Spatial Logics for Distributed Systems

Luca Cardelli

Microsoft Research

FWAN, 2002-07-12

Joint work with Luís Caires.
Also reflecting work with Andrew D. Gordon and Cristiano Calcagno.

Widely Distributed Systems

Concurrent systems that are *spatially* distributed:

- Not in the same box.
- Not on the same LAN.
- Not inside the same firewall.
- Not always in the same place.

They have well-defined subsystems that:

- Fail independently.
- Recover independently.
- Hold secrets, mistrust each other.
- Move around.

Spatial distribution is (in practice) an observable.

The New Machine

The "machine" we now write programs for, is the whole Internet.

- New instruction sets (programming models):
  - Message-centric, asynchronous, often stateless.
    Cannot rely on distributed consensus.
  - In striking contrast to shared-memory concurrency, and handshake-based (synchronous) concurrency.
- New type systems:
  - Traditional "strong" type systems have been (finally!) enthusiastically adopted as a foundation for security.
  - But entirely new type systems are needed for regulating communication, and to manage application-level security.
- New program logics:
  - Privacy/security concerns override everything else.
  - Need "location awareness" and "resource awareness".

Talking About *Where*

Informal statements:

- Distribution: *Where* are things happening?
- Security: *Where* are things kept, and who can get there?
- Privacy: *Where* are things known, and where are they leaked?

We need a new way of reasoning (i.e. a new logic):

- Classical logic: *Whether* something is true.
- Intuitionistic logic: *How* something is true.
- Temporal logic: *When* something is true.
- *Spatial* logic: *Where* something is true.

Why logic?

- Essentially as a foundation for future type/analysis systems.
- The technical sequent calculus presentation is actually very similar to type systems judgments.

Approach

We have looked, concretely, at specific logics for specific models:

- For trees, for graphs, for mobility, for communication + privacy.

With some common, new-ish, techniques:

- Semantically: Modal logics for structured worlds.
- Syntactically: Many-world sequent calculi.

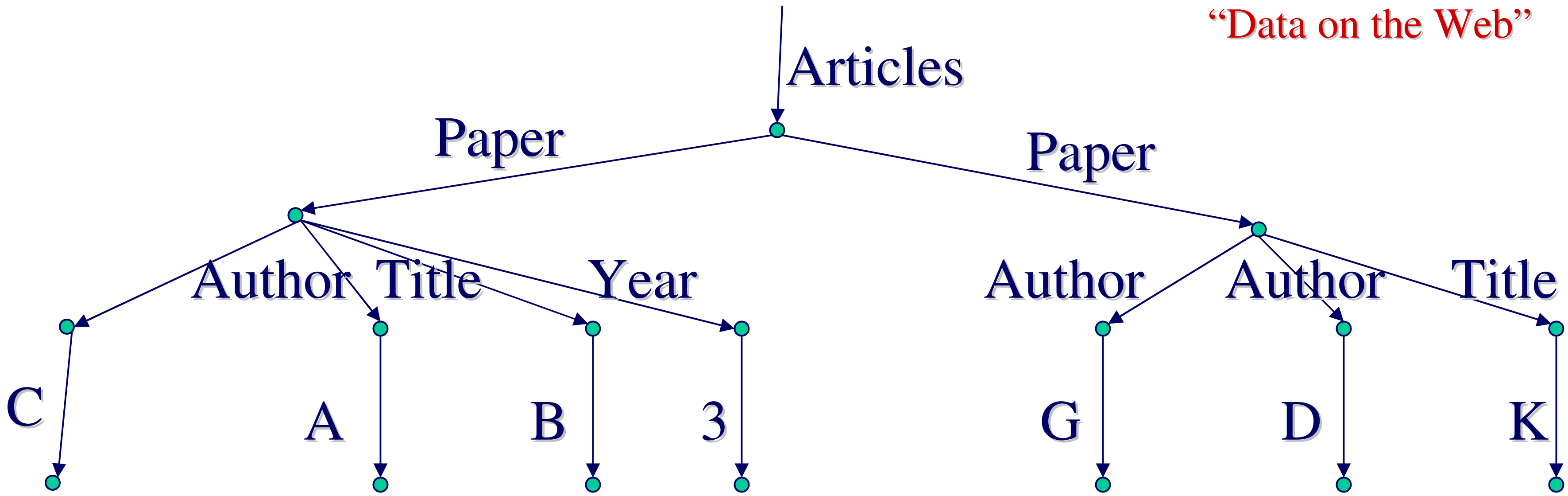
Outline:

- Warm-up: a logic for (finite, edge-labeled) trees.
    - Spatial interpretation: a formula talks about a particular (sub-) tree.
- Composition
    - Spatial interpretation: a formula talks about part of a system.
- Restriction
    - Spatial interpretation: a formula talks about a private resource.

Semistructured Data

(I.e.: XML after parsing)

Abiteboul, Buneman, Suciu:
"Data on the Web"



A tree (or graph), unordered (or ordered). With labels on the edges.

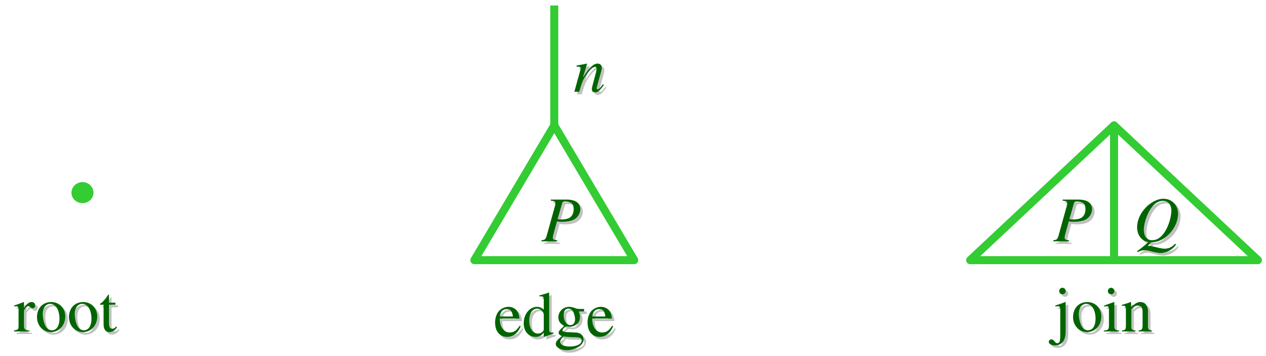
Invented for "flexible" data representation, for quasi-regular data like address books and bibliographies.

Adopted by the DB community as a solution to the "database merge" problem: merging databases from uncoordinated (web) sources.

Adopted by W3C as "web data", then by everybody else.

Trees and their Descriptions

Trees



Syntax for Trees (P, Q)

$\mathbf{0}$	root
$n[P]$	edge
$P \mid Q$	join

Basic Descriptions $(\mathcal{A}, \mathcal{B})$

$\mathbf{0}$	there is only a root
$n[\mathcal{A}]$	there is an edge n to a subtree
$\mathcal{A} \mid \mathcal{B}$	there are two joined trees
$\mathbf{T}$	there is anything

$P \equiv Q$ iff they represent the same tree.
It is the congruence induced by:

$$P_1 \mid P_2 \equiv P_2 \mid P_1$$
$$P_1 \mid (P_2 \mid P_3) \equiv (P_1 \mid P_2) \mid P_3$$
$$P \mid \mathbf{0} \equiv P$$

Formulas and Satisfaction Relation

$P \vDash \mathbf{F}$	*never*		$(\mathbf{T} \triangleq \mathbf{F} \Rightarrow \mathbf{F})$
$P \vDash \mathcal{A} \wedge \mathcal{B}$	$\triangleq$	$P \vDash \mathcal{A} \wedge P \vDash \mathcal{B}$	
$P \vDash \mathcal{A} \Rightarrow \mathcal{B}$	$\triangleq$	$P \vDash \mathcal{A} \Rightarrow P \vDash \mathcal{B}$	
$P \vDash \mathbf{0}$	$\triangleq$	$P \equiv \mathbf{0}$	
$P \vDash \mathcal{A} \mid \mathcal{B}$	$\triangleq$	$\exists P', P'' \in \Pi.\ P \equiv P' \mid P'' \wedge P' \vDash \mathcal{A} \wedge P'' \vDash \mathcal{B}$	
$P \vDash \mathcal{A} \triangleright \mathcal{B}$	$\triangleq$	$\forall P' \in \Pi.\ P' \vDash \mathcal{A} \Rightarrow P \mid P' \vDash \mathcal{B}$	
$P \vDash n[\mathcal{A}]$	$\triangleq$	$\exists P' \in \Pi.\ P \equiv n[P'] \wedge P' \vDash \mathcal{A}$	
$P \vDash \mathcal{A}@n$	$\triangleq$	$n[P] \vDash \mathcal{A}$	

