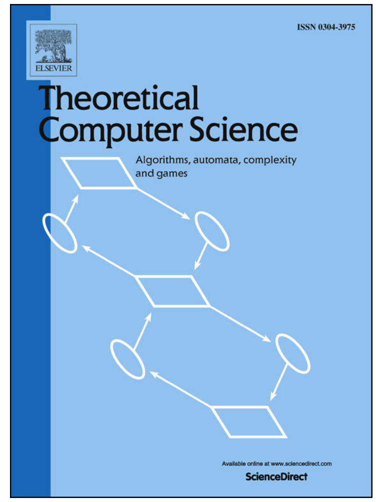
Accepted Manuscript



Behavioural and abstractor specifications revisited

Rolf Hennicker, Alexandre Madeira, Martin Wirsing

PII: S0304-3975(18)30130-0
DOI: https://doi.org/10.1016/j.tcs.2018.02.033
Reference: TCS 11497

To appear in: *Theoretical Computer Science*

Received date: 21 August 2017
Revised date: 26 January 2018
Accepted date: 26 February 2018

Behavioural and Abstractor Specifications Revisited

- Dedicated to Don Sannella -

Rolf Hennicker[a], Alexandre Madeira[b,c], Martin Wirsing[a]

[a]*Institut für Informatik, Ludwig-Maximilians-Universität München, Germany*
[b]*HASLab INESC TEC & Universidade do Minho, Portugal*
[c]*CIDMA - Dep. Mathematics, Universidade de Aveiro, Portugal*

Abstract

In the area of algebraic specification there are two main approaches for defining observational abstraction: behavioural specifications use a notion of observational satisfaction for the axioms of a specification, whereas abstractor specifications define an abstraction from the standard semantics of a specification w.r.t. an observational equivalence relation between algebras. Earlier work by Bidoit, Hennicker, Wirsing has shown that in the case of first-order logic specifications both concepts coincide semantically under mild assumptions. Analogous results have been shown by Sannella and Hofmann for higher-order logic specifications and recently, by Hennicker and Madeira, for specifications of reactive systems using a dynamic logic with binders. In this paper, we bring these results into a common setting: we isolate a small set of characteristic principles to express the behaviour/abstractor equivalence and show that all three mentioned specification frameworks satisfy these principles and therefore their behaviour and abstractor specifications coincide semantically (under mild assumptions). As a new case we consider observational modal logic where observational satisfaction of Hennessy-Milner logic formulae is defined "up to" silent transitions and observational abstraction is defined by weak bisimulation. We show that in this case the behaviour/abstractor equivalence can only be obtained, if we restrict models to weakly deterministic labelled transition systems.

Keywords: algebraic specification, specification of reactive systems, observable behaviour, observational abstraction

1. Introduction

The observable behaviour of a system is a key concept in software development. Typically, a requirement describes an observable property of a system and an implementation is correct if it satisfies the required observable properties; a reactive system interacts with its environment by observable actions whereas its internal actions are considered as hidden or non-observable. In the literature, one can find two main concepts for semantically formalising observational behaviour. The so-called abstractor specification is based on abstracting the standard model class of a specification by an observational equivalence relation between algebras [18, 23, 20] whereas the so-called behavioural specification defines an observational satisfaction relation where equality is not interpreted as identity but as observational indistinguishability of objects or states [19, 17, 8].

Already in the eighties it was shown that the two concepts coincide if the axioms of a specification are conditional equations with observable premises [19, 17]. In [2], Bidoit, Hennicker, Wirsing generalise these results and show that in the case of first-order logic specifications there exists a duality between both concepts which allows to express each one by the other; in particular, behaviour and abstractor specifications coincide semantically under mild assumptions. Similar results have been proven by Sannella and Hofmann

Email addresses: `hennicker@ifi.lmu.de` (Rolf Hennicker), `madeira@ua.pt` (Alexandre Madeira), `wirsing@ifi.lmu.de` (Martin Wirsing)

for higher-order logic specifications [13], and recently by Hennicker and Madeira for specifications of reactive systems [12].

As Hofmann and Sannella observe in [13], the results of [2] are largely independent of the underlying logic; they are based on the relation between the (partial) observational congruence of states, the abstraction equivalence of models, and the quotient algebra. In this work we generalise these ideas and propose a new approach, called behaviour-abstractor framework, which is based on a few characteristic principles and entails the relationships between behavioural and abstractor specifications. The key idea is that for each model we require the existence of an observationally equivalent "black box model" for which behavioural satisfaction of sentences coincides with standard satisfaction. Moreover, abstraction equivalence of models has to preserve behavioural satisfaction of sentences.

Then, for any concrete logical framework which satisfies these requirements, we get the semantic relationships between behavioural and abstractor specifications for free. In particular, we show that all three mentioned specification frameworks admit black box models and satisfy the characteristic principles of the behaviour-abstractor framework. As a novel case we consider observational modal logic where observational satisfaction of Hennessy-Milner logic formulae is defined "up to" silent transitions and observational abstraction is defined by weak bisimulation. We show that in this case a behaviour-abstractor framework can only be obtained, if we restrict models to weakly deterministic labelled transition systems.

An idea similar to the behaviour-abstractor framework is pursued by Misiak [16] but, in contrast to our approach, Misiak's formalisation uses behavioural institutions with specific semantic conditions on behavioural signature morphisms. His notion of behavioural satisfaction is predefined in terms of standard satisfaction by using partial congruence relations and categorical quotient constructions. Instead, we are working with an arbitrary behavioural satisfaction relation which must be respected by abstraction equivalence and with a simple and general notion of black box model, for which behavioural satisfaction and standard satisfaction coincide.

The paper is organised as follows: in Section 2 we present the behaviour-abstractor framework and show that it entails the semantic relationships between behavioural and abstractor specifications. In Sections 3 – 6 we show that first-order logic, higher-order logic, dynamic logic with binders, and (observable) Hennessy-Milner logic with weakly deterministic models form behaviour-abstractor frameworks. We finish with some concluding remarks in Section 7.

Personal Note. Don, Martin and Rolf (the third and first authors of this paper) know each other since the eighties where all three were investigating algebraic specifications. In 1981 during his stay at the University of Edinburgh, Martin meets Don, at that time a PhD student of Rod Burstall. Don and Martin became close friends and started working together. They propose the "forget-restrict-identify" notion of implementation for parameterised specifications and prove that (under appropriate assumptions) implementations compose horizontally and vertically [22]. Moreover, they introduce the kernel specification language ASL which includes an operator for abstractor specifications and has a loose semantics [23]. Rolf's PhD thesis and his further work on behavioural specifications were inspired by ASL and Don's and Andrzej Tarlecki's work on observational equivalence of specifications [20]. Later, Don was the external reviewer of Rolf's habilitation thesis [9]. As stated above, the starting point of this paper was a remark in Don's and Martin Hofmann's paper on behavioural abstraction and behavioural satisfaction in higher-order logic [13].

Working and discussing with Don is a very pleasant experience; he is not only an outstanding scientist with deep theoretical insights and an excellent sense for practical applications; he is also a warm-hearted and kind friend and colleague. We are looking forward to many further inspiring exchanges with him.

2. Behaviour-Abstractor Framework

In this section we identify a small but significant set of abstract requirements which are enough to define behavioural and abstractor specifications and to study relationships between their semantics. Our basic framework is independent of concrete logical formalisms.

Definition 1. A *behaviour-abstractor framework* $\mathrm{BA} = (\mathrm{Sign}, \mathrm{Sen}, \mathrm{Mod}, \models, \equiv, \models_{\mathrm{beh}}, \mathcal{BB})$ consists of

- a class Sign of *signatures*,
- a family $\text{Sen} = (\text{Sen}(\Sigma))_{\Sigma\in\text{Sign}}$ of sets $\text{Sen}(\Sigma)$ of Σ-*sentences*,
- a family $\text{Mod} = (\text{Mod}(\Sigma))_{\Sigma\in\text{Sign}}$ of classes $\text{Mod}(\Sigma)$ of Σ-*models*,
- a family $\models\, = (\models_\Sigma)_{\Sigma\in\text{Sign}}$ of *satisfaction relations* $\models_\Sigma \subseteq \text{Mod}(\Sigma)\times\text{Sen}(\Sigma)$,
- a family $\equiv\, = (\equiv_\Sigma)_{\Sigma\in\text{Sign}}$ of *abstraction equivalences* $\equiv_\Sigma \subseteq \text{Mod}(\Sigma)\times\text{Mod}(\Sigma)$,
- a family $\models_{\text{beh}} = (\models_{\text{beh},\Sigma})_{\Sigma\in\text{Sign}}$ of *behavioural satisfaction relations* $\models_{\text{beh},\Sigma} \subseteq \text{Mod}(\Sigma)\times\text{Sen}(\Sigma)$, and
- a family $\mathcal{BB} = (\mathcal{BB}_\Sigma)_{\Sigma\in\text{Sign}}$ of *black box* functions $\mathcal{BB}_\Sigma : \text{Mod}(\Sigma)\to\text{Mod}(\Sigma)$,

such that the following conditions (1) - (3) are satisfied for each signature $\Sigma\in\text{Sign}$ and for all Σ-models $\mathcal{M},\mathcal{M}'\in\text{Mod}(\Sigma)$:

(1) $\mathcal{M}\equiv_\Sigma\mathcal{M}' \Rightarrow (\mathcal{M}\models_{\text{beh},\Sigma}\varphi$ iff $\mathcal{M}'\models_{\text{beh},\Sigma}\varphi$ for all $\varphi\in\text{Sen}(\Sigma))$.

(2) $\mathcal{M}\equiv_\Sigma\mathcal{BB}_\Sigma(\mathcal{M})$.

(3) $\mathcal{BB}_\Sigma(\mathcal{M})\models_{\text{beh},\Sigma}\varphi$ iff $\mathcal{BB}_\Sigma(\mathcal{M})\models_\Sigma\varphi$ for all $\varphi\in\text{Sen}(\Sigma)$.

The idea of an abstraction equivalence is to relate models which show the same observable behaviour. The idea of behavioural satisfaction is to relax the (ordinary) satisfaction relation such that it is sufficient if properties are satisfied from the observational point of view and not necessarily literally. Condition (1) relates abstraction equivalence and behavioural satisfaction by requiring that abstraction equivalence preserves behavioural satisfaction of sentences. The black box function constructs, for each Σ-model $\mathcal{M}$, a so-called *black box view* of $\mathcal{M}$. The intuitive idea is that $\mathcal{BB}_\Sigma(\mathcal{M})$ shows the observable behaviour of $\mathcal{M}$ abstracting away implementation details which are not visible for the user of a system. Of course, the black box view of $\mathcal{M}$ should be equivalent to $\mathcal{M}$ according to the abstraction equivalence. This is expressed by condition (2). Condition (3) formalises an intrinsic property of black box views, for which behavioural satisfaction of sentences should be the same as ordinary satisfaction.

