

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



# Claims

- The satisfaction relation looks natural (to us):
  - The definitions of  $\mathbf{0}$ ,  $n[\mathcal{A}]$ , and  $\mathcal{A}|\mathcal{B}$  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 connective  $n\textcircled{\mathcal{R}}\mathcal{A}$  is useful in security specs.
  - 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

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

Sequents

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

Rules

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

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

(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 (4 of them!):

- $\wedge / \Rightarrow$  (classical)

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

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

$$\mathcal{A} | C \vdash \mathcal{B} \quad \text{iff} \quad \mathcal{A} \vdash C \triangleright \mathcal{B}$$

- $n[-] / -@n$  (location)

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

- $n^{\textcircled{R}}- / -\textcircled{O}n$  (restriction)

$$n^{\textcircled{R}}\mathcal{A} \vdash \mathcal{B} \quad \text{iff} \quad \mathcal{A} \vdash \mathcal{B}\textcircled{O}n$$

■ 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 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, we can derive all the standard rules of sequent and natural deduction systems with multiple premises/conclusions.
  - By taking  $|$  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  $|$  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)  $A \wedge (C \wedge D) \vdash B \quad \{ \} \quad (A \wedge C) \wedge D \vdash B$
- (A-R)  $A \vdash (C \vee D) \vee B \quad \{ \} \quad A \vdash C \vee (D \vee B)$
- (X-L)  $A \wedge C \vdash B \quad \{ \} \quad C \wedge A \vdash B$
- (X-R)  $A \vdash C \vee B \quad \{ \} \quad A \vdash B \vee C$
- (C-L)  $A \wedge A \vdash B \quad \{ \} \quad A \vdash B$
- (C-R)  $A \vdash B \vee B \quad \{ \} \quad A \vdash B$
- (W-L)  $A \vdash B \quad \{ \} \quad A \wedge C \vdash B$
- (W-R)  $A \vdash B \quad \{ \} \quad A \vdash C \vee B$
- (Id)  $\{ \} \quad A \vdash A$
- (Cut)  $A \vdash C \vee B; A' \wedge C \vdash B' \quad \{ \} \quad A \wedge A' \vdash B \vee B'$
- (T)  $A \wedge \mathbf{T} \vdash B \quad \{ \} \quad A \vdash B$
- (F)  $A \vdash \mathbf{F} \vee B \quad \{ \} \quad A \vdash B$
- ( $\neg$ -L)  $A \vdash C \vee B \quad \{ \} \quad A \wedge \neg C \vdash B$
- ( $\neg$ -R)  $A \wedge C \vdash B \quad \{ \} \quad A \vdash \neg C \vee B$

# Rules: Composition

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

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

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

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

$\mathcal{A} || \mathcal{B}$  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

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

Alternative formulations and special cases:

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

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

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

"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  $\mathcal{B}$ ."

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

$$\{ \neg(\mathcal{A} | \mathcal{B}) \vdash (\neg \mathcal{A} | \mathbf{T}) \vee (\mathbf{T} | \neg \mathcal{B})$$



# The Composition Adjunct

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

"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,  $P \models \mathcal{A} \triangleright \mathcal{B}$  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

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

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

Proof:  $A \triangleright B \vdash A \triangleright B \{ (A \triangleright B) \mid A \vdash B$  by (Id), ( $\mid \triangleright$ )

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

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

Proof:

$$\begin{array}{l} \mathcal{D} \vdash A; A \triangleright B \vdash A \triangleright B \{ \mathcal{D} \mid A \triangleright B \vdash A \mid A \triangleright B \quad \text{assumption, (Id), } (\mid \vdash) \\ A \mid A \triangleright B \vdash B \quad \text{above} \\ B \vdash C \quad \text{assumption} \end{array}$$

## More Derived Rules

- $\{ \mathcal{A} \vdash \mathbf{T} \mid \mathcal{A}$       you can always add more pieces (if they are  $\mathbf{0}$ )
- $\{ \mathbf{F} \mid \mathcal{A} \vdash \mathbf{F}$       if a piece is absurd, so is the whole
- $\{ \mathbf{0} \vdash \neg(\neg\mathbf{0} \mid \neg\mathbf{0})$        $\mathbf{0}$  is single-threaded
- $\{ \mathcal{A} \mid \mathcal{B} \wedge \mathbf{0} \vdash \mathcal{A}$       you can split  $\mathbf{0}$  (but you get  $\mathbf{0}$ ). Proof uses (  $\mid \parallel$  )

