Observational Semantics for Dynamic Logic with Binders

Rolf Hennicker, Alexandre Madeira

Observational Semantics for Dynamic Logic with Binders

Rolf Hennicker[1] and Alexandre Madeira[2,3]*

[1] Ludwig-Maximilians-Universität München, Germany
[2] HASLab INESC TEC & Univ. Minho, Portugal
[3] CIDMA - Dep. Mathematics, Univ. Aveiro, Portugal

Abstract. The dynamic logic with binders $\mathcal{D}^{\downarrow}$ was recently introduced as a suitable formalism to support a rigorous stepwise development method for reactive software. The commitment of this logic concerning bisimulation equivalence is, however, not satisfactory: the model class semantics of specifications in $\mathcal{D}^{\downarrow}$ is not closed under bisimulation equivalence; there are $\mathcal{D}^{\downarrow}$-sentences that distinguish bisimulation equivalent models, i.e., $\mathcal{D}^{\downarrow}$ does not enjoy the modal invariance property. This paper improves on these limitations by providing an observational semantics for dynamic logic with binders. This involves the definition of a new model category and of a more relaxed satisfaction relation. We show that the new logic $\mathcal{D}^{\downarrow}_{\sim}$ enjoys modal invariance and even the Hennessy-Milner property. Moreover, the new model category provides a categorical characterisation of bisimulation equivalence by observational isomorphism. Finally, we consider abstractor semantics obtained by closing the model class of a specification SP in $\mathcal{D}^{\downarrow}$ under bisimulation equivalence. We show that, under mild conditions, abstractor semantics of SP in $\mathcal{D}^{\downarrow}$ is the same as observational semantics of SP in $\mathcal{D}^{\downarrow}_{\sim}$.

1 Introduction

The study of logics and formal methods for rigorous development of reactive systems, i.e. systems which interact with their environment during the computation [1], is an active topic of research. Dynamic logic with binders, called $\mathcal{D}^{\downarrow}$-logic, has been introduced in [7] as a logical framework which allows to express properties of reactive systems, from abstract safety and liveness requirements down to concrete specifications of the (recursive) structure of executable processes. $\mathcal{D}^{\downarrow}$-logic combines in the same formalism modalities indexed by regular expressions of actions, as in Dynamic Logic [6], with binders of Hybrid Logic [4], which bind state variables to particular states and thus allow us to specify concrete processes. We have shown in [7] how the whole development process of reactive systems can be supported by stepwise refinement of $\mathcal{D}^{\downarrow}$-specifications whose models are labelled transition systems with initial state.

* This work is financed by the ERDF European Regional Development Fund through the Operational Programme for Competitiveness and Internationalisation - COMPETE 2020 by National Funds through the Portuguese funding agency, FCT - Fundação para a Ciência e a Tecnologia, within projects POCI-01-0145-FEDER-016692 and UID/MAT/04106/2013 and also with its Operational Programme NORTE 2020, trough the project NORTE-01-0145-FEDER-000037. The second author is also supported by the individual grant SFRH/BPD/103004/2014.

However, the satisfaction relation used in $\mathcal{D}^{\downarrow}$ and its notion of isomorphism, the categorical formalisation of identity among objects, are too strict to allow proper behavioural abstraction. As it is well known, bisimulation equivalence is usually adopted to identify behaviourally equivalent systems. However, this is not reflected in the model category of $\mathcal{D}^{\downarrow}$ where model classes are closed under isomorphism but, in general, not under bisimulation equivalence. Thus $\mathcal{D}^{\downarrow}$-logic does not enjoy the *modal invariance property* which requires that bisimilar models satisfy exactly the same logical sentences.

To find a solution, we draw an analogy to algebraic specifications of data types: Equational and first-order logic specifications do generally not support abstraction w.r.t. behaviourally equivalent data structures. This fact led to a significant number of studies proposing different solutions; see Chap. 8 in [10] for a summary. One idea, originally proposed by Reichel in [9], was to relax the satisfaction relation of first-order logic such that equations are not necessarily interpreted by the set-theoretic equality but by observational equality of elements; see, e.g., [5, 2]. We take up this idea and propose, in Sect. 3, a new logic, called $\mathcal{D}^{\downarrow}_{\sim}$, which has the same sentences and models as $\mathcal{D}^{\downarrow}$ but more relaxed notions of satisfaction and model morphism. The idea of satisfaction in $\mathcal{D}^{\downarrow}_{\sim}$, called *observational satisfaction*, is that state variables x occurring in a formula can be interpreted by arbitrary states as long as they are bisimilar to the state to which x was bound before. This leads to *observational semantics* of a specification SP consisting of all models which observationally satisfy the axioms of SP. Model morphisms in $\mathcal{D}^{\downarrow}_{\sim}$, called *observational morphisms*, capture the idea of simulation. We show that observational satisfaction of positive sentences is preserved by observational morphisms. Moreover, we show that models which are observationally isomorphic satisfy observationally the same sentences, i.e. we get modal invariance of sentences w.r.t. satisfaction and isomorphism in $\mathcal{D}^{\downarrow}_{\sim}$.

In Sect. 4, we study relationships between isomorphism in $\mathcal{D}^{\downarrow}_{\sim}$ and bisimulation equivalence and prove that both concepts are indeed equivalent. Thus, we get (i) a categorical characterisation of bisimulation equivalence and (ii) the modal invariance property w.r.t. observational satisfaction and bisimulation equivalence, which solves our problem discussed above. But the new logic $\mathcal{D}^{\downarrow}_{\sim}$ allows us to go even a step further: We prove a Hennessy-Milner Theorem which shows that two image finite models satisfy in $\mathcal{D}^{\downarrow}_{\sim}$ the same sentences if and only if they are bisimilar - which in turn is equivalent to being isomorphic in $\mathcal{D}^{\downarrow}_{\sim}$.

In Sect. 5, we compare observational semantics of specifications in $\mathcal{D}^{\downarrow}_{\sim}$ with another possibility for behavioural abstraction called *abstractor semantics*. The idea of abstractor semantics goes again back to algebraic specifications where Sannella und Tarlecki have proposed to abstract from the "standard" model class of a specification by taking its closure under an appropriate equivalence relation; see [10]. For reactive system specifications this means that we consider our original $\mathcal{D}^{\downarrow}$-logic, specifications over $\mathcal{D}^{\downarrow}$ and their model classes (in terms of satisfaction in $\mathcal{D}^{\downarrow}$) but then abstract from a specification's model class by closing it under bisimulation equivalence. We investigate that observational se-

mantics and abstractor semantics of reactive system specifications can be related completely analogously as it has been done for algebraic specifications of data types in [3]. We show that both semantics coincide if and only if any model of a specification SP interpreted in $\mathcal{D}^{\downarrow}$ is also a model when SP is interpreted in $\mathcal{D}^{\downarrow}_{\sim}$.

2 $\mathcal{D}^{\downarrow}$-Logic: Background and Motivations

2.1 Overview on $\mathcal{D}^{\downarrow}$

This section reviews $\mathcal{D}^{\downarrow}$-logic introduced in [7] and proves additionally that satisfaction in $\mathcal{D}^{\downarrow}$ is preserved by isomorphism. $\mathcal{D}^{\downarrow}$-logic is designed to express properties of reactive systems, from abstract safety and liveness properties down to concrete ones specifying the (recursive) structure of processes. It thus combines modalities indexed by regular expressions of actions, as in Dynamic Logic [6], and state variables with binders, as in Hybrid Logic [4]. These motivations are reflected in its semantics. Differently from what is usual in modal logics, whose semantics is given by Kripke structures and satisfaction of formulas is evaluated globally, $\mathcal{D}^{\downarrow}$ models are reachable, labelled transition systems with initial states where satisfaction is evaluated. This reflects our focus on computations, i.e. on effective processes. In modal logic this corresponds to submodels of Kripke structures generated by a given point, which represents the initial state of computations.

