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 properies of ordinary concurrent computations, options include equational reasoning (hard), reasoning on traces (ugly), and reasoning via modal (e.g. temporal) logics.

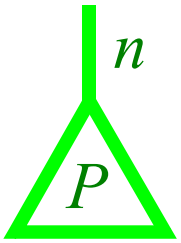
Spatial Logics

- 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		*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)

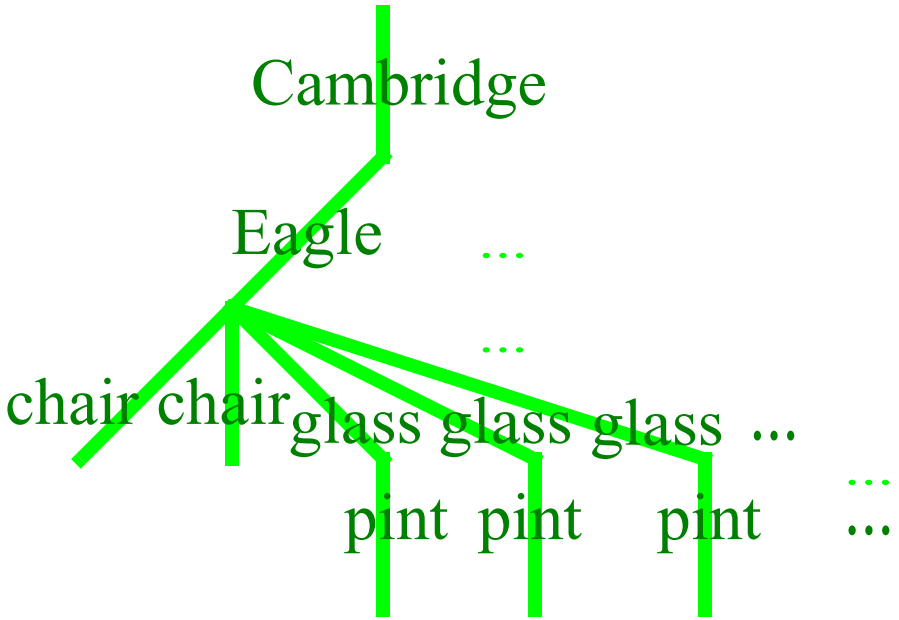


(location)

(composition)

Spatial Structures

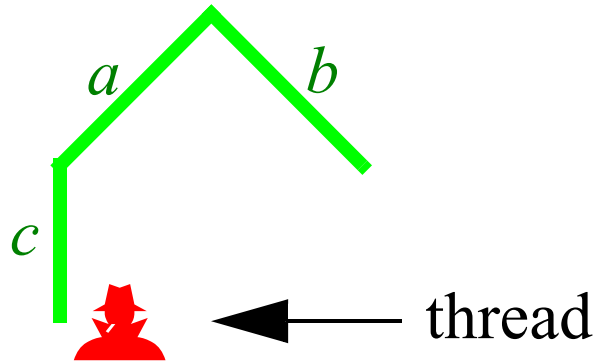
- Our basic model of space is going to be *finite-depth edge-labeled unordered trees*; for short: *spatial trees*, represented by a syntax of *spatial expressions*. Unbounded resources are represented by infinite branching:



Cambridge[Eagle[chair[**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.