Remark 1. The first four ingredients of a behaviour-abstractor framework in Def. 1 are close to an institution [4] but omit signature morphisms. We do deliberately not work with institutions here, since signature morphisms play no role for the semantic equivalence of behavioural and abstractor specifications, see Theorem 5.11 in [2], Theorem 6.7 in [13], Theorem 8 in [12], and Lemma 2 in [16]. Of course, instead of the first four items in Def. 1, we could also use a standard institution. However, the behavioural satisfaction relation assumed in item 6 does, in general, not respect the satisfaction condition of institutions for standard signatures and signature morphisms. For instance, none of the concrete behavioural specification frameworks considered later on forms an institution.[1]

Given a behaviour-abstractor framework BA, a (flat) specification $SP = (\Sigma,\Phi)$ over BA consists of a signature $\Sigma\in\text{Sign}$ and a set $\Phi\subseteq\text{Sen}(\Sigma)$ of Σ-sentences, also called *axioms*, which specifiy properties of the models of the specification. The (ordinary) semantics of SP is given by the class of all Σ-models satisfying the axioms, i.e. $Mod(SP) = \{\mathcal{M}\in\text{Mod}(\Sigma) \mid \mathcal{M}\models_\Sigma\varphi \text{ for all } \phi\in\Phi\}$. In many cases the ordinary semantics of a specification is too restrictive since for its realisation it is often not necessary that all properties of the specification are literally satisfied but it is sufficient if the realisation has the desired observable behaviour. In the literature two prominent approaches have been proposed to provide semantics for a specification which takes into account abstraction w.r.t. observable behaviour. One way is to use the abstraction equivalence

[1] To obtain a behavioural institution specific notions of behavioural signatures are needed which require appropriate restrictions on signature morphisms to get the satisfaction condition of an institution w.r.t. behavioural satisfaction. Examples are hidden algebra [5], constructor-based observational logic [1], its institution-independent generalisation [16], and the recently proposed behavioural institution for dynamic logic with binders [11].

and to consider the *abstractor specification* **abstract** SP **wrt** $\equiv_\Sigma$ whose model class consists of all Σ-models equivalent to an ordinary model of SP, i.e.

$$Mod(\textbf{abstract } SP \textbf{ wrt } \equiv_\Sigma) = \{\mathcal{M} \in \text{Mod}(\Sigma) \mid \exists \mathcal{N} \in Mod(SP) : \mathcal{M} \equiv_\Sigma \mathcal{N}\}.$$

Another possibility is to rely on the behavioural satisfaction relation and to consider the *behavioural specification* **behaviour** SP **wrt** $\models_{\text{beh},\Sigma}$ whose model class consists of all Σ-models which satisfy behaviourally the axioms of the specification, i.e.

$$Mod(\textbf{behaviour } SP \textbf{ wrt } \models_{\text{beh},\Sigma}) = \{\mathcal{M} \in \text{Mod}(\Sigma) \mid \mathcal{M} \models_{\text{beh},\Sigma} \varphi \text{ for all } \phi \in \Phi\}.$$

As explained in Sect. 1 several papers have established relationships between the two approaches in concrete specification formalisms, like many-sorted first-order logic, higher-order logic, and recently, in the domain of reactive systems using a dynamic logic with binders. The purpose of the behaviour-abstractor framework is to identify the crucial concepts needed to relate (the semantics of) behavioural and abstractor specifications such that one gets for free the results of the following theorem whenever a concrete formalism is a behaviour-abstractor framework. The first part of the theorem shows that behavioural semantics is always included in abstractor semantics; the second part shows that behavioural and abstractor semantics coincide if all ordinary models of a specification SP satisfy also behaviourally the axioms of SP. It may sound strange that ordinary satisfaction does not always imply behavioural satisfaction but there are indeed some cases where this can happen as illustrated in [2], Example 3.18, and in [12], Sect. 5.

Theorem 1. *Let* BA *be a behaviour-abstractor framework and* $SP = (\Sigma, \Phi)$ *a specification over* BA*.*

1. $Mod(\textbf{behaviour } SP \textbf{ wrt} \models_{\text{beh},\Sigma}) \subseteq Mod(\textbf{abstract } SP \textbf{ wrt} \equiv_\Sigma)$.
2. $Mod(SP) \subseteq Mod(\textbf{behaviour } SP \textbf{ wrt} \models_{\text{beh},\Sigma})$ *if and only if* $Mod(\textbf{behaviour } SP \textbf{ wrt} \models_{\text{beh},\Sigma}) = Mod(\textbf{abstract } SP \textbf{ wrt} \equiv_\Sigma)$.

Proof. 1. Let $\mathcal{M} \in Mod(\textbf{behaviour } SP \textbf{ wrt} \models_{\text{beh},\Sigma})$. Then $\mathcal{M} \models_{\text{beh},\Sigma} \Phi$ (i.e. $\mathcal{M} \models_{\text{beh},\Sigma} \varphi$ for all $\phi \in \Phi$). By property (2) of a behaviour-abstractor framework, $\mathcal{M} \equiv_\Sigma \mathcal{BB}_\Sigma(\mathcal{M})$. Hence, by property (1), $\mathcal{BB}_\Sigma(\mathcal{M}) \models_{\text{beh},\Sigma} \Phi$. Thus, by property (3), $\mathcal{BB}_\Sigma(\mathcal{M}) \models_\Sigma \Phi$, i.e. $\mathcal{BB}_\Sigma(\mathcal{M}) \in Mod(SP)$. Since $\mathcal{M} \equiv_\Sigma \mathcal{BB}_\Sigma(\mathcal{M})$, we get $\mathcal{M} \in Mod(\textbf{abstract } SP \textbf{ wrt } \equiv_\Sigma)$.

2. "$\Rightarrow$": "$\subseteq$" follows from 1. For the proof of "$\supseteq$", let $\mathcal{M} \in Mod(\textbf{abstract } SP \textbf{ wrt } \equiv_\Sigma)$. Then there exists $\mathcal{N} \in Mod(SP)$ such that $\mathcal{M} \equiv_\Sigma \mathcal{N}$. By assumption, $\mathcal{N} \in Mod(\textbf{behaviour } SP \textbf{ wrt} \models_{\text{beh},\Sigma})$. Hence, $\mathcal{N} \models_{\text{beh},\Sigma} \Phi$ and, by property (1), $\mathcal{M} \models_{\text{beh},\Sigma} \Phi$. Therefore, $\mathcal{M} \in Mod(\textbf{behaviour } SP \textbf{ wrt} \models_{\text{beh},\Sigma})$.
"$\Leftarrow$": Is trivial, since, by definition, $Mod(SP) \subseteq Mod(\textbf{abstract } SP \textbf{ wrt } \equiv_\Sigma)$. □

To prove that a concrete framework is a behaviour-abstractor framework, it is sometimes useful to show, instead of condition (3), that condition (3') formulated in the following lemma holds.

Lemma 2. *Let* $\text{BA} = (\text{Sign}, \text{Sen}, \text{Mod}, \models, \equiv, \models_{\text{beh}}, \mathcal{BB})$ *satisfy conditions (1) and (2) of a behaviour-abstractor framework. Then* BA *satisfies condition (3), i.e.,* BA *is a behaviour-abstractor framework, if and only if* BA *satisfies the following condition (3') for each signature* Σ *and for all* Σ*-models* $\mathcal{M} \in \text{Mod}(\Sigma)$*:*

(3') $\mathcal{M} \models_{\text{beh},\Sigma} \varphi$ iff $\mathcal{BB}_\Sigma(\mathcal{M}) \models_\Sigma \varphi$ for all $\varphi \in \text{Sen}(\Sigma)$.

Proof. Let $\mathcal{M} \in \text{Mod}(\Sigma)$ and $\varphi \in \text{Sen}(\Sigma)$. Conditions (1) and (2) imply

$$(*) \quad \mathcal{M} \models_{\text{beh},\Sigma} \varphi \text{ iff } \mathcal{BB}_\Sigma(\mathcal{M}) \models_{\text{beh},\Sigma} \varphi.$$

"$\Rightarrow$": Assume condition (3) holds. Then: $\mathcal{M} \models_{\text{beh},\Sigma} \varphi$ iff, by (*), $\mathcal{BB}_\Sigma(\mathcal{M}) \models_{\text{beh},\Sigma} \varphi$ iff, by (3), $\mathcal{BB}_\Sigma(\mathcal{M}) \models_\Sigma \varphi$. Hence (3') holds.
"$\Leftarrow$": Assume condition (3') holds. Then: $\mathcal{BB}_\Sigma(\mathcal{M}) \models_{\text{beh},\Sigma} \varphi$ iff, by (*), $\mathcal{M} \models_{\text{beh},\Sigma} \varphi$ iff, by (3'), $\mathcal{BB}_\Sigma(\mathcal{M}) \models_\Sigma \varphi$. Hence (3) holds. □

3. Many-Sorted First-Order Logic with Equality

In this section we consider a behaviour-abstractor framework in the context of many-sorted first-order logic with equality (without predicate symbols). In this context relationships between behavioural and abstractor specifications have been studied in detail in [2]. The purpose of this section is mainly to show which bits and pieces of [2] are significant to instantiate Sect. 2 and to get the relationships between behavioural and abstractor specifications for free by applying Thm. 1. In the following some basic notions of algebraic specifications are only briefly summarised; for more details see e.g. [21].

Signatures and sentences. A *many-sorted signature* $\Sigma = (S, \mathrm{OP})$ consists of a set S of *sorts* and a set OP of *operation symbols* $op : s_1, \ldots, s_n \to s$. For any $\Sigma = (S, \mathrm{OP})$, we assume a family $X = (X_s)_{s \in S}$ of pairwise disjoint sets X_s of variables of sort s. For each $s \in S$, $T_\Sigma(X)_s$ denotes the set of terms of sort s built in the usual way over Σ and X and $T_\Sigma(X)$ denotes the family $(T_\Sigma(X)_s)_{s \in S}$. To take into account the aspect of observability we consider *observational signatures* $\Sigma_{\mathrm{Obs}} = (\Sigma, \mathrm{Obs})$ where $\Sigma = (S, \mathrm{OP})$ is a many-sorted signature and $\mathrm{Obs} \subseteq S$ is a set of *observable sorts*. The class of observational signatures is denoted by $\mathrm{Sign}^{\mathrm{FO}}$ to emphasise that our basic logic is first-order logic. In fact the observable sorts are still irrelevant here up to the point where we consider abstraction equivalences. For any many-sorted signature Σ, the set of Σ-*formulas* is given by

$$\varphi ::= t = r \mid \varphi \wedge \varphi \mid \varphi \vee \varphi \mid \neg\varphi \mid \forall x{:}s.\varphi \mid \exists x{:}s.\varphi$$

where $t, r \in T_\Sigma(X)_s$ are terms of the same sort s and x is a variable of some sort s. For any observational signature $\Sigma_{\mathrm{Obs}} = (\Sigma, \mathrm{Obs})$, a Σ_{Obs}-*sentence* is a Σ-formula φ which contains no free variables. Free variables are defined as usual in first-order logic. The set of Σ_{Obs}-sentences is denoted by $\mathrm{Sen}^{\mathrm{FO}}(\Sigma_{\mathrm{Obs}})$.

