Spatial Logics

Luca Cardelli

Microsoft Research

Agay, March 2002

Reflecting joint work with Luís Caires, Andrew D. Gordon.

Motivation

Plenty of logics for *sequential* (i.e. deterministic) computation.

We want logics for *concurrent* computation (Ex.: Hennessy-Milner).

We want logics for *distributed* computation.

- Spatial arrangements of processes are explicit.
- Formulas are modal in time and space.
- The spatial intuition is strong for process calculi with locations.
- But we are now applying it to a standard π-calculus.

We are *not* doing Curry-Howard.

- Because spatial properties are not meant to be preserved by reduction (because of mobility).
- A formula is not realized by a proof tree/computation; it is realized by a *world* (at a particular place and time).

Aim: Describing Distributed Systems

Distributed Systems

- Concurrent systems that are *spatially* distributed.
- And have well-defined subsystems that hold secrets (administrative domains).

Spatial Operators and Spatial Properties

- Are common to all process calculi (e.g., $P \mid Q$).
- Are prominent in calculi with locations (e.g., $n[P]$).
- Spatial properties are finer that popular equivalences such as (temporal) *bisimulation*. (*Cf.* space-time bisimulation.)

We want formal tools to talk about spatial properties.

- So we can precisely describe modern distributed systems.

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 good at expressing such arrangements operationally (*c.f.*, chemical semantics, structural congruence).
- 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.

Typical Spatial Formulas

Processes		*Formulas*	
$\mathbf{0}$	(void)	$\mathbf{0}$	(nothing here)
$P \mid Q$	(composition)	$\mathcal{A} \mid \mathcal{B}$	(two things here)
$n[P]$	(composition)	$n[\mathcal{A}]$	(one thing here)
$(\nu n)P$	(restriction)	$n \circledR \mathcal{A}$	(hidden thing here)
$n\langle m \rangle$	(message)	$n\langle m \rangle$	(a message here)

Modal Logic Revisited

(Alex Simpson's Thesis)

(Id)

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

Finite graph $S = \{x_i \to y_i\}$

x enjoys $\mathcal{A}$

(Cut)

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

+ contraction

($\wedge$ L)

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

($\wedge$ R)

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

($\Rightarrow$ L)

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

($\Rightarrow$ R)

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

(F L)

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

(F R)

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

x reduces to y

($\diamond$ L) *y not in the conclusion*

$$\frac{\langle S, x \to y\rangle\ \Gamma, y : \mathcal{A} \vdash \Delta}{\langle S\rangle\ \Gamma, x : \diamond\mathcal{A} \vdash \Delta}$$

$\diamond\mathcal{A}$: someone I reduce to enjoys $\mathcal{A}$

($\diamond$ R)

$$\frac{\langle S\rangle\ \Gamma \vdash y : \mathcal{A}, \Delta \quad x \to_S y}{\langle S\rangle\ \Gamma \vdash x : \diamond\mathcal{A}, \Delta}$$

($\Box$ L)

$$\frac{\langle S\rangle\ \Gamma, y : \mathcal{A} \vdash \Delta \quad x \to_S y}{\langle S\rangle\ \Gamma, x : \Box\mathcal{A} \vdash \Delta}$$

$\Box\mathcal{A}$: everyone I reduce to enjoys $\mathcal{A}$

($\Box$ R) *y not in the conclusion*

$$\frac{\langle S, x \to y\rangle\ \Gamma \vdash y : \mathcal{A}, \Delta}{\langle S\rangle\ \Gamma \vdash x : \Box\mathcal{A}, \Delta}$$

x reduces to arbitrary y

Modal Variations

That is minimal modal logic.

Additional knowledge about the visibility relation (e.g. transitivity) can be added without modifying the rules for logical connectives.