Definition 1 (Models and model morphisms). *Let A be a set of atomic actions. An* A-model *is triple (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 $w \in W$, there is a finite sequence of transitions $R_{a^k}(w^{k-1}, w^k)$, $1 \leq k \leq n$, with $w^k \in W$, $a^k \in A$, such that $w^0 = w_0$ and $w^n = w$.*

Given two A-models $\mathcal{M} = (W, w_0, R)$ and $\mathcal{M}' = (W', w'_0, R')$, a model morphism *$h : \mathcal{M} \to \mathcal{M}'$ is a function $h : W \to W'$ such that $h(w_0) = w'_0$ and, for each $a \in A$, if $(w_1, w_2) \in R_a$ then $(h(w_1), h(w_2)) \in R'_a$.*

Lemma 1. *The class of A-models and A-model morphisms define a category denoted by* $\mathrm{Mod}^{\mathcal{D}^{\downarrow}}(A)$*. The identity morphisms $id_{\mathcal{M}}$ are the identity functions.*

As usual, we say that two models $\mathcal{M}, \mathcal{M}' \in \mathrm{Mod}^{\mathcal{D}^{\downarrow}}(A)$ are *isomorphic*, in symbols $\mathcal{M}$ **iso** $\mathcal{M}'$, if there is a pair of morphisms $h : \mathcal{M} \to \mathcal{M}'$ and $h^{-1} : \mathcal{M}' \to \mathcal{M}$ such that $h \cdot h^{-1} = id_{\mathcal{M}}$ and $h^{-1} \cdot h = id_{\mathcal{M}'}$.

The *set of (composed) actions*, $\mathrm{Act}(A)$, induced by a set of atomic actions A is given by

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

where $a \in A$. In the context of a finite set of atomic actions $A = \{a_1, \ldots, a_n\}$, we may briefly write A for the complex action $a_1 + \ldots + a_n$. For a set X of variables

and an A-model $\mathcal{M} = (W, w_0, R)$, 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 $y \in X, y \neq x$.

Definition 2 (Formulas and sentences). *The set of* A-formulas *is given by*

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

where $x \in X$ *and* $\alpha \in \mathrm{Act}(A)$. *An* A*-formula* φ *is called* A-sentence *if* φ *contains no free variables. Free variables are defined as usual with* $\downarrow$*, the only operator binding variables.*

The binder operator $\downarrow x.\varphi$ assigns to variable x the current state of evaluation and evaluates φ. The operator $@_x\varphi$ evaluates φ in the state assigned to x. To define the satisfaction relation formally we need to clarify how composed actions are interpreted in models. Let $\alpha \in \mathrm{Act}(A)$ and $\mathcal{M} \in \mathrm{Mod}^{\mathcal{D}^{\downarrow}}(A)$. 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. Given an A-model $\mathcal{M} = (W, w_0, R)$, $w \in W$ and $g : X \to W$,

- $\mathcal{M}, g, w \models \mathbf{tt}$ is true; $\mathcal{M}, s \models \mathbf{ff}$ is false;
- $\mathcal{M}, g, w \models x$ iff $g(x) = w$;
- $\mathcal{M}, g, w \models \downarrow x.\varphi$ iff $\mathcal{M}, g[x \mapsto w], w \models \varphi$;
- $\mathcal{M}, g, w \models @_x\varphi$ iff $\mathcal{M}, g, g(x) \models \varphi$;
- $\mathcal{M}, g, w \models \langle\alpha\rangle\varphi$ iff there is a $v \in W$ with $(w, v) \in R_\alpha$ and $\mathcal{M}, g, v \models \varphi$;
- $\mathcal{M}, g, w \models [\alpha]\varphi$ iff for any $v \in W$ with $(w, v) \in R_\alpha$ it holds $\mathcal{M}, g, v \models \varphi$;
- $\mathcal{M}, g, w \models \neg\varphi$ iff it is false that $\mathcal{M}, g, w \models \varphi$;
- $\mathcal{M}, g, w \models \varphi \wedge \varphi'$ iff $\mathcal{M}, g, w \models \varphi$ and $\mathcal{M}, g, w \models \varphi'$;
- $\mathcal{M}, g, w \models \varphi \vee \varphi'$ iff $\mathcal{M}, g, w \models \varphi$ or $\mathcal{M}, g, w \models \varphi'$.

We write $\mathcal{M}, w \models \varphi$ if, for any valuation $g : X \to W$, we have $\mathcal{M}, g, w \models \varphi$. If φ is an A-sentence, then the valuation is irrelevant, i.e., $\mathcal{M}, g, w \models \varphi$ iff $\mathcal{M}, w \models \varphi$. $\mathcal{M}$ *satisfies* an A-sentence φ, written $\mathcal{M} \models \varphi$, if $\mathcal{M}, w_0 \models \varphi$.

Hence, $\mathcal{D}^{\downarrow}$-logic expresses properties of states reachable from the initial one. For instance, if A is finite, $\mathcal{D}^{\downarrow}$ is able to express liveness requirements such as "*after the occurrence of an action* a*, an action* b *can be eventually realised*" with $[A^*; a]\langle A^*; b\rangle\mathbf{tt}$, safety properties by sentences of the form $[A^*]\varphi$, in particular, deadlock freeness by $[A^*]\langle A\rangle\mathbf{tt}$. $\mathcal{D}^{\downarrow}$-logic is also suited to express process structures and, thus, the implementation of abstract requirements. The binder operator is crucial for this. The ability to give names to visited states together with the modal features allows to express recursive process patterns. For instance, the following sentence captures processes with two states and alternating a and b transitions.

$$\downarrow x_0.\big(\langle a\rangle \downarrow x_1.(\langle b\rangle x_0)\big)$$

Definition 3 (Specification). *A* specification *SP is a pair* $SP = (A, \Phi)$ *where* A *is a set of atomic actions and* Φ *is a set of* A*-sentences.*

Definition 4 (Semantics). *The* semantics *of a specification* $SP = (A, \Phi)$ *in* $\mathcal{D}^{\downarrow}$ *is given by the class of models*

$$Mod(SP) = \{\mathcal{M} \in \mathrm{Mod}^{\mathcal{D}^{\downarrow}}(A) \mid \mathcal{M} \models \varphi \text{ for all } \varphi \in \Phi\}.$$

Lemma 2. *Let* $\mathcal{M} = (W, w_0, R)$ *and* $\mathcal{M}' = (W', w_0', R')$ *be two* A*-models and* $h : \mathcal{M} \to \mathcal{M}'$ *an isomorphism. Then for any* $w \in W$*, valuation* $g : X \to W$ *and* A*-formula* φ*, we have*

$$\mathcal{M}, g, w \models \varphi \text{ iff } \mathcal{M}', g \circ h, h(w) \models \varphi.$$

Proof. The proof is performed by induction on the structure of A-formulas. The base cases $\varphi = \mathbf{tt}$ and $\varphi = \mathbf{ff}$ are trivial.
Case $\varphi = x$:

$$\begin{array}{l|l} \mathcal{M}, g, w \models x & h(g(x)) = h(w) \\ \Leftrightarrow \quad \{\models \text{defn}\} & \Leftrightarrow \quad \{\circ \text{ composition}\} \\ g(x) = w & (g \cdot h)(x) = h(w) \\ \Leftrightarrow \quad \{h \text{ injective}\} & \Leftrightarrow \quad \{\models \text{defn}\} \\ & \mathcal{M}', g \circ h, h(w) \models x \end{array}$$

Case $\varphi = \downarrow x.\, \phi$:

$$\begin{array}{l|l} \mathcal{M}, g, w \models \downarrow x.\phi & \mathcal{M}', g[x \mapsto w] \circ h, h(w) \models \phi \\ \Leftrightarrow \quad \{\models \text{defn}\} & \Leftrightarrow \quad \{\text{since } g[x \mapsto w] \circ h = (g \circ h)[x \mapsto h(w)]\} \\ \mathcal{M}, g[x \mapsto w], w \models \phi & \mathcal{M}', (g \circ h)[x \mapsto h(w)], h(w) \models \phi \\ \Leftrightarrow \quad \{\text{ I.H. }\} & \Leftrightarrow \quad \{\models \text{defn}\} \\ & \mathcal{M}', g \circ h, h(w) \models \downarrow x.\phi \end{array}$$

