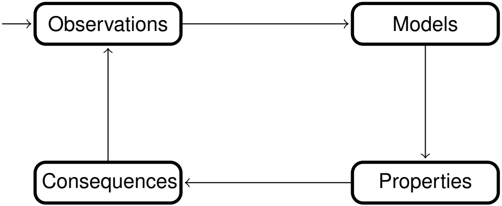
# Bunched Resource Process Calculus

Gabrielle Anderson, David Pym

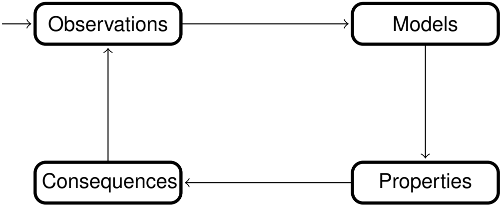
University College London, U.K.
gabrielle.anderson@ucl.ac.uk, d.pym@ucl.ac.uk

Tuesday 14th April, 2015

# Systems Modelling



# Systems Modelling




- A sound model: captures just those aspects that are relevant to the questions that model should address.

# Dynamical Systems

- Applied mathematics modelling: typically described by difference equations concerning a system's evolution from on step to the next.
- An flow operator is derived that completely describes the behaviour of the system.
- Large and/or complex systems: models are rarely susceptible to exact solution

# Dynamical Systems Modelling

- Systems can be modelled using:
  - Processes, which describe the system's dynamics and behaviour,
  - Resources, which describe the building blocks of the system, and
  - Locations, which describe the distribution of processes and resources.

# Processes

- Provide the dynamics of the system.
- Describe how the model progresses.
- Have algebraic structure, including sequential, non-determinstic, and concurrent composition.

# Resources

- Conceptually, resource elements can be combined and compared.
- Properties characterised by a (preordered) commutative partial resource monoid.

$$\mathbf{R} = (\mathbf{R}, \sqsubseteq, \circ, e).$$

- Examples: the monoid of natural numbers with addition (with unit 0, ordered by $\leq$, computer memory (as in separation logic), and Petri nets.

# Locations

- Places around which resources are distributed.
- The places have connections between them.
- Leading examples are directed graphs and topological constructions

# Environment

- (Complex) aspects of the system which we needn't model in detail.
- External events which are incident upon the system.
- Often modelled by random/stochastic events.

# Properties

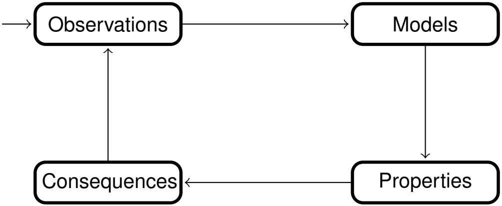
- This mathematical formulation supports a modal logic of actions for assertions about the state of the model

$$R, E \models \phi$$

- The link between the logic and the operational semantics derives from the action modalities, $\langle a \rangle$ and $[a]$, such that, e.g.

$$R, E \models \langle a \rangle \phi \quad \text{iff} \quad \begin{array}{l} \text{there exist } R', E' \text{ such that} \\ R, E \xrightarrow{a} R', E' \text{ and} \\ R', E' \models \phi. \end{array}$$

# Systems Modelling




- Can use logic to rigorously determine properties of models.

# Hennessy–Milner completeness theorem

- Relates logical equivalence and behavioural equivalence:

  *For all resource-processes, $R_1, E_1$ is bisimilar to $R_2, E_2$ if and only if, for all logical formulae $\phi$, $R_1, E_1 \models \phi$ if and only if $R_2, E_2 \models \phi$.*

- Behaviourally equivalent models are logically equivalent.
  - Permits us to substitute bisimilar models without affecting logical results.

- Logically equivalent models are behaviourally equivalent.
  - SCRP only has this for a fragment of the logic.