Models. Models for an observational signature $\Sigma_{\mathrm{Obs}} = (\Sigma, \mathrm{Obs})$ are Σ-*algebras* $A = ((A_s)_{s \in S}, (op^A)_{op \in \mathrm{OP}})$ with (non-empty) carrier sets A_s and functions op^A respecting the arity of op. The class of all Σ_{Obs}-models is denoted by $\mathrm{Mod}^{\mathrm{FO}}(\Sigma_{\mathrm{Obs}})$. Together with Σ-algebra homomorphisms this class forms a category.

Satisfaction relation. Given a Σ-algebra A and a valuation $\alpha : X \to A$, there is an interpretation function $I_\alpha : T_\Sigma(X) \to A$ which evaluates terms as usual. (More precisely, α and I_α are S-sorted families of functions.) For any Σ-algebra A and valuation $\alpha : X \to A$,

- $A, \alpha \models^{\mathrm{FO}}_\Sigma t = r$ iff $I_\alpha(t) = I_\alpha(r)$;
- $A, \alpha \models^{\mathrm{FO}}_\Sigma \forall x{:}s.\varphi$ iff for all valuations $\beta : X \to A$ with $\beta(y) = \alpha(y)$ for all $y \neq x$: $A, \beta \models^{\mathrm{FO}}_\Sigma \varphi$.

We omit the remaining cases which are inductively defined as usual in first-order logic. For any observational signature $\Sigma_{\mathrm{Obs}} = (\Sigma, \mathrm{Obs})$, a model $A \in \mathrm{Mod}^{\mathrm{FO}}(\Sigma_{\mathrm{Obs}})$ *satisfies* a Σ_{Obs}-sentence φ, denoted by $A \models^{\mathrm{FO}}_{\Sigma_{\mathrm{Obs}}} \varphi$, iff $A, \alpha \models^{\mathrm{FO}}_\Sigma \varphi$ for some valuation α (which is anyway irrelevant, since Σ_{Obs}-sentences have no free variables).

Abstraction equivalence. Let $\Sigma_{\mathrm{Obs}} = (\Sigma, \mathrm{Obs}) \in \mathrm{Sign}^{\mathrm{FO}}$ and $A, A' \in \mathrm{Mod}^{\mathrm{FO}}(\Sigma_{\mathrm{Obs}})$. A is *observationally equivalent* to A', denoted by $A \equiv^{\mathrm{FO}}_{\Sigma_{\mathrm{Obs}}} A'$, if there exists an S-sorted family $Y = (Y_s)_{s \in S}$ of variables with $Y_s = \emptyset$ for all $s \notin \mathrm{Obs}$ and valuations $\alpha : Y \to A$, $\alpha' : Y \to A'$ which are surjective on observable sorts, such that for all equations $t = r$ with terms $t, r \in T_\Sigma(Y)_s$ of observable sort $s \in \mathrm{Obs}$,

$$A, \alpha \models^{\mathrm{FO}}_{\Sigma_{\mathrm{Obs}}} t = r \text{ iff } A', \alpha' \models^{\mathrm{FO}}_{\Sigma_{\mathrm{Obs}}} t = r.$$

The basic idea behind this definition is that two algebras are equivalent from the observational point of view if they cannot be distinguished by interpreting equations of observable sorts. This idea stems from the algebraic specification language ASL [23] where an arbitrary set W of terms could be used to compare algebras. A subtle point is to determine which variables are allowed in the terms. There are different variations studied in the literature; for an overview see [2], Example 4.4. We have decided to follow Nivela, Orejas [17] and allow variables of observable sorts whose values are considered as inputs for the observable experiments.

Behavioural satisfaction relation. Abstraction equivalences compare the observable behaviour of algebras. Another possibility for taking care about observability is to consider the elements "inside" an algebra and to define an indistinguishability relation for them. This idea goes back to Reichel [19] and has later been defined in different variations concerning the input variables of observable experiments; for an overview see [2], Example 3.5. We follow here again Nivela, Orejas [17] and allow variables of observable sorts. Let $\Sigma_{\mathrm{Obs}} = (\Sigma, \mathrm{Obs})$ be an observational signature. Observable experiments are represented by observable contexts. An *observable context* with application sort s and result sort $s' \in \mathrm{Obs}$ is a Σ-term of sort s', which contains a distinguished variable $z_s \notin X$ of sort s and possibly further variables in X of arbitrary observable sorts. Let A be a Σ-algebra. The sub-algebra of A generated over the carrier sets of observable sorts by using functions op^A of A is denoted by $\mathrm{Gen}_{\Sigma_{\mathrm{Obs}}}(A)$. Two elements $a, b \in A$ are *observationally equal*, denoted by $a \approx_{\Sigma_{\mathrm{Obs}},A} b$, if and only if $a, b \in \mathrm{Gen}_{\Sigma_{\mathrm{Obs}}}(A)$ and for all observable contexts c (applicable to a and b) the application of c to a and to b yields the same observable result. The application of observable contexts is defined as expected (see, e.g.,[2]) but taking into account that variables $x \in X$ occurring in an observable context must be evaluated in the generated part $\mathrm{Gen}_{\Sigma_{\mathrm{Obs}}}(A)$.

The *behavioural satisfaction relation* for $A \in \mathrm{Mod}^{\mathrm{FO}}(\Sigma_{\mathrm{Obs}})$ and $\varphi \in \mathrm{Sen}^{\mathrm{FO}}(\Sigma_{\mathrm{Obs}})$, written $A \models^{\mathrm{FO}}_{\mathrm{beh},\Sigma_{\mathrm{Obs}}} \varphi$, is defined analogously to the standard satisfaction relation with the exception that the equality symbol "=" is interpreted by the observational equality $\approx_{\Sigma_{\mathrm{Obs}},A}$ and quantifiers range only over elements in $\mathrm{Gen}_{\Sigma_{\mathrm{Obs}}}(A)$.

Condition (1) of a behaviour-abstractor framework in Def. 1 requires that behavioural satisfaction is preserved by abstraction equivalence. In the context of many-sorted first-order logic this is indeed the case:

Lemma 3. *For any* $\Sigma_{\mathrm{Obs}} \in \mathrm{Sign}^{\mathrm{FO}}$ *and for all* $A, A' \in \mathrm{Mod}^{\mathrm{FO}}(\Sigma_{\mathrm{Obs}})$,

(1) $A \equiv^{\mathrm{FO}}_{\Sigma_{\mathrm{Obs}}} A' \Rightarrow (A \models^{\mathrm{FO}}_{\mathrm{beh},\Sigma_{\mathrm{Obs}}} \varphi$ iff $A' \models^{\mathrm{FO}}_{\mathrm{beh},\Sigma_{\mathrm{Obs}}} \varphi$ for all $\varphi \in \mathrm{Sen}^{\mathrm{FO}}(\Sigma_{\mathrm{Obs}}))$.

Proof. An analogous statement to (1) has been proved in [2], Proposition 5.5, in a more abstract setting considering partial Σ-congruences $\approx$ and equivalences $\equiv$, such that $\equiv$ is factorizable by $\approx$. Factorizability means that algebras are equivalent w.r.t. $\equiv$ if and only if their quotients w.r.t. $\approx$ are isomorphic. In [2], Example 5.4, it was shown that $\equiv^{\mathrm{FO}}_{\Sigma_{\mathrm{Obs}}}$ is factorizable by $\approx_{\Sigma_{\mathrm{Obs}}}$ and therefore (1) holds. □

We have also shown in [2], Theorem 5.6, that even the converse direction of Lemma 3 holds if quotients w.r.t. $\approx$ are countable.

Black box function. The black box view of a Σ_{Obs}-model A is defined as the quotient algebra of $\mathrm{Gen}_{\Sigma_{\mathrm{Obs}}}(A)$ w.r.t. the observational equality $\approx_{\Sigma_{\mathrm{Obs}},A}$, i.e. $\mathcal{BB}^{\mathrm{FO}}_{\Sigma_{\mathrm{Obs}}}(A) =_{\mathrm{def}} \mathrm{Gen}_{\Sigma_{\mathrm{Obs}}}(A)/\approx_{\Sigma_{\mathrm{Obs}},A}$. It is well-defined, since $\approx_{\Sigma_{\mathrm{Obs}},A}$ is a total Σ-congruence on $\mathrm{Gen}_{\Sigma_{\mathrm{Obs}}}(A)$.

Theorem 4. $\mathrm{BA}^{\mathrm{FO}} = (\mathrm{Sign}^{\mathrm{FO}}, \mathrm{Sen}^{\mathrm{FO}}, \mathrm{Mod}^{\mathrm{FO}}, \models^{\mathrm{FO}}, \equiv^{\mathrm{FO}}, \models^{\mathrm{FO}}_{\mathrm{beh}}, \mathcal{BB}^{\mathrm{FO}})$ *is a behaviour-abstractor framework, where* $\mathrm{Sen}^{\mathrm{FO}} = (\mathrm{Sen}^{\mathrm{FO}}(\Sigma_{\mathrm{Obs}}))_{\Sigma_{\mathrm{Obs}} \in \mathrm{Sign}^{\mathrm{FO}}}$ *is the family of sets* $\mathrm{Sen}^{\mathrm{FO}}(\Sigma_{\mathrm{Obs}})$ *of* Σ_{Obs}*-sentences, and similarly for the other components of* $\mathrm{BA}^{\mathrm{FO}}$.

Proof. We have to show that conditions (1) - (3) of Def. 1 hold. (1) holds by Lemma 3. It remains to show that conditions (2) and (3) are satisfied by the black box construction, i.e. that for any $\Sigma_{\mathrm{Obs}} \in \mathrm{Sign}^{\mathrm{FO}}$ and for all $A \in \mathrm{Mod}^{\mathrm{FO}}(\Sigma_{\mathrm{Obs}})$,

(2) $A \equiv^{\mathrm{FO}}_{\Sigma_{\mathrm{Obs}}} \mathcal{BB}^{\mathrm{FO}}_{\Sigma_{\mathrm{Obs}}}(A)$, and

(3) $\mathcal{BB}^{\mathrm{FO}}_{\Sigma_{\mathrm{Obs}}}(A) \models^{\mathrm{FO}}_{\mathrm{beh},\Sigma_{\mathrm{Obs}}} \varphi$ iff $\mathcal{BB}^{\mathrm{FO}}_{\Sigma_{\mathrm{Obs}}}(A) \models^{\mathrm{FO}}_{\Sigma_{\mathrm{Obs}}} \varphi$ for all $\varphi \in \mathrm{Sen}^{\mathrm{FO}}(\Sigma_{\mathrm{Obs}})$.

