An intensionally fully-abstract sheaf model for π

Clovis Eberhart Tom Hirschowitz
CNRS and Université Savoie Mont Blanc

Thomas Seiller
CNRS and Université Paris 7

Issues raised by standard operational semantics

Standard operational semantics

Execution traces = paths in labelled transition systems (LTSs).

As Castellan, Clairambault, and Winskel '15 argue:

Different interleaving of independent actions $\rightsquigarrow$ different paths.

- State explosion problem in verification.
- Loss of causality information $\rightsquigarrow$ difficult error diagnostics.

Causal models

Intended to restore causality information.

Petri nets ('81), CCS ('82)
Nielsen, Plotkin, Winskel

duplication & uniformity

output of private channels

Linear logic ('03 - '07)
Melliès

π-calculus ('12)
Crafa et al.

- Castellan, Clairambault, Winskel ('15): as Melliès + concurrent strategies.
- All three extensions: very hard!

A different approach to causal models

- First main result published at Calco '13: intensional full abstraction for CCS.
- Here, extended to the π-calculus.

Construction of model

- Same pattern as for CCS.
- Difficulty: need to restrict traces to subconfigurations.
- Dealt with using factorisation systems.

Proof of intensional full abstraction

- New proof method required.
- Actually simpler than for CCS.

An important architectural difference

Standard denotational semantics:

- a large `ambient' category: event structures, concurrent games;
- interpretation of terms/programs in this ambient category.

Here:

- For each considered calculus, a playground $\approx$ a notion of trace.
- Intuition: a playground gives the `rules of the game'.
- Denotations are then innocent presheaves on traces.

Hopefully: paves the way for studying relations between calculi.

Traces

Very intensional notion of trace

- Configurations X,Y,... $\approx$ network topologies:
  - Agents.
  - Communication channels between them.
- Traces $Y \nrightarrow X$ describe each agent's actions leading from X to Y.

(Where bits of Y come from in X)

Naive strategies

Naive strategies: presheaves on traces

- Each trace $\mapsto$ possibly empty set of ways of accepting them.
- Cf. presheaf models (Joyal, Nielsen, Winskel '93).
- Deals at once with:
  - prefix-closedness,
  - permutation of independent actions,
  - channel renaming (cf. nominal sets).

Problem: too general

Agents may `communicate' without using the network.

Innocent strategies

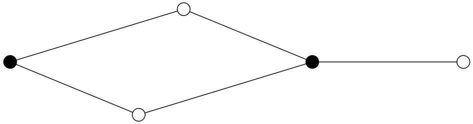
To rectify the deficiency, restrict to

Innocent strategies: sheaves on traces

- Accepting a trace should be `local'.
- I.e., determined only by each agent's `view' of the trace.

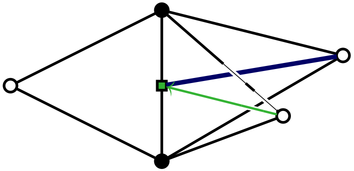
Each trace covered by its collection of views	Grothendieck topology
Ways of accepting trace u $\cong$ collections of ways of accepting u's views	Sheaf condition

Configurations

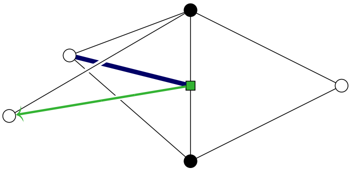


- $\bullet \approx$ agent.
- $\circ \approx$ communication channel.
- Edges: agent knows channel.
- Now, traces:
  - Actions are not a mere binary relation (initial, final configuration).
  - Indeed, want to represent how one moves from initial to final configuration.
  - We use cospans: initial $\rightarrow$ stuff $\leftarrow$ final.
  - What stuff? A kind of higher-dimensional graph.
  - Formally: presheaves on a countable category $\mathbb{C}$, see paper.

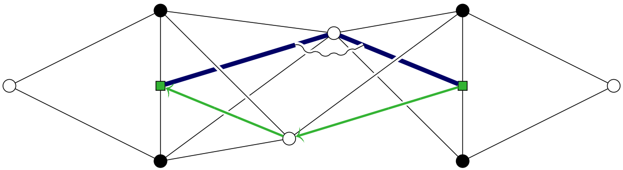
Generators for actions: particular presheaves on $\mathbb{C}$



Output

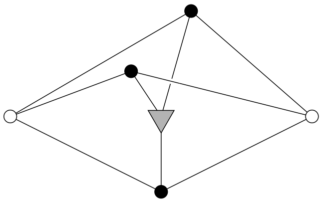


Input



Synchronisation

Generators for actions: particular presheaves on $\mathbb{C}$



...

