

# Refinement in hybridised institutions

Alexandre Madeira<sup>1</sup>, Manuel A. Martins<sup>2</sup>, Luís S. Barbosa<sup>1</sup>, and Rolf Hennicker<sup>3</sup>

<sup>1</sup> HASLab INESC TEC and Univ. Minho, Braga, Portugal

<sup>2</sup> CIDMA-Center for R&D in Mathematics and Applications, Department of Mathematics, Univ. Aveiro, Portugal

<sup>3</sup> Ludwig-Maximilians-Universität München, Munich, Germany

**Abstract.** Hybrid logics, which add to the modal description of transition structures the ability to refer to specific states, offer a generic framework to approach the specification and design of reconfigurable systems, i.e., systems with reconfiguration mechanisms governing the dynamic evolution of their execution configurations in response to both external stimuli or internal performance measures. A formal representation of such systems is through transition structures whose states correspond to the different configurations they may adopt. Therefore, each node is endowed with, for example, an algebra, or a first-order structure, to precisely characterise the semantics of the services provided in the corresponding configuration. This paper characterises equivalence and refinement for these sorts of models in a way which is independent of (or parametric on) whatever logic (propositional, equational, fuzzy, etc) is found appropriate to describe the local configurations. A Hennessy–Milner like theorem is proved for hybridised logics.

**Keywords:** Hybridisation, Bisimulation, Refinement

## 1. Introduction

This paper discusses equivalence and refinement of *structured* transition systems. Or, to put it in another way, of models of specifications written in *hybridised* logics. These two qualifiers entail the need for a word of explanation. States in a *structured* transition system are endowed with a specific structure (e.g., algebraic, first order, etc.). In the development of software systems, one may think of such sort of states as (local) specifications of individual system configurations. The global transition structure, on the other hand, defines how the software evolves from a configuration to another. Such systems are called *reconfigurable* in the sense that they behave differently in different modes of operation (*configurations*) and commute between them along their lifetime.

At present, reconfigurable software is the norm than the exception: a typical, everyday example is provided by cloud based applications that elastically react to client demand levels, for example by allocating new server units to meet higher rates of service requests. Modern cars offer a second example: in each of them hundreds of electronic control units must operate in different modes, depending on the current situation—such as driving on a highway or in town where different speed regulations are applied. Switching between these modes is a typical example of a dynamic reconfiguration. Actually, reconfigurability [SC11], together with related issues like self-adaptation or context-awareness, became a main research topic, in the triple perspective of foundations, methods and technologies.

Specifications of this sort of systems, as discussed in [MFMB11], should be able to make assertions both about the transition dynamics and, locally, about each particular configuration. This leads to the adoption of hybrid logic [AtC06, Bra10], which adds to the modal description of transition structures the ability to refer to specific states, as the specification *lingua franca* for reconfigurable systems.

An elementary example to be discussed later in the paper (see Example 5.3) is that of a storing system equipped with a *read* operation which retrieves the *first* or the *last* element stored depending on the current execution mode. Reconfiguration between such modes is achieved by a control event, *shift*. The properties of each mode are specified equationally, whereas switching between them is encoded as a modality. Nominals provide a unique way to refer to each execution mode and its properties. Therefore, hybridised (equational) logic provides a suitable framework to develop the overall specification.


However, because specific problems may require specific logics to describe their configurations (e.g., equational, first-order, fuzzy, etc.), our approach is rooted on very general grounds. Instead of choosing a particular version of hybrid logic, we play with *hybridised* logics. The latter are the result of hybridising [MMDB11] whatever logic is found suitable for expressing and reasoning about the requirements at the configuration (static) level. This process, *hybridisation*, was characterised in [MMDB11, DM14] as well as in [Mad13]. To be completely general, it is framed in the context of the theory of institutions of J. Goguen and R. Burstall [GB92, Dia08], each logic (base and hybridised) treated abstractly as an *institution*. This is later taken as the *base* logic on top of which the characteristic features of hybrid logic, both at the level of syntax (i.e. modalities, nominals, etc.) and of the semantics (i.e. possible worlds), are developed.

In this context, the quest for suitable notions of *equivalence* and *refinement* between models of hybridised logic specifications becomes fundamental to the development of a design methodology for reconfigurable systems. Such is the purpose of the present paper. Its contributions are characterisations of bisimilarity and of two notions of refinement for (models of) specifications in hybridised logics. As discussed below, this requires a form of *elementary equivalence* [Hod97] between bisimilar states, as a generic formulation of the usual informal requirement that *truth remains invariant*. Clearly what *elementary equivalent* means in each case boils down to the way the satisfaction relation is defined for the base logic used in local configurations.

The choice of similarity and bisimilarity to base refinement and equivalence of (models of) reconfigurable systems seems quite standard as a fine grained approach to observational methods for systems comparison. The notion of bisimulation and the associated conductive proof method, which is now pervasive in Computer Science, originated in concurrency theory due to the seminal work of David Park [Par81] and Robin Milner in the quest for an appropriate definition of observational equivalence for communicating processes as understood in CCS [Mil89]. But the concept also arose independently in modal logic as a refinement of notions of homomorphism between algebraic models—see [San09] for an extensive historical account.

**Contributions and organisation** This paper extends preliminary work on refinement in hybridised institutions [MMB13] along three main directions: (1) the proof of a Hennessy–Milner result for hybridised logics, (2) the characterisation of two dual notions of refinement, forward and backward, and (3) a discussion on refinement of specifications. From a wider perspective, it is part of a broader research line on *logics for software reconfigurability* documented in [MMDB11, DM14] (for the hybridisation process), and [MFMB11, MNMB13, MMDB11, MMB13] (for the associated design methodology).

The paper is organised as follows: Sect. 2 recalls institutions as abstract characterisations of logics and provides a brief, and simplified, overview of the hybridisation method proposed in [MMDB11, DM14]. This forms the context for the paper’s contribution. Then, Sect. 3 introduces a general notion of bisimulation for hybridised logics and Sect. 4 proves a Hennessy–Milner like theorem. Section 5 introduces notions of forward and backward refinement and discusses preservation of logic satisfaction under them. This discussion is extended to the specification level in Sect. 6. Finally, Sect. 7 concludes and points out directions for further research.

	1650327	B	Dispatch: 3/12/2014	Journal: FAC
	Jour. No		Ms. No.	Total pages: 21
			Disk Received <input type="checkbox"/>	Corrupted <input type="checkbox"/>
			Disk Used <input type="checkbox"/>	Mismatch <input type="checkbox"/>

## 2. Background

### 2.1. Institutions

An *institution* is a category theoretic formalisation of a logical system, encompassing syntax, semantics and satisfaction. The concept was put forward by Goguen and Burstall, in the end of the seventies, in order to “formalise the formal notion of logical systems”, in response to the “population explosion among the logical systems used in Computing Science” [GB92].

The universal character of institutions proved effective and resilient as witnessed by the wide number of logics formalised in this framework. Examples range from the usual logics in classical mathematical logic (propositional, equational, first order, etc.), to the ones underlying specification and programming languages or used for describing particular systems from different domains. Well-known examples include *probabilistic logics* [BKI05], *quantum logics* [CMSS06], *hidden and observational logics* [BD94, BH06], *coalgebraic logics* [C06], as well as logics for reasoning about *process algebras* [MR06], *functional* [ST12, SM09] and *imperative programming languages* [ST12].

The theory of institutions (see [Dia08] for an extensive account) was motivated by the need to abstract from the particular details of each individual logic and characterise generic issues, such as satisfaction and combination of logics, in very general terms. In Computer Science, this lead to the development of a solid *institution-independent specification theory*, on which structuring and parameterisation mechanisms, required to scale up software specification methods, are defined ‘once and for all’, irrespective of the concrete logic used in each application domain [Tar03]. The definition is recalled below (e.g., [GB92, Dia08]) and illustrated with a few examples to which we return later in the paper.

**Definition 2.1 (Institution)** An institution

$$I = (\text{Sign}^I, \text{Sen}^I, \text{Mod}^I, (\models_{\Sigma}^I)_{\Sigma \in |\text{Sign}^I|})$$

consists of

- a category  $\text{Sign}^I$  whose objects are called *signatures* and arrows *signature morphisms*;
- a functor  $\text{Sen}^I : \text{Sign}^I \rightarrow \text{Set}$  giving for each signature a set whose elements are called *sentences* over that signature;
- a functor  $\text{Mod}^I : (\text{Sign}^I)^{op} \rightarrow \text{CAT}$ , giving for each signature  $\Sigma$  a category whose objects are called  $\Sigma$ -*models*, and whose arrows are called  $\Sigma$ -*(model) homomorphisms*; each arrow  $\varphi : \Sigma \rightarrow \Sigma' \in \text{Sign}^I$ , (i.e.,  $\varphi : \Sigma' \rightarrow \Sigma \in (\text{Sign}^I)^{op}$ ) is mapped into a functor  $\text{Mod}^I(\varphi) : \text{Mod}^I(\Sigma') \rightarrow \text{Mod}^I(\Sigma)$  called a *reduct functor*, whose effect is to cast a model of  $\Sigma'$  as a model of  $\Sigma$ ; when  $M = \text{Mod}^I(\varphi)(M')$  we say that  $M$  is the  $\varphi$ -*reduct* of  $M'$  and that  $M$  is an  $\varphi$ -*expansion* of  $M'$ ;
- a relation  $\models_{\Sigma}^I \subseteq |\text{Mod}^I(\Sigma)| \times \text{Sen}^I(\Sigma)$  for each  $\Sigma \in |\text{Sign}^I|$ , called the *satisfaction relation*,


such that for each morphism  $\varphi : \Sigma \rightarrow \Sigma' \in \text{Sign}^I$ , the satisfaction condition

$$M' \models_{\Sigma'}^I \rho \text{ iff } \text{Mod}^I(\varphi)(M') \models_{\Sigma}^I \rho \quad (1)$$

holds for each  $M' \in |\text{Mod}^I(\Sigma')|$  and  $\rho \in \text{Sen}^I(\Sigma)$ . Graphically,

$$\begin{array}{ccccc}
 \Sigma & & \text{Mod}^I(\Sigma) & \xrightarrow{\models_{\Sigma}^I} & \text{Sen}^I(\Sigma) \\
 \downarrow \varphi & & \uparrow \text{Mod}^I(\varphi) & & \downarrow \text{Sen}^I(\varphi) \\
 \Sigma' & & \text{Mod}^I(\Sigma') & \xrightarrow{\models_{\Sigma'}^I} & \text{Sen}^I(\Sigma')
 \end{array}$$

**Example 2.1** (The trivial institution *TRIV*) The simplest institution one can think of is *TRIV*. Its category of signatures,  $\text{Sign}^{TRIV}$ , is the *final category*, i.e., the category whose class of objects is the singleton set  $\{*\}$  and morphisms reduce to the identity  $1_*(*) = *$ . Functor  $\text{Sen}^{TRIV}$  sends object  $*$  into the empty set  $\emptyset$  and morphism  $1_*$  into the empty function. The models functor,  $\text{Mod}^{TRIV}$ , sends the signature  $*$  to the final category. Since the set of sentences is empty, the satisfaction condition holds trivially.

	<b>1650327</b>	<b>B</b>	Dispatch: 3/12/2014	Journal: FAC
	Jour. No		Ms. No.	Total pages: 21
			Disk Received <input type="checkbox"/>	Corrupted <input type="checkbox"/>
			Disk Used <input type="checkbox"/>	Mismatch <input type="checkbox"/>

114 *Example 2.2* (Propositional Logic  $PL$ ) A signature  $Prop \in | \text{Sign}^{PL} |$  in the institution  $PL$  is a set of symbols,  
 115 called propositional variables, and a signature morphism is just a function  $\varphi : Prop \rightarrow Prop'$ . Therefore,  $\text{Sign}^{PL}$   
 116 coincides with the category  $\text{Set}$ .

117 Functor  $\text{Mod}$  maps each signature  $Prop$  to the category  $\text{Mod}^{PL}(Prop)$  and each signature morphism  $\varphi$  to  
 118 the reduct functor  $\text{Mod}^{PL}(\varphi)$ . Objects of  $\text{Mod}^{PL}(Prop)$  are functions  $M : Prop \rightarrow \{\top, \perp\}$  and its morphisms  
 119 functions  $h : Prop \rightarrow Prop$  such that  $M(p) = M'(h(p))$ . Given a signature morphism  $\varphi : Prop \rightarrow Prop'$ ,  
 120 the reduct of a model  $M' \in | \text{Mod}^{PL}(Prop') |$ , say  $M = \text{Mod}^{PL}(\varphi)(M')$ , is defined, for each  $p \in Prop$ , as  
 121  $M(p) = M'(\varphi(p))$ .

122 Functor  $\text{Sen}^{PL}$  maps each signature  $Prop$  to the set of propositional sentences  $\text{Sen}^{PL}(Prop)$  and each morphism  
 123  $\varphi : Prop \rightarrow Prop'$  to the sentences' translation  $\text{Sen}^{PL}(\varphi) : \text{Sen}^{PL}(Prop) \rightarrow \text{Sen}^{PL}(Prop')$ . The set  $\text{Sen}^{PL}(Prop)$   
 124 is the usual set of propositional formulas defined by the grammar

$$125 \quad \rho ::= p \mid \rho \vee \rho \mid \rho \wedge \rho \mid \rho \Rightarrow \rho \mid \neg \rho$$

126 for  $p \in Prop$ . The translation of a sentence  $\text{Sen}^{PL}(\varphi)(\rho)$  is obtained by replacing each proposition of  $\rho$  by the  
 127 respective  $\varphi$ -image.

128 Finally, for each  $Prop \in \text{Sen}^{PL}$ , the satisfaction relation  $\models_{Prop}^{PL}$  is defined as usual:

- 129 –  $M \models_{Prop}^{PL} p$  iff  $M(p) = \top$ , for any  $p \in Prop$ ,
- 130 –  $M \models_{Prop}^{PL} \rho \vee \rho'$  iff  $M \models_{Prop}^{PL} \rho$  or  $M \models_{Prop}^{PL} \rho'$ .

131 and similarly for the other connectives.

132 *Example 2.3* (Equational logic  $EQ$ ) Signatures in the institution  $EQ$  of equational logic are pairs  $(S, F)$  where  
 133  $S$  is a set of sort symbols and  $F = \{F_{\text{ar} \rightarrow s} \mid \text{ar} \in S^*, s \in S\}$  is a family of sets of operation symbols indexed  
 134 by arities  $\text{ar}$  (for the arguments) and sorts  $s$  (for the results). *Signature morphisms* map both components in a  
 135 compatible way: they consist of pairs  $\varphi = (\varphi^{\text{st}}, \varphi^{\text{op}}) : (S, F) \rightarrow (S', F')$ , where  $\varphi^{\text{st}} : S \rightarrow S'$  is a function, and  
 136  $\varphi^{\text{op}} = \{\varphi_{\text{ar} \rightarrow s}^{\text{op}} : F_{\text{ar} \rightarrow s} \rightarrow F'_{\varphi^{\text{st}}(\text{ar}) \rightarrow \varphi^{\text{st}}(s)} \mid \text{ar} \in S^*, s \in S\}$  is a family of functions mapping operation symbols  
 137 according to their arities.


