

Introduction to calculus for mobile systems

A. Dorman

Journée Vérité et Preuve

8 novembre 2010

Concurrency

Multiple agents that interact among each other independently from one another.

Like mathematicians and philosopher's meeting one-on-one, by profession.

- Hilbert can meet Poincaré or Russell;
- Poincaré can also meet Dedekind;
- Russel can meet lots of people, among which Wittgenstein.

Mobility

Agents can modify their interaction structure.

- Hilbert can meet Poincaré or Russell;
- Poincaré can also meet Dedekind;
- Russel can meet lots of people, among which Wittgenstein.

Now, imagine meeting *Hilbert* magically turns you into a *mathematician*. If Russell decides to have diner with him instead of his beloved student, he becomes *one*. And can now meet Dedekind!

Models for Mobile processes

They should be, as usual

- simple
- expressive
- formal
- provide reasoning techniques

Like λ -calculus for sequential computation. But different.

Because **concurrent computation** is usually *interactive*, *non-terminating* and *non-confluent*.

Let

- Math be capacity of talking about math
- Philo of talking about philosophy,
- Learn be the capacity of learning something,
- Teach of teaching something.

Our truth seekers can be describes as:

Poincaré: Math & Learn(Truth).Truth

Dedekind: Math & Learn(Truth).Truth

Russell: Philo & Learn(Truth).Truth

Hilbert: Math & Philo & Teach(Math)

Poincaré: Math & Learn(Truth).Truth
Dedekind: Math & Learn(Truth).Truth
Russell: Philo & Learn(Truth).Truth
Hilbert: Math & Philo & Teach(Math)

What can happen?

Poincaré, Hilbert and Dedekind can have a party. But poor Russell won't be invited.

Unless...

Poincaré: Math & Learn(Truth).Truth
Dedekind: Math & Learn(Truth).Truth
Russell: Philo & Learn(Truth).Truth
Hilbert: Math & Philo & Teach(Math)

What can happen?

Poincaré, Hilbert and Dedekind can have a party. But poor Russell won't be invited.

Unless...

he learns math from Hilbert!

Poincaré: Math & Learn(Truth).Truth
 Dedekind: Math & Learn(Truth).Truth
 Russell: Philo & Learn(Truth).Truth
 Hilbert: Math & Philo & Teach(Math)

$\underbrace{\text{Philo \& Learn(Truth).Truth}}_{\text{Russell}} \mid \underbrace{\text{Math \& Philo \& Teach(Math)}}_{\text{Hilbert}}$

$\rightarrow \underbrace{\text{Philo \& Math}}_{\text{Russell}} \mid \underbrace{\text{Math \& Philo}}_{\text{Hilbert}}$

Poincaré:	Math & Learn(Truth).Truth
Dedekind:	Math & Learn(Truth).Truth
Russell:	Philo & Learn(Truth).Truth
Hilbert:	Math & Philo & Teach(Math)

Now imagine at the philosophers meeting arrived Wittgenstein:

Philo & !Teach(UltimateTruth).

Poincaré:	Math & Learn(Truth).Truth
Dedekind:	Math & Learn(Truth).Truth
Russell:	Philo & Learn(Truth).Truth
Hilbert:	Math & Philo & Teach(Math)
Wittgenstein:	Philo & !Teach(UltimateTruth)

Then, things can happen as before. Unless... if Russell becomes crazy about Wittgy,

$\underbrace{\text{Philo \& Learn(Truth).Truth}}_{\text{Russell}}$	$\underbrace{\text{Math \& Philo \& Teach(Math)}}_{\text{Hilbert}}$	$\underbrace{\text{Math \& Philo \& !Teach(UltimateTruth)}}_{\text{Wittgenstein}}$
→ $\underbrace{\text{Philo \& UltimateTruth}}_{\text{Russell}}$	$\underbrace{\text{Math \& Philo \& Teach(Math)}}_{\text{Hilbert}}$	$\underbrace{\text{Math \& Philo \& !Teach(UltimateTruth)}}_{\text{Wittgenstein}}$

He will never be able to meet Poincaré anymore!