Additional knowledge is embedded in "world" rules for S. E.g.:

Additional Visibility Structure:

(S → refl)

$$\frac{\langle S,\ x{\to}x\rangle\ \Gamma \vdash \Delta}{\langle S\rangle\ \Gamma \vdash \Delta}$$

If $\to$ is by assumption reflexive, we can discard a superfluous assumption that $x{\to}x$

(S → trans)

$$\frac{\langle S,\ x{\to}z\rangle\ \Gamma \vdash \Delta \quad x{\to_s}y \quad y{\to_s}z}{\langle S\rangle\ \Gamma \vdash \Delta}$$

If $\to$ is by assumption transitive, and can already derive in S that $x{\to}y$ and $y{\to}z$, then we can discard a superfluous assumption that $x{\to}z$

3 $\langle x{\to}x\rangle\ x : \mathcal{A} \vdash x : \mathcal{A}$ (Id)
2 $\langle x{\to}x\rangle\ x : \Box\mathcal{A} \vdash x : \mathcal{A}$ 3, ($\Box$ L)
1 $\langle\rangle\ x : \Box\mathcal{A} \vdash x : \mathcal{A}$ 2, (S → refl)

5 $\langle x{\to}y, y{\to}z, x{\to}z\rangle\ z : \mathcal{A} \vdash z : \mathcal{A}$ (Id)
4 $\langle x{\to}y, y{\to}z, x{\to}z\rangle\ x : \Box\mathcal{A} \vdash z : \mathcal{A}$ 5, ($\Box$ L)
3 $\langle x{\to}y, y{\to}z\rangle\ x : \Box\mathcal{A} \vdash z : \mathcal{A}$ 4, (S → trans)
2 $\langle x{\to}y\rangle\ x : \Box\mathcal{A} \vdash y : \Box\mathcal{A}$ 3, ($\Box$ R)
1 $\langle\rangle\ x : \Box\mathcal{A} \vdash x : \Box\Box\mathcal{A}$ 2, ($\Box$ R)

What's going on

Ex.: $\langle x \to y \rangle\, x : \Box\mathcal{A} \vdash y : \Box\mathcal{A}$

This is a bit strange because we embed a piece of the semantics (the worlds) into the sequents. However it is done abstractly ("x").

It is natural in the sense that sequents looks very much like a type/ND system: there are terms and their "types" $x : \mathcal{A}$.

Unlike a type sytem, the terms on the left of $\vdash$ are not just unrestricted variables. We need the $\langle S \rangle$ part to express constraints on how these terms relate to each other.

Within a single sequent, we can talk about properties of different worlds. This give us lots of freedom and orthogonality in proofs.

Despite the $x : \mathcal{A}$ look, we are not doing Curry-Howard. The terms do not encode proof trees: in standard modal logics, the terms are just variables with no structure. (But we will use structured terms.)

Basic Process Calculus

Intended Model

$P,Q \in \Pi ::=$ Processes

$\mathbf{0}$	void
$P \mid Q$	composition
$n\langle m\rangle$	output ($n,m \in \Lambda$)
$n(m).P$	input

$n\langle m\rangle \mid n(r).P \rightarrow P\{r \leftarrow m\}$

$P \rightarrow Q \Rightarrow P \mid R \rightarrow Q \mid R$

$P \equiv P' \wedge P' \rightarrow Q' \wedge Q' \equiv Q \Rightarrow P \rightarrow Q$

$P \mid \mathbf{0} \equiv P$

$P \mid Q \equiv Q \mid P$

$(P \mid Q) \mid R \equiv P \mid (Q \mid R)$

$P \equiv P$

$P \equiv Q \Rightarrow Q \equiv P$

$P \equiv R \wedge R \equiv Q \Rightarrow P \equiv Q$

$P \equiv Q \Rightarrow P \mid R \equiv Q \mid R$

$P \equiv Q \Rightarrow n(m).P \equiv n(m).Q$

Labeled transitions:

$P \rightarrow^{\tau} Q \triangleq P \rightarrow Q$

$P \rightarrow^{n\langle m\rangle} Q \triangleq P \equiv n\langle m\rangle \mid Q$

$P \rightarrow^{n(m)} Q \triangleq P \equiv n(p).P' \mid P'' \wedge Q \equiv P'\{p \leftarrow m\} \mid P''$

$x\langle y\rangle^* \triangleq x(y)$

$x(y)^* \triangleq x\langle y\rangle$

Inversion lemmas:

$P \mid Q \equiv \mathbf{0} \Rightarrow P \equiv \mathbf{0}$

$U \mid V \equiv T \mid S \Rightarrow \exists\, x,y,z,w$ s.t. $U \equiv x \mid y$, $V \equiv z \mid w$, $T \equiv x \mid z$, $S \equiv y \mid w$

$\mathbf{0} \rightarrow^{a} P$ never

$a \neq \tau \wedge U \mid V \rightarrow^{a} T \Rightarrow \exists\, x,y$ s.t.
$(T = x \mid V \wedge U \rightarrow^{a} x)$
$\vee\, (T = U \mid y \wedge V \rightarrow^{a} y)$