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

$$(n[] \neg 0) \quad \{ \quad \} \quad n[A] \vdash \neg 0$$

$$(n[] \neg |) \quad \{ \quad \} \quad n[A] \vdash \neg(\neg 0 \mid \neg 0)$$

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

$$(n[] \wedge) \quad \{ \quad \} \quad n[A] \wedge n[C] \vdash n[A \wedge C]$$

$$(n[] \vee) \quad \{ \quad \} \quad n[C \vee B] \vdash n[C] \vee n[B]$$

$$(n[] @) \quad n[A] \vdash B \quad \{ \quad \} \quad A \vdash B @ n$$

$$(\neg @) \quad \{ \quad \} \quad A @ n \dashv\vdash \neg((\neg A) @ n)$$

locations exist

are not decomposable

$n[]$  congruence

$n[]$ - $\wedge$  distribution

$n[]$ - $\vee$  distribution

$n[]$ - $@$  adjunction

$@$  is self-dual

# Rules: Revelation

- ( $\mathbb{R}$ )  $\{ x\mathbb{R}x\mathbb{R}\mathcal{A} \dashv\vdash x\mathbb{R}\mathcal{A}$
- ( $\mathbb{R}$   $\mathbb{R}$ )  $\{ x\mathbb{R}y\mathbb{R}\mathcal{A} \vdash y\mathbb{R}x\mathbb{R}\mathcal{A}$
- ( $\mathbb{R}$   $\vee$ )  $\{ x\mathbb{R}(\mathcal{A} \vee \mathcal{B}) \vdash x\mathbb{R}\mathcal{A} \vee x\mathbb{R}\mathcal{B}$
- ( $\mathbb{R}$   $\vdash$ )  $\mathcal{A} \vdash \mathcal{B} \{ x\mathbb{R}\mathcal{A} \vdash x\mathbb{R}\mathcal{B}$
- 
- ( $\mathbb{R}$   $\odot$ )  $\eta\mathbb{R}\mathcal{A} \vdash \mathcal{B} \{ \} \mathcal{A} \vdash \mathcal{B} \odot \eta$
- ( $\odot$   $\neg$ )  $\{ (\neg\mathcal{A}) \odot x \dashv\vdash \neg(\mathcal{A} \odot x)$
- ( $\odot$   $\triangleright$  **F**)  $\{ \mathcal{A}^{\mathbf{F}} \odot x \dashv\vdash \mathcal{A}^{\mathbf{F}}$

$$(\mathbb{R} \mathbf{0}) \quad \{ \quad x \mathbb{R} \mathbf{0} \dashv\vdash \mathbf{0}$$

$$(\mathbb{O} \mathbf{0}) \quad \{ \quad \mathbf{0} \mathbb{O} x \vdash \mathbf{0}$$

$$(\mathbb{R} |) \quad \{ \quad x \mathbb{R} (\mathcal{A} | x \mathbb{R} \mathcal{B}) \dashv\vdash x \mathbb{R} \mathcal{A} | x \mathbb{R} \mathcal{B}$$

$$(\mathbb{O} |) \quad \{ \quad (\mathcal{A} | \mathcal{B}) \mathbb{O} x \vdash \mathcal{A} \mathbb{O} x | \mathcal{B} \mathbb{O} x$$

$$(\mathbb{R} \mathbb{O} |) \quad \{ \quad x \mathbb{R} ((\mathcal{A} | \mathcal{B}) \mathbb{O} x) \vdash x \mathbb{R} (\mathcal{A} \mathbb{O} x) | x \mathbb{R} (\mathcal{B} \mathbb{O} x)$$

$$(\mathbb{R} n[]) \quad \{ \quad x \mathbb{R} y[\mathcal{A}] \dashv\vdash y[x \mathbb{R} \mathcal{A}] \quad (x \neq y)$$

$$(\mathbb{O} n[]) \quad \{ \quad y[\mathcal{A}] \mathbb{O} x \vdash y[\mathcal{A} \mathbb{O} x] \quad (x \neq y)$$

$$(\mathbb{O} n[]) \quad \{ \quad x[\mathcal{A}] \mathbb{O} x \vdash \mathbf{F}$$