Basic fact: if $P \vDash \mathcal{A}$ and $P \equiv Q$, then $Q \vDash \mathcal{A}$

Model:

- The collection of those sets of *P's* that are closed under $\equiv$.
  (I.e., in this simple case, the collection of all sets of trees.)
- A boolean algebra ($\mathbf{F}\ \wedge\ \Rightarrow$), a quantale ($\mid\ \triangleright$), and more ($n[]\ \ @n$).
- With some interesting interactions: $\mathcal{A} \triangleright \mathbf{F}$ = "$\mathcal{A}$ unsatisfiable"

Examples

"Vertical" implications about nesting

"Business Policy"

Borders[
  Starbucks[…] |
  Books[…] |
  Records[…]
]

$Borders[\mathbf{T}] \Rightarrow$
$Borders[Starbucks[\mathbf{T}] \mid Books[\mathbf{T}] \mid \mathbf{T}]$

If it's a Borders,
then it must contain a Starbucks
(and some books)

"Horizontal" implications about proximity

"Social Policy"

Smoker[…] |
NonSmoker[…] |
Smoker[…]

$(NonSmoker[\mathbf{T}] \mid \mathbf{T}) \Rightarrow$
$(Smoker[\mathbf{T}] \mid \mathbf{T})$

If there is a NonSmoker,
then there must be a Smoker nearby

What makes a room bad for a nonsmoker?

$? \vDash \mathit{NonSmoker}[\mathbf{T}] \triangleright \mathit{BadRoom}$

$$\mathit{BadRoom} \triangleq (\mathit{NonSmoker}[\mathbf{T}] \mid \mathbf{T}) \Rightarrow (\mathit{Smoker}[\mathbf{T}] \mid \mathbf{T})$$

Answer: $? = \mathit{Smoker}[\ldots]$

What makes a Borders legal?

$? \vDash \mathit{OkBorders}@\mathit{Borders}$

$$\mathit{OkBorders} \triangleq \mathit{Borders}[\mathbf{T}] \Rightarrow \mathit{Borders}[\mathit{Starbucks}[\mathbf{T}] \mid \mathit{Books}[\mathbf{T}] \mid \mathbf{T}]$$

Answer: $? = \mathit{Starbucks}[\ldots] \mid \mathit{Books}[\ldots]$

Or illegal:

$? \vDash (\neg \mathit{OkBorders})@\mathit{Borders}$

Answer: $? = \mathit{Books}[\ldots]$

Ground Propositional Spatial Logic (for Trees)

$$\ldots\ t_i : \mathcal{A}_i \ldots \ \vdash\ \ldots\ u_j : \mathcal{B}_j \ldots$$

Identity, Cut, and Contraction

(Id)
$$\frac{t \equiv u}{\Gamma, t : \mathcal{A} \vdash u : \mathcal{A}, \Delta}$$

(Cut)
$$\frac{\Gamma \vdash t : \mathcal{A}, \Delta \qquad \Gamma, t : \mathcal{A} \vdash \Delta}{\Gamma \vdash \Delta}$$

(C L)
$$\frac{\Gamma, t : \mathcal{A}, t : \mathcal{A} \vdash \Delta}{\Gamma, t : \mathcal{A} \vdash \Delta}$$

(C R)
$$\frac{\Gamma \vdash t : \mathcal{A}, t : \mathcal{A}, \Delta}{\Gamma \vdash t : \mathcal{A}, \Delta}$$

Propositional Connectives

(F L)
$$\frac{}{\Gamma, t : \mathbf{F} \vdash \Delta}$$

(F R)
$$\frac{\Gamma \vdash \Delta}{\Gamma \vdash t : \mathbf{F}, \Delta}$$

(∧ L)
$$\frac{\Gamma, t : \mathcal{A}, t : \mathcal{B} \vdash \Delta}{\Gamma, t : \mathcal{A} \wedge \mathcal{B} \vdash \Delta}$$

(∧ R)
$$\frac{\Gamma \vdash t : \mathcal{A}, \Delta \qquad \Gamma \vdash t : \mathcal{B}, \Delta}{\Gamma \vdash t : \mathcal{A} \wedge \mathcal{B}, \Delta}$$

(⇒ L)
$$\frac{\Gamma \vdash t : \mathcal{A}, \Delta \qquad \Gamma, t : \mathcal{B} \vdash \Delta}{\Gamma, t : \mathcal{A} \Rightarrow \mathcal{B} \vdash \Delta}$$

(⇒ R)
$$\frac{\Gamma, t : \mathcal{A} \vdash t : \mathcal{B}, \Delta}{\Gamma \vdash t : \mathcal{A} \Rightarrow \mathcal{B}, \Delta}$$

adjunction:
$$\frac{\mathcal{A} \wedge \mathcal{B} \vdash \mathcal{C}}{\overline{\mathcal{A} \vdash \mathcal{B} \Rightarrow \mathcal{C}}}$$

Spatial Connectives

(0 L)

$$\frac{t \not\equiv 0}{\Gamma, t : \mathbf{0} \vdash \Delta}$$

(0 R)

$$\frac{t \equiv 0}{\Gamma \vdash t : \mathbf{0}, \Delta}$$

(| L)

$$\frac{\forall u,v \therefore u|v \equiv t.\ \ \Gamma, u : \mathcal{A}, v : \mathcal{B} \vdash \Delta}{\Gamma, t : \mathcal{A} \mid \mathcal{B} \vdash \Delta}$$

(| R)

$$\frac{\exists u,v \therefore u|v \equiv t.\ \ \Gamma \vdash u : \mathcal{A}, \Delta \quad \Gamma \vdash v : \mathcal{B}, \Delta}{\Gamma \vdash t : \mathcal{A} \mid \mathcal{B}, \Delta}$$

(▷ L)

$$\frac{\exists u.\ \ \Gamma \vdash u : \mathcal{A}, \Delta \quad \Gamma, t|u : \mathcal{B} \vdash \Delta}{\Gamma, t : \mathcal{A} \triangleright \mathcal{B} \vdash \Delta}$$

(▷ R)

$$\frac{\forall u.\ \ \Gamma, u : \mathcal{A} \vdash t|u : \mathcal{B}, \Delta}{\Gamma \vdash t : \mathcal{A} \triangleright \mathcal{B}, \Delta}$$

adjunction:

$$\frac{\mathcal{A} \mid \mathcal{B} \vdash \mathcal{C}}{\overline{\mathcal{A} \vdash \mathcal{B} \triangleright \mathcal{C}}}$$

(n[] L)

$$\frac{\forall u \therefore n[u] \equiv t.\ \ \Gamma, u : \mathcal{A} \vdash \Delta}{\Gamma, t : n[\mathcal{A}] \vdash \Delta}$$

(n[] R)

$$\frac{\exists u \therefore n[u] \equiv t.\ \ \Gamma \vdash u : \mathcal{A}, \Delta}{\Gamma \vdash t : n[\mathcal{A}], \Delta}$$

(@n L)

$$\frac{\Gamma, n[t] : \mathcal{A} \vdash \Delta}{\Gamma, t : \mathcal{A}@n \vdash \Delta}$$

(@n R)

$$\frac{\Gamma \vdash n[t] : \mathcal{A}, \Delta}{\Gamma \vdash t : \mathcal{A}@n, \Delta}$$

adjunction:

$$\frac{n[\mathcal{A}] \vdash \mathcal{C}}{\overline{\mathcal{A} \vdash \mathcal{C}@n}}$$

Calcagno-Cardelli-Gordon:
***Deciding Validity in a Spatial Logic for Trees*.**

N.B.: neither t nor $\mathcal{A}$ contain variables. Then:

- $t \vDash \mathcal{A}$ is decidable.
- Validity is expressible in the logic, so it is also decidable whether $\mathcal{A}$ is valid (i.e.: whether $0 \vDash (\mathcal{A} \Rightarrow \mathbf{F}) \triangleright \mathbf{F}$).
- There is a finitary version of the proof system.
- There is a complete decision procedure for $\Gamma \vdash \Delta$.

$(\mathcal{A} \mid \mathcal{B}) \wedge \mathbf{0} \vdash \mathcal{A} \wedge \mathcal{B}$

N.B. This is not a proof, it is a proof schema showing how to obtain a proof (a finite derivation) for each ground instance of t.

