On symbolic semantics for name-decorated contexts

(extended abstract)

Andrea Bracciali Roberto Bruni Alberto Lluch Lafuente

Dipartimento di Informatica

Università di Pisa

{bruni,braccia,lafuente}@di.unipi.it

Contexts

Open systems: systems that are not fully specified at some point in time.

- components, processes, services
- autonomous, distributed, cross-domain
- dynamically reconfiguring

computation + interaction + dynamics

synchronisation may happen with “unkown” partners

Symbolic semantics

(Tractable) Abstractions of unknown/infinite behaviours.

Example:

the infinitely many messages an intruder can use to attack a security protocol.

$\ldots?\mathtt{X}\ldots.$	any (free to choose later on)
$\ldots?\{\mathtt{X}\}_{\mathtt{k}}\ldots$	a message encrypted either with $\mathtt{k}$ or with a different one

a kind of lazy/late evaluation/instantiation !

[Humia, Amadio, Boreale, ... early 00s]

Some (symbolic) approaches to open systems

1. bisimulation up to contexts, i.e. “determine the most general context [amongst the infinite ones] in which two process are bisimilar” [Larsen, et alt. 90s];
2. from rewrite rules to bisimulation congruence, i.e. “extract the minimal context in which a reduction can happen as a precondition for SOS congruent transitions” [Sewell, Leifer-Milner, Sassone, Sobocinski, ...from late 90s];
3. minimal boolean conditions for value-passing semantics [Hennessy-Lin 95]
4. minimal (behavioural) requirements over (parallel) context for a transition to occur [Rensink 00],
5. saturated semantics [Bonchi-Montanari 06]
6. ... and others !

BBB approach

Define a semantics for open systems, i.e. contexts:

$$C[X]$$

BBB approach

Define a semantics for open systems, i.e. contexts:

$$C[X] = a.0|X$$

A term with X a process varialble representing *any* ground process p (or even open context $D[Z]$).

BBB approach

Define a semantics for open systems, i.e. contexts:

$$C[X] = a.0|X \xrightarrow{X}_a 0|X$$

However, X either does nothing...

BBB approach

Define a semantics for open systems, i.e. contexts:

$$C[X] = a.0|X \xrightarrow{\diamond aY}_a a.0|Y$$

... or it evolves alone ...

BBB approach

Define a semantics for open systems, i.e. contexts:

$$C[X] = a.0|X \xrightarrow{\diamond \bar{a} Y}_a Y$$

... or is able to synch.
as prescribed by the semantical rules (finite)!

BBB approach

Symbolic transition system:

$$C[X] \xrightarrow{\phi}_a D[Y]$$

1. abstracting from components not playing an active role in the transition;
2. specifying the active components as little as possible;
3. making assumptions both on the *structure* and on the *behaviour* of the active components (Spatial logics, [Cardelli, Gordon]).

BBB approach

Symbolic transition system:

$$C[X] \xrightarrow{\phi}_a D[Y]$$

The logic expresses the (minimal) capabilities required to plugged-in components so as to fire the next transition:

$$\phi \ ::= \ \ldots \mid \ \diamond a.\phi' \mid \ldots \mid f(\phi') \mid X$$

BBB approach

Symbolic transition system:

$$C[X] \overset{\phi}{\rightarrow}_a D[Y]$$

The logic expresses the (minimal) capabilities required to plugged-in components so as to fire the next transition:

$$\phi \ ::= \ \ldots \mid \ \diamond\, a.\phi' \mid \ldots \mid f(\phi') \mid X$$

and a satisfiability (with residuals) notion for ground processes, e.g.:

$$p \models \diamond a\phi' \text{ iff } \exists q.\ p \rightarrow_a \ q \wedge q \models \phi'$$

BBB approach

A notion of correspondence
(soundness and completeness) - informally:

$$C[X] \stackrel{\phi}{\longrightarrow}_a D[Y]$$

$$\Uparrow$$

$$\forall p \models \phi[q/Y]$$

$$\Downarrow$$

$$C[p] \rightarrow_a D[q]$$

BBB approach

A constructive procedure based on unification:
Unify:

$$\frac{P \rightarrow_a P' \quad Q \rightarrow_{\bar{a}} Q'}{P|Q \rightarrow_\tau P'|Q'}$$

with

$$a.0|X$$

i.e.

$$a.0|X \xrightarrow{\diamond \bar{a} Y}_\tau Y$$

A reference *sound* and *complete* STS.

BBB approach

Natural definition of *strict symbolic bisimulation*:

$$\begin{array}{ccc} C[X] & \stackrel{\phi}{\longrightarrow}_a & C'[Y] \\ \sim_{\mathrm{s}} & & \sim_{\mathrm{s}} \\ D[X] & \stackrel{\phi}{\longrightarrow}_a & D'[Y] \end{array}$$

same (syntactic equality) formula!