Case $\varphi = \langle\alpha\rangle\phi$:

$$\begin{array}{l|l} \mathcal{M}, g, w \models \langle\alpha\rangle\phi & \\ \Leftrightarrow \quad \{\models \text{defn}\} & \\ \mathcal{M}, g, v \models \phi \text{ for some } v \in W, (w, v) \in R_\alpha & \Leftrightarrow \quad \{\models \text{defn} + h \text{ surjective}\} \\ \Leftrightarrow \quad \{\text{I.H.} + h \text{ iso} + \star\} & \end{array} \begin{array}{l} \mathcal{M}', g \circ h, h(v) \models \phi \\ \text{for some } v \in W, (h(w), h(v)) \in R'_\alpha \\ \\ \mathcal{M}', g \circ h, h(w) \models \langle\alpha\rangle\phi \end{array}$$

$\star$: We use the fact, that morphisms also satisfy $(w_1, w_2) \in R_\alpha$ then $(h(w_1), h(w_2)) \in R'_\alpha$ for composed actions $\alpha \in \mathrm{Act}(A)$.
The proof for the remaining cases is straightforward. □

Theorem 1. *Let* $\mathcal{M}$ *and* $\mathcal{M}'$ *be* A*-models such that* $\mathcal{M}$ **iso** $\mathcal{M}'$*. Then, for any* A*-sentence* φ*, we have*

$$\mathcal{M} \models \varphi \text{ iff } \mathcal{M}' \models \varphi.$$

Proof. Since φ has no free variables, it follows from Lemma 2, that for any $w \in W$, we have $\mathcal{M}, w \models \varphi$ iff $\mathcal{M}', h(w) \models \varphi$ where h is an isomorphism between $\mathcal{M}$ and $\mathcal{M}'$. In particular, since $h(w_0) = w_0'$, we have $\mathcal{M}, w_0 \models \varphi$ iff $\mathcal{M}', w_0' \models \varphi$, i.e., $\mathcal{M} \models \varphi$ iff $\mathcal{M}' \models \varphi$. □

Corollary 1. *For any specification SP, Mod(SP) is closed under* **iso** .

2.2 Motivations

Let us recall the well-known notion of bisimulation between transition systems:

Definition 5 (Bisimulation). *Let $\mathcal{M} = (W, w_0, R)$ and $\mathcal{M}' = (W', w_0', R')$ be two A-models. A* bisimulation *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 $\mathcal{M}$ and $\mathcal{M}'$ are called *bisimulation equivalent*, denoted by $\mathcal{M} \equiv \mathcal{M}'$, if there exists a bisimulation 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 $\mathcal{M} \equiv \mathcal{M}'$, then there exists a greatest bisimulation between $\mathcal{M}$ and $\mathcal{M}'$, which we denote by $\sim_{\mathcal{M}'}^{\mathcal{M}}$.

Bisimulation equivalence plays a central role in the analysis and development of reactive systems. It can be taken as the standard behavioural equivalence between processes in the sense that, given two bisimulation equivalent processes, it should be irrelevant for the correctness of an implementation which one is chosen to realise a given system specification. The notion of bisimulation equivalence plays also an important role in the theory of modal logics: the satisfaction in most of modal logics is invariant w.r.t. bisimulation equivalence, i.e. bismulation equivalent models satisfy the same sentences. However, this is not the case for the logic $\mathcal{D}^{\downarrow}$. In order to see that, let us consider the two $\{a\}$-models $\mathcal{M}$ and $\mathcal{M}'$ presented in Fig. 1 and the specification $SP = (\{a\}, \{\downarrow x.\langle a \rangle x\})$. It is easy to see that $\mathcal{M} \in Mod(SP)$ and $\mathcal{M}' \notin Mod(SP)$. However, $\mathcal{M} \equiv \mathcal{M}'$ which shows that $\mathcal{D}^{\downarrow}$ does not obey the implementation principle from above. From the logic, point of view it illustrates that $\mathcal{D}^{\downarrow}$ does not enjoy of the modal invariance property.

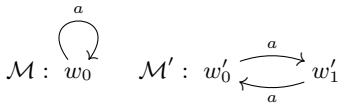


Fig. 1. Bisimilar models

3 $\mathcal{D}^{\downarrow}_{\sim}$-Logic

In this section we introduce a new logic, called $\mathcal{D}^{\downarrow}_{\sim}$, which generalises $\mathcal{D}^{\downarrow}$-logic by supporting abstraction w.r.t. observationally indistinguishable states. The formulas and sentences of $\mathcal{D}^{\downarrow}_{\sim}$ are the same as in $\mathcal{D}^{\downarrow}$. The essential difference lies in the definition of model morphisms and in a relaxation of the satisfaction relation which is adjusted to the observational paradigm. As a central result we will show that in the new category $\mathcal{D}^{\downarrow}_{\sim}$ observationally isomorphic models satisfy observationally the same sentences; i.e. we get modal invariance w.r.t. observational isomorphism and the relaxed (observational) satisfaction relation.

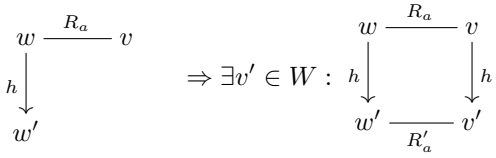
3.1 Observational Models Category

We introduce a new category of models for a set A of atomic actions. The objects of this category are, as in $\mathcal{D}^{\downarrow}$, reachable (labelled) transition systems with initial states. However, we introduce a new kind of model morphism, called observational morphism. Such morphisms are not functions but relations which abstract away the difference between states with an observationally equal behaviour. For this purpose, we consider for any A-model $\mathcal{M} = (W, w_0, R)$ the *observational equality* relation $\sim_{\mathcal{M}} \subseteq W \times W$, which is defined as the greatest bisimulation $\sim^{\mathcal{M}}_{\mathcal{M}}$ between $\mathcal{M}$ and $\mathcal{M}$[4]. Then an observational morphism $h : \mathcal{M} \to \mathcal{M}'$ is a relation between the state spaces of two A-models $\mathcal{M}$ and $\mathcal{M}'$ containing their initial states which has the following properties: (1) h is a simulation relation such that any transition in $\mathcal{M}$ is simulated by a transition in $\mathcal{M}'$ with the same label (i.e. observational morphisms satisfy the "zig" condition of a bisimulation), (2) h preserves observational equality of states from $\mathcal{M}$ to $\mathcal{M}'$ and (3) h is closed under the observational equalities $\sim_{\mathcal{M}}$ and $\sim'_{\mathcal{M}}$ of $\mathcal{M}$ and $\mathcal{M}'$ resp. These properties are expressed by the three conditions in the subsequent definition. We note that observational morphisms could be equivalently defined by morphisms between the quotient structures of $\mathcal{M}$ and $\mathcal{M}'$ considered later on in Def. 10. We prefer, however, to give a direct definition on the state spaces of $\mathcal{M}$ and $\mathcal{M}'$ since those models are actually the representations of concrete implementations and not their quotient structures.

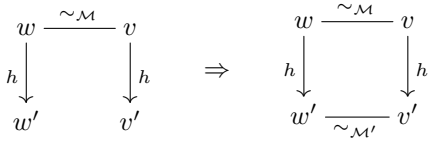
Definition 6 (Observational morphisms). *Let $\mathcal{M} = (W, w_0, R)$ and $\mathcal{M}' = (W', w'_0, R')$ be two A-models. An* observational morphism $h : \mathcal{M} \to \mathcal{M}'$ *is a relation $h \subseteq W \times W'$ containing (w_0, w'_0) such that the following conditions are satisfied:*

[4] It exists since bisimulation equivalence is reflexive and it is an equivalence relation on the states of $\mathcal{M}$.

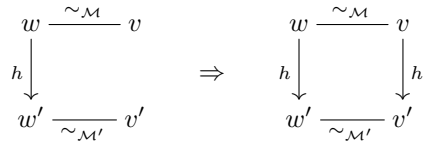
1. *For any $a \in A$, $w, v \in W, w' \in W'$ such that $(w, w') \in h$:*
   if $(w, v) \in R_a$, then there is a $v' \in W'$ such that $(w', v') \in R'_a$ and $(v, v') \in h$.