138 A model  $M$  for a signature  $(S, F)$  is an algebra interpreting each sort symbol  $s$  as a carrier set  $M_s$  and each  
 139 operation symbol  $\sigma \in F_{\text{ar} \rightarrow s}$  as a function  $M_\sigma : M_{\text{ar}} \rightarrow M_s$ , where  $M_{\text{ar}}$  is the product of the arguments'  
 140 carriers. This interpretation is extended to  $(S, F)$ -terms  $t = \sigma(t_1, \dots, t_n)$ , by  $M_{\sigma(t_1, \dots, t_n)} = M_\sigma(M_{t_1}, \dots, M_{t_n})$ .  
 141 Model morphisms are homomorphisms of algebras, i.e.,  $S$ -indexed families of functions  $\{h_s : M_s \rightarrow M'_s \mid s \in S\}$   
 142 such that for any  $m \in M_{\text{ar}}$ , and for each  $\sigma \in F_{\text{ar} \rightarrow s}$ ,  $h_s(M_\sigma(m)) = M'_\sigma(h_{\text{ar}}(m))$ . For each signature morphism  $\varphi$ ,  
 143 the *reduct* of a model  $M'$ , say  $M = \text{Mod}^{EQ}(\varphi)(M')$  is defined by  $(M)_x = M'_{\varphi(x)}$  for each sort and function symbol  
 144  $x$  from the domain signature of  $\varphi$ . The models functor maps signatures to categories of algebras and signature  
 145 morphisms to the respective reduct functors.

146 Sentences are universally quantified equations  $(\forall X)t = t'$ . Sentence translations along a signature morphism  
 147  $\varphi : (S, F) \rightarrow (S', F')$ , i.e.,  $\text{Sen}^{EQ}(\varphi) : \text{Sen}^{EQ}(S, F) \rightarrow \text{Sen}^{EQ}(S', F')$ , replace symbols of  $(S, F)$  by the respective  
 148  $\varphi$ -images in  $(S', F')$ . Functor  $\text{Sen}^{EQ}$  maps each signature to the set of universally quantified equations and each  
 149 signature morphism to the respective sentences translation.

150 The satisfaction relation is the usual Tarskian satisfaction defined recursively on the structure of the sentences  
 151 as follows:

- 152 •  $M \models_{(S, F)} t = t'$  when  $M_t = M_{t'}$ ,
- 153 •  $M \models_{(S, F)} (\forall X)\rho$  when  $M' \models_{(S, F \uplus X)} \rho$  for any *inc*-expansion  $M'$  of  $M$  where *inc* :  $(S, F) \hookrightarrow (S, F \uplus X)$  is  
 154 the inclusion morphism that enrich  $(S, F)$  with the set of variables  $X$ .

155 *Example 2.4* (Propositional Fuzzy Logic  $MVL_L$ ) Multi-valued logics [Got01] generalise classic logics by replac-  
 156 ing, as their *truth domain*, the 2-element Boolean algebra by larger sets structured as *complete residuate lattices*.  
 157 They were originally formalised as institutions in [ACEGG90] (see also [Dia11] for a recent reference).

	<b>1650327</b>	<b>B</b>	Dispatch: 3/12/2014	Journal: FAC
	Jour. No		Ms. No.	Total pages: 21
			Disk Received <input type="checkbox"/>	Corrupted <input type="checkbox"/>
			Disk Used <input type="checkbox"/>	Mismatch <input type="checkbox"/>

A *residuate lattice* is a tuple  $L = (\mathbf{L}, \leq, \wedge, \vee, \top, \perp, \otimes, \Rightarrow)$ , where

- $(\mathbf{L}, \wedge, \vee, \top, \perp)$  is a lattice ordered by  $\leq$ , with carrier  $\mathbf{L}$ , with (binary) infimum ( $\wedge$ ) and supremum ( $\vee$ ), and biggest and smallest elements  $\top$  and  $\perp$ ;
- $\otimes$  is an associative binary operation such that, for any elements  $x, y, z \in L$ ,
  - $x \otimes \top = \top \otimes x = x$ ,
  - $y \leq z$  implies that  $(x \otimes y) \leq (x \otimes z)$ ,
  - the following Galois connection holds:
 
$$y \leq (x \Rightarrow z) \text{ iff } x \otimes y \leq z.$$

A residuate lattice  $L$  is complete if any subset  $S \subseteq \mathbf{L}$  has infimum and supremum, denoted by  $\bigwedge S$  and  $\bigvee S$ , respectively.

Given a complete residuate lattice  $L$ , the institution  $MVLL_L$  is defined as follows:

- $MVLL_L$ -signatures are  $PL$ -signatures, i.e., signatures are sets  $Prop$  and morphisms are functions  $\varphi : Prop \rightarrow Prop'$ .
- Sentences of  $MVLL_L$  consist of pairs  $(\rho, p)$  where  $p$  is an element of  $L$  and  $\rho$  is defined as a  $PL$ -sentence over the set of connectives  $\{\Rightarrow, \vee, \top, \perp, \otimes\}$ .
- A  $MVLL_L$ -model  $M$  is a function  $M : Prop \rightarrow L$ ,
- For any  $M \in \text{Mod}^{MVLL_L}(Prop)$  and for any  $(\rho, p) \in \text{Sen}^{MVLL_L}(Prop)$ , the satisfaction relation is

$$M \models_{Prop}^{MVLL_L} (\rho, p) \text{ iff } p \leq (M \models \rho),$$

where  $M \models \rho$  is inductively defined as follows:

- for any proposition  $p \in Prop$ ,  $(M \models p) = M(p)$ ,
- $(M \models \top) = \top$ ,
- $(M \models \perp) = \perp$ ,
- $(M \models \rho_1 \star \rho_2) = (M \models \rho_1) \star (M \models \rho_2)$ , for  $\star \in \{\vee, \Rightarrow, \otimes\}$ .

This institution captures many multi-valued logics in the literature. For instance, taking  $L$  as the Łukasiewicz arithmetic lattice over the closed interval  $[0, 1]$ , where  $x \otimes y = 1 - \max\{0, x + y - 1\}$  (and  $x \Rightarrow y = \min\{1, 1 - x + y\}$ ), yields the standard *propositional fuzzy logic*.

## 2.2. Hybridisation

The *hybridisation* method proposed in [MMDB11, DM14, Mad13], enriches an arbitrary institution  $I = (\text{Sign}^I, \text{Sen}^I, \text{Mod}^I, (\models_{\Sigma}^I)_{\Sigma \in |\text{Sign}^I|})$  with the (modal) hybrid logic features and the corresponding Kripke semantics. The result is still an institution,  $\mathcal{HI}$ , called the *hybridisation of I*. The construction is revisited in the sequel. This overview is focussed on a simplified version, consisting of the quantifier-free and non-constrained version of the general method. The results in this paper are developed in the context of this simplified version, referred to as the hybridisation process.

*The category of  $\mathcal{HI}$ -signatures.* First of all the base signature is enriched with nominals and polyadic modalities. Therefore, the category of *I-hybrid signatures*, denoted by  $\text{Sign}^{\mathcal{HI}}$ , is defined as the direct (cartesian) product of categories:

$$\text{Sign}^{\mathcal{HI}} = \text{Sign}^I \times \text{Sign}^{REL}.$$

where  $REL$  is the sub-institution of (the institution of) single sorted first order logic, without non-constant operation symbols. Thus, signatures are triples  $(\Sigma, \text{Nom}, \Lambda)$ , where  $\Sigma \in |\text{Sign}^I|$  and, in the  $REL$ -signature  $(\text{Nom}, \Lambda)$ ,  $\text{Nom}$  is a set of constants called *nominals* and  $\Lambda$  is a set of relational symbols called *modalities*;  $\Lambda_n$  stands for the set of modalities of arity  $n$ . Morphisms  $\varphi \in \text{Sign}^{\mathcal{HI}}((\Sigma, \text{Nom}, \Lambda), (\Sigma', \text{Nom}', \Lambda'))$  are triples  $\varphi = (\varphi_{\text{Sign}}, \varphi_{\text{Nom}}, \varphi_{\text{MS}})$  where  $\varphi_{\text{Sign}} \in \text{Sign}^I(\Sigma, \Sigma')$ ,  $\varphi_{\text{Nom}} : \text{Nom} \rightarrow \text{Nom}'$  is a function and  $\varphi_{\text{MS}} = (\varphi_n : \Lambda_n \rightarrow \Lambda'_n)_{n \in \mathbb{N}}$  a  $\mathbb{N}$ -family of functions mapping nominals and  $n$ -ary-modality symbols, respectively.

	<b>1650327</b>	<b>B</b>	Dispatch: 3/12/2014	Journal: FAC
	Jour. No		Ms. No.	Total pages: 21
			Disk Received <input type="checkbox"/>	Corrupted <input type="checkbox"/>
			Disk Used <input type="checkbox"/>	Mismatch <input type="checkbox"/>

201 *Functor of the  $\mathcal{HL}$ -sentences.* The second step is to enrich the base sentences accordingly. The sentences of the  
 202 base institution and the nominals are taken as atoms and composed with the boolean connectives, modalities,  
 203 and satisfaction operators as follows:  $\text{Sen}^{\mathcal{HI}}(\Sigma, \text{Nom}, \Lambda)$  is the least set such that

- 204 •  $\text{Sen}^I(\Sigma) \subseteq \text{Sen}^{\mathcal{HI}}(\Delta)$ ,
- 205 •  $\text{Nom} \subseteq \text{Sen}^{\mathcal{HI}}(\Delta)$ ,
- 206 •  $\rho \star \rho' \in \text{Sen}^{\mathcal{HI}}(\Delta)$  for any  $\rho, \rho' \in \text{Sen}^{\mathcal{HI}}(\Delta)$  and any  $\star \in \{\vee, \wedge, \Rightarrow\}$ ,
- 207 •  $\neg\rho \in \text{Sen}^{\mathcal{HI}}(\Delta)$ , for any  $\rho \in \text{Sen}^{\mathcal{HI}}(\Delta)$ ,
- 208 •  $@_i\rho \in \text{Sen}^{\mathcal{HI}}(\Delta)$  for any  $\rho \in \text{Sen}^{\mathcal{HI}}(\Delta)$  and  $i \in \text{Nom}$ ,
- 209 •  $[\lambda](\rho_1, \dots, \rho_n)$ , for any  $\lambda \in \Lambda_{n+1}$ ,  $\rho_i \in \text{Sen}^{\mathcal{HI}}(\Delta)$ ,  $i \in \{1, \dots, n\}$ ,
- 210 •  $\langle\lambda\rangle(\rho_1, \dots, \rho_n)$ , for any  $\lambda \in \Lambda_{n+1}$ ,  $\rho_i \in \text{Sen}^{\mathcal{HI}}(\Delta)$ ,  $i \in \{1, \dots, n\}$ .

211 Given a  $\mathcal{HL}$ -signature morphism  $\varphi = (\varphi_{\text{Sign}}, \varphi_{\text{Nom}}, \varphi_{\text{MS}}) : (\Sigma, \text{Nom}, \Lambda) \rightarrow (\Sigma', \text{Nom}', \Lambda')$ , the translation of  
 212 sentences  $\text{Sen}^{\mathcal{HI}}(\varphi)$  is defined as follows:

- 213 •  $\text{Sen}^{\mathcal{HI}}(\varphi)(\rho) = \text{Sen}^I(\varphi_{\text{Sign}})(\rho)$  for any  $\rho \in \text{Sen}^I(\Sigma)$ ,
- 214 •  $\text{Sen}^{\mathcal{HI}}(\varphi)(i) = \varphi_{\text{Nom}}(i)$ ,
- 215 •  $\text{Sen}^{\mathcal{HI}}(\varphi)(\rho \star \rho') = \text{Sen}^{\mathcal{HI}}(\varphi)(\rho) \star \text{Sen}^{\mathcal{HI}}(\varphi)(\rho')$ ,  $\star \in \{\vee, \wedge, \Rightarrow\}$ ,
- 216 •  $\text{Sen}^{\mathcal{HI}}(\varphi)(\neg\rho) = \neg\text{Sen}^{\mathcal{HI}}(\varphi)(\rho)$ ,
- 217 •  $\text{Sen}^{\mathcal{HI}}(\varphi)(@_i\rho) = @_{\varphi_{\text{Nom}}(i)}\text{Sen}^{\mathcal{HI}}(\rho)$ ,
- 218 •  $\text{Sen}^{\mathcal{HI}}(\varphi)([\lambda](\rho_1, \dots, \rho_n)) = [\varphi_{\text{MS}}(\lambda)](\text{Sen}^{\mathcal{HI}}(\rho_1), \dots, \text{Sen}^{\mathcal{HI}}(\rho_n))$ ,
- 219 •  $\text{Sen}^{\mathcal{HI}}(\varphi)(\langle\lambda\rangle(\rho_1, \dots, \rho_n)) = \langle\varphi_{\text{MS}}(\lambda)\rangle(\text{Sen}^{\mathcal{HI}}(\rho_1), \dots, \text{Sen}^{\mathcal{HI}}(\rho_n))$ .

220  *$\mathcal{HL}$ -models functor* Models of the hybridised logic  $\mathcal{HL}$  can be regarded as  $(\Lambda)$ -relational structures whose  
 221 worlds are  $I$ -models. Formally  $(\Sigma, \text{Nom}, \Lambda)$ -models are pairs  $(M, W)$  where


- 222 •  $W$  is a  $(\text{Nom}, \Lambda)$ -model in  $REL$ , called a hybrid structure,
- 223 •  $M$  is a function  $| W | \rightarrow | \text{Mod}^I(\Sigma) |$ .