BBB approach

Natural definition of *strict symbolic bisimulation*:

$$\begin{array}{ccc} C[X] & \stackrel{\phi}{\longrightarrow}_a & C'[Y] \\ \sim_{\mathrm{s}} & & \sim_{\mathrm{s}} \\ D[X] & \stackrel{\phi}{\longrightarrow}_a & D'[Y] \end{array}$$

same (syntactic equality) formula!

Relaxation: *loose symbolic bisimulation*

$$\begin{array}{ccc} C[X] & \stackrel{\phi}{\longrightarrow}_a & C'[Y] \\ \dot{\sim}_{\mathrm{l}} & & \dot{\sim}_{\mathrm{l}} \\ D[X] & \stackrel{\psi}{\longrightarrow}_a & D'[Z] \text{ and } D'[\psi'] \end{array}$$

and $\exists\ \psi'$ spatial such that $\phi = \psi; \psi'$

BBB approach

$$C[X] \stackrel{\phi_1;\cdots;\phi_h}{\Longrightarrow}_{\ell} D[Y] \text{ if } C[X] \xrightarrow{\phi_1}_{\tau} \cdots \xrightarrow{\phi_{k-1}}_{\tau} \xrightarrow{\phi_k}_{\ell} \xrightarrow{\phi_{k+1}}_{\tau} \cdots \xrightarrow{\phi_h}_{\tau} D[Y]$$

BBB approach

$C[X] \stackrel{\phi_1;\cdots;\phi_h}{\Longrightarrow}_\ell D[Y]$ if $C[X] \xrightarrow{\phi_1}_\tau \cdots \xrightarrow{\phi_{k-1}}_\tau \xrightarrow{\phi_k}_\ell \xrightarrow{\phi_{k+1}}_\tau \cdots \xrightarrow{\phi_h}_\tau D[Y]$

strict weak symbolic bisimulation (symmetric!): $\approx_{\mathrm{s}}$

$$\begin{array}{ccc} C[X] & \stackrel{\phi}{\longrightarrow}_\ell & C'[Y] \\ \approx_{\mathrm{s}} & & \approx_{\mathrm{s}} \\ D[X] & \stackrel{\phi}{\Longrightarrow}_\ell & D'[Y] \end{array}$$

loose weak symbolic bisimulation (symmetric!): $\approx_{\mathrm{l}}$

$$\begin{array}{ccc} C[X] & \stackrel{\phi}{\longrightarrow}_\ell & C'[Y] \\ \approx_{\mathrm{l}} & & \approx_{\mathrm{l}} \\ D[X] & \stackrel{\psi}{\Longrightarrow}_\ell & D'[Y] \text{ and } D'[\psi'] \end{array}$$

and $\exists\ \psi'$ spatial such that $\phi = \psi;\psi'$

BBB approach

All the symbolic bisimilarities imply (are correct approximations of) universal bisimilarity:

$$\left.\begin{array}{l} \sim_{\mathrm{s}} \Rightarrow \dot{\sim}_{\mathrm{l}} \\ \sim_{\mathrm{s}} \Rightarrow \approx_{\mathrm{s}} \\ \dot{\sim}_{\mathrm{l}} \Rightarrow \approx_{\mathrm{l}} \end{array}\right\} \Rightarrow \sim_{\mathrm{u}} (\approx_{\mathrm{u}}) \qquad \forall p\ C[p] \sim D[p]$$

BBB approach

All the symbolic bisimilarities imply (are correct approximations of) universal bisimilarity:

$$\left.\begin{array}{l} \sim_{\mathrm{s}} \Rightarrow \dot{\sim}_{\mathrm{l}} \\ \sim_{\mathrm{s}} \Rightarrow \approx_{\mathrm{s}} \\ \dot{\sim}_{\mathrm{l}} \Rightarrow \approx_{\mathrm{l}} \end{array}\right\} \Rightarrow \sim_{\mathrm{u}} (\approx_{\mathrm{u}}) \qquad \forall p\ C[p] \sim D[p]$$

Instantiation time matters !