2. *For any $w, v \in W, w', v' \in W'$ such that $(w, w') \in h$ and $(v, v') \in h$:*
   if $w \sim_{\mathcal{M}} v$, then $w' \sim_{\mathcal{M}'} v'$.



3. *For any $w, v \in W, w', v' \in W'$ such that $(w, w') \in h$:*
   if $w \sim_{\mathcal{M}} v$ and $w' \sim_{\mathcal{M}} v'$, then $(v, v') \in h$.



By the definition of composed actions and their interpretation as relations the simulation condition 1 of Def. 6 can be lifted to composed actions:

Remark 1. Condition 1 of Def. 6 implies that for any $\alpha \in \mathrm{Act}(A)$ and any $w, v \in W, w' \in W'$ such that $(w, w') \in h$:
if $(w, v) \in R_\alpha$, then there is a $v' \in W'$ such that $(w', v') \in R'_\alpha$ and $(v, v') \in h$.

Lemma 3. *Observational morphisms are total relations.*

Proof. This is a direct consequence of the reachability of states. On the one hand, we have $(w_0, w'_0) \in h$. The induction step corresponds to 1 of Def. 6. □

Theorem 2. *The class of A-models together with observational morphisms form a category, denoted by $\mathrm{Mod}^{\mathcal{D}^{\downarrow}_{\sim}}(A)$. For each $\mathcal{M} \in \mathrm{Mod}^{\mathcal{D}^{\downarrow}_{\sim}}(A)$, the identity morphism $1_{\mathcal{M}}$ is the observational equality $\sim_{\mathcal{M}}$.*

Proof. Observational morphisms are closed under composition of relations: Given two observational morphisms $h : \mathcal{M} \to \mathcal{M}'$ and $h' : \mathcal{M}' \to \mathcal{M}''$, their composition $h \cdot h' : \mathcal{M} \to \mathcal{M}''$ is the relation $\{(w, w'')|$ there exists w' s.t. $(w, w') \in h$ and $(w', w'') \in h'\}$. It is straightforward to show, by standard set-theoretic reasoning, that $h \cdot h'$ satisfies the conditions 1 - 3 of Def. 6 since h and h' do so.

Also it is clear that relational composition is associative.

For each A-model $\mathcal{M}$, $1_{\mathcal{M}} = \sim_{\mathcal{M}}$ is an observational morphism $\mathcal{M} \to \mathcal{M}$: Since $\sim_{\mathcal{M}}$ is a bisimulation it satisfies 1 of Def. 6. Since $\sim_{\mathcal{M}}$ is the greatest bisimulation on $\mathcal{M}$ it is closed under composition and therefore, taking into account that $\sim_{\mathcal{M}}$ is an equivalence relation, it satisfies 2 and 3. Finally, because of the closure property 3 of Def. 6, it is obvious that, for any observational morphism $\mathcal{M} \xrightarrow{h} \mathcal{M}'$, we have $1_{\mathcal{M}} \cdot h = h$ and $h \cdot 1_{\mathcal{M}'} = h$.

□

For A-models $\mathcal{M}$ and $\mathcal{M}'$ we write $\mathcal{M}$ **iso**$_\sim$ $\mathcal{M}'$ whenever $\mathcal{M}$ and $\mathcal{M}'$ are observationally isomorphic in the category $\mathrm{Mod}^{\mathcal{D}^{\downarrow}_{\sim}}(A)$. The next lemma states a useful property which shows that the inverse of an observational isomorphism $h : \mathcal{M} \to \mathcal{M}'$ in the category $\mathrm{Mod}^{\mathcal{D}^{\downarrow}_{\sim}}(A)$ is just the inverse relation of h.

Lemma 4. *Let $\mathcal{M} = (W, w_0, R)$ and $\mathcal{M}' = (W', w_0', R')$ be two A-models and $h : \mathcal{M} \to \mathcal{M}'$ an observational isomorphism with inverse $h^{-1} : \mathcal{M}' \to \mathcal{M}$. Then for all $w \in W$ and $w' \in W'$ the following holds: $(w, w') \in h$ if and only if $(w', w) \in h^{-1}$.*

Proof. For the proof we use Lem. 3 and condition 3 of Def. 6. Assume $(w, w') \in h$. Since $h^{-1} : \mathcal{M}' \to \mathcal{M}$ is an observational morphism it is total, by Lem. 3. Hence, there exists $v \in W$ such that $(w', v) \in h^{-1}$. By the isomorphism property we have $h \cdot h^{-1} = 1_{\mathcal{M}}$. Since $(w, v) \in h \cdot h^{-1}$, we get $(w, v) \in 1_{\mathcal{M}}$, i.e. $w \sim_{\mathcal{M}} v$. Since $h^{-1} : \mathcal{M}' \to \mathcal{M}$ satisfies 3 of Def. 6, $(w', v) \in h^{-1}$ and $v \sim_{\mathcal{M}} w$ implies $(w', w) \in h^{-1}$. The converse direction is proved analogously by using again condition 3 of Def. 6. □

As a consequence of Lem. 4, we can show that observational isomorphisms satisfy the "zag" condition of a bisimulation.

Lemma 5. *Let $\mathcal{M} = (W, w_0, R)$ and $\mathcal{M}' = (W', w_0', R')$ be two A-models and $h : \mathcal{M} \to \mathcal{M}'$ an observational isomorphism. Then the following holds:*
For any $a \in A$, $w \in W$, $w', v' \in W'$ such that $(w, w') \in h$:
if $(w', v') \in R'_a$, then there is a $v \in W$ such that $(w, v) \in R_a$ and $(v, v') \in h$.

Proof. Assume $(w, w') \in h$ and $(w', v') \in R'_a$. Let h^{-1} be the inverse of h. Then, by Lem. 4, $(w', w) \in h^{-1}$. Since h^{-1} satisfies condition 1 of Def. 6, there is a $v \in W$ such that $(w, v) \in R_a$ and $(v', v) \in h^{-1}$. By Lem. 4, $(v, v') \in h$ and we are done. □

As an example, consider the two $\{a\}$-models $\mathcal{M}$ and $\mathcal{M}'$ in Fig. 1. The relation $h = \{(w_0, w_0'), (w_0, w_1')\}$ is an observational isomorphism between $\mathcal{M}$ and $\mathcal{M}'$. We have also seen in Sect. 2.2 that $\mathcal{M}$ and $\mathcal{M}'$ are bisimilar. In fact, we will show later, in Sect. 4, that observational isomorphism coincides with bisimulation equivalence.

3.2 Observational Satisfaction

We are now ready to generalise the satisfaction relation of $\mathcal{D}^{\downarrow}$-logic to take into account observational abstraction. We use the same formulas as in $\mathcal{D}^{\downarrow}$, which were called A-formulas for a given set A of atomic actions. But now, in the logic $\mathcal{D}^{\downarrow}_{\sim}$, the observational satisfaction of an A-formula allows to interpret variables x by states which are not identical but only observationally equal to the current valuation of x.

Definition 7 (Observational satisfaction). *Let $\mathcal{M} = (W, w_0, R)$ be an A-model, $w \in W$ and $g : X \to W$ a valuation. The* observational satisfaction *of an A-formula φ in state w of $\mathcal{M}$ w.r.t. valuation g, denoted by $\mathcal{M}, g, w \models_{\sim} \varphi$, is defined analogously to the satisfaction as shown in Sect. 2.1, with the exception of*

$$\mathcal{M}, g, w \models_{\sim} x \text{ iff } g(x) \sim_{\mathcal{M}} w.$$

For each A-sentence φ, the valuation is irrelevant and $\mathcal{M}$ satisfies observationally *φ, denoted by $\mathcal{M} \models_{\sim} \varphi$, if $\mathcal{M}, w_0 \models_{\sim} \varphi$.*

As an example, we consider the $\{a\}$-model $\mathcal{M}'$ in Fig. 1 for which we have: $\mathcal{M}' \models_{\sim} \downarrow x.\langle a \rangle x$. This is true since the a-transition reaches state w'_1 which is observationally equal to state w'_0.

Using the observational satisfaction relation we can equip specifications, as defined in Def. 3, with an observational semantics.

