Theory and Models of the π-Calculus using FMG

Murdoch J. Gabbay, November 2002

Introduction

The subject of this talk is getting rid of infinities and side conditions in the transition system of the π-calculus. For example:

$$\nu n.\overline{a}n.\overline{a}n \overset{\overline{a}n'}{\rightarrow}{}' \ \overline{a}n \qquad \text{any } n' \neq a$$

$$ax.xz \overset{ay}{\rightarrow}{}' \ yz \qquad \text{any } y$$

Morally there are just three transitions here: output of fresh n', input of a, and input of fresh y. *Actually* there is an infinity of inputs.

Concerning side conditions, the inductive definition of π-calculus transitions is full of them.

The π-calculus using FMG

Standard notion of a Labelled Transition System (LTS) is

$$\to \subseteq X \times L \times X,$$

for X a set of states and L a set of labels. Let an **LTS with binding** (LTSB) be

$$\to \subseteq X \times [\mathbb{A}](L \times X).$$

For Z arbitrary, $[\mathbb{A}]Z$ is the well-known $\mathbb{A}$-abstraction set, as implemented for example in $\mathrm{FreshML}$. Elements $\hat{z} : [\mathbb{A}]Z$ are like elements of an abstract datatype; secretly they are pairs $\langle a, z\rangle$ of a 'bound atom' a and a 'body' z. However, to get at the body we must provide the a. This is **concretion** $@$, $\hat{z}$ is secretly $\langle a, \hat{z}@a\rangle$ for fresh a (not included, like batteries).

The π-calculus using FMG

So $\langle x, [a]\langle l, x'\rangle\rangle \in\rightarrow$ is like a transition which generates a fresh name, but it does not concretely appear in the transition because it's bound. We pass around this abstract object and if eventually we need access to l and x' we must provide a fresh name a for the bound atom and open out the abstraction using concretion.

By convention we write LTSB transitions as follows:

$$x \overset{\nu a.l}{\rightarrow} x'.$$

An LTSB for the π-calculus, version I

(Tau)

$$\forall P.\, \text{И} z.\, \tau.P \xrightarrow{\nu z.\tau} P$$

(Out)

$$\forall x, y, P.\, \text{И} z.\, \overline{x}y.P \xrightarrow{\nu z.\overline{x}y} P$$

(In)

$$\forall x, y.\, \text{И} n.\, \forall P.\, x[n]P \xrightarrow{\nu n.xy} P\{y/n\}$$

(Par1)

$$\forall P_1, P_2.\, \text{И} z.\, \forall \mu, Q_1.\, \frac{P_1 \xrightarrow{\nu z.\mu} Q_1}{P_1 \mid P_2 \xrightarrow{\nu z.\mu} Q_1 \mid P_2}$$

(Close1)

$$\forall P_1, P_2, x.\, \text{И} y.\, \forall Q_1, Q_2.\, \text{И} z.\, \frac{P_1 \xrightarrow{\nu y.\overline{x}y} Q_1,\ P_2 \xrightarrow{\nu z.xy} Q_2}{P_1 \mid P_2 \xrightarrow{\nu z.\tau} \nu[y](Q_1 \mid Q_2)}$$

(Com1)

$$\forall P_1, P_2, x, y, Q_1, Q_2.\, \text{И} z.\, \frac{P_1 \xrightarrow{\nu z.\overline{x}y} Q_1,\ P_2 \xrightarrow{\nu z.xy} Q_2}{P_1 \mid P_2 \xrightarrow{\nu z.\tau} Q_1 \mid Q_2}$$

(Open)

$$\forall x.\, \text{И} y.\, \forall P, Q.\, \text{И} z.\, \frac{P \xrightarrow{\nu z.\overline{x}y} Q}{\nu[y]P \xrightarrow{\nu y.\overline{x}y} Q}$$

(Res)

$$\forall \hat{P}.\, \text{И} z.\, \forall \hat{Q}, \mu.\, \text{И} y.\, \frac{\hat{P}@y \xrightarrow{\nu z.\mu} \hat{Q}@y}{\nu\hat{P} \xrightarrow{\nu z.\mu} \nu\hat{Q}}$$

(Rep)

$$\forall P.\, \text{И} z.\, \forall \mu, Q.\, \frac{!P \mid P \xrightarrow{\nu z.\mu} Q}{!P \xrightarrow{\nu z.\mu} Q}$$

Example transitions

$$\overline{x}y.\overline{x}y \overset{\nu n.\overline{x}y}{\rightarrow} \overline{x}y$$

from $\mathbf{(Out)}$. Also

$$x[n].x[n] \overset{\nu n'.xy}{\rightarrow} x[y]$$

from $\mathbf{(In)}$.