$$C[X] = a.0 + a.b.0 + a.one_b(X) \qquad D[X] = a.0 + a.b.0 + a.stop(X).$$

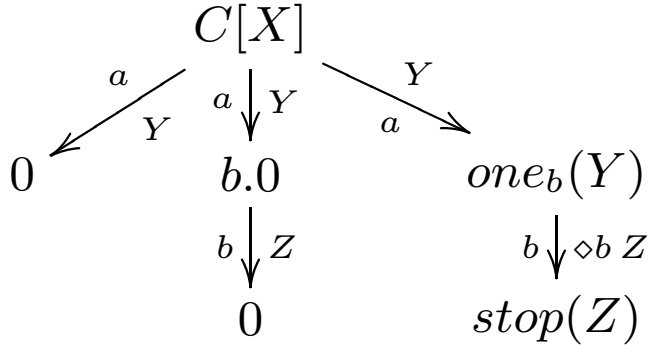
BBB approach

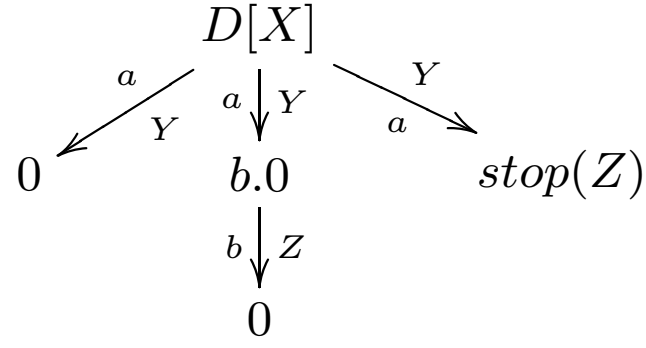
All the symbolic bisimilarities imply (are correct approximations of) universal bisimilarity:

$$\left.\begin{array}{l} \sim_{\mathrm{s}} \Rightarrow \dot{\sim}_{\mathrm{l}} \\ \sim_{\mathrm{s}} \Rightarrow \approx_{\mathrm{s}} \\ \dot{\sim}_{\mathrm{l}} \Rightarrow \approx_{\mathrm{l}} \end{array}\right\} \Rightarrow \sim_{\mathrm{u}} (\approx_{\mathrm{u}}) \qquad \forall p\, C[p] \sim D[p]$$

Instantiation time matters !

$$C[X] = a.0 + a.b.0 + a.one_b(X) \qquad D[X] = a.0 + a.b.0 + a.stop(X).$$





Towards Names ...

Full name discipline in open processes is difficult.
E.g.

$$(\nu a)(a|X)$$

Is the a of any X the a of the restriction? (design choice)
Does α conversion commute with instantiation? (semantic choice)

...

Scenario: Web Crawlers

A simplistic proof-of-concept scenario.

$$s \quad ::= \quad \mathbf{0} \quad | \quad c \quad | \quad \mathsf{link}(x, y) \quad | \quad s|s$$

$$c \quad ::= \quad \mathsf{rash}(a, x, \tilde{y}) \quad | \quad \mathsf{cautious}(a, x, \tilde{y}) \quad | \quad \mathsf{scrupulous}(a, x, \tilde{y})$$

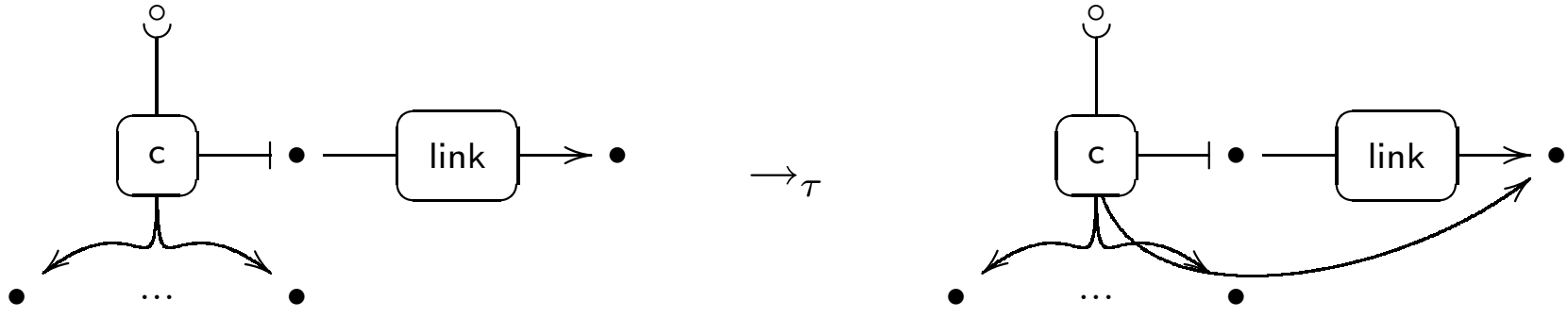
Scenario: Web Crawlers

A simplistic proof-of-concept scenario.