$U \rightarrow^{\tau} V \Rightarrow \exists\, x,y,x',y',a$ s.t.
$U = x \mid y \wedge x \rightarrow^{a} x'$
$\wedge\, y \rightarrow^{a^*} y' \wedge x' \mid y' = V$

Minimal Process Logic

$\mathcal{A}, \mathcal{B} \in \Phi ::=$	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
$a \gg \mathcal{A}$	after a	$\mathcal{A} \ll a$	before a
$\forall x.\mathcal{A}$	universal name quantifier		
$\forall X.\mathcal{A}$	propositional quantifier		
X	propositional variables		
$a ::=$	Actions $(a \in \mathcal{A}ct, x,y \in \mathcal{V})$		
τ	silent		
$x\langle y \rangle$	output		
$x(y)$	input		

$$\gg\mathcal{A} \triangleq \tau\gg\mathcal{A}$$

$$\mathcal{A}\ll \triangleq \mathcal{A}\ll\tau$$

Things one can say

Single-threaded (or void):

$\neg(\neg\mathbf{0} \mid \neg\mathbf{0})$ $\qquad$ $(\neg\mathcal{A} \triangleq \mathcal{A}\Rightarrow\mathbf{F})$

Somewhere $\mathcal{A}$ holds:

$\mathcal{A} \mid \mathbf{T}$ $\qquad$ $(\mathbf{T} \triangleq \neg\mathbf{F})$

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

$n\langle m\rangle$ $\qquad$ $(n\langle m\rangle \triangleq n\langle m\rangle\!\!\gg\!\!\mathbf{0})$

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

$n\langle m\rangle \triangleright \gg m\langle n\rangle$

Fixed input: inputs m on n and then satisfies $\mathcal{A}$:

$n(m)\!\!\gg\!\!\mathcal{A}$

Parametric input: inputs some x on n and then satisfies:

$n(x).\mathcal{A} \quad \triangleq \quad \forall x.\, n(x)\!\!\gg\!\!\mathcal{A}$

Satisfaction

Intended Model

$\mathbf{P} \triangleq \{S \subseteq \Pi \mid P \in S \wedge P \equiv Q \Rightarrow Q \in S\}$ the *properties*

$P \models_\sigma \mathbf{F}$	never	
$P \models_\sigma \mathcal{A} \wedge \mathcal{B}$	iff	$P \models_\sigma \mathcal{A} \wedge P \models_\sigma \mathcal{B}$
$P \models_\sigma \mathcal{A} \Rightarrow \mathcal{B}$	iff	$P \models_\sigma \mathcal{A} \Rightarrow P \models_\sigma \mathcal{B}$
$P \models_\sigma \mathbf{0}$	iff	$P \equiv 0$
$P \models_\sigma \mathcal{A} \mid \mathcal{B}$	iff	$\exists P', P'' \in \Pi.\ P \equiv P' \mid P'' \wedge P' \models_\sigma \mathcal{A} \wedge P'' \models_\sigma \mathcal{B}$
$P \models_\sigma \mathcal{A} \triangleright \mathcal{B}$	iff	$\forall Q \in \Pi.\ Q \models_\sigma \mathcal{A} \Rightarrow P \mid Q \models_\sigma \mathcal{B}$
$P \models_\sigma a \mathbin{\cdot\!\!>} \mathcal{A}$	iff	$\exists P' \in \Pi.\ P \rightarrow^{\sigma a} P' \wedge P' \models_\sigma \mathcal{A}$
$P \models_\sigma \mathcal{A} \mathbin{<\!\!\cdot} a$	iff	$\forall P' \in \Pi.\ P' \rightarrow^{\sigma a} P \Rightarrow P' \models_\sigma \mathcal{A}$
$P \models_\sigma \forall x.\mathcal{A}$	**iff**	$\forall n \in \Lambda.\ P \models_{\sigma\{x \leftarrow n\}} \mathcal{A}$
$P \models_\sigma \forall X.\mathcal{A}$	**iff**	$\forall S \in \mathbf{P}.\ P \models_{\sigma\{X \leftarrow S\}} \mathcal{A}$
$P \models_\sigma X$	**iff**	$P \in \sigma(X)$

Closed formulas denote properties:

$$\forall \mathcal{A} \in \Phi.\ \forall P, Q \in \Pi.\ \{P \mid P \models \mathcal{A}\} \in \mathbf{P}$$

N.B.: $\mathbf{P}$ is a commutative quantale and a boolean algebra.