A single transition corresponds to the transitions

$$\nu n.\overline{a}n.\overline{a}n \overset{\overline{a}n'}{\rightarrow}{}_{'} \overline{a}n' \qquad \text{any } n' \neq a$$

previously mentioned, namely

$$\nu[n]\overline{a}n.\overline{a}n \overset{\nu n'.\overline{a}n'}{\rightarrow} \overline{a}n'.$$

This is one transition, n' is bound. Let's use proper terminology since this is object-level binding: n' *is not in the support* of the transition above (reserve 'bound' for meta-level!). That deals with that infinity.

Example transitions

$$\nu[n]\overline{a}n.\overline{a}n \overset{\nu n'.\overline{a}n'}{\rightarrow} \overline{a}n'.$$

Let's choose some fresh atom for the bound atom in this transition. In fact choose $n' = n$: it need only be fresh for the body of the abstraction $[n']\langle\overline{a}n', \overline{a}n'\rangle$, which has support $\{a\}$.

By $(\mathbf{In})$,

$$a[n].P \overset{\nu z.an}{\rightarrow} P[n/n] = P.$$

Here z is a dummy binder: it is bound in the abstraction but does not occur in the body, so it's vacuous. Recall we have

$$\nu[n]\overline{a}n.\overline{a}n \overset{\nu n.\overline{a}n}{\rightarrow} \overline{a}n$$

So from $(\mathbf{Close1})$

$$a[n].P \mid \nu[n]\overline{a}n.\overline{a}n \overset{\nu z.\tau}{\rightarrow} \nu[n](P \mid \overline{a}n).$$

The other infinity

Recall that $ax.ax \xrightarrow{ay}{}' \, ay$ enjoys an infinity of transitions even though morally there are just two: input of a and input of fresh n. The corresponding transition

$$a[n].\overline{a}n \xrightarrow{\nu n'.ay} \overline{a}y$$

displays the same problem—at least, it's a problem if you want to build models of behaviour of processes. So we consider a 'minimised' transition system:

An LTSB for the π-calculus, version II

(1) $$\forall P, Q, x, y, z.\ P \overset{\nu z.\overline{x}y}{\longrightarrow} Q \implies P \underset{m}{\overset{\nu z.\overline{x}y}{\longrightarrow}} Q$$

(2) $$\forall P, Q, z.\ P \overset{\nu z.\tau}{\longrightarrow} Q \implies P \underset{m}{\overset{\nu z.\tau}{\longrightarrow}} Q$$

(3) $$\forall P, Q, x, y, z.\ P \overset{\nu z.xy}{\longrightarrow} Q \implies P \underset{m}{\overset{\nu y.xy}{\longrightarrow}} Q$$

$\underset{m}{\longrightarrow}$ has an inductive definition as well:

An LTSB for the π-calculus, version II

(mOut) $$\forall x, y, P.\, \text{И} z.\, \overline{x}y.P \xrightarrow[m]{\nu z.\overline{x}y} P$$

(mIn) $$\forall x.\, \text{И} n.\, \forall P, y.\, x[n]P \xrightarrow[m]{\nu y.xy} P\{y/n\}$$

(mPar1a) $$\forall P_1, P_2.\, \text{И} z.\, \forall \mu, Q_1.\, \frac{P_1 \xrightarrow[m]{\nu z.\mu} Q_1}{P_1 \mid P_2 \xrightarrow[m]{\nu z.\mu} Q_1 \mid P_2} \qquad \mu \text{ output or } \tau$$

(mPar1b) $$\forall P_1, P_2, x, y, Q_1, Q_2.\, \frac{P_1 \xrightarrow[m]{\nu y.xy} Q_1}{P_1 \mid P_2 \xrightarrow[m]{\nu y.xy} Q_1 \mid P_2}$$

(mClose1) $$\forall P_1, P_2, x.\, \text{И} y.\, \forall Q_1, Q_2.\, \frac{P_1 \xrightarrow[m]{\nu y.\overline{x}y} Q_1 \quad P_2 \xrightarrow[m]{\nu y.xy} Q_2}{P_1 \mid P_2 \xrightarrow[m]{\nu z.\tau} \nu[y](Q_1 \mid Q_2)}$$