$$s \;::=\; \mathbf{0} \;\mid\; c \;\mid\; \mathsf{link}(x,y) \;\mid\; s|s$$

$$c \;::=\; \mathsf{rash}(a,x,\tilde{y}) \;\mid\; \mathsf{cautious}(a,x,\tilde{y}) \;\mid\; \mathsf{scrupulous}(a,x,\tilde{y})$$

$$\mathsf{c}(a,x,\tilde{y}) \;\mid\; \mathsf{link}(x,z) \;\mid\; s \;\longrightarrow_\tau\; \mathsf{c}(a,x,\tilde{y}+z) \;\mid\; \mathsf{link}(x,z) \;\mid\; s$$

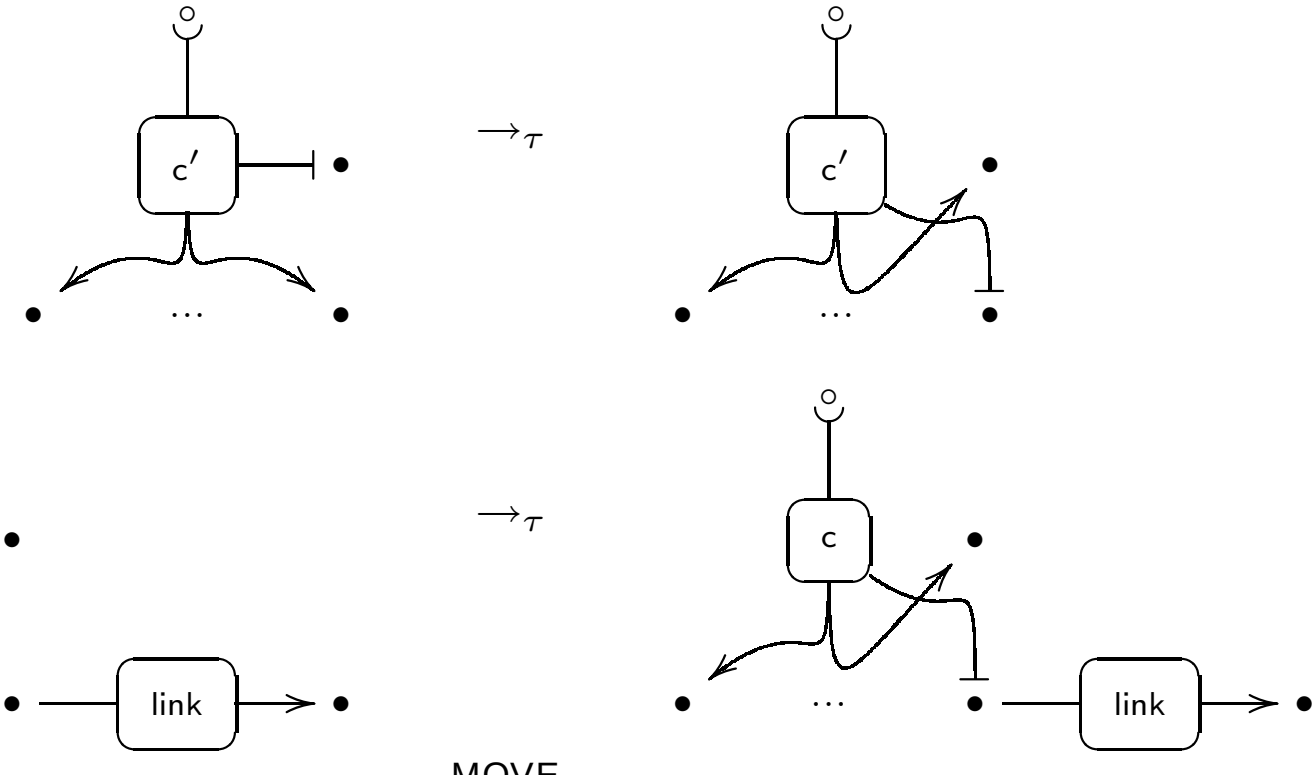


LEARN

Scenario: Web Crawlers

$$\mathsf{rash}(a, x, \tilde{y} + z) \mid s \quad \rightarrow_\tau \quad \mathsf{rash}(a, z, \tilde{y} + x) \mid s$$

