Proof Methodologies for Behavioural Equivalence in DPI

Alberto Ciaffaglione[1], Matthew Hennessy[2], Julian Rathke[2]

[1] Dipartimento di Matematica e Informatica, Università di Udine (Italy)

[2] Department of Informatics, University of Sussex (United Kingdom)

Conference of the Types Project

University of Nottingham, United Kingdom

April 18-21, 2006

Syntax of DPI [HR02]

$M, N \ ::=$	*Systems*
$l[\![P]\!]$	Located Processes
$M \mid N$	Composition
$(\mathsf{new}\, e : \mathsf{E})\, M$	Name Scoping
$\mathbf{0}$	Termination

$R, U \ ::=$	*Processes*
$u!\langle V\rangle\, R$	Output
$u?(X)\, R$	Input
$\mathsf{goto}\, v.T$	Migration
$(\mathsf{newc}\, c : \mathsf{C})\ R$	Local channel creation
$(\mathsf{newloc}\, k : \mathsf{K})\ R$	Location creation
$\mathsf{if}\ v_1 = v_2\ \mathsf{then}\ R\ \mathsf{else}\ U$	Matching
$R \mid U$	Parallelism
$*R$	Iteration
stop	Termination

Behaviour

A *configuration* consists of a pair $\mathcal{I} \triangleright M$, where:

- $\mathcal{I}$ is a *type environment*, associating some type to every free name in M
- there is a type environment Γ such that $\Gamma \vdash M$ and $\Gamma <: \mathcal{I}$

The behaviour is defined in terms of *actions* over configurations:

$$\mathcal{I} \triangleright M \xrightarrow{\mu} \mathcal{I}' \triangleright M', \text{ where } \mu \text{ ranges on:}$$

- τ: an internal action, requiring no participation by the user
- $(\tilde{e} : \tilde{\mathsf{E}})k.a?V$: the input of value V along the channel a, located at the site k; the bound names in $(\tilde{e})$ are freshly generated by the user
- $(\tilde{e} : \tilde{\mathsf{E}})k.a!V$: analogous for the output

Internal actions

(M-COMM)

$$\frac{\mathcal{I}_1 \triangleright M \xrightarrow{(\tilde{e}:\tilde{\mathsf{E}})k.a?V} \mathcal{I}'_1 \triangleright M' \qquad \mathcal{I}_2 \triangleright N \xrightarrow{(\tilde{e}:\tilde{\mathsf{E}})k.a!V} \mathcal{I}'_2 \triangleright N'}{\mathcal{I} \triangleright M \mid N \xrightarrow{\tau} \mathcal{I} \triangleright (\mathsf{new}\,\widetilde{e} : \widetilde{\mathsf{E}})(M' \mid N')}$$

(M-COMM)

$$\frac{\mathcal{I}_1 \triangleright M \xrightarrow{(\tilde{e}:\tilde{\mathsf{E}})k.a!V} \mathcal{I}'_1 \triangleright M' \qquad \mathcal{I}_2 \triangleright N \xrightarrow{(\tilde{e}:\tilde{\mathsf{E}})k.a?V} \mathcal{I}'_2 \triangleright N'}{\mathcal{I} \triangleright M \mid N \xrightarrow{\tau} \mathcal{I} \triangleright (\mathsf{new}\,\widetilde{e} : \widetilde{\mathsf{E}})(M' \mid N')}$$

(M-SPLIT)

$$\mathcal{I} \triangleright k[\![P \mid Q]\!] \xrightarrow{\tau}_\beta \mathcal{I} \triangleright k[\![P]\!] \mid k[\![Q]\!]$$

(M-L.CREATE)

$$\mathcal{I} \triangleright k[\![(\mathsf{newloc}\, l : \mathsf{L})\ \ P]\!] \xrightarrow{\tau}_\beta \mathcal{I} \triangleright (\mathsf{new}\, l : \mathsf{L})\, k[\![P]\!]$$