(mCom1) $$\forall P_1, P_2, x, y, Q_1, Q_2.\, \text{И} z.\, \frac{P_1 \xrightarrow[m]{\nu z.\overline{x}y} Q_1 \quad P_2 \xrightarrow[m]{\nu y.xy} Q_2}{P_1 \mid P_2 \xrightarrow[m]{\nu z.\tau} Q_1 \mid Q_2} \qquad y \in PI(P_2, x, y, Q_2)$$

(mOpen) $$\forall x.\, \text{И} y.\, \forall P, Q.\, \text{И} z.\, \frac{P \xrightarrow[m]{\nu z.\overline{x}y} Q}{\nu[y]P \xrightarrow[m]{\nu y.\overline{x}y} Q}$$

Infinity vanishes

So both infinities vanish:

$$\nu n.\overline{a}n.\overline{a}n \overset{\overline{a}n'}{\longrightarrow}{}' \ \overline{a}n \qquad \text{any } n' \neq a$$

$$ax.xz \overset{ay}{\longrightarrow}{}' \ yz \qquad \text{any } y$$

$$\nu[n]\overline{a}n.\overline{a}n \underset{m}{\overset{\nu n.\overline{a}n}{\longrightarrow}} \overline{a}n$$

$$a[b].b[z] \underset{m}{\overset{\nu y.ay}{\longrightarrow}} y[z]$$

Here either $y = a$ or $y \neq a$, so this last expression describes a two-element set in $\underset{m}{\longrightarrow}$ whose elements we can write

$$a[b].b[z] \underset{m}{\overset{\nu a.aa}{\longrightarrow}} a[z]$$

$$a[b].b[z] \underset{m}{\overset{\nu b.ab}{\longrightarrow}} b[z]$$

(b is not in the support of $a[b].b[z]$.)

Name-regular

$\xrightarrow[m]{}$ has another property which seems to be quite important. It is **name-regular**:

$$P \xrightarrow[m]{\hat{\alpha}} \hat{Q} \wedge a\#P \implies a\#\hat{\alpha}, \hat{Q}.$$

where $a\#x$ means "a is not in the support of x".

Now we have a fighting chance of building models of processes: it is not hard to prove that $\xrightarrow[m]{}$ is finitely branching, and $\xrightarrow[m]{}$ is name-regular. The latter is intimitely related to the validity of the former. Name-regularity means that fresh names do not appear out of nowhere; either broadcast from a restriction or input from the environment.

Models

The remaining problem is that we do not have an LTS but an LTSB. If we are willing to consider 'model' to be an LTSB we can stop here—check bisimilarity of P with Q on-the-fly, generating a fresh name n for the abstractions when we go from P to $[n]\langle \mu, Q\rangle$ at each transition (and quotienting by structural equivalence).

Similar to taking representative transitions and that kind of thing, except that with abstractions we do not wed ourselves to particular representatives. FM gives us nicer semantics. It was designed to.

In order to statically create a concrete model of behaviour we need to convert the LTSB $\underset{m}{\longrightarrow}$ into some kind of LTS. We do this by unfolding the on-the-fly process. A theorem then states that if P is finite, the LTS modelling behaviours of P is finite. What we get is *much simpler* than HD-automata.

The labelled transition $\underset{dB}{\longrightarrow}$

Definition: Given name-regular LTSB $\underset{m}{\longrightarrow} \subseteq \Pi \times [\mathbb{A}]Act \times [\mathbb{A}]\Pi$, we construct

$$\underset{dB}{\longrightarrow} \subseteq ([\mathbb{L}]\Pi \times \mathbb{N}) \times [\mathbb{L}]Act \times ([\mathbb{L}]\Pi \times \mathbb{N})$$

defined by

$$\text{(4)} \qquad \langle p, i\rangle \overset{\alpha}{\underset{dB}{\longrightarrow}} \langle q, i+1\rangle \quad \overset{\text{def}}{\Leftrightarrow} \quad \text{И}u : \mathbb{L}.\ p@u \overset{\nu u_{i+1}.\alpha@u}{\underset{m}{\longrightarrow}} q@u.$$

Here u_j is the jth element of the list $u : \mathbb{L}$. I said this “unfolds the on-the-fly process”. The index i means every transition takes place at a stage i, we use u_{i+1} as the fresh name for the transition to stage $i+1$. Name-regularity means we can choose the list $u : \mathbb{L}$ *first*, no other names will be created or enter from the environment to interfere with it.