If $t \not\equiv 0$ **then**

2 $\Gamma, t : \mathcal{A} \mid \mathcal{B}, t : \mathbf{0} \vdash t : \mathcal{A} \wedge \mathcal{B}, \Delta$ (**0** L)

1 $\Gamma, t : (\mathcal{A} \mid \mathcal{B}) \wedge \mathbf{0} \vdash t : \mathcal{A} \wedge \mathcal{B}, \Delta$ 1, ($\wedge$ L)

If $t \equiv 0$ **then**

4.2 $\forall u,v \therefore u|v \equiv t.\ \ \Gamma, u : \mathcal{A}, v : \mathcal{B}, t : \mathbf{0} \vdash t : \mathcal{A}, \Delta$ (Id) since $u|v\equiv\mathbf{0} \Rightarrow u\equiv\mathbf{0} \Rightarrow t\equiv\mathbf{0}$

3.2 $\Gamma, t : (\mathcal{A} \mid \mathcal{B}), t : \mathbf{0} \vdash t : \mathcal{A}, \Delta$ 4.2, (| L)

2.2 $\Gamma, t : (\mathcal{A} \mid \mathcal{B}) \wedge \mathbf{0} \vdash t : \mathcal{A}, \Delta$ 3.2, ($\wedge$ L)

...

2.1 $\langle S \rangle\ \Gamma, t : (\mathcal{A} \mid \mathcal{B}) \wedge \mathbf{0} \vdash t : \mathcal{B}, \Delta$ Similarly

1 $\langle S \rangle\ \Gamma, t : (\mathcal{A} \mid \mathcal{B}) \wedge \mathbf{0} \vdash t : \mathcal{A} \wedge \mathcal{B}, \Delta$ 2.1, 2.2, ($\wedge$ R)

New Logics for Concurrency

In the process of making spatial sense of $n[\mathcal{A}]$, we also had to make spatial sense of $\mathcal{A} \mid \mathcal{B}$. The latter is, in fact, the harder part. So, in retrospect, it makes sense to consider it on its own.

An outcome is spatial logics for CCS/CSP-like process calculi. Basic idea: take a Hennessy-Milner modal logic and add an $\mathcal{A} \mid \mathcal{B}$ operator. ([Dam] Very hard to reconcile with bisimulation.)

One can go further and investigate spatial logics for restriction, with a *hiding quantifier* $\mathsf{H}x.\mathcal{A}$ (e.g. for π-calculus). This is essential for security/privacy specifications.
([Caires] Very hard to reconcile with bisimulation.)

We can make all that work smoothly by taking a very *intensional* point of view. The logical formulas are not *up-to-bisimulation*: they are *up-to-structural-congruence*. This requires a pretty drastic change in point of view.

Caires-Cardelli: ***A Spatial Logic for Concurrency (Part I,II).*** TACS'01, CONCUR'02.

Spatial Properties: Identifiable Subsystems

A system is often composed of identifiable subsystems.

- "A message is sent from Alice to Bob."
- "The protocol is split between two participants."
- "The virus attacks the server."

Such partitions of a system are (obviously) spatial properties. They correspond to a spatial arrangement of processes in different places.

- Process calculi are *very* good at expressing such arrangements operationally (*c.f.*, chemical semantics, structural congruence).
- To the point that a process is often used as a specification of another process. (We consider this as an anomaly!)
- We want something equally good at the specification, or logical, level.

Spatial Properties: Restricted Resources

A system often restricts the use of certain resources to certain subsystems.

- "A shared private key n is established between two processes."
- "A fresh nonce n is generated locally and transmitted."
- "The applet runs in a secret sandbox."

Something is *hidden/secret/private* if it is present only in a limited subsystem. So these are spatial properties too.

- If something is secret, by assumption it cannot be known. Still, we want to talk about it in specifications.
- We can talk about a secret name only by using a *fresh* name for it (we cannot assume the secret name matches any known name).
- So freshness will be an important concept. Logics of freshness are very new.

Spatial-style Protocol Specification

Right now, we have a spatial configuration, and later, we have another spatial configuration.

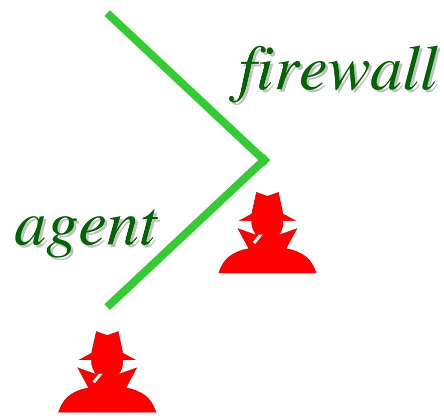
E.g.: Right now, the agent is outside the firewall, …

(*agent*[**T**] | *firewall*[**T**] | **T**)

Spatial-style Protocol Specification

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.

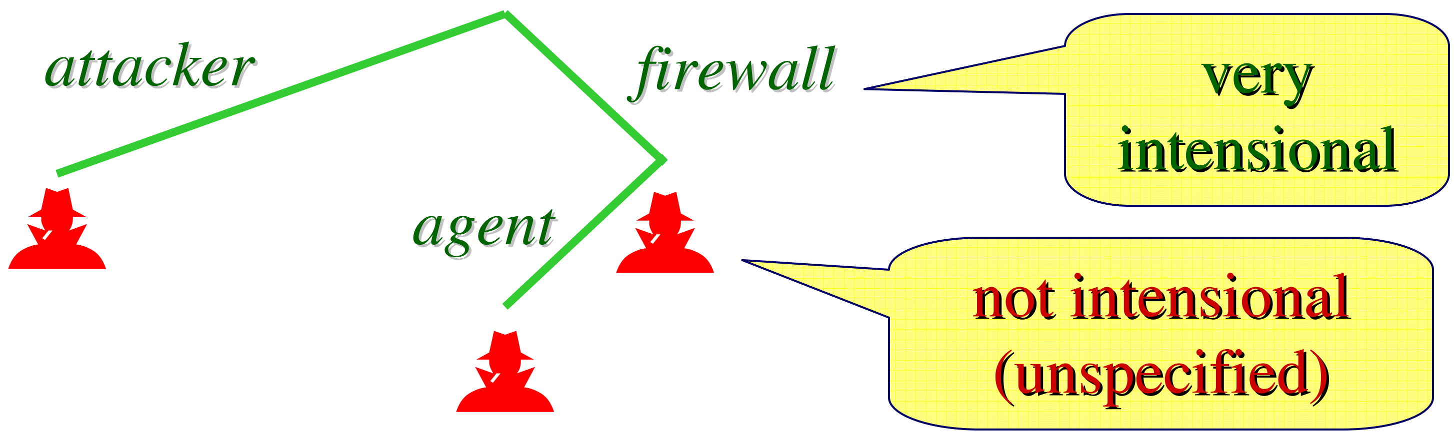


$(\mathit{agent}[\mathbf{T}] \mid \mathit{firewall}[\mathbf{T}] \mid \mathbf{T}) \wedge \Diamond(\mathit{firewall}[\mathit{agent}[\mathbf{T}] \mid \mathbf{T}] \mid \mathbf{T})$

Spatial-style Protocol Specification

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. And this works in presence of any (reasonable) attacker.



$$\mathit{Attack} \triangleright ((\mathit{agent}[\mathbf{T}] \mid \mathit{firewall}[\mathbf{T}] \mid \mathbf{T}) \wedge \Diamond(\mathit{firewall}[\mathit{agent}[\mathbf{T}] \mid \mathbf{T}] \mid \mathbf{T}))$$

Shocking things one may say

Single-threaded (or void):

$\neg(\neg\mathbf{0} \mid \neg\mathbf{0})$

Output: outputs a message m on n (and is/does nothing else):

$n\langle m\rangle$

In presence of a message m on n, sends a message n on m and stops:

$n\langle m\rangle \triangleright \text{»}m\langle n\rangle$

Contains a name free:

$\copyright n \quad \triangleq \quad \neg n\circledR\mathbf{T}$

$P \vDash \neg n\circledR\mathbf{T}$ iff $\neg\, P \equiv (\nu n)P'$ iff $n \in fn(P)$

Has a shared secret:

$\mathsf{H}x.\ \copyright x \mid \copyright x$

Logical Formulas for π-Worlds

$\mathcal{A}, \mathcal{B} \in \Phi ::=$	Formulas		
$\mathbf{F}$	false		
$\mathcal{A} \wedge \mathcal{B}$	conjunction	$\mathcal{A} \Rightarrow \mathcal{B}$	implication
$\mathbf{0}$	void		
$\mathcal{A} \mid \mathcal{B}$	composition	$\mathcal{A} \triangleright \mathcal{B}$	guarantee
$n ® \mathcal{A}$	revelation	$\mathcal{A} \oslash n$	hiding
$n\langle m \rangle$	message		
$»\mathcal{A}$	next	$\mathcal{A}«$	previous
$\forall x.\mathcal{A}$	universal name quantifier		
$\text{И}x.\mathcal{A}$	fresh name quantifier		
$\forall X.\mathcal{A}$	propositional quantifier		
X	propositional variables		
$n ::=$	Terms ($n,m,p \in \mathcal{N}$)		
x	name var ($x \in \mathcal{V}$)		
$(n \leftrightarrow m)p$	name transposition		