(M-MOVE)

$$\mathcal{I} \triangleright k[\![\mathsf{goto}\, l.P]\!] \xrightarrow{\tau}_\beta \mathcal{I} \triangleright l[\![P]\!]$$

(M-C.CREATE)

$$\mathcal{I} \triangleright k[\![(\mathsf{newc}\, c : \mathsf{C})\ \ P]\!] \xrightarrow{\tau}_\beta \mathcal{I} \triangleright (\mathsf{new}\, c@k : \mathsf{C})\, k[\![P]\!]$$

(M-UNWIND)

$$\mathcal{I} \triangleright k[\![*P]\!] \xrightarrow{\tau}_\beta \mathcal{I} \triangleright k[\![*P \mid P]\!]$$

External actions

(M-IN)

$$\frac{\mathcal{I}^w(k,a)\downarrow \qquad \mathcal{I} \vdash_k V : \mathcal{I}^w(k,a)}{\mathcal{I} \triangleright k[\![a?(X)\,R]\!] \xrightarrow{k.a?V} \mathcal{I} \triangleright k[\![R\{^V\!/\!_X\}]\!]}$$

(M-OUT)

$$\frac{\mathcal{I}^r(k,a)\downarrow}{\mathcal{I} \triangleright k[\![a!\langle V\rangle\,P]\!] \xrightarrow{k.a!V} \mathcal{I},\ \langle V : \mathcal{I}^r(k,a)\rangle@k \triangleright k[\![P]\!]}$$

(M-WEAK)

$$\frac{\mathcal{I},\langle e : \mathsf{E}\rangle \triangleright M \xrightarrow{(\tilde{d}:\tilde{\mathsf{D}})k.a?V} \mathcal{I}' \triangleright M'}{\mathcal{I} \triangleright M \xrightarrow{(e:\mathsf{E}\,\tilde{d}:\tilde{\mathsf{D}})k.a?V} \mathcal{I}' \triangleright M'}\ \mathsf{bn}(e) \notin \mathcal{I}$$

(M-OPEN)

$$\frac{\mathcal{I},\langle e : \top\rangle \triangleright M \xrightarrow{(\tilde{d}:\tilde{\mathsf{D}})k.a!V} \mathcal{I}' \triangleright M'}{\mathcal{I} \triangleright (\mathsf{new}\,e : \mathsf{E})\,M \xrightarrow{(e:\mathsf{E}\tilde{d}:\tilde{\mathsf{D}})k.a!V} \mathcal{I}' \triangleright M'}$$

(M-CTXT)

$$\frac{\mathcal{I} \triangleright M \xrightarrow{\mu} \mathcal{I}' \triangleright M'}{\begin{array}{l}\mathcal{I} \triangleright M \mid N \xrightarrow{\mu} \mathcal{I}' \triangleright M' \mid N \\ \mathcal{I} \triangleright N \mid M \xrightarrow{\mu} \mathcal{I}' \triangleright N \mid M'\end{array}}\ \mathsf{bn}(\mu) \notin \mathsf{fn}(N)$$

(M-NEW)

$$\frac{\mathcal{I},\langle e : \top\rangle \triangleright M \xrightarrow{\mu} \mathcal{I}',\langle e : \top\rangle \triangleright M'}{\mathcal{I} \triangleright (\mathsf{new}\,e : \mathsf{E})\,M \xrightarrow{\mu} \mathcal{I}' \triangleright (\mathsf{new}\,e : \mathsf{E})\,M'}\ \mathsf{bn}(e) \notin \mu$$

Bisimulation equivalence

A binary relation over configurations is a *bisimulation* [HMR04]
if both it, and its inverse, satisfy the following transfer property:

$$
\begin{array}{ccc}
(\mathcal{I}_M \triangleright M) \;\; \mathcal{R} \;\; (\mathcal{I}_N \triangleright N) & & (\mathcal{I}_M \triangleright M) \;\; \mathcal{R} \;\; (\mathcal{I}_N \triangleright N) \\
\mu \Big\downarrow \qquad\qquad & \text{implies} & \qquad\qquad \hat{\mu} \Big\Downarrow \\
(\mathcal{I}_{M'} \triangleright M') \qquad\qquad & & (\mathcal{I}_{M'} \triangleright M') \; \mathcal{R} \; (\mathcal{I}_{N'} \triangleright N')
\end{array}
$$

