

# Fair testing vs. must testing in a fair setting

Tom Hirschowitz and Damien Pous

Amsterdam, Novembre 2010



UMR 5127

# Goal

Reconcile, in the particular case of Milner's CCS,

- Joyal, Nielsen, and Winskel's 1993 (JNW) approach to concurrency theory,

with

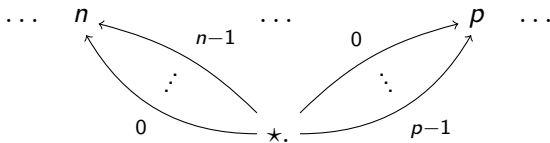
- the **interactive** approach to behavioural equivalences:
  - ▶ testing semantics in process algebra (Hennessy and De Nicola, Beffara),
  - ▶ Krivine realisability,
  - ▶ game semantics (Hyland and Ong, Abramsky et al.), Girard's **ludics**.

# Review of JNW

- Category  $\mathbb{P}$  of (non-empty) **paths**, i.e.:
  - ▶ objects: non-empty words over an alphabet  $\mathcal{A}$ ;
  - ▶ morphisms: prefix extensions, e.g.,  $abc \rightarrow abcd$ .
- Presheaves  $\widehat{\mathbb{P}}$ , i.e., functors  $\mathbb{P}^{op} \rightarrow \text{Set}$ .
- Presheaves are like trees. Examples  $ab + ac$  and  $a(b + c)$ .
- Natural transformations are like functional simulations.  
Example.

# Positions

Let  $\mathbb{C}$  be:



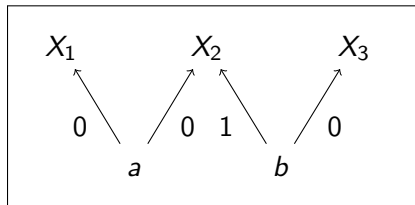
## Definition

Positions are presheaves on  $\mathbb{C}$ .

Positions form a category  $\mathbb{B}$ .

## Example

- $F(\star) = \{a, b\}$ ,
- $F(1) = \{X_1, X_3\}$ ,
- $F(2) = \{X_2\}$ ,
- $F(\star \xrightarrow{0} 1)(X_1) = a$ ,  
Notation:  $X_1 \cdot 0 = a$ .
- $X_2 \cdot 0 = a, X_2 \cdot 1 = b$ ,
- $X_3 \cdot 0 = b$ .

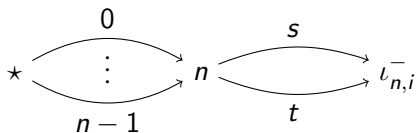


The category of elements  $\int F$ .

# Moves from natural deduction, example: input

$$\frac{a_1, \dots, a_n \vdash P}{a_1, \dots, a_n \vdash a_j.P}$$

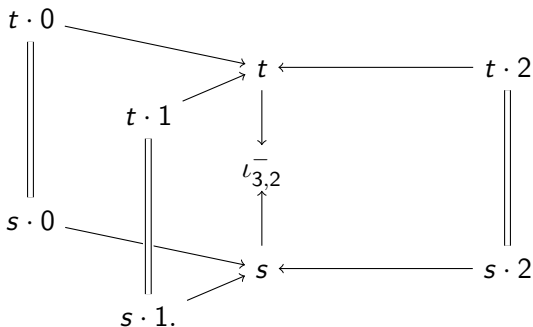
Add an object  $\iota_{n,i}^-$  to  $\mathbb{C}$ :



and quotient by  $s \circ j = t \circ j$  for all  $j \in n$ .

## Motivating the definition

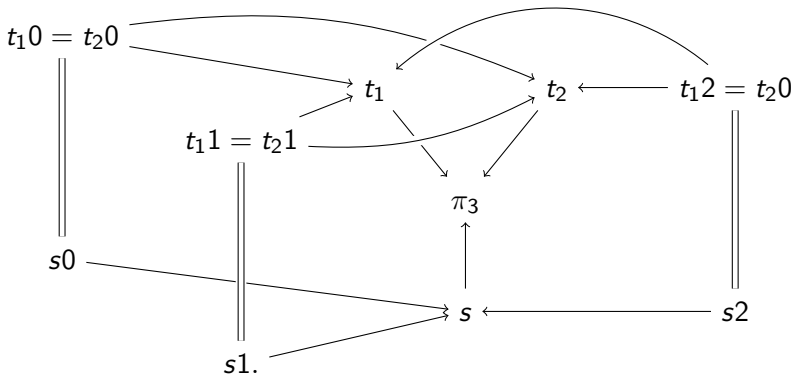
The category of elements of the representable  $\iota_{3,2}^-$  is the partially ordered set generated by



Output: do the same with  $\iota_{n,i}^+$ .