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)

Indexes (denote processes, i.e. "worlds")

$$\langle \ldots u' \doteq v' \ldots u'' \rightarrow^{a} v'' \ldots \rangle \ldots u : \mathcal{A} \ldots \vdash \ldots v : \mathcal{B} \ldots$$

(Temporal) reduction constraints (denote process reduction)

Formulas (denote properties)

Indexes and Actions

$u ::=$	Index terms ($u,v \in \mathcal{I}$)	algebraic free vars:
X	process vars ($X \in \mathcal{X}$)	$afv(X) = \{X\}$
0	void	$afv(0) = \{\}$
$u \mid v$	composition	$afv(u \mid v) = afv(u) \cup afv(v)$

index interpretation $\quad \sigma \in \mathcal{X} \to \Pi \cup \mathcal{V} \to \Lambda$

Intended Model

$$I(X)_\sigma = X_\sigma$$
$$I(0)_\sigma = 0$$
$$I(u \mid v)_\sigma = I(u)_\sigma \mid I(v)_\sigma$$

$a ::=$	Actions	($a \in \mathcal{A}ct$, $x,y \in \mathcal{V}$)	
τ	silent	$\to \triangleq \to^\tau$	
$x\langle y\rangle$	output	$x\langle y\rangle^* \triangleq x(y)$	
$x(y)$	input	$x(y)^* \triangleq x\langle y\rangle$	(τ^* undefined)

Constraints

$S = \{u_i \doteq v_i,\ u_j \rightarrow^{a} v_j\}$

constraint closure (computing the *consequences* of S)

$u \doteqdot_s v$ means $u \doteq v$ is derivable from S

$u \rightarrow^{a}_{s} v$ means $u \rightarrow^{a} v$ is derivable from S

$u \doteq v \in S \Rightarrow u \doteqdot_s v$

$u \rightarrow^{a} v \in S \Rightarrow u \rightarrow^{a}_{s} v$

$u \rightarrow^{a}_{s} u' \wedge v \rightarrow^{a^*}_{s} v' \Rightarrow u|v \rightarrow_s u'|v'$

$u \rightarrow^{a}_{s} v \Rightarrow t|u \rightarrow^{a}_{s} t|v$

$u \doteqdot_s u' \wedge u' \rightarrow^{a}_{s} v' \wedge v' \doteqdot_s v \Rightarrow u \rightarrow^{a}_{s} v$

$u \mid 0 \doteqdot_s u$

$u \mid v \doteqdot_s v \mid u$

$(u \mid v) \mid t \doteqdot_s u \mid (v \mid t)$

$u \doteqdot_s u$

$u \doteqdot_s v \Rightarrow v \doteqdot_s u$

$u \doteqdot_s t \wedge t \doteqdot_s v \Rightarrow u \doteqdot_s v$

$u \doteqdot_s v \Rightarrow u \mid t \doteqdot_s v \mid t$

constraint interpretation

$\sigma \in \mathcal{X} \rightarrow \Pi \cup \mathcal{V} \rightarrow \Lambda$

$I(u \doteq v)_\sigma = I(u)_\sigma \equiv I(v)_\sigma$

$I(u \rightarrow^{a} v)_\sigma = I(u)_\sigma \rightarrow^{\sigma a} I(v)_\sigma$

Intended Model

Rules

General pattern:

- *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.
  Going up: add deducible constraints.
  Going down: remove redundant constaints.
  Commute easily with cuts.

Propositional Connectives

Identity, Cut, and Contraction:

(Id)

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

(Cut)

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

(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)

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

Propositional Connectives:

($\wedge$ L)

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

($\wedge$ R)

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

($\Rightarrow$ L)

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

($\Rightarrow$ 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 Connectives

Composition:

(0 L)

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

(0 R)

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

(| 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)

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

Guarantee:

(▷ L)

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

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

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

i.e.:

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

Additional World Structure:

(S | 0)

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

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

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

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

Suppose $u|v=t|s \Rightarrow \exists\ x,y,z,w$ s.t. $u=x|y$, $v=z|w$, $t=x|z$, $s=y|w$. Then, if we can already deduce that $u|v \doteq_S t|w$, we can eliminate a redundant assumptions