(2) has been proved in [2], Lemma 5.8, in the more abstract setting explained in the proof of Lemma 3. It assumes again factorizability but also "weak regularity" of $\approx_{\Sigma_{\mathrm{Obs}}}$, a property which requires that the quotient construction is idempotent up to isomorphism. Since this is fulfilled for quotients w.r.t. observational equalities, see [2], Example 3.15, (2) holds.

Instead of (3) we show condition (3'), see Lemma 2, i.e. that for any Σ_{Obs}-model A and Σ_{Obs}-sentence φ, $A \models^{\mathrm{FO}}_{\mathrm{beh},\Sigma_{\mathrm{Obs}}} \varphi$ iff $A/\approx_{\Sigma_{\mathrm{Obs}},A} \models^{\mathrm{FO}}_{\Sigma_{\mathrm{Obs}}} \varphi$. But this is a direct application of Thm. 3.11 in [2] since we know that observational equalities are partial congruences. □

As a consequence of Thm. 4 we can instantiate Thm. 1 and get the respective relationships between behavioural and abstractor specifications in the context of many-sorted first-order logic. Analogous results have been obtained in Thm. 5.9 and Thm. 5.11 of [2] for factorizable equivalences and weakly regular partial congruences.

4. Higher-Order Logic

The results of [2] have been generalised to higher-order logic by Hofmann and Sannella in [13]. In the following of this section we will collect those pieces of [13] which constitute a behaviour-abstractor framework. We will only give a compact summary; for more details see [13].

Signatures and sentences. We consider again *observational signatures* $\Sigma_{\mathrm{Obs}} = (\Sigma, \mathrm{Obs})$ where $\Sigma = (S, \mathrm{OP})$ is a many-sorted signature and $\mathrm{Obs} \subseteq S$ is a set of *observable sorts*. In contrast to first-order logic, operation symbols $op : s_1, \ldots, s_n \to s$ are considered as constants of type $s_1, \ldots, s_n \to s$. The sorts in S are called *base types* and observable sorts are base types as well. Hofmann and Sannella argue "All other types, including bracket types are *hidden* in the sense that their values may only be inspected indirectly by performing experiments (i.e. evaluating terms) that yield a result of a type in *OBS*". The class of observational signatures is denoted by $\mathrm{Sign}^{\mathrm{HO}}$ to emphasise that we are going to work in higher-order logic. Given $\Sigma_{\mathrm{Obs}} = (\Sigma, \mathrm{Obs})$, the types over Σ are defined by the grammar

$$\tau ::= b \mid [\tau_1, \ldots, \tau_n]$$

where $b \in S$ and $n \geq 0$. Bracket types denote n-ary predicates; the type $[\,]$ is regarded as a proposition.

The *terms* over Σ are given by the grammar

$$t ::= x \mid op(t_1, \ldots, t_n) \mid \lambda(x_1{:}\tau_1, \ldots, x_n{:}\tau_n).t \mid t(t_1, \ldots, t_n) \mid t \Rightarrow t' \mid \forall x{:}\tau.t$$

where $x, x_1, \ldots, x_n$ are variables. A sequence $\Gamma = (x_1{:}\tau_1, \ldots, x_n{:}\tau_n)$ with pairwise distinct typed variables x_i is called a *variable context*. In [13] there are typing rules to derive $t : \tau$ from a context Γ and then t is called a *term in context* Γ. A term is *closed* if it is typable in the empty context. A *formula* in context Γ is a term φ such that $\varphi : [\,]$ is derivable from Γ. Hofmann and Sannella point out that "there is no need to include equality as a built-in predicate, since it is expressible using higher-order quantification". An equation $t =_\tau t'$ is an abbreviation for $\forall P{:}[\tau].P(t) \Rightarrow P(t')$. A closed formula φ is a *higher-order* Σ_{Obs}*-sentence*. The set of higher-order Σ_{Obs}-sentences is denoted by $\mathrm{Sen}^{\mathrm{HO}}(\Sigma_{\mathrm{Obs}})$.

Models. Models for an observational signature $\Sigma_{\mathrm{Obs}} = (\Sigma, \mathrm{Obs})$ are again Σ-*algebras* $A = ((A_s)_{s\in S}, (op^A)_{op\in \mathrm{OP}})$. The class of all Σ_{Obs}-models is denoted by $\mathrm{Mod}^{\mathrm{HO}}(\Sigma_{\mathrm{Obs}})$. Together with Σ-algebra homomorphisms this class forms a category. Given a Σ-algebra A, types of the form $[\tau_1, \ldots, \tau_n]$ are interpreted by $[\![[\tau_1, \ldots, \tau_n]]\!]^A = Pow([\![\tau_1]\!]^A \times \ldots \times [\![\tau_n]\!]^A)$ where Pow denotes the power set functor for sets. In particular, $[\![[\,]]\!]^A$ is a two element set $\{\emptyset, \{*\}\}$. Following [13], we write $\mathbf{ff}$ for $\emptyset$ and $\mathbf{tt}$ for $\{*\}$.

Satisfaction relation. Given a Σ-algebra A and a variable context Γ, a Γ-*environment on* A is a $Types(\Sigma)$-sorted family of valuations $\rho = (\rho_\tau : \Gamma_\tau \to [\![\tau]\!]^A)_{\tau\in Types(\Sigma)}$ where Γ_τ shows the variables of type τ occurring in Γ. For a given Γ-environment ρ, terms t in context Γ can be interpreted such that, if $t : \tau$ is derivable from Γ, then $[\![t]\!]^A_\rho \in [\![\tau]\!]^A$; see [13], Proposition 3.6. For a formula φ in context Γ and Γ-environment ρ, A satisfies φ, denoted here by $A, \rho \models^{\mathrm{HO}}_\Sigma \varphi$, iff $[\![\varphi]\!]^A_\rho = \mathbf{tt}$. For any observational signature $\Sigma_{\mathrm{Obs}} = (\Sigma, \mathrm{Obs})$, a model $A \in \mathrm{Mod}^{\mathrm{HO}}(\Sigma_{\mathrm{Obs}})$ *satisfies* a higher-order Σ_{Obs}-sentence φ, denoted here by $A \models^{\mathrm{HO}}_{\Sigma_{\mathrm{Obs}}} \varphi$, iff $A, \rho \models^{\mathrm{HO}}_\Sigma \varphi$ for some environment ρ (which is anyway irrelevant, since Σ_{Obs}-sentences are closed terms).

Abstraction equivalence. Let $\Sigma_{\mathrm{Obs}} = (\Sigma, \mathrm{Obs}) \in \mathrm{Sign}^{\mathrm{HO}}$ and $A, A' \in \mathrm{Mod}^{\mathrm{HO}}(\Sigma_{\mathrm{Obs}})$. Then A and A' are ordinary Σ-algebras with distinguished carrier sets of observable elements, as in the first-order case. Hofmann and Sannella use in [13] indeed the same observational equivalence between algebras as defined in the last section, which we denote here by $\equiv^{\mathrm{HO}}_{\Sigma_{\mathrm{Obs}}}$ (and which is denoted by $\equiv_{\mathrm{OBS}}$ in [13]). They write "It might seem surprising that the definition of $\equiv_{\mathrm{OBS}}$ does not make use of the higher-order features of the language, except as a result of the way that equality is expressed via quantification over predicates. ... The reason for this choice is that the natural modification of the definition of $\equiv_{\mathrm{OBS}}$ to make use of higher-order formulae (Defintion 5.19) gives exactly the same relation, see Corollary 5.22."

Behavioural satisfaction relation. In higher-order logic observational equality of elements on the base types is defined as in the first-order case and denoted again by $\approx_{\Sigma_{\mathrm{Obs}},A}$, for any Σ-algebra A. The situation is, however, more complicated for higher-order types. Hofmann and Sannella show in [13] how to extend partial congruence relations $\approx$ on base types to bracket types. The point is that "We must make sure that the predicate variables only range over predicates which "respect" the partial congruence"; see [13]. This means that predicates do "not differentiate between values that are related by $\approx$". Then, Hofmann and Sannella give an interpretation for all types, such that $\approx$ is respected, and an interpretation of terms in those domains; see Def. 3.21 and Def. 3.26 in [13]. For a given Γ-environment ρ w.r.t. $\approx$ and term t in context Γ, if $t : \tau$ is derviable from Γ, then $[\![t]\!]^{\approx,A}_{\rho} \in [\![\tau]\!]^{\approx,A}$; see [13], Corollary 3.28. Hofmann and Sannella explain that a comparison of the interpretation of terms w.r.t. $\approx$ with the standard interpretation "reveals that the only difference is the change to the meaning of λ-abstraction and universal quantification induced by the different interpretation of types".

For a formula φ in context Γ and a Γ-environment ρ w.r.t. $\approx$, A satisfies behaviourally φ, denoted here by $A, \rho \models^{\mathrm{HO}}_{\mathrm{beh},\Sigma} \varphi$, iff $[\![\varphi]\!]^{\approx,A}_{\rho} = \mathbf{tt}$. Since the observational equality $\approx_{\Sigma_{\mathrm{Obs}},A}$ is a partial Σ-congruence for any Σ-algebra A, one defines, for any observational signature $\Sigma_{\mathrm{Obs}} = (\Sigma, \mathrm{Obs})$, $A \in \mathrm{Mod}^{\mathrm{HO}}(\Sigma_{\mathrm{Obs}})$ and higher-order Σ_{Obs}-sentence φ: *A satisfies behaviourally φ*, denoted here by $A \models^{\mathrm{HO}}_{\mathrm{beh},\Sigma_{\mathrm{Obs}}} \varphi$, iff $A, \rho \models^{\mathrm{HO}}_{\mathrm{beh},\Sigma} \varphi$ for some environment ρ (which is again irrelevant, since Σ_{Obs}-sentences are closed terms).

Black box function. The black box view of a Σ_{Obs}-model A is defined, as in first-order logic, as the quotient algebra of $\mathrm{Gen}_{\Sigma_{\mathrm{Obs}}}(A)$ w.r.t. the observational equality $\approx_{\Sigma_{\mathrm{Obs}},A}$, i.e. $\mathcal{BB}^{\mathrm{HO}}_{\Sigma_{\mathrm{Obs}}}(A) =_{\mathrm{def}} \mathrm{Gen}_{\Sigma_{\mathrm{Obs}}}(A)/\!\approx_{\Sigma_{\mathrm{Obs}},A}$. Elements of $\mathrm{Gen}_{\Sigma_{\mathrm{Obs}}}(A)$ are called "*OBS*-reachable" in [13].