Definition 8 (Observational semantics). *The* observational semantics *of a specification $SP = (A, \Phi)$ is given by the class of models*

$$Mod_{\sim}(SP) = \{\mathcal{M} \in \mathrm{Mod}^{\mathcal{D}^{\downarrow}_{\sim}}(A) \mid \mathcal{M} \models_{\sim} \varphi \text{ for all } \varphi \in \Phi\}.$$

In the following we want to analyse relationships between observational satisfaction and observational morphisms. First, we show that observational satisfaction of positive A-sentences is preserved by observational morphisms; see Thm. 3. Then we show that observational satisfaction of arbitrary A-sentences is preserved and reflected in the case of observational isomorphisms; see Thm. 4.

Definition 9 (Positive formulas and sentences). *An A-formula (A-sentence) φ is a* positive A-formula (A-sentence)*, if it does not contain negation $\neg$ and the box operator $[.]$.*

Lemma 6. *Let $\mathcal{M} = (W, w_0, R)$ and $\mathcal{M}' = (W', w'_0, R')$ be two A-models and $h : \mathcal{M} \to \mathcal{M}'$ an observational morphism. Then for any $w \in W, w' \in W'$ with $(w, w') \in h$, for any valuations $g : X \to W$, $g' : X \to W'$ with $(g(x), g'(x)) \in h$ for all $x \in X$, and for any positive A-formula φ, we have*

$$\mathcal{M}, g, w \models_{\sim} \varphi \text{ implies } \mathcal{M}', g', w' \models_{\sim} \varphi.$$

Proof. The proof is performed by induction on the structure of positive A-formulas.

The base cases $\varphi = \mathbf{tt}$ and $\varphi = \mathbf{ff}$ are trivial.

Case $\varphi = x$:

$$\begin{array}{l|l} \quad \mathcal{M}, g, w \models_\sim x & \\ \Leftrightarrow \quad \{ \models_\sim \text{defn}\} & \quad g'(x) \sim_{\mathcal{M}'} w' \\ \quad g(x) \sim_{\mathcal{M}} w & \Leftrightarrow \quad \{ \models_\sim \text{defn}\} \\ \Rightarrow \quad \{ \ \text{step} \star \ \} & \quad \mathcal{M}', g', w' \models_\sim x \end{array}$$

Step $\star$ follows from condition 2 of Def. 6 and the assumptions $(g(x), g'(x)) \in h$ and $(w, w') \in h$.

Case $\varphi = \downarrow x.\, \phi$:

$$\begin{array}{l|l} \quad \mathcal{M}, g, w \models_\sim \downarrow x.\, \phi & \\ \Leftrightarrow \quad \{ \models_\sim \text{defn}\} & \quad \mathcal{M}', g'[x \mapsto w'], w' \models_\sim \phi \\ \quad \mathcal{M}, g[x \mapsto w], w \models_\sim \phi & \Leftrightarrow \quad \{ \models_\sim \text{defn}\} \\ \Rightarrow \quad \{ \ \text{step} \star\star \ \} & \quad \mathcal{M}', g', w' \models_\sim \downarrow x.\, \phi \end{array}$$

Step $\star\star$ follows from the Induction Hypothesis, since $(g(y), g'(y)) \in h$ for all $y \in X$ and $(w, w') \in h$ implies $(g[x \mapsto w](y), g'[x \mapsto w'](y)) \in h$ for all $y \in X$.

Case $\varphi = @_x \phi$:

$$\begin{array}{l|l} \quad \mathcal{M}, g, w \models_\sim @_x \phi & \\ \Leftrightarrow \quad \{ \models_\sim \text{defn}\} & \quad \mathcal{M}', g', g'(x) \models_\sim \phi \\ \quad \mathcal{M}, g, g(x) \models_\sim \phi & \Leftrightarrow \quad \{ \models_\sim \text{defn}\} \\ \Rightarrow \quad \{ \ \text{by I.H. since } (g(x), g'(x)) \in h \ \} & \quad \mathcal{M}', g', w' \models_\sim @_x \phi \end{array}$$

Case $\varphi = \langle \alpha \rangle \phi$:

$$\begin{array}{l} \quad \mathcal{M}, g, w \models_\sim \langle \alpha \rangle \phi \\ \Leftrightarrow \quad \{ \models_\sim \text{defn}\} \\ \quad \mathcal{M}, g, v \models_\sim \phi \text{ for some } v \in W \text{ with } (w, v) \in R_\alpha \\ \Rightarrow \quad \{ \text{Remark 1 + I.H.} \} \\ \quad \mathcal{M}', g', v' \models_\sim \phi \text{ for some } v' \in W' \text{ with } (w', v') \in R'_\alpha \\ \Leftrightarrow \quad \{ \models_\sim \text{defn}\} \\ \quad \mathcal{M}', g', w' \models_\sim \langle \alpha \rangle \phi \end{array}$$

The cases $\varphi = \phi \wedge \phi'$ and $\varphi = \phi \vee \phi'$ are straightforward by Induction Hypothesis. □

Theorem 3. *Let $\mathcal{M}$ and $\mathcal{M}'$ be two A-models and $h : \mathcal{M} \to \mathcal{M}'$ an observational morphism. Then, for any positive A-sentence φ, we have*

$$\mathcal{M} \models_\sim \varphi \text{ implies } \mathcal{M}' \models_\sim \varphi.$$

Proof. Since φ is a sentence, it follows from Lemma 6, that for any $w \in W, w' \in W'$ with $(w, w') \in h$, we have: $\mathcal{M}, w \models_\sim \varphi$ implies $\mathcal{M}', w' \models_\sim \varphi$. In particular, since $(w_0, w_0') \in h$, $\mathcal{M}, w_0 \models_\sim \varphi$ implies $\mathcal{M}', w_0' \models_\sim \varphi$, i.e., $\mathcal{M} \models_\sim \varphi$ implies $\mathcal{M}' \models_\sim \varphi$. □

Let us now consider the case in which h is an observational isomorphism.

Lemma 7. *Let $\mathcal{M} = (W, w_0, R)$ and $\mathcal{M}' = (W', w_0', R')$ be two A-models and $h : \mathcal{M} \to \mathcal{M}'$ an observational isomorphism. Then for any $w \in W, w' \in W'$ with $(w, w') \in h$, for any valuations $g : X \to W$, $g' : X \to W'$ with $(g(x), g'(x)) \in h$ for all $x \in X$, and for any A-formula φ, we have*

$$\mathcal{M}, g, w \models_\sim \varphi \text{ iff } \mathcal{M}', g', w' \models_\sim \varphi.$$

Proof. The proof is performed by induction on the structure of the formulas. The base case $\varphi = \mathbf{tt}$ is trivial and for $\varphi = \mathbf{ff}$ we note that neither $\mathcal{M}, g, w \models_\sim \mathbf{ff}$ nor $\mathcal{M}, g, w \models_\sim \mathbf{ff}$ holds.

Case $\varphi = x$: The proof is performed as for Lem. 6 with the addition that the "⇒" step (step $\star$) holds also in the opposite direction for the following reason: Let h^{-1} be the inverse of h. Since $(g(x), g'(x)) \in h$ and $(w, w') \in h$ we obtain, by Lem. 4, that $(g'(x), g(x)) \in h^{-1}$ and $(w', w) \in h^{-1}$. Now we can apply condition 2 of Def. 6 for h^{-1} such that $g'(x) \sim_{\mathcal{M}'} w'$ implies $g(x) \sim_{\mathcal{M}} w$.

Cases $\varphi = \downarrow x.\, \phi$ **and** $\varphi = @_x \phi$: The proof is performed as for Lem. 6 with the addition that the "⇒" steps hold also in the opposite direction since now the Induction Hypothesis holds also in the other direction.

Case $\varphi = \langle \alpha \rangle \phi$: The proof is performed as for Lem. 6 with the addition that the "⇒" step holds also in the opposite direction. To see this, we know by Lem. 5 that the "zag" condition of a bisimulation holds for h and for atomic actions $a \in A$. It is straightforward to prove that then the "zag" condition holds also for structured actions $\alpha \in \mathrm{Act}(A)$. Taking into account the I.H. we are done.