# Actions

- We use the free monoid over actions: any two actions $a$ and $b$ can be combined into action $ab$.
- Relationship between actions and resources defined by a *partial* modification function

$$\mu : (a, R) \mapsto R'$$

  - If an action is not defined on a particular resource then a process cannot perform that action when paired with that resource.

# Modal Logic

$$R, E \models \langle a \rangle \phi \quad \text{iff} \quad \text{there exist } R', E' \text{ such that } R, E \xrightarrow{a} R', E' \text{ and } R', E' \models \phi$$

$$R, E \models \phi_1 * \phi_2 \quad \text{iff} \quad \text{there exist } R_1, E_1, R_2, E_2 \text{ such that } R, E \sim R_1 \circ R_2, E_1 \times E_2 \text{ and } R_1, E_1 \models \phi_1 \text{ and } R_2, E_2 \models \phi_2$$

$$R, E \models \phi_1 \multimap\!\!* \, \phi_2 \quad \text{iff} \quad \text{for all } S, F, \text{ if } S, F \models \phi_1, \text{ then } R \circ S, E \times F \models \phi_2$$

# Semaphore Example

$$\mu(a, s) = s \quad \mu(a, e) \uparrow$$

$$E = \text{fix}\, X.(a : X) + (1 : X)$$

- Note, only one process can grab the resource.

$$\frac{s, E \xrightarrow{a} s, E \quad e, E \xrightarrow{1} e, E \quad e \circ s = s}{s, E \times E \xrightarrow{a} s, E \times E}$$

$$s, E \times E \not\xrightarrow{aa} s, E \times E$$

# Bisimulation $\sim$

$$E = \text{fix}\, X.(a : X) + (1 : X) \qquad \mathbf{1} = \text{fix}\, \mathbf{X}.\mathbf{1} : \mathbf{X}$$

- Do processes behave the same with a specific resource?

$$\frac{e, 1 : E \xrightarrow{1} \mu(1, e), E}{e, \text{fix}\, X.(a : X) + (1 : X) \xrightarrow{1} e, E} \quad e, \mathbf{1} \xrightarrow{1} e, \mathbf{1}$$

$$e, E \stackrel{a}{\not\rightarrow} \qquad\qquad e, \mathbf{1} \stackrel{a}{\not\rightarrow}$$

- Hence $e, E \sim e, \mathbf{1}$.

# Bisimulation and multiplicative implication.

$$
\begin{aligned}
R, E \quad \vDash \quad \phi_1 * \phi_2 \quad \text{iff} \quad & \text{there exist } R_1, E_1, R_2, E_2 \text{ such that} \\
& R, E \sim R_1 \circ R_2, E_1 \times E_2 \\
& \text{and } R_1, E_1 \vDash \phi_1 \text{ and } R_2, E_2 \vDash \phi_2
\end{aligned}
$$

- In order to get the HM result for $-\!\!*$, we need for product to preserve bisimulation.
  - We want to have that if $R, E \sim R', E'$ and $R \circ S, E \times F \vDash \varphi_2$ implies that $R' \circ S, E' \times F \vDash \varphi_2$.

# Resource Leakage

$$\frac{s, \mathrm{fix}\, X.(a : X) + (1 : X) \xrightarrow{a} s, E \quad e, \mathbf{1} \xrightarrow{1} e, \mathbf{1}}{s \circ e, (\mathrm{fix}\, X.(a : X) + (1 : X)) \times \mathbf{1} \xrightarrow{a} s \circ e, E \times \mathbf{1}}$$

- There is non-determinism in terms of how resources are allocated.
  - Could instead allocate $e$ to $E$ and $s$ to $\mathbf{1}$.
  - Then we would have $s \circ e, E \times \mathbf{1} \xrightarrow{1} s \circ e, E \times \mathbf{1}$
- Resources can 'leak' from one part of the model to another.

