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
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.

...?x.... any (free to choose later on)
...?{x}_{k}... a message encrypted either with \( k \) 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:

\[ C[X] \]
Define a semantics for open systems, i.e. contexts:

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

A term with \( X \) a process variable 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:

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

... or it evolves alone ...
Define a semantics for open systems, i.e. contexts:

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

... or is able to synch.

as prescribed by the semantical rules (finite)!
BBB approach

Symbolic transition system:

\[ C[X] \xrightarrow{\phi} aD[Y] \]

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:

\[ C[X] \xrightarrow{\phi} aD[Y] \]

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:

\[ C[X] \xrightarrow{\phi} a D[Y] \]

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

\[ \phi ::= \ldots \mid \Diamond a.\phi' \mid \ldots \mid f(\phi') \mid X \]

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

\[ p \models \Diamond a\phi' \iff \exists q. p \rightarrow a q \land q \models \phi' \]
A notion of correspondence
(soundness and completeness) - informally:

\[ C[X] \xrightarrow{\phi} a D[Y] \]

\[ \uparrow \]

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

\[ \downarrow \]

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

\[
C[X] \xrightarrow{\phi_a} C'[Y] \\
\sim_s \hspace{1cm} \sim_s \\
D[X] \xrightarrow{\phi_a} D'[Y]
\]

same (syntactic equality) formula!
BBB approach

Natural definition of *strict symbolic bisimulation*:

\[
C[X] \xrightarrow{\phi} a \quad C'[Y]
\]

\[
\sim_s \quad \sim_s
\]

\[
D[X] \xrightarrow{\phi} a \quad D'[Y]
\]

same (syntactic equality) formula!

Relaxation: *loose symbolic bisimulation*

\[
C[X] \xrightarrow{\psi} a \quad C'[Y]
\]

\[
\sim_1 \quad \sim_1
\]

\[
D[X] \xrightarrow{\psi} a \quad D'[Z] \quad \text{and} \quad D'[\psi']
\]

and \( \exists \psi' \) spatial such that \( \phi = \psi; \psi' \)
BBB approach

\[ C[X] \xrightarrow{\phi_1; \ldots; \phi_h} \ell D[Y] \text{ if } C[X] \xrightarrow{\phi_1} \tau \cdots \xrightarrow{\phi_{k-1}} \tau \xrightarrow{\phi_k} \ell \xrightarrow{\phi_{k+1}} \tau \cdots \xrightarrow{\phi_h} \tau D[Y] \]
BBB approach

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

strict weak symbolic bisimulation (symmetric!): \( \approx_s \)

\[
\begin{align*}
C[X] & \xrightarrow{\phi} \ell \quad C''[Y] \\
\approx_s & \quad \approx_s \\
D[X] & \xrightarrow{\phi} \ell \quad D'[Y]
\end{align*}
\]

loose weak symbolic bisimulation (symmetric!): \( \approx_1 \)

\[
\begin{align*}
C[X] & \xrightarrow{\phi} \ell \quad C''[Y] \\
\approx_1 & \quad \approx_1 \\
D[X] & \xrightarrow{\psi} \ell \quad D'[Y] \text{ and } D'[^{\psi'}]
\end{align*}
\]

and \( \exists \psi' \) spatial such that \( \phi = \psi; \psi' \)
BBB approach

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

\[
\begin{align*}
\sim_s & \Rightarrow \dot{\sim}_1 \\
\sim_s & \Rightarrow \sim_s \\
\dot{\sim}_1 & \Rightarrow \sim_1 \end{align*}
\Rightarrow \sim_u (\approx_u) \quad \forall p \ C[p] \sim D[p]
\]
BBB approach

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

$$\sim_s \Rightarrow \sim_1 \quad \sim_s \Rightarrow \approx_s \quad \Rightarrow \sim_u (\approx_u) \quad \forall p \ C[p] \sim D[p]$$

Instantiation time matters!

$$C[X] = a.0 + a.b.0 + a.\text{one}_b(X) \quad D[X] = a.0 + a.b.0 + a.\text{stop}(X).$$
BBB approach

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

\[
\sim_s \Rightarrow \sim_1 \\
\sim_s \Rightarrow \sim_s \\
\sim_1 \Rightarrow \sim_1 \\
\Rightarrow \sim_u (\approx_u) \quad \forall p \ C[p] \sim D[p]
\]