224 In each model  $(M, W)$ ,  $\{W_n \mid n \in \text{Nom}\}$  provides interpretations for *nominals* in  $\text{Nom}$ , whereas relations  $\{W_\lambda \mid$   
 225  $\lambda \in \Lambda_n, n \in \mathbb{N}\}$  interpret *modalities*  $\Lambda$ . We denote the  $I$ -model  $M(w)$  simply by  $M_w$ . The reduct definition is lifted  
 226 from the base institution  $I$ : the reduct of a  $\Delta'$ -model  $(M', W')$  along a signature morphism  $\varphi = (\varphi_{\text{Sign}}, \varphi_{\text{Nom}}, \varphi_{\text{MS}}) :$   
 227  $\Delta \rightarrow \Delta'$ , denoted by  $\text{Mod}^{\mathcal{HI}}(\varphi)(M', W')$ , is the  $\Delta$ -model  $(M, W)$  such that

- 228 •  $W$  is the  $(\varphi_{\text{Nom}}, \varphi_{\text{MS}})$ -reduct of  $W'$ , i.e.
  - 229 –  $| W | = | W' |$ ,
  - 230 – for any  $n \in \text{Nom}$ ,  $W_n = W'_{\varphi_{\text{Nom}}(n)}$ ,
  - 231 – for any  $\lambda \in \Lambda$ ,  $W_\lambda = W'_{\varphi_{\text{MS}}(\lambda)}$ ,
- 232 • for any  $w \in | W |$ ,  $M_w = \text{Mod}^I(\varphi_{\text{Sign}})(M'_w)$ .

233 *The Satisfaction Relation.* Let  $(\Sigma, \text{Nom}, \Lambda) \in | \text{Sign}^{\mathcal{HI}} |$  and  $(M, W) \in | \text{Mod}^{\mathcal{HI}}(\Sigma, \text{Nom}, \Lambda) |$ . For any  $w \in | W |$   
 234 we define:

- 235 •  $(M, W) \models^w \rho$  iff  $M_w \models^I \rho$ , when  $\rho \in \text{Sen}^I(\Sigma)$ ,
- 236 •  $(M, W) \models^w i$  iff  $W_i = w$ ; when  $i \in \text{Nom}$ ,
- 237 •  $(M, W) \models^w \rho \vee \rho'$  iff  $(M, W) \models^w \rho$  or  $(M, W) \models^w \rho'$ ,
- 238 •  $(M, W) \models^w \rho \wedge \rho'$  iff  $(M, W) \models^w \rho$  and  $(M, W) \models^w \rho'$ ,
- 239 •  $(M, W) \models^w \rho \Rightarrow \rho'$  iff  $(M, W) \models^w \rho$  implies that  $(M, W) \models^w \rho'$ ,
- 240 •  $(M, W) \models^w \neg\rho$  iff  $(M, W) \not\models^w \rho$ ,
- 241 •  $(M, W) \models^w @_j\rho$  iff  $(M, W) \models^{W_j} \rho$ ,
- 242 •  $(M, W) \models^w [\lambda](\xi_1, \dots, \xi_n)$  iff for any  $(w, w_1, \dots, w_n) \in W_\lambda$  we have that  $(M, W) \models^{w_i} \xi_i$  for some  $1 \leq i \leq n$ ,
- 243 •  $(M, W) \models^w \langle\lambda\rangle(\xi_1, \dots, \xi_n)$  iff there exists  $(w, w_1, \dots, w_n) \in W_\lambda$  such that and  $(M, W) \models^{w_i} \xi_i$  for any  $1 \leq i \leq n$ .

	<b>1650327B</b>	Dispatch: 3/12/2014	Journal: FAC
	Jour. No	Ms. No.	Total pages: 21
		Disk Received <input type="checkbox"/>	Not Used <input type="checkbox"/>
		Disk Used <input type="checkbox"/>	Corrupted <input type="checkbox"/>
			Mismatch <input type="checkbox"/>

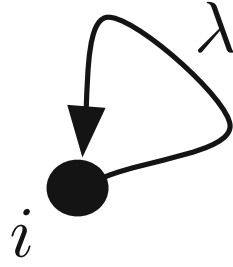


Fig. 1.  $\mathcal{H}TRIV$ -model

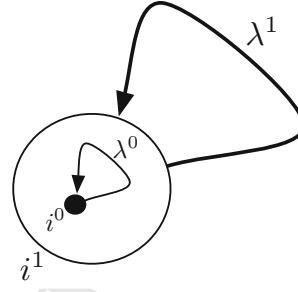


Fig. 2.  $\mathcal{H}^2TRIV$ -model

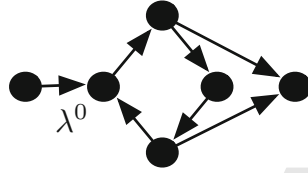


Fig. 3.  $\mathcal{H}TRIV$ -model

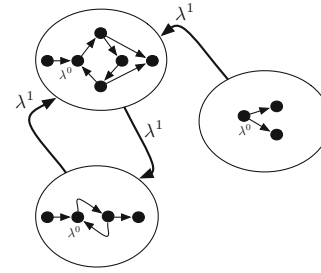


Fig. 4.  $\mathcal{H}^2TRIV$ -model

244 We write  $(M, W) \models \rho$  iff  $(M, W) \models^w \rho$  for any  $w \in |W|$ .

245 As expected,  $\mathcal{H}I$  is itself an institution satisfying the satisfaction condition:

246 **Theorem 2.1** [MMDB11] Let  $\Delta = (\Sigma, \text{Nom}, \Lambda)$  and  $\Delta' = (\Sigma', \text{Nom}', \Lambda')$  be two  $\mathcal{H}\mathcal{I}$ -signatures and  $\varphi : \Delta \rightarrow \Delta'$   
 247 a morphism of signatures. For any  $\rho \in \text{Sen}^{\mathcal{H}I}(\Delta)$ ,  $(M', W') \in |\text{Mod}^C(\Delta')|$ , and  $w \in |W'|$ ,

248  $\text{Mod}^{\mathcal{H}I}(\varphi)(M', W') \models^w \rho$  iff  $(M', W') \models^w \text{Sen}^{\mathcal{H}I}(\varphi)(\rho)$ .

249 Let us illustrate the method by applying it to the trivial institution (twice) as well as to the three other  
 250 institutions described above.

251 *Example 2.5* ( $\mathcal{H}TRIV$  and  $\mathcal{H}^2TRIV$ ) Let us consider the hybridisation of the institution  $TRIV$  of Example 2.1.  
 252 The signature category corresponds to

253 
$$\text{Sign}^{TRIV} \times \text{Sign}^{REL} \cong \text{Sign}^{REL}$$

254 Since  $\text{Sen}^{TRIV}(\ast) = \emptyset$ ,  $\text{Sen}^{\mathcal{H}TRIV}(\ast, \text{Nom}, \Lambda)$  is the set of sentences built up from nominals in  $\text{Nom}$  by the  
 255 application of modalities in  $\Lambda$  and boolean connectives. This kind of formulas are called *pure hybrid formulas* in  
 256 [BdRV01, Ind07]. Models of  $\text{Mod}^{\mathcal{H}TRIV}(\ast, \text{Nom}, \Lambda)$  are relational structures  $(W, M)$ , where  $M$  is the constant  
 257 function  $M_w = \ast$ , for any  $w \in |W|$  (see Figs. 1, 2).

258 An interesting institution for the specification of hierarchical state transition systems is obtained through  
 259 the hybridisation of  $\mathcal{H}TRIV$  i.e., the double hybridisation of  $TRIV$ , which we denote by  $\mathcal{H}^2TRIV$ . Models  
 260 of this institution are hybrid structures of hybrid structures (see Fig. 2). Thus  $\mathcal{H}^2TRIV$  signatures are triples  
 261  $((\ast, \text{Nom}^0, \Lambda^0), \text{Nom}^1, \Lambda^1)$  with  $\text{Nom}^0, \Lambda^0$  and  $\text{Nom}^1, \Lambda^1$  denoting the nominals and the modalities of the first  
 262 and second layer of hybridisation, respectively. In order to prevent ambiguities, we tag the symbols of each hybrid  
 263 signature, as well as the connectives and satisfaction operator introduced in each hybridisation, with 0 for the  
 264 first layer, and with 1 for the second one. For instance, the expression  $@_{j^1} k^0 \wedge^1 [\lambda^1](\rho_1, \dots, \rho_n)$  is a sentence of  
 265  $\mathcal{H}^2TRIV$  where the symbols  $k$  and  $j$  represent nominals of the first and second level of hybridisation, respectively.  
 266 Our tagging convention is extended also to  $\mathcal{H}^2TRIV$  models: a  $(P, \text{Nom}^0, \text{Nom}^1)$ -model is denoted by  $(M^1, W^1)$   
 267 where, for any  $w \in |W^1|$ , the models  $M_w^1$  are denoted by  $(W_w^0, M_w^0)$  (Figs. 3, 4).

268 *Example 2.6 (HPL)* The hybridisation of the propositional logic institution  $PL$  is an institution where signatures  
 269 are triples  $(Prop, Nom, \Lambda)$  and sentences are generated by

$$270 \quad \rho ::= \rho_0 \mid i \mid @_i \rho \mid \rho \odot \rho \mid \neg \rho \mid \langle \lambda \rangle (\rho, \dots, \rho) \mid [\lambda] (\rho, \dots, \rho) \quad (2)$$

271 where  $\rho_0 \in \text{Sen}^{PL}(Prop)$ ,  $i \in \text{Nom}$ ,  $\lambda \in \Lambda_n$  and  $\odot = \{\vee, \wedge, \Rightarrow\}$ . Note that there is a double level of connectives in  
 272 the sentences: one coming from base  $PL$ -sentences and another introduced by the hybridisation process. However,  
 273 they “semantically collapse” in the sense that the semantic interpretation of boolean connectives in both levels is  
 274 the same, and, hence, no distinction between them needs to be done. (see [DM14] for details). A  $(Prop, \text{Nom}, \Lambda)$ -  
 275 model is a pair  $(M, W)$ , where  $W$  is a transition structure with a set of worlds  $|W|$ . Constants  $W_i$ ,  $i \in \text{Nom}$ ,  
 276 stand for the named worlds and  $(n + 1)$ -ary relations  $W_\lambda$ ,  $\lambda \in \Lambda_n$ , are the accessibility relations characterising  
 277 the structure. For each world  $w \in |W|$ ,  $M(w)$  is a (local)  $PL$ -model assigning propositions in  $Prop$  to the world  
 278  $w$ .

279 Restricting the signatures to those with just a single unary modality (i.e., where  $\Lambda_2 = \{\lambda\}$  and  $\Lambda_n = \emptyset$  for  
 280  $n \neq 2$ ), results in the usual institution for classical hybrid propositional logic [Bra10].

281 *Example 2.7 (HMVL<sub>L</sub>)* The institution obtained through the hybridisation of  $MVL_L$ , for a fixed  $L$ , is similar to  
 282  $HPL$  defined above, but for two aspects,

- 283 • sentences are defined as in (2) but considering  $MVL$   $Prop$ -sentences  $(\rho_0, p)$  as atomic;
- 284 • a function, associated to each world  $w \in |W|$ , assigning to each proposition its value in  $L$ .

285 It is interesting to note that expressivity increases even if one restricts to the case of a (one-world) standard  
 286 semantics. For instance, differently from the base case where each sentence is tagged by a  $L$ -value, one may now  
 287 deal with more structured expressions involving several  $L$ -values, as in, for example,  $(\rho, p) \wedge (\rho', p')$ .


288 *Example 2.8 (HEQ)* Signatures of  $HEQ$  are triples  $((S, F), \text{Nom}, \Lambda)$  and sentences are defined as in (2) but taking  
 289  $(S, F)$ -equations  $(\forall X)t = t'$  as atomic base sentences. Models are hybrid structures with a (local)- $(S, F)$ -algebra  
 290 per world. This institution is a suitable framework to specify reconfigurable systems in a “configurations-as-  
 291 worlds” perspective: distinct configurations are modelled by distinct algebras; and reconfigurations are expressed  
 292 by transitions (cf. [MFMB11, Mad13]). Clearly, in this sort of specifications configurations can be specified  
 293 equationally, based on  $EQ$ -signatures, with an initial algebra interpretation. Nominals identify the “relevant”  
 294 configurations and reconfigurations amount to state transitions. Therefore, one resorts to local equations (i.e.  
 295 equations tagged by satisfaction operators  $@_i(\forall X)t = t'$ ) to specify local properties of named configurations;  
 296 to global equations, (i.e. non tagged equations) to specify global properties, i.e. properties true in any state; and,  
 297 finally, to modal features to specify the reconfigurability dynamics.

### 298 3. Bisimulation for hybridised logics

299 Having briefly reviewed what an institution is and how, through a systematic process, one may build upon an  
 300 arbitrary logic both modalities and nominals to explicitly refer to states in a specification, we may now focus on  
 301 the paper’s specific contribution. Our starting point is a method to specify reconfigurable software as transition  
 302 systems whose states represent particular configurations. Each state can endow an algebra, a relation structure  
 303 or even another, local transition system. Such two-staged specifications are common in the Software Engineering  
 304 practice (see, e.g., Gurevich’s Abstract State Machines [BS03]).

305 The originality of our method lies in its genericity: whatever logic is found useful to specify each concrete  
 306 configuration, a method is offered to compute its hybrid counterpart. In this setting, within the next three  
 307 sections, we look for suitable notions of equivalence and refinement for this kind of specifications. Naturally,  
 308 such notions should also be parametric on the base logic used, i.e. on the language in which the specification of  
 309 each concrete configuration is written. The price to pay is, of course, some extra notation and the use of a generic  
 310 framework—that of *institutions*—in which concepts can be formulated and results proved once and for all.

311 As the external layer of a reconfigurable system specification is that of a transition system, it is natural to  
 312 resort to suitable formulations of *bisimilarity* and *similarity* to capture equivalence and refinement, respectively.  
 313 The precise characterisation of such notions at the high level of abstraction chosen, is, in fact, the paper’s main  
 314 contribution.

	<b>1650327</b>	<b>B</b>	Dispatch: 3/12/2014	Journal: FAC
	Jour. No		Ms. No.	Total pages: 21
			Disk Received <input type="checkbox"/>	Corrupted <input type="checkbox"/>
			Disk Used <input type="checkbox"/>	Mismatch <input type="checkbox"/>



Intuitively a bisimulation relates worlds which exhibit the “same” (observable) information and preserve this property along transitions. Thus, to define a general notion of bisimulation over Kripke structures whose states are models of whatever base logic was chosen for expressing specifications, we have to make precise what the “same” information actually means. For example, if the system’s configurations are specified by *equations*, establish that two such configurations are bisimilar will certainly require that each specification generates the same variety. Actually, in this case they are essentially the same data type. In the more general setting of this paper the base logic  $I$  is a parameter and we have to deal with its hybridised version  $\mathcal{HI}$ .

Our proposal is, thus, to resort to the broader notion of *elementary equivalence* (see e.g. [Hod97]), and add to the definition of bisimulation the requirement that local configurations, i.e. local  $I$ -models related by a bisimulation have to be *elementarily equivalent*. Two models  $M, M' \in \text{Mod}(\Sigma)$  are elementarily equivalent if they satisfy the same sentences, as formalised in Definition 3.1 below.

In certain cases, as detailed below, it is convenient to restrict this equivalence by considering only a specific subset of sentences. For instance, we may want to identify *FOL*-models with elementarily equivalent algebraic reducts. As an illustration consider two models  $N_{\text{odd}}$  and  $N_{\text{even}}$  over the natural numbers, both with the operation  $+$ , one with a predicate *even* and the other with a predicate *odd*. Clearly they are not elementarily equivalent if we consider the entire set of sentences. However,  $N_{\text{odd}} \equiv^S N_{\text{even}}$ , for a subfunctor  $S$  of the sentences functor defined without making use of predicates. Another example, in hybrid Kripke semantics, is to consider models elementarily equivalent only at the frames level, which can be achieved by restricting the sentences to the so-called pure formulas (i.e. sentences without propositional variables). This can be done by parameterising the definition of elementary equivalence (and, consequently, those of bisimulation and refinement) with a subfunctor  $S$  of the sentences’ functor in order to capture the ‘right’ set of sentences, as proposed in [MMB13]. Doing this, however, is equivalent to restrict the base institution  $I$  to an institution defined as  $I$  but replacing  $\text{Sen}^I$  by  $S$ . In the sequel we stick to this alternative to simplify notation.

**Definition 3.1** Let  $M, M' \in \text{Mod}^I(\Sigma)$  be two models.  $M$  and  $M'$  are elementarily equivalent, in symbols  $M \equiv M'$ , if for any  $\rho \in \text{Sen}^I(\Sigma)$

$$M \models^I \rho \text{ iff } M' \models^I \rho. \quad (3)$$

Under the institution theory *motto—truth is invariant under change of notation—*we write  $M \equiv_{\varphi} M'$  whenever  $M \equiv \text{Mod}^I(\varphi)(M')$  for a given  $\varphi \in \text{Sign}^I(\Sigma, \Sigma')$ ,  $M \in \text{Mod}^I(\Sigma)$  and  $M' \in \text{Mod}^I(\Sigma')$ . Then  $M$  and  $M'$  are said to be  $\varphi$ -elementarily equivalent. If only the left to right implication of (3) holds, we write  $M \gg_{\varphi} M'$ .

Resorting to the satisfaction condition in  $I$ , the following characterisation of  $\varphi$ -elementary equivalence pops out:


**Corollary 3.1**  $M \equiv_{\varphi} M'$  iff, for any  $\rho \in \text{Sen}^I(\Sigma)$ ,  $M \models_{\Sigma}^I \rho \Leftrightarrow M' \models_{\Sigma}^I \text{Sen}^I(\varphi)(\rho)$ .

Note the role of  $\varphi$  above: as a signature morphism it captures the possible *change of notation* from a specification to another. For example it may cater for a renaming of propositions, as in Example 3.1, or signature components, as in Example 3.2. However, its pertinence becomes clearer in refinement situations, as discussed in the next section. At that level it may accommodate a number of forms of interface enrichment or adaptation (e.g. through the introduction of auxilliary operations).

Let us now define bisimulation in this general setting.

**Definition 3.2** Let  $\mathcal{HI}$  be the hybridisation of the institution  $I$  and  $\varphi \in \text{Sign}^{\mathcal{HI}}(\Delta, \Delta')$  a signature morphism. A  $\varphi$ -bisimulation between models  $(M, W) \in \text{Mod}^{\mathcal{HI}}(\Delta)$  and  $(M', W') \in \text{Mod}^{\mathcal{HI}}(\Delta')$  is a non-empty relation  $B_{\varphi} \subseteq |W| \times |W'|$  such that

- (i) for any  $wB_{\varphi}w'$ ,  $M_w \equiv_{\varphi_{\text{Sign}}} M'_{w'}$ ,
- (ii) for any  $wB_{\varphi}w'$ , and for any  $i \in \text{Nom}$ ,  $W_i = w$  iff  $W'_{\varphi_{\text{Nom}}(i)} = w'$ ,
- (iii) for any  $i \in \text{Nom}$ ,  $W_i B_{\varphi} W'_{\varphi_{\text{Nom}}(i)}$ ,
- (iv) For any  $\lambda \in \Lambda_n$ , if  $(w, w_1, \dots, w_n) \in W_{\lambda}$  and  $wB_{\varphi}w'$ , then for each  $k \in \{1, \dots, n\}$  there is a  $w'_k \in |W'|$  such that  $w_k B_{\varphi} w'_k$  and  $(w', w'_1, \dots, w'_n) \in W'_{\varphi_{\text{MS}}(\lambda)}$  (*zig-condition*),
- (v) For any  $\lambda \in \Lambda_n$  if  $(w', w'_1, \dots, w'_n) \in W'_{\varphi_{\text{MS}}(\lambda)}$  and  $wB_{\varphi}w'$ , then for each  $k \in \{1, \dots, n\}$  there is a  $w_k \in |W|$ , such that  $w_k B_{\varphi} w'_k$  and  $(w, w_1, \dots, w_n) \in W_{\lambda}$  (*zag-condition*).

	<b>1650327</b>	<b>B</b>	Dispatch: 3/12/2014	Journal: FAC
	Jour. No		Ms. No.	Total pages: 21
			Disk Received <input type="checkbox"/>	Corrupted <input type="checkbox"/>
			Disk Used <input type="checkbox"/>	Mismatch <input type="checkbox"/>

363 Note that clause (i) enforces local models of bisimilar states to be elementary equivalent. Clauses (ii) and  
 364 (iii) deal with nominals: named bisimilar states are identified by the same nominal (ii) and all of them are in the  
 365 bisimulation (iii). Finally, clauses (iv) and (v) correspond to the usual zig-zag conditions. As usual, a *bisimilarity*  
 366 relation can be defined as the greatest bisimulation whose existence is guaranteed by Lemma 3.1 below. Therefore,  
 367 we say that  $(M, W)$  and  $(M', W')$  are  $\varphi$ -bisimilar, and write  $(M, W) \rightleftharpoons_{\varphi} (M', W')$ , if there is a  $\varphi$ -bisimulation  
 368  $B_{\varphi}$  between them. Whenever  $\varphi$  is the identity we simply talk of a bisimulation  $B$  and the bisimilarity relation  $\rightleftharpoons$ .

369 **Lemma 3.1** *Let  $\mathcal{HI}$  be the hybridisation of the institution  $I$  and  $\varphi \in \text{Sign}^{\mathcal{HI}}(\Delta, \Delta')$  a signature morphism. The set*  
 370 *of  $\varphi$ -bisimulations between models  $(M, W) \in \text{Mod}^{\mathcal{HI}}(\Delta)$  and  $(M', W') \in \text{Mod}^{\mathcal{HI}}(\Delta')$  is closed under union.*

371 *Proof.* Let  $B_{\varphi}^0, B_{\varphi}^1 \subseteq |W| \times |W'|$  be two  $\varphi$ -bisimulations between models  $(M, W) \in \text{Mod}^{\mathcal{HI}}(\Delta)$  and  
 372  $(M', W') \in \text{Mod}^{\mathcal{HI}}(\Delta')$ . Their union  $B_{\varphi} = B_{\varphi}^0 \cup B_{\varphi}^1$  is also a  $\varphi$ -bisimulation because

- 373 1. Clearly, all points named by nominals are related by  $B_{\varphi}$  as they are either by  $B_{\varphi}^0$  or  $B_{\varphi}^1$ . Moreover, for any pair  
 374  $(w, w')$  such that  $wB_{\varphi}w'$  either  $wB_{\varphi}^0w'$  or  $wB_{\varphi}^1w'$ . As both  $B_{\varphi}^0$  and  $B_{\varphi}^1$  are  $\varphi$ -bisimulations, clauses (i), (ii) and  
 375 (iii) in Definition 3.2 hold for  $B_{\varphi}$ .
- 376 2. A similar argument applies to both (*zig*) and (*zag*) conditions. For clause (iv) let  $(w, w_1, \dots, w_n) \in W_{\lambda}$  and  
 377  $wB_{\varphi}w'$ . Then, either  $wB_{\varphi}^0w'$  or  $wB_{\varphi}^1w'$ . Then, for each  $k \in \{1, \dots, n\}$  there is a  $w'_k \in |W'|$  such that  $w_kB_{\varphi}^0w'_k$   
 378 or  $w_kB_{\varphi}^1w'_k$ , i.e.,  $w_kB_{\varphi}w'_k$ , and  $(w', w'_1, \dots, w'_n) \in W'_{\varphi_{\text{MS}}(\lambda)}$ . The (*zag*) condition is proved similarly.  $\square$

379 Consider, now, the relational composition of bisimulations.

380 **Lemma 3.2** *Let  $\mathcal{HI}$  be the hybridisation of the institution  $I$ ,  $\varphi \in \text{Sign}^{\mathcal{HI}}(\Delta, \Delta'')$  and  $\psi \in \text{Sign}^{\mathcal{HI}}(\Delta'', \Delta')$  two*  
 381 *signature morphisms. Consider a  $\varphi$ -bisimulation  $B_{\varphi}$  between models  $(M, W) \in \text{Mod}^{\mathcal{HI}}(\Delta)$  and  $(M'', W'') \in$   
 382  $\text{Mod}^{\mathcal{HI}}(\Delta'')$  and a  $\psi$ -bisimulation  $B_{\psi}$  between models  $(M'', W'') \in \text{Mod}^{\mathcal{HI}}(\Delta'')$  and  $(M', W') \in \text{Mod}^{\mathcal{HI}}(\Delta')$ .*  
 383 *Then  $B_{\psi} \cdot B_{\varphi}$  is a  $(\psi \cdot \varphi)$ -bisimulation between models  $(M, W)$  and  $(M', W')$ .*

384 *Proof.* Let  $wB_{\psi} \cdot B_{\varphi}w'$ . Therefore, there is a  $w'' \in |W''|$  such that  $wB_{\varphi}w''$  and  $w''B_{\psi}w'$ . Then, for any  $i \in \text{Nom}$ ,  
 385  $W_i = w$  iff  $W''_{\varphi_{\text{Nom}}(i)} = w''$  iff  $W'_{\psi_{\text{Nom}}(i)} = w'$ , which proves clause (ii) in Definition 3.2. Clauses (i) and (iii) follow  
 386 from similar arguments, considering, for the former, that elementary equivalence is an equivalence relation. To  
 387 establish (iv) suppose that  $(w, w_1, \dots, w_n) \in W_{\lambda}$ . As  $B_{\varphi}$  is a  $\varphi$ -bisimulation, for each  $k \in \{1, \dots, n\}$  there is  $w''_k$   
 388 such that  $w_kB_{\varphi}w''_k$  and  $(w'', w''_1, \dots, w''_n) \in W''_{\lambda}$ . As  $B_{\psi}$  is a  $\psi$ -bisimulation, there is also a  $w'_k$  such that  $w''_kB_{\psi}w'_k$   
 389 and  $(w', w'_1, \dots, w'_n) \in W'_{\lambda}$ , which establishes the (*zig*)-condition for relation  $B_{\psi} \cdot B_{\varphi}$ . The (*zag*)-condition, (v), is  
 390 shown similarly.  $\square$

391 Clearly,

392 **Corollary 3.2**  $\rightleftharpoons$  is an equivalence relation.

393 *Proof.* If no change of signature is involved, this follows from Lemma 3.2 for  $\varphi, \psi$  the identity, together with the  
 394 observation that the identity relation and the converse of a *id*-bisimulation are themselves *id*-bisimulations (for  
 395 the latter resort to the (*zig*) and (*zag*) conditions interchangeably).  $\square$


396 **Theorem 3.1** *Let  $\mathcal{HI}$  be the hybridisation of the institution  $I$  and  $\varphi \in \text{Sign}^{\mathcal{HI}}(\Delta, \Delta')$  a signature morphism. Let*  
 397  *$(M', W') \in \text{Mod}^{\mathcal{HI}}(\Delta')$ . Then,*

$$398 \quad \text{Mod}^{\mathcal{HI}}(\varphi)(M', W') \rightleftharpoons_{\varphi} (M', W')$$

399 *witnessed by the identity relation.*

400 *Proof.* All the conditions in Definition 3.2 follow from the definition of reduct of  $\mathcal{HI}$ .  $\square$

401 **Example 3.1** (Bisimulation in  $\mathcal{HPL}$ ) Let us instantiate Definition 3.2 for the  $\mathcal{HPL}$  case (cf. Example 2.2). More  
 402 precisely, a sub-institution of  $\mathcal{HPL}$  with  $\Lambda_2 = \{\lambda\}$  and  $\Lambda_n = \emptyset$  for  $n \neq 2$ . A bisimulation  $B$  is such that  
 403  $(M, W)B(M', W')$ , for any two models  $(M, W), (M', W') \in |\text{Mod}^{\mathcal{HPL}}(P, \text{Nom}, \{\lambda\})|$ , if

	<b>1650327</b>	<b>B</b>	Dispatch: 3/12/2014	Journal: FAC
	Jour. No		Ms. No.	Total pages: 21
			Disk Received <input type="checkbox"/>	Corrupted <input type="checkbox"/>
			Disk Used <input type="checkbox"/>	Mismatch <input type="checkbox"/>

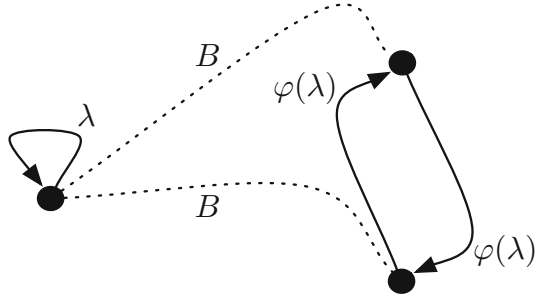


Fig. 5.  $\mathcal{H}TRIV$ -Bisimulation

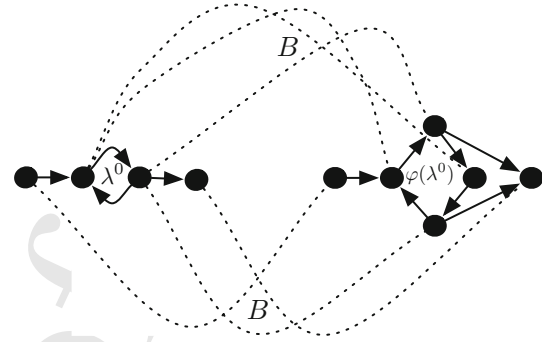


Fig. 6.  $\mathcal{H}TRIV$ -Bisimulation

- 404 (i)  $M_w \equiv M_{w'}$ , i.e., bisimilar states satisfy the same sentences,
- 405 (ii) for any  $i \in \text{Nom}$ ,  $wBw'$ ,  $w = W_i$  iff  $w' = W'_i$ ,
- 406 (iii) for any  $i \in \text{Nom}$ ,  $W_iB W'_i$ ,
- 407 (iv) for any  $(w, w_1) \in W_\lambda$  with  $wBw'$ , there is a  $w'_1 \in |W'|$  such that  $w_1Bw'_1$  and  $(w', w'_1) \in W'_\lambda$ ,
- 408 (v) for any  $(w', w'_1) \in W'_\lambda$  with  $wBw'$ , there is a  $w_1 \in |W|$  such that  $w_1Bw'_1$  and  $(w, w_1) \in W_\lambda$ .

409 Note that condition (i) is equivalent to say that bisimilar states are assigned the same set of propositions (for any  
 410  $p \in P$ ,  $M_w(p) = \top$  iff  $M_{w'}(p) = \top$ ). As expected, this definition corresponds exactly to standard bisimulation  
 411 for propositional hybrid logic (see, e.g. [tC05, Defn. 4.1.1]).

412 The definition of bisimulation computed in the previous example can also capture the case of propositional  
 413 modal logic: just consider pure modal signatures (i.e. with an empty set of nominals), as condition (i) is trivially  
 414 satisfied. Moreover, instantiating Theorem 4.1 below, we get the classical result about preservation of modal truth  
 415 by bisimulation.

416 *Example 3.2* (Bisimulation for  $\mathcal{H}EQ$ ) Consider now the instantiation of 3.2 for  $\mathcal{H}EQ$  (cf. Ex 2.8). All one has to  
 417 do is to replace condition (ii) in Defn 3.2 by its instantiation for algebras: two algebras are elementarily equivalent  
 418 if the respective generated varieties coincide [Grä79].

419 *Example 3.3* (Bisimulation in  $\mathcal{H}TRIV$  and  $\mathcal{H}^2TRIV$ ) Let us play the same game for  $\mathcal{H}TRIV$ . Since there are  
 420 no sentences in  $\text{Sen}^{TRIV}(\ast)$ , property (i) trivially holds. Hence bisimulations for  $\mathcal{H}TRIV$  consist of standard  
 421 bisimulations in labeled transition systems with the additional assumptions on named states [clauses (ii) and (iii)  
 422 in Definition 3.2]. Two examples are depicted in Figs. 5 and 6.

423 Finally, consider bisimulations in  $\mathcal{H}^2TRIV$ . At the local level, according to the forthcoming Theorem 4.2  
 424 it is enough to have a total and surjective bisimulation to guarantee elementary equivalence in condition (i).  
 425 Therefore, bisimulation in  $\mathcal{H}^2TRIV$  follows from hierarchical bisimulation between structured transition systems.  
 426 An example is depicted in Fig. 7 where  $B^0$  and  $B^1$  are the bisimulations at the local and global levels, respectively.  
 427 Another example is illustrated in Fig. 8.

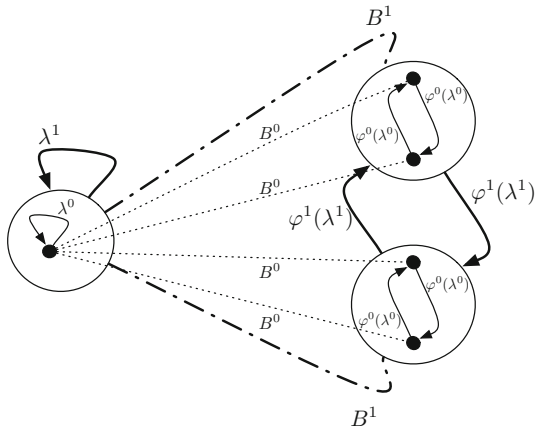
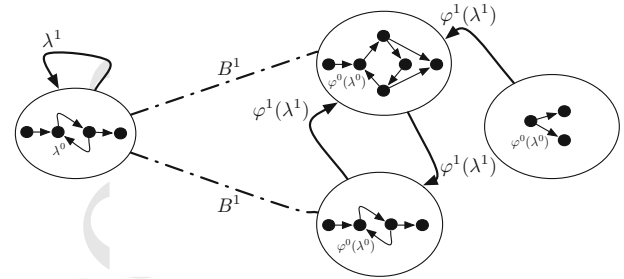
#### 428 4. A Hennessy–Milner theorem

429 This section discusses the relationship between bisimulation and logical equivalence in the context of hybridised  
 430 logics. The following result establishes that (local)-hybrid satisfaction is invariant under  $\varphi$ -bisimulations:

431 **Theorem 4.1** *Let  $\mathcal{H}I$  be the hybridisation of the institution  $I$  and  $\varphi \in \text{Sign}^{\mathcal{H}I}(\Delta, \Delta')$  a signature morphism. Let*  
 432  $B_\varphi \subseteq |W| \times |W'|$  *be a  $\varphi$ -bisimulation. Then, for any  $wB_\varphi w'$  and for any  $\rho \in \text{Sen}^{\mathcal{H}I}(\Delta)$ ,*

433  $(M, W) \models^w \rho$  *iff*  $(M', W') \models^{w'} \text{Sen}^{\mathcal{H}I}(\varphi)(\rho)$ . (4)

	<b>1650327</b>	<b>B</b>	Dispatch: 3/12/2014	Journal: FAC
	Jour. No		Ms. No.	Total pages: 21
			Disk Received <input type="checkbox"/>	Corrupted <input type="checkbox"/>
			Disk Used <input type="checkbox"/>	Mismatch <input type="checkbox"/>

Fig. 7.  $\mathcal{H}^2$  TRIV-BisimulationFig. 8.  $\mathcal{H}^2$  TRIV-Bisimulation

434 *Proof.* The proof is by induction on the structure of the sentences.

435 1.  $\rho = i$  for some  $i \in \text{Nom}$ :

436  $(M, W) \models^w i$

437  $\Leftrightarrow \{ \text{definition of } \models^w \}$

438  $W_i = w$

439  $\Leftrightarrow \{ \text{clause (ii) of Definition 3.2} \}$

440  $W'_{\varphi(i)} = w'$

441  $\Leftrightarrow \{ \text{definition of } \models^{w'} \}$

442  $(M', W') \models^{w'} \varphi_{\text{Nom}}(i)$

443  $\Leftrightarrow \{ \text{definition of } \text{Sen}^{\mathcal{H}I}(\varphi) \}$

444  $(M', W') \models^{w'} \text{Sen}^{\mathcal{H}I}(\varphi)(i)$

445 2.  $\rho \in \text{Sen}^I(\Sigma)$ :

446  $(M, W) \models^w \rho$

447  $\Leftrightarrow \{ \text{definition of } \models^w \}$

448  $M_w \models^I \rho$

449  $\Leftrightarrow \{ \text{by hypothesis } M_w \equiv_{\varphi_{\text{Sign}}} M'_{w'} \text{ and Corollary 3.1} \}$

450  $M'_{w'} \models \text{Sen}^I(\varphi_{\text{Sign}})(\rho)$

451  $\Leftrightarrow \{ \text{definition of } \models^{w'} \}$

452  $(M', W') \models^{w'} \text{Sen}^I(\varphi_{\text{Sign}})(\rho)$

453  $\Leftrightarrow \{ \text{definition of } \text{Sen}^{\mathcal{H}I}(\varphi) \}$

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

455 3.  $\rho = \xi \vee \xi'$  for some  $\xi, \xi' \in \text{Sen}^{\mathcal{H}I}(\Delta)$ :

456  $(M, W) \models^w \xi \vee \xi'$

457  $\Leftrightarrow \{ \text{definition of } \models^w \}$

458  $(M, W) \models^w \xi \text{ or } (M, W) \models^w \xi'$

	<b>1650327</b>	<b>B</b>	Dispatch: 3/12/2014	Journal: FAC
	Jour. No		Ms. No.	Total pages: 21
			Disk Received <input type="checkbox"/>	Corrupted <input type="checkbox"/>
			Disk Used <input type="checkbox"/>	Mismatch <input type="checkbox"/>

$$\begin{aligned}
459 \quad & \Leftrightarrow \quad \{ \text{induction hypothesis} \} \\
460 \quad & (M', W') \models^{w'} \text{Sen}^{\mathcal{H}I}(\varphi)(\xi) \text{ or} \\
461 \quad & (M', W') \models^{w'} \text{Sen}^{\mathcal{H}I}(\varphi)(\xi') \\
462 \quad & \Leftrightarrow \quad \{ \text{definition of } \models^w \} \\
463 \quad & (M', W') \models^{w'} \text{Sen}^{\mathcal{H}I}(\varphi)(\xi \vee \xi')
\end{aligned}$$

464 The proofs for cases  $\rho = \xi \wedge \xi'$ ,  $\rho = \xi \Rightarrow \xi'$ ,  $\rho = \neg\xi$ , etc. are analogous.

465 4.  $\rho = [\lambda](\xi_1, \dots, \xi_n)$  for some  $\xi_1, \dots, \xi_n \in \text{Sen}^{\mathcal{H}I}(\Delta)$ ,  $\lambda \in \Lambda_{n+1}$ :

$$\begin{aligned}
466 \quad & (M, W) \models^w [\lambda](\xi_1, \dots, \xi_n) \\
467 \quad & \Leftrightarrow \quad \{ \text{definition of } \models^w \} \\
468 \quad & \text{for any } (w, w_1, \dots, w_n) \in W_\lambda \text{ there is some } k \in \{1, \dots, n\} \\
469 \quad & \text{such that } (M, W) \models^{w_k} \xi_k \\
470 \quad & \Leftrightarrow \quad \{ * \} \\
471 \quad & \text{for any } (w', w'_1, \dots, w'_n) \in W'_{\varphi_{\text{MS}}(\lambda)} \text{ there is some} \\
472 \quad & p \in \{1, \dots, n\} \text{ such that } (M', W') \models^{w'_p} \text{Sen}^{\mathcal{H}I}(\varphi)(\xi_p) \\
473 \quad & \Leftrightarrow \quad \{ \text{definition of } \models^{w'} \} \\
474 \quad & (M', W') \models^{w'} [\varphi_{\text{MS}}(\lambda)](\text{Sen}^{\mathcal{H}I}(\varphi)(\xi_1), \dots, \text{Sen}^{\mathcal{H}I}(\varphi)(\xi_n)) \\
475 \quad & \Leftrightarrow \quad \{ \text{definition of } \text{Sen}^{\mathcal{H}I}(\varphi) \} \\
476 \quad & (M', W') \models^{w'} \text{Sen}^{\mathcal{H}I}(\varphi)([\lambda](\xi_1, \dots, \xi_n))
\end{aligned}$$


477 For the step marked with \* we proceed as follows. Assuming  $(w', w'_1, \dots, w'_n) \in W'_{\varphi_{\text{MS}}(\lambda)}$  with  $w \mathbf{B}_\varphi w'$ , we have  
478 by clause (v) of Definition 3.2 that there are  $w_k$ , with  $k \in \{1, \dots, n\}$ , such that  $(w, w_1, \dots, w_n) \in W_\lambda$ . By  
479 hypothesis,  $(M, W) \models^{w_p} \xi_p$  for some  $p \in \{1, \dots, n\}$ . Moreover, by the induction hypothesis,  $(M', W') \models^{w'_p}$   
480  $\text{Sen}^{\mathcal{H}I}(\varphi)(\xi_p)$ . Clause (iv) of Definition 3.2 entails the converse implication. The proof for sentences with  
481 shape  $\rho = \langle \lambda \rangle(\xi_1, \dots, \xi_n)$  is analogous.

482 5.  $\rho = @_i \xi$  for some  $\xi \in \text{Sen}^{\mathcal{H}I}(\Delta)$  and  $i \in \text{Nom}$ :

$$\begin{aligned}
483 \quad & (M, W) \models^w @_i \xi \\
484 \quad & \Leftrightarrow \quad \{ \text{definition of } \models^w \} \\
485 \quad & (M, W) \models^{W_i} \xi \\
486 \quad & \Leftrightarrow \quad \{ \text{induction hypothesis and clause (iii) of Definition 3.2} \} \\
487 \quad & (M', W') \models^{W'_{\varphi_{\text{Nom}}(i)}} \text{Sen}^{\mathcal{H}I}(\varphi)(\xi) \\
488 \quad & \Leftrightarrow \quad \{ \text{definition of } \models^w \} \\
489 \quad & (M', W') \models^w @_{\varphi_{\text{Nom}}(i)} \text{Sen}^{\mathcal{H}I}(\varphi)(\xi) \\
490 \quad & \Leftrightarrow \quad \{ \text{definition of } \text{Sen}^{\mathcal{H}I}(\varphi) \} \\
491 \quad & (M', W') \models^w \text{Sen}^{\mathcal{H}I}(\varphi)(@_i \xi)
\end{aligned}$$

□

493 As in the standard modal case the converse of Theorem 4.1 does not hold in general, i.e., logical equivalence  
494 is not a bisimulation. Such is the case, however, for image-finite Kripke models, as well known from the plain  
495 case of modal logic [BVB07]. A model  $(M, W)$  is *image-finite* if for each state  $w \in W$  and each relation  $W_\lambda$ ,  
496  $\lambda \in \Lambda$ , the set  $\{(w_1, \dots, w') : (w, w_1, \dots, w') \in W_\lambda\}$  is finite. No condition is imposed on the number of relations  
497 present or the cardinality of  $W$ .

	<b>1650327</b>	<b>B</b>	Dispatch: 3/12/2014	Journal: FAC
	Jour. No		Ms. No.	Total pages: 21
			Disk Received <input type="checkbox"/>	Corrupted <input type="checkbox"/>
			Disk Used <input type="checkbox"/>	Mismatch <input type="checkbox"/>

We are, thus, prepared to state and prove the following Hennessy–Milner like theorem:

**Theorem 4.2** Let  $\mathcal{HI}$  be the hybridisation of the institution  $I$  and  $\varphi \in \text{Sign}^{\mathcal{HI}}(\Delta, \Delta')$  a signature morphism. Let  $(M, W)$  and  $(M', W')$  be two image-finite  $\Delta$  and  $\Delta'$ -models, respectively. Then, for every  $w \in W$  and  $w' \in W'$ , the following conditions are equivalent:

- (i)  $(M, W) \models^w \rho$  iff  $(M', W') \models^{w'} \text{Sen}^{\mathcal{HI}}(\varphi)(\rho)$ , for any formula  $\rho$ ,
- (ii) There is a  $\varphi$ -bisimulation  $B_\varphi \subseteq |W| \times |W'|$  such that  $wB_\varphi w'$ .

*Proof.* We have just to prove that (i) implies (ii). Let us prove that

$$Z := \{(w, w') \in W \times W' : \text{for any } \rho, (M, W) \models^w \rho \text{ iff } (M', W') \models^{w'} \text{Sen}^{\mathcal{HI}}(\varphi)(\rho)\}$$

is a bisimulation.

The atomic conditions trivially hold. For the (zig) condition, let  $\lambda \in \Lambda$  be, without loss of generality, a binary modality symbol. Assume that  $wZw'$  and let  $u \in W$  such that  $wW_\lambda u$ . To obtain a contradiction, suppose that there is no  $u' \in W'$  with  $w'W'_\lambda u'$  and  $uZu'$ . As in the standard case the image-finite condition makes  $S' = \{u' : w'W'_\lambda u'\}$  finite. Moreover,  $S'$  cannot be empty since in such a case  $(M, W) \models^w [\lambda]\neg(@_i i)$  [equivalently,  $(M, W) \models^w \neg(\lambda)(@_i i)$ ], which is incompatible with the fact that  $(M, W) \models^w \langle \lambda \rangle (@_i i)$ , which holds because  $wW_\lambda u$ .

By assumption, for every  $v \in S'$  there is a formula  $\psi_v$  such that  $(M, W) \models^u \psi_v$  and it is false that  $(M', W') \models^{v'} \text{Sen}^{\mathcal{HI}}(\varphi)(\psi_v)$ . Consider now the conjunction

$$\psi = \bigwedge_{v \in S'} \psi_v$$

of all of these formulas. Then, on the one hand,  $(M, W) \models^w \langle \lambda \rangle \psi$ . On the other, however, for all  $v \in S'$ , it is false that  $(M', W') \models^{v'} \text{Sen}^{\mathcal{HI}}(\varphi)(\langle \lambda \rangle \psi)$ . This contradicts the fact that  $wZw'$ .

The (zag) condition is shown in a similar way. □

## 5. Forward and backward refinement

Consider again a reconfigurable system described by a set of configurations and a transition structure entailing changes from one to another. If equivalence of such systems corresponds to a notion of bisimilarity in which bisimilar configurations are enforced to be elementary equivalent, a *refinement* relation corresponds to *similarity*. This can be defined in two different ways. One of them entails preservation of transitions from the abstract to the concrete model; the other proceeds dually.

### 5.1. Forward refinement

Forward refinement means that behaviours (on the system's global dynamics) valid in the abstract model are also allowed in the concrete one, which, however, may exhibit further behaviour. On the other hand, at each local configuration, the original properties are preserved along local refinement. We call this *forward* refinement.

**Definition 5.1** Let  $\mathcal{HI}$  be the hybridisation of an institution  $I$  and  $\varphi \in \text{Sign}^{\mathcal{HI}}(\Delta, \Delta')$  a signature morphism. A *forward  $\varphi$ -refinement relation between models*  $(M, W) \in \text{Mod}^{\mathcal{HI}}(\Delta)$  and  $(M', W') \in \text{Mod}^{\mathcal{HI}}(\Delta')$  is a non-empty relation  $R_\varphi \subseteq |W| \times |W'|$  such that, for any  $wR_\varphi w'$ ,

- (i)  $M_w \gg_\varphi M'_{w'}$ ,
- (ii) for any  $i \in \text{Nom}$ , if  $W_i = w$  then  $W'_{\varphi_{\text{Nom}}(i)} = w'$ ,
- (iii) for any  $i \in \text{Nom}$ ,  $W_i R_\varphi W'_{\varphi_{\text{Nom}}(i)}$ ,
- (iv) for any  $\lambda \in \Lambda_n$ , if  $(w, w_1, \dots, w_n) \in W_\lambda$  then for each  $k \in \{1, \dots, n\}$  there is a  $w'_k \in |W'|$  such that  $w_k R_\varphi w'_k$  and  $(w', w'_1, \dots, w'_n) \in W'_{\varphi_{\text{MS}}(\lambda)}$ .

	<b>1650327</b>	<b>B</b>	Dispatch: 3/12/2014	Journal: FAC
	Jour. No		Ms. No.	Total pages: 21
			Disk Received <input type="checkbox"/>	Corrupted <input type="checkbox"/>
			Disk Used <input type="checkbox"/>	Mismatch <input type="checkbox"/>

537 We say that  $(M', W')$  is a *forward  $\varphi$ -refinement* of  $(M, W)$ , in symbols  $(M, W) \rightarrow_{\varphi} (M', W')$ , if there is a forward  
538  $\varphi$ -refinement between them. When  $\varphi$  is the identity we denote it simply by  $\rightarrow$ .

539 The relevant question is whether (forward) refinement preserves (hybrid) satisfaction. Actually, this is not  
540 the case. Note that in the proof of Theorem 4.1 preservation of hybrid satisfaction of sentences of the form  
541  $[\lambda](\xi_1, \dots, \xi_n)$  is entailed by conditions (iv) and (v) of Definition 3.2, but the latter is not considered in a (forward)  
542 refinement situation. Boxed formulas are, as a matter of fact, not preserved. As a simple counter-example, define  
543 a  $R_{\varphi}$ -refinement from a  $\Delta$ -hybrid model  $(M, W)$  with  $|W| = \{w\}$  and  $W_{\lambda} = \emptyset$ , for  $\lambda \in \Lambda_n$ , to any other  $\Delta'$ -  
544 hybrid model  $(M', W')$  such that  $\text{Mod}^{\mathcal{H}I}(\varphi_{\text{Sign}})(M')_{w'} = M_w$  for some  $w' \in |W'|$ . Any sentence  $[\lambda](\xi_1, \dots, \xi_n)$ ,  
545 which trivially holds in the world  $w$  of  $(M, W)$ , may fail to be satisfied in the  $R_{\varphi}$ -related world  $w'$  of  $(M', W')$ .  
546 Negative sentences  $\neg\xi$ , are also in general not preserved through refinement because, only the (zig) condition  
547 being enforced, non satisfaction in one direction does not imply non satisfaction in the other.

548 **Definition 5.2** (*Positive existential sentences*) The positive existential sentences of a signature  $\Delta \in |\text{Sign}^{\mathcal{H}I}|$  are  
549 given by the subfunctor  $\text{Sen}_{\diamond}^{\mathcal{H}I} \subseteq \text{Sen}^{\mathcal{H}I}$  defined inductively for each signature  $\Delta$  as  $\text{Sen}^{\mathcal{H}I}(\Delta)$ , but excluding both  
550 negation and boxed formulas. For each signature morphism  $\varphi : \Delta \rightarrow \Delta'$ ,  $\text{Sen}_{\diamond}^{\mathcal{H}I}(\varphi)$  is the restriction of  $\text{Sen}^{\mathcal{H}I}(\varphi)$   
551 to  $\text{Sen}_{\diamond}^{\mathcal{H}I}(\Delta)$ .

552 **Theorem 5.1** *Let  $\mathcal{H}I$  be the hybridisation of an institution  $I$ ,  $\varphi \in \text{Sign}^{\mathcal{H}I}(\Delta, \Delta')$  a signature morphism,  $R_{\varphi}$  a  $\varphi$ -  
553 refinement relation and  $(M, W) \in \text{Mod}^{\mathcal{H}I}(\Delta)$  and  $(M', W') \in \text{Mod}^{\mathcal{H}I}(\Delta')$  two models such that  $(M', W')$  is a  
554 forward refinement of  $(M, W)$  witnessed by relation  $R_{\varphi}$ . Then, for any  $wR_{\varphi}w'$  and  $\rho \in \text{Sen}_{\diamond}^{\mathcal{H}I}(\Delta)$ ,*

$$555 \quad (M, W) \models^w \rho \text{ implies that } (M', W') \models^{w'} \text{Sen}_{\diamond}^{\mathcal{H}I}(\varphi)(\rho).$$

556 *Proof.* The proof is by induction on the structure of the existential positive sentences and comes directly from  
557 the proof of Theorem 4.1, taking the left to right implication. What remains to be proved is the case  $\rho =$   
558  $\langle \lambda \rangle(\xi_1, \dots, \xi_n)$ . Thus,

$$559 \quad (M, W) \models^w \langle \lambda \rangle(\xi_1, \dots, \xi_n)$$

$$560 \quad \Leftrightarrow \quad \{ \text{definition of } \models^w \}$$

$$561 \quad \text{there exists } (w, w_1, \dots, w_n) \in W_{\lambda}$$

$$562 \quad \text{such that } (M, W) \models^{w_k} \xi_k \text{ for any } k \in \{1, \dots, n\}$$

$$563 \quad \Rightarrow \quad \{ \text{By (iii) and (iv) (the (zig) condition) and the induction hypothesis.} \}$$

$$564 \quad \text{there exists } (w', w'_1, \dots, w'_n) \in W'_{\varphi_{\text{MS}}(\lambda)}$$

$$565 \quad \text{such that } (M', W') \models^{w'_k} \xi_k \text{ for any } k \in \{1, \dots, n\}$$

$$566 \quad \Leftrightarrow \quad \{ \text{definition of } \models^{w'} \}$$

$$567 \quad (M', W') \models^{w'} \langle \varphi_{\text{MS}}(\lambda) \rangle (\text{Sen}^{\mathcal{H}I}(\varphi)(\xi_1), \dots, \text{Sen}^{\mathcal{H}I}(\varphi)(\xi_n))$$


$$568 \quad \Leftrightarrow \quad \{ \text{definition of } \text{Sen}^{\mathcal{H}I}(\varphi) \}$$

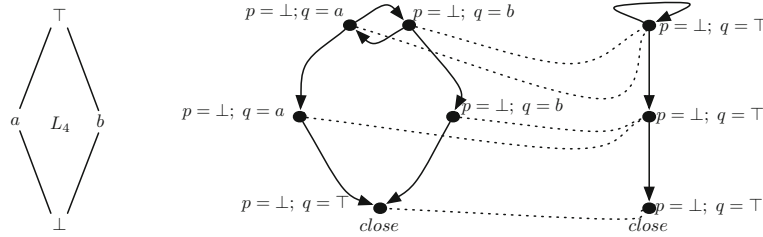
$$569 \quad (M', W') \models^{w'} \text{Sen}^{\mathcal{H}I}(\varphi)(\langle \lambda \rangle(\xi_1, \dots, \xi_n)) \quad \square$$

571 The following examples illustrate refinement situations in this setting.

572 *Example 5.1* (Refinement in  $\mathcal{H}PL$ ) Forward refinement notion in  $\mathcal{H}PL$  consists of the standard notion of simu-  
573 lation in Kripke structures. Theorem 5.1 generalises the well known preservation result of positive sentences by  
574 simulation (see [BdRV01] for the modal standard case). In this case  $\text{Sen}_{\diamond}^{\mathcal{H}PL}(\Delta)$  consists exactly in the restriction  
575 of  $\text{Sen}^{\mathcal{H}PL}(\Delta)$  to all the sentences without occurrences of negations and boxes.

576 *Example 5.2* (Refinement in  $\mathcal{H}MVL_L$ ) Figure 9 presents an example of a refinement in multi-valued logic based  
577 on the lattice  $L_4$  (on the left of Fig. 9). Let  $MVL_{L_4}^*$  be the institution obtained from  $MVL_{L_4}$  by restricting the  
578 functor of the sentences to the subfunctor  $S$  defined by  $S(LProp) = \{(p, l), p \in LProp \text{ and } l \in L_4\}$ . Consider  
579 now the hybridisation  $\mathcal{H}MVL_{L_4}^*$  of  $MVL_{L_4}^*$ .

	<b>1650327</b>	<b>B</b>	Dispatch: 3/12/2014	Journal: FAC
	Jour. No		Ms. No.	Total pages: 21
			Disk Received <input type="checkbox"/>	Corrupted <input type="checkbox"/>
			Disk Used <input type="checkbox"/>	Mismatch <input type="checkbox"/>

Fig. 9. Forward refinement in  $\mathcal{HMVLL}$ 

580 Conditions (ii) and (iii) are obviously satisfied. In what concerns the verification of condition (i) for which  
 581  $(p, l) \in \mathcal{S}(LProp)$ ,  $M_w \models_{LProp}^{MVL_{L_A}^*} (p, l) \Rightarrow M'_{w'} \models_{LProp}^{MVL_{L_A}^*} (p, l)$ , it is sufficient to see that,  $(M_w \models p) \leq (M'_{w'} \models p)$ ,  
 582  $p \in LProp$ .

583 *Example 5.3 (Refinement in  $\mathcal{HEQ}$ )* Consider a store system abstractly modelled as the initial algebra  $A$  with  
 584 signature  $((S, F), \Gamma)$  where  $S = \{mem, elem\}$ ,  $F_{\rightarrow mem} = \{new\}$ ,  $F_{\rightarrow elem} = \{0\}$ ,  $F_{mem \times elem \rightarrow mem} = \{write\}$ ,  
 585  $F_{mem \rightarrow mem} = \{del\}$  and  $F_{\underline{ar} \rightarrow s} = \emptyset$  otherwise, and where  $\Gamma$  is the following set of equations:

586  $del(new) = new,$   
 587  $del(write(m, e)) = m.$

588 Suppose one intends to refine this structure by adding a *read* function configurable in two different modes:  
 589 in one of them it reads the first element in the store, in the other the last. Reconfiguration between the two  
 590 execution modes is enforced by an external control event *shift*. Note that this abstract model can be seen as the  
 591  $((S, F), \emptyset, \{shift\})$ -hybrid model  $\mathcal{M} = (M, W)$ , taking  $| W | = \{\star\}$ ,  $W_{shift} = id$  and  $M_{\star} = A$  (see Fig. 10). Then,  
 592 we take the inclusion morphism  $\varphi_{Sign} : (S, F) \hookrightarrow (S, F')$  where  $F'$  extends  $F$  with  $F'_{mem \rightarrow elem} = \{read\}$ . For the  
 593 envisaged refinement let us consider model  $\mathcal{M}' = (M', W')$  where  $W' = \{s_1, s_2\}$  and  $W'_{shift} = \{(s_1, s_2), (s_2, s_1)\}$   
 594 and where  $M'_{s_1}$  and  $M'_{s_2}$  are respectively, two algebras satisfying the equations

595  $read(new) = 0,$   
 596  $del(new) = new,$   
 597  $del(write(m, e)) = m,$   
 598  $read(write(m, e)) = e,$

599 and

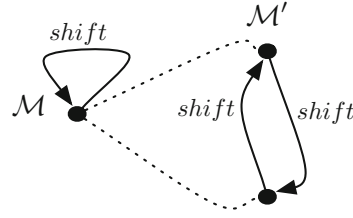
600  $read(new) = 0,$   
 601  $del(new) = new,$   
 602  $del(write(m, e)) = m,$   
 603  $read(write(write(m, e), e')) = read(write(m, e)),$   
 604  $read(write(new, e)) = e$

605 respectively.

606 It is not difficult to see that  $R = \{(\star, s_1), (\star, s_2)\}$  is a  $\varphi$ -refinement relation: conditions (ii) and (iii) are trivially  
 607 fulfilled; the initiality of (the algebra)  $M_{\star}$  entails the condition (i): as is well known (e.g. [EM85]) properties valid  
 608 in the initial model of a set of equation are the ones valid in all the models of the respective variety. This includes  
 609 the models  $\text{Mod}(\varphi)(M_{s_1})$  and  $\text{Mod}(\varphi)(M_{s_2})$ .

	<b>1650327</b>	<b>B</b>	Dispatch: 3/12/2014	Journal: FAC
	Jour. No		Ms. No.	Total pages: 21
			Disk Received <input type="checkbox"/>	Corrupted <input type="checkbox"/>
			Disk Used <input type="checkbox"/>	Mismatch <input type="checkbox"/>



Fig. 10. Forward refinement in  $\mathcal{HEQ}$ .

## 610 5.2. Backward refinement

611 Forward refinement simulates the abstract model behaviour by the concrete one, i.e. the refined model allows  
 612 all behaviours specified at the abstract level. A dual notion goes in the opposite direction, enforcing all concrete  
 613 behaviours to be allowed in the abstract model. Actually this notion is more common in the literature: it constrains  
 614 the concrete, refined model to exhibit only behaviours allowed in its specification. Formally this leads to a notion  
 615 of *backward* refinement by replacing condition (iv) in Definition 5.1 by the (*zag*) condition:

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

618 leading to

619 **Definition 5.3** Let  $\mathcal{HI}$  be the hybridisation of an institution  $I$  and  $\varphi \in \text{Sign}^{\mathcal{HI}}(\Delta, \Delta')$  a signature morphism. A  
 620 *backward  $\varphi$ -refinement relation between models*  $(M, W) \in \text{Mod}^{\mathcal{HI}}(\Delta)$  and  $(M', W') \in \text{Mod}^{\mathcal{HI}}(\Delta')$  is a non-empty  
 621 relation  $\mathbf{R}_\varphi \subseteq |W| \times |W'|$  such that, for any  $w \mathbf{R}_\varphi w'$ ,

622 (i)  $M_w \gg_\varphi M'_{w'}$ ,

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

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

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

627 We say that  $(M', W')$  is a *backward  $\varphi$ -refinement* of  $(M, W)$ , in symbols  $(M, W) \leftarrow_\varphi (M', W')$ , if there is a  
 628 backward  $\varphi$ -refinement between them. Again  $\leftarrow_\varphi$  is abbreviated to  $\leftarrow$  whenever  $\varphi$  is the identity.

629 Note that existential ('diamond') sentences are no longer preserved through backward refinement: effective  
 630 transitions at the abstract level can be backward-refined into a non-transition at the concrete level. Universal  
 631 ('boxed') sentences, however, are preserved, leading to a re-phrasing of Theorem 5.1 for positive, universal  
 632 sentences, collected in  $\text{Sen}_{\square}^{\mathcal{HI}}(\Delta)$ . Formally,

633 **Definition 5.4** (*Positive universal sentences*) The positive universal sentences of a signature  $\Delta \in |\text{Sign}^{\mathcal{HI}}|$  are  
 634 given by the subfunctor  $\text{Sen}_{\square}^{\mathcal{HI}} \subseteq \text{Sen}^{\mathcal{HI}}$  defined inductively for each signature  $\Delta$  as  $\text{Sen}^{\mathcal{HI}}(\Delta)$ , but excluding  
 635 both negation and  $\diamond$ -formulas. For each signature morphism  $\varphi : \Delta \rightarrow \Delta'$ ,  $\text{Sen}_{\square}^{\mathcal{HI}}(\varphi)$  is the restriction of  $\text{Sen}^{\mathcal{HI}}(\varphi)$   
 636 to  $\text{Sen}_{\square}^{\mathcal{HI}}(\Delta)$ .

637 **Theorem 5.2** Let  $\mathcal{HI}$  be the hybridisation of an institution  $I$ ,  $\varphi \in \text{Sign}^{\mathcal{HI}}(\Delta, \Delta')$  a signature morphism,  $\mathbf{R}_\varphi$  a  
 638 backward  $\varphi$ -refinement relation and  $(M, W) \in \text{Mod}^{\mathcal{HI}}(\Delta)$  and  $(M', W') \in \text{Mod}^{\mathcal{HI}}(\Delta')$  two models such that  
 639  $(M', W')$  is a backward  $\varphi$ -refinement of  $(M, W)$  witnessed by relation  $\mathbf{R}_\varphi$ . Then, for any  $w \mathbf{R}_\varphi w'$  and  $\rho \in \text{Sen}_{\square}^{\mathcal{HI}}(\Delta)$ ,

640  $(M, W) \models^w \rho$  implies that  $(M', W') \models^{w'} \text{Sen}_{\square}^{\mathcal{HI}}(\varphi)(\rho)$ .

	<b>1650327</b>	<b>B</b>	Dispatch: 3/12/2014	Journal: FAC
	Jour. No		Ms. No.	Total pages: 21
			Disk Received <input type="checkbox"/>	Corrupted <input type="checkbox"/>
			Disk Used <input type="checkbox"/>	Mismatch <input type="checkbox"/>

641 *Proof.* The crucial step in the proof is the preservation of ‘boxed’ formulas  $\rho = [\lambda](\xi_1, \dots, \xi_n)$ , as follows:

$$\begin{aligned}
642 & (M, W) \models^w [\lambda](\xi_1, \dots, \xi_n) \\
643 & \Leftrightarrow \{ \text{definition of } \models^w \} \\
644 & \text{for all } (w, w_1, \dots, w_n) \in W_\lambda, (M, W) \models^{w_k} \xi_k, \text{ for any } k \in \{1, \dots, n\} \\
645 & \Rightarrow \{ (\star) \} \\
646 & \text{for all } (w', w'_1, \dots, w'_n) \in W'_{\varphi_{MS}(\lambda)}, (M', W') \models^{w'_k} \xi_k, \text{ for any } k \in \{1, \dots, n\} \\
647 & \Leftrightarrow \{ \text{definition of } \models^{w'} \} \\
648 & (M', W') \models^{w'} [\varphi_{MS}(\lambda)](\text{Sen}^{\mathcal{H}I}(\varphi)(\xi_1), \dots, \text{Sen}^{\mathcal{H}I}(\varphi)(\xi_n)) \\
649 & \Leftrightarrow \{ \text{definition of } \text{Sen}^{\mathcal{H}I}(\varphi) \} \\
650 & (M', W') \models^{w'} \text{Sen}^{\mathcal{H}I}(\varphi)([\lambda](\xi_1, \dots, \xi_n))
\end{aligned}$$

651 The proof step marked with  $(\star)$  above is justified as follows: the (*zag*) condition guarantees that if there is a set of  
652 transitions from  $w$  in the abstract model, a subset (possibly empty) of corresponding transitions is also present  
653 in the concrete model from state  $w'$ . Actually, this is an equivalence step, with the implication from right to left  
654 being just a direct consequence of the (*zag*) condition.  $\square$

655 Of course the restriction to *positive* sentences is also enforced here. If such was not the case the whole argument  
656 would collapse as existential sentences could be built from universal ones and vice-versa.

657 Therefore, we end up with two notions of refinement defined in terms of which transitions are globally  
658 preserved and in which direction. If one regards ‘boxed’ properties as a sort of (elementary) *safety* requirements,  
659 one could state that backward refinement preserves safety. Dually, regarding existential sentences as (elementary)  
660 *liveness* requirements, forward refinement preserves liveness. It comes to no surprise that the more common notion  
661 of refinement, that of backward refinement, preserves safety.

## 662 6. Refinement of specifications

663 Until now we have been seeking for suitable notions of equivalence and refinement between models of specifica-  
664 tions in hybridised institutions. We shall now turn to the *specifications* themselves, in the sense the word has in  
665 the tradition of *property oriented* specification methods (see [ST12] for a recent overview).

666 A specification is a collection of properties a system is supposed to obey, i.e. a theory in a suitable institution. Its  
667 semantics is the class of models satisfying such a theory. Formally, a (non-structured) specification in a institution  
668  $I$  consists of a pair  $(\Delta, E)$ , where  $\Delta \in \text{Sign}^I$  and  $E \subseteq \text{Sen}^I(\Delta)$ . Its (loose) semantics is given by


- 669 – its signature  $\text{Sig}[SP] = \Delta$ , for some  $\Delta \in |\text{Sign}^I|$ ,
- 670 – its class of models  $[[SP]] = \{M \in |\text{Mod}^I(\Delta)| : M \models_\Delta E\}$ .

671 Conceptually,  $[[SP]]$  can be understood as the class of admissible implementations for the system and, the  
672 implementation of  $SP$ , as one of these models chosen to realise the system. The construction of this particular  
673 model proceeds by a stepwise refinement process. Formally, we say that  $SP'$  refines  $SP$  via  $\varphi$ , in symbols,  $SP' \rightsquigarrow_\varphi$   
674  $SP$ , if

- 675 –  $\varphi \in \text{Sign}^I(\text{Sig}(SP), \text{Sig}(SP'))$ ,
- 676 –  $[[SP']] \upharpoonright_{\varphi} \subseteq [[SP]]$ , where  $[[SP']] \upharpoonright_{\varphi} = \{\text{Mod}^I(\varphi)(M) \mid M \in [[SP]]\}$ .

677 Note that this is a straightforward generalisation of the notion of *simple refinement* in algebraic specification e.g.  
678 [San99], in which case  $\text{Sig}[SP] = \text{Sig}[SP']$  and  $\varphi$  is the identity. Similarly, two specifications  $SP$  and  $SP'$  are  
679 equivalent up to a signature morphism  $\varphi : \text{Sig}[SP] \rightarrow \text{Sig}[SP']$  when  $[[SP']] \upharpoonright_{\varphi} = [[SP]]$ .

680 Back to dealing with classes of models, we are also back to the notions of bisimulation and refinement used  
681 before. Although in process algebra, where such notions were born, their formulation is essentially local (e.g.,  
682 two processes are bisimilar if their *initial* states are related by a bisimulation), when reasoning with specifications

	<b>1650327</b>	<b>B</b>	Dispatch: 3/12/2014	Journal: FAC
	Jour. No		Ms. No.	Total pages: 21
			Disk Received <input type="checkbox"/>	Corrupted <input type="checkbox"/>
			Disk Used <input type="checkbox"/>	Mismatch <input type="checkbox"/>

683 a notion of initial state is usually absent. This entails the need for a shift of perspective for “globalising” the  
 684 preservation results. In particular, the local characterisation established in Theorem 4.1, can be re-framed as  
 685 follows:

686 **Theorem 6.1** Let  $\mathcal{HI}$  be the hybridisation of institution  $I$  and  $\varphi \in \text{Sign}^{\mathcal{HI}}(\Delta, \Delta')$  a signature morphism. Let  
 687  $\mathbf{B}_\varphi \sqsubseteq |W| \times |W'|$  be a total and surjective  $\varphi$ -bisimulation. Then,

$$688 \quad (M, W) \models^{\mathcal{HI}} \rho \text{ iff } (M', W') \models^{\mathcal{HI}} \text{Sen}^{\mathcal{HI}}(\varphi)(\rho) \quad (5)$$

689 *Proof.* Let us suppose  $(M, W) \models^{\mathcal{HI}} \rho$ , i.e. that for any  $w \in |W|$ ,  $(M, W) \models^w \rho$ . Since  $\mathbf{B}_\varphi$  is surjective, for any  
 690  $w' \in |W'|$  there is a  $w \in |W|$  such that  $w\mathbf{B}_\varphi w'$ . Since  $(M, W) \models^w \rho$ , by Theorem 4.1,  $(M, W) \models^{w'} \text{Sen}^{\mathcal{HI}}(\varphi)(\rho)$ .  
 691 Hence  $(M, W) \models^{\mathcal{HI}} \text{Sen}^{\mathcal{HI}}(\varphi)(\rho)$ . The converse implication is proved similarly using resorting to the totality  
 692 of  $\mathbf{B}_\varphi$ .  $\square$

693 A similar global characterisation of preservation results for both forward and backward refinements arises as  
 694 a corollary of Theorem 5.1 and its backward counterpart explained in Sect. 5.2.

695 **Corollary 6.1** Let  $\mathcal{HI}$  be the hybridisation of an institution  $I$ ,  $\varphi \in \text{Sign}^{\mathcal{HI}}(\Delta, \Delta')$  a signature morphism,  $(M, W) \in$   
 696  $\text{Mod}^{\mathcal{HI}}(\Delta)$  and  $(M', W') \in \text{Mod}^{\mathcal{HI}}(\Delta')$  two  $\mathcal{HI}$ -models and  $\mathbf{R}_\varphi : |W| \times |W'|$  a relation.

697 1. if  $\mathbf{R}_\varphi$  is a surjective forward  $\varphi$ -refinement relation, we have that for any  $\rho \in \text{Sen}_\diamond^{\mathcal{HI}}(\Delta)$ ,

$$698 \quad (M, W) \models^{\mathcal{HI}} \rho \text{ implies that } (M', W') \models \text{Sen}^{\mathcal{HI}}(\varphi)(\rho).$$

699 2. if  $\mathbf{R}_\varphi$  is a total backward  $\varphi$ -refinement relation, we have that for any  $\rho \in \text{Sen}_\square^{\mathcal{HI}}(\Delta)$ ,

$$700 \quad (M, W) \models^{\mathcal{HI}} \rho \text{ implies that } (M', W') \models \text{Sen}^{\mathcal{HI}}(\varphi)(\rho).$$

701 The following results relate specification refinement ( $\rightsquigarrow$ ) with bisimulation and with refinement of specification  
 702 models as previously introduced.

703 **Theorem 6.2** Let  $SP = (\Delta, E)$  and  $SP' = (\Delta, E')$  be two specifications. Then, the following statements are  
 704 equivalent:

705 1.  $SP \rightsquigarrow_\varphi SP'$ ,

706 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  
 707 and surjective bisimulation.

708 *Proof.* **1**  $\Rightarrow$  **2** By assumption, that for any  $(M', W') \in [|SP'|]$ ,  $\text{Mod}^{\mathcal{HI}}(\varphi)(M', W') \in [|SP|]$ . By Theorem 3.1,  
 709 there is a model  $(M, W) \in [|SP|] (= \text{Mod}^{\mathcal{HI}}(\varphi)(M', W'))$  such that  $(M, W) \rightleftharpoons_\varphi (M', W')$  witnessed by the  
 710 identity relation, a total and surjective bisimulation.

711 **2**  $\Rightarrow$  **1** Let us consider a model  $(M', W') \in [|SP'|]$ . By hypothesis there is a  $(M, W) \in [|SP|]$  such that  
 712  $(M, W) \rightleftharpoons_\varphi (M', W')$ . Hence by Corollary 6.1, for any  $\rho \in \text{Sen}^{\mathcal{HI}}(\Delta)$ ,  $(M, W) \models \rho$  iff  $(M', W') \models \text{Sen}^{\mathcal{HI}}(\varphi)(\rho)$ .  
 713 In particular,  $(M', W') \models \text{Sen}^{\mathcal{HI}}(\varphi)(E)$ . By Satisfaction Condition we have  $\text{Mod}^{\mathcal{HI}}(\varphi)(W', M') \models E$ ,  
 714 i.e.,  $\text{Mod}^{\mathcal{HI}}(\varphi)(M', W') \in [|SP|]$ . Therefore  $SP \rightsquigarrow_\varphi SP'$ .  $\square$


715 **Theorem 6.3** Let  $SP = (\Delta, E)$  and  $SP' = (\Delta, E')$  be two specifications with  $E \subseteq \text{Sen}_\diamond^{\mathcal{HI}}(\Delta)$ . Then, the following  
 716 statements are equivalent:

717 1.  $SP \rightsquigarrow_\varphi SP'$ ,

718 2. for any  $(M', W') \in [|SP'|]$ , there is a  $(M, W) \in [|SP|]$  such that  $(M, W) \rightarrow_\varphi (M', W')$  witnessed by a  
 719 surjective refinement relation.

720 *Proof.* **1**  $\Rightarrow$  **2**. This implication is proved analogously to the implication **1**  $\Rightarrow$  **2** in Theorem 6.2 using the fact  
 721 that  $(M, W) \rightleftharpoons_\varphi (M', W')$  implies  $(M, W) \rightarrow_\varphi (M', W')$  and also  $(M, W) \leftarrow_\varphi (M', W')$ .

722 **2**  $\Rightarrow$  **1**. Let us consider a model  $(M', W') \in [|SP'|]$ . By hypothesis there is a  $(M, W) \in [|SP|]$  such that  
 723  $(M, W) \rightarrow_\varphi (M', W')$ . Hence by item 1. of Corollary 6.1, for any  $\rho \in \text{Sen}_\diamond^{\mathcal{HI}}(\Delta)$ ,  $(M, W) \models \rho$  implies  
 724 that  $(M', W') \models \text{Sen}^{\mathcal{HI}}(\varphi)(\rho)$ . In particular,  $(M', W') \models \text{Sen}^{\mathcal{HI}}(\varphi)(E)$ . The Satisfaction Condition entails  
 725  $\text{Mod}^{\mathcal{HI}}(\varphi)(W', M') \models E$ , i.e.,  $\text{Mod}^{\mathcal{HI}}(\varphi)(M', W') \in [|SP|]$ . Therefore  $SP \rightsquigarrow_\varphi SP'$ .  $\square$

	<b>1650327</b>	<b>B</b>	Dispatch: 3/12/2014	Journal: FAC
	Jour. No		Ms. No.	Total pages: 21
			Disk Received <input type="checkbox"/>	Corrupted <input type="checkbox"/>
			Disk Used <input type="checkbox"/>	Mismatch <input type="checkbox"/>

726 **Theorem 6.4** Let  $SP = (\Delta, E)$  and  $SP' = (\Delta, E')$  be two specifications with  $E \subseteq \text{Sen}_{\square}^{\text{HI}}(\Delta)$ . Then, the following  
727 statements are equivalent:

- 728 1.  $SP \rightsquigarrow_{\varphi} SP'$ ,  
729 2. for any  $(M', W') \in \llbracket SP' \rrbracket$ , there is a  $(M, W) \in \llbracket SP \rrbracket$  such that  $(M, W) \leftarrow_{\varphi} (M', W')$  witnessed by a  
730 total refinement relation.

731 *Proof.* The proof is analogous to the one of Theorem 6.3 but using, in the implication  $2 \Rightarrow 1$ , item 2. of Corollary  
732 6.1.  $\square$

## 733 7. Conclusions

734 This paper introduced notions of equivalence and refinement for models of hybrid specifications, i.e., specifications  
735 formalised in hybridised versions of logics used to describe systems' possible configurations. The definition is  
736 parametric on precisely the base logic relevant for each application.

737 From an engineering point of view, the characterisation of suitable, generic notions of equivalence and refine-  
738 ment is fundamental to a software design methodology to deal with systems' reconfigurability in a rigorous way.  
739 Such a methodology was introduced in [MFMB11], and provided with effective, computer-based proof support  
740 through the recent implementation [NMMB13] of the hybridisation method in the HETS platform [MML07].


741 Current work on this topic includes the study of typical constructions on Kripke structures (e.g. bounded  
742 morphism images, substructures and disjoint unions) and their characterisation under bisimilarity and refinement.  
743 Whether the complexity of each hybridised logic can be computed from the complexity of the corresponding base  
744 logic remains a somehow lateral, but challenging research topic.

## 745 Acknowledgements

746 This work is funded by ERDF—European Regional Development Fund, through the COMPETE Programme,  
747 and by National Funds through FCT within project FCOMP-01-0124-FEDER-028923 and by project NORTE-  
748 07-0124-FEDER-000060, co-financed by the North Portugal Regional Operational Programme (ON.2), under the  
749 National Strategic Reference Framework (NSRF), through the European Regional Development Fund (ERDF).  
750 The work had also partial financial assistance by the project PEst-OE/MAT/UI4106/2014 at CIDMA, FCOMP-  
751 01-0124-FEDER-037281 at INESC TEC and the Marie Curie project FP7-PEOPLE-2012-IRSES (GetFun).

## 752 References

- 753 [ACEGG90] Agusti-Cullell J, Esteva F, Garcia P, Godo L (1990) Formalizing multiple-valued logics as institutions. In: Bouchon-Meunier  
754 B, Yager RR, Zadeh LA (eds) 3rd International conference on information processing and management of uncertainty in  
755 knowledge-based systems (IPMU 90, Paris, France, July 2–6, 1990). Lecture notes in computer science, vol 521. Springer, pp  
756 269–278
- 757 [AtC06] Areces C, ten Cate B (2006) Hybrid logics. In: Blackburn P, Wolter F, van Benthem J (eds) Handbook of modal logics. Elsevier,  
758 Amsterdam, pp 821–868
- 759 [BD94] Burstall R, Diaconescu R (1994) Hiding and behaviour: an institutional approach. In: Roscoe W (ed) A classical mind: essays  
760 in honour of C.A.R. Hoare. Prentice-Hall, Hertfordshire, pp 75–92
- 761 [BdRV01] Blackburn P, de Rijke M, Venema Y (2001) Modal logic. Number 53 in Cambridge Tracts in Theoretical Computer Science,  
762 Cambridge University Press, Cambridge
- 763 [BH06] Bidoit M, Hennicker R (2006) Constructor-based observational logic. J Logic Algebr Progr 67(1–2):3–51
- 764 [BK105] Beierle C, Kern-Isberner G (2005) Looking at probabilistic conditionals from an institutional point of view. In: Kern-Isberner  
765 G, Rödder W, Kulmann F (eds) Conditionals, information, and inference (revised selected papers of WCII 2002, Hagen,  
766 Germany, May 13–15, 2002). Lecture notes in computer science, vol 3301. Springer, pp 162–179
- 767 [Bra10] Brauner T (2010) Hybrid logic and its proof-theory. Applied logic series, Springer, Netherlands
- 768 [BS03] Börger E, Stärk R (2003) Abstract state machines: a method for high-level system design and analysis. Springer, Berlin
- 769 [BVB07] Blackburn P, Van Benthem J (2007) Modal logic: a semantic perspective. In: Blackburn P, Wolter F, van Benthem J (eds)  
770 Handbook of modal logic, studies in logic and practical reasoning, vol 3. Elsevier, Amsterdam, pp 1–82


	<b>1650327</b>	<b>B</b>	Dispatch: 3/12/2014	Journal: FAC
	Jour. No		Ms. No.	Total pages: 21
			Disk Received <input type="checkbox"/>	Corrupted <input type="checkbox"/>
			Disk Used <input type="checkbox"/>	Mismatch <input type="checkbox"/>

- 771 [C06] Cirstea C (2006) An institution of modal logics for coalgebras. *J Logic Algebr Progr* 67(1–2):87–113
- 772 [CMSS06] Caleiro C, Mateus P, Sernadas A, Sernadas C (2006) Quantum institutions. In: Futatsugi K, Jouannaud J-P, Meseguer J (eds)
- 773 Algebra, meaning, and computation, essays dedicated to Joseph A. Goguen on the occasion of his 65th birthday. Lecture
- 774 notes in computer science, vol 4060. Springer, pp 50–64
- 775 [Dia08] Diaconescu R (2008) Institution-independent model theory. *studies in universal logic*. Birkhäuser, Basel
- 776 [Dia11] Diaconescu R (2011) On quasi-varieties of multiple valued logic models. *Math Log Q* 57(2):194–203
- 777 [DM14] Diaconescu R, Madeira A (2014) Encoding hybridized institutions into first order logic. *Math Struct Comput Sci*. doi:10.
- 778 [1017/S0960129514000383](https://doi.org/10.1017/S0960129514000383)
- 779 [EM85] Ehrig H, Mahr B (1985) Fundamentals of algebraic specification 1: equations and initial semantics. *Monographs in theoretical*
- 780 *computer science, an EATCS Series*. Springer, Berlin
- 781 [GB92] Goguen JA, Burstall RM (1992) Institutions: abstract model theory for specification and programming. *J ACM* 39(1):95–146
- 782 [Got01] Gottwald S (2001) A treatise on many-valued logics. *studies in logic and computation*, vol 9. Research Studies Press, Baldock
- 783 [Grä79] Grätzer G (1979) *Universal algebra*. Springer, New York, Heidelberg, Berlin
- 784 [Hod97] Hodges W (1997) *A shorter model theory*. Cambridge University Press, Cambridge
- 785 [Ind07] Indrzejczak A (2007) Modal hybrid logic. *Logic Log Philos* 16:147–257
- 786 [Mad13] Madeira A (2013) Foundations and techniques for software reconfigurability. Ph.D. thesis, Universidades do Minho, Aveiro
- 787 and Porto (Joint MAP-i Doctoral Programme)
- 788 [MFMB11] Madeira A, Faria JM, Martins MA, Barbosa LS (2011) Hybrid specification of reactive systems: an institutional approach.
- 789 In: Barthe G, Pardo A, Schneider G (eds) *Software engineering and formal methods (SEFM 2011, Montevideo, Uruguay,*
- 790 *November 14–18, 2011)*. Lecture notes in computer science, vol 7041. Springer, pp 269–285
- 791 [Mil89] Milner R (1989) *Communication and concurrency*. series in computer science. Prentice-Hall, Englewood Cliffs
- 792 [MMB13] Madeira A, Martins MA, Barbosa LS (2013) Bisimilarity and refinement for hybrid(ised) logics. In: Derrick J, Boiten EA,
- 793 Reeves S (eds) *Refine-Proceedings 16th international refinement workshop*. Electronic proceedings in theoretical computer
- 794 science, vol 115, pp 84–98
- 795 [MMDB11] Martins MA, Madeira A, Diaconescu R, Barbosa LS (2011) Hybridization of institutions. In: Corradini A, Klin B, Cirstea
- 796 C (eds) *Algebra and coalgebra in computer science (CALCO 2011, Winchester, UK, August 30–September 2, 2011)*. Lecture
- 797 notes in computer science, vol 6859. Springer, pp 283–297
- 798 [MML07] Mossakowski T, Maeder C, Lüttich K (2007) The heterogeneous tool set, Hets. In: Grumberg O, Huth M (eds) *Tools and*
- 799 *algorithms for the construction and analysis of systems (TACAS 2007-Braga, Portugal, March 24–April 1, 2007)*. Lecture
- 800 notes in computer science, vol 4424. Springer, pp 519–522
- 801 [MNMB13] Madeira A, Neves R, Martins MA, Barbosa LS (2013) When even the interface evolves. In: Wang H, Banach R (eds) *Proceed-*
- 802 *ings of TASE (7th IEEE symposium on theoretical aspects of software engineering, Birmingham, July, 2013)*. IEEE Computer
- 803 Society, pp 79–82
- 804 [MR06] Mossakowski T, Roggenbach M (2006) Structured CSP—a process algebra as an institution. In: Fiadeiro JL, Schobbens
- 805 P-Y (eds) *Recent trends in algebraic development techniques (revised selected papers of WADT 2006, La Roche en Ardenne,*
- 806 *Belgium, June 1–3, 2006)*. Lecture notes in computer science, vol 4409. Springer, pp 92–110
- 807 [NMMB13] Neves R, Madeira A, Martins MA, Barbosa LS (2013) Hybridisation at work. In: Heckel R, Milius S (eds) *Algebra and coal-*
- 808 *gebra in computer science—5th international conference, CALCO 2013, Warsaw, Poland, September 3–6, 2013*. Proceedings,
- 809 Lecture notes in computer science, vol 8089, Springer, pp 340–345
- 810 [Par81] Park D (1981) Concurrency and automata on infinite sequences. In: Deussen P (ed) *Theoretical computer science (5th GI-*
- 811 *conference, Karlsruhe, Germany, March 23–25, 1981)*. Lecture notes in computer science, vol 104. Springer, pp 167–183
- 812 [San99] Sannella D (1999) Algebraic specification and program development by stepwise refinement. In: Bossi A (ed) *Logic-based*
- 813 *program synthesis and transformation*. Lecture notes in computer science, vol 1817. Springer, Venezia, Italy, pp 1–9
- 814 [San09] Sangiorgi D (2009) On the origins of bisimulation and coinduction. *ACM Trans Progr Lang Syst* 31(4):1–41. doi:10.1145/
- 815 [1516507.1516510](https://doi.org/10.1145/1516507.1516510)
- 816 [SC11] Szepesia R, Ciocarlie H (2011) An overview on software reconfiguration. *Theory Appl Math Comput Sci* 1:74–79
- 817 [SM09] Schröder L, Mossakowski T (2009) HasCasl: integrated higher-order specification and program development. *Theor Comput*
- 818 *Sci* 410(12–13):1217–1260
- 819 [ST12] Sannella D, Tarlecki A (2012) Foundations of algebraic specification and formal software development. *Monographs on*
- 820 *theoretical computer science, an EATCS series*. Springer
- 821 [Tar03] Tarlecki A (2003) Abstract specification theory: an overview. In: Broy M, Pizka M (eds) *Models, algebras, and logics of*
- 822 *engineering software*. NATO science series, computer and systems sciences, vol 191. IOS Press, pp 43–79
- 823 [tC05] ten Cate BD (2005) Model theory for extended modal languages. Ph.D. thesis, Institute for Logic, Language and Computation
- 824 Universiteit van Amsterdam

825 Received 5 November 2013

826 Revised 30 October 2014

827 Accepted 3 November 2014 by John Derrick, Steve Reeves, and Eerke Boiten

	1 6 5 0 3 2 7	B	Dispatch: 3/12/2014	Journal: FAC
	Jour. No		Ms. No.	Total pages: 21
			Disk Received <input type="checkbox"/>	Corrupted <input type="checkbox"/>
			Disk Used <input type="checkbox"/>	Mismatch <input type="checkbox"/>