# Bisimulation Is *Not A Congruence*

- Bisimulation is not a congruence for product, as resources from one equivalent pair can 'leak' to the other, and hence we have that

$$e, \mathrm{fix}\, X.(a : X) + (1 : X) \sim e, \mathrm{fix}\, X.1 : X \qquad s, \mathbf{1} \sim s, \mathbf{1}$$

$$e \circ s, (\mathrm{fix}\, X.(a : X) + (1 : X)) \times \mathbf{1} \not\sim e \circ s, \mathbf{1} \times \mathbf{1}$$

# Leakage Repurcussions

- Bisimulation isn't a congruence.
- We can only get the forward direction of the HM result with a fragment of the logic that excludes multiplicative implication.

# New Resource Semantics

- Two conjunctive combinators, giving sharing and separating combinations of resources.

$$R ::= r \mid R \& R \mid R \otimes R$$

- Provides combinatorial match between the structure of processes and the structure of resources.

# Operational Semantics

$$\frac{}{R, a \xrightarrow{a} \mu(a, R), \mathbf{0}}\ (\textsc{Act}) \qquad \frac{R_i, E_i \xrightarrow{a} R'_i, E'_i}{R_1 \mathbin{\&} R_2, E_1 + E_2 \xrightarrow{a} R'_i, E'_i}\ (\textsc{Sum})$$

$$\frac{R_1, E_1 \xrightarrow{a_1} R'_1, E'_1 \qquad R_2, E_2 \xrightarrow{a_2} R'_2, E'_2}{R_1 \otimes R_2, E_1 \times E_2 \xrightarrow{a_1 \cdot a_2} R'_1 \otimes R'_2, E'_1 \times E'_2}\ (\textsc{Prod})$$

# 'Simple' Example

- Take resource bunches and process

$$R_1 = s \& s \quad R_2 = e \& e \quad R = R_1 \otimes R_2 \quad S = R_2 \otimes R_1$$

$$E = (1 + a) \times (1 + a).$$

- We then can derive the reduction

$$\dfrac{\dfrac{\dfrac{s, a \xrightarrow{a} s, \mathbf{0}}{s \& s, (1+a) \xrightarrow{a} s, \mathbf{0}} \quad \dfrac{e, 1 \xrightarrow{1} s, \mathbf{0}}{e \& e, (1+a) \xrightarrow{1} s \otimes e, \mathbf{0}}}{R_1 \otimes R_2, (1+a) \times (1+a) \xrightarrow{a} s \otimes e, \mathbf{0} \times \mathbf{0}}}{R \& S, E + E \xrightarrow{a} s \otimes e, \mathbf{0} \times \mathbf{0}}$$

# Modelling Semantics

$$\frac{R_1, E_1 \xrightarrow{a_1} R_1', E_1' \quad R_2, E_2 \xrightarrow{a_2} R_2', E_2'}{R_1 \otimes R_2, E_1 \times E_2 \xrightarrow{a_1 \cdot a_2} R_1' \otimes R_2', E_1' \times E_2'} \text{ (PROD)}$$

- Reduction semantics is syntax directed from both the process component *and* the resource component.
- In order to permit non determinism we need to make copies of resources and processes.
- As resources cannot ‘leak’ through parallel compositions, bisimulation is then a congruence.

# Resource Semantics

- Supports the semantics of connectives of the bunched logic BI:

$$R \models \phi_1 * \phi_2 \quad \text{iff} \quad \text{there are } R_1 \text{ and } R_2 \text{ such that } R = R_1 \otimes R_2, \text{ and } R_1 \models \phi_1 \text{ and } R_2 \models \phi_2$$

and

$$R \models \phi_1 \wedge \phi_2 \quad \text{iff} \quad R \models \phi_1 \quad \text{and} \quad R \models \phi_2.$$

# Conclusions

- We define a resource semantics with two conjunctive combinators.
- This provides a better combinatorial match with the structure of processes.
- Results in bisimulation being a congruence, and richer system that can embed previous work.
- Provides more stable modelling results: Hennessy–Milner completeness theorem holds.