# Rules: Time and Space Modalities

- $(\diamond)$   $\{ \diamond A \vdash \neg \square \neg A \}$      $(\blacksquare)$   $\{ \blacksquare A \vdash \neg \# \neg A \}$   
 $(\square K)$   $\{ \square(A \Rightarrow B) \vdash \square A \Rightarrow \square B \}$      $(\# K)$   $\{ \#(A \Rightarrow B) \vdash \# A \Rightarrow \# B \}$   
 $(\square T)$   $\{ \square A \vdash A \}$      $(\# T)$   $\{ \# A \vdash A \}$   
 $(\square 4)$   $\{ \square A \vdash \square \square A \}$      $(\# 4)$   $\{ \# A \vdash \# \# A \}$   
 $(\square T)$   $\{ \mathbf{T} \vdash \square \mathbf{T} \}$      $(\# T)$   $\{ \mathbf{T} \vdash \# \mathbf{T} \}$   
 $(\square \vdash)$   $\{ A \vdash B \vdash \square A \vdash \square B \}$      $(\# \vdash)$   $\{ A \vdash B \vdash \# A \vdash \# B \}$   
 $(\diamond n[\ ])$   $\{ n[\diamond A] \vdash \diamond n[A] \}$      $(\blacksquare n[\ ])$   $\{ n[\blacksquare A] \vdash \blacksquare A \}$   
 $(\diamond |)$   $\{ \diamond A | \diamond B \vdash \diamond(A | B) \}$      $(\blacksquare |)$   $\{ \blacksquare A | \blacksquare B \vdash \blacksquare(A | \mathbf{T}) \}$   
 $(\blacksquare \diamond)$   $\{ \blacksquare \diamond A \vdash \diamond \blacksquare A \}$

S4, but not S5:  $\neg \text{vld } \diamond A \vdash \square \diamond A$      $\neg \text{vld } \blacksquare A \vdash \# \blacksquare A$

$(\blacksquare \diamond)$ : if somewhere sometime  $A$ , then sometime somewhere  $A$

## Some Derived Rules

Consequences:

$$A \vdash B \quad \} \quad A@n \vdash B@n$$

@ congruence

$$\} \quad n[A@n] \vdash A$$

$$\} \quad A \dashv\vdash n[A]@n$$

$$\} \quad n[\neg A] \vdash \neg n[A]$$

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



# 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  $\mathcal{A}$

$\#((n[\mathbf{T}] \Rightarrow n[\mathcal{A}])^\forall)$

every  $n$  everywhere satisfies  $\mathcal{A}$

# Ex: Immovable Object vs. Irresistible Force

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

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

$$\begin{aligned} Im \mid Ir &= (\mathbf{T} \triangleright \Box(obj[\mathbf{0}] \mid \mathbf{T})) \mid Ir \\ &\vdash \Box(obj[\mathbf{0}] \mid \mathbf{T}) \\ &\vdash \Diamond\Box(obj[\mathbf{0}] \mid \mathbf{T}) \end{aligned}$$

$$\begin{aligned} \mathcal{A} &\vdash \mathbf{T} \\ (\mathcal{A} \triangleright \mathcal{B}) &\mid \mathcal{A} \vdash \mathcal{B} \\ \mathcal{A} &\vdash \Diamond\mathcal{A} \end{aligned}$$

$$\begin{aligned} Im \mid Ir &= Im \mid (\mathbf{T} \triangleright \Box\Diamond\neg(obj[\mathbf{0}] \mid \mathbf{T})) \\ &\vdash \Box\Diamond\neg(obj[\mathbf{0}] \mid \mathbf{T}) \\ &\vdash \neg\Diamond\Box(obj[\mathbf{0}] \mid \mathbf{T}) \end{aligned}$$

$$\begin{aligned} \Diamond\neg\mathcal{A} &\vdash \neg\Box\mathcal{A} \\ \Box\neg\mathcal{A} &\vdash \neg\Diamond\mathcal{A} \end{aligned}$$

$$\text{Hence, } Im \mid Ir \vdash \mathbf{F}$$

$$\mathcal{A} \wedge \neg\mathcal{A} \vdash \mathbf{F}$$

## Ex: Thief!

A *shopper* is likely to pull out a wallet. A *thief* is likely to grab it.

