ystems Modelling via Resources and Processes: Philosophy, Calculus, Semantics, and Logic

David Pym

HP Labs, Bristol

Acknowledgements

- Joint work with Chris Tofts, HP Labs, Bristol.
- We are grateful to Matthew Collinson, Graham Birtwistle, Didier Galmiche, Jon Hayman, Dominique Larchey-Wendling, Daniel Méry, Brian Monahan, Richard Taylor, Mike Yearworth, and two anonymous referees, for their detailed comments and corrections. Many other colleagues have given helpful advice.
- The University of Bath.
- This work builds on, and draws from, *A Calculus and Logic of Resources and Processes*, by David Pym and Chris Tofts, to appear in *Formal Aspects of Computing*.

This Talk ...

. is intended to be rather informal, a tour of some ideas in ystems modelling using algebraic, logical, and stochastic ools. I will elide details wherever possible.

eminds me of many times talking to Gordon on the way to ne bus stop ... it was (as is usual in Edinburgh) a dark and tormy night ... .

nfluence of logical frameworks project (LF, etc) can be een in background to bunched logic, of which more later.

The Problem

- To establish and deliver upon attainable expectations that systems, which are constructed in order to deliver services, will function according to their specification, at predicted costs, throughout their intended lifetimes.
- We propose to address this problem partly by deploying mathematical models of systems and services within their socio-economic environments.
- This is not fantasy: some of our technologies and processes have been deployed in contracts worth billions of dollars.

A Modelling Philosophy, I

- Adopt the methods of applied mathematics in engineering: the classical modelling cycle.
- Abstraction: pick the level carefully.
- Pragmatics: time-related value of modelling — a crude model now may be far more useful than a (perhaps too late) more detailed model later
- The map is not the territory (Korzybski; use of phrase here due to R. Taylor and C. Tofts).
- So, models should be directed to answer specific questions at specific levels of abstraction.
- Capture the Big Bad World stochastically.

A Modelling Philosophy, II

ll of this modelling is of limited value, at least in an dustrial context, unless it is

- embedded in an *economic model* of its environment, within which
- the *business processes* that drive the systems operations, the purpose of which is to deliver a service, are representable, understandable, and manipulable.

tage III here represents one line of our ongoing research.

ystems Modelling, I: Conceptual Components

- *Externalities* (big bad world) and *internalities* (system internals), in the sense of economics.
- Externalities: Basic idea is to model stochastically, capturing classes of events using probability distributions. We will illustrate with examples.
- Internalities: Model *static* structure as ‘resources’, *dynamic* structure as ‘processes’. Avoid confusion.
- Some internalities also require stochastic representation.
- Stochastic events drive processes that must access resources. This sets up systems of *queues*.

Systems Modelling, II: Demos2k

- These conceptual components are partially captured by the Demos2k tool (Birtwistle, Tofts, Christodolou, . . .).
- Discrete event simulation (executable models).
- Rigorous conceptual analysis:
  - Clear externalities–internalities separation;
  - Clear resource–process distinction;
  - Stochastic representation of environments.
- Semantically well-founded in, essentially, SCSS; stochastics ‘wrap around’ this semantics.

A Example of a Demos2k Model

```
ons arrival=negexp(10.0);
ons docking=2.0;  Cons unloading=normal(14,3);
ons leaving=2.0;  Cons tug=3; Cons jetty=2;
ons simdur=1000;

es(tugs,tug); Res(jetties,jetty);

lass boat={ Entity(Boat,boat,arrival);
  getR(jetties,1); getR(tugs,2); hold(docking);
  putR(tugs,2); hold(unloading); getR(tugs,1);
  hold(leaving); putR(tugs,1); putR(jetties,1);
 (***boat***)

ntity(Boat,boat,0.0); hold(simdur); close;
```

Demos2k lacks . . .

- A structured notion of resource – composition, ordering;
- Any (explicit) associated notion of local resource;
- Any (explicit) notion of location.

ut its use of stochastic representation of environmental ariability is highly effective. Captures queueing networks ery cleanly.

irst thing to do is recall a simple model of resource. Then tegrate with a simple model of process.

Resource Semantics, I

- Apply modelling philosophy to idea of resource.
- Intend to capture familiar notions of resource: money, count nouns in general, memory, processor cycles, time, . . . , mass nouns?
- Look for a simple but useable starting point:
  - Take a collection of *elements* of a resource;
  - Take a *composition* of elements;
  - Take a *comparison* of elements.