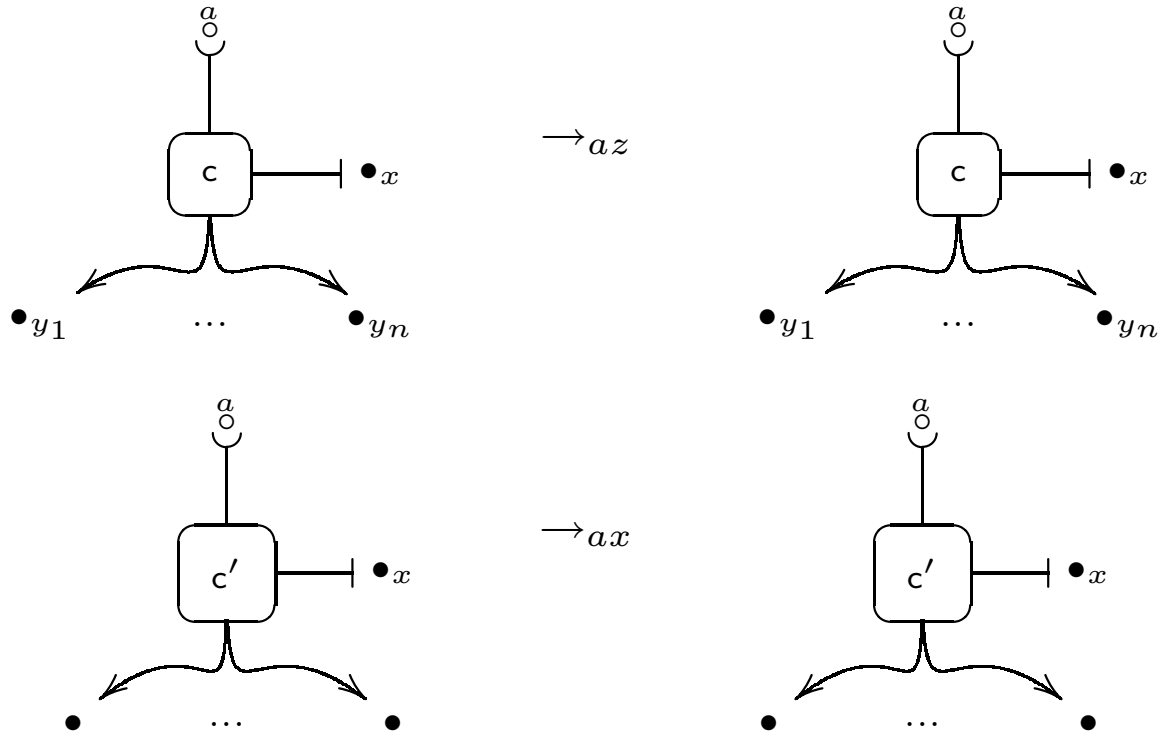
$$\mathsf{c}(a, x, \tilde{y} + z) \mid \mathsf{link}(z, w) \mid s \quad \rightarrow_\tau \quad \mathsf{c}(a, z, \tilde{y} + x) \mid \mathsf{link}(z, w) \mid s$$



Scenario: Web Crawlers

$\mathsf{c}(a, x, \tilde{y}) \mid s \quad \rightarrow_{az} \quad \mathsf{c}(a, x, \tilde{y}) \mid s$ with $z \in \tilde{y} + x$

$\mathsf{scrupulous}(a, x, \tilde{y}) \mid s \quad \rightarrow_{ax} \quad \mathsf{scrupulous}(a, x, \tilde{y}) \mid s$



OBSERVE

Scenario: Web Crawlers

$$\mathsf{R}[X] \stackrel{\text{def}}{=} \mathsf{rash}(a, x, \tilde{y}) \mid X$$

$$\mathsf{K}[X] \stackrel{\text{def}}{=} \mathsf{cautious}(a, x, \tilde{y}) \mid X$$

$$\mathsf{S}[X] \stackrel{\text{def}}{=} \mathsf{scrupulous}(a, x, \tilde{y}) \mid X$$

$\mathsf{R}[X]$	$\xrightarrow{\mathsf{link}(x,z)\mid Y}_{\tau}$	$\mathsf{rash}(a, x, \tilde{y} + z) \mid \mathsf{link}(x, z) \mid Y$	(for any z)
$\mathsf{R}[X]$	$\xrightarrow{Y}_{\tau}$	$\mathsf{rash}(a, y_i, \tilde{y} + x - y_i) \mid Y$	
$\mathsf{R}[X]$	$\xrightarrow{Y}_{ax}$	$\mathsf{R}[Y]$	
$\mathsf{R}[X]$	$\xrightarrow{Y}_{ay_i}$	$\mathsf{R}[Y]$	
$\mathsf{K}[X]$	$\xrightarrow{\mathsf{link}(x,z)\mid Y}_{\tau}$	$\mathsf{cautious}(a, x, \tilde{y} + z) \mid \mathsf{link}(x, z) \mid Y$	(for any z)
$\mathsf{K}[X]$	$\xrightarrow{\mathsf{link}(y_i,z)\mid Y}_{\tau}$	$\mathsf{cautious}(a, y_i, \tilde{y} + x - y_i) \mid \mathsf{link}(y_i, z) \mid Y$	(for any z)
$\mathsf{K}[X]$	$\xrightarrow{Y}_{ax}$	$\mathsf{K}[Y]$	
$\mathsf{K}[X]$	$\xrightarrow{Y}_{ay_i}$	$\mathsf{K}[Y]$	
$\mathsf{S}[X]$	$\xrightarrow{\mathsf{link}(x,z)\mid Y}_{\tau}$	$\mathsf{scrupulous}(a, x, \tilde{y} + z) \mid \mathsf{link}(x, z) \mid Y$	(for any z)
$\mathsf{S}[X]$	$\xrightarrow{\mathsf{link}(y_i,z)\mid Y}_{\tau}$	$\mathsf{scrupulous}(a, y_i, \tilde{y} + x - y_i) \mid \mathsf{link}(y_i, z) \mid Y$	(for any z)
$\mathsf{S}[X]$	$\xrightarrow{Y}_{ax}$	$\mathsf{S}[Y]$	