$Shopper \triangleq$

$Person[Wallet[£] \mid \mathbf{T}] \wedge$

$\diamond(Person[NoWallet] \mid Wallet[£])$

$NoWallet \triangleq \neg(Wallet[£] \mid \mathbf{T})$

$Thief \triangleq Wallet[£] \triangleright \diamond NoWallet$

By simple logical deductions involving the laws of  $\triangleright$  and  $\diamond$ :

$Shopper \mid Thief \Rightarrow$

$(Person[Wallet[£] \mid \mathbf{T}] \mid Thief) \wedge$

$\diamond(Person[NoWallet] \mid NoWallet)$

# 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:

$$P \models \Box(" \text{ an } n \Rightarrow \Box " \text{ an } n)$$

## ■ Expressing Immobility

- If  $E, p:Amb^\bullet[S], q:Amb^\bullet[{}^Y S'] \vdash P : T$  (a typing judgment asserting that no ambient called  $q$  can ever move within  $P$ ), then:

$$P \models \Box(" (p \text{ parents } q) \Rightarrow \Box " (p \text{ parents } q))$$

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

# Model Checking

- If  $P$  is  $!$ -free and  $\mathcal{A}$  is  $\triangleright$ -free, then  $P \models \mathcal{A}$  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.)

## 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:

$$\# \triangleq \neg (n[\mathbf{T}] \mid \mathbf{T})$$

$$\text{unique } n \triangleq \mu \mathcal{X}. \# \mid (n[\#] \vee \exists y \neq n. y[\mathcal{X}])$$

# 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:

$$\begin{aligned} \mathbf{1}_{\text{MILL}} &\triangleq \mathbf{0} \\ \mathcal{A} \otimes_{\text{MILL}} \mathcal{B} &\triangleq \mathcal{A} | \mathcal{B} \\ \mathcal{A} \multimap_{\text{MILL}} \mathcal{B} &\triangleq \mathcal{A} \triangleright \mathcal{B} \end{aligned}$$

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

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

$$\begin{array}{ll}
 \mathbf{1}_{\text{ILL}} \triangleq \mathbf{0} & \mathcal{A} \oplus \mathcal{B} \triangleq \mathcal{A} \vee \mathcal{B} \\
 \perp_{\text{ILL}} \triangleq \mathbf{F} & \mathcal{A} \& \mathcal{B} \triangleq \mathcal{A} \wedge \mathcal{B} \\
 \top_{\text{ILL}} \triangleq \mathbf{T} & \mathcal{A} \otimes \mathcal{B} \triangleq \mathcal{A} | \mathcal{B} \\
 \mathbf{0}_{\text{ILL}} \triangleq \mathbf{F} & \mathcal{A} \multimap \mathcal{B} \triangleq \mathcal{A} \triangleright \mathcal{B} \\
 & !\mathcal{A} \triangleq \mathbf{0} \wedge (\mathbf{0} \Rightarrow \mathcal{A})^{-\mathbf{F}}
 \end{array}$$

- 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,  $\mathcal{A}_1, \dots, \mathcal{A}_n \vdash_{\text{ILL}} \mathcal{B}$  implies  $\mathcal{A}_1 | \dots | \mathcal{A}_n \vdash \mathcal{B}$ .
- Some discrepancies:  $\perp_{\text{ILL}} = \mathbf{0}_{\text{ILL}}$ ; the additives distribute;  $!\mathcal{A}$  is not "replication";  $!\mathcal{A} \multimap \mathcal{B}$  is not so interesting;  $\mathcal{A}^\perp / \mathcal{A}^0$  is unusually interesting.



## Connections 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  $A|B$  is defined just like *intensional conjunction*, and  $A\triangleright B$  is defined just like *relevant implication* in that semantics.
- Except:
  - We do not have contraction. This does not make sense in process calculi, because  $P | P \neq P$ . 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.)

## 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 adjoints 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.

# Process Domain

## Semantic domain: $\Phi$

	$\Pi$	$\triangleq$	the set of process expressions
$\forall C \subseteq \Pi.$	$C^{\equiv}$	$\triangleq$	$\{P \in \Pi \mid \exists P' \in C. P' \equiv P\}$
	$\Phi$	$\triangleq$	$\{C^{\equiv} \mid C \subseteq \Pi\}$

The domain  $\Phi$  is both a quantale  $(1, \otimes, \subseteq, \bigcup)$  and a boolean algebra  $(\emptyset, \Pi, \cup, \cap, \Pi)$ . It has additional structure induced by  $n[P]$  and  $(\forall n)P$ .

