A Higher-Order Distributed Calculus with Name Creation

Adrien Piérard
Eijiro Sumii

Tohoku University
Sendai, Japan

Executive Summary

(In)equivalence theory of process calculus with passivation and name creation

- An extreme form of distribution
- Different from name restriction
- Tricky!

Passivation
[Schmitt-Stefani]

Process a[P]
(process P running at location a)
can output P to channel a
<u>at any time</u> and become 0

Passivation can express:

- Migration

$a[P] \mid a(X).b[X] \rightarrow 0 \mid b[P]$

- Duplication

$a[P] \mid a(X).(b[X] \mid c[X])$
$\rightarrow 0 \mid (b[P] \mid c[P])$

- Failure

$a[P] \mid a(X).0 \rightarrow 0 \mid 0$

Name Creation
[Stark-Pitts]

$$s \vdash \nu a.P \;\rightarrow\; s,a' \vdash [a'/a]P$$

for fresh a'

- where $s \vdash Q$ means "process Q with name set s"
- $s \vdash$ is omitted when unimportant

Syntax of Processes

P	$::=$	0	inaction
		$a(X).P$	input
		$\overline{a}\langle P\rangle.Q$	output
		$P \mid Q$	parallel
		$a[P]$	located
		$\nu a.P$	name creation
		$!P$	replication
		X	spawn

Operational Semantics by Labeled Transition System

General form: $s \vdash P \xrightarrow{\alpha} t \vdash Q$

"P makes action α and becomes Q"

α ::= $a(R)$ input

$\overline{a}\langle R\rangle$ output

τ internal (often omitted)

- $s \vdash \nu a.P \rightarrow s,a' \vdash [a'/a]P$ if $a' \notin s$ (name creation)
- $\overline{a}\langle R\rangle.P \xrightarrow{\overline{a}\langle R\rangle} P$ $\qquad a(X).P \xrightarrow{a(R)} [R/X]P$
- $P_1 | P_2 \rightarrow P_1' | P_2'$ if $P_i \xrightarrow{\overline{a}\langle R\rangle} P_i'$ and $P_{3-i} \xrightarrow{a(R)} P_{3-i}'$ (i=1,2)
- $a[P] \xrightarrow{\alpha} a[P']$ if $P \xrightarrow{\alpha} P'$
- $a[P] \xrightarrow{\overline{a}\langle P\rangle} 0$ (passivation)

Equivalence of Processes

Environmental bisimialrity:

[Sumii et al.]

$P \sim_E Q$

"P and Q are bisimilar under environment E (knowledge of the context)"

Environmental Bisimilarity

Largest $\sim$ s.t. $P \sim_E Q$ implies:

- If P can output M and become P', then Q can output N and become Q' with $P' \sim_{E \cup \{(M,N)\}} Q'$
- For any (M,N) composed from E, if P can input M and become P', then Q can input N and become Q' with $P' \sim_E Q'$

(cont.)

- For any (M,N) composed from E, $P|a[M] \sim_E Q|a[N]$
  - i.e. $M = C[M_1,\ldots,M_n]$ and $N = C[N_1,\ldots,N_n]$ for a context C and $(M_1,N_1),\ldots,(M_n,N_n) \in E$
- $Q \sim_{E^{-1}} P$

Environmental Bisimilarity

- Can be proved by coinduction
- Sound and complete w.r.t. standard equivalence (reduction-closed barbed equivalence)

Bisimilar Examples: Distributed FoldL and FoldR

$$\nu fl.\ \overline{fl}\langle l,0,k\rangle \mid a_1[L] \mid \ldots \mid a_n[L] \ \sim_\emptyset$$
$$\nu fr.\ \overline{fr}\langle l,0,k\rangle \mid a_1[R] \mid \ldots \mid a_n[R]$$

$$L = !fl(l,i,k).\ \text{if } null(l) \text{ then } \overline{k}\langle i\rangle \text{ else } \nu k'.\ \overline{fl}\langle cdr(l), i+car(l), k'\rangle.\ k'(x).\ \overline{k}\langle x\rangle$$

$$R = !fr(l,i,k).\ \text{if } null(l) \text{ then } \overline{k}\langle i\rangle \text{ else } \nu k'.\ \overline{fr}\langle cdr(l), i, k'\rangle.\ k'(x).\ \overline{k}\langle car(l)+x\rangle$$