Instantiation time matters!

\[
C[X] = a.0 + a.b.0 + a.\text{one}_b(X) \\
D[X] = a.0 + a.b.0 + a.\text{stop}(X).
\]
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 $\alpha$ conversion commute with instantiation? (semantic choice)

...
Scenario: Web Crawlers

A simplistic proof-of-concept scenario.

\[ s ::= 0 \mid c \mid \text{link}(x, y) \mid s|s \]

\[ c ::= \text{rash}(a, x, y) \mid \text{cautious}(a, x, y) \mid \text{scrupulous}(a, x, y) \]
Scenario: Web Crawlers

A simplistic proof-of-concept scenario.

\[ s ::= 0 \mid c \mid \text{link}(x, y) \mid s | s \]
\[ c ::= \text{rash}(a, x, \tilde{y}) \mid \text{cautious}(a, x, \tilde{y}) \mid \text{scrupulous}(a, x, \tilde{y}) \]

\[ c(a, x, \tilde{y}) \mid \text{link}(x, z) \mid s \rightarrow_{\tau} c(a, x, \tilde{y} + z) \mid \text{link}(x, z) \mid s \]
Scenario: Web Crawlers

\[
\begin{align*}
rash(a, x, \tilde{y} + z) & \mid s \quad \rightarrow_\tau \quad rash(a, z, \tilde{y} + x) \mid s \\
c(a, x, \tilde{y} + z) \mid \text{link}(z, w) \mid s & \quad \rightarrow_\tau \quad c(a, z, \tilde{y} + x) \mid \text{link}(z, w) \mid s
\end{align*}
\]
Scenario: Web Crawlers

\[
c(a, x, \tilde{y}) | s \rightarrow_{az} c(a, x, \tilde{y}) | s
\]

\[
\text{scrupulous}(a, x, \tilde{y}) | s \rightarrow_{ax} \text{scrupulous}(a, x, \tilde{y}) | s
\]

with \( z \in \tilde{y} + x \)

\[
\text{OBserve}
\]
Scenario: Web Crawlers

\[
R[X] \overset{\text{def}}{=} \text{rash}(a, x, \tilde{y}) \mid X \\
K[X] \overset{\text{def}}{=} \text{cautious}(a, x, \tilde{y}) \mid X \\
S[X] \overset{\text{def}}{=} \text{scrupulous}(a, x, \tilde{y}) \mid X
\]

\[
\begin{align*}
R[X] \xrightarrow{\text{link}(x,z)} Y & \quad \text{rash}(a, x, \tilde{y} + z) \mid \text{link}(x, z) \mid Y \quad \text{(for any } z) \\
R[X] \xrightarrow{Y} \tau & \quad \text{rash}(a, y_i, \tilde{y} + x - y_i) \mid Y \\
R[X] \xrightarrow{ax} & \quad R[Y] \\
R[X] \xrightarrow{ay_i} & \quad R[Y] \\
K[X] \xrightarrow{\text{link}(x,z)} Y & \quad \text{cautious}(a, x, \tilde{y} + z) \mid \text{link}(x, z) \mid Y \quad \text{(for any } z) \\
K[X] \xrightarrow{\text{link}(y_i,z)} Y & \quad \text{cautious}(a, y_i, \tilde{y} + x - y_i) \mid \text{link}(y_i, z) \mid Y \quad \text{(for any } z) \\
K[X] \xrightarrow{ax} & \quad K[Y] \\
K[X] \xrightarrow{ay_i} & \quad K[Y] \\
S[X] \xrightarrow{\text{link}(x,z)} Y & \quad \text{scrupulous}(a, x, \tilde{y} + z) \mid \text{link}(x, z) \mid Y \quad \text{(for any } z) \\
S[X] \xrightarrow{\text{link}(y_i,z)} Y & \quad \text{scrupulous}(a, y_i, \tilde{y} + x - y_i) \mid \text{link}(y_i, z) \mid Y \quad \text{(for any } z) \\
S[X] \xrightarrow{ax} & \quad S[Y]
\end{align*}
\]
Scenario: Web Crawlers

Universally:

\[ \text{rash}(a, x, \tilde{y}) \mid s \approx_u \text{cautious}(a, x, \tilde{y}) \mid s \]