Scenario: Web Crawlers

Universally:

$$\mathsf{rash}(a, x, \tilde{y})|s \approx_{\mathrm{u}} \mathsf{cautious}(a, x, \tilde{y})|s$$

(they communicate all the addresses they gather – valid or not)

$$\mathsf{rash}(a, x, \emptyset)|\mathsf{link}(x, y) \not\approx_{\mathrm{w}} \mathsf{scrupulous}(a, x, \emptyset)|\mathsf{link}(x, y)$$

$$\mathsf{R}[X] \not\approx_{\mathrm{u}} \mathsf{S}[X] \not\approx_{\mathrm{u}} \mathsf{K}[X] \approx_{\mathrm{u}} \mathsf{R}[X]$$

Scenario: Web Crawlers

Universally:

$$\mathsf{rash}(a, x, \tilde{y})|s \approx_{\mathrm{u}} \mathsf{cautious}(a, x, \tilde{y})|s$$

(they communicate all the addresses they gather – valid or not)

$$\mathsf{rash}(a, x, \emptyset)|\mathsf{link}(x, y) \not\approx_{\mathrm{w}} \mathsf{scrupulous}(a, x, \emptyset)|\mathsf{link}(x, y)$$

$$\mathsf{R}[X] \not\approx_{\mathrm{u}} \mathsf{S}[X] \not\approx_{\mathrm{u}} \mathsf{K}[X] \approx_{\mathrm{u}} \mathsf{R}[X]$$

Symbolically:

$$\begin{array}{lll} \mathsf{R}[X] & \xrightarrow{Y}_{\tau} & \mathsf{rash}(a, y_i, \tilde{y} + x - y_i) \mid Y \\ \mathsf{K}[X] & \xrightarrow{\mathsf{link}(y_i,z)|Y}_{\tau} & \mathsf{cautious}(a, y_i, \tilde{y} + x - y_i) \mid \mathsf{link}(y_i, z) \mid Y \end{array} \qquad \text{(for any } z\text{)}$$

$$\mathsf{R}[X] \not\approx_{\mathrm{s}} \mathsf{K}[X]$$

$$\mathsf{R}[X] \approx_{\mathrm{l}} \mathsf{K}[X]$$

Scenario: Web Crawlers

$$\mathsf{K}[X] \not\approx_{\mathrm{l}} \mathsf{S}[X]$$

$\mathsf{S}[X]$ observes only valid sites y_i:

$$\mathsf{S}[X] \xrightarrow{\mathsf{link}(y_i,z)|Y}_{\tau} \mathsf{scrupulous}(a, y_i, \tilde{y} + x - y_i) \mid \mathsf{link}(y_i, z) \mid Y \xrightarrow{Y}_{ay_i} \ldots$$

while $\mathsf{K}[X]$ observes known sites:

$$\mathsf{K}[X] \xrightarrow{Y}_{ay_i} \mathsf{K}[Y]$$

cautious $\approx_{\mathrm{l}}$ scrupulous on a “valid” (no broken link) network!

Typed symbolic semantics

Types as contracts!

(Software Architectures: Type as Interfaces; Service-Oriented Computing: Types as Service (level) Contract; ...).

Types discipline a (naive - e.g. no restriction) form of names:

$$s : T_{\tilde{d},\tilde{p}} \text{ iff}$$

- for any $x \in \tilde{d}$ there exists y such that s contains $\mathsf{link}(x, y)$;
- for any link $\mathsf{link}(x, y)$ in s such that $y \notin \tilde{p}$ then it must be the case that $\mathsf{link}(y, z)$ is in s for some z.

$$s \textit{ valid} \text{ if } s : T_{\_,\emptyset}$$

- every s has a type;
- subject-reduction;

$$C[X : T_{\tilde{d},\tilde{p}}] \approx_{\mathrm{u}} D[X : T_{\tilde{d},\tilde{p}}] \text{ if for any } s : T_{\tilde{d},\tilde{p}} \;\; C[s] \approx D[s]$$

