Innocent strategies as sheaves, and interactive equivalences for CCS

Tom Hirschowitz and Damien Pous

PPS, Février 2010

LAMA
Laboratoire de Mathématiques
Université de Savoie

UMR 5127

Programming languages: a technology

Claim

Research in programming languages is mainly technological.

Applies a non-formalised method, e.g.:

- Syntax.
- Quotienting by variable renaming ($x \mapsto x = y \mapsto y$).
- Reduction relation to model program execution.
- Reasoning on reduction.

Programming languages: a technology

Claim

Research in programming languages is mainly technological.

Long-term goal

Contribute to finding a general setting for this.

Leads to stupid questions like:

- What is a programming language?
- What is an observational equivalence?
- What is a compilation?

Related work

- Higher-order rewriting (Nipkow, 1991), with models in cartesian closed 2-categories.
- Does not account for calculi with a structural congruence.
- Formats and their functorial interpretation by Plotkin and Turi.
- Anything else?

Outline

- A category $\mathbb{E}$ of executions, with a (Grothendieck) topology on $\mathbb{E}$.

Innocent strategies as sheaves.

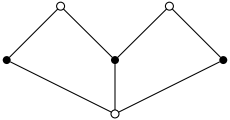
- The stack of strategies.

Interaction by amalgamation.

- Notions of observation.

Fair testing $=$ must testing.

Positions

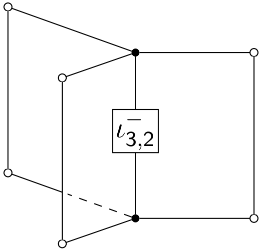


- $\bullet$'s = players,
- $\circ$'s = channels.
- Close to (multi-hole) active contexts in CCS:

$$\nu abc.X_1(a, c)|X_2(a, b, c)|X_3(b, c).$$

Moves from natural deduction: in/out

$$\frac{a_0, \ldots, a_{n-1} \vdash P}{a_0, \ldots, a_{n-1} \vdash a_i.P}$$

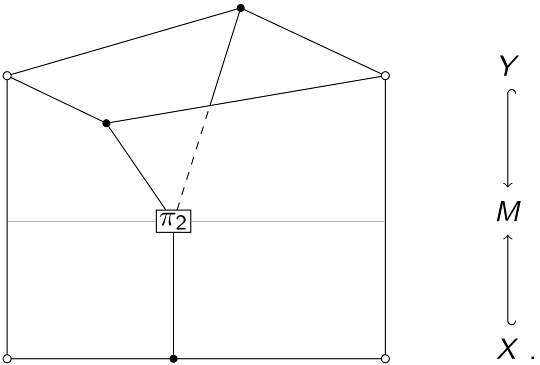


$$\begin{array}{c} Y \\ \downarrow \\ M \\ \uparrow \\ X\ . \end{array}$$

Output: same with a $\iota^+_{n,i}$.

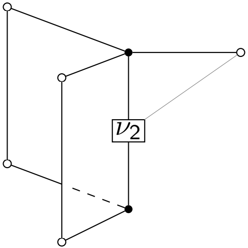
Moves from natural deduction: parallel composition

$$\frac{\Gamma \vdash P \qquad \Gamma \vdash Q}{\Gamma \vdash P|Q}$$



Moves from natural deduction: name creation

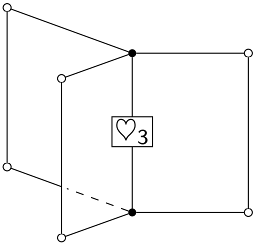
$$\frac{\Gamma, a \vdash P}{\Gamma \vdash \nu a.P}$$



$$Y \hookrightarrow M \hookleftarrow X \; .$$

Moves from natural deduction: tick

$$\frac{\Gamma \vdash P}{\Gamma \vdash \heartsuit.P}$$

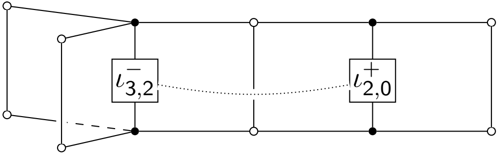


$$\begin{array}{c} Y \\ \downarrow \\ M \\ \uparrow \\ X \end{array} .$$

A cheap daimon.

Synchronisation

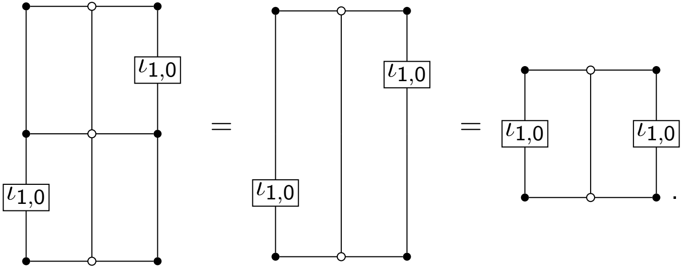
$$a.P \mid \overline{a}.Q \longrightarrow P \mid Q$$



Executions

Glueings of diagrams of the above kind together:

- horizontally,
- vertically (possibly denumerable).