Basic observation

Used to define a “hiding quantifier” for $(\nu n)P$

Used to define μ-calculus style least and greatest fixpoints via F-algebra style encodings

A Motivating Example

$$Client \triangleq \mathsf{H}x.\ (Protocol(x) \mid Request(x))$$

A *Client* generates a secret x and then engages in a $Protocol(x)$ (e.g. simply $pub\langle x\rangle$) in order to perform a request $Request(x)$ (e.g. some communication on x) which is uniquely associated with the secret x.

$$Server \triangleq \text{И}x.(Protocol(x) \triangleright \Diamond(Handler(x) \mid Server))$$

A (recursive) *Server*, in presence of an instance of *Protocol* for a fresh x, produces a $Handler(x)$ uniquely associated with the secret x, and is ready again as a *Server*.

$$Client \mid Server \Rightarrow \Diamond(Server \mid \mathsf{H}x.\ (Request(x) \mid Handler(x)))$$

When a client interacts with a server, the result is eventually again a server, together with a <u>private</u> handler for the client request.

We can show this implication in the logic, without looking at any implementation of *Client* and *Server*.

Note the subtle distinction between having/creating a secret ($\mathsf{H}x$) and obtaining/using a fresh secret ($\text{И}x$). The quantifier $\mathsf{H}x$ must match a restriction (νn), while the quantifier $\text{И}x$ must match a fresh name that may be generated by a restriction.

Sequents

Many-world sequents: $\langle S \rangle\, \Gamma \vdash \Delta$

Validity: if all the constraints S_k and all the assumptions Γ_i are satisfied, then one of the conclusions Δ_j is satisfied

(Spatial) equivalence constraints (denote structural congruence)

(Nominal) distinction constraints (denote name distinctions)

$$\langle \ldots u' \doteq v' \ldots u'' \rightarrow v'' \ldots n\#m \ldots n\#X \ldots \rangle \ldots u : \mathcal{A} \ldots \vdash \ldots v : \mathcal{B} \ldots$$

(Temporal) reduction constraints (denote process reduction)

Formulas (denote properties)

Indexes (denote processes)

Constraint Resolution:

$S \vdash u \doteq v$ $\quad$ $S \vdash u \rightarrow v$ $\quad$ $S \vdash n\#m$ $\quad$ $S \vdash n\#X$

Recipe for Rules

Left rules, *right rules*. Operate mainly on the $\Gamma \vdash \Delta$ part.

- When operating on constraints $\langle S \rangle$:
  - Going up: One adds, the other checks constraints.
  - Going down: One removes, the other assumes constraints.
- They form cut elimination pairs.

World rules (optional). Operate on the $\langle S \rangle$ part only.

- Embody inversion lemmas: deep properties of process calculi.
  (In temporal logic, they embody properties such as reflexivity and transitivity of the reachibility relation.)
  - Going up: add deducible constraints.
  - Going down: remove redundant constraints.
- Commute easily with cuts.

Composition

$\mathcal{A} \mid \mathcal{B}$ the system is made of two distinct components satisfying $\mathcal{A}$ and $\mathcal{B}$.

Right Rule

$\exists v, t$

(| R)

$$\frac{\langle S\rangle\, \Gamma \vdash v : \mathcal{A}, \Delta \quad \langle S\rangle\, \Gamma \vdash t : \mathcal{B}, \Delta \quad S \vdash u \doteq v|t}{\langle S\rangle\, \Gamma \vdash u : \mathcal{A} \mid \mathcal{B}, \Delta}$$

check constraint

$\forall \mathcal{X}, \mathcal{Y}$

Left Rule

(| L) *$\mathcal{X}, \mathcal{Y}$ not free in the conclusion*

remove constraint

$$\frac{\langle S, u \doteq \mathcal{X} \mid \mathcal{Y}\rangle\, \Gamma, \mathcal{X} : \mathcal{A}, \mathcal{Y} : \mathcal{B} \vdash \Delta}{\langle S\rangle\, \Gamma, u : \mathcal{A} \mid \mathcal{B} \vdash \Delta}$$

World Rules

(S | 0)

$$\frac{\langle S, u \doteq \mathbf{0}\rangle\, \Gamma \vdash \Delta \quad S \vdash u|v \doteq \mathbf{0}}{\langle S\rangle\, \Gamma \vdash \Delta}$$

(S | |)

$$\frac{\ldots \quad S \vdash u|v \doteq t|w}{\langle S\rangle\, \Gamma \vdash \Delta}$$

Suppose $u|v=0 \Rightarrow u=0$. Then, if we can already deduce that $u|v \doteq 0$, we can eliminate a redundant assumption $u \doteq 0$.

Restriction

$n®\mathcal{A}$

The system has a hidden resource, that we shall call n,
and an interior satisfying $\mathcal{A}$.

We say that we "reveal" the hidden resource as n (if possible).

Right Rule

(® R)

$$\frac{\langle S\rangle\, \Gamma \vdash t : \mathcal{A}, \Delta \quad S \vdash u \doteq (\nu n)t}{\langle S\rangle\, \Gamma \vdash u : n®\mathcal{A}, \Delta}$$

check that u has the form (νn)t, for that precise n (hence $n \notin fn(u)$)

Left Rule

(® L) *Υ not free in the conclusion*

$$\frac{\langle S, u \doteq (\nu n)\Upsilon\rangle\, \Gamma, \Upsilon : \mathcal{A} \vdash \Delta}{\langle S\rangle\, \Gamma, u : n®\mathcal{A} \vdash \Delta}$$

assuming $n \notin fn(u)$…

World Rules

(S ν 0)

$$\frac{\langle S, u \doteq \mathbf{0}\rangle\, \Gamma \vdash \Delta \quad S \vdash (\nu n)u \doteq \mathbf{0}}{\langle S\rangle\, \Gamma \vdash \Delta}$$

(S ν |)

$$\frac{\ldots \quad S \vdash (\nu n)u \doteq t|v}{\langle S\rangle\, \Gamma \vdash \Delta}$$

(S ν ν)

$$\frac{\ldots \quad S \vdash (\nu n)u \doteq (\nu m)v}{\langle S\rangle\, \Gamma \vdash \Delta}$$

Freshness and Hiding

$Ⅎx.\ \mathcal{A}$ for all/some fresh name n denoted by x, the system satisfies $\mathcal{A}\{x\leftarrow n\}$. (The name n is fresh both in the system and in $\mathcal{A}$)

$\mathsf{H}x.\mathcal{A} \triangleq Ⅎx.\ x®\mathcal{A}$ the system has a hidden resource x that we can reveal as any fresh n, and has an interior satisfying $\mathcal{A}\{x\leftarrow n\}$.

$\mathsf{H}x.\mathcal{A}$ is the logical construct that corresponds to restriction:

Derived Right Rule

(H **R**)

$$\frac{\langle S\rangle\ \Gamma \vdash v : \mathcal{A}\{x\leftarrow n\}, \Delta \quad S \vdash u \doteq (\nu n)v \quad S \vdash n\#\mathsf{H}x.\mathcal{A}}{\langle S\rangle\ \Gamma \vdash\ u : \mathsf{H}x.\mathcal{A}, \Delta}$$

check that n is fresh for all names in u and $\mathcal{A}$

Ex.: $\mathsf{H}x.p\langle x\rangle$ is a system that outputs a fresh name on channel p.

Implementable as $u = (\nu n)p\langle n\rangle$.