Finally, some philosophers want to differentiate *esoteric* teaching from *exoteric*.

Lets see what **Pythagoras** is capable of:

$$\text{Teach}(\mathfrak{Beauty}) \ \& \ \text{Esoterikal}[\sqrt{2}](\text{Master.Teach}(\sqrt{2}))$$

in which case Hippasis of Metaponte is capable of

$$\text{Learn}(\mathfrak{Truth}) \ \& \ \text{Disciple.Learn}(\mathfrak{Secret})$$

but the neighbor's son, who can only $\text{Learn}(\mathfrak{Truth})$, will never find out about *irrationality*.

To summarize, we want to be able to describe:

- Communication between agents;
- Independence (parallelism);
- Sequentiality for agents (evolution/mobility);
- Possibility of unbounded repetition of actions;
- Secrecy of certain communications;
- Choice.

Lets be serious now.

- Let $\mathcal{N} = a, \bar{a}, b, \bar{b}, c, \bar{c}, \dots$ be a countable set of names;
- Prefixes:

$$\pi ::= \bar{x}y \mid x(z) \mid \tau \mid [x = y]\pi$$

- Processes and summations:

$$P ::= M \mid P|P' \mid \nu z P \mid !P$$

$$M ::= 0 \mid \pi.P \mid M + M'$$

- Let $\mathcal{N} = a, \bar{a}, b, \bar{b}, c, \bar{c}, \dots$ be a countable set of names;
- Prefixes:

$$\pi ::= \bar{x}y \mid x(z) \mid \tau \mid [x = y]\pi$$

- Processes and summations:

$$P ::= M \mid P|P' \mid \nu z P \mid !P$$

$$M ::= 0 \mid \pi.P \mid M + M'$$

- Let $\mathcal{N} = a, \bar{a}, b, \bar{b}, c, \bar{c}, \dots$ be a countable set of names;
- Prefixes:

$$\pi ::= \bar{x}y \mid x(z) \mid \tau \mid [x = y]\pi$$

- Processes and summations:

$$P ::= M \mid P|P' \mid \nu z P \mid !P$$

$$M ::= 0 \mid \pi.P \mid M + M'$$

We don't want: $\nu z P + !Q + (R|R')$

unless each is triggered by an action: the *choice* of the action determines the choice of the branch.

Reduction:

$$\bar{x}y.P + M \mid x(z).Q + N \longrightarrow P \mid Q\{y/z\}$$

$$\tau.P + M \longrightarrow P$$

Example:

$$x(z).\bar{z}a.0 + \nu z\ z(z).0 \mid \bar{x}w.\bar{y}w.0 \mid y(v).v(u).0 + y(u).0$$

Example:

$$\textcolor{red}{x}(z).\bar{z}a.0 + \nu z\ z(z).0 \mid \bar{\textcolor{red}{x}}w.\bar{y}w.0 \mid y(\nu).\nu(u).0 + y(u).0$$

Example:

$$\begin{aligned} & x(z).\bar{z}a.0 + \nu z\, z(z).0 \mid \bar{x}w.\bar{y}w.0 \mid y(v).v(u).0 + y(u).0 \\ \longrightarrow & \bar{w}a.0 \mid \bar{y}w.0 \mid y(v).v(u).0 + y(u).0 \end{aligned}$$

Example:

$$\begin{aligned} & x(z).\bar{z}a.0 + \nu z\, z(z).0 \mid \bar{x}w.\bar{y}w.0 \mid y(v).v(u).0 + y(u).0 \\ \longrightarrow & \bar{w}a.0 \mid \bar{y}w.0 \mid y(v).v(u).0 + y(u).0 \end{aligned}$$

