# Refinement in hybrid(ised) institutions

Luis S. Barbosa

(joint work with M. A. Martins, A. Madeira, R. Hennicker)

HASLab
HIGH-ASSURANCE SOFTWARE LABORATORY
INESCTEC

Universidade do Minho

IFIP WG 1.3

Theddingworth, 7-10 January 2014

# Specification of reconfigurable systems

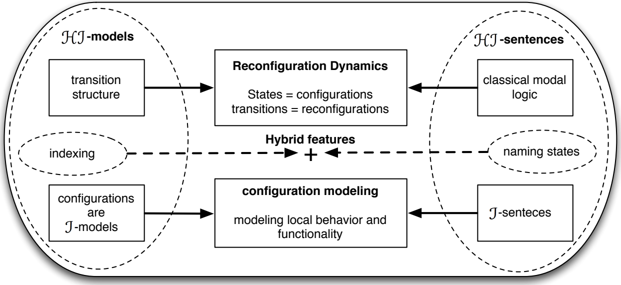
- States endowed with local specifications
- The global transition structure models system's evolution through possible configurations

Hybrid logic as a lingua franca for reconfigurable systems.

# Why hybrid logic?

- Incorporates part of the classical theory of
  - equality: $@_i\, j$
  - and reference: $@_i\, \Diamond j$
- Strictily more expressive than modal logic, e.g.
  - irreflexive frames: $i \Rightarrow \neg \Diamond i$
  - singleton state frames: $i$
- Direct reference to configurations expressing local configuration properties and global system's evolution

# Going generic




- ... specific problems require specific (local) logics: equational, first-order, fuzzy, etc.
- leading to a hybridisation process: choose a base logic and develop hybrid features on top of it

# Objectives

- Revisiting the hybridisation process ...
  (cf, Madeira, Diaconescu, Martins, Barbosa starting at CALCO'11)
- ... to study suitable notions of bisimulation and refinement for hybrid(ised) logics

# Hybridisation

$$I = \left(\mathrm{Sign}^I, \mathrm{Sen}^I, \mathrm{Mod}^I, (\models^I_\Sigma)_{\Sigma \in |\mathrm{Sign}^I|}\right) \rightsquigarrow \mathcal{H}I$$

- formulas are hybrid sentences (e.g. $@_i\rho$, $\langle\lambda\rangle\rho$, ...) taking $I$-sentences and nominals as atoms
- models are transition systems with states endowed with a $I$-model
- hybrid satisfaction is built on top of $\models^I$

$\mathcal{H}I$ forms an institution and *FOL*-encodings are lifted

# Hybridisation

## Syntax

$$\mathrm{Sign}^{\mathcal{H}I} = \mathrm{Sign}^{I} \times \mathrm{Sign}^{REL}$$

- Signatures: $(\Sigma, \mathrm{Nom}, \Lambda)$
- Morphisms $\varphi = (\varphi_{\mathrm{Sign}}, \varphi_{\mathrm{Nom}}, \varphi_{\mathrm{MS}})$
- Sentences:
  - Atoms: $\mathrm{Sen}^{I}(\Sigma), \mathrm{Nom} \subseteq \mathrm{Sen}^{\mathcal{H}I}(\Delta)$
  - Composed, e.g., $[\lambda](\rho_1, \ldots, \rho_n)$ or $@_i\rho$
- Translation of sentences along $\varphi$ is structural, e.g.,

$$\mathrm{Sen}^{\mathcal{H}I}(\varphi)(i) = \varphi_{\mathrm{Nom}}(i)$$
$$\mathrm{Sen}^{\mathcal{H}I}(\varphi)([\lambda](\rho_1, \ldots, \rho_n)) = [\varphi_{\mathrm{MS}}(\lambda)](\mathrm{Sen}^{\mathcal{H}I}(\rho_1), \ldots, \mathrm{Sen}^{\mathcal{H}I}(\rho_n))$$

# Hybridisation

## Semantics

$(\Sigma, \mathrm{Nom}, \Lambda)$-models are pairs $(M, W)$

- $W$ is a $(\mathrm{Nom}, \Lambda)$-model in *REL*
- $M$ is a function $|W| \to |\mathrm{Mod}^I(\Sigma)|$

Reducts are lifted from $I$

- $W$ is the $(\varphi_{\mathrm{Nom}}, \varphi_{\mathrm{MS}})$-reduct of $W'$:
  - $|W| = |W'|$
  - for any $n \in \mathrm{Nom}$, $W_n = W'_{\varphi_{\mathrm{Nom}}(n)}$
  - for any $\lambda \in \Lambda$, $W_\lambda = W'_{\varphi_{\mathrm{MS}}(\lambda)}$
- for any $w \in |W|$, $M_w = \mathrm{Mod}^I(\varphi_{\mathrm{Sign}})(M'_w)$.

# Hybridisation

**Satisfaction**

Resorts to $I$:

- $(M, W) \models^w \rho$ iff $M_w \models^I \rho \quad$ when $\rho \in \mathrm{Sen}^I(\Sigma)$,

captures the semantics of nominals

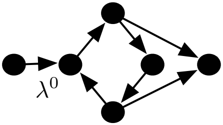
- $(M, W) \models^w i$ iff $W_i = w \quad$ , when $i \in \mathrm{Nom}$
- $(M, W) \models^w @_j \rho$ iff $(M, W) \models^{W_j} \rho$

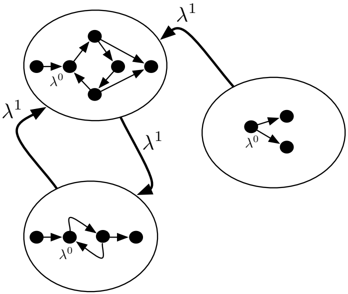
and modalities, as in

- $(M, W) \models^w [\lambda](\xi_1, \ldots, \xi_n)$ iff, for any $(w, w_1, \ldots, w_n) \in W_\lambda$, $(M, W) \models^{w_i} \xi_i$ for some $1 \leq i \leq n$

and is defined as usual for the boolean connectives

# Example: $\mathcal{H}\,TRIV$ and $\mathcal{H}^2\,TRIV$




- $\mathcal{H}\,TRIV$: pure hybrid formulas
- $\mathcal{H}^2\,TRIV$: hierarchical sturctures, e.g.

$$@_{j^1} k^0 \wedge^1 [\lambda^1](\rho_1, \ldots, \rho_n)$$

# Example: $\mathcal{H}PL$

**Signatures**

- $\mathrm{Sign}^{\mathcal{PL}}$ is the category *Set*;
- Category $\mathrm{Sign}^{\mathcal{HPL}}$:

$$(P, \mathrm{Nom}, \Lambda) \xrightarrow{(\varphi_{Sig}, \varphi_{\mathrm{Nom}}, \varphi_{MS})} (P', \mathrm{Nom}', \Lambda')$$

**Sentences**

$$\rho, \rho' \ni \ \mid \neg\rho \mid \rho \odot \rho' \mid \langle\lambda\rangle\rho \mid @_i\rho \mid i$$

**Models**

- $(M, W)$, where for each $w \in |W|$, $M_w : P \to \{\top, \bot\}$

**Satisfaction**

- for any $\rho \in \mathrm{Sen}^{\mathcal{PL}}(P)$, $(M, W) \models^w \rho$ if $M_w \models_P^{\mathcal{PL}} \rho$
- $(M, W) \models^s @_i\rho$ if $(M, W) \models^{W_i} \rho$
- ...

# Example: $\mathcal{H}EQ$

**Signatures** $\langle (S, F), \mathrm{Nom}, \Lambda \rangle$

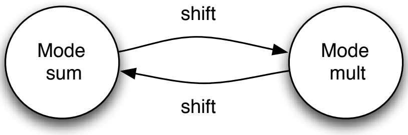
**Sentences** $\varphi, \psi \ni i \mid t \approx t' \mid @_i\varphi \mid \neg\varphi \mid \varphi \odot \psi \mid [\lambda]\varphi$

**Models** $(M, W)$, for each $w \in |W|$, $M_w$ is an $(S, F)$-algebra

**Satisfaction**

- $(M, W) \models^s t \approx t'$ if $M_w \models^{EQ} t \approx t'$.
- ...

# Example: $\mathcal{H}EQ$




$$\langle \Sigma, \{shift\}, \{mult, sum\} \rangle$$

where $\Sigma$ is the algebraic signature

**sorts** *nat*

**ops** $c : \longrightarrow nat$

$suc : nat \longrightarrow nat$

$pred : nat \longrightarrow nat$

$\star : nat \times nat \longrightarrow nat$

# Example: $\mathcal{H}EQ$

## Global properties

- $pred(suc(n)) = n$
- $\star(n,k) = \star(k,n)$, $\star(n,\star(k,l)) = \star(\star(n,k),l)$
- $\star(\star(n,m),\star(k,l)) = \star(\star(n,k),\star(l,m))$

## Local properties

- $@_{sum} \star (n,c) = n$
- $@_{sum} suc(n) = \star(n, suc(c))$
- $@_{mult} \star (n,c) = c$
- $@_{mult} \star (n, suc(c)) = n$

## Dynamics

- $\star(n,c) = n \to [shift] \star (n,c) = c$

# Hybridisation at work

... to transport specifications from a logical system to another
lifting $I2FOL$ to $\mathcal{H}I2FOL$

- extend the classical standard translation of (hybrid) modal logic into the (one-sorted) first order logic
- flattening construction to an unique (global) $FOL$-model: restricting to a $w$ gives a slice $M|_w$, a $FOL$-interpretation of the local $I$-model $M_w$, through $I2FOL$
- Encodings are conservative comorphisms
- Incorporatiion in the HETS platform

# $\varphi$-bisimulation

$$\mathrm{B}_\varphi \subseteq |W| \times |W'|$$

(i) for any $w\mathrm{B}_\varphi w'$, $w, w'$ exhibit the "same" observable information

(ii) for any $w\mathrm{B}_\varphi w'$, $i \in \mathrm{Nom}$, $W_i = w$ iff $W'_{\varphi_{\mathrm{Nom}}(i)} = w'$

(iii) for any $i \in \mathrm{Nom}$, $W_i \mathrm{B}_\varphi W'_{\varphi_{\mathrm{Nom}}(i)}$

(iv) (zig) For any $\lambda \in \Lambda_n$, if $(w, w_1, \ldots, w_n) \in W_\lambda$ and $w\mathrm{B}_\varphi w'$, then for each $k \in \{1, \ldots, n\}$ there is a $w'_k \in |W'|$ such that $w_k \mathrm{B}_\varphi w'_k$ and $(w', w'_1, \ldots, w'_n) \in W'_{\varphi_{\mathrm{MS}}(\lambda)}$

(v) (zag) ...

# $\varphi$-Bisimulation

**... the "same" observable information**

for $\mathcal{H}PL$

(i) for any $p \in Prop$, $M_w(p) = \top \Leftrightarrow M'_{w'}(p) = \top$

for $\mathcal{H}EQ$

(i) $M_w$ and $M'_{w'}$ generates the same variety

captured through the notion of $\boxed{\text{elementary equivalence}}$

# Elementary equivalence

$M \equiv M'$ if for any $\rho \in \mathrm{Sen}^I(\Sigma)$

$$M \models^I \rho \text{ iff } M' \models^I \rho$$

*truth is invariant under change of notation*

$M \equiv_\varphi M'$ if $M \equiv \mathrm{Mod}^I(\varphi)(M')$ for a given $\varphi \in \mathrm{Sign}^I(\Sigma, \Sigma')$

Thus, $M \equiv_\varphi M'$ if, for any $\rho \in \mathrm{Sen}^I(\Sigma)$

$$M \models^I_\Sigma \rho \text{ iff } M' \models^I_{\Sigma'} \mathrm{Sen}^I(\varphi)(\rho)$$

# $\varphi$-Bisimulation

$$\mathrm{B}_\varphi \subseteq |W| \times |W'|$$

(i) for any $w\mathrm{B}_\varphi w'$, $M_w \equiv_{\varphi_{\mathrm{Sign}}} M'_{w'}$

(ii) for any $w\mathrm{B}_\varphi w'$, $i \in \mathrm{Nom}$, $W_i = w$ iff $W'_{\varphi_{\mathrm{Nom}}(i)} = w'$