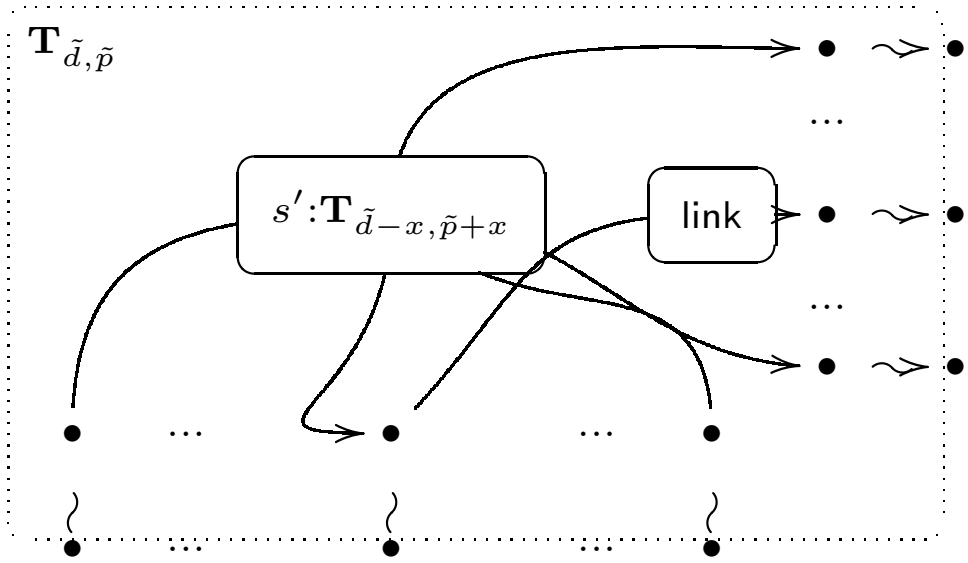
Typing context variables

1) Decomposing types (type structural equivalence $\equiv_T$):

$$s : T_{\tilde{d},\tilde{p}} \text{ iff}$$

- $s \equiv_T \text{link}(x, y)|s'$ and $s' : T_{\tilde{d}-x,\tilde{p}+x}$, or
- $s \equiv_T \text{link}(x, z)|s'$ and $s' : T_{\tilde{d}-x+z,\tilde{p}+z+x}$.

with $x \in \tilde{d}$, $y \in \tilde{p}$, $z \notin \tilde{p}$



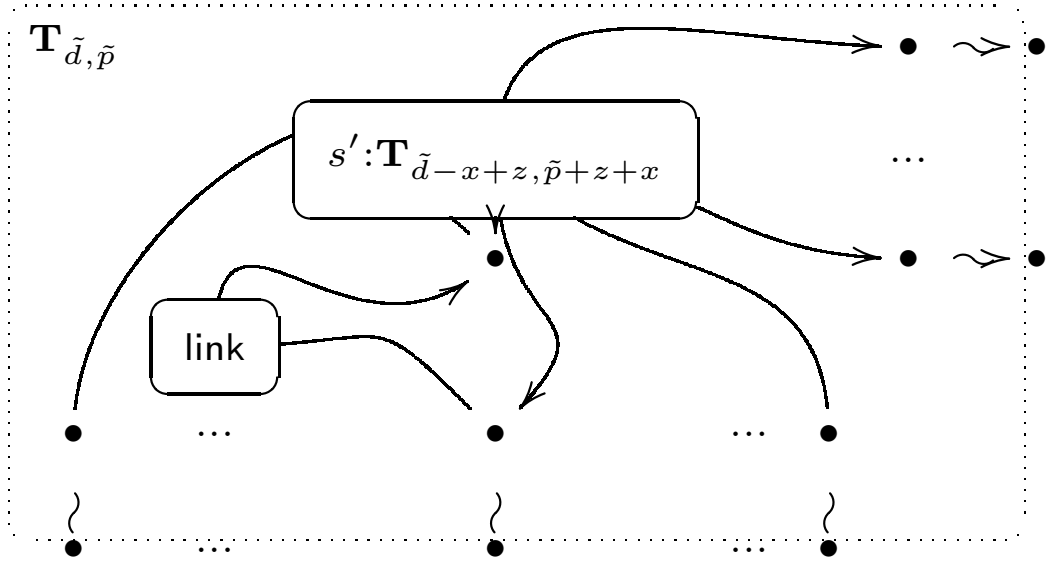
Typing context variables

1) Decomposing types (type structural equivalence $\equiv_T$):

$$s : T_{\tilde{d},\tilde{p}} \text{ iff}$$

- $s \equiv_T \text{link}(x, y)|s'$ and $s' : T_{\tilde{d}-x,\tilde{p}+x}$, or
- $s \equiv_T \text{link}(x, z)|s'$ and $s' : T_{\tilde{d}-x+z,\tilde{p}+z+x}$.