Keeping track of the base position: $X \hookrightarrow U$.

A word on representing executions

- These diagrams: formalised as certain presheaves on a category $\mathbb{C}$.
- Basic diagrams: representables.
- Glueing = taking colimits.

More in the end if time permits.

The category $\mathbb{E}$ of executions

- Objects: $X \hookrightarrow U$ well-formed.
- Morphisms: all commuting squares

$$\begin{array}{ccc} U & \longrightarrow & V \\ \uparrow & & \uparrow \\ X & \longrightarrow & Y. \end{array}$$

- Obvious functor $\pi \colon \mathbb{E} \to \mathbb{B}$:

$$(X \hookrightarrow U) \mapsto X,$$

where $\mathbb{B}$ is the category of positions.

A Grothendieck topology

- We will now introduce a Grothendieck topology on $\mathbb{E}$.
- Whose canonical neighbourhoods will be views, in a sense very close to game semantics.

First we recall the definition of a Grothendieck topology.

Sieves

Definition

A sieve on an object U is

- a class of morphisms to U
- stable under precomposition by arbitrary morphisms.

Equivalently:

- A subpresheaf of the representable $\mathbb{E}(-, U)$.
- A subfibration of the domain fibration $\mathbb{E}/U \to \mathbb{E}$.

Grothendieck topologies

Definition

A Grothendieck topology J on $\mathbb{E}$ assigns to each object U a class $J(U)$ of sieves satisfying

1. the total sieve $\mathbb{E}(-, U)$ is in $J(U)$;
2. if $S \in J(U)$ and $f \colon V \to U$, then $f^*(S) \in J(V)$;
   (A covering sieve restricts to covering sieves on all opens.)
3. if $S \in J(U)$ and R is another sieve on U, then if for all $f \colon V \to U$ in S we have $f^*(R) \in J(V)$, then $R \in J(U)$.
   (If a sieve covers all the opens of a covering sieve, then it is covering.)

Here $f^*(S) = \{g \colon W \to V \mid fg \in S\}$.

Our Grothendieck topology

Let $\star$ have dimension 0, n have dimension 1, and so on up to 3.

Definition

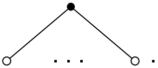
Let a sieve S on $X \hookrightarrow U$ in $\mathbb{E}$ be view-covering when it is jointly surjective in dimensions 1 and 2.

- Apart from unused channel names, this also implies surjectivity in dim 0.
- Let's get to views.

Representable sequents

A representable sequent, denoted by n is a position with

- one player,
- knowing n names:



Elementary views

Definition

An elementary view *V from n to n' is a cospan $n \hookrightarrow V \hookleftarrow n'$ isomorphic to a composite of*

- *a move M from a representable sequent n,*
- *followed by a restriction to a representable sequent n',*

i.e., a cospan of the shape

$$n \hookrightarrow M \hookleftarrow X \hookleftarrow n'.$$

Views

Definition

A view *is a possibly denumerable (vertical) composition of elementary views in* $\mathrm{Cospan}(\widehat{\mathbb{C}})$*.*

Examples.

Views form a canonical covering

Proposition

For any execution $X \hookrightarrow U$, the sieve generated by morphisms from views into U is covering.

Proposition

Any covering sieve contains all morphisms from views.

Sheaves on a site

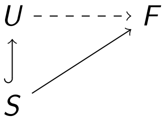
Let $\mathbb{E}$ be equipped with a Grothendieck topology J.

Definition

A presheaf F is a sheaf when for any sieve S covering U, precomposition by $S \hookrightarrow U$ yields a bijection

$$\widehat{\mathbb{E}}(U, F) \cong \widehat{\mathbb{E}}(S, F).$$

Let $\mathrm{Sh}(\mathbb{E})$ the full subcategory of such.



(Notation: $U = \mathbb{E}(-, U)$.)

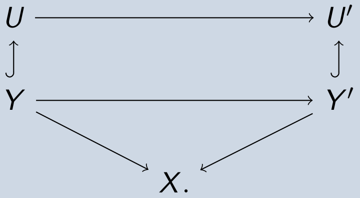
(Being defined on the opens in S is enough.)

Relativising to a base position X

Definition

Let $(\mathbb{E})_X$ have

- as objects $U \hookleftarrow Y \to X$, with $Y \hookrightarrow U$ well-formed, and
- as morphisms commuting diagrams



$(\mathbb{E})_X$ inherits a Grothendieck topology from $\mathbb{E}$.