We denote $\approx_{bis}$ the largest bisimulation between configurations, and write:

$$\mathcal{I} \models \; M \approx_{bis} N$$

This is a relation over systems, parameterised over type environments

$\Rightarrow$ Tractable proof techniques can be developed for it

Proof techniques

Theorem 1 (Contextuality) [HMR04] Suppose $\mathcal{I} \models M \approx_{bis} N$. Then:

- $\mathcal{I} \vdash O$ implies $\mathcal{I} \models M \mid O \approx_{bis} N \mid O$
- $\mathcal{I}, \langle e : \mathsf{E} \rangle \models M \approx_{bis} N$ implies $\mathcal{I} \models (\mathsf{new}\, e : \mathsf{E})\, M \approx_{bis} (\mathsf{new}\, e : \mathsf{E})\, N$

Proposition 1 (Structural Equivalence) If $M \equiv N$, then $M \approx_{bis} N$.

Proposition 2 (β-actions) Suppose $\mathcal{I} \triangleright M \xrightarrow{\tau}{}_{\beta}^{*} N$. Then $\mathcal{I} \models M \approx_{bis} N$.

Proof techniques (cont'd)

A binary relation between configurations is a *bisimulation up-to-β* if both it, and its inverse, satisfy the following transfer property:

$$
\begin{array}{ccccc}
(\mathcal{I}_M \triangleright M) \;\mathcal{R}\; (\mathcal{I}_N \triangleright N) & & (\mathcal{I}_M \triangleright M) & \mathcal{R} & (\mathcal{I}_N \triangleright N) \\
\mu \downarrow & \text{implies} & & & \Downarrow \hat{\mu} \\
(\mathcal{I}_{M'} \triangleright M') & & (\mathcal{I}_{M'} \triangleright M') & (\xrightarrow{\tau}{}^{*}_{\beta} \circ \equiv) \circ \mathcal{R} \circ \approx_{bis} & (\mathcal{I}_{N'} \triangleright N')
\end{array}
$$

Proposition 3 (Bisimulations up-to–β)

If $(\mathcal{I} \triangleright M)\,\mathcal{R}\,(\mathcal{I} \triangleright N)$, where $\mathcal{R}$ is a bisimulation up-to-β, then $\mathcal{I} \models M \approx_{bis} N$.

Crossing a firewall

Firewall [CG98,CG99,LS00,MN03] as a domain to which access is restricted:

$$F \Leftarrow (\mathsf{new}\ f : \mathsf{F})\ f[\![P \mid *\mathsf{goto}\ a.\mathsf{tell}!\langle f\rangle]\!]$$

The existence of the firewall is made known only to a located agent:

$$A \Leftarrow a[\![R \mid \mathsf{tell}?(x)\ \mathsf{goto}\ x.Q]\!]$$

Then, we prove the equivalence:

$$\mathcal{I} \models F \mid A \approx_{bis} (\mathsf{new}\ f : \mathsf{F})(f[\![P \mid *\mathsf{goto}\ a.\mathsf{tell}!\langle f\rangle \mid Q]\!]) \mid a[\![R]\!] \qquad (1)$$

relative to a restricted environment $\mathcal{I}$, such that:

(i) $\mathcal{I} \vdash_a^{max} \mathsf{tell} : \mathsf{r}\langle\mathsf{F}\rangle$