Far from trivial due to passivation

Non-Bisimilar Examples

- "Tail-recursive" version of FoldL is <u>not</u> bisimilar to the original!
  - Because the former is "less faulty"
- Distributed O(log(n)) and O(n) power functions are <u>not</u> bisimilar
  - Ditto

More Non-Bisimilar Examples

- $n[\nu a.\nu b.P] \nsim_{\emptyset} n[\nu b.\nu a.P]$
  for $P = \overline{a}.\overline{b}.\overline{a}.\overline{v} \mid a.b.b.\overline{w}$
  - Because n may be passivated (and duplicated) <u>between</u> the two name creations
- $n[\nu a.(\overline{a} \mid a.\overline{w})] \nsim_{\emptyset} n[\nu a.\nu b.(\overline{a}.\overline{b} \mid a.b.\overline{w})]$
  - Because n may be passivated <u>between</u> the two communications

$$n[va.vb.P] \nsim_{\emptyset} n[vb.va.P]$$
$$\text{for } P = \overline{a}.\overline{b}.\overline{a}.\overline{v} \mid a.b.b.\overline{w}$$

- $n[va.vb.P] \rightarrow n[vb.P]$

  By duplication: $n_1[vb.P] | n_2[vb.P]$

  $\twoheadrightarrow n_1[\overline{a}.\overline{b}_1.\overline{a}.\overline{v} \mid a.b_1.b_1.\overline{w}] | n_2[\overline{a}.\overline{b}_2.\overline{a}.\overline{v} \mid a.b_2.b_2.\overline{w}]$

  $\twoheadrightarrow n_1[\overline{v} \mid b_1.\overline{w}] | n_2[\overline{a}.\overline{b}_2.\overline{a}.\overline{v} \mid b_2.b_2.\overline{w}] \not\rightarrow$
- $n[vb.va.P] \twoheadrightarrow n[P]$

  By duplication: $n_1[P] | n_2[P]$

  $= n_1[\overline{a}.\overline{b}.\overline{a}.\overline{v} \mid a.b.b.\overline{w}] | n_2[\overline{a}.\overline{b}.\overline{a}.\overline{v} \mid a.b.b.\overline{w}]$

  $\twoheadrightarrow n_1[\overline{v} \mid b.\overline{w}] | n_2[\overline{a}.\overline{b}.\overline{a}.\overline{v} \mid b.b.\overline{w}]$

  $\twoheadrightarrow n_1[\overline{v} \mid \overline{w}] | n_2[\overline{a}.\overline{b}.\overline{a}.\overline{v} \mid b.\overline{w}]$

$$n[\nu a.(\overline{a} \mid a.\overline{w})] \not\approx_{\emptyset} n[\nu a.\nu b.(\overline{a}.\overline{b} \mid a.b.\overline{w})]$$

- $n[\nu a.\nu b.(\overline{a}.\overline{b} \mid a.b.\overline{w})] \twoheadrightarrow n[\overline{a}.\overline{b} \mid a.b.\overline{w}]$
  By duplication: $n_1[\overline{a}.\overline{b} \mid a.b.\overline{w}] \mid n_2[\overline{a}.\overline{b} \mid a.b.\overline{w}]$
  $\twoheadrightarrow n_1[\overline{b} \mid a.b.\overline{w}] \mid n_2[\overline{a}.\overline{b} \mid b.\overline{w}]$
  By failures: $n_1[\overline{b} \mid a.b.\overline{w}]$ or $n_2[\overline{a}.\overline{b} \mid b.\overline{w}]$
- $n[\nu a.(\overline{a} \mid a.\overline{w})] \rightarrow n[\overline{a} \mid a.\overline{w}]$
  By duplication: $n_1[\overline{a} \mid a.\overline{w}] \mid n_2[\overline{a} \mid a.\overline{w}]$
  $\twoheadrightarrow n_1[a.\overline{w}] \mid n_2[\overline{a} \mid \overline{w}]$
  By failures: $n_1[a.\overline{w}]$ or $n_2[\overline{a} \mid \overline{w}]$

Conclusion

Bisimilarity of processes with passivation and name creation is tricky (but interesting)

Other equivalences equate previous examples:

- **Simulation equivalence (deadlock insensitive)**
- **Testing equivalence (linear-time; harder proof)**