Evolved Logic: the next step

Murdoch J Gabbay
Joint work with Joe Wells

Tel Aviv University, Israel 28/5/2006

Process calculi

There is a plethora of so-called ‘process calculi’ out there.

The π-calculus. The ambient calculus. The spi-calculus. CCS. Brane calculus. Fusion calculus.

They are used as models of concurrency, biological systems, parallelism, mobility, communications protocols, security, and also unstructured datatypes and XML . . . and so on.

Millions of systems? Perhaps. Thousands, certainly.

Process calculi

Notably (for my understanding) are the π-calculus which started it all, and also a bright idea by Cardelli: build a process calculus with a dedicated logic for reasoning about it (ambient calculus — ambient logic).

My impression is that this provoked an explosion of similar systems-with-logics. Hundreds, and climbing.

What is a process calculus?

. . . and how does a process calculus differ from any other calculus, e.g. the λ-calculus?

I propose: a process calculus has a multiplicative or separating conjunction. In other terminology this is a parallel composition. Or, as I like to think of it, process calculi have geography.

Simple example:

A simple process calculus

$$P ::= 0 \quad | \quad x.P \quad | \quad \overline{x}.P \quad | \quad P|P.$$

Intuitively:

- 0 is the nil process which does nothing and takes up no space.
- $P|Q$ is P and Q placed side-by-side. This has geography which is the geography of P, placed next to the geography of Q.
- The calculus has to do something aside from geography, of course!
- $x.P$ is input x, then do P.
- $\overline{x}.P$ is output x, then do P.

A simple process calculus

$$P ::= 0 \quad | \quad x.P \quad | \quad \overline{x}.P \quad | \quad P|P.$$

If we are feeling clever we can add more to the syntax, but actually that's not so important.

Reduction rules give operational semantics, which may exploit the geography. E.g. a reduction rule

$$x.P \quad | \quad \overline{x}.Q \quad \Longrightarrow \quad P \quad | \quad Q$$

uses the fact that we can 'split the world into two parts'.

This is separation.

Separation logic

This is a Hoare-style logic for reasoning about properties of programs. It came out of a heap semantics in which programs manipulate memory. Memory has a notion of geography given by splitting the heap into two smaller heaps.

The distinguishing feature of this logic, and this interests us here, is the two notions of conjunction:

Separating or multiplicative conjunction and implication

$$\frac{P, Q, \Gamma \vdash \Delta}{P \otimes Q, \Gamma \vdash \Delta}\,(\otimes L) \qquad \frac{\Gamma \vdash \Delta, P \quad \Gamma' \vdash \Delta', Q}{\Gamma, \Gamma' \vdash \Delta, \Delta', P \otimes Q}\,(\otimes R)$$

$$\frac{Q, \Gamma \vdash \Delta \quad \Gamma' \vdash \Delta', P}{P \multimap Q, \Gamma, \Gamma' \vdash \Delta, \Delta'}\,(\multimap L) \qquad \frac{P, \Gamma \vdash \Delta, Q}{\Gamma \vdash \Delta, P \multimap Q}\,(\multimap R)$$

Geography is modelled by splitting the contexts, e.g. in $(\otimes R)$ we can only use Γ to prove P above the line, not Γ'!

Separating or multiplicative conjunction and implication

Ambient logic, for example, has a separating conjunction whose semantics is intensional; split the process term along a $|$.

‘Logical’ or additive conjunction and implication

We still want to say ‘if P then Q’. This has no notion of geography, it’s just either true or false.

$$\frac{P, Q, \Gamma \vdash \Delta}{P \wedge Q, \Gamma \vdash \Delta}\,(\wedge L) \qquad \frac{\Gamma \vdash \Delta, P \quad \Gamma \vdash \Delta, Q}{\Gamma \vdash \Delta, P \wedge Q}\,(\wedge R)$$

$$\frac{Q, \Gamma \vdash \Delta \quad \Gamma \vdash \Delta, P}{P \supset Q, \Gamma \vdash \Delta}\,(\supset L) \qquad \frac{P, \Gamma \vdash \Delta, Q}{\Gamma \vdash \Delta, P \supset Q}\,(\supset R)$$

Question:

So there are a zillion systems out there with geography.

What do we do when we see a zillion things?

Find out what they all have in common and call it . . .

LOGIC!

Evolved logic

A logic for fast prototyping of process calculi, and also for reasoning about them.

Joe Wells et al . . .

. . . had already got a major project up and running on precisely this topic called Polystar. This is a fast prototyping system for process calculi but it doesn't have a very standard logic attached.

In other words, the system needs a front end which abstracts from the computational content.

The model:

Kripke structures — that’s trees.

Simple. Standard. Well-known.

The syntax

$$\begin{aligned}\phi ::= & \bot \mid \phi \wedge \phi \mid \phi \supset \phi \mid \\ & 1 \mid \phi \otimes \phi \mid \phi \multimap \phi \mid \\ & \bigcirc w \mid t.\phi \mid \Box \phi \mid \\ & \forall w.\phi.\end{aligned}$$

Intuitions

A behaviour is a subtree of the Kripke structure — we think of it as a slightly abstract notion of syntax of process term; the only thing we assume of the process term is geography, which is very nicely modelled by the Kripke structure's tree structure.

The semantics of a predicate ϕ is a behaviour.

Intuitions

- $\bot$ is absurd, the empty tree without even a root.
- $\phi \wedge \psi$ is the empty tree unless ϕ and ψ are equal, in which case $\phi \wedge \psi = \phi = \psi$.
- 1 is the trivial behaviour, $\phi \otimes \psi$ is the disjoint composite of ϕ and ψ where this is defined, otherwise it is the empty behaviour.

Intuitions

- $\bigcirc w$ is nondeterministically a behaviour rooted at w.
- $\Box\phi$ is nondeterministically a behaviour isomorphic to ϕ.
- $x.\phi$ is a behaviour which is an x transition leading to ϕ.

Intuitions

- $\forall w.\phi$ is a behaviour which is equal to ϕ for all worlds w.
- @ is the root of the universe and $\bigcirc$@ is nondeterministically a behaviour at the root.

Examples

An easy one:

$\phi \otimes \phi'$ looks just like $P|Q$.

Also $1 \otimes \phi$ contains the same behaviours as ϕ and $\phi \otimes 1$, and so on.

(Go on, ask me to draw it out on the board.)

Examples

$x.(\bigcirc w)$ is a behaviour which makes an x-transition to a behaviour at w.

$x.(\bigcirc w) \wedge \bigcirc @$ is a behaviour which makes an x-transition from the root, to w. Write this $@ \stackrel{x}{\longrightarrow} w$.

Examples

$\Box\phi$ is a behaviour isomorphic to ϕ.

$\Box\phi \wedge \bigcirc w$ is a behaviour isomorphic to ϕ which is equal to a behaviour rooted at w.

Write

$$\phi \downarrow w \qquad \text{for} \qquad \Box\phi \wedge \bigcirc w.$$

The reduction rule

The reduction rule

$$x.P \mid \overline{x}.Q \implies P \mid Q$$

may be encoded as

$$\forall w, w'.((@ \xrightarrow{x} w) \otimes (@ \xrightarrow{\overline{x}} w')) \supset (\bigcirc w \downarrow @ \otimes \bigcirc w' \downarrow @).$$

Conclusions

Evolved logic seems to combine many interesting elements:

- Separation (what I like to call ‘geography’) captures an essential feature of process calculi.
- Traditional Kripke semantics; everything else goes into the accessibility relation.
- Nondeterministic predicates like $\bigcirc w$ and modalities like $\Box\phi$.