Theorem 5. $\mathrm{BA}^{\mathrm{HO}} = (\mathrm{Sign}^{\mathrm{HO}}, \mathrm{Sen}^{\mathrm{HO}}, \mathrm{Mod}^{\mathrm{HO}}, \models^{\mathrm{HO}}, \equiv^{\mathrm{HO}}, \models^{\mathrm{HO}}_{\mathrm{beh}}, \mathcal{BB}^{\mathrm{HO}})$ *is a behaviour-abstractor framework, where* $\mathrm{Sen}^{\mathrm{HO}} = (\mathrm{Sen}^{\mathrm{HO}}(\Sigma_{\mathrm{Obs}}))_{\Sigma_{\mathrm{Obs}} \in \mathrm{Sign}^{\mathrm{HO}}}$ *is the family of sets* $\mathrm{Sen}^{\mathrm{HO}}(\Sigma_{\mathrm{Obs}})$ *of higher-order* Σ_{Obs}*-sentences, and similarly for the other components of* $\mathrm{BA}^{\mathrm{HO}}$*.*

Proof. Let Σ_{Obs} be an observational signature. First we show that condition (3') of Lemma 2 holds, i.e. that for any $A \in \mathrm{Mod}^{\mathrm{HO}}(\Sigma_{\mathrm{Obs}})$,

(3') $A \models^{\mathrm{HO}}_{\mathrm{beh},\Sigma_{\mathrm{Obs}}} \varphi$ iff $A/\!\approx_{\Sigma_{\mathrm{Obs}},A} \models^{\mathrm{HO}}_{\Sigma_{\mathrm{Obs}}} \varphi$ for all $\varphi \in \mathrm{Sen}^{\mathrm{FO}}(\Sigma_{\mathrm{Obs}})$.

But this is a direct application of Thm. 3.35 in [13].

Now we can prove condition (1) of Def. 1 which is not explicitly discussed in [13] but is interesting, since it shows that also in higher-order logic behavioural satisfaction is preserved by abstraction equivalence. For all $A, A' \in \mathrm{Mod}^{\mathrm{HO}}(\Sigma_{\mathrm{Obs}})$,

(1) $A \equiv^{\mathrm{HO}}_{\Sigma_{\mathrm{Obs}}} A' \Rightarrow (A \models^{\mathrm{HO}}_{\mathrm{beh},\Sigma_{\mathrm{Obs}}} \varphi$ iff $A' \models^{\mathrm{HO}}_{\mathrm{beh},\Sigma_{\mathrm{Obs}}} \varphi$ for all $\varphi \in \mathrm{Sen}^{\mathrm{HO}}(\Sigma_{\mathrm{Obs}}))$.

For the proof of (1), we assume $A \equiv^{\mathrm{HO}}_{\Sigma_{\mathrm{Obs}}} A'$. Let $A \models^{\mathrm{HO}}_{\mathrm{beh},\Sigma_{\mathrm{Obs}}} \varphi$ for some $\varphi \in \mathrm{Sen}^{\mathrm{HO}}(\Sigma_{\mathrm{Obs}})$. By (3'), we know, $A/\!\approx_{\Sigma_{\mathrm{Obs}},A} \models^{\mathrm{HO}}_{\Sigma_{\mathrm{Obs}}} \varphi$, i.e. $\mathcal{BB}^{\mathrm{HO}}_{\Sigma_{\mathrm{Obs}}}(A) \models^{\mathrm{HO}}_{\Sigma_{\mathrm{Obs}}} \varphi$. Since $\equiv^{\mathrm{HO}}_{\Sigma_{\mathrm{Obs}}}$ is factorizable by $\approx_{\Sigma_{\mathrm{Obs}}}$ (Prop. 4.15 and Cor. 5.16 in [13]), $\mathcal{BB}^{\mathrm{HO}}_{\Sigma_{\mathrm{Obs}}}(A)$ and $\mathcal{BB}^{\mathrm{HO}}_{\Sigma_{\mathrm{Obs}}}(A')$ are isomorphic. Hence, by Cor. 3.14 in [13], $\mathcal{BB}^{\mathrm{HO}}_{\Sigma_{\mathrm{Obs}}}(A') \models^{\mathrm{HO}}_{\Sigma_{\mathrm{Obs}}} \varphi$. Then we can apply again (3') and obtain $A' \models^{\mathrm{HO}}_{\mathrm{beh},\Sigma_{\mathrm{Obs}}} \varphi$. The converse direction is analogous.

At next, we show that (2) of Def. 1 holds, i.e. that for all $A \in \mathrm{Mod}^{\mathrm{HO}}(\Sigma_{\mathrm{Obs}})$,

(2) $A \equiv^{\mathrm{HO}}_{\Sigma_{\mathrm{Obs}}} \mathcal{BB}^{\mathrm{HO}}_{\Sigma_{\mathrm{Obs}}}(A)$.

(2) has been stated in [13] within the proof of Theorem 6.5 for factorizable abstraction equivalences and "regular" partial congruences. That both is valid for $\equiv_{\mathrm{OBS}}$ and $\approx_{\Sigma_{\mathrm{Obs}}}$ has been shown in [13]; Prop. 4.15, Cor. 5.16 and Prop. 4.7.

Now we know that (3') holds and that (1) and (2) hold. Hence, according to Lemma 2, $\mathrm{BA}^{\mathrm{HO}}$ is a behaviour-abstractor framework. □

As a consequence of Thm. 5 we can instantiate Thm. 1 and get the respective relationships between behavioural and abstractor specifications in the context of higher-order logic. Analogous results have been obtained in Thm. 6.6 and Thm. 6.7 of [13] for factorizable equivalences and weakly regular partial congruences.

5. Dynamic Logic with Binders

Dynamic logic with binders, called $\mathcal{D}^{\downarrow}$-logic, has been introduced in [14] as a logic which allows to express properties of reactive systems from abstract safety and liveness properties down to concrete ones specifying the (recursive) structure of processes. It combines modalities indexed by regular expressions of actions, as in Dynamic Logic [6], and state variables with binders, as in Hybrid Logic [3]. We show in this section that $\mathcal{D}^{\downarrow}$-logic offers all ingredients required for a behaviour-abstractor framework.

Signatures and sentences. A $\mathcal{D}^{\downarrow}$*-signature* is a set A of *atomic actions*. The class of $\mathcal{D}^{\downarrow}$-signatures is denoted by $\mathrm{Sign}^{\mathcal{D}^{\downarrow}}$. The set of *composed actions* $\mathrm{Act}(A)$, induced by atomic actions A, is given by

$$\alpha ::= a \mid \alpha;\alpha \mid \alpha + \alpha \mid \alpha^*$$

where $a \in A$. For any $A \in \mathrm{Sign}^{\mathcal{D}^{\downarrow}}$, the set of A*-formulas* is given by

$$\varphi ::= \mathbf{tt} \mid \mathbf{ff} \mid \varphi \wedge \varphi \mid \varphi \vee \varphi \mid \neg\varphi \mid \langle\alpha\rangle\varphi \mid [\alpha]\varphi \mid x \mid \downarrow x.\,\varphi \mid @_x\varphi$$

where $\alpha \in \mathrm{Act}(A)$ and $x \in X$ is a variable belonging to a universal set X of state variables. An A*-sentence* is an A-formula φ which contains no free variables. Free variables are defined as usual with $\downarrow$ being the only operator binding variables. The idea of the binder operator $\downarrow x.\varphi$ is to assign to variable x the current state of evaluation and then to continue with evaluating φ. The operator $@_x\varphi$ evaluates φ in the state assigned to x. $\mathcal{D}^{\downarrow}$ retains from Hybrid Logic these two constructions but omits the use of nominals since we are only interested in properties of states reachable from the initial state, i.e. processes. The set of A-sentences is denoted by $\mathrm{Sen}^{\mathcal{D}^{\downarrow}}(A)$.

Models. Models in $\mathcal{D}^{\downarrow}$ are reachable, labelled transition systems with initial state. Let $A \in \mathrm{Sign}^{\mathcal{D}^{\downarrow}}$ be a set of atomic actions. An A*-model* is a triple $\mathcal{M} = (W, w_0, R)$ where W is a *set of states*, $w_0 \in W$ is the *initial state* and $R = (R_a \subseteq W \times W)_{a \in A}$ is a family of *transition relations* such that, for each $w \in W$, either $w = w_0$ or there is a finite sequence of transitions $(w_{k-1}, w_k) \in R_{a_k}$, $1 \le k \le n$, with $a_k \in A$, such that $w_n = w$. The class of A-models is denoted by $\mathrm{Mod}^{\mathcal{D}^{\downarrow}}(A)$.

Satisfaction relation. To define the satisfaction relation we need to clarify how composed actions are interpreted in models. Let $\alpha \in \mathrm{Act}(A)$ and $\mathcal{M} = (W, w_0, R)$. The interpretation of α in $\mathcal{M}$ extends the interpretation of atomic actions by $R_{\alpha;\alpha'} = R_\alpha \cdot R_{\alpha'}$, $R_{\alpha+\alpha'} = R_\alpha \cup R_{\alpha'}$ and $R_{\alpha^*} = (R_\alpha)^\star$, with the operations $\cdot$, $\cup$ and $\star$ standing for relational composition, union and reflexive-transitive closure. A *valuation* is a function $g : X \to W$. Given such a valuation g, a variable $x \in X$ and a state $w \in W$, $g[x \mapsto w]$ denotes the valuation with $g[x \mapsto w](x) = w$ and $g[x \mapsto w](y) = g(y)$ for any $y \in X, y \neq x$. For any A-model $\mathcal{M} = (W, w_0, R) \in \mathrm{Mod}^{\mathcal{D}^{\downarrow}}(A)$, state $w \in W$ and valuation $g : X \to W$,

- $\mathcal{M}, g, w \models^{\mathcal{D}^{\downarrow}}_A \langle\alpha\rangle\varphi$ iff there is a $v \in W$ with $(w, v) \in R_\alpha$ and $\mathcal{M}, g, v \models^{\mathcal{D}^{\downarrow}}_A \varphi$;

- $\mathcal{M}, g, w \models_A^{\mathcal{D}^\downarrow} x$ iff $g(x) = w$;
- $\mathcal{M}, g, w \models_A^{\mathcal{D}^\downarrow} \downarrow x.\, \varphi$ iff $\mathcal{M}, g[x \mapsto w], w \models_A^{\mathcal{D}^\downarrow} \varphi$;
- $\mathcal{M}, g, w \models_A^{\mathcal{D}^\downarrow} @_x\varphi$ iff $\mathcal{M}, g, g(x) \models_A^{\mathcal{D}^\downarrow} \varphi$.