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

6.2 $\langle S,\ u \doteq X \mid Y,\ u \doteq \mathbf{0},\ X \doteq \mathbf{0} \rangle\ \Gamma,\ X : \mathcal{A},\ Y : \mathcal{B} \vdash u : \mathcal{A},\ \Delta$	(Id) since $u = X$
5.2 $\langle S,\ u \doteq X \mid Y,\ u \doteq \mathbf{0} \rangle\ \Gamma,\ X : \mathcal{A},\ Y : \mathcal{B} \vdash u : \mathcal{A},\ \Delta$	6.2, (S | **0**) since $X \mid Y \doteq \mathbf{0}$
4.2 $\langle S,\ u \doteq X \mid Y \rangle\ \Gamma,\ X : \mathcal{A},\ Y : \mathcal{B},\ u : \mathbf{0} \vdash u : \mathcal{A},\ \Delta$	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 Connectives

(a» L) *X not free in the conclusion*

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

(a» R)

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

(«a L)

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

(«a R) *X not free in the conclusion*

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

Additional World Structure:

(S 0 →ᵃ)

$$\frac{0 \to^a_s u}{\langle S \rangle\ \Gamma \vdash \Delta}$$

0 has no action

(S | →^≠τ) *a≠τ, X,Y not free in the conclusion*

$$\frac{\langle S,\ t \doteq X|v,\ u \to^a X \rangle\ \Gamma \vdash \Delta \quad \langle S,\ t \doteq u|Y,\ v \to^a Y \rangle\ \Gamma \vdash \Delta}{u|v \to^a_s t}$$

$$\frac{}{\langle S \rangle\ \Gamma \vdash \Delta}$$

$a \neq \tau,\ u|v \to^a t \Rightarrow \exists\ x,y$ s.t.
$(t = x|v \wedge u \to^a x) \vee (t = u|y \wedge v \to^a y)$

(S →^τ) *X,Y, X₀,Y₀, x,y not free in the conclusion*

$$\frac{\langle S,\ u \doteq X|Y,\ X \to^{x(y)} X_0,\ Y \to^{x(y)} Y_0,\ X_0|Y_0 \doteq v \rangle\ \Gamma \vdash \Delta}{u \to^\tau_s v}$$

$$\frac{}{\langle S \rangle\ \Gamma \vdash \Delta}$$

$u \to^\tau v \Rightarrow \exists\ x,y,x',y',a$ s.t.
$u = x|y \wedge x \to^a x' \wedge y \to^{a^*} y' \wedge x'|y' = v$

Derivable

(S | →)' *X,Y, x,y not free in the conclusion*

$$\frac{\langle S,\ t \doteq X|v,\ u \to X\rangle\ \Gamma \vdash \Delta \quad \langle S,\ t \doteq u|Y,\ v \to Y\rangle\ \Gamma \vdash \Delta \quad \langle S,\ t \doteq X|Y,\ u \to^{x(y)} X,\ v \to^{x(y)} Y\rangle\ \Gamma \vdash \Delta \quad u|v \to_s t}{\langle S\rangle\ \Gamma \vdash \Delta}$$

$u|v \to t \Rightarrow \exists\ x,y.a$ s.t.
$(t = x|v \wedge u \to x) \vee (t = u|y \wedge v \to y) \vee$
$(t = x|y \wedge u \to^a x \wedge v \to^{a^*} y)$.

Quantification

(∀ L)

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

(∀ R) *y not free in the conclusion*

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

(∀2 L)

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

(∀2 R) *Y not free in the conclusion*

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

A use for (S →ʔ)

$\mathbf{»0} \vdash \exists x,y.\ x\langle y\rangle\mathbf{»0} \mid x(y)\mathbf{»0}$

$\mathbf{8.2}\ \langle S,\ u\to Z,\ Z\doteq\mathbf{0},\ u\doteq X\mid Y,\ X\to^{x(y)}X_0,\ Y\to^{x(y)}Y_0,\ X_0\mid Y_0\doteq Z,\ Y_0\doteq\mathbf{0}\rangle\ \Gamma\vdash Y_0:\mathbf{0},\Delta$ (0 R)

$\mathbf{7.2}\ \langle S,\ u\to Z,\ Z\doteq\mathbf{0},\ u\doteq X\mid Y,\ X\to^{x(y)}X_0,\ Y\to^{x(y)}Y_0,\ X_0\mid Y_0\doteq Z\rangle\ \Gamma\vdash Y_0:\mathbf{0},\Delta$ (S | 0)