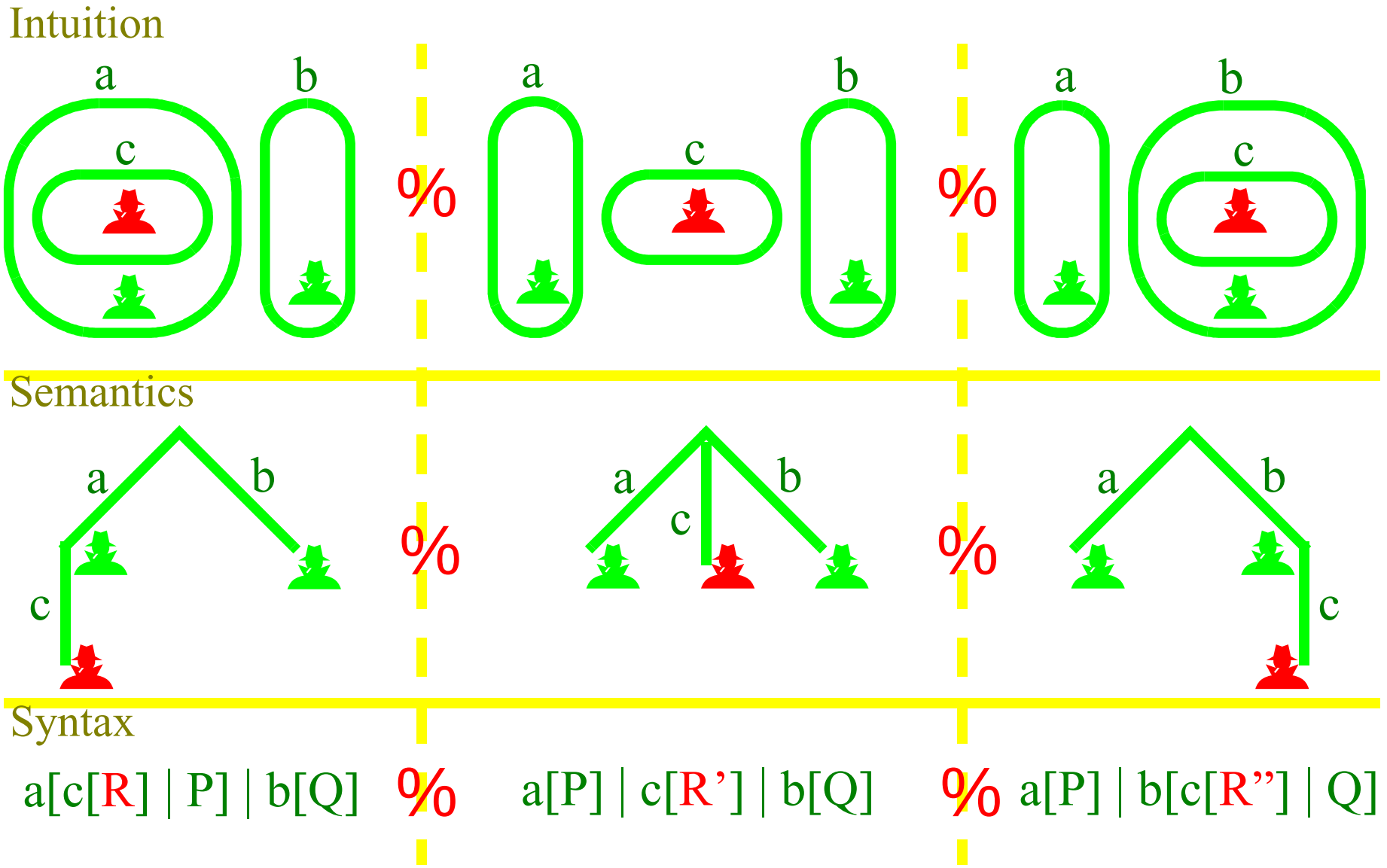


- An ambient tree is a spatial tree with, possibly, threads at each node that can locally change the shape of the tree.

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

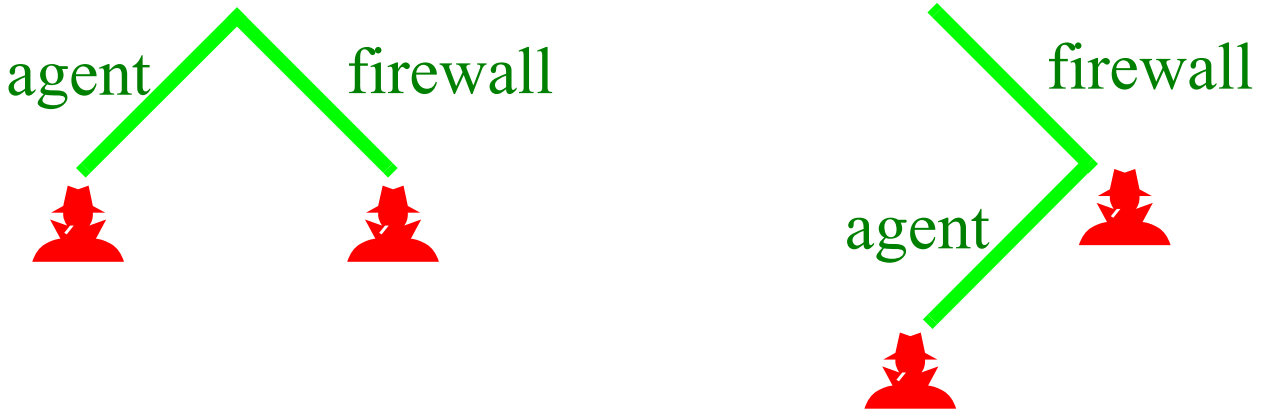
Mobility

Mobility is change of spatial structures over time.