We omit the remaining cases which are (inductively) defined as usual. If φ is an A-sentence, then the valuation is irrelevant, i.e., $\mathcal{M}, g, w \models_A^{\mathcal{D}^\downarrow} \varphi$ iff $\mathcal{M}, w \models_A^{\mathcal{D}^\downarrow} \varphi$. $\mathcal{M}$ *satisfies* an A-sentence φ, denoted by $\mathcal{M} \models_A^{\mathcal{D}^\downarrow} \varphi$, iff $\mathcal{M}, w_0 \models_A^{\mathcal{D}^\downarrow} \varphi$.

Abstraction equivalence. As abstraction equivalence for A-models we use bisimulation equivalence. Let $\mathcal{M} = (W, w_0, R)$ and $\mathcal{M}' = (W', w_0', R')$ be two A-models. A *bisimulation relation* between $\mathcal{M}$ and $\mathcal{M}'$ is a relation $S \subseteq W \times W'$ that contains (w_0, w_0') and satisfies

(zig) for any $a \in A$, $w, v \in W$, $w' \in W'$ such that $(w, w') \in S$:
if $(w, v) \in R_a$, then there is a $v' \in W'$ such that $(w', v') \in R_a'$ and $(v, v') \in S$;

(zag) for any $a \in A$, $w \in W$, $w', v' \in W'$ such that $(w, w') \in S$:
if $(w', v') \in R_a'$, then there is a $v \in W$ such that $(w, v) \in R_a$ and $(v, v') \in S$.

Two A-models $\mathcal{M}, \mathcal{M}' \in \mathrm{Mod}^{\mathcal{D}^\downarrow}(A)$ are *bisimulation equivalent*, denoted by $\mathcal{M} \equiv_A^{\mathcal{D}^\downarrow} \mathcal{M}'$, if there exists a bisimulation relation between $\mathcal{M}$ and $\mathcal{M}'$. It is well known that bisimulation equivalence is indeed an equivalence relation on the class of A-models. Moreover, if $\mathcal{M} \equiv_A^{\mathcal{D}^\downarrow} \mathcal{M}'$, then there exists a greatest bisimulation relation between $\mathcal{M}$ and $\mathcal{M}'$, which we denote by $\sim_{\mathcal{M}}^{\mathcal{M}'}$.

Behavioural satisfaction relation. In [12] we have shown that satisfaction of A-sentences in $\mathcal{D}^\downarrow$ is, in general, not preserved by bisimulation equivalence. To overcome this we have introduced a behavioural satisfaction relation (called observational satisfaction in [12]) between A-models and A-sentences which relaxes the satisfaction relation in $\mathcal{D}^\downarrow$ defined above. The crucial idea is that behavioural satisfaction allows to interpret variables x by states which are not identical but only observationally equal to the current value of x. For this purpose, we consider for any A-model $\mathcal{M} = (W, w_0, R)$ the greatest bisimulation relation $\sim_{\mathcal{M}}^{\mathcal{M}} \subseteq W \times W$ on the states of $\mathcal{M}$ which we call *observational equality*. Instead of $\sim_{\mathcal{M}}^{\mathcal{M}}$ we write briefly $\sim_{\mathcal{M}}$.

Let $\mathcal{M} = (W, w_0, R)$ be an A-model, $w \in W$ and $g : X \to W$ a valuation. The *behavioural satisfaction* of an A-formula φ in state w of $\mathcal{M}$ w.r.t. valuation g, denoted by $\mathcal{M}, g, w \models_{\mathrm{beh},A}^{\mathcal{D}^\downarrow} \varphi$, is defined analogously to the satisfaction relation $\models_A^{\mathcal{D}^\downarrow}$ above with the exception of

$$\mathcal{M}, g, w \models_{\mathrm{beh},A}^{\mathcal{D}^\downarrow} x \text{ iff } g(x) \sim_{\mathcal{M}} w.$$

For each A-sentence $\varphi \in \mathrm{Sign}^{\mathcal{D}^\downarrow}(A)$, the valuation is irrelevant and $\mathcal{M}$ *satisfies behaviourally* φ, denoted by $\mathcal{M} \models_{\mathrm{beh},A}^{\mathcal{D}^\downarrow} \varphi$, iff $\mathcal{M}, w_0 \models_{\mathrm{beh},A}^{\mathcal{D}^\downarrow} \varphi$.

In the context of $\mathcal{D}^\downarrow$-logic, condition (1) of a behaviour-abstractor framework in Def. 1 expresses modal invariance of A-sentences w.r.t. bisimulation equivalence and behavioural satisfaction. This was one of the main results in [12] (Corollary 3) and is formulated in the following lemma. We have also shown in [12] that even the converse direction holds for image-finite transition systems.

Lemma 6. *For any $A \in \mathrm{Sign}^{\mathcal{D}^\downarrow}$ and for all $\mathcal{M}, \mathcal{M}' \in \mathrm{Mod}^{\mathcal{D}^\downarrow}(A)$,*

(1) $\mathcal{M} \equiv_A^{\mathcal{D}^\downarrow} \mathcal{M}' \Rightarrow (\mathcal{M} \models_{\mathrm{beh},A}^{\mathcal{D}^\downarrow} \varphi \text{ iff } \mathcal{M}' \models_{\mathrm{beh},A}^{\mathcal{D}^\downarrow} \varphi \text{ for all } \varphi \in \mathrm{Sen}^{\mathcal{D}^\downarrow}(A))$.

Black box function. To define the black box view of an A-model $\mathcal{M}$ we consider a quotient construction which identifies observationally equal states. Let $\mathcal{M} = (W, w_0, R)$. The *quotient of* $\mathcal{M}$ w.r.t. $\sim_{\mathcal{M}}$ is the A-model $\mathcal{M}/\!\sim = (W/\!\sim, [w_0], R/\!\sim)$, where

- $W/\!\sim = \{[w] \mid w \in W\}$ with $[w] = \{w' \mid w' \sim_{\mathcal{M}} w\}$, and for all $a \in A$,
- $(R/\!\sim)_a = \{([w],[v]) \mid \exists w' \in [w], v' \in [v] : (w', v') \in R_a\}$.

Since $\sim_{\mathcal{M}}$ is a bisimulation relation, $\mathcal{M}/\!\sim$ is well-defined. For any $\mathcal{M} \in \mathrm{Mod}^{\mathcal{D}^{\downarrow}}(A)$, the *black box view* of $\mathcal{M}$ is defined by $\mathcal{BB}_A^{\mathcal{D}^{\downarrow}}(\mathcal{M}) =_{\mathrm{def}} \mathcal{M}/\!\sim$.

Theorem 7. $\mathrm{BA}^{\mathcal{D}^{\downarrow}} = (\mathrm{Sign}^{\mathcal{D}^{\downarrow}}, \mathrm{Sen}^{\mathcal{D}^{\downarrow}}, \mathrm{Mod}^{\mathcal{D}^{\downarrow}}, \models^{\mathcal{D}^{\downarrow}}, \equiv^{\mathcal{D}^{\downarrow}}, \models^{\mathcal{D}^{\downarrow}}_{\mathrm{beh}}, \mathcal{BB}^{\mathcal{D}^{\downarrow}})$ *is a behaviour-abstractor framework, where* $\mathrm{Sen}^{\mathcal{D}^{\downarrow}} = (\mathrm{Sen}^{\mathcal{D}^{\downarrow}}(A))_{A \in \mathrm{Sign}^{\mathcal{D}^{\downarrow}}}$ *is the family of sets* $\mathrm{Sen}^{\mathcal{D}^{\downarrow}}(A)$ *of A-sentences, and similary for the other components of* $\mathrm{BA}^{\mathcal{D}^{\downarrow}}$.

Proof. Condition (1) of Def. 1 holds by Lemma 6. Conditions (2) and (3) expressed in $\mathcal{D}^{\downarrow}$-logic require, that for any $A \in \mathrm{Sign}^{\mathcal{D}^{\downarrow}}$ and for all $\mathcal{M} \in \mathrm{Mod}^{\mathcal{D}^{\downarrow}}(A)$,

(2) $\mathcal{M} \equiv_A^{\mathcal{D}^{\downarrow}} \mathcal{BB}_A^{\mathcal{D}^{\downarrow}}(\mathcal{M})$.

(3) $\mathcal{BB}_A^{\mathcal{D}^{\downarrow}}(\mathcal{M}) \models^{\mathcal{D}^{\downarrow}}_{\mathrm{beh},A} \varphi$ iff $\mathcal{BB}_A^{\mathcal{D}^{\downarrow}}(\mathcal{M}) \models_A^{\mathcal{D}^{\downarrow}} \varphi$ for all $\varphi \in \mathrm{Sen}^{\mathcal{D}^{\downarrow}}(A)$.

For (2) it is straightforward to show that $\mathcal{M} \equiv_A^{\mathcal{D}^{\downarrow}} \mathcal{M}/\!\sim$, since the definition of $R/\!\sim$ entails that the relation $B \subseteq W \times W/\!\sim$ with $B = \{(w,[w]) \mid w \in W\}$ is a bisimulation relation between $\mathcal{M}$ and $\mathcal{M}/\!\sim$, and hence between $\mathcal{M}$ and $\mathcal{BB}_A^{\mathcal{D}^{\downarrow}}(\mathcal{M})$. For a detailed proof of this fact see proof of Thm. 8 in [12].

Instead of (3) we show condition (3'), see Lemma 2, i.e., that for any A-model $\mathcal{M}$ and A-sentence φ, $\mathcal{M} \models^{\mathcal{D}^{\downarrow}}_{\mathrm{beh},A} \varphi$ iff $\mathcal{M}/\!\sim \models_A^{\mathcal{D}^{\downarrow}} \varphi$. This is exactly the content of Thm. 5 in [12]. □

As a consequence of Thm. 7 we can instantiate Thm. 1 and get the respective relationships between behavioural and abstractor specifications in the context of $\mathcal{D}^{\downarrow}$-logic. The same results have been obtained in Thm. 8 of [12] with a direct proof in $\mathcal{D}^{\downarrow}$-logic.

6. Hennessy-Milner Logic

Hennessy-Milner Logic is a modal logic introduced by Hennessy and Milner to characterise bisimulation equivalence; c.f. [7]. In this section we discuss how to obtain a behaviour-abstractor framework for Hennessy-Milner logic.

Signatures and sentences. A HM-*signature* is a set V of *visible actions*. The class of HM-signatures is denoted by $\mathrm{Sign}^{\mathrm{HM}}$. For any $V \in \mathrm{Sign}^{\mathrm{HM}}$, the set of V*-sentences* is given by

$$\varphi ::= \mathbf{tt} \mid \mathbf{ff} \mid \varphi \wedge \varphi \mid \varphi \vee \varphi \mid \langle a \rangle \varphi \mid [a]\varphi$$

where $a \in V \cup \{\epsilon\}$ is a visible action or the empty action ϵ. As we will see below the empty action has no effect when evaluating sentences; it is also not part of classical Hennessy-Milner logic but we have introduced it here because we will use the same set of sentences when considering "observable" Hennessy-Milner logic below. The set of V-sentences is denoted by $\mathrm{Sen}^{\mathrm{HM}}(V)$.

Models. Models are reachable, labelled transition systems with initial state. Additionally to visible actions in V, transitions can also be labelled with the internal (invisible) action τ. Thus, for any $V \in \mathrm{Sign}^{\mathrm{HM}}$, a V*-model* is an A-model as defined in Sect. 5 with $A = V \cup \{\tau\}$. A V-model is τ*-free* if it does not contain (silent) τ-transitions. The class of V-models is denoted by $\mathrm{Mod}^{\mathrm{HM}}(V)$.

Satisfaction relation. The satisfaction relation $\models^{\mathrm{HM}}_{V}$ between V-models $\mathcal{M}$ and V-sentences φ is defined by restricting the satisfaction relation defined for $\mathcal{D}^{\downarrow}$-logic in Sect. 5 to V-sentences and adding the (trivial) cases

- $\mathcal{M}, w \models^{\mathrm{HM}}_{V} \langle\epsilon\rangle\varphi$ iff $\mathcal{M}, w \models^{\mathrm{HM}}_{V} [\epsilon]\varphi$ iff $\mathcal{M}, w \models^{\mathrm{HM}}_{V} \varphi$

where $w \in W$. Note that valuations of variables are omitted since V-sentences are variable-free. $\mathcal{M}$ *satisfies* a V-sentence φ, denoted by $\mathcal{M} \models^{\mathrm{HM}}_{V} \varphi$, if $\mathcal{M}, w_0 \models^{\mathrm{HM}}_{V} \varphi$.

Abstraction equivalence. As abstraction equivalence we use weak bisimulations, called observable bisimulations in [24]. For the definition we must first define the τ-closure of transition relations with visible actions. Let $\mathcal{M} = (W, w_0, R)$ be a V-model with transition relations $R = (R_a \subseteq W \times W)_{a \in V \cup \{\tau\}}$. For each $a \in V$, the τ-closure of R_a is the set $\hat{R}_a \subseteq W \times W$ such that $(w, v) \in \hat{R}_a$ if and only if there is a finite sequence of transitions from w to v containing exactly one transition labelled with visible action a surrounded by arbitrarily many τ-transitions. The set $\hat{R}_\epsilon \subseteq W \times W$ contains all pairs (w, v) such that there is a finite, possibly empty, sequence of τ-transitions from w to v. Let $\mathcal{M} = (W, w_0, R)$ and $\mathcal{M}' = (W', w'_0, R')$ be two V-models. A *weak bisimulation relation* between $\mathcal{M}$ and $\mathcal{M}'$ is a relation $S \subseteq W \times W'$ that contains (w_0, w'_0) and satisfies

(weak-zig) for any $a \in V \cup \{\epsilon\}$, $w, v \in W$, $w' \in W'$ such that $(w, w') \in S$:
if $(w, v) \in \hat{R}_a$, then there is a $v' \in W'$ such that $(w', v') \in \hat{R'}_a$ and $(v, v') \in S$;

(weak-zag) for any $a \in V \cup \{\epsilon\}$, $w \in W$, $w', v' \in W'$ such that $(w, w') \in S$:
if $(w', v') \in \hat{R'}_a$, then there is a $v \in W$ such that $(w, v) \in \hat{R}_a$ and $(v, v') \in S$.

Two V-models $\mathcal{M}, \mathcal{M}' \in \mathrm{Mod}^{\mathrm{HM}}(A)$ are *weakly bisimulation equivalent*, denoted by $\mathcal{M} \equiv^{\mathrm{HM}}_{V} \mathcal{M}'$, if there exists a weak bisimulation relation between $\mathcal{M}$ and $\mathcal{M}'$. It is well known that weak bisimulation equivalence is indeed an equivalence relation on the class of V-models. Moreover, if $\mathcal{M} \equiv^{\mathcal{D}^{\downarrow}}_{A} \mathcal{M}'$, then there exists a greatest weak bisimulation relation between $\mathcal{M}$ and $\mathcal{M}'$, which we denote by $\approx^{\mathcal{M}'}_{\mathcal{M}}$.

Behavioural satisfaction relation. For behavioural satisfaction of V-sentences we use the satisfaction relation defined for observable modal logic in [24] which abstracts from invisble τ-transitions. For this purpose we use again the relations $\hat{R}_a$ (with $a \in V \cup \{\epsilon\}$) defined above. For any $\mathcal{M} = (W, w_0, R) \in \mathrm{Mod}^{\mathrm{HM}}(V)$, state $w \in W$ and $a \in V \cup \{\epsilon\}$,

- $\mathcal{M}, w \models^{\mathrm{HM}}_{\mathrm{beh}, V} \langle a\rangle\varphi$ iff there is a $v \in W$ with $(w, v) \in \hat{R}_a$ and $\mathcal{M}, v \models^{\mathrm{HM}}_{\mathrm{beh}, V} \varphi$;
- $\mathcal{M}, w \models^{\mathrm{HM}}_{V} [a]\varphi$ iff for any $v \in W$ with $(w, v) \in \hat{R}_a$ it holds $\mathcal{M}, v \models^{\mathrm{HM}}_{V} \varphi$.

Behavioural satisfaction for the other cases $\mathbf{tt}, \mathbf{ff}, \varphi \wedge \varphi'$ and $\varphi \vee \varphi'$ is defined as expected. $\mathcal{M}$ *satisfies behaviourally* a V-sentence φ, denoted by $\mathcal{M} \models^{\mathrm{HM}}_{\mathrm{beh}, V} \varphi$, iff $\mathcal{M}, w_0 \models^{\mathrm{HM}}_{\mathrm{beh}, V} \varphi$.

To prove condition (1) of a behaviour-abstractor framework in Def. 1 in the context of Hennessy-Milner logic with weak bisimulation equivalence and behavioural satisfaction, we need the following lemma. The validity of the lemma is stated in [24], Sect. 3.5, Prop. 3. The converse direction of (1) is also shown in [24], Prop. 4, under the assumption of observationally image-finite processes.

Lemma 8. *For any $A \in \mathrm{Sign}^{\mathrm{HM}}$ and for all $\mathcal{M}, \mathcal{M}' \in \mathrm{Mod}^{\mathrm{HM}}(V)$,*

(1) $\mathcal{M} \equiv^{\mathrm{HM}}_{V} \mathcal{M}' \Rightarrow (\mathcal{M} \models^{\mathrm{HM}}_{\mathrm{beh}, V} \varphi$ iff $\mathcal{M}' \models^{\mathrm{HM}}_{\mathrm{beh}, V} \varphi$ for all $\varphi \in \mathrm{Sen}^{\mathrm{HM}}(V))$.

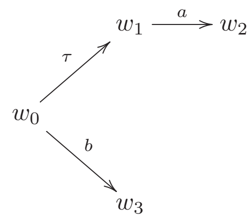


Figure 1: Counterexample: V-model $\mathcal{M}$

Black box function. To define a black box view of a V-model $\mathcal{M}$ we must construct $\mathcal{BB}_V^{\mathrm{HM}}(\mathcal{M})$ such that:

(2) $\mathcal{M} \equiv_V^{\mathrm{HM}} \mathcal{BB}_V^{\mathrm{HM}}(\mathcal{M})$.

(3) $\mathcal{BB}_V^{\mathrm{HM}}(\mathcal{M}) \models_{\mathrm{beh},V}^{\mathrm{HM}} \varphi$ iff $\mathcal{BB}_V^{\mathrm{HM}}(\mathcal{M}) \models_V^{\mathrm{HM}} \varphi$ for all $\varphi \in \mathrm{Sen}^{\mathrm{HM}}(V)$.

Interestingly, such a model does, in general, *not* exist. For the proof, we use the counterexample represented by the V-model $\mathcal{M}$ in Fig. 1 with initial state w_0.

Let us assume that there exists a V-model $\mathcal{N}$ such that (2) $\mathcal{M} \equiv_V^{\mathrm{HM}} \mathcal{N}$ and (3) $\mathcal{N} \models_{\mathrm{beh},V}^{\mathrm{HM}} \varphi$ iff $\mathcal{N} \models_V^{\mathrm{HM}} \varphi$ for all $\varphi \in \mathrm{Sen}^{\mathrm{HM}}(V)$. Let φ be the V-sentence $\langle a\rangle\mathbf{tt} \wedge \langle b\rangle\mathbf{tt}$. Obviously, $\mathcal{M} \models_{\mathrm{beh},V}^{\mathrm{HM}} \langle a\rangle\mathbf{tt} \wedge \langle b\rangle\mathbf{tt}$. If (2) holds, then we obtain by (1): $\mathcal{N} \models_{\mathrm{beh},V}^{\mathrm{HM}} \langle a\rangle\mathbf{tt} \wedge \langle b\rangle\mathbf{tt}$. If (3) holds we get $\mathcal{N} \models_V^{\mathrm{HM}} \langle a\rangle\mathbf{tt} \wedge \langle b\rangle\mathbf{tt}$. Hence the initial state of $\mathcal{N}$, say v_0, must have a choice between (at least) two transitions, one labeled with a and the other one labelled with b. But then one can easily check that there is no weak bisimulation between $\mathcal{M}$ and $\mathcal{N}$ containing (w_0, v_0). Thus we get a contradiction to the assumption (2).

As a consequence we cannot construct an appropriate black box view for *all* models $\mathcal{M} \in \mathrm{Mod}^{\mathrm{HM}}(V)$. This leads us to the idea to restrict the class of V-models in an appropriate way. To do so, we consider weakly deterministic V-models as defined in [10], and similarly under the notion of (weak) determinacy in [15]. For the definition we need some auxiliary notions: Let $\mathcal{M} = (W, w_0, R) \in \mathrm{Mod}^{\mathrm{HM}}(V)$. A state $w \in W$ is *observably reachable* in $\mathcal{M}$ if either $(w_0, w) \in \hat{R}_\epsilon$ or there exists a non-empty sequence $a_1 \dots a_n \in V^*$ of visible actions and a finite sequence of transitions $(w_{k-1}, w_k) \in \hat{R}_{a_k}, 1 \leq k \leq n$, such that $w_n = w$. An *observable trace* of $\mathcal{M}$ is a finite, possibly empty, sequence $\lambda \in V^*$ such that there is some $w \in W$ which is observably reachable by λ. Let $\approx_\mathcal{M}$ denote the greatest weak bisimulation relation $\approx_\mathcal{M}^\mathcal{M}$ between $\mathcal{M}$ and $\mathcal{M}$. $\mathcal{M}$ is called *weakly deterministic* if for all states $w, w' \in W$ which are reachable by the same observable trace λ it holds: $w \approx_\mathcal{M} w'$.