Propositional Rules

Identity, Cut, and Contraction: (Exchange is implicit)

(Id)

$$\frac{S \vdash u \doteq v \qquad S \vdash \mathcal{A} \equiv \mathcal{B}}{\langle S \rangle\, \Gamma, u : \mathcal{A} \vdash v : \mathcal{B}, \Delta}$$

(Cut)

$$\frac{\langle S \rangle\, \Gamma \vdash u : \mathcal{A}, \Delta \qquad \langle S \rangle\, \Gamma, u : \mathcal{A} \vdash \Delta}{\langle S \rangle\, \Gamma \vdash \Delta}$$

(C L)

$$\frac{\langle S \rangle\, \Gamma, u : \mathcal{A}, u : \mathcal{A} \vdash \Delta}{\langle S \rangle\, \Gamma, u : \mathcal{A} \vdash \Delta}$$

(C R)

$$\frac{\langle S \rangle\, \Gamma \vdash u : \mathcal{A}, u : \mathcal{A}, \Delta}{\langle S \rangle\, \Gamma \vdash u : \mathcal{A}, \Delta}$$

L/R Rules:

(∧ L)

$$\frac{\langle S \rangle\, \Gamma, u : \mathcal{A}, u : \mathcal{B} \vdash \Delta}{\langle S \rangle\, \Gamma, u : \mathcal{A} \wedge \mathcal{B} \vdash \Delta}$$

(∧ R)

$$\frac{\langle S \rangle\, \Gamma \vdash u : \mathcal{A}, \Delta \qquad \langle S \rangle\, \Gamma \vdash u : \mathcal{B}, \Delta}{\langle S \rangle\, \Gamma \vdash u : \mathcal{A} \wedge \mathcal{B}, \Delta}$$

(⇒ L)

$$\frac{\langle S \rangle\, \Gamma \vdash u : \mathcal{A}, \Delta \qquad \langle S \rangle\, \Gamma, u : \mathcal{B} \vdash \Delta}{\langle S \rangle\, \Gamma, u : \mathcal{A} \Rightarrow \mathcal{B} \vdash \Delta}$$

(⇒ R)

$$\frac{\langle S \rangle\, \Gamma, u : \mathcal{A} \vdash u : \mathcal{B}, \Delta}{\langle S \rangle\, \Gamma \vdash u : \mathcal{A} \Rightarrow \mathcal{B}, \Delta}$$

(F L)

$$\frac{}{\langle S \rangle\, \Gamma, u : \mathbf{F} \vdash \Delta}$$

(F R)

$$\frac{\langle S \rangle\, \Gamma \vdash \Delta}{\langle S \rangle\, \Gamma \vdash u : \mathbf{F}, \Delta}$$

Spatial Rules

L/R Rules:

(0 L)

$$\frac{\langle S,\ u \doteq \mathbf{0}\rangle\ \Gamma \vdash \Delta}{\langle S\rangle\ \Gamma,\ u : \mathbf{0} \vdash \Delta}$$

(0 R)

$$\frac{S \vdash u \doteq \mathbf{0}}{\langle S\rangle\ \Gamma \vdash u : \mathbf{0},\ \Delta}$$

(| L) *$\mathcal{X}, \mathcal{Y}$ not free in the conclusion*

$$\frac{\langle S,\ u \doteq \mathcal{X} \mid \mathcal{Y}\rangle\ \Gamma,\ \mathcal{X} : \mathcal{A},\ \mathcal{Y} : \mathcal{B} \vdash \Delta}{\langle S\rangle\ \Gamma,\ u : \mathcal{A} \mid \mathcal{B} \vdash \Delta}$$

(| R)

$$\frac{\langle S\rangle\ \Gamma \vdash v : \mathcal{A},\ \Delta \quad \langle S\rangle\ \Gamma \vdash t : \mathcal{B},\ \Delta \quad S \vdash u \doteq v | t}{\langle S\rangle\ \Gamma \vdash u : \mathcal{A} \mid \mathcal{B},\ \Delta}$$

(▷ L)

$$\frac{\langle S\rangle\ \Gamma \vdash t : \mathcal{A},\ \Delta \quad \langle S\rangle\ \Gamma,\ t | u : \mathcal{B} \vdash \Delta}{\langle S\rangle\ \Gamma,\ u : \mathcal{A} \triangleright \mathcal{B} \vdash \Delta}$$

(▷ R) *$\mathcal{X}$ not free in the conclusion*

$$\frac{\langle S\rangle\ \Gamma,\ \mathcal{X} : \mathcal{A} \vdash v : \mathcal{B},\ \Delta \quad S \vdash v \doteq \mathcal{X} | u}{\langle S\rangle\ \Gamma \vdash u : \mathcal{A} \triangleright \mathcal{B},\ \Delta}$$

(® L) *$\mathcal{Y}$ not free in the conclusion*

$$\frac{\langle S,\ u \doteq (\nu n)\mathcal{Y}\rangle\ \Gamma,\ \mathcal{Y} : \mathcal{A} \vdash \Delta}{\langle S\rangle\ \Gamma,\ u : n®\mathcal{A} \vdash \Delta}$$

(® R)

$$\frac{\langle S\rangle\ \Gamma \vdash t : \mathcal{A},\ \Delta \quad S \vdash u \doteq (\nu n)t}{\langle S\rangle\ \Gamma \vdash u : n®\mathcal{A},\ \Delta}$$

(⦸ L)

$$\frac{\langle S\rangle\ \Gamma,\ (\nu n)u : \mathcal{A} \vdash \Delta}{\langle S\rangle\ \Gamma,\ u : \mathcal{A} ⦸ n \vdash \Delta}$$

(⦸ R)

$$\frac{\langle S\rangle\ \Gamma \vdash t : \mathcal{A},\ \Delta \quad S \vdash t \doteq (\nu n)u}{\langle S\rangle\ \Gamma \vdash u : \mathcal{A} ⦸ x,\ \Delta}$$

S Rules:

(S | 0)

$$\frac{\langle S,\ u \doteq \mathbf{0}\rangle\ \Gamma \vdash \Delta \qquad S \vdash u|v \doteq \mathbf{0}}{\langle S\rangle\ \Gamma \vdash \Delta}$$

(S | |) *$\mathcal{X},\mathcal{Y},\mathcal{U},\mathcal{V}$ not free in the conclusion*

$$\frac{\langle S,\ u \doteq \mathcal{X}\,|\,\mathcal{Y},\ v \doteq \mathcal{U}\,|\,\mathcal{V},\ t \doteq \mathcal{X}\,|\,\mathcal{U}, w \doteq \mathcal{Y}\,|\,\mathcal{V}\rangle\ \Gamma \vdash \Delta \qquad S \vdash u|v \doteq t|w}{\langle S\rangle\ \Gamma \vdash \Delta}$$

(S ν 0)

$$\frac{\langle S,\ u \doteq \mathbf{0}\rangle\ \Gamma \vdash \Delta \qquad S \vdash (\nu n)u \doteq \mathbf{0}}{\langle S\rangle\ \Gamma \vdash \Delta}$$

(S ν |) *$\mathcal{X},\mathcal{Y}$ not free in the conclusion*

$$\frac{\langle S,\ u \doteq \mathcal{X}\,|\,\mathcal{Y},\ (\nu n)\mathcal{X} \doteq t,\ (\nu n)\mathcal{Y} \doteq v\rangle\ \Gamma \vdash \Delta \qquad S \vdash (\nu n)u \doteq t|v}{\langle S\rangle\ \Gamma \vdash \Delta}$$

(S ν ν) *$\mathcal{X}$ not free in the conclusion*

$$\frac{\langle S,\ u \doteq (n{\leftrightarrow}m)v\rangle\ \Gamma \vdash \Delta \qquad \langle S,\ u \doteq (\nu m)\mathcal{X},\ v \doteq (\nu n)\mathcal{X}\rangle\ \Gamma \vdash \Delta \qquad S \vdash (\nu n)u \doteq (\nu m)v}{\langle S\rangle\ \Gamma \vdash \Delta}$$

$(\mathcal{A} \mid \mathcal{B}) \wedge \mathbf{0} \vdash \mathcal{A} \wedge \mathcal{B}$

6.2 $\langle S,\ u \doteq \mathcal{X} \mid \mathcal{Y},\ u \doteq \mathbf{0},\ \mathcal{X} \doteq \mathbf{0} \rangle\ \Gamma,\ \mathcal{X} : \mathcal{A},\ \mathcal{Y} : \mathcal{B} \vdash u : \mathcal{A},\ \Delta$	(Id) since $u = \mathcal{X}$
5.2 $\langle S,\ u \doteq \mathcal{X} \mid \mathcal{Y},\ u \doteq \mathbf{0} \rangle\ \Gamma,\ \mathcal{X} : \mathcal{A},\ \mathcal{Y} : \mathcal{B} \vdash u : \mathcal{A},\ \Delta$	6.2, (S | **0**) since $\mathcal{X} \mid \mathcal{Y} = \mathbf{0}$
4.2 $\langle S,\ u \doteq \mathcal{X} \mid \mathcal{Y} \rangle\ \Gamma,\ \mathcal{X} : \mathcal{A},\ \mathcal{Y} : \mathcal{B},\ u : \mathbf{0} \vdash u : \mathcal{A},\ \Delta$	5.2, (**0** L)
3.2 $\langle S \rangle\ \Gamma,\ u : (\mathcal{A} \mid \mathcal{B}),\ u : \mathbf{0} \vdash u : \mathcal{A},\ \Delta$	4.2, (| L)
2.2 $\langle S \rangle\ \Gamma,\ u : (\mathcal{A} \mid \mathcal{B}) \wedge \mathbf{0} \vdash u : \mathcal{A},\ \Delta$	3.2, ($\wedge$ L)
...	
2.1 $\langle S \rangle\ \Gamma,\ u : (\mathcal{A} \mid \mathcal{B}) \wedge \mathbf{0} \vdash u : \mathcal{B},\ \Delta$	Similarly
1 $\langle S \rangle\ \Gamma,\ u : (\mathcal{A} \mid \mathcal{B}) \wedge \mathbf{0} \vdash u : \mathcal{A} \wedge \mathcal{B},\ \Delta$	2.1, 2.2, ($\wedge$ R)