Forking

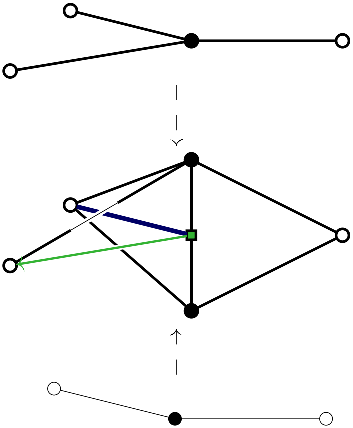
These presheaves vaguely look like actions.

How to

- add temporal information (initial/final),
- put generators in context,
- compose them to get traces with more than one action?

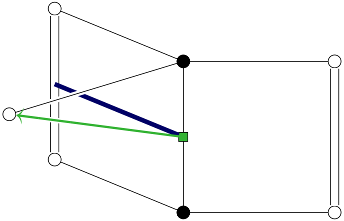
Temporal (initial/final) information through cospans

Cospan for the input action:



$$\begin{tikzcd} \text{final configuration} \arrow[d, dashed] \\ \text{stuff} \\ \text{initial configuration} \arrow[u, dashed] \end{tikzcd}$$

drawn for conciseness as:



Inclusion into larger configurations

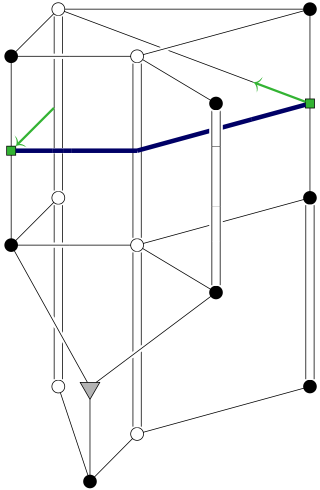
Definition

Interface of the cospan for a generator: channels shared between initial and final.

$$
\begin{tikzcd}
 & Y_0 \arrow[rr] \arrow[d] & & Y \arrow[d, dashed] \\
 & A_0 \arrow[rr] & & A \\
I \arrow[uur] \arrow[ur] \arrow[rr] \arrow[dr] & & Z \arrow[uur] \arrow[ur] \arrow[dr] & \\
 & X_0 \arrow[uu] \arrow[rr] & & X \arrow[uu, dashed]
\end{tikzcd}
$$

Intuition: glue Z and initial configuration (resp. action, final) along I.

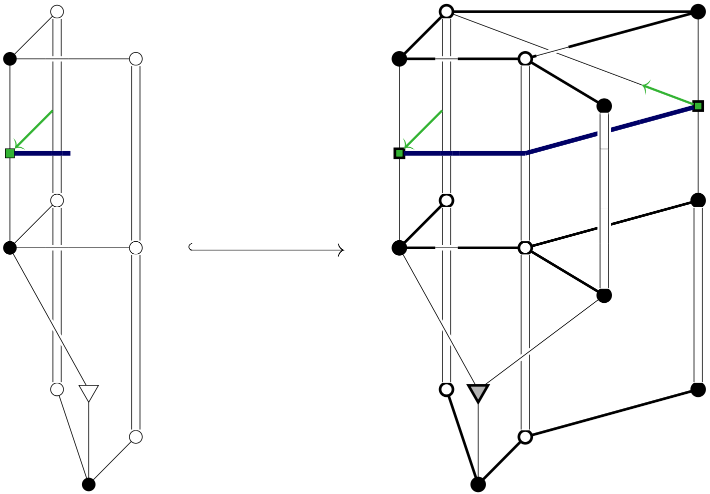
Sequential composition of traces



- By composition in $\mathrm{Cospan}(\widehat{\mathbb{C}})$!
- Retains causality, not syntactic ordering.
- $\leadsto$ a category $\mathscr{T}_X$ of traces over X.

- Naive strategies over X: $\widehat{\mathscr{T}_X} = [\mathscr{T}_X^{op}, \mathrm{sets}]$.

Views and innocence



Strategies on a configuration X = sheaves on $\mathscr{T}_X \simeq$ presheaves on $\mathcal{V}_X$.

The problem

- Everything works as in previous work on CCS.
- Except:

Needed for the machinery to work

A way of restricting traces over X to any subconfiguration $Y \hookrightarrow X$.