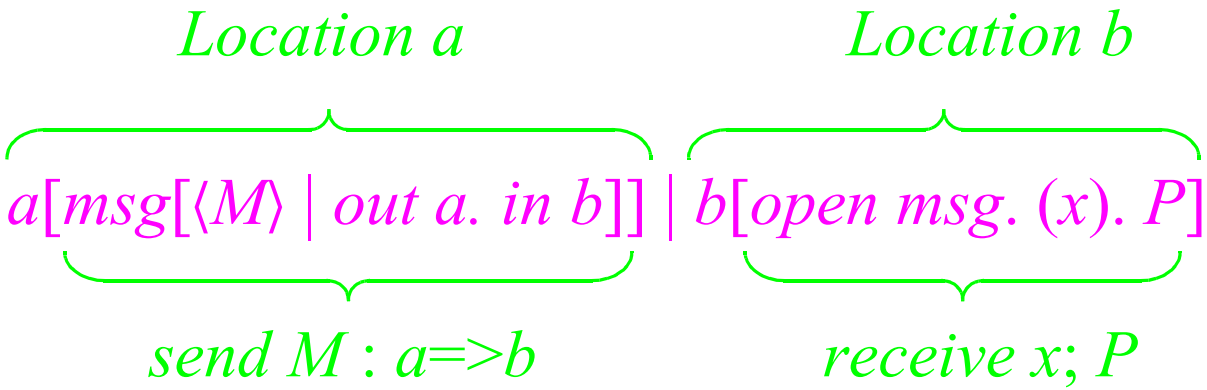
Properties of Mobile Computation

- 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.



Now Later

Ambient Calculus: Example



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

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

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

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

$M \triangleq M.\mathbf{0}$ (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 thread are "trivially equivalent".
  - Prominent in the definition of the logic.
- A *reduction* relation $P \longrightarrow^{*} Q$:
  - Defining the mobility and communication actions.
  - Up to structural congruence:

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

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)

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

$(n).P \mid \langle M \rangle \longrightarrow P\{n \leftarrow M\}$ (Red Comm)

$P \longrightarrow Q \ \Rightarrow\ (\nu n)P \longrightarrow (\nu n)Q$ (Red Res)

$P \longrightarrow Q \ \Rightarrow\ n[P] \longrightarrow n[Q]$ (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 $\equiv$)

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

Structural Congruence

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

$$P \equiv P \qquad \text{(Struct Refl)}$$

$$P \equiv Q \;\Rightarrow\; Q \equiv P \qquad \text{(Struct Symm)}$$

$$P \equiv Q,\ Q \equiv R \;\Rightarrow\; P \equiv R \qquad \text{(Struct Trans)}$$

$$P \equiv Q \;\Rightarrow\; (\nu n)P \equiv (\nu n)Q \qquad \text{(Struct Res)}$$

$$P \equiv Q \;\Rightarrow\; P \mid R \equiv Q \mid R \qquad \text{(Struct Par)}$$

$$P \equiv Q \;\Rightarrow\; !P \equiv !Q \qquad \text{(Struct Repl)}$$

$$P \equiv Q \;\Rightarrow\; M[P] \equiv M[Q] \qquad \text{(Struct Amb)}$$

$$P \equiv Q \;\Rightarrow\; M.P \equiv M.Q \qquad \text{(Struct Action)}$$

$$P \equiv Q \;\Rightarrow\; (x).P \equiv (x).Q \qquad \text{(Struct Input)}$$

$$\varepsilon.P \equiv P \qquad \text{(Struct } \varepsilon\text{)}$$

$$(M.M').P \equiv M.M'.P \qquad \text{(Struct .)}$$

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

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

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

$(\nu n)(m[P]) \equiv m[(\nu n)P] \quad \text{if } n \neq m$ (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 $n[\mathbf{0}]$ 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

$\mathcal{A}, \mathcal{B} : \Phi ::=$ (η is a name n or a variable x)

$\mathbf{T}$	true
$\neg\mathcal{A}$	negation
$\mathcal{A} \vee \mathcal{B}$	disjunction
$\mathbf{0}$	void
$\mathcal{A} \mid \mathcal{B}$	composition
$\mathcal{A} \triangleright \mathcal{B}$	composition adjunct
$\eta[\mathcal{A}]$	location
$\mathcal{A}@\eta$	location adjunct
$\eta \circledR \mathcal{A}$	revelation
$\mathcal{A} \oslash \eta$	revelation adjunct
$"\mathcal{A}$	somewhere modality
$\Diamond\mathcal{A}$	sometime modality
$\forall x.\mathcal{A}$	universal quantification over names

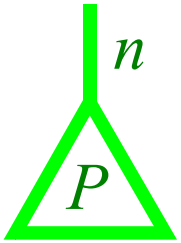
Satisfaction Relation

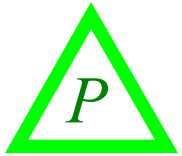
$$
\begin{array}{lcl}
P \models \mathbf{T} & & \\
P \models \neg\mathcal{A} & \triangleq & \neg\, P \models \mathcal{A} \\
P \models \mathcal{A}\vee\mathcal{B} & \triangleq & P \models \mathcal{A} \vee P \models \mathcal{B} \\
P \models \mathbf{0} & \triangleq & P \equiv \mathbf{0} \\
P \models \mathcal{A}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

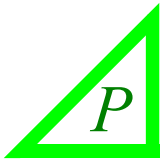
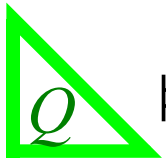
$P \downarrow P'$ iff $\exists n, P''.\ P \equiv n[P'] \mid P''$. $\downarrow^{*}$ is the refl-trans closure of $\downarrow$