Strategies as sheaves

Definition

Let the category S_X of strategies on X be $\mathrm{Sh}((\mathbb{E})_X)$.

Intution: a strategy S specifies for each execution $E \in (\mathbb{E})_X$ a number of ways for it to accept E.

Restriction to a subposition

- Consider $Y \to X$, and a strategy $S \in \mathsf{S}_X$.
- Let $S_{|Y}$ send $U \hookleftarrow Z \to Y$ to

$$S(U \hookleftarrow Z \to Y \to X).$$

- This extends to morphisms.

Proposition

This forms a functor $\mathsf{S} \colon \mathbb{B}^{op} \to \mathrm{CAT}$.

The stack of strategies

Proposition

This functor $\mathrm{S}\colon \mathbb{B}^{op} \to \mathrm{CAT}$ *is a stack for the "surjective in dim 1" topology on* $\mathbb{B}$.

- Stacks are like sheaves but one dimension up.
- For sheaves: a bijection $\widehat{\mathbb{E}}(U, F) \cong \widehat{\mathbb{E}}(S, F)$.
- For stacks: an equivalence of categories.
- Kown fact: sheaves on slices form a stack.
- Here: mild generalisation.
- Why stacks? Intuitively, only the number of possible states should matter, not the precise set of states.

Canonical covering in $\mathbb{B}$

Proposition

For a given position X, the collection of morphisms $n \to X$ (for all n) is covering in $\mathbb{B}$.

Proposition

Any covering contains it.

Canonical covering continued

For any square

$$\begin{array}{ccc} Y & \longrightarrow & n \\ \downarrow & & \downarrow x \\ m & \xrightarrow[x']{} & X \end{array}$$

with $x \neq x'$, Y has dimension 0.

Canonical covering continued

Proposition

If Y has dim 0, then $\mathsf{S}_Y \simeq 1$.

Indeed:

- any execution U on Y is covered by the empty family,
- which has a unique $\emptyset \to F$ for any sheaf F,
- so $F(U) \cong 1$, which determines F up to iso.

Canonical spatial decomposition

Let $\mathrm{Sq}(X) = \coprod_{n} X(n)$.

Proposition

$$\mathsf{S}_X \simeq \prod_{(n,x)\in \mathrm{Sq}(X)} \mathsf{S}_n.$$

Temporal decomposition

- Let $\mathcal{M}_X$ be the set of possible moves from X (explain the size).
- For each $i \in \mathcal{M}_X$, let X_i be the domain of the corresponding move.
- For any $\mathbb{C}$, let $\mathrm{Fam}(\mathbb{C})$ denote the category with
  - objects families $f : X \to \mathrm{ob}\,\mathbb{C}$,
  - morphisms $f \to g$ the pairs of
    - $u : X \to Y$ such that $gu = f$, and
    - $v : X \to \mathbb{C}_1$ with

$$\mathrm{dom}\, v(x) = f(x) \qquad\qquad \mathrm{cod}(v(x)) = g(u(x)).$$

Examples.

Temporal decomposition

Theorem

Equivalence of categories: $\mathsf{S}_n \simeq \mathrm{Fam}\left(\prod_{i \in \mathcal{M}_n} \mathsf{S}_{X_i}\right)$.

A strategy is determined by

- its initial states, and
- what remains of them after each possible move.

Almost a sketch: would be a bijection of sets

$$\mathsf{S}_n \cong \prod_{i \in \mathcal{M}_n} \mathsf{S}_{X_i}.$$

Scenarioses

In concurrency,

- Physical, or fair scenario: players are really independent;
- Interpreted, or potentially unfair scenario: a scheduler is responsible for parallelism.

Must testing

Supposing a fixed move $\heartsuit$:

Definition

A process P is must orthogonal to a context C, when all maximal traces of $C[P]$ play $\heartsuit$ at some point.
Notation: $P \perp^m C$, $P^{\perp^m}$.

Definition

P and Q are must equivalent, notation $P \sim_m Q$, when $P^{\perp^m} = Q^{\perp^m}$.

Must testing in an unfair setting

Usually, only the unfair scenario is formalised:

$$P = (\Omega \mid \overline{a}) \qquad \text{and} \qquad Q = \Omega$$

are must equivalent.

The obvious test $C = a.\heartsuit \mid \square$ is not orthogonal to P.

Indeed, there is an infinite looping trace, maximal.

Fair testing in an unfair setting

- The example

$$(\Omega \mid \overline{a}) \sim_m \Omega$$

  takes potential unfairness of the scheduler into account.
- Usually people do not want to, and resort to:

Definition

A process P is fair orthogonal to a context C, when all finite traces of $C[P]$ extend to traces that play $\heartsuit$ at some point.
Notation: $P \perp^f C$, $P^{\perp^f}$.