Example:

$$\begin{aligned} & x(z).\bar{z}a.0 + \nu z\ z(z).0 \mid \bar{x}w.\bar{y}w.0 \mid y(v).v(u).0 + y(u).0 \\ \longrightarrow & \bar{w}a.0 \mid \bar{y}w.0 \mid y(v).v(u).0 + y(u).0 \\ \longrightarrow & \bar{w}a.0 \mid 0 \mid w(u).0 \end{aligned}$$

Example:

$$x(z).\bar{z}a.0 + \nu z z(z).0 \mid \bar{x}w.\bar{y}w.0 \mid y(v).v(u).0 + y(u).0$$

$$\longrightarrow \bar{w}a.0 \mid \bar{y}w.0 \mid y(v).v(u).0 + y(u).0$$

$$\longrightarrow \bar{w}a.0 \mid 0 \mid w(u).0$$

Example:

$$\begin{aligned} & x(z).\bar{z}a.0 + \nu z\ z(z).0 \mid \bar{x}w.\bar{y}w.0 \mid y(v).v(u).0 + y(u).0 \\ \longrightarrow & \bar{w}a.0 \mid \bar{y}w.0 \mid y(v).v(u).0 + y(u).0 \\ \longrightarrow & \bar{w}a.0 \mid 0 \mid w(u).0 \\ \longrightarrow & 0 \mid 0 \mid 0 \end{aligned}$$

Example:

$$x(z).\bar{z}a.0 + \nu z z(z).0 \mid \bar{x}w.\bar{y}w.0 \mid y(v).v(u).0 + y(u).0$$

$$\longrightarrow \bar{w}a.0 \mid \bar{y}w.0 \mid y(v).v(u).0 + y(u).0$$

$$\longrightarrow \bar{w}a.0 \mid 0 \mid w(u).0$$

$$\longrightarrow 0 \mid 0 \mid 0$$

$$\longrightarrow 0$$

Structural congruence

Sc-mat:	$[x = x]\pi.P$	$\equiv$	$\pi.P$
Sum associativity:	$P_1 + (P_2 + P_3)$	$\equiv$	$(P_1 + P_2) + P_3$
Sum commutativity:	$P_1 + P_2$	$\equiv$	$P_2 + P_1$
Sum inaction:	$P + 0$	$\equiv$	P
Compos. associativity:	$P_1 \mid (P_2 \mid P_3)$	$\equiv$	$(P_1 \mid P_2) \mid P_3$
Compos. commutativity:	$P_1 \mid P_2$	$\equiv$	$P_2 \mid P_1$
Compos. inaction:	$P \mid 0$	$\equiv$	P
Restrict. commutativity:	$\nu V \nu W P$	$\equiv$	$\nu W \nu V P$
Restrict. inaction:	$\nu z 0$	$\equiv$	0
Restrict./compos.:	$\nu z (P_1 \mid P_2)$	$\equiv$	$P_1 \mid \nu z P_2$, if $z \notin \text{fn}(P_1)$
Sc-rep:	$!P$	$\equiv$	$P \mid !P$

$$\overline{\bar{x}y.P \mid x(z).Q \mid R \longrightarrow P \mid Q\{y/z\} \mid R} \quad (\pi\text{-red})$$

$$\overline{\tau.P \longrightarrow P} \quad (\tau\text{-red})$$

$$\frac{P \longrightarrow Q}{P \mid R \longrightarrow Q \mid R} \quad (\text{Parr.})$$

$$\frac{P \longrightarrow Q}{(\nu x)P \longrightarrow (\nu x)Q} \quad (\text{Restr.})$$

$$\frac{P' \equiv P \longrightarrow Q \equiv Q'}{P' \longrightarrow Q'} \quad (\text{Struct.})$$

- Behavioral equivalence
- Polyadicity
- Asynchronous π -calculus
- Local and private π -calculus
- Higher Order π -calculus
- ...