(ii) $\mathcal{I} \vdash a[\![R]\!]$

(iii) $\mathcal{I} \vdash (\mathsf{new}\ f : \mathsf{F})\ f[\![P]\!]$

Firewall: the formal proof

Since, up-to-structural equivalence:

$$F \mid A \xrightarrow{\tau}_{\beta} F \mid a[\![\mathsf{tell?}(x)\,\mathsf{goto}\,x.Q]\!] \mid a[\![R]\!]$$

by *Propositions 1* and *2* it is sufficient to prove:

$$\mathcal{I} \models F|a[\![\mathsf{tell?}(x)\,\mathsf{goto}\,x.Q]\!]|a[\![R]\!] \approx_{bis} (\mathsf{new}\ f : \mathsf{F})(f[\![P|*\mathsf{goto}\,a.\mathsf{tell!}\langle f\rangle|Q]\!]) \mid a[\![R]\!]$$

By *Contextuality* and assumption (ii) we reduce to:

$$\mathcal{I} \models F \mid a[\![\mathsf{tell?}(x)\,\mathsf{goto}\,x.Q]\!] \approx_{bis} (\mathsf{new}\ f : \mathsf{F})(f[\![P \mid *\mathsf{goto}\,a.\mathsf{tell!}\langle f\rangle \mid Q]\!])$$

Then, by structural equivalence, and again *Contextuality*, to:

$$\mathcal{I}_f \models f[\![P \mid *\mathsf{goto}\,a.\mathsf{tell!}\langle f\rangle]\!] \mid a[\![\mathsf{tell?}(x)\,\mathsf{goto}\,x.Q]\!] \approx_{bis} f[\![P \mid *\mathsf{goto}\,a.\mathsf{tell!}\langle f\rangle \mid Q]\!]$$

where $\mathcal{I}_f$ is a shorthand for $\mathcal{I}, \langle f : \mathsf{F}\rangle$

Firewall: the formal proof (cont'd)

Since:

- $f[\![P \mid *\mathsf{goto}\, a.\mathsf{tell!}\langle f\rangle]\!] \mid a[\![\mathsf{tell?}(x)\,\mathsf{goto}\, x.Q]\!] \xrightarrow{\tau}_{\beta}$
  $f[\![P]\!] \mid f[\![*\mathsf{goto}\, a.\mathsf{tell!}\langle f\rangle]\!] \mid a[\![\mathsf{tell?}(x)\,\mathsf{goto}\, x.Q]\!]$
- $f[\![P \mid *\mathsf{goto}\, a.\mathsf{tell!}\langle f\rangle \mid Q]\!] \xrightarrow{\tau}{}^{*}_{\beta} f[\![P]\!] \mid f[\![*\mathsf{goto}\, a.\mathsf{tell!}\langle f\rangle]\!] \mid f[\![Q]\!]$

by *Proposition 2*, *Contextuality* and assumption (iii), we reduce finally to:

$$\mathcal{I}_f \models\ f[\![*\mathsf{goto}\, a.\mathsf{tell!}\langle f\rangle]\!] \mid a[\![\mathsf{tell?}(x)\,\mathsf{goto}\, x.Q]\!] \approx_{bis} f[\![*\mathsf{goto}\, a.\mathsf{tell!}\langle f\rangle]\!] \mid f[\![Q]\!]$$

$\Rightarrow$ We define the parameterised relation $\mathcal{R}$ by letting $\mathcal{J} \models\ M \,\mathcal{R}\, N$ whenever:

(a) $\mathcal{J} \triangleright M$ is a configuration and N is the same as M

(b) or $\mathcal{J}$ is $\mathcal{I}_f$ and

- M has form $f[\![*\mathsf{goto}\, a.\mathsf{tell!}\langle f\rangle]\!] \mid a[\![\mathsf{tell?}(x)\,\mathsf{goto}\, x.Q]\!] \mid \Pi_n\ (a[\![\mathsf{tell!}\langle f\rangle]\!])^n$
- N has form $f[\![*\mathsf{goto}\, a.\mathsf{tell!}\langle f\rangle]\!] \mid f[\![Q]\!] \mid \Pi_n\ (a[\![\mathsf{tell!}\langle f\rangle]\!])^n$