## Spatial operators over $\Phi$

	$1$	$\triangleq$	$\{\mathbf{0}\}^{\equiv}$
$\forall C, D \in \Phi.$	$C \otimes D$	$\triangleq$	$\{P \mid Q \mid P \in C \wedge Q \in D\}^{\equiv}$
$\forall n \in \Lambda, C \in \Phi.$	$n[C]$	$\triangleq$	$\{n[P] \mid P \in C\}^{\equiv}$
$\forall n \in \Lambda, C \in \Phi.$	$n \circledast C$	$\triangleq$	$\{(\forall n)P \mid P \in C\}^{\equiv}$

# Semantics of Revelation

$$n^{\textcircled{R}}C \triangleq \{(\nu n)P \mid P \in C\}^{\equiv}$$

- This means: take all processes of the form  $(\nu n)P$  (*not* up to renaming of  $n$ ), remove the ones such that  $P \notin C$ , and  $\equiv$ -close the result (thus adding, in particular, all the  $\alpha$ -variants).
- $n^{\textcircled{R}}C$  is read, informally:
  - *Reveal* a private name as  $n$  and check that the contents are in  $C$ .
  - Pull (by  $\equiv$ ) a  $(\nu n)$  binder at the top and check the rest is in  $C$ .
- Ex.:  $n^{\textcircled{R}}n[1]$ : reveal a private name (say,  $p$ ) as  $n$  and check the presence of an empty  $n$  ambient in the revealed process.

$$(\nu p)p[0] \in n^{\textcircled{R}}n[1]$$

$$\text{since } (\nu p)p[0] \equiv (\nu n)n[0] \text{ and } n[0] \in n[1]$$

- More examples of  $n^{\circledast}C \triangleq \{(\nu n)P \mid P \in C\}^{\equiv}$ :

$\mathbf{0} \in n^{\circledast}1$                       since  $\mathbf{0} \equiv (\nu n)\mathbf{0}$  and  $\mathbf{0} \in 1$

$m[\mathbf{0}] \in n^{\circledast}\Pi$                       since  $m[\mathbf{0}] \equiv (\nu n)m[\mathbf{0}]$  and  $m[\mathbf{0}] \in \Pi$

$n[\mathbf{0}] \notin n^{\circledast}\Pi$                       since:  $n[\mathbf{0}] \not\equiv (\nu n)\dots$

- Therefore,  $n^{\circledast}C$  is

- closed under  $\alpha$ -variants
- closed under  $\equiv$ -variants
- not closed under changes in the set of free names
- not closed under reduction (free names may disappear)
- not closed under any equivalence that includes reduction
- still ok for temporal reasoning:  $\neg n^{\circledast}\mathcal{A} \wedge \diamond n^{\circledast}\mathcal{A}$

# Semantics of the Logic

$\llbracket \mathbf{T} \rrbracket$	$\triangleq \Pi$
$\llbracket \neg \mathcal{A} \rrbracket$	$\triangleq \Pi - \llbracket \mathcal{A} \rrbracket$
$\llbracket \mathcal{A} \vee \mathcal{B} \rrbracket$	$\triangleq \llbracket \mathcal{A} \rrbracket \cup \llbracket \mathcal{B} \rrbracket$
$\llbracket \mathbf{0} \rrbracket$	$\triangleq 1$
$\llbracket \mathcal{A} \mid \mathcal{B} \rrbracket$	$\triangleq \llbracket \mathcal{A} \rrbracket \otimes \llbracket \mathcal{B} \rrbracket$
$\llbracket n[\mathcal{A}] \rrbracket$	$\triangleq n[\llbracket \mathcal{A} \rrbracket]$
$\llbracket n^{\circledast} \mathcal{A} \rrbracket$	$\triangleq n^{\circledast}[\llbracket \mathcal{A} \rrbracket]$
$\llbracket \mathcal{A} \triangleright \mathcal{B} \rrbracket$	$\triangleq \bigcup \{ C \in \Phi \mid C \otimes \llbracket \mathcal{A} \rrbracket \subseteq \llbracket \mathcal{B} \rrbracket \}$
$\llbracket \mathcal{A} @ n \rrbracket$	$\triangleq \bigcup \{ C \in \Phi \mid n[C] \subseteq \llbracket \mathcal{A} \rrbracket \}$
$\llbracket \blacksquare \mathcal{A} \rrbracket$	$\triangleq \{ P \in \Pi \mid \exists P' \in \Pi. P \downarrow^* P' \wedge P' \in \llbracket \mathcal{A} \rrbracket \}$
$\llbracket \blacklozenge \mathcal{A} \rrbracket$	$\triangleq \{ P \in \Pi \mid \exists P' \in \Pi. P \rightarrow^* P' \wedge P' \in \llbracket \mathcal{A} \rrbracket \}$
$\llbracket \forall x. \mathcal{A} \rrbracket$	$\triangleq \bigcap_{m \in \Lambda} \llbracket \mathcal{A} \{ x \leftarrow m \} \rrbracket$