## Forking

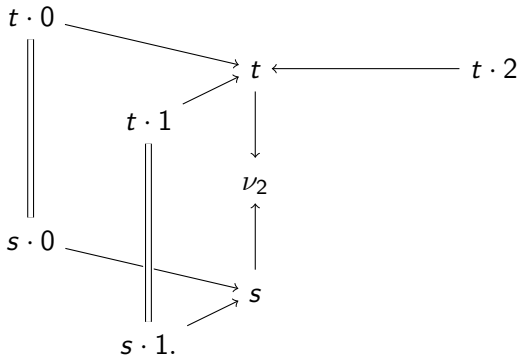
The category of elements of the representable  $\pi_3$  is the partially ordered set generated by



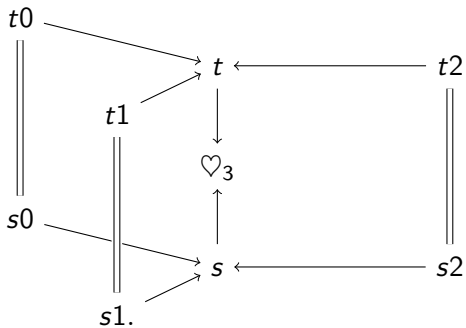


## Name creation

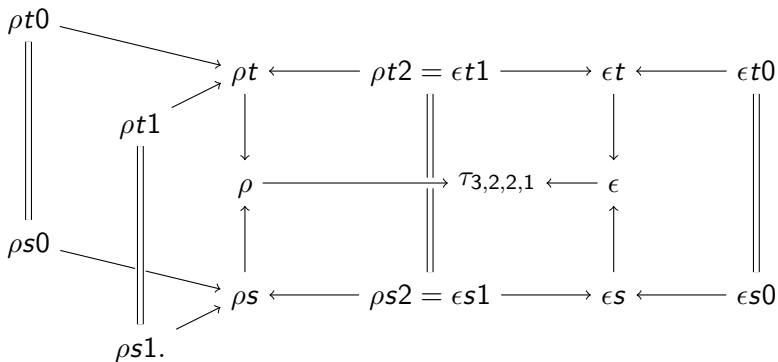
The category of elements of the representable  $\nu_2$  is the partially ordered set generated by



# Tick



# Synchronisation: the 4th dimension



# Examples

- The two maximal executions of  $\bar{a} \mid b$ , which are actually equal.
- If  $a = b$ , one more execution.
- An execution of  $\bar{a} \mid \mu X.(X \mid X)$ .
- Some “wrong” examples.

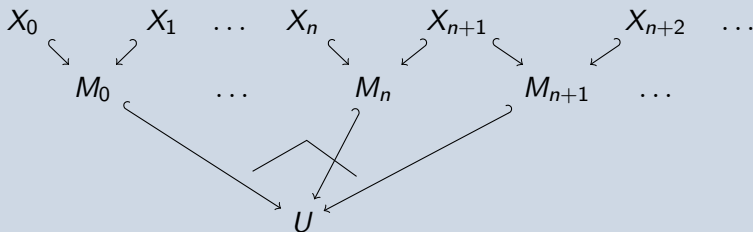
# Restrictions and moves

- A **restriction** from  $X$  to  $Y$  is a cospan  $Y \hookrightarrow X \xleftarrow{id} X$ .
- A **move** from  $X$  to  $Y$  is a cospan  $Y \hookrightarrow M \hookleftarrow X$  of presheaves obtained
  - ▶ from a cospan  $Y_0 \xrightarrow{t's} M_0 \xleftarrow{s} X_0$ ,
  - ▶ with  $M_0$  a representable of dim 2 or 3,
  - ▶ by identifying some names.

# Observations

## Definition

An *observation* is a presheaf  $U \in \widehat{\mathbb{C}}$  isomorphic to a possibly denumerable “composition” of moves and restrictions in  $\text{Cospan}(\widehat{\mathbb{C}})$ :



The *base* is the morphism  $X_0 \hookrightarrow U$ .