A server and its clients

Let us consider:

$$S \Leftarrow s[\![*\mathsf{req}?(x, y_{@}z)\mathsf{goto}\, z.y!\langle isprime(x)\rangle \mid S']\!]$$

$$C_i \Leftarrow c_i[\![(\mathsf{newc}\, r : \mathsf{rw}\langle \mathbf{bool}\rangle)\ \mathsf{goto}\, s.\mathsf{req}!\langle v_i, r_{@}c_i\rangle \mid C'_i]\!]$$

Then one might want to derive:

$$\mathcal{I} \models S \mid \Pi_{i\in[1,n]}\, C_i \approx_{bis} S \mid \Pi_{i\in[1,n]}\, c_i[\![(\mathsf{newc}\, r : \mathsf{rw}\langle \mathbf{bool}\rangle)\ r!\langle isprime(v_i)\rangle \mid C'_i]\!]$$

We must require that *the computational context can not read on* req:

(i) $\mathcal{I} \vdash_s^{max} \mathsf{req} : \mathsf{w}\langle\, \mathbf{int}, \mathsf{w}\langle \mathbf{bool}\rangle_{@}\mathsf{loc}\,\rangle$

(ii) $\mathcal{I} \vdash s[\![S']\!]$

(iii) $\mathcal{I} \vdash C_i$

$\Rightarrow$ The major proof technique we use is *Contextuality*

Metaservers

Memory service: a domain installing the service at a new site. Two versions:

$$
\begin{array}{lcl}
S & \Leftarrow & s[\![*\mathsf{setup}?(y@z)\,(\mathsf{newloc}\, m : \mathsf{M})\ \mathsf{goto}\, m.\mathsf{Mem} \mid \mathsf{goto}\, z.y!\langle m\rangle]\!] \\
C_i & \Leftarrow & c_i[\![(\mathsf{newc}\, r : \mathsf{R})\ \mathsf{goto}\, s.\mathsf{setup}!\langle r@c_i\rangle \mid r?(x)\, P_i(x)]\!] \\
S' & \Leftarrow & s'[\![*\mathsf{setup}'?(x, y@z)\ \mathsf{goto}\, x.\mathsf{Mem} \mid \mathsf{goto}\, z.y!]\!] \\
C'_i & \Leftarrow & c_i[\![(\mathsf{newc}\, t : \mathsf{T})\ (\mathsf{newloc}\, m_i : \mathsf{M})\ \mathsf{goto}\, s'.\mathsf{setup}'!\langle m_i, t@c_i\rangle \mid t?P_i(m_i)]\!]
\end{array}
$$

where $P_i(x), P_i(m_i)$ is parametric code, $\mathsf{R} = \mathsf{rw}\langle\mathsf{M}\rangle$, and $\mathsf{T} = \mathsf{rw}\langle\mathbf{unit}\rangle$

The two different kinds of servers S and S' lead to equivalent behaviour:

$$\mathcal{I} \models S \mid C_1 \mid C_2 \approx_{bis} S' \mid C'_1 \mid C'_2 \qquad (2)$$

provided *the context has neither write nor read access* to setup, setup′:

$$\mathcal{I} \vdash^{max}_{s} \mathsf{setup} : \top \qquad\qquad \mathcal{I} \vdash^{max}_{s'} \mathsf{setup}' : \top$$

Bibliography

[CG98] L. Cardelli, A. D. Gordon. Mobile ambients. In Proc. of FoSSaCS, LNCS 1378, Springer, 1998.

[CG99] A. D. Gordon, L. Cardelli. Equational properties of mobile ambients. In Proc. of FoSSaCS, LNCS 1578, Springer, 1999.

[HMR04] M. Hennessy, M. Merro, J. Rathke. Towards a behavioural theory of access and mobility control in distributed systems. TCS 322(3), 2004.

[HR02] M. Hennessy, J. Riely. Resource access control in systems of mobile agents. Information and Computation 173(1), 2002.

[LS00] F. Levi, D. Sangiorgi. Controlling interference in ambients. In Proc. of POPL, 2000.

[MN03] M. Merro, F. Zappa Nardelli. Bisimulation proof methods for mobile ambients. In Proc. of ICALP, LNCS 2719, Springer, 2003.