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

\[ \text{rash}(a, x, \emptyset) \mid \text{link}(x, y) \not\approx_w \text{scrupulous}(a, x, \emptyset) \mid \text{link}(x, y) \]

\[ R[X] \not\approx_u S[X] \not\approx_u K[X] \approx_u R[X] \]
Scenario: Web Crawlers

Universally:

\[ \text{rash}(a, x, \tilde{y})|s \approx_u \text{cautious}(a, x, \tilde{y})|s \]

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

\[ \text{rash}(a, x, \emptyset)|\text{link}(x, y) \not\approx_w \text{scrupulous}(a, x, \emptyset)|\text{link}(x, y) \]

\[ \text{R}[X] \not\approx_u \text{S}[X] \not\approx_u \text{K}[X] \approx_u \text{R}[X] \]

Symbolically:

\[ \begin{align*}
\text{R}[X] & \xrightarrow{Y} \tau \quad \text{rash}(a, y_i, \tilde{y} + x - y_i) \mid Y \\
\text{K}[X] & \xrightarrow{\text{link}(y_i, z)\mid Y} \tau \quad \text{cautious}(a, y_i, \tilde{y} + x - y_i) \mid \text{link}(y_i, z) \mid Y \quad \text{(for any z)}
\end{align*} \]

\[ \text{R}[X] \not\approx_s \text{K}[X] \]

\[ \text{R}[X] \approx_1 \text{K}[X] \]
Scenario: Web Crawlers

\[ K[X] \not\approx_1 S[X] \]

\( S[X] \) observes only valid sites \( y_i \):

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

while \( K[X] \) observes known sites:

\[ K[X] \xrightarrow{Y} ay_i K[Y] \]

cautious \( \approx_1 \) 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 \( \text{link}(x, y) \);
- for any link \( \text{link}(x, y) \) in \( s \) such that \( y \notin \tilde{p} \) then it must be the case that \( \text{link}(y, z) \) is in \( s \) for some \( z \).

\( s \text{ valid if } s : T_{\_,\_\_}\) 

- every \( s \) has a type;
- subject-reduction;

\[ C[X : T_{\tilde{d},\tilde{p}}] \approx_u D[X : T_{\tilde{d},\tilde{p}}] \text{ if for any } s : T_{\tilde{d},\tilde{p}} \quad C[s] \approx D[s] \]
Typing context variables

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

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

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

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

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

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

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

with $x \in \tilde{d}, y \in \tilde{p}, z \notin \tilde{p}$
2) Decorating symbolic transitions, e.g.:

\[ C[X : T_{\tilde{d},\tilde{p}}] \equiv_T C[\text{link}(x, y) \mid Y : T_{\tilde{d} - x, \tilde{p} + x}] \overset{Y}{\to} \alpha D[Y : T_{\tilde{d} - x + y, \tilde{p} + y + x}] \text{ if } y \in \tilde{p} \]

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

3) Considering decorated weak loose symbolic bisimulation in the decorated symbolic transition system up to \( \equiv_T (\approx_d) \).
Typed symbolic semantics

Finally,

\[ S[X : T\tilde{y} + x, 0] \approx_d K[X : T\tilde{y} + x, 0] \]

Indeed

\[ K[X : T\tilde{y} + x, 0] \xrightarrow{Y} ay_i K[Y : T\tilde{y} + x, 0] \]

can be weakly simulated by the symbolic moves

\[ S[X : T\tilde{y} + x, 0] \equiv_T S[link(y_i, z) | Y : T\tilde{y} + x - y_i, y_i] \xrightarrow{Y} ay_i \]

scrupulous\( (a, y_i, \tilde{y} + x - y_i) \mid link(y_i, z) \mid Y : T\tilde{y} + x - y_i, y_i \quad (z \in \tilde{y} + x) \)

and

\[ S[X : T\tilde{y} + x, 0] \equiv_T S[link(y_i, z) | Y : T\tilde{y} + x - y_i + z, y_i + z] \xrightarrow{Y} ay_i \]

scrupulous\( (a, y_i, \tilde{y} + x - y_i) \mid link(y_i, z) \mid Y : T\tilde{y} + x - y_i + z, y_i + z \quad (z \notin \tilde{y} + x) \)

(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