$\mathbf{6.2}\ \langle S,\ u\to Z,\ Z\doteq\mathbf{0},\ u\doteq X\mid Y,\ X\to^{x(y)}X_0,\ Y\to^{x(y)}Y_0,\ X_0\mid Y_0\doteq Z\rangle\ \Gamma\vdash Y:x(y)\mathbf{»0},\Delta$ (*a*» R)

$\mathbf{8.1}\ \langle S,\ u\to Z,\ Z\doteq\mathbf{0},\ u\doteq X\mid Y,\ X\to^{x(y)}X_0,\ Y\to^{x(y)}Y_0,\ X_0\mid Y_0\doteq Z,\ X_0\doteq\mathbf{0}\rangle\ \Gamma\vdash X_0:\mathbf{0},\Delta$ (0 R)

$\mathbf{7.1}\ \langle S,\ u\to Z,\ Z\doteq\mathbf{0},\ u\doteq X\mid Y,\ X\to^{x(y)}X_0,\ Y\to^{x(y)}Y_0,\ X_0\mid Y_0\doteq Z\rangle\ \Gamma\vdash X_0:\mathbf{0},\Delta$ (S | 0)

$\mathbf{6.1}\ \langle S,\ u\to Z,\ Z\doteq\mathbf{0},\ u\doteq X\mid Y,\ X\to^{x(y)}X_0,\ Y\to^{x(y)}Y_0,\ X_0\mid Y_0\doteq Z\rangle\ \Gamma\vdash X:x\langle y\rangle\mathbf{»0},\Delta$ (*a*» R)

$\mathbf{5}\ \langle S,\ u\to Z,\ Z\doteq\mathbf{0},\ u\doteq X\mid Y,\ X\to^{x(y)}X_0,\ Y\to^{x(y)}Y_0,\ X_0\mid Y_0\doteq Z\rangle\ \Gamma\vdash u:x\langle y\rangle\mathbf{»0}\mid x(y)\mathbf{»0},\Delta$ (| R)

$\mathbf{4}\ \langle S,\ u\to Z,\ Z\doteq\mathbf{0},\ u\doteq X\mid Y,\ X\to^{x(y)}X_0,\ Y\to^{x(y)}Y_0,\ X_0\mid Y_0\doteq Z\rangle$
$\Gamma\vdash u:\exists x,y.\ x\langle y\rangle\mathbf{»0}\mid x(y)\mathbf{»0},\Delta$ (∃ R)

$\mathbf{3}\ \langle S,\ u\to Z,\ Z\doteq\mathbf{0}\rangle\ \Gamma\vdash u:\exists x,y.\ x\langle y\rangle\mathbf{»}\mathcal{A}\mid x(y)\mathbf{»}\mathcal{B},\Delta$ (S →ʔ)

$\mathbf{2}\ \langle S,\ u\to Z\rangle\ \Gamma,\ Z:\mathbf{0}\vdash u:\exists x,y.\ x\langle y\rangle\mathbf{»}\mathcal{A}\mid x(y)\mathbf{»}\mathcal{B},\Delta$ (0 L)

$\mathbf{1}\ \langle S\rangle\ \Gamma,\ u:\mathbf{»0}\vdash u:\exists x,y.\ x\langle y\rangle\mathbf{»0}\mid x(y)\mathbf{»0},\Delta$ (*a*» L)

Notation for Output Formulas

$x\langle y\rangle \quad \triangleq \quad x\langle y\rangle\text{»}\mathbf{0}$

$u \doteq x\langle y\rangle \quad \triangleq \quad u \rightarrow^{x\langle y\rangle} 0$

($x\langle y\rangle$ L)

$$\frac{\langle S,\ u \doteq x\langle y\rangle\rangle\ \Gamma \vdash \Delta}{\langle S\rangle\ \Gamma,\ u : x\langle y\rangle \vdash \Delta}$$

($x\langle y\rangle$ R)

$$\frac{u \doteq_s x\langle y\rangle}{\langle S\rangle\ \Gamma \vdash u : x\langle y\rangle,\ \Delta}$$

$\langle S,\ u \rightarrow^{x\langle y\rangle} 0\rangle\ \Gamma \vdash \Delta$ (Hyp)

