Behavioural and Abstractor Specifications for a Dynamic Logic with Binders and Silent Transitions

Rolf Hennicker[1], Alexander Knapp[2], Alexandre Madeira[3], and Felix Mindt[1⋆]

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

Abstract. We extend dynamic logic with binders (for state variables) by distinguishing between observable and silent transitions. This differentiation gives rise to two kinds of observational interpretations of the logic: abstractor and behavioural specifications. Abstractor specifications relax the standard model class semantics of a specification by considering its closure under weak bisimulation. Behavioural specifications, however, rely on a behavioural satisfaction relation which relaxes the interpretation of state variables and the satisfaction of modal formulas $\langle\alpha\rangle\varphi$ and $[\alpha]\varphi$ by abstracting from silent transitions. A formal relation between abstractor and behavioural specifications is provided which shows that both coincide semantically under mild conditions. For the proof we instantiate the previously introduced concept of a behaviour-abstractor framework to the case of dynamic logic with binders and silent transitions.

1 Introduction

Observability plays an important role in software development: a system is correct if it exhibits the desired observable behaviour. Formal observability notions for abstracting from internal details have been established in the theory of algebraic specifications of data types, e.g., by distinguishing between observable and non-observable sorts, and also in concurrency theory, e.g., by Milner's notion of observational equivalence of processes. For algebraic specifications an "externalised" and an "internalised" view of observability have been pursued leading to the concepts of abstractor and behavioural specification respectively. An abstractor specification **abstract** *Sp* **wrt** $\equiv$ abstracts from the standard model class of a specification *Sp* by considering its closure under an observational equivalence relation $\equiv$ between algebras [13,16,15]. A behavioural specification

⋆ This work is supported by ERDF European Regional Development Fund, through the COMPETE Programme, and by National Funds through FCT - Portuguese Foundation for Science and Technology - within projects POCI-01-0145-FEDER-016692 and UID/MAT/04106/2019. This author is supported in the scope of the framework contract foreseen in the numbers 4, 5 and 6 of the article 23, of the Decree-Law 57/2016, of August 29, changed by Portuguese Law 57/2017, of July 19.

behaviour *Sp* **wrt** $\models\!\!\approx$ relies on an observational equality relation $\approx$ between the elements of an algebra and a behavioural satisfaction relation $\models\!\!\approx$ which interprets the equality symbol by observational rather than set-theoretic equality [14,12,4]. It has been shown that for first-order logic specifications both approaches are semantically equivalent under mild conditions [1]. This result has been transferred to higher-order logic [8], to arbitrary (concrete) institutions [11] and, more recently in the context of reactive system specifications [5], to dynamic logic $\mathcal{D}^{\downarrow}$ with binders $\downarrow x\,.\,\varphi$ for state variables. In the case of $\mathcal{D}^{\downarrow}$-logic the abstraction equivalence $\equiv$ is strong bisimulation between labelled transition systems (LTS) and behavioural satisfaction $\models\!\!\approx$ interprets state variables up to (strong) bisimilarity of states. In [7] we were able to extract some general conditions under which, independently of the concrete logical framework at hand, the behaviour-abstractor relationships generally hold: (BA1) behavioural satisfaction of sentences must be invariant under abstraction equivalence and, for each semantic structure, (BA2) an observationally equivalent "black-box structure" must exist for which (BA3) behavioural satisfaction of sentences coincides with standard satisfaction. The results of [7] have been applied in [7, Section 3 and 4] to first-order logic and higher-order logic resp., as well as to $\mathcal{D}^{\downarrow}$-logic [7, Section 5] and observable Hennessy-Milner logic [7, Section 6].

We extend $\mathcal{D}^{\downarrow}$-logic by distinguishing between observable actions and the invisible action τ (interpreted by silent transitions). The resulting logic is denoted by $\mathcal{D}^{\downarrow}_{\tau}$. Then *weak* bisimulation between LTSs (like in observable Hennessy-Milner logic) is the adequate choice for the observational abstraction equivalence $\equiv$. For the internalised observational equality we use the greatest weak bisimulation relation $\approx_M$ between the states of an LTS M. Behavioural satisfaction $\models\!\!\approx$ is now defined by interpreting state variables up to $\approx_M$ and the interpretation of the diamond operator (and thus also of the derived box operator) is relaxed as in observable modal logic [17] and [7, Section 6]: a sentence $\langle a\rangle\varphi$ with observable action a holds behaviourally in a state w if there exist arbitrarily many silent transitions starting in w which are followed by an a-transition and then again by arbitrarily many silent transitions such that the resulting state v satisfies behaviourally φ.

The goal of this paper is to establish also in the setting of $\mathcal{D}^{\downarrow}_{\tau}$ a relationship between abstractor specifications **abstract** *Sp* **wrt** $\equiv$ and behavioural specifications **behaviour** *Sp* **wrt** $\models\!\!\approx$. For this purpose, we show that $\mathcal{D}^{\downarrow}_{\tau}$ gives rise to an instantiation of the behaviour-abstractor framework in the sense of [7] satisfying the conditions (BA1–BA3) as described above. