Fair testing vs. must testing in a fair setting

Tom Hirschowitz and Damien Pous

Amsterdam, Novembre 2010
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., $abc \to abcd$.
- Presheaves $\widehat{\mathbb{P}}$, i.e., functors $\mathbb{P}^{op} \to \text{Set}$.
- Presheaves are like trees. Examples $ab + ac$ and $a(b + c)$.
- Natural transformations are like functional simulations. Example.
Positions

Let $C$ be:

\[ \ldots \xrightarrow{n} \ldots \xleftarrow{n-1} \ldots \xrightarrow{0} \ldots \xleftarrow{p-1} \ldots \]

Definition

Positions are presheaves on $C$.

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

- $F(\ast) = \{a, b\}$,
- $F(1) = \{X_1, X_3\}$,
- $F(2) = \{X_2\}$,
- $F(\ast \overset{0}{\to} 1)(X_1) = a$,
  - 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 $\int F$. 

![Diagram of the category of elements $\int F$.](image-url)
Moves from natural deduction, example: input

\[
\frac{a_1, \ldots, a_n \vdash P}{a_1, \ldots, a_n \vdash a_i.P}
\]

Add an object \( \iota_{n,i} \) to \( \mathcal{C} \):

\[
\begin{array}{c}
\star \\
\ldots \\
n - 1 \\
n \\
s \\
t \\
\iota_{n,i}
\end{array}
\]

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

\[
\begin{array}{c}
\text{s} \cdot 0 \\
\text{s} \cdot 1. \\
\text{t} \cdot 0 \\
\text{t} \cdot 1 \\
\text{t} \\
\text{t} \cdot 2 \\
\text{s} \\
\text{s} \cdot 2
\end{array}
\]

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

- $t_10 = t_20$
- $t_11 = t_21$
- $s0$
- $s1.$
- $s2$
Name creation

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

\[ t \cdot 0 \rightarrow t \rightarrow t \cdot 2 \]
\[ t \cdot 1 \Downarrow \nu_2 \]
\[ s \cdot 0 \rightarrow s \rightarrow s \cdot 1. \]
Tick

\begin{center}
\begin{tikzpicture}
    \node (t0) at (0,0) {$t_0$};
    \node (t1) at (1,-1) {$t_1$};
    \node (s0) at (0,-2) {$s_0$};
    \node (s1) at (1,-3) {$s_1$};
    \node (s2) at (2,-2) {$s_2$};
    \node (t) at (1,0) {$t$};
    \node (t2) at (2,0) {$t_2$};

    \draw[->] (t0) to (t1);
    \draw[->] (t0) to (s1);
    \draw[->] (t1) to (t);
    \draw[->] (t1) to (s0);
    \draw[->] (t2) to (t);
    \draw[->] (t2) to (s2);
    \draw[->] (s0) to (s1);
    \draw[->] (s1) to (s2);
    \draw[->] (t) to (s);
    \draw[->] (t) to (s);
    \draw[->] (s) to (t);
    \draw[->] (s) to (t);

    \node[below] at (t) {$\heartsuit_3$};
\end{tikzpicture}
\end{center}
Synchronisation: the 4th dimension

\[
\begin{align*}
\rho t_0 \\
\rho t_1 & \quad \rho t \quad \rho t_2 = \epsilon t_1 & \quad \epsilon t & \quad \epsilon t_0 \\
\rho s_0 \\
\rho s_1. & \quad \rho s & \quad \rho s_2 = \epsilon s_1 & \quad \epsilon s & \quad \epsilon s_0 \\
\end{align*}
\]
Examples

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

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

Definition

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

\[
\begin{array}{ccccccc}
X_0 & \rightarrow & X_1 & \rightarrow & \cdots & \rightarrow & X_n & \rightarrow & X_{n+1} & \rightarrow & X_{n+2} & \rightarrow & \cdots \\
\downarrow & & \downarrow & & \cdots & & \downarrow & & \downarrow & & \downarrow & & \cdots \\
M_0 & \rightarrow & \cdots & \rightarrow & M_n & \rightarrow & M_{n+1} & \rightarrow & \cdots \\
\downarrow & & \downarrow & & \downarrow & & \downarrow & & \downarrow \\
U & & & & & & & & & & & \\
\end{array}
\]

The base is the morphism $X_0 \rightarrow U$. 

Tom Hirschowitz and Damien Pous
Fair testing vs. must testing in a fair setting
14/38
The category $\mathcal{E}$ of observations

- **Objects**: $X \hookrightarrow U$ in $\hat{\mathcal{C}}$ with
  - $U$ an observation,
  - $X$ its base;

- **Morphisms**: all commuting squares

\[
\begin{array}{ccc}
U & \rightarrow & V \\
\uparrow & & \uparrow \\
X & \rightarrow & Y.
\end{array}
\]

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

\[(X \hookrightarrow U) \mapsto X.\]
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:

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

Keeps track of one trajectory.
Views

Definition

A view is an observation $X \hookrightarrow U$ 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 $\mathcal{E}_X$

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

**Definition**

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

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

$U \leftarrow Y \rightarrow X$
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 $S: \mathcal{B}^{\text{op}} \to \text{CAT}$, which is a stack for the restriction of the view-covering topology to $\mathcal{B}$.

Why stacks?

- Strategies are only sensible up to iso.
- Intuitively, only the number of possible states should matter, not the precise set of states.
Let $\text{Sq}(X) = \bigsqcup_n X(n)$.

**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 $S_n \simeq \prod_{i \in \mathcal{M}_n} S_{X_i}$. 
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:

\[ P = (\Omega \mid \overline{a}) \quad \text{and} \quad Q = \Omega \]

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

$$\prod_{n,i} U(\iota^+_{n,i}) \leftrightarrow \prod_{n,i,m,j} U(\tau_{n,i,m,j}) \xrightarrow{\rho} \prod_{n,i} U(\iota^-_{n,i})$$

are surjective.
Global behaviours

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

**Definition**

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

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

**Definition**

An *observable criterion* consists for all positions $X$, of a subcategory $\mathcal{L}_X \hookrightarrow G_X$. 
Interactive equivalence

**Definition**

For any strategy $S$ on $X$ and any pushout $P$

\[
\begin{array}{c}
I \\ \downarrow \\
X \\
\end{array} \quad \begin{array}{c}
\rightarrow \\
Y \\
\downarrow \\
\rightarrow \\
Z \\
\end{array}
\]

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

<table>
<thead>
<tr>
<th>Definition</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Definition</strong></td>
<td>A closed-world story is <strong>successful</strong> when it contains a $\Diamond_n$.</td>
</tr>
<tr>
<td><strong>Definition</strong></td>
<td>Given a global behaviour $G \in G_X$, an <strong>extension</strong> of a state $s \in G(U)$ to $U'$ is an $s' \in G(U')$ with $i: U \rightarrow U'$ and $s' \cdot i = s$.</td>
</tr>
<tr>
<td><strong>Definition</strong></td>
<td>The <strong>fair</strong> criterion $\perp^f_X$ contains all global behaviours $G$ such that any state $s \in G(U)$ for finite $U$ admits a successful extension.</td>
</tr>
</tbody>
</table>
## Must testing

### Definition

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

### Definition

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

### Definition

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

Thanks to the theorem, we have:

**Lemma**

For all $S \in S_X$, $Gl(S) \in \bot_X^m$ iff $Gl(S) \in \bot_X^f$.

**Proof.**

Let $G = Gl(S)$.

$(\Rightarrow)$ 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:

$$\text{Gl}(S \parallel T) \in \bot^f \iff \text{Gl}(S \parallel T) \in \bot^m$$

$$\text{iff } \text{Gl}(S' \parallel T) \in \bot^m \iff \text{Gl}(S' \parallel T) \in \bot^f.$$

$(\Leftarrow)$ Symmetric.
Perspectives

Short term:
- Link with CCS.
- Kleene theorem.

Longer term:
- Treat $\pi, \lambda, \ldots$
- Understand the abstract structure.
- What is a compilation?