Temporal Rules

L/R Rules:

(» L) *$\mathcal{X}$ not free in the conclusion*

$$\frac{\langle S,\ u \longrightarrow \mathcal{X}\rangle\ \Gamma, \mathcal{X} : \mathcal{A} \vdash \Delta}{\langle S\rangle\ \Gamma, u : \text{»}\mathcal{A} \vdash \Delta}$$

(» R)

$$\frac{\langle S\rangle\ \Gamma \vdash v : \mathcal{A}, \Delta \quad S \vdash u \longrightarrow v}{\langle S\rangle\ \Gamma \vdash u : \text{»}\mathcal{A}, \Delta}$$

(« L)

$$\frac{\langle S\rangle\ \Gamma, v : \mathcal{A} \vdash \Delta \quad S \vdash v \longrightarrow u}{\langle S\rangle\ \Gamma, u : \mathcal{A}\text{«} \vdash \Delta}$$

(« R) *$\mathcal{X}$ not free in the conclusion*

$$\frac{\langle S,\ \mathcal{X} \longrightarrow u\rangle\ \Gamma \vdash \mathcal{X} : \mathcal{A}, \Delta}{\langle S\rangle\ \Gamma \vdash u : \mathcal{A}\text{«}, \Delta}$$

S Rules:

(S 0 $\longrightarrow$)

$$\frac{S \vdash \mathbf{0} \longrightarrow u}{\langle S\rangle\ \Gamma \vdash \Delta}$$

(S ν $\longrightarrow$) *$\mathcal{X}$ not free in the conclusion*

$$\frac{\langle S,\ u \longrightarrow \mathcal{X},\ v \doteq (\nu n)\mathcal{X}\rangle\ \Gamma \vdash \Delta \quad S \vdash (\nu n)u \longrightarrow v}{\langle S\rangle\ \Gamma \vdash \Delta}$$

No rule (S | $\longrightarrow$).

Quantification Rules

L/R Rules:

($\forall$ L)

$$\frac{\langle S\rangle\, \Gamma, u : \mathcal{A}\{x \leftarrow n\} \vdash \Delta}{\langle S\rangle\, \Gamma, u : \forall x.\mathcal{A} \vdash \Delta}$$

($\forall$ R) *y not free in the conclusion*

$$\frac{\langle S\rangle\, \Gamma \vdash u : \mathcal{A}\{x \leftarrow y\}, \Delta}{\langle S\rangle\, \Gamma \vdash u : \forall x.\mathcal{A}, \Delta}$$

($\forall$2 L)

$$\frac{\langle S\rangle\, \Gamma, u : \mathcal{A}\{X \leftarrow \mathcal{B}\} \vdash \Delta}{\langle S\rangle\, \Gamma, u : \forall X.\mathcal{A} \vdash \Delta}$$

($\forall$2 R) *Y not free in the conclusion*

$$\frac{\langle S\rangle\, \Gamma \vdash u : \mathcal{A}\{X \leftarrow Y\}, \Delta}{\langle S\rangle\, \Gamma \vdash u : \forall X.\mathcal{A}, \Delta}$$

Freshness Rules

L/R Rules:

(И L)

$$\frac{\langle S\rangle\ \Gamma, u : \mathcal{A}\{x\leftarrow n\} \vdash \Delta \quad S \vdash u \doteq (\nu n)v \quad S \vdash n\#\text{И}x.\mathcal{A}}{\langle S\rangle\ \Gamma, u : \text{И}x.\mathcal{A} \vdash \Delta}$$

cf.:

($\forall$ L)

$$\frac{\langle S\rangle\ \Gamma, u : \mathcal{A}\{x\leftarrow n\} \vdash \Delta}{\langle S\rangle\ \Gamma, u : \forall x.\mathcal{A} \vdash \Delta}$$

(И R)

$$\frac{\langle S\rangle\ \Gamma \vdash u : \mathcal{A}\{x\leftarrow n\}, \Delta \quad S \vdash u \doteq (\nu n)v \quad S \vdash n\#\text{И}x.\mathcal{A}}{\langle S\rangle\ \Gamma \vdash u : \text{И}x.\mathcal{A}, \Delta}$$

cf.:

($\exists$ R)

$$\frac{\langle S\rangle\ \Gamma \vdash u : \mathcal{A}\{x\leftarrow n\}, \Delta}{\langle S\rangle\ \Gamma \vdash u : \exists x.\mathcal{A}, \Delta}$$

S Rules:

(И) *Υ, x not free in the conclusion, u or N*

$$\frac{\langle S, x\#N, u \doteq (\nu x)\Upsilon\rangle\ \Gamma \vdash \Delta}{\langle S\rangle\ \Gamma \vdash \Delta}$$

Bottom-up reading: For any process u and set N (of names free in some formula) there is a name x fresh in u and N. *Cf.* GP's Fresh axiom.

Top-down reading: eliminate unused freshness assumptions

Local transposition:

(τ)

$$\frac{\langle S\rangle\ \Gamma, (m\leftrightarrow n)u : \{m\leftrightarrow n\}\cdot\mathcal{A} \vdash \Delta \quad S \vdash m,n\#\, fpv(\mathcal{A})}{\langle S\rangle\ \Gamma, u : \mathcal{A} \vdash \Delta}$$

A main theorem from Part I.
($\{m\leftrightarrow n\}\cdot\mathcal{A}$ applies $m\leftrightarrow n$ to $\mathcal{A}$, possibly attaching explicit transpositions to the free name variables of $\mathcal{A}$.)

This is the basis for the *equivariance* property of the logic.

Examples of Derivable Properties

$\mathsf{H}x.\mathcal{A} \triangleq \text{И}x.\ x®\mathcal{A}$

This is the proper "hiding quantifier" s.t. $u : \mathcal{A} \Rightarrow (\nu x)u : \mathsf{H}x.\mathcal{A}$

Scope Extrusions:

$(®\,|)\quad \langle S\rangle\ \Gamma, u : x®\mathcal{A} \mid x®\mathcal{B} \dashv\vdash u : x®(\mathcal{A} \mid x®\mathcal{B}), \Delta$

$(\text{И}\,|)\quad \langle S\rangle\ \Gamma, u : \text{И}x.\mathcal{A} \mid \text{И}x.\mathcal{B} \dashv\vdash u : \text{И}x.(\mathcal{A} \mid \mathcal{B}), \Delta$

$(\mathsf{H}\,|\,®)\quad \langle S\rangle\ \Gamma, u : (\mathsf{H}x.\mathcal{A}) \mid (\mathsf{H}x.\mathcal{B}) \dashv\vdash u : \mathsf{H}x.\ (\mathcal{A} \mid x®\mathcal{B}), \Delta$

$(\mathsf{H}\,|\,\forall)\quad \langle S\rangle\ \Gamma, u : \mathsf{H}x.\mathcal{A} \mid \forall x.\mathcal{B} \vdash u : \mathsf{H}x.(\mathcal{A} \mid \mathcal{B}), \Delta$

Input: $x(y).\mathcal{A} \triangleq \forall y.\ x\langle y\rangle \rhd »\mathcal{A}$

Recursive nonce generators:

$\mathcal{N}c \triangleq \nu X.\ (\mathsf{H}x.\ nc\langle x\rangle) \mid X$

$\langle S\rangle\ \Gamma, u : \mathcal{N}c \mid nc(y).\mathcal{A}\{y\} \vdash u : »(\mathcal{N}c \mid \mathsf{H}z.\ \mathcal{A}\{z\}), \Delta$

$\langle S\rangle\ \Gamma, u : \mathcal{N}c \mid \mathcal{N}c \vdash u : \mathcal{N}c, \Delta$

(two nonce generators will not accidentally produce the same names)

И-Cut Elimination

Equivariance is essential in cut-elimination.