$\langle S,\ u \rightarrow^{x\langle y\rangle} 0,\ u \rightarrow^{x\langle y\rangle} \mathcal{X},\ \mathcal{X} \doteq 0\rangle\ \Gamma \vdash \Delta$ (W)

$\langle S,\ u \rightarrow^{x\langle y\rangle} \mathcal{X},\ \mathcal{X} \doteq 0\rangle\ \Gamma \vdash \Delta$ (CS)

$\langle S,\ u \rightarrow^{x\langle y\rangle} \mathcal{X}\rangle\ \Gamma,\ \mathcal{X} : \mathbf{0} \vdash \Delta$ (0 L)

$\langle S\rangle\ \Gamma,\ u : n\langle m\rangle\text{»}\mathbf{0} \vdash \Delta$ (a» L)

$\langle S\rangle\ \Gamma \vdash 0 : \mathbf{0},\ \Delta$ (0 R)

$u \rightarrow^{x\langle y\rangle}_s 0$ (Hyp)

$\langle S\rangle\ \Gamma \vdash u : x\langle y\rangle\text{»}\mathbf{0},\ \Delta$ (a» R)

(S 0 $x\langle y\rangle$)

$$\frac{0 \doteq_s x\langle y\rangle}{\langle S\rangle\ \Gamma \vdash \Delta}$$

$0 \to^{n\langle m\rangle}_s 0$ (Hyp)

$\langle S\rangle\ \Gamma \vdash \Delta$ (S $0 \to^a$)

(S | $x\langle y\rangle$)

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

$\langle S,\ u \doteq 0,\ v \to^{x\langle y\rangle} 0\rangle\ \Gamma \vdash \Delta$ (Hyp)

$\langle S,\ u \doteq 0,\ v \to^{x\langle y\rangle} 0,\ 0 \doteq u|\mathcal{Y},\ v \to^{x\langle y\rangle} \mathcal{Y},\ \mathcal{Y} \doteq 0\rangle\ \Gamma \vdash \Delta$ (W) $\mathcal{Y}$ fresh

$\langle S,\ 0 \doteq u|\mathcal{Y},\ v \to^{x\langle y\rangle} \mathcal{Y},\ \mathcal{Y} \doteq 0\rangle\ \Gamma \vdash \Delta$ (CS)

$\langle S,\ 0 \doteq u|\mathcal{Y},\ v \to^{x\langle y\rangle} \mathcal{Y}\rangle\ \Gamma \vdash \Delta$ (S | 0)

$\langle S,\ v \doteq 0,\ u \to^{x\langle y\rangle} 0\rangle\ \Gamma \vdash \Delta$ (Hyp)

$\langle S,\ 0 \doteq \mathcal{X}|v,\ u \to^{x\langle y\rangle} \mathcal{X}\rangle\ \Gamma \vdash \Delta$ Similarly, $\mathcal{X}$ fresh

$u|v \to^{x\langle y\rangle} 0$ (Hyp)

$\langle S\rangle\ \Gamma \vdash \Delta$ (S $| \to^{\neq ?}$)

Notation for Input Formulas

$x(y).\mathcal{A} \triangleq \forall y.x(y)\text{»}\mathcal{A}$

$x\langle z\rangle \mid x(y).\mathcal{A} \vdash \text{»}\mathcal{A}\{y\leftarrow z\}$

$\langle S\rangle\ \Gamma, u : x\langle z\rangle \mid x(y).\mathcal{A} \vdash u : \text{»}\mathcal{A}\{y\leftarrow z\}, \Delta$

6 $\langle S, u \doteq X \mid Y,\ X \rightarrow^{x\langle z\rangle} X',\ Y \rightarrow^{x(z)} Y',\ X' \doteq 0\rangle\ \Gamma, Y' : \mathcal{A}\{y\leftarrow z\} \vdash X' \mid Y' : \mathcal{A}\{y\leftarrow z\}, \Delta$ (Id)

5 $\langle S, u \doteq X \mid Y,\ X \rightarrow^{x\langle z\rangle} X',\ Y \rightarrow^{x(z)} Y'\rangle\ \Gamma, X' : \mathbf{0}, Y' : \mathcal{A}\{y\leftarrow z\} \vdash X' \mid Y' : \mathcal{A}\{y\leftarrow z\}, \Delta$ (0 L)
$u \rightarrow_S X' \mid Y'$