The cases $\varphi = \neg\phi$, $\varphi = \phi \wedge \phi'$ and $\varphi = \phi \vee \phi'$ are straightforward by Induction Hypothesis. The case $\varphi = [\alpha]\phi$ can be shown either by using the I.H. or by taking into account that the box operator can be expressed by negation and diamond. □

Theorem 4. *Let $\mathcal{M}, \mathcal{M}'$ be two A-models such that $\mathcal{M}$ **iso**$_\sim$ $\mathcal{M}'$. Then, for any A-sentence φ, we have*

$$\mathcal{M} \models_\sim \varphi \text{ iff } \mathcal{M}' \models_\sim \varphi.$$

Proof. The proof is completely analogous to the proof of Thm. 3, using Lem. 7 instead of Lem. 6. □

Corollary 2. *For any specification SP, its observational semantics* $Mod_{\sim}(SP)$ *is closed under* $\mathbf{iso}_{\sim}$.

The next theorem establishes a connection between the observational satisfaction in $\mathcal{D}^{\downarrow}_{\sim}$ and the satisfaction in $\mathcal{D}^{\downarrow}$. It relies on the construction of the quotient $\mathcal{M}/\sim$ of an A-model $\mathcal{M}$ that identifies observationally equal (i.e. bisimilar) states.

Definition 10. *Let* $\mathcal{M} = (W, w_0, R)$ *be an* A*-model. 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* $a \in A$*,*
- $(R/\sim)_a = \{([w],[v]) \mid$ *there exist* $w' \in [w]$ *and* $v' \in [v]$ *s.t.* $(w, v) \in R_a\}$.

Remark 2. For any $a \in A$ and $w, v \in W$, if $([w],[v]) \in (R/\sim)_a$ then there exists $\hat{v} \in [v]$ such that $(w, \hat{v}) \in R_a$. This follows from the (zig) property of $\sim_{\mathcal{M}}$. This fact can be generalised to composed actions $\alpha \in \mathrm{Act}(A)$.

Sentences are observationally satisfied by an A-model $\mathcal{M}$, if and only if they are satisfied by its quotient $\mathcal{M}/\sim$:

Theorem 5. *For any* A*-model* $\mathcal{M}$ *and for any* A*-sentence* φ*,*

$$\mathcal{M} \models_{\sim} \varphi \text{ iff } \mathcal{M}/\sim \models \varphi.$$

Proof. For the proof we show, more generally, that for any $w \in W$, valuation $g : X \to W$ and A-formula φ,

$$\mathcal{M}, g, w \models_{\sim} \varphi \text{ iff } \mathcal{M}/\sim, g/\sim, [w] \models \varphi$$

where $g/\sim\colon X \to W$ is defined by $(g/\sim)(x) = [g(x)]$. The proof can be performed by induction over the structure of A-formulas. For the base formulas $\varphi = x$, we have:

$$\begin{array}{ll|ll}
 & \mathcal{M}, g, w \models_{\sim} x & & [g(x)] = [w] \\
\Leftrightarrow & \{ \models_{\sim} \text{ defn}\} & \Leftrightarrow & \{ [g(x)] = (g/\sim)(x) + \models \text{ defn}\} \\
 & g(x) \sim_{\mathcal{M}} w & & \mathcal{M}/\sim, g/\sim, [w] \models x \\
\Leftrightarrow & \{ \text{ equivalence classes defn}\} & & \\
\end{array}$$

For the case $\varphi = \langle\alpha\rangle\phi$, we have:

$\mathcal{M}, g, w \models_{\sim} \langle\alpha\rangle\phi$

$\Leftrightarrow$ $\{ \models_{\sim} \text{ defn}\}$

there exists $v \in W$ with $(w, v) \in R_\alpha$ and $\mathcal{M}, g, v \models_{\sim} \phi$

$\Leftrightarrow$ $\{ \text{ step } \star \}$

there exists $[v'] \in W/\sim$ with $([w],[v']) \in (R/\sim)_\alpha$ and $\mathcal{M}/\sim, g/\sim, [v'] \models_{\sim} \phi$

$\Leftrightarrow$ $\{ \models_{\sim} \text{ defn}\}$

$\mathcal{M}/\sim, g/\sim, [w] \models_{\sim} \langle\alpha\rangle\phi$

Step $\star$: The direction "$\Rightarrow$" is trivial using $v' = v$ and the Induction Hypothesis. For the direction "$\Leftarrow$" assume $([w], [v']) \in (R/{\sim})_\alpha$ for some v'. By Remark 2 we know that there exists $\hat{v} \in [v']$ such that $(w, \hat{v}) \in R_\alpha$. From $\mathcal{M}/{\sim}, g/{\sim}, [v'] \models_\sim \phi$ it follows that $\mathcal{M}/{\sim}, g/{\sim}, [\hat{v}] \models_\sim \phi$ (since $[\hat{v}] = [v']$). By Ind. Hyp. we get $\mathcal{M}, g, \hat{v} \models_\sim \phi$. Since $(w, \hat{v}) \in R_\alpha$, we have $\mathcal{M}, g, w \models_\sim \langle\alpha\rangle\phi$.

The remaining cases are straightforward. □

4 Recovering Modal Invariance for Bisimulation

Thm. 4 of the last section shows modal invariance of sentences in the $\mathcal{D}^{\downarrow}_{\sim}$-logic. In this section we will transfer this result to the case in which bisimulation equivalence is used instead of an observational isomorphism. In fact, this is a consequence of our general result (Thm. 6) that bisimulation equivalence can be characterised as an isomorphism in the category $\mathrm{Mod}^{\mathcal{D}^{\downarrow}_{\sim}}(A)$. Finally, we can even prove a Hennessy-Milner-Theorem for observational satisfaction; see Thm. 7.

Lemma 8. *Let $\mathcal{M} = (W, w_0, R)$ and $\mathcal{M}' = (W', w_0', R')$ be two A-models. If $\mathcal{M} \equiv \mathcal{M}'$, then $\mathcal{M}$ $\mathbf{iso}_\sim$ $\mathcal{M}'$.*

Proof. Since $\mathcal{M} \equiv \mathcal{M}'$ we can consider the greatest bisimulation relation $\sim^{\mathcal{M}}_{\mathcal{M}'} \subseteq W \times W'$ between $\mathcal{M}$ and $\mathcal{M}'$. We show that $\sim^{\mathcal{M}}_{\mathcal{M}'}$ is an isomorphism in the category $\mathrm{Mod}^{\mathcal{D}^{\downarrow}_{\sim}}(A)$. First, we note that $\sim^{\mathcal{M}}_{\mathcal{M}'}$ contains (w_0, w_0'). Then we show that $\sim^{\mathcal{M}}_{\mathcal{M}'}$ is an observational morphism. This is proved by using two simple properties of greatest bisimulations: The inverse of $\sim^{\mathcal{M}}_{\mathcal{M}'}$ is $\sim^{\mathcal{M}'}_{\mathcal{M}}$ and the composition of $\sim^{\mathcal{M}}_{\mathcal{M}'}$ and $\sim^{\mathcal{M}'}_{\mathcal{M}''}$ is $\sim^{\mathcal{M}}_{\mathcal{M}''}$.

- Condition 1 of Def. 6 holds, since $\sim^{\mathcal{M}}_{\mathcal{M}'}$ is a bisimulation.
- For 2 of Def. 6, let us suppose $(w, w') \in \sim^{\mathcal{M}}_{\mathcal{M}'}$ and $(v, v') \in \sim^{\mathcal{M}}_{\mathcal{M}'}$ and $(w, v) \in \sim^{\mathcal{M}}_{\mathcal{M}}$. Hence, we have $(w', w) \in \sim^{\mathcal{M}'}_{\mathcal{M}}$ and by composition of bisimulation relations and the fact that $\sim^{\mathcal{M}'}_{\mathcal{M}'}$ is the greatest bisimulation we get $(w', v') \in \sim^{\mathcal{M}'}_{\mathcal{M}'}$.
- For 3 of Def. 6, let us suppose $(w, w') \in \sim^{\mathcal{M}}_{\mathcal{M}'}$, $(w, v) \in \sim^{\mathcal{M}}_{\mathcal{M}}$ and $(w', v') \in \sim^{\mathcal{M}'}_{\mathcal{M}'}$ Hence, $(v, w) \in \sim^{\mathcal{M}}_{\mathcal{M}}$ and by composition of bisimulation relations and the fact that $\sim^{\mathcal{M}}_{\mathcal{M}'}$ is the greatest bisimulation we get $(v, v') \in \sim^{\mathcal{M}}_{\mathcal{M}'}$.