$$
\dfrac{
\dfrac{\dfrac{\pi_1}{u \doteq_s (\nu n)v \quad n \#_s \text{И}z.\mathcal{A} \quad \langle S\rangle\, \Gamma \vdash u : \mathcal{A}\{z \leftarrow n\}, \Delta}}{\langle S\rangle\, \Gamma \vdash u : \text{И}z.\mathcal{A}, \Delta}\;(\text{И R})
\qquad
\dfrac{\dfrac{\pi_2}{u \doteq_s (\nu m)t \quad m \#_s \text{И}z.\mathcal{A} \quad \langle S\rangle\, \Gamma, u : \mathcal{A}\{z \leftarrow m\} \vdash \Delta}}{\langle S\rangle\, \Gamma, u : \text{И}z.\mathcal{A} \vdash \Delta}\;(\text{И L})
}{\langle S\rangle\, \Gamma \vdash \Delta}\;(\text{Cut})
$$

Original Proof Tree

main problem: may have used different n,m in two branches

(size-preserving equivariance of π_1)

$$
\dfrac{
\dfrac{\pi'_1}{\langle S\rangle\, \Gamma, u : \mathcal{A}\{z \leftarrow m\} \vdash \Delta}
\qquad
\dfrac{\pi_2}{\langle S\rangle\, \Gamma, u : \mathcal{A}\{z \leftarrow m\} \vdash \Delta}
}{\langle S\rangle\, \Gamma \vdash \Delta}\;(\text{Cut})
$$

Restructured Proof Tree

Main difficulty: α-conversion of derivations. Solution: equivariance transformation of $\langle S\rangle\, \Gamma \vdash u : \mathcal{A}\{z \leftarrow n\}, \Delta$ derivation to $\langle S\rangle\, \Gamma, u : \mathcal{A}\{z \leftarrow m\} \vdash \Delta$ derivation, possible because of assumptions $u \doteq_s (\nu n)v$, $n \#_s \text{И}z.\mathcal{A}$, $u \doteq_s (\nu m)t$, $m \#_s \text{И}z.\mathcal{A}$.

(И) just commutes with (Cut), so it is not a problem

Conclusions

We set out to find logics for describing properties of distributed systems.
(After trying equational reasoning, traces, etc.)

Spatial logics exhibit the trade-offs of temporal logics: compact notation for implicit state, nice proof systems, reduced expressiveness.

Along the way, we discovered many other applications for the basic techniques. We believe there is something intriguing and new in the approach and its formalization.

With respect to traditional logics of concurrency, we are very *intensional*.
But another word for it is *precise*.

With Caires, we now have a logic and sequent calculus (with cut-elimination) for π-calculus, where we can express privacy properties.

Related work:

- With Calcagno and Godon: Model checking and validity checking.
- Sangiorgi: Spacetime bisimulation.
- O'Hearn and Pym: Logics for heaps.

http://www.luca.demon.co.uk/SpatialLogics.html

EXTRA

Equivariance

(EV R)

$$\frac{\langle S\rangle\, \Gamma \vdash u : \mathcal{A}, \Delta \quad S \vdash (\nu m)t \doteq u \doteq (\nu n)v \quad S \vdash m,n \,\#\, fpv(\mathcal{A})}{\langle S\rangle\, \Gamma \vdash u : \{m\leftrightarrow n\}\cdot\mathcal{A}, \Delta}$$

3.2 $\langle S\rangle\, \Gamma \vdash u : \mathcal{A}, \Delta$ — $m,n \,\#_S\, fpv(\mathcal{A})$ (Hyp)

2.2 $\langle S\rangle\, \Gamma \vdash (m\leftrightarrow n)u : \{m\leftrightarrow n\}\cdot\mathcal{A}, \Delta$ — 3.2, (τ R)

3.1 $S \vdash (m\leftrightarrow n)u \doteq u$ — $(\nu m)t \doteq_S u \doteq_S (\nu n)v$ (Hyp) (Swap Erase)

2.1 $\langle S\rangle\, \Gamma, (m\leftrightarrow n)u : \{m\leftrightarrow n\}\cdot\mathcal{A} \vdash u : \{m\leftrightarrow n\}\cdot\mathcal{A}, \Delta$ — 3.1, (Id)

1 $\langle S\rangle\, \Gamma \vdash u : \{m\leftrightarrow n\}\cdot\mathcal{A}, \Delta$ — 2.1, 2.2, (Cut)

(τ R)

$$\frac{\langle S\rangle\, \Gamma \vdash u : \mathcal{A}, \Delta \quad S \vdash m,n \,\#\, fpv(\mathcal{A})}{\langle S\rangle\, \Gamma \vdash (m\leftrightarrow n)u : \{m\leftrightarrow n\}\cdot\mathcal{A}, \Delta}$$

2.2 $\langle S\rangle\, \Gamma \vdash u : \mathcal{A}, \Delta$ — $m,n \,\#_S\, fpv(\mathcal{A})$ (Hyp)

3.1 $\langle S\rangle\, \Gamma, (m\leftrightarrow n)u : \{m\leftrightarrow n\}\cdot\mathcal{A} \vdash (m\leftrightarrow n)u : \{m\leftrightarrow n\}\cdot\mathcal{A}, \Delta$ — 3.1, (Id)

2.1 $\langle S\rangle\, \Gamma, u : \mathcal{A} \vdash (m\leftrightarrow n)u : \{m\leftrightarrow n\}\cdot\mathcal{A}, \Delta$ — 3.1, $m,n \,\#_S\, fpv(\mathcal{A})$ (Hyp), (τ)

1 $\langle S\rangle\, \Gamma \vdash (m\leftrightarrow n)u : \{m\leftrightarrow n\}\cdot\mathcal{A}, \Delta$ — 2.1, 2.2, (Cut)

Combining freshness assumptions:

(И Aux) *$\Upsilon, \mathcal{Z}$ not free in the conclusion*

$$\frac{\langle S,\ u \doteq (\nu n)\Upsilon,\ v \doteq (\nu n)\mathcal{Z}\rangle\ \Gamma \vdash \Delta}{\langle S,\ u|v \doteq (\nu n)t\rangle\ \Gamma \vdash \Delta}$$

This can be useful before applying (И),
which works on a single (ν n) constraint.

$\langle S,\ u \doteq (\nu n)\Upsilon,\ v \doteq (\nu n)\mathcal{Z}\rangle\ \Gamma \vdash \Delta$	(Hyp)
$\langle S,\ u|v \doteq (\nu n)t,\ t \doteq \Upsilon|\mathcal{Z},\ u \doteq (\nu n)\Upsilon,\ v \doteq (\nu n)\mathcal{Z}\rangle\ \Gamma \vdash \Delta$	(W S)
$\langle S,\ u|v \doteq (\nu n)t\rangle\ \Gamma \vdash \Delta$	*$\Upsilon, \mathcal{Z}$ gone* (S ν |)

®-Cut Elimination

(® L) *ϒ not free in the conclusion*

$$\frac{\langle S, u \doteq (\nu n)\Upsilon\rangle\ \Gamma, \Upsilon : \mathcal{A} \vdash \Delta}{\langle S\rangle\ \Gamma, u : n\circledR\mathcal{A} \vdash \Delta}$$

(® R CF)

$$\frac{\langle S\rangle\ \Gamma \vdash t : \mathcal{A}, u : n\circledR\mathcal{A}, \Delta \qquad S \vdash u \doteq (\nu n)t}{\langle S\rangle\ \Gamma \vdash u : n\circledR\mathcal{A}, \Delta}$$

Original Proof Tree

$$\dfrac{\dfrac{\dfrac{\pi_1}{\langle S\rangle\ \Gamma \vdash t : \mathcal{A}, u : n\circledR\mathcal{A}, \Delta} \qquad S \vdash u \doteq (\nu n)t}{\langle S\rangle\ \Gamma \vdash u : n\circledR\mathcal{A}, \Delta}\ (\circledR\ \mathrm{R\ CF}) \qquad \dfrac{\dfrac{\pi_2}{\langle S, u \doteq (\nu n)\Upsilon\rangle\ \Gamma, \Upsilon : \mathcal{A} \vdash \Delta}}{\langle S\rangle\ \Gamma, u : n\circledR\mathcal{A} \vdash \Delta}\ (\circledR\ \mathrm{L})}{\langle S\rangle\ \Gamma \vdash \Delta}\ (\mathrm{Cut}\ n\circledR\mathcal{A})$$