In [10], Prop. A.1, we have proved that for any weakly deterministic V-model $\mathcal{M}$ there exist a minimal V-model $\mathcal{N}$ without τ-transitions, which is weakly bisimilar to $\mathcal{M}$ and hence $\mathcal{M} \equiv_V^{\mathrm{HM}} \mathcal{N}$. Therefore, we restrict the class of V-models to weakly deterministic V-models and denote this class by $\mathrm{Mod}_{wd}^{\mathrm{HM}}(V)$. For each $\mathcal{M} \in \mathrm{Mod}_{wd}^{\mathrm{HM}}(V)$ we define the black box view of $\mathcal{M}$ by using the construction of [10] which works as follows:

First, we define an equivalence relation $\approx_{tr}$ on the observable traces of $\mathcal{M}$ such that, for observable traces $\lambda_1, \lambda_2 \in V^*, \lambda_1 \approx_{tr} \lambda_2$ iff for all states $w \in W$ reachable by λ_1 and for all states $w' \in W$ reachable by λ_2 it holds: $w \approx_\mathcal{M} w'$. For each observable trace λ, $[\lambda]_{\approx_{tr}}$ denotes the equivalence class of λ w.r.t. $\approx_{tr}$. Then, for $\mathcal{M} \in \mathrm{Mod}_{wd}^{\mathrm{HM}}(V)$, we define $\mathcal{BB}_V^{\mathrm{HM}}(\mathcal{M}) =_{\mathrm{def}} (W_B, w_{0,B}, R_B)$ with

- $W_B = \{[\lambda]_{\approx_{tr}} \mid \lambda \in V^*$ is an observable trace of $\mathcal{M}\}$,
- $w_{0,B} = [\epsilon]_{\approx_{tr}}$,
- $(R_B)_\tau = \emptyset$, and for $a \in V$, $(R_B)_a = \{([\lambda]_{\approx_{tr}}, [\lambda']_{\approx_{tr}}) \mid \lambda a \in [\lambda']_{\approx_{tr}}\}$.

Since $\mathcal{M}$ is weakly deterministic everything is well-defined, and according to [10], Prop. A.1, we get (2) $\mathcal{M} \equiv_V^{\mathrm{HM}} \mathcal{BB}_V^{\mathrm{HM}}(\mathcal{M})$. Since $\mathcal{BB}_V^{\mathrm{HM}}(\mathcal{M})$ has no τ-transitions, behavioural satisfaction coincides with standard satisfaction of V-sentences and thus also condition (3) of Def. 1 is satisfied. Moreover, (1) holds by Lemma 8. Thus the following theorem holds:

Theorem 9. $\mathrm{BA}^{\mathrm{HM}} = (\mathrm{Sign}^{\mathrm{HM}}, \mathrm{Sen}^{\mathrm{HM}}, \mathrm{Mod}_{wd}^{\mathrm{HM}}, \models^{\mathrm{HM}}, \equiv^{\mathrm{HM}}, \models_{\mathrm{beh}}^{\mathrm{HM}}, \mathcal{BB}^{\mathrm{HM}})$ *is a behaviour-abstractor framework, where* $\mathrm{Sen}^{\mathrm{HM}} = (\mathrm{Sen}^{\mathrm{HM}}(V))_{V \in \mathrm{Sign}^{\mathrm{HM}}}$ *is the family of sets* $\mathrm{Sen}^{\mathrm{HM}}(V)$ *of* V*-sentences,* $\mathrm{Mod}_{wd}^{\mathrm{HM}} = (\mathrm{Mod}_{wd}^{\mathrm{HM}}(V))_{V \in \mathrm{Sign}^{\mathrm{HM}}}$ *is the family of classes* $\mathrm{Mod}_{wd}^{\mathrm{HM}}(V)$ *of weakly deterministic* V*-models, and similarly for the other components of* $\mathrm{BA}^{\mathrm{HM}}$.

As a consequence of Thm. 9 we can instantiate Thm. 1 and get the respective relationships between behavioural and abstractor specifications in the context of Hennessy-Milner logic with weakly deterministic models.

7. Concluding Remarks

In this paper we have proposed a new behaviour-abstractor framework with a few characteristic principles for expressing the semantic relationships between abstractor and behavioural specifications. The key idea is that for each model of a specification an observationally equivalent black box model must exist for which behavioural satisfaction of sentences coincides with standard satisfaction. In contrast to the original approach in [2] and the general approach of Misiak [16], the behaviour-abstractor framework is neither based on partial (observational) congruences nor on standard/categorical quotient constructions but requires (only) the existence of black box models.

In the second part of the paper we have recovered the main currently known behaviour/abstractor relationships for specific logical frameworks: first-order logic, higher-order logic, and dynamic logic with binders are all instances of the behaviour-abstractor framework. Moreover, as a new result we have shown that (observational) Hennessy-Milner logic is also an instance of the behaviour-abstractor framework, subject to the condition that only weakly deterministic models are considered. The unrestricted Hennessy-Milner setting provides a counterexample. As the example in Section 6 shows, a black box model satisfying conditions (2) and (3) of a behaviour-abstractor framework does, in general, not exist and thus the unrestricted Hennessy-Milner setting is not a behaviour-abstractor framework.

This work covers the case of flat specifications. Future work could consider an extension to structured specifications, either following the approach in [2] or using structured behavioural specifications as in [16].

References

[1] Michel Bidoit and Rolf Hennicker. Constructor-based observational logic. *J. Log. Algebr. Program.*, 67(1-2):3–51, 2006.

[2] Michel Bidoit, Rolf Hennicker, and Martin Wirsing. Behavioural and abstractor specifications. *Sci. Comput. Program.*, 25(2–3):149–186, 1995.

[3] Torben Bräuner. *Hybrid Logic and its Proof–Theory.* App. Logic Series. Springer, 2010.

[4] Joseph A. Goguen and Rod M. Burstall. Institutions: Abstract model theory for specification and programming. *J. ACM*, 39(1):95–146, 1992.

[5] Joseph A. Goguen and Grigore Rosu. Hiding more of hidden algebra. In *World Congress on Formal Methods*, volume 1709 of *Lecture Notes in Computer Science*, pages 1704–1719. Springer, 1999.

[6] David Harel, Dexter Kozen, and Jerzy Tiuryn. *Dynamic Logic.* MIT Press, 2000.

[7] M. Hennessy and R. Milner. Algebraic laws for nondeterminism and concurrency. *Journal of the Association of Computer Machinery*, 32:137–162, 1985.

[8] Rolf Hennicker. Context induction: A proof principle for behavioural abstractions and algebraic implementations. *Formal Asp. Comput.*, 3(4):326–345, 1991.

[9] Rolf Hennicker. *Structured Specifications with Behavioural Operators: Semantics, Proof Methods and Applications.* Habilitation thesis. LMU Munich, 1997.

[10] Rolf Hennicker, Stephan Janisch, and Alexander Knapp. On the observable behaviour of composite components. *Electr. Notes Theor. Comput. Sci.*, 260:125–153, 2010.

[11] Rolf Hennicker and Alexandre Madeira. Institutions for behavioural dynamic logic with binders. In *ICTAC 2017*, volume 10580 of *Lecture Notes in Computer Science*, pages 13–31. Springer, 2017.

[12] Rolf Hennicker and Alexandre Madeira. Observational semantics for dynamic logic with binders. In *Recent Trends in Algebraic Development Techniques, 23rd IFIP WG 1.3 International Workshop, WADT 2016, Revised Selected Papers*, volume 10644 of *Lecture Notes in Computer Science*, pages 135–152. Springer, 2017.

[13] Martin Hofmann and Donald Sannella. On behavioural abstraction and behavioural satisfaction in higher-order logic. *Theor. Comput. Sci.*, 167(1&2):3–45, 1996.

[14] Alexandre Madeira, Luís Soares Barbosa, Rolf Hennicker, and Manuel A. Martins. Dynamic logic with binders and its application to the development of reactive systems. In Augusto Sampaio and Farn Wang, editors, *Theoretical Aspects of Computing - ICTAC 2016*, volume 9965 of *Lecture Notes in Computer Science*, pages 422–440, 2016.

[15] Robin Milner. *Communication and Concurrency*. Prentice Hall, 1989.

[16] Michal Misiak. Behavioural semantics of algebraic specifications in arbitrary logical systems. In *Recent Trends in Algebraic Development Techniques, 17th International Workshop, WADT 2004, Revised Selected Papers*, volume 3423 of *Lecture Notes in Computer Science*, pages 144–161. Springer, 2004.

[17] P. Nivela and F. Orejas. Initial behaviour semantics for algebraic specifications. In D.T. Sannella and A. Tarlecki, editors, *Recent Trends in Data Type Specification, 5th Wsh. on Specification of Abstract Data Types WADT 1987*, volume 332 of *Lecture Notes in Computer Science*, pages 184–207. Springer, 1988.

[18] Horst Reichel. Behavioural equivalence – a unifying concept for initial and final specifications. In M. Arato and L. Varga, editors, *Proc. of the Third Hungarian Computer Science Conference*, pages 27–39. Akademiai Kiado, 1981.

[19] Horst Reichel. Behavioural validity of conditional equations in abstract data types. In *Proc. of the Vienna Conference on Contributions to General Algebra 3*, pages 301–324. Verlag B.G. Teubner, 1985.

[20] Donald Sannella and Andrzej Tarlecki. On observational equivalence and algebraic specification. *J. Comput. Syst. Sci.*, 34(2-3):150–178, June 1987.

[21] Donald Sannella and Andrzej Tarlecki. *Foundations of Algebraic Specification and Formal Software Development*. Monographs on TCS, an EATCS Series. Springer, 2012.

[22] Donald Sannella and Martin Wirsing. Implementation of parameterised specifications (extended abstract). In Mogens Nielsen and Erik Meineche Schmidt, editors, *Automata, Languages and Programming, 9th Colloquium, Aarhus, Denmark, July 12-16, 1982, Proceedings*, volume 140 of *Lecture Notes in Computer Science*, pages 473–488. Springer, 1982.

[23] Donald Sannella and Martin Wirsing. A kernel language for algebraic specifications and implementations. In *Colloq. on Foundations of Computation Theory*, volume 158 of *Lecture Notes in Computer Science*, pages 413–427. Springer, 1983.

[24] Colin Stirling. *Modal and Temporal Properties of Processes*. Springer Science Business Media New York, 2001.