  Choose to capture this as ‘Kripke resource monoid’ (preordered monoid, bifunctorial).
- Examples: $(\mathbb{N}, +, 0, \leq)$; memory cells, as in separation logic; Petri nets; logic programs. In practical modelling, lots done with (combinations of) natural numbers.

Resource Semantics, II

- The preorder allows intuitionistic connectives (and quantification) to be defined. Can take also classical.
- The monoidal structure admits multiplicative conjunction, $*$, and implication, $-\!*$; also multiplicative quantification — though less well-behaved in general than I first thought.
- Generalizes to 'doubly-closed categories'. Lots of examples via Day's tensor.
- Proof systems, and tableaux, with a range of soundness, completeness, and finiteness results available.

his is the logic of bunched implications, BI (BSL paper; BI ook, with errata; TCS and MSCS papers).

Resource Semantics, III

istorical Attributions.

rigins of BI can be seen in two lines of work:

- The logical frameworks (LF) project, begun at Edinburgh in the 80s, considering the question of how to represent substructural systems, leading to Samin Ishtiaq's doctoral thesis;
- The functor-category view of denotational semantics, deriving from Bob Tennent, looking at the semantics of local variables, leading to Peter O'Hearn's doctoral thesis;
- In the wake of BI, these two then came together to develop pointer logic.

A Calculus of Resources and Processes, I

- Idea is to make resources and processes co-evolve:

$$R\,,\;E \xrightarrow{a} R'\,,\;E'$$

  where R is an element of a powerset resource monoid.
- This requires that we specify, using a ‘modification function’, the interaction between actions and resources:

$$\mu : Act \times \wp(\mathbf{R}) \rightharpoonup \wp(\mathbf{R})$$

  so that $R' = \mu(a, R)$. We require some coherence conditions.
- We work with a synchronous calculus over a commutative monoid of actions.

A Calculus of Resources and Processes, II

ketching the operational semantics, for example:

- Action prefix:

$$\frac{}{R\,,\; a : E \xrightarrow{a} \mu(a, R)\,,\; E}$$

- Product:

$$\frac{R\,,\; E \xrightarrow{a} R'\,,\; E' \qquad S\,,\; F \xrightarrow{b} S'\,,\; F'}{R \circ S\,,\; E \times F \overset{a\#b}{\to} R' \circ S'\,,\; E' \times F'}$$

- Hiding:

$$\frac{R \circ S\,,\; E \xrightarrow{a} R' \circ S'\,,\; E'}{R\,,\; (\nu S)E \overset{\hat{a}}{\to} R'\,,\; (\nu S')E'}$$

$\hat{a}$ is a 'without S'

- Bisimulation is written

$$R\,,\,E \sim_\mu R\,,\,F$$

and note dependence on μ. This is not subtle.
- Usual largest relation s.t ....
- Bisimulation is a congruence.
- Interesting to consider 'change of base' here: $R\,,\,E \sim_\mu S\,,\,F$, for which there would be a counterpart in the modal logic that comes later.

A Sketched Example: Asynchronous Handover

A sketch of a producer–consumer problem:

$$
\begin{aligned}
Prod &\stackrel{\text{def}}{=} nowork : Prod + work : Prod \\
Cons &\stackrel{\text{def}}{=} wait : Cons + cons : Cons,
\end{aligned}
$$

where

$$
\begin{aligned}
\mu(nowork, \{e\}) &= \{e\} & \mu(nowork, R^n) &= R^n \\
\mu(wait, \{e\}) &= \{e\} & \mu(wait, R^n) &= R^n \\
\mu(work, \{e\}) &= \{R\} & \mu(work, R^n) &= R^{n+1} \\
& & \mu(cons, R^n) &= R^{n-1}.
\end{aligned}
$$

e}, $Prod \times Cons$ behaves as a producer–consumer with a ounter R:

$$\{e\}\,,\ Prod \times Cons \overset{nowork\#wait}{\longrightarrow} \{e\}\,,\ Prod \times Cons$$

$$\{e\}\,,\ Prod \times Cons \overset{work\#wait}{\longrightarrow} R\,,\ Prod \times Cons$$

$$R^n\,,\ Prod \times Cons \overset{nowork\#wait}{\longrightarrow} R^n\,,\ Prod \times Cons$$

$$R^n\,,\ Prod \times Cons \overset{nowork\#cons}{\longrightarrow} R^{n-1}\,,\ Prod \times Cons$$

$$R^n\,,\ Prod \times Cons \overset{work\#cons}{\longrightarrow} R^n\,,\ Prod \times Cons$$

$$R^n\,,\ Prod \times Cons \overset{work\#wait}{\longrightarrow} R^{n+1}\,,\ Prod \times Cons.$$