(iii) for any $i \in \mathrm{Nom}$, $W_i \mathrm{B}_\varphi W'_{\varphi_{\mathrm{Nom}}(i)}$

(iv) (zig) For any $\lambda \in \Lambda_n$, if $(w, w_1, \ldots, w_n) \in W_\lambda$ and $w\mathrm{B}_\varphi w'$, then for each $k \in \{1, \ldots, n\}$ there is a $w'_k \in |W'|$ such that $w_k \mathrm{B}_\varphi w'_k$ and $(w', w'_1, \ldots, w'_n) \in W'_{\varphi_{\mathrm{MS}}(\lambda)}$

(v) (zag) ...

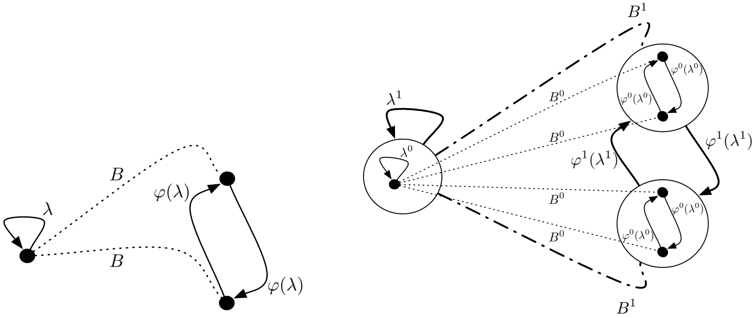
# $\varphi$-Bisimilarity

$$(M, W) \rightleftharpoons_{\varphi} (M', W')$$

The expected results:

- $\rightleftharpoons$ is an equivalence relation
- $B_{\psi}.B_{\varphi}$ is a $(\psi.\varphi)$-bisimulation
- $\mathrm{Mod}^{\mathcal{H}I}(\varphi)(M', W') \rightleftharpoons_{\varphi} (M', W')$

# Example: $\mathcal{H}\,TRIV$ and $\mathcal{H}^2\,TRIV$



# A Hennessy-Milner theorem

Let $\varphi \in \mathrm{Sign}^{\mathcal{H}I}(\Delta, \Delta')$ a signature morphism and $(M, W)$, $(M', W')$ be two image-finte $\Delta$ and $\Delta'$-models.

Then, for every $w \in W$ and $w' \in W'$, the following conditions are equivalent:

(i) $(M, W) \models^{w} \rho$ iff $(M', W') \models^{w'} \mathrm{Sen}^{\mathcal{H}I}(\varphi)(\rho)$, for any $\rho$

(ii) There is a $\varphi$-bisimulation $\mathrm{B}_{\varphi} \subseteq |W| \times |W'|$ such that $w \mathrm{B}_{\varphi} w'$

# Forward refinement

- Global behaviour allowed in the abstract model is also allowed in the concrete one (which may exhibit further behaviour)
- At each local configuration, properties are preserved along local refinement.

# $(M, W) \rightharpoondown_{\varphi} (M', W')$

$\mathrm{R}_{\varphi} \subseteq |W| \times |W'|$ such that, for any $w \mathrm{R}_{\varphi} w'$,

(i) for any $i \in \mathrm{Nom}$, if $W_i = w$ then $W'_{\varphi_{\mathrm{Nom}}(i)} = w'$

(ii) $M_w \gg_{\varphi} M'_{w'}$

(iii) for any $i \in \mathrm{Nom}$, $W_i \, \mathrm{R}_{\varphi} \, W'_{\varphi_{\mathrm{Nom}}(i)}$

(iv) for any $\lambda \in \Lambda_n$, if $(w, w_1, \ldots, w_n) \in W_{\lambda}$ then for each $k \in \{1, \ldots, n\}$ there is a $w'_k \in |W'|$ such that $w_k \mathrm{R}_{\varphi} w'_k$ and $(w', w'_1, \ldots, w'_n) \in W'_{\varphi_{\mathrm{MS}}(\lambda)}$

# Forward refinement

Preservation of hybrid satisfaction fails for

- boxed sentences ($[\lambda](\xi_1, \ldots, \xi_n)$):
- and negative sentences ($\neg\xi$)