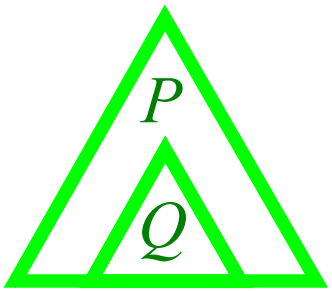
Satisfaction Relation for Trees

- $\models \mathbf{0}$

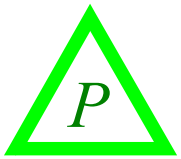


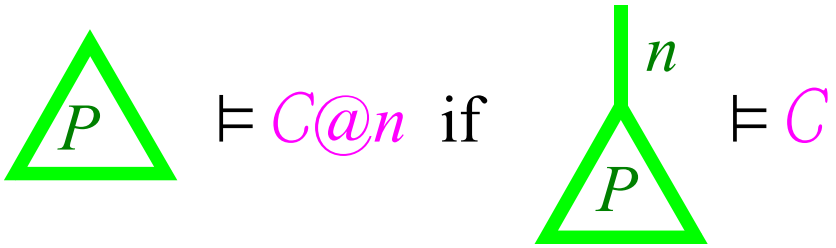
$\models n[\mathcal{A}]$ if  $\models \mathcal{A}$

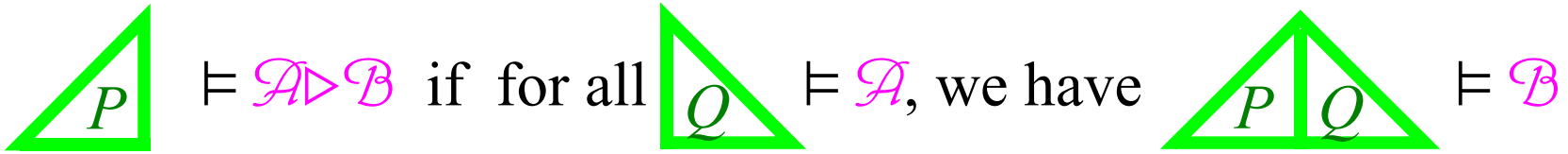
$\models \mathcal{A} \mid \mathcal{B}$ if  $\models \mathcal{A}$ and  $\models \mathcal{B}$



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

$\models \Diamond\mathcal{A}$ if  % *  and  $\models \mathcal{A}$





Basic Fact: Satisfaction is invariant under structural congruence:

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

I.e.: $\{P{:}\Pi \parallel P \models \mathcal{A}\}$ 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) " (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) " (4)

somewhere there is a p with a child q

Revelation

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

- $n\circledR\mathcal{A}$ is read, informally:
  - *Reveal* a private name as n and check that the revealed process satisfies $\mathcal{A}$.
  - Pull (by $\equiv$) a (νn) binder at the top and check that the stripped process satisfies $\mathcal{A}$.
- Ex.: $n\circledR n[\mathbf{0}]$: reveal a private name (say, p) as n and check the presence of an empty n ambient in the revealed process.

$$(\nu p)p[\mathbf{0}] \models n\circledR n[\mathbf{0}]$$

since $(\nu p)p[\mathbf{0}] \equiv (\nu n)n[\mathbf{0}]$ and $n[\mathbf{0}] \models n[\mathbf{0}]$

- More examples of revelation:

$\mathbf{0} \models n\circledR\mathbf{0}$	since $\mathbf{0} \equiv (\nu n)\mathbf{0}$ and $\mathbf{0} \models \mathbf{0}$
$m[\mathbf{0}] \models n\circledR\mathbf{T}$	since $m[\mathbf{0}] \equiv (\nu n)m[\mathbf{0}]$ and $m[\mathbf{0}] \models \mathbf{T}$
$n[\mathbf{0}] \not\models n\circledR\mathbf{T}$	since: $n[\mathbf{0}] \not\equiv (\nu n)...$

- Therefore, the set of processes satisfying $n\circledR\mathcal{A}$ is
  - closed under α-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: $\neg n\circledR\mathcal{A} \wedge \Diamond n\circledR\mathcal{A}$

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 $\exists m{:}\Lambda.\ P \models \mathcal{A}\{x \leftarrow m\}$
$\#\mathcal{A}$	$\triangleq \neg$ " $\neg\mathcal{A}$	$P \models \text{-}$ 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 $\exists P'{:}\Pi.\ P' \models \mathcal{A}$

Revelation Derived Formulas

$\copyright n$	$\triangleq \neg n\circledR\mathbf{T}$	$P \models \text{-}$ iff $\neg\exists P' \in \Pi.\ P \equiv (\nu n)P'$ iff $n \in fn(P)$
closed	$\triangleq \neg\exists x.\copyright x$	$P \models \text{-}$ iff $\neg\exists n{:}\Lambda.\ n \in fn(P)$
separate	$\triangleq \neg\exists x.\copyright x \mid \copyright x$	$P \models \text{-}$ 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 :

$n[] \models \copyright n$

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

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

Name Equality

Name equality can be defined within the logic:

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

Since (for any substitution applied to 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":

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

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 $n\circledR\mathcal{A}$ 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

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

Sequents

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

Rules

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

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

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

Conventions:

- $\dashv\vdash$ means $\vdash$ in both directions
- $\{\ \}$ means $\}$ in both directions

Logical Adjunctions

- This is a logic with multiple logical adjunctions (4 of them!):
  - $\wedge$ / $\Rightarrow$ (classical)

    $\mathcal{A} \wedge C \vdash \mathcal{B}$ iff $\mathcal{A} \vdash C \Rightarrow \mathcal{B}$
  - $|$ / $\triangleright$ (linear, $\otimes$ / $\multimap$)

    $\mathcal{A} \mid C \vdash \mathcal{B}$ iff $\mathcal{A} \vdash C \triangleright \mathcal{B}$
  - $n[\text{-}]$ / $\text{-}@n$ (location)

    $n[\mathcal{A}] \vdash \mathcal{B}$ iff $\mathcal{A} \vdash \mathcal{B}@n$
  - $n\circledR\text{-}$ / $\text{-}\oslash n$ (restriction)

    $n\circledR\mathcal{A} \vdash \mathcal{B}$ iff $\mathcal{A} \vdash \mathcal{B}\oslash n$
- 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) $\mathcal{A}\wedge(\mathcal{C}\wedge\mathcal{D})\vdash\mathcal{B} \;\{\}\; (\mathcal{A}\wedge\mathcal{C})\wedge\mathcal{D}\vdash\mathcal{B}$

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

Rules: Composition

$(\,|\,\mathbf{0})$ $\quad \} \ \mathcal{A} \,|\, \mathbf{0} \dashv\vdash \mathcal{A}$ — **0** is nothing

$(\,|\,\neg\mathbf{0})$ $\quad \} \ \mathcal{A} \,|\, \neg\mathbf{0} \vdash \neg\mathbf{0}$ — if a part is non-**0**, so is the whole

$(\mathrm{A}\,|\,)$ $\quad \} \ \mathcal{A} \,|\, (\mathcal{B} \,|\, \mathcal{C}) \dashv\vdash (\mathcal{A} \,|\, \mathcal{B}) \,|\, \mathcal{C}$ — | associativity

$(\mathbf{X}\,|\,)$ $\quad \} \ \mathcal{A} \,|\, \mathcal{B} \vdash \mathcal{B} \,|\, \mathcal{A}$ — | commutativity

$(\,|\,\vdash)$ $\quad \mathcal{A}' \vdash \mathcal{B}';\ \mathcal{A}'' \vdash \mathcal{B}'' \ \} \ \mathcal{A}' \,|\, \mathcal{A}'' \vdash \mathcal{B}' \,|\, \mathcal{B}''$ — | congruence

$(\,|\,\vee)$ $\quad \} \ (\mathcal{A} \vee \mathcal{B}) \,|\, \mathcal{C} \vdash \mathcal{A} \,|\, \mathcal{C} \vee \mathcal{B} \,|\, \mathcal{C}$ — |-∨ distribution

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

$(\,|\,\triangleright)$ $\quad \mathcal{A} \,|\, \mathcal{C} \vdash \mathcal{B} \ \{\,\} \ \mathcal{A} \vdash \mathcal{C} \triangleright \mathcal{B}$ — |-▷ adjunction

$(\triangleright\mathbf{F}\,\neg)$ $\quad \} \ \mathcal{A}^{\mathbf{F}} \vdash \mathcal{A}^{\neg}$ — 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

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 $|$:

$\mathcal{A} \,||\, \mathcal{B} \;\triangleq\; \neg(\neg\mathcal{A} \,|\, \neg\mathcal{B})$ $\quad P \vDash$ - 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:

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

"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 $\mathcal{B}$."

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

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

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

"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: $\mathcal{A} \triangleright \mathcal{B} \vdash \mathcal{A} \triangleright \mathcal{B} \vdash (\mathcal{A} \triangleright \mathcal{B}) \mid \mathcal{A} \vdash \mathcal{B}$ by (Id), ($\mid \triangleright$)

$\mathcal{D} \vdash \mathcal{A};\ \mathcal{B} \vdash C \vdash \mathcal{D} \mid (\mathcal{A} \triangleright \mathcal{B}) \vdash C$ (*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:

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

More Derived Rules

$\vdash \mathcal{A} \vdash \mathbf{T} \mid \mathcal{A}$ — you can always add more pieces (if they are **0**)

$\vdash \mathbf{F} \mid \mathcal{A} \vdash \mathbf{F}$ — if a piece is absurd, so is the whole

$\vdash \mathbf{0} \vdash \neg(\neg\mathbf{0} \mid \neg\mathbf{0})$ — **0** is single-threaded

$\vdash \mathcal{A} \mid \mathcal{B} \wedge \mathbf{0} \vdash \mathcal{A}$ — you can split **0** (but you get **0**). Proof uses ($\mid \parallel$)