Models of behaviour

The model of behaviour of some P is the $\underset{dB}{\rightarrow}$ evolutions of P quotiented by structural congruence, call it $M(P)$. It is a theorem that if P is finitary, $M(P)$ is finite. There is a notion of bisimilarity of $M(P)$ and $M(Q)$ which is not quite bisimilarity of rooted graphs; we must take account of the stages.

The nicest thing about all this is that $[\mathbb{A}]-$ and $[\mathbb{L}]-$ distribute up and down through the structure of the graph. For example $[\mathbb{L}](X \times Y) \cong [\mathbb{L}]X \times [\mathbb{L}]Y$. Thus we can think of these graphs of behaviours in name-carrying and nameless forms, depending as where we put the abstractions and whether we unpack them with a concrete fresh $u : \mathbb{L}$.

We already used this, writing P above (of type Π)...

Playing with abstractions

…taking for granted we can pull abstraction up to top level (whatever that may be), unpack it, and look at a node P inside. For example the following are equivalent:

$$\mathcal{P}(([\mathbb{L}]\Pi) \times \mathbb{N} \times ([\mathbb{L}]Act) \times ([\mathbb{L}]\Pi) \times \mathbb{N})$$
$$\mathcal{P}([\mathbb{L}]\big(\mathbb{L} \times \mathbb{N} \times Act \times \mathbb{L} \times \mathbb{N}\big))$$
$$[\mathbb{L}]\mathcal{P}(\mathbb{L} \times \mathbb{N} \times Act \times \mathbb{L} \times \mathbb{N}).$$

Because $[\mathbb{L}](X \times Y) \cong [\mathbb{L}]X \times [\mathbb{L}]Y$, and $[\mathbb{L}]\mathbb{N} \cong \mathbb{N}$, and $\mathcal{P}([\mathbb{L}]X) \cong [\mathbb{L}]\mathcal{P}(X)$.

Bisimilarity of staged graphs with abstractions

Two graphs are bisimilar when there is a relation $\simeq$ between the nodes and assignement $f\colon \simeq \to \mathbb{L} \times \mathbb{L}$ such that whenever $P, i \simeq Q, j$ then, writing $\langle v, w \rangle$ for $f(P, i, Q, j)$,

(5) $\quad P, 0 \simeq Q, j \implies v = u$

(6) $\quad \forall P', i', \alpha.\ P, i \overset{\alpha}{\to} P', i' \implies \exists Q', j'.\ Q, j \overset{(v\ w)\cdot\alpha}{\to} Q', j' \wedge$

$$f(P', i', Q', j') = \langle cut(i, i', v), cut(j, j', w) \rangle.$$

$$cut(i, i+1, v) = v$$

$i' = i + 1,$ no change.

$$cut(3, 1, [v_1, v_2, v_3, v_4, v_5, \ldots]) = [v_1, v_4, v_5, \ldots]$$

$i' < i + 1,$ cut i' to $i + 1$ exclusive

$$cut(1, 4, [v_1, v_2, v_3, v_4, v_5, \ldots]) = [v_1, a_2, a_3, v_2, v_3, \ldots]$$

$i' > i + 1,$ pad in $i + 1 - i'$ fresh atoms at i.

A simple example

(7) $$\bullet, 0 \overset{\overline{x}u_1}{\rightarrow} \bullet', 1 \overset{\overline{x}u_2}{\rightarrow} \bullet, 2 \overset{\overline{x}u_3}{\rightarrow} \bullet', 3 \rightarrow \ldots$$

is bisimilar to

(8) $$\begin{tikzcd}\bullet, 0 \arrow[r, shift left, "\overline{x}u_1"] & \bullet', 1 \arrow[l, shift left, "\overline{x}u_2"]\end{tikzcd}$$

Axioms of FMG

$\pi, \pi' : P_{\mathbb{A}}$ range over all permutations, $x : X$ over all elements of X, X over all types, $a : \mathbb{A}$ over all atoms.

(9) $\pi \cdot a = \pi(a)$

(10) $\pi \cdot \pi' \cdot x = (\pi \circ \pi') \cdot x$

(11) $\mathbf{Id} \cdot x = x$

(12) $\pi \cdot f(x) = (\pi \cdot f)(\pi \cdot x)$

(13) $\pi \cdot c = c$ c a closed term

(14) $\{A \in \mathbb{A}^{\mathcal{S}} \mid A \; supports \; x\}$ has a least element