However

# Positive existential preservation

## Lemma

Let $(M, W) \rightharpoondown_{\varphi} (M', W')$.
Then, for any $w \mathrm{R}_{\varphi} w'$ and $\rho \in \mathrm{Sen}_{\Diamond}^{\mathcal{H}I}(\Delta)$,

$$(M, W) \models^{w} \rho \text{ implies that } (M', W') \models^{w'} \mathrm{Sen}^{\mathcal{H}I}(\varphi)(\rho)$$

where $\mathrm{Sen}_{\Diamond}^{\mathcal{H}I}(\varphi)$ is the restriction of $\mathrm{Sen}^{\mathcal{H}I}(\varphi)$ to $\mathrm{Sen}_{\Diamond}^{\mathcal{H}I}(\Delta)$

# Backward refinement

- Enforces all concrete global behaviours to be allowed in the abstract model (use the (zag) condition)
- Preservation of satisfaction is restricted to positive universal sentences in $\mathrm{Sen}_{\Box}^{\mathcal{H}I}(\Delta)$

# Refinement

Two notions of refinement defined in terms of which transitions are globally preserved and in which direction.

- $\Box$ properties as a sort of (elementary) safety requirements $\implies$ preserved by backward refinement
- $\Diamond$ properties as a sort of (elementary) liveness requirements $\implies$ preserved by forward refinement

# Back to specifications

A (non-structured) specification in a institution $I$

$(\Delta, E)$, where $\Delta \in \mathrm{Sign}^I$ and $E \subseteq \mathrm{Sen}^I(\Delta)$

Its (loose) semantics is given by

- its signature $Sig[SP] = \Delta$, for some $\Delta \in |\mathrm{Sign}^I|$,
- its class of models $[|SP|] = \{M \in |\mathrm{Mod}^I(\Delta)| : M \models^I_\Delta E\}$

# Specification refinement

$SP' \rightsquigarrow_{\varphi} SP$ ($SP'$ refines $SP$ via $\varphi$) if

- $\varphi \in \mathrm{Sign}^{I}(Sig(SP), Sig(SP'))$
- $[|SP'|]|_{\varphi} \subseteq [|SP|]$

where $[|SP'|]|_{\varphi} = \{\mathrm{Mod}^{I}(\varphi)(M) | M \in [|SP|]\}$

# Lemma

Let $SP = (\Delta, E)$ and $SP' = (\Delta, E')$ be two specifications.

Then, the following statements are equivalent:

1. $SP \rightsquigarrow_{\varphi} SP'$
2. for any $(M', W') \in [|SP'|]$, there is a $(M, W) \in [|SP|]$ such that $(M, W) \rightleftharpoons_{\varphi} (M', W')$ witnessed by a total and surjective bisimulation

# Lemma

Let $SP = (\Delta, E)$ and $SP' = (\Delta, E')$ be two specifications. If $E \subseteq \mathrm{Sen}_{\diamond}^{\mathcal{H}I}(\Delta)$, then the following statements are equivalent:

1. $SP \rightsquigarrow_{\varphi} SP'$
2. for any $(M', W') \in [|SP'|]$, there is a $(M, W) \in [|SP|]$ such that $(M, W) \rightharpoondown_{\varphi} (M', W')$ witnessed by a surjective refinement relation

# Lemma

Let $SP = (\Delta, E)$ and $SP' = (\Delta, E')$ be two specifications. If $E \subseteq \mathrm{Sen}^{\mathcal{H}I}_{\Box}(\Delta)$, then the following statements are equivalent:

1. $SP \rightsquigarrow_{\varphi} SP'$
2. for any $(M', W') \in [|SP'|]$, there is a $(M, W) \in [|SP|]$ such that $(M, W) \leftharpoondown_{\varphi} (M', W')$ witnessed by a total refinement relation

# Conclusions

## Work done

- Development parametric on the base institution
- Application to a method of software design for reconfigurability
  cf, [Martins et al, 2011], [Madeira et al, 2013]

## Current work

- Hybridisation for quantitative reasoning:
  - locally (easy)
  - globally (replacing the REL-component in models by coalgebras over suitable categories)
- Inference of complexity and generation of calculi