Finally, $\sim^{\mathcal{M}}_{\mathcal{M}'}$ is an isomorphism, since $(\sim^{\mathcal{M}}_{\mathcal{M}'} \cdot \sim^{\mathcal{M}'}_{\mathcal{M}}) = \sim^{\mathcal{M}}_{\mathcal{M}} = 1_{\mathcal{M}}$ and, conversely, $(\sim^{\mathcal{M}'}_{\mathcal{M}} \cdot \sim^{\mathcal{M}}_{\mathcal{M}'}) = \sim^{\mathcal{M}'}_{\mathcal{M}'} = 1_{\mathcal{M}'}$. □

Theorem 6. *For any two A-models $\mathcal{M}$ and $\mathcal{M}'$, we have:*

$$\mathcal{M} \ \mathbf{iso}_\sim \ \mathcal{M}' \ \textit{iff} \ \mathcal{M} \equiv \mathcal{M}'.$$

Proof. The direction "$\Rightarrow$" follows from condition 1 in Def. 6 and from Lem. 5. The direction "$\Leftarrow$" follows from Lem. 8. □

As a consequence of Thm. 6 and the modal invariance for $\mathcal{D}^{\downarrow}_{\sim}$-logic (Thm. 4), we get modal invariance for bisimulation equivalence.

Corollary 3. *Let $\mathcal{M}, \mathcal{M}'$ be two A-models such that $\mathcal{M} \equiv \mathcal{M}'$. Then for any A-sentence φ, we have*

$$\mathcal{M} \models_\sim \varphi \text{ iff } \mathcal{M}' \models_\sim \varphi.$$

As an example, we consider the two bisimilar $\{a\}$-models $\mathcal{M}$ and $\mathcal{M}'$ in Fig. 1 for which we have: $\mathcal{M} \models_\sim \downarrow x.\langle a\rangle x$ and $\mathcal{M}' \models_\sim \downarrow x.\langle a\rangle x$.

Corollary 4. *For any specification SP, its observational semantics $Mod_\sim(SP)$ is closed under $\equiv$.*

Proof. Direct consequence of Corollary 3. □

The next lemma provides the basis for proving the converse of Cor. 3 which will lead to a Hennessy-Milner Theorem w.r.t. $\mathcal{D}^{\downarrow}_{\sim}$-logic (if models are image finite).

Lemma 9. *Let $\mathcal{M}, \mathcal{M}'$ be two image finite[5] A-models and $w \in W$, $w' \in W'$ two states such that, for any A-sentence φ,*

$$\mathcal{M}, w \models_\sim \varphi \text{ iff } \mathcal{M}', w' \models_\sim \varphi.$$

Then, there is a relation $h \subseteq W \times W'$ such that $(w, w') \in h$ and h satisfies the conditions "zig" and "zag" of a bisimulation; cf. Def. 5.

Proof. Let us consider the relation

$$h := \{(u, u') \mid \mathcal{M}, u \models_\sim \varphi \text{ iff } \mathcal{M}', u' \models_\sim \varphi,\ \varphi \text{ is an } A\text{-sentence}\}.$$

Obviously, $(w, w') \in h$. In order to prove "zig" we follow the strategy adopted in [8] for the proof of the so-called Hennessy-Milner Theorem. Planning to derive a contradiction, let us suppose there exists $(u, u') \in h$, $a \in A$ and $v \in W$ with $(u, v) \in R_a$, for which

$$\text{there is not a } v' \in W' \text{ such that } (u', v') \in R'_a \text{ and } (v, v') \in h. \tag{1}$$

By assumption, $\mathcal{M}'$ is image finite and hence the set $R'_a[u'] := \{v'_1, \ldots, v'_k\}$ of a-successors of u' in $\mathcal{M}'$ is finite. It is also not empty since $(u, u') \in h$. By (1), for each $i \in \{1, \ldots, k\}$ there is a formula φ_i such that

$$\mathcal{M}, v \models_\sim \varphi_i \text{ and } \mathcal{M}', v'_i \not\models_\sim \varphi_i. \tag{2}$$

Hence, we have $\mathcal{M}, u \models_\sim \langle a\rangle(\varphi_1 \wedge \cdots \wedge \varphi_k)$ and $\mathcal{M}', u' \not\models_\sim \langle a\rangle(\varphi_1 \wedge \cdots \wedge \varphi_k)$, contradicting the assumption $\mathcal{M}, u \models_\sim \varphi$ iff $\mathcal{M}', u' \models_\sim \varphi$ for all A-sentences φ. Therefore h satisfies "zig". One can show analogously that h satisfies "zag". □

Theorem 7. *Let $\mathcal{M}, \mathcal{M}'$ be two image finite A-models. Then the following properties are equivalent:*

[5] i.e. in any state there are at most finitely many outgoing transitions labelled with the same atomic action

1. $\mathcal{M}$ **iso**$_\sim$ $\mathcal{M}'$,
2. $\mathcal{M} \equiv \mathcal{M}'$,
3. *for any A-sentence* φ, $\mathcal{M} \models_\sim \varphi$ *iff* $\mathcal{M}' \models_\sim \varphi$.

Proof. 1. $\Leftrightarrow$ 2.: Thm. 6.
2. $\Rightarrow$ 3.: Cor. 3.
2. $\Leftarrow$ 3.: Follows from Lem. 9 by taking for w and w' the initial states w_0 and w_0' of $\mathcal{M}$ and $\mathcal{M}'$ resp. □

5 Relating Abstractor and Observational Semantics

Another possibility to provide an abstract semantics for a specification SP is to consider all models that are bisimulation equivalent to a "standard" model of SP, i.e. to a model of SP in the logic $\mathcal{D}^{\downarrow}$. This semantics is called *abstractor semantics*. In this section we investigate relationships between abstractor semantics and observational semantics. It turns out that results obtained in the framework of algebraic specifications, see [3], can be transferred to our logics $\mathcal{D}^{\downarrow}$ and $\mathcal{D}^{\downarrow}_{\sim}$ for reactive systems' specifications as well.

Definition 11 (Abstractor semantics). *The* abstractor semantics *of a specification* $SP = (A, \Phi)$ *is given by the class of models*

$$Abs_{\equiv}(SP) = \{\mathcal{M} \in \mathrm{Mod}^{\mathcal{D}^{\downarrow}}(A) \mid \mathcal{M} \equiv \mathcal{N} \text{ for some } \mathcal{N} \in Mod(SP)\}.$$

Part 1. of the next theorem shows that observational semantics is a subclass of abstractor semantics. The converse does, in general, not hold. It may even be the case that standard models of a specification, which always belong to the abstractor semantics, do not belong to the observational semantics. This happens, if axioms of a specification contradict the observational equality between states. In order to illustrate this, let us consider the specification $SP = \langle\{a\}, \{\downarrow x.\langle a\rangle\neg x\}\rangle$. If we consider the model $\mathcal{M}'$ with two states depicted in Fig. 1, we have that $\mathcal{M}' \models \downarrow x.\langle a\rangle\neg x$ but $\mathcal{M}' \not\models_\sim \downarrow x.\langle a\rangle\neg x$ since the state w_1' reached by the a-transition from w_0' is observationally equal to w_0' but the negation $\neg x$ would forbid this. Hence, $\mathcal{M}' \in Mod(SP)$ but $\mathcal{M}' \notin Mod_\sim(SP)$. If, however, the axioms of a specification SP have the form that all models of SP in $\mathcal{D}^{\downarrow}$ belong to the observational semantics of SP in $\mathcal{D}^{\downarrow}_{\sim}$, then part 2. of the next theorem shows that abstractor and observational semantics coincide.