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

$\downarrow^*$  is the refl-tran closure of  $\downarrow$

# Basic Fact

$$\forall \mathcal{A}. [[\mathcal{A}]] \in \Phi$$

Hence, formulas describe only congruence-invariant properties.

# Recovering the Satisfaction Relation

$$P \models \mathcal{A} \quad \triangleq \quad P \in \llbracket \mathcal{A} \rrbracket$$

- The properties of satisfaction for each logic constructs are then derivable.
- This approach to defining satisfaction is particularly good for introducing recursive formulas in the logic: it is easy to give them semantics as least and greatest fixpoints in the model, while it is not easy to define them directly via a satisfaction relation.



# Semantic Connections with Linear Logic

■ A (commutative) quantale  $Q$  is a structure

$\langle S : \text{Set}, \leq : S^2 \rightarrow \text{Bool}, \bigvee : \mathcal{P}(S) \rightarrow S, \otimes : S^2 \rightarrow S, 1 : S \rangle$  such that:

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

$\otimes, 1$  : a commutative monoid

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

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

$$\llbracket A \oplus B \rrbracket \triangleq \bigvee \{ \llbracket A \rrbracket, \llbracket B \rrbracket \}$$

$$\llbracket \mathbf{1}_{\text{ILL}} \rrbracket \triangleq 1$$

$$\llbracket A \& B \rrbracket \triangleq \bigvee \{ C \mid C \leq \llbracket A \rrbracket \wedge C \leq \llbracket B \rrbracket \}$$

$$\llbracket \perp_{\text{ILL}} \rrbracket \triangleq \text{any element of } S$$

$$\llbracket A \otimes B \rrbracket \triangleq \llbracket A \rrbracket \otimes \llbracket B \rrbracket$$

$$\llbracket \top_{\text{ILL}} \rrbracket \triangleq \bigvee S$$

$$\llbracket A \multimap B \rrbracket \triangleq \bigvee \{ C \mid C \otimes \llbracket A \rrbracket \leq \llbracket B \rrbracket \}$$

$$\llbracket \mathbf{0}_{\text{ILL}} \rrbracket \triangleq \bigvee \emptyset$$

$$\llbracket !A \rrbracket \triangleq \bigvee X. \llbracket \mathbf{1} \& A \& X \otimes X \rrbracket \text{ where } \bigvee X. A\{X\} \triangleq \bigvee \{ C \mid C \leq A\{C\} \}$$

$$\mathbf{vld}_{\text{ILL}}(A_1, \dots, A_n \vdash_{\text{ILL}} B)_Q \triangleq \llbracket A_1 \rrbracket_Q \otimes_Q \dots \otimes_Q \llbracket A_n \rrbracket_Q \leq_Q \llbracket B \rrbracket_Q$$

# The Process Quantale

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

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

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

$$1_\Phi \triangleq \{\mathbf{0}\}^\equiv$$

$$A \otimes_\Phi B \triangleq \{P \mid Q \mid P \in A \wedge Q \in B\}^\equiv$$

- ILL validity in  $\Phi$ :

$$\mathbf{vld}_{\text{ILL}}(\mathcal{A}_1, \dots, \mathcal{A}_n \vdash_{\text{ILL}} \mathcal{B})_\Phi$$

$$\Leftrightarrow [[\mathcal{A}_1]] \otimes_\Phi \dots \otimes_\Phi [[\mathcal{A}_n]] \subseteq [[\mathcal{B}]]$$

$$\Leftrightarrow [[\mathcal{A}_1 \mid \dots \mid \mathcal{A}_n]] \subseteq [[\mathcal{B}]]$$

$$\Leftrightarrow (\Pi - [[\mathcal{A}_1 \mid \dots \mid \mathcal{A}_n]]) \cup [[\mathcal{B}]] = \Pi$$

$$\Leftrightarrow [[\mathcal{A}_1 \mid \dots \mid \mathcal{A}_n \Rightarrow \mathcal{B}]] = \Pi$$

## 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.