A Calculus of Resources and Processes, III

- A denotational semantics: several possibilities. Decided here to go with a parametrization (as functor category of resources) of Abramsky's use of the *Plotkin power-domain* to construct a (fully abstract) domain-theoretic model, $\mathcal{D}$, of SCCS using synchronization trees.
- Full abstraction for SCCS adapts to this semantics for SCRP.
- Pros: relatively simple and appealing. Cons: not a good general definition of a model; for that, we'll need some suitable category of sheaves, cf. Winskel et al.

A Hint of the Semantics

or a Kripke resource monoid $\mathcal{R} = (\mathbf{R}, \circ, e, \sqsubseteq)$, interpret
CRP (over $\mathbf{R}$) in $[\wp(\mathbf{R}), \mathcal{D}]$:

- For actions,

$$[\![a : E]\!]_{\mu}^{\mathcal{D}}(R) \simeq \{\!|\, \langle a\,,\, [\![E]\!]_{\mu}^{\mathcal{D}} \mu(a, R) \rangle \,|\!\}$$

- For product, where f is Abramsky's combinator,

$$[\![E \times F]\!]_{\mu}^{\mathcal{D}}(R) \simeq \biguplus_{S \circ T \sqsubseteq R} (\mu\Phi \in [\mathcal{D}^2 \to \mathcal{D}]\,.\, f\Phi)([\![E]\!]_{\mu}^{\mathcal{D}} S)([\![F]\!]_{\mu}^{\mathcal{D}} T)$$

Note the appearance of Day's tensor;

- Hiding goes like restriction in SCCS; sum goes like sum in SCCS.

SCRP and Demos2k

- Demos2k partially realizes our conceptual perspective:
  - Resources do not have composition;
  - Resources do not have comparison, though, as we shall see later, a bit of ordering can be implicit;
  - No notion of hiding.
- A project at HP Labs (Collinson, Pym, Tofts) to build SCRP/MBI-based tools (simulation, model-checking, visualization) in the spirit of Demos2k. Collaboration, particularly on the logical work, with Galmiche, Larchey-Wendling (LORIA, Nancy) and Méry (Verimag, Grenoble); and with Sassone (Southampton).

A Modal Logic, I

ecall that Hennessy-Milner logic is based on a semantic dgement $E \models \phi$. The corresponding judgement in our etting is

$$R\,,\ E \models_{\mu} \phi.$$

- The two-dimensional worlds give rise to some amusing connectives.
- We get the usual addtives of Hennessy-Milner, all relative to Es. For example, $R, E \models_{\mu} \phi \vee \psi$ iff $R, E \models_{\mu} \phi$ or $R, E \models_{\mu} \psi$.
- Mutiplicatives, as in BI, exploit the resource decomposition.

A Modal Logic, II

or example, we get a simple logical characterization of oncurrent composition,

$R\,,\,E \models_\mu \phi * \psi$ iff there exist S, T and F, G such that $S \circ T \sqsubseteq R$, that $R, E \sim_\mu R, F \times G$, and $S\,,\,F \models_\mu \phi$ and $T\,,\,G \models_\mu \psi$,

sing $*$ as in BI, and in separation logic, a well-known oecific model of (Boolean) BI.

A Modal Logic, III

ome other bits of $\models_\mu$ (sketched).

- Atoms: $R\,,\;E \models_\mu p(a)$ iff $\mu(a,R)\downarrow$ and $R \in [\![p]\!]$ (could also require that E can do a).
- A multiplicative modality:

$$R\,,\;E \models_\mu \langle a\rangle_\nu\,\phi \quad \text{iff} \quad \text{there is some } R\circ S\,,\;E \xrightarrow{a} \mu(a, R\circ S)\,,\;E' \\ \mu(a, R\circ S)\,,\;E' \models_\mu \phi$$

- A multiplicative quantifier:

$$R\,,\;E \models_\mu \exists_\nu x.\phi \quad \text{iff} \quad \text{for some } R\,,\;E \sim_\mu R\,,\;(\nu S)F \text{ s.t. } R\circ S\downarrow, \\ R\circ S \models_\mu \phi[b/x], \text{ for some } b \text{ enabled by } S$$

n Example: Asynchronous Handover Revisited

ecall the producer–consumer system,

$$Prod \stackrel{\text{def}}{=} nowork : Prod + work : Prod$$
$$Cons \stackrel{\text{def}}{=} wait : Cons + cons : Cons$$

et ϕ_{Prod} and ϕ_{Cons} be properties of $Prod$ and $Cons$, espectively, relative to resource R. Then the system $e\}, Prod \times Cons$ has the property

$$\{e\}\,,\; Prod \times Cons \models \langle nowork\#cons \rangle_{\nu}(\phi_{Prod} * \phi_{Cons})$$

his property says that the system $\{e\}, Prod \times Cons$ may erform the action $nowork\#cons$ provided the required esource, R, be added.

More on MBI

- Equivalenece Theorem: For image-finite resource-processes,

$$R\,,\,E \sim_{\mu} R\,,\,F \quad \text{iff} \quad R\,,\,E \equiv_{\mathsf{MBI}} R\,,\,F.$$

- Change of Base? For bisimulation, for models? Practical motivation: ‘refinement’.
- Development of tableaux systems for the family of modal logics that includes MBI is under way (Collinson, Galmiche, Larchey-Wendling, Pym).

Spatial and Intensional Enrichments

o far so, so good, we have a well-founded, *practical*, ystems modelling methodology. But *experience*, articularly from (i) access control policies, (ii) modelling ne *cost–benefit* of *IT security operations*, and (iii) the pparent demands of understanding the value proposition f *utility computing*, suggests that more organizational tructure is needed.

- A notion of *location*;
- notions such as *principals*; and
- modalities for *assertions* by principals.

Location, I

ollowing the same modelling philosophy used to derive our ssumptions about resources, we need

- a collection of locations, L, M, L', $\ldots$.
- a notion of *sublocation*, $L \preceq M$,
- *substitution* of locations, $M[L'/L]$, of location L' for a sublocation L of M,
- a notion of *connection* between locations, and
- a *product* of locations.

xample: directed graphs.

Location, II

- Judgements become,
  - in SCRP

$$\frac{}{L\,,\;R\,,\;a:E \xrightarrow{a} L'\,,\;R'\,,\;E} \quad \mu(a,L,R) = (L',R')$$

    etc. and,
  - in MBI,

$$L\,,\;R\,,\;E \models_{\mu} \phi$$

- Framework permits association of resources with locations that are either single points or whole networks, depending on choice of level of abstraction of the model.

Demos2k: Boats Revisted

esources:

- Two types of boat, ‘regular’ and ‘secure’;
- Two types of tug and two types of jetty, similarly.

yanamics:

- Boats and secure boats arrive according to given probability distributions, queues are set up;
- Secure boats require secure tugs and must enter secure jetties;
- Regular boats may use either regular or secure tugs but enter only regular jetties.

his model has implicit notions of *location* and implicitly *rders* resources in order to control access.

Intensionality: Rôles and Impersonation

loving on from this simple practical example, we can ropose, within the SCRP/MBI framework, some ideas to apture aspects of principals' (or agents') identities:

- For example, 'E in rôle F',

$$\frac{R\,,\,F \xrightarrow{a} R'\,,\,F' \qquad S\,,\,E \xrightarrow{a} S'\,,\,E'}{S, E \propto F \xrightarrow{a} S'\,,\,E' \propto F'} \quad R \sqsubseteq S, \quad S\,,\,E \sim_{\mu} S\,,\,F,$$

- together with 'E says ϕ',

$$R\,,\,G \models_{\mu} \{E\}\phi \quad \text{iff} \quad \text{for some } F \text{ s.t. } R, G \sim_{\mu} R, E \propto F, \\ R, F \models_{\mu} \phi$$

- And we could add location to these judgements . . .

Some Directions

- A probabilistic calculus; cf. WSCCS.
- Corresponding logic predicates over *weights*, not traces. Deeper connections with queueing theory.
- Towards a field theory of systems evolution.
- Various tools, as mentioned before, for SCRP, MBI — e.g., simulation and visualization tools, model checking.