4 $\langle S, u \doteq X \mid Y,\ X \rightarrow^{x\langle z\rangle} X',\ Y \rightarrow^{x(z)} Y'\rangle\ \Gamma, X' : \mathbf{0}, Y' : \mathcal{A}\{y\leftarrow z\} \vdash u : \text{»}\mathcal{A}\{y\leftarrow z\}, \Delta$ (*a*» R)

3 $\langle S, u \doteq X \mid Y\rangle\ \Gamma, X : x\langle z\rangle\text{»}\mathbf{0}, Y : x(z)\text{»}\mathcal{A}\{y\leftarrow z\} \vdash u : \text{»}\mathcal{A}\{y\leftarrow z\}, \Delta$ (*a*» L) (*a*» L)

2 $\langle S, u \doteq X \mid Y\rangle\ \Gamma, X : x\langle z\rangle\text{»}\mathbf{0}, Y : \forall y.x(y)\text{»}\mathcal{A} \vdash u : \text{»}\mathcal{A}\{y\leftarrow z\}, \Delta$ (∀ L)

1 $\langle S\rangle\ \Gamma, u : x\langle z\rangle\text{»}\mathbf{0} \mid \forall y.x(y)\text{»}\mathcal{A} \vdash u : \text{»}\mathcal{A}\{y\leftarrow z\}, \Delta$ (| L)

Exercise: n-Threaded

(Silvano Dal-Zilio)

At-most-one-thread: $\leq 1t \triangleq \neg(\neg 0 \mid \neg 0)$

not decomposible in two parts that are both non-void.

At-most-two-threads: $\leq 2t \triangleq \leq 1t \mid \leq 1t$

At-least-three-threads: $\geq 3t \triangleq \neg 0 \mid \neg 0 \mid \neg 0$

Prove 2 < 3: at-most-two-threads implies not at-list-three-threads.

$$\leq 2t \vdash \neg \geq 3t$$

i.e. show for any u:

$$\langle\rangle\, u : \neg(\neg 0 \mid \neg 0) \mid \neg(\neg 0 \mid \neg 0) \vdash u : \neg(\neg 0 \mid \neg 0 \mid \neg 0)$$

Recursion

Least and greatest fixpoint formulas are definable from second-order quantification (omitted):

$\mu X.\, \mathcal{A} \quad \nu X.\, \mathcal{A}$

Hence, we have a power similar to modal μ-calculus. E.g., standard temporal modalities are definable:

$\Diamond \mathcal{A} \triangleq \mu X.\, \mathcal{A} \vee \raisebox{0.15ex}{»} X$

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

Ex: Immovable Object vs. Irresistible Force

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

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

$Im \mid Ir \vdash (\mathbf{T} \triangleright \Box(obj\langle\rangle \mid \mathbf{T})) \mid \mathbf{T}$	$\mathcal{A} \vdash \mathbf{T}$
$\vdash \Box(obj\langle\rangle \mid \mathbf{T})$	$(\mathcal{A} \triangleright \mathcal{B}) \mid \mathcal{A} \vdash \mathcal{B}$
$\vdash \Diamond\Box(obj\langle\rangle \mid \mathbf{T})$	$\mathcal{A} \vdash \Diamond\mathcal{A}$
$Im \mid Ir \vdash \mathbf{T} \mid (\mathbf{T} \triangleright \Box\Diamond\neg(obj\langle\rangle \mid \mathbf{T}))$	$\mathcal{A} \vdash \mathbf{T}$
$\vdash \Box\Diamond\neg(obj\langle\rangle \mid \mathbf{T})$	$\Diamond\neg\mathcal{A} \vdash \neg\Box\mathcal{A}$
$\vdash \neg\Diamond\Box(obj\langle\rangle \mid \mathbf{T})$	$\Box\neg\mathcal{A} \vdash \neg\Diamond\mathcal{A}$
Hence: $Im \mid Ir \vdash \mathbf{F}$	$\mathcal{A} \wedge \neg\mathcal{A} \vdash \mathbf{F}$

Conclusions: Scaling Up

We do this kind of thing for a whole asynchronous π-calculus.

This gets considerably more complex, but allows us to the write one-line specifications of spatial properties such as:

> The protocol ensures that there is a private name shared between two distinct parts of the system, and nowhere else.

Adding locations (e.g. switching to ambient calculus) is quite easy.

The general methodology seems very flexible.