$\mathcal{A}' \vdash \mathcal{A};\ \mathcal{B} \vdash \mathcal{B}' \vdash \mathcal{A} \triangleright \mathcal{B} \vdash \mathcal{A}' \triangleright \mathcal{B}'$ — $\triangleright$ is contravariant on the left

$\vdash \mathcal{A} \triangleright \mathcal{B} \mid \mathcal{B} \triangleright \mathcal{C} \vdash \mathcal{A} \triangleright \mathcal{C}$ — $\triangleright$ is transitive

$\vdash (\mathcal{A} \mid \mathcal{B}) \triangleright \mathcal{C} \dashv\vdash \mathcal{A} \triangleright (\mathcal{B} \triangleright \mathcal{C})$ — $\triangleright$ curry/uncurry

$\vdash \mathcal{A} \triangleright (\mathcal{B} \triangleright \mathcal{C}) \vdash \mathcal{B} \triangleright (\mathcal{A} \triangleright \mathcal{C})$ — contexts commute

$\vdash \mathbf{T} \dashv\vdash \mathbf{T} \triangleright \mathbf{T}$ — truth can withstand any attack

$\vdash \mathbf{T} \vdash \mathbf{F} \triangleright \mathcal{A}$ — anything goes if you can find an absurd partner

$\vdash \mathbf{T} \triangleright \mathcal{A} \vdash \mathcal{A}$ — if $\mathcal{A}$ resists any attack, then it holds

Rules: Location

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

Rules: Revelation

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

$(\mathbb{R}\ \mathbb{R})$ $\quad \} \; x\mathbb{R}y\mathbb{R}\mathcal{A} \vdash y\mathbb{R}x\mathbb{R}\mathcal{A}$

$(\mathbb{R} \vee)$ $\quad \} \; x\mathbb{R}(\mathcal{A} \vee \mathcal{B}) \vdash x\mathbb{R}\mathcal{A} \vee x\mathbb{R}\mathcal{A}$

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

$(\mathbb{R}\ \oslash)$ $\quad \eta\mathbb{R}\mathcal{A} \vdash \mathcal{B} \; \{ \} \; \mathcal{A} \vdash \mathcal{B} \oslash \eta$

$(\oslash\ \neg)$ $\quad \} \; (\neg\mathcal{A}) \oslash x \dashv\vdash \neg(\mathcal{A} \oslash x)$

$(\oslash \triangleright \mathbf{F})$ $\quad \} \; \mathcal{A}^{\mathbf{F}} \oslash x \dashv\vdash \mathcal{A}^{\mathbf{F}}$

$(\circledR\ \mathbf{0})$ $(\oslash\ \mathbf{0})$ $\}$ $x \circledR \mathbf{0} \dashv\vdash \mathbf{0}$

$\mathbf{0} \oslash x \vdash \mathbf{0}$

$(\circledR \mid)$ $\}$ $x \circledR (\mathcal{A} \mid x \circledR \mathcal{B}) \dashv\vdash x \circledR \mathcal{A} \mid x \circledR \mathcal{B}$

$(\oslash \mid)$ $\}$ $(\mathcal{A} \mid \mathcal{B}) \oslash x \vdash \mathcal{A} \oslash x \mid \mathcal{B} \oslash x$

$(\circledR \oslash \mid)$ $\}$ $x \circledR ((\mathcal{A} \mid \mathcal{B}) \oslash x) \vdash x \circledR (\mathcal{A} \oslash x) \mid x \circledR (\mathcal{B} \oslash x)$

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

$(\oslash\ n[])$ $\}$ $y[\mathcal{A}] \oslash x \vdash y[\mathcal{A} \oslash x]$ $(x \neq y)$

$(\oslash\ n[])$ $\}$ $x[\mathcal{A}] \oslash x \vdash \mathbf{F}$

Rules: Time and Space Modalities

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

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

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

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

$(\Box\ \mathbf{T})$ $\quad \vdash \mathbf{T} \vdash \Box\mathbf{T}$ $\quad$ $(\#\ \mathbf{T})$ $\quad \vdash \mathbf{T} \vdash \#\mathbf{T}$

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

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

$(\Diamond\,|\,)$ $\quad \vdash \Diamond\mathcal{A}\,|\,\Diamond\mathcal{B} \vdash \Diamond(\mathcal{A}\,|\,\mathcal{B})$ $\quad$ $(\text{"}\ |\,)$ $\quad \vdash \text{"}\mathcal{A}\,|\,\mathcal{B} \vdash \text{"}(\mathcal{A}\,|\,\mathbf{T})$

$(\text{"}\Diamond)$ $\quad \vdash \text{"}\Diamond\mathcal{A} \vdash \Diamond\text{"}\mathcal{A}$

S4, but not S5: $\quad \neg\ \textbf{\textit{vld}}\ \Diamond\mathcal{A} \vdash \Box\Diamond\mathcal{A}$ $\quad$ $\neg\ \textbf{\textit{vld}}\ \text{"}\mathcal{A} \vdash \#\ \text{"}\mathcal{A}$

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

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

Ex: Immovable Object vs. Irresistible Force

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

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

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

$$\mathcal{A} \vdash \mathbf{T}$$

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

$$\mathcal{A} \vdash \Diamond\mathcal{A}$$

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

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

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

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

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

Ex: Thief!