with $x \in \tilde{d}$, $y \in \tilde{p}$, $z \notin \tilde{p}$



Typing context variables

2) Decorating symbolic transitions, e.g.:

$C[X : T_{\tilde{d},\tilde{p}}] \equiv_T C[\mathsf{link}(x,y) \mid Y : T_{\tilde{d}-x,\tilde{p}+x}] \xrightarrow{Y}_\alpha D[_{\tilde{d}-x,\tilde{p}+x}]$ if $y \in \tilde{p}$

$C[X : T_{\tilde{d},\tilde{p}}] \equiv_T C[\mathsf{link}(x,y) \mid Y : T_{\tilde{d}-x+y,\tilde{p}+y+x}] \xrightarrow{Y}_\alpha D[Y : T_{\tilde{d}-x+y,\tilde{p}+y+x}]$ if $y \notin \tilde{p}$

3) Considering decorated weak loose symbolic bisimulation in the decorated symbolic transition system up to $\equiv_T$ ($\approx_{\mathrm{d}}$).

Typed symbolic semantics

Finally,

$$\mathsf{S}[X : T_{\tilde{y}+x,\emptyset}] \approx_{\mathrm{d}} \mathsf{K}[X : T_{\tilde{y}+x,\emptyset}]$$

Indeed

$$\mathsf{K}[X : T_{\tilde{y}+x,\emptyset}] \xrightarrow{Y}_{ay_i} \mathsf{K}[Y : T_{\tilde{y}+x,\emptyset}]$$

can be weakly simulated by the symbolic moves

$$\mathsf{S}[X : T_{\tilde{y}+x,\emptyset}] \equiv_T \mathsf{S}[\mathsf{link}(y_i, z) | Y : T_{\tilde{y}+x-y_i,y_i}] \stackrel{Y}{\Longrightarrow}_{ay_i}$$
$$\mathsf{scrupulous}(a, y_i, \tilde{y}+x-y_i) \mid \mathsf{link}(y_i, z) \mid Y : T_{\tilde{y}+x-y_i,y_i} \qquad (z \in \tilde{y}+x)$$

and

$$\mathsf{S}[X : T_{\tilde{y}+x,\emptyset}] \equiv_T \mathsf{S}[\mathsf{link}(y_i, z) | Y : T_{\tilde{y}+x-y_i+z,y_i+z}] \stackrel{Y}{\Longrightarrow}_{ay_i}$$
$$\mathsf{scrupulous}(a, y_i, \tilde{y}+x-y_i) \mid \mathsf{link}(y_i, z) \mid Y : T_{\tilde{y}+x-y_i+z,y_i+z} \qquad (z \notin \tilde{y}+x)$$

(whose target states are again bisimilar)

Summing up

- an ongoing step toward name-based symbolic semantics

Summing up

- an ongoing step toward name-based symbolic semantics
- the introduction of a type discipline (as proof of concepts)

Summing up

- an ongoing step toward name-based symbolic semantics
- the introduction of a type discipline (as proof of concepts)
- the definition of suitable equivalence relations

Summing up

- an ongoing step toward name-based symbolic semantics
- the introduction of a type discipline (as proof of concepts)
- the definition of suitable equivalence relations

Summing up

- an ongoing step toward name-based symbolic semantics
- the introduction of a type discipline (as proof of concepts)
- the definition of suitable equivalence relations

- universal quantification on names needs symbolic semantics as well (– even for this simple scenario)

Summing up

- an ongoing step toward name-based symbolic semantics
- the introduction of a type discipline (as proof of concepts)
- the definition of suitable equivalence relations

- universal quantification on names needs symbolic semantics as well (– even for this simple scenario)
- a more complete scenario to be addressed (restriction)

Summing up

- an ongoing step toward name-based symbolic semantics
- the introduction of a type discipline (as proof of concepts)
- the definition of suitable equivalence relations

- universal quantification on names needs symbolic semantics as well (– even for this simple scenario)
- a more complete scenario to be addressed (restriction)
- study of congruence properties

Summing up

- an ongoing step toward name-based symbolic semantics
- the introduction of a type discipline (as proof of concepts)
- the definition of suitable equivalence relations

- universal quantification on names needs symbolic semantics as well (– even for this simple scenario)
- a more complete scenario to be addressed (restriction)
- study of congruence properties

Summing up

- an ongoing step toward name-based symbolic semantics
- the introduction of a type discipline (as proof of concepts)
- the definition of suitable equivalence relations

- universal quantification on names needs symbolic semantics as well (– even for this simple scenario)
- a more complete scenario to be addressed (restriction)
- study of congruence properties

- a toy implementation to play with `www.di.unipi.it/ lafuente/ice08`