Restructured Proof Tree

(Cut $n\circledR\mathcal{A}$**)** applied to a smaller tree

(Cut $\mathcal{A}$**)** applied to a smaller formula

$$\dfrac{\dfrac{\dfrac{\pi_1}{\langle S\rangle\ \Gamma \vdash t : \mathcal{A}, u : n\circledR\mathcal{A}, \Delta} \qquad \dfrac{\dfrac{\pi_2}{\langle S, u \doteq (\nu n)\Upsilon\rangle\ \Gamma, \Upsilon : \mathcal{A} \vdash \Delta}}{\langle S\rangle\ \Gamma, u : n\circledR\mathcal{A} \vdash \Delta}}{\langle S\rangle\ \Gamma \vdash t : \mathcal{A}, \Delta}\ (\mathrm{Cut}\ n\circledR\mathcal{A}) \qquad \dfrac{\pi_2\text{-inst}(t/\Upsilon)}{\langle S\rangle\ \Gamma, t : \mathcal{A} \vdash \Delta}}{\langle S\rangle\ \Gamma \vdash \Delta}\ (\mathrm{Cut}\ \mathcal{A})$$

|-Cut Elimination

(| L) *$\mathcal{X},\mathcal{Y}$ not free in the conclusion*

$$\frac{\langle S, u \doteq \mathcal{X} \mid \mathcal{Y}\rangle\ \Gamma, \mathcal{X} : \mathcal{A}, \mathcal{Y} : \mathcal{B} \vdash \Delta}{\langle S\rangle\ \Gamma, u : \mathcal{A} \mid \mathcal{B} \vdash \Delta}$$

(| R CF)

$$\frac{\langle S\rangle\ \Gamma \vdash v : \mathcal{A}, u : \mathcal{A} \mid \mathcal{B}, \Delta \qquad \langle S\rangle\ \Gamma \vdash t : \mathcal{B}, u : \mathcal{A} \mid \mathcal{B}, \Delta \qquad S \vdash u \doteq v|t}{\langle S\rangle\ \Gamma \vdash u : \mathcal{A} \mid \mathcal{B}, \Delta}$$

Original Proof Tree

$$\dfrac{\dfrac{\dfrac{\pi_1}{\langle S\rangle\ \Gamma \vdash v : \mathcal{A},\ u : \mathcal{A}|\mathcal{B}, \Delta} \quad \dfrac{\pi_2}{\langle S\rangle\ \Gamma \vdash t : \mathcal{B},\ u : \mathcal{A}|\mathcal{B}, \Delta} \quad S \vdash u \doteq v|t}{\langle S\rangle\ \Gamma \vdash u : \mathcal{A} \mid \mathcal{B}, \Delta\ \textbf{(| R CF)}} \qquad \dfrac{\dfrac{\pi_3}{\langle S, u \doteq \mathcal{X} \mid \mathcal{Y}\rangle\ \Gamma, \mathcal{X} : \mathcal{A}, \mathcal{Y} : \mathcal{B} \vdash \Delta}}{\langle S\rangle\ \Gamma, u : \mathcal{A} \mid \mathcal{B} \vdash \Delta\ \textbf{(| L)}}}{\langle S\rangle\ \Gamma \vdash \Delta\ \textbf{(Cut } \mathcal{A} \mid \mathcal{B}\textbf{)}}$$

Restructured Proof Tree

$$\dfrac{\dfrac{\dfrac{\pi_2}{\langle S\rangle\ \Gamma \vdash t : \mathcal{B},\ u : \mathcal{A}|\mathcal{B}, \Delta} \quad \dfrac{\pi_3 \ldots}{\langle S\rangle\ \Gamma, u : \mathcal{A} \mid \mathcal{B} \vdash \Delta}}{\langle S\rangle\ \Gamma \vdash t : \mathcal{B}, \Delta\ \textbf{(Cut } \mathcal{A} \mid \mathcal{B}\textbf{)}} \qquad \dfrac{\dfrac{\pi_3\text{-inst}}{\langle S\rangle\ \Gamma, t : \mathcal{B}, v : \mathcal{A} \vdash \Delta} \quad \dfrac{\pi_1\text{-weakn} \qquad \pi_3\text{-weakn}}{\langle S\rangle\ \Gamma, t : \mathcal{B} \vdash v : \mathcal{A}, \Delta\ \textbf{(Cut } \mathcal{A} \mid \mathcal{B}\textbf{)}}}{\langle S\rangle\ \Gamma, t : \mathcal{B} \vdash \Delta\ \textbf{(Cut } \mathcal{A}\textbf{)}}}{\langle S\rangle\ \Gamma \vdash \Delta\ \textbf{(Cut } \mathcal{B}\textbf{)}}$$

Example: "Shared Secret" Postcondition

Consider a situation where "a hidden name x is shared by two locations n and m, and is not known outside those locations".

$$\mathsf{H}x.(n[©x] \mid m[©x])$$

What can we do with such a spec? We can fully expand the definitions and work it out in the process calculus:

- $P \vDash \mathsf{H}x.(n[©x] \mid m[©x])$

  $\Leftrightarrow \exists r{\in}\Lambda.\ r{\notin}fn(P){\cup}\{n,m\} \wedge \exists R',R''{\in}\Pi.\ P \equiv (\nu r)(n[R'] \mid m[R''])$
  $\wedge\ r{\in}fn(R') \wedge r{\in}fn(R'')$

- E.g.: take $P = (\nu p)\ (n[p[]] \mid m[p[]])$.

Or we can work logically at the formula level, within a proof system.

Ex: Immovable Object vs. Irresistible Force

$$Im \triangleq \mathbf{T} \rhd \Box(obj\langle\rangle \mid \mathbf{T})$$

$$Ir \triangleq \mathbf{T} \rhd \Box\Diamond\neg(obj\langle\rangle \mid \mathbf{T})$$

$Im \mid Ir \;\vdash\; (\mathbf{T} \rhd \Box(obj\langle\rangle \mid \mathbf{T})) \mid \mathbf{T}$	$\mathcal{A} \vdash \mathbf{T}$
$\vdash\; \Box(obj\langle\rangle \mid \mathbf{T})$	$(\mathcal{A} \rhd \mathcal{B}) \mid \mathcal{A} \vdash \mathcal{B}$
$\vdash\; \Diamond\Box(obj\langle\rangle \mid \mathbf{T})$	$\mathcal{A} \vdash \Diamond\mathcal{A}$
$Im \mid Ir \;\vdash\; \mathbf{T} \mid (\mathbf{T} \rhd \Box\Diamond\neg(obj\langle\rangle \mid \mathbf{T}))$	$\mathcal{A} \vdash \mathbf{T}$
$\vdash\; \Box\Diamond\neg(obj\langle\rangle \mid \mathbf{T})$	$\Diamond\neg\mathcal{A} \vdash \neg\Box\mathcal{A}$
$\vdash\; \neg\Diamond\Box(obj\langle\rangle \mid \mathbf{T})$	$\Box\neg\mathcal{A} \vdash \neg\Diamond\mathcal{A}$

Hence: $Im \mid Ir \vdash \mathbf{F}$ $\qquad$ $\mathcal{A} \wedge \neg\mathcal{A} \vdash \mathbf{F}$

Rules for Messages

L/R Rules:

($n\langle m\rangle$ L)

$$\frac{\langle S,\ u \doteq n\langle m\rangle\rangle\ \Gamma \vdash \Delta}{\langle S\rangle\ \Gamma,\ u : n\langle m\rangle \vdash \Delta}$$

($n\langle m\rangle$ R)

$$\frac{S \vdash u \doteq n\langle m\rangle}{\langle S\rangle\ \Gamma \vdash u : n\langle m\rangle,\ \Delta}$$

S Rules:

(S $\mathbf{0}$ $n\langle m\rangle$)

$$\frac{S \vdash \mathbf{0} \doteq n\langle m\rangle}{\langle S\rangle\ \Gamma \vdash \Delta}$$

(S $n\langle m\rangle$ $n\langle m\rangle$)

$$\frac{\langle S,\ m \doteq m',\ n \doteq n'\rangle\ \Gamma \vdash \Delta \qquad S \vdash n\langle m\rangle \doteq n'\langle m'\rangle}{\langle S\rangle\ \Gamma \vdash \Delta}$$

(S | $n\langle m\rangle$)

$$\frac{\langle S,\ u \doteq \mathbf{0},\ v \doteq n\langle m\rangle\rangle\ \Gamma \vdash \Delta \qquad \langle S,\ v \doteq \mathbf{0},\ u \doteq n\langle m\rangle\rangle\ \Gamma \vdash \Delta \qquad S \vdash u|v \doteq n\langle m\rangle}{\langle S\rangle\ \Gamma \vdash \Delta}$$

(S ν $n\langle m\rangle$)

$$\frac{\langle S,\ u \doteq n\langle m\rangle\rangle\ \Gamma \vdash \Delta \qquad n \#_N p \qquad m \#_N p \qquad S \vdash (\nu p)u \doteq n\langle m\rangle}{\langle S\rangle\ \Gamma \vdash \Delta}$$

(S $n\langle m\rangle$ $\longrightarrow$)

$$\frac{S \vdash n\langle m\rangle \longrightarrow u}{\langle S\rangle\ \Gamma \vdash \Delta}$$