Definition

P and Q are fair equivalent, notation $P \sim_f Q$, when $P^{\perp^f} = Q^{\perp^f}$.

Solves the issue.

Closed-world observations

Definition

An observation $X \hookrightarrow U$ is closed-world when both

$$\coprod_{n,i} U(\iota^+_{n,i}) \xleftarrow{\epsilon} \coprod_{n,i,m,j} U(\tau_{n,i,m,j}) \xrightarrow{\rho} \coprod_{n,i} U(\iota^-_{n,i}) \quad (1)$$

are surjective.

Global behaviours

- Let $\mathbb{W} \hookrightarrow \mathbb{E}$ be the full subcategory of closed-world observations.
- Let $\mathbb{W}(X)$ be the fibre over X for the projection functor $\mathbb{W} \to \mathbb{B}$.

Definition

Let the category of global behaviours on X be simply $\mathsf{G}_X = \widehat{\mathbb{W}(X)}$.

- Cf. Joyal, Nielsen, and Winskel.
- The inclusion $\mathbb{W}(X) \hookrightarrow (\mathbb{E})_X$ induces a functor $\mathsf{Gl} \colon \mathsf{S}_X \to \mathsf{G}_X$.

Observable criterion

Definition

An observable criterion consists for all positions X, of a subcategory $\perp\!\!\!\perp_X \hookrightarrow \mathrm{G}_X$.

Interactive equivalence

Definition

For any strategy S on X and any pushout P

$$\begin{array}{ccc} I & \longrightarrow & Y \\ \downarrow & & \downarrow \\ X & \longrightarrow & Z \end{array} \quad (2)$$

of positions with I of dimension 0, let $S^{\perp\!\!\!\perp_P}$ be the class of all strategies T on Y such that $\mathrm{GI}(S \parallel T) \in \perp\!\!\!\perp_Z$.

- Here $\parallel$ denotes amalgamation in the stack S.
- Let us make this concrete.

Fair testing

Definition

A closed-world execution is successful when it contains a $\heartsuit_n$.

Definition

Given a global behaviour $G \in \mathrm{G}_X$, an extension of a state $s \in G(U)$ to U' is an $s' \in G(U')$ with $i \colon U \to U'$ and $s' \cdot i = s$.

Definition

The fair criterion $\perp\!\!\!\perp^f_X$ contains all global behaviours G such that any state $s \in G(U)$ for finite U admits a successful extension.

Must testing

Definition

An extension of $s \in G(U)$ is strict when $U \to U'$ is not surjective.

Definition

For any global behaviour $G \in \mathrm{G}_X$, a state $s \in G(U)$ is G-maximal when it has no strict extension.

Definition

Let the must criterion $\perp\!\!\!\perp^m_X$ consist of all global behaviours G such that for all closed-world U, and G-maximal $s \in G(U)$, U is successful.

The key result

Theorem

For any strategy S, any state $s \in \mathsf{Gl}(S)(U)$ admits a $\mathsf{Gl}(S)$-maximal extension.

Fair vs. must

Thanks to the theorem, we have:

Lemma

For all $S \in \mathsf{S}_X$, $\mathrm{GI}(S) \in \perp^m_X$ *iff* $\mathrm{GI}(S) \in \perp^f_X$.

Proof.

Let $G = \mathrm{GI}(S)$.
(⇒) By the theorem, any state $s \in G(U)$ has a G-maximal extension $s' \in G(U')$, for which U' is successful by hypothesis, hence s has a successful extension.
(⇐) Any G-maximal $s \in G(U)$ admits by hypothesis a successful extension which may only be on U by G-maximality, and hence U is successful. □

Fair equals must

Theorem

For all $S, S' \in \mathsf{S}_X$, $S \sim_m S'$ iff $S \sim_f S'$.

Proof.

(⇒) Consider two strategies S and S' on X, and a strategy T on Y (as in the pushout P). We have:

$$
\begin{aligned}
\mathrm{Gl}(S \parallel T) \in \perp\!\!\!\perp^f \quad & \text{iff } \mathrm{Gl}(S \parallel T) \in \perp\!\!\!\perp^m \\
& \text{iff } \mathrm{Gl}(S' \parallel T) \in \perp\!\!\!\perp^m \\
& \text{iff } \mathrm{Gl}(S' \parallel T) \in \perp\!\!\!\perp^f.
\end{aligned}
$$

(⇐) Symmetric. □

Perspectives

Short term:

- We have a translation of CCS processes into this model.
- Identify the equivalence induced by this translation.

Longer term:

- Treat π, λ, ...
- Understand the abstract structure.
- What is a compilation?