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

$$\begin{aligned} &\mathit{Shopper} \triangleq \\ &\quad \mathrm{Person}[\mathrm{Wallet}[£] \mid \mathbf{T}] \wedge \\ &\quad \Diamond(\mathrm{Person}[\mathit{NoWallet}] \mid \mathrm{Wallet}[£]) \end{aligned}$$

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

$$\mathit{Thief} \triangleq \mathrm{Wallet}[£] \triangleright \Diamond \mathit{NoWallet}$$

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

$$\begin{aligned} &\mathit{Shopper} \mid \mathit{Thief} \Rightarrow \\ &\quad (\mathrm{Person}[\mathrm{Wallet}[£] \mid \mathbf{T}] \mid \mathit{Thief}) \wedge \\ &\quad \Diamond(\mathrm{Person}[\mathit{NoWallet}] \mid \mathit{NoWallet}) \end{aligned}$$

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

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

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

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:

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

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

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

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

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

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

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:

$$\mathbf{1}_{\mathrm{MILL}} \triangleq \mathbf{0}$$
$$\mathcal{A} \otimes_{\mathrm{MILL}} \mathcal{B} \triangleq \mathcal{A} \mid \mathcal{B}$$
$$\mathcal{A} \multimap_{\mathrm{MILL}} \mathcal{B} \triangleq \mathcal{A} \rhd \mathcal{B}$$

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

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

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

- 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 $\mathcal{A}_1 \mid \ldots \mid \mathcal{A}_n \vdash \mathcal{B}$.
- Some discrepancies: $\bot_{\mathrm{ILL}} = \mathbf{0}_{\mathrm{ILL}}$; 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.

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

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.

Process Domain

Semantic domain: Φ

$$
\begin{array}{lll}
 & \Pi & \triangleq \text{ the set of process expressions} \\
\forall C \subseteq \Pi. & C^{\equiv} & \triangleq \{P \in \Pi \parallel \exists P' \in C.\ P' \equiv P\} \\
 & \Phi & \triangleq \{C^{\equiv} \parallel C \subseteq \Pi\}
\end{array}
$$

The domain Φ is both a quantale (1, $\otimes$, $\subseteq$, $\bigcup$) and a boolean algebra ($\emptyset$, Π, $\cup$, $\cap$, Π^{-}). It has additional structure induced by $n[P]$ and $(\nu n)P$.

Spatial operators over Φ

$$
\begin{array}{lll}
 & 1 & \triangleq \{\mathbf{0}\}^{\equiv} \\
\forall C,D \in \Phi. & C \otimes D & \triangleq \{P|Q \parallel P \in C \wedge Q \in D\}^{\equiv} \\
\forall n \in \Lambda,\ C \in \Phi. & n[C] & \triangleq \{n[P] \parallel P \in C\}^{\equiv} \\
\forall n \in \Lambda,\ C \in \Phi. & n \circledR C & \triangleq \{(\nu n)P \parallel P \in C\}^{\equiv}
\end{array}
$$

Semantics of Revelation

$$n®C \triangleq \{(\nu n)P \parallel P \in C\}^{\equiv}$$

- 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 α-variants).
- $n®C$ is read, informally:
  - *Reveal* a private name as n and check that the contents are in C.
  - Pull (by $\equiv$) a (νn) binder at the top and check the rest is in C.
- Ex.: $n®n[1]$: reveal a private name (say, p) as n and check the presence of an empty n ambient in the revealed process.

$$(\nu p)p[\mathbf{0}] \in n®n[1]$$

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

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

$\mathbf{0} \in n®1$	since $\mathbf{0} \equiv (\nu n)\mathbf{0}$ and $\mathbf{0} \in 1$
$m[\mathbf{0}] \in n®\Pi$	since $m[\mathbf{0}] \equiv (\nu n)m[\mathbf{0}]$ and $m[\mathbf{0}] \in \Pi$
$n[\mathbf{0}] \notin n®\Pi$	since: $n[\mathbf{0}] \not\equiv (\nu n)...$

- Therefore, $n®C$ is
  - closed under α-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: $\neg n®\mathcal{A} \wedge \Diamond n®\mathcal{A}$