- We want to reason about **behavior** of systems more than about “results” (the *normal* form of a π -term. . .).
- Main concern in concurrency theory: **observable equivalence**. Here, through **bisimulation**.
 - Connected to non-well-founded sets, domain theory, modal logic, final coalgebras (says Sangiorgi...)
 - Induces a nice framework: *event structures*

Actions

Four types: $\bar{x}y$ $x(y)$ $\bar{x}(y)$ τ .

Labeled transition

Evolution of a process due to a given kind of action.

$$x(z).\bar{z}y.0 \xrightarrow{x(a)} \bar{a}y.0 \xrightarrow{\bar{a}y} 0 \quad x(z).P \mid \bar{x}y.Q \xrightarrow{\tau} P \mid Q\{y/z\}$$

$$\text{If } P \xrightarrow{\bar{x}z} P', \text{ then } \nu z P \xrightarrow{\bar{x}(z)} P' \dots$$

Strong bisimulation

Relation $\sim^*$ s.t. if $P \sim^* Q$ then

- if $P \downarrow_\mu$, then $Q \downarrow_\mu$;
- $P \xrightarrow{\alpha} P'$ implies $Q \xrightarrow{\alpha} Q'$ for some Q' and $P' \sim^* Q'$;
- vice-versa.

Strong bisimilarity

It is the union of all strong bisimulation, e.g. $P \sim Q$ if there exists $\sim^*$ s.t. $P \sim^* Q$.

Strong full bisimilarity

P and Q are *strong full bisimilar*, $P \sim^c Q$ if $P\sigma \sim Q\sigma$ for every substitution σ .

In directed graphs

$\mathcal{G}$, nodes are processes and arrows are given by the transition relations. A play begins with two tokens on a node of each graph $\llbracket P \rrbracket$ and $\llbracket Q \rrbracket$.

P1 can move any of the two tokens along one edge.

P2 responds by moving the other token along an outgoing edge with the same label.

If Player 2 can't move anymore, he loses.

The second player has a winning strategy iff the processes are strong bisimilar.

$$\bar{z} \mid a \sim \bar{z}.a + a.\bar{z}$$

but

$$x(z).(\bar{z} \mid a) \not\sim x(z).(\bar{z}.a + a.\bar{z})$$

Strong full bisimilarity is a **congruence**.

$$\bar{z} \mid a \sim \bar{z}.a + a.\bar{z}$$

but

$$x(z).(\bar{z} \mid a) \not\sim x(z).(\bar{z}.a + a.\bar{z})$$

Strong full bisimilarity is a **congruence**.

$$\bar{z} \mid a \sim \bar{z}.a + a.\bar{z}$$

but

$$x(z).(\bar{z} \mid a) \not\sim x(z).(\bar{z}.a + a.\bar{z})$$

because one of the names received via x can be a . The following continuations: $\bar{a} \mid a$ and $\bar{a}.a + a.\bar{a}$ don't both have a τ transition.

Strong full bisimilarity is a **congruence**.

Asynchronous communications

Concurrent system in which the act of sending and the act of receiving are separate.

For π -calculus, this can be modeled by only allowing output prefixes to guard 0.

$$\begin{aligned} P &::= \bar{x}y.0 \mid M \mid P|P' \mid \nu z P \mid !P \\ M &::= 0 \mid x(z).P \mid \tau.P \mid M + M' \end{aligned}$$

y is considered to be sent when $\bar{x}.y.0$ becomes unguarded, and received when the reduction takes place.

Asynchronous π -calculus is expressive enough to express synchronize communications.

Rather simple (just name by name substitution), but

- encodes data structures
- encodes functions (λ -calculus...)
- encodes higher order π -calculus
- encoded by asynchronous π -calculus
- encoding polyadic communications with 2-adic
- ...

The purpose is that at the end of the meetings Vérité et Preuve, we all be of the form:

$\text{!Math} \ \& \ \text{!Philo} \ \& \ \text{understand}(\text{Truth}) \ \& \\ \text{understand}(\text{Proofs}) \ \& \ \text{!Learn}(\text{Stuff})$

Merci