## The category $\mathbb{E}$ of observations

- Objects:  $X \hookrightarrow U$  in  $\widehat{\mathbb{C}}$  with
  - ▶  $U$  an observation,
  - ▶  $X$  its base;
- Morphisms: all commuting squares

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

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

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

# A 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 dimension 1.



## Elementary views

An **elementary view** from  $X$  to  $Y$  is a composite of

- a move from a representable,
- followed by a restriction to a representable:

$$n' \hookrightarrow X \xleftarrow{id} X \hookrightarrow M \hookleftarrow n.$$

Keeps track of one trajectory.

# Views

## Definition

A *view* is an observation  $X \leftrightarrow U$  isomorphic to a possibly denumerable “composition” of elementary views.

# Views are a canonical covering

## Proposition

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

## Proposition

*Any covering sieve contains all morphisms from finite views.*

## The categories $\mathbb{E}_X$

Here we want to relativise to a base position  $X$ .

### Definition

Let  $\mathbb{E}_X$  have as objects  $U \leftrightarrow Y \rightarrow X$ , and morphisms transformations between such with  $X$  fixed.

$$\begin{array}{ccc} U & \longrightarrow & U' \\ \updownarrow & & \updownarrow \\ Y & \longrightarrow & Y' \\ & \searrow & \swarrow \\ & X & \end{array}$$

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

# Strategies as sheaves

## Definition

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

# The stack of strategies

## Proposition

*This  $X \mapsto S_X$  extends to a functor  $S: \mathbb{B}^{op} \rightarrow \text{CAT}$ , which is a *stack* for the restriction of the view-covering topology to  $\mathbb{B}$ .*

Why stacks?

- Strategies are only sensible up to iso.
- Intuitively, only the number of possible states should matter, not the precise set of states.

# Canonical spatial decomposition

Let  $\text{Sq}(X) = \coprod_n X(n)$ .

## Proposition

$$S_X \simeq \prod_{(n,x) \in \text{Sq}(X)} S_n.$$

## Temporal decomposition

- Let  $\mathcal{M}_X$  be the set of moves from  $X$  (explain the size).
- For each  $i \in \mathcal{M}_X$ , let  $X_i$  be the domain of  $i$ .

### Theorem

$$S_n \simeq \text{Fam} \left( \prod_{i \in \mathcal{M}_n} S_{X_i} \right).$$

A strategy is determined by

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

Almost a sketch: would be  $S_n \cong \prod_{i \in \mathcal{M}_n} S_{X_i}$ .



# Scenarios

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:

$$P = (\Omega \mid \bar{a}) \quad \text{and} \quad Q = \Omega$$

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

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

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

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

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  $\mathbb{W} \rightarrow \mathbb{B}$ .

### Definition

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

- The inclusion  $\mathbb{W}(X) \hookrightarrow \mathbb{W}_X \hookrightarrow \mathbb{E}_X$  induces a functor  $\text{Gl}: S_X \rightarrow G_X$ .

# Observable criterion

## Definition

An **observable criterion** consists for all positions  $X$ , of a subcategory  $\perp_X \hookrightarrow G_X$ .

# 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  $S^{\perp_P}$  be the class of all strategies  $T$  on  $Y$  such that  $\text{Gl}(S \parallel T) \in \perp_Z$ .

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



# Fair testing

## Definition

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

## Definition

Given a global behaviour  $G \in G_X$ , an *extension* of a state  $s \in G(U)$  to  $U'$  is an  $s' \in G(U')$  with  $i: U \rightarrow U'$  and  $s' \cdot i = s$ .

## Definition

The *fair* criterion  $\perp\!\!\!\perp_X^f$  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  $U \rightarrow U'$  is not surjective.

## Definition

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

## Definition

Let the **must** criterion  $\perp\!\!\!\perp_X^m$  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  $s \in \text{Gl}(S)(U)$  admits a  $\text{Gl}(S)$ -maximal extension.*

## Fair vs. must

Thanks to the theorem, we have:

### Lemma

*For all  $S \in S_X$ ,  $GI(S) \in \perp_X^m$  iff  $GI(S) \in \perp_X^f$ .*

### Proof.

Let  $G = GI(S)$ .

( $\Rightarrow$ ) 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.

( $\Leftarrow$ ) 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  $S, S' \in S_X$ ,  $S \sim_m S'$  iff  $S \sim_f S'$ .

## Proof.

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

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

( $\Leftarrow$ ) Symmetric. □

# Perspectives

Short term:

- Link with CCS.
- Kleene theorem.

Longer term:

- Treat  $\pi, \lambda, \dots$
- Understand the abstract structure.
- What is a compilation?