Semantics of the Logic

$$
\begin{array}{lcl}
[\![\mathbf{T}]\!] & \triangleq & \Pi \\
[\![\neg\mathcal{A}]\!] & \triangleq & \Pi - [\![\mathcal{A}]\!] \\
[\![\mathcal{A}\vee\mathcal{B}]\!] & \triangleq & [\![\mathcal{A}]\!] \cup [\![\mathcal{B}]\!] \\
[\![\mathbf{0}]\!] & \triangleq & 1 \\
[\![\mathcal{A} \mid \mathcal{B}]\!] & \triangleq & [\![\mathcal{A}]\!] \otimes [\![\mathcal{B}]\!] \\
[\![n[\mathcal{A}]]\!] & \triangleq & n[[\![\mathcal{A}]\!]] \\
[\![n\circledR\mathcal{A}]\!] & \triangleq & n\circledR[\![\mathcal{A}]\!] \\
[\![\mathcal{A}\triangleright\mathcal{B}]\!] & \triangleq & \bigcup\{C\in\Phi \parallel C \otimes [\![\mathcal{A}]\!] \subseteq [\![\mathcal{B}]\!]\} \\
[\![\mathcal{A}@n]\!] & \triangleq & \bigcup\{C\in\Phi \parallel n[C] \subseteq [\![\mathcal{A}]\!]\} \\
[\![\ "\ \mathcal{A}]\!] & \triangleq & \{P\in\Pi \parallel \exists P'\in\Pi.\ P{\downarrow}^{*}P' \wedge P'\in[\![\mathcal{A}]\!]\} \\
[\![\Diamond\mathcal{A}]\!] & \triangleq & \{P\in\Pi \parallel \exists P'\in\Pi.\ P{\rightarrow}^{*}P' \wedge P'\in[\![\mathcal{A}]\!]\} \\
[\![\forall x.\mathcal{A}]\!] & \triangleq & \bigcap_{m\in\Lambda} [\![\mathcal{A}\{x\leftarrow m\}]\!]
\end{array}
$$

$P{\downarrow}P' \triangleq \exists n, P''.\ P \equiv n[P'] \mid P''$ $\qquad$ ${\downarrow}^{*}$ 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

$$P \models \mathcal{A} \quad \triangleq \quad P \in [\![\mathcal{A}]\!]$$

- The properies 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 greates 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 $\mathcal{Q}$ is a structure
  $<S : \mathrm{Set}, \leq : S^2 \to \mathrm{Bool}, \bigvee : \mathcal{P}(S) \to S, \otimes : S^2 \to S, 1 : S>$ 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):

$$[\![\mathcal{A} \oplus \mathcal{B}]\!] \triangleq \bigvee \{[\![\mathcal{A}]\!], [\![\mathcal{B}]\!]\} \qquad [\![\mathbf{1}_{\mathrm{ILL}}]\!] \triangleq 1$$

$$[\![\mathcal{A} \,\&\, \mathcal{B}]\!] \triangleq \bigvee \{C \parallel C \leq [\![\mathcal{A}]\!] \wedge C \leq [\![\mathcal{B}]\!]\} \qquad [\![\bot_{\mathrm{ILL}}]\!] \triangleq \text{any element of } S$$

$$[\![\mathcal{A} \otimes \mathcal{B}]\!] \triangleq [\![\mathcal{A}]\!] \otimes [\![\mathcal{B}]\!] \qquad [\![\top_{\mathrm{ILL}}]\!] \triangleq \bigvee S$$

$$[\![\mathcal{A} \multimap \mathcal{B}]\!] \triangleq \bigvee \{C \parallel C \otimes [\![\mathcal{A}]\!] \leq [\![\mathcal{B}]\!]\} \qquad [\![\mathbf{0}_{\mathrm{ILL}}]\!] \triangleq \bigvee \emptyset$$

$$[\![!\mathcal{A}]\!] \triangleq \upsilon X.\, [\![\mathbf{1} \,\&\, \mathcal{A} \,\&\, X \otimes X]\!] \text{ where } \upsilon X.\, A\{X\} \triangleq \bigvee \{C \parallel C \leq A\{C\}\}$$

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

The Process Quantale

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

  $\Phi \triangleq \langle \Phi, \subseteq, \bigcup, \otimes, \mathbf{1} \rangle$ 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 Φ:

  $$\mathbf{vld}_{\mathrm{ILL}}(\mathcal{A}_1, \ldots, \mathcal{A}_n \vdash_{\mathrm{ILL}} \mathcal{B})_\Phi$$
  $$\Leftrightarrow \quad [\![\mathcal{A}_1]\!] \otimes_\Phi \ldots \otimes_\Phi [\![\mathcal{A}_n]\!] \subseteq [\![\mathcal{B}]\!]$$
  $$\Leftrightarrow \quad [\![\mathcal{A}_1 \mid \ldots \mid \mathcal{A}_n]\!] \subseteq [\![\mathcal{B}]\!]$$
  $$\Leftrightarrow \quad (\Pi - [\![\mathcal{A}_1 \mid \ldots \mid \mathcal{A}_n]\!]) \cup [\![\mathcal{B}]\!] = \Pi$$
  $$\Leftrightarrow \quad [\![\mathcal{A}_1 \mid \ldots \mid \mathcal{A}_n \Rightarrow \mathcal{B}]\!] = \Pi$$

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.