Theorem 8. *Let* $SP = (A, \Phi)$ *be a specification.*

1. $Mod_\sim(SP) \subseteq Abs_\equiv(SP)$.
2. $Mod(SP) \subseteq Mod_\sim(SP)$ *if and only if* $Mod_\sim(SP) = Abs_\equiv(SP)$.

Proof. Part 1.: Let $\mathcal{M} \in Mod_\sim(SP)$ and $\mathcal{M}/\!\sim$ its quotient according to Def. 10. By Theorem 5, we have that $\mathcal{M} \models_\sim \varphi$ iff $\mathcal{M}/\!\sim \models \varphi$ for all A-sentences φ and hence for all $\varphi \in \Phi$. Since $\mathcal{M} \in Mod_\sim(SP)$, we get $\mathcal{M}/\!\sim \in Mod(SP)$. Moreover, it is straightforward to show that $\mathcal{M} \equiv \mathcal{M}/\!\sim$, 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. The (zig) condition of a bisimulation is obvious. For the (zag) condition assume that $([w], [v]) \in (R/\sim)_a$. By Remark 2 we know that there exists $\hat{v} \in [v]$ such that $(w, \hat{v}) \in R_a$. Sinve $[\hat{v}] = [v]$ and $(\hat{v}, [\hat{v}]) \in B$ we have $(\hat{v}, [v]) \in B$. Finally, from $\mathcal{M} \equiv \mathcal{M}/\sim$ and $\mathcal{M}/\sim \in \mathit{Mod}(SP)$ we get $\mathcal{M} \in \mathit{Abs}_{\equiv}(SP)$.
Part 2.: "$\Rightarrow$:" Assume $\mathit{Mod}(SP) \subseteq \mathit{Mod}_{\sim}(SP)$. By 1. we have $\mathit{Mod}_{\sim}(SP) \subseteq \mathit{Abs}_{\equiv}(SP)$. Let $\mathcal{M} \in \mathit{Abs}_{\equiv}(SP)$, i.e. there is a model $\mathcal{N} \in \mathit{Mod}(SP)$ such that $\mathcal{M} \equiv \mathcal{N}$. By assumption $\mathcal{N} \in \mathit{Mod}_{\sim}(SP)$, i.e., $\mathcal{N} \models_{\sim} \Phi$. By Cor. 3, $\mathcal{M} \models_{\sim} \Phi$, and hence $\mathcal{M} \in \mathit{Mod}_{\sim}(SP)$.

"$\Leftarrow$:" For this direction, assume $\mathcal{M} \in \mathit{Mod}(SP)$. Hence, $\mathcal{M} \in \mathit{Abs}_{\equiv}(SP)$. By assumption $\mathit{Mod}_{\sim}(SP) = \mathit{Abs}_{\equiv}(SP)$ and hence $\mathcal{M} \in \mathit{Mod}_{\sim}(SP)$. □

Finally we want to discuss the relationship of observational semantics with abstractor semantics in the context of fully abstract models. An A-model $\mathcal{M}$ is *fully abstract* if the observational equality $\sim_{\mathcal{M}}$ coincides with the set-theoretic equality of states. The *fully abstract semantics* of a specification $SP = (A, \Phi)$ in $\mathcal{D}^{\downarrow}$ is given by the class of its fully abstract models

$$\mathit{Mod}^{fa}(SP) = \{\mathcal{M} \in \mathit{Mod}(SP) \mid \mathcal{M} \textit{ is fully abstract}\}.$$

If we consider all A-models which are bisimulation equivalent to some fully abstract model of a specification we get the class

$$\mathit{Abs}^{fa}_{\equiv}(SP) = \{\mathcal{M} \in \mathrm{Mod}^{\mathcal{D}^{\downarrow}}(A) \mid \mathcal{M} \equiv \mathcal{N} \text{ for some } \mathcal{N} \in \mathit{Mod}^{fa}(SP)\}.$$

Our final result shows that this class coincides with the observational semantics of a specification. A similar result has been obtained for algebraic specifications in [3].

Theorem 9. *For any specification $SP = (A, \Phi)$, $\mathit{Mod}_{\sim}(SP) = \mathit{Abs}^{fa}_{\equiv}(SP)$.*

Proof. The proof of the inclusion "$\subseteq$" is the same as for part 1 in Thm. 8 taking into account that $\mathcal{M}/\sim$ is fully abstract. It remains to show $\mathit{Abs}^{fa}_{\equiv}(SP) \subseteq \mathit{Mod}_{\sim}(SP)$. Let $\mathcal{M} \in \mathit{Abs}^{fa}_{\equiv}(SP)$. Then $\mathcal{M} \equiv \mathcal{N}$ for some $\mathcal{N} \in \mathit{Mod}^{fa}(SP)$. Since $\mathcal{N} \models \Phi$ and $\mathcal{N}$ is fully abstract, we have $\mathcal{N} \models_{\sim} \Phi$. Since $\mathcal{M} \equiv \mathcal{N}$ we get, by Cor. 3, that $\mathcal{M} \models_{\sim} \Phi$. Hence $\mathcal{M} \in \mathit{Mod}_{\sim}(SP)$. □

6 Conclusion

This paper follows the motivations of [7] on the definition of a logic to develop reactive systems in a stepwise manner from abstract requirements specifications to concrete specifications of processes. In this context, the quest for a more liberal semantics appeared that is closed under behavioural equivalence. Following ideas from algebraic specifications of data structures, we have proposed a new logic for specifications of reactive systems, called $\mathcal{D}^{\downarrow}_{\sim}$, which satisfies both the modal invariance property and a Hennessy-Milner Theorem. The key to achieve this was

a new, relaxed satisfaction relation, which allows interpreting state variables up to bisimilarity.

There are several interesting research questions to be pursued on the basis of $\mathcal{D}^{\downarrow}_{\sim}$. For instance, we want to investigate how $\mathcal{D}^{\downarrow}_{\sim}$ can be extended to an institution. A preliminary study shows that a straightforward extension using functions $\sigma : A \to A'$ between action sets as signature morphisms would not work. The reason is that A' may introduce new actions that distinguish, in some A'-models, states which are observationally equal when using only actions in A. Then the satisfaction condition of an institution would not be valid. Therefore we must investigate adjustments on signatures, signature morphisms and models to establish the satisfaction condition. Another interesting extension to follow concerns the incorporation of weak bisimulations which would allow further behavioural abstraction w.r.t. silent transitions.

Acknowledgement. We would like to thank the anonymous reviewers of this paper for their careful reviews with many useful comments and suggestions.

References

1. L. Aceto, A. Ingólfsdóttir, K. G. Larsen, and J. Srba. *Reactive Systems: Modelling, Specification and Verification*. Cambridge University Press, 2007.
2. M. Bidoit and R. Hennicker. Constructor-based observational logic. *J. Log. Algebr. Program.*, 67(1-2):3–51, 2006.
3. M. Bidoit, R. Hennicker, and M. Wirsing. Behavioural and abstractor specifications. *Sci. Comput. Program.*, 25(2–3):149–186, 1995.
4. T. Bräuner. *Hybrid Logic and its Proof–Theory*. App. Logic Series. Springer, 2010.
5. J. A. Goguen and G. Malcolm. A hidden agenda. *Theor. Comput. Sci.*, 245(1):55–101, 2000.
6. D. Harel, D. Kozen, and J. Tiuryn. *Dynamic Logic*. MIT Press, 2000.
7. A. Madeira, L. S. Barbosa, R. Hennicker, and M. A. Martins. Dynamic logic with binders and its application to the development of reactive systems. In A. Sampaio and F. Wang, editors, *Theoretical Aspects of Computing - ICTAC 2016*, volume 9965 of *Lecture Notes in Computer Science*, pages 422 – 440, 2016.
8. R. Milner. *Communication and concurrency*. PHI Series in computer science. Prentice Hall, 1989.
9. H. Reichel. Behavioural validity of conditional equations in abstract data types. In *Proc. of the Vienna Conference on Contributions to General Algebra 3, Verlag B.G. Teubner*, pages 301–324, 1985.
10. D. Sannella and A. Tarlecki. *Foundations of Algebraic Specification and Formal Software Development*. Monographs on TCS, an EATCS Series. Springer, 2012.