The basic idea

Given any cospan (s, v) as on the right

$$\begin{tikzcd} Y' \arrow[r, "h''"] \arrow[d, "s'"'] \arrow[dr, phantom, "\lrcorner", very near start] & X' \arrow[d, "s"] \\ V \arrow[r, "h'"] & U \\ Y \arrow[u, "v'"] \arrow[r, "h"'] & X, \arrow[u, "v"'] \end{tikzcd}$$

we compute its restriction along $Y \xrightarrow{h} X$ by:

1. factorising $v \circ h$ as $h' \circ v'$, where

   v' does as many actions as it can;
2. then taking the pullback of s and h'.

What does it mean to \`do as many actions as one can'?

Factorisation system!

Generating cofibrations

Factorisation system generated from a set of so-called cofibrations.

Consider the set $\mathscr{V}_0$ of inclusions $X \xrightarrow{t} A$

- of the initial configuration of a generator
- into the generator itself ($\in \widehat{\mathbb{C}}$).

Horizontal maps

- Consider now maps g right-orthogonal to $\mathscr{V}_0$, i.e., for all commuting squares

$$\begin{tikzcd} X \arrow[r, "u"] \arrow[d, "t"'] & C \arrow[d, "g"] \\ A \arrow[r, "v"'] \arrow[ur, dashed, "h"] & D \end{tikzcd}$$

  with $t \in \mathscr{V}_0$, there exists a unique filler h making both triangles commute.
- Idea: g may not add new actions from C.
- Indeed: any added action was already in C.

Notation

$t \perp g$, $\mathscr{V}_0 \perp g$, or $g \in \mathscr{V}_0^{\perp}$.

A factorisation system

Theorem (Bousfield)

Any morphism $A \to B$ factors as

$$A \xrightarrow{v} C \xrightarrow{h} D$$

with $v \in {}^{\perp}(\mathscr{V}_0{}^{\perp})$ and $h \in \mathscr{V}_0{}^{\perp}$.

Not quite there yet: need to prove the obtained (v', s') is again a trace!

Theorem

Traces are stable under restriction.

Main result

- We define a translation $[\![-]\!] : \mathrm{Pi} \longrightarrow \mathrm{Strategies}$.
- Compositional $\rightsquigarrow$ easy to define semantic counterparts to testing equivalences.
- Idea: P passes the test T iff $P|T$ satisfies some property.

(e.g., eventually `ticks')

- Notation: $P|T \in \perp$.
- $P \sim Q$ iff $\forall T, (P|T \in \perp) \iff (Q|T \in \perp)$.

For any testing equivalence (with mild hypotheses):

Theorem (intensional full abstraction)

The translation induces a bijection on quotients:

$$\mathrm{Pi}/\!\sim\; \xrightarrow{\cong} \mathrm{Strategies}/\!\sim\,.$$

Conclusion

- Notably left out of this talk:
  - Proper definition of $\mathbb{C}$.
  - Proof that traces are stable under restriction.
  - New approach to proving intensional full abstraction.
- Future work:
  - more complex calculi (functional, then functional & concurrent);
  - applying notion of trace (see EI talk);
  - study morphisms between calculi.

Universal property of restriction

$$
\begin{tikzcd}
Z' \arrow[dr] \arrow[drr, bend left] \arrow[dd] & & \\
 & Y' \arrow[r] \arrow[dd] \arrow[dr, phantom, "\lrcorner", very near start] & X' \arrow[dd] \\
W \arrow[dr] \arrow[drr] & & \\
 & V \arrow[r, "h' \in \mathcal{H}"'] & U \\
Z \arrow[uu, "\mathcal{V} \ni v''"] \arrow[dr] \arrow[drr] & & \\
 & Y \arrow[uu] \arrow[r] & X \arrow[uu]
\end{tikzcd}
$$

From presheaves on views to sheaves on traces

Use right Kan extension : for any configuration X, consider

$$\begin{tikzcd} {\mathcal{V}_X}^{op} \arrow[rr, hook, "i^{op}"] \arrow[dr, "S"'] & \arrow[d, phantom, "\cong"] & {\mathcal{T}_X}^{op} \arrow[dl, "S' = \mathrm{ran}_{i^{op}}(S)"] \\ & \text{sets} & \end{tikzcd}$$

Explicit formula

- General : $S'(p) = \int_{v \in \mathcal{V}_X} S(v)^{\mathcal{T}_X(v,p)}$.
- Boolean case; p accepted iff all its views are:

$$S'(p) = \bigwedge_{\{(v \xrightarrow{\alpha} p) \in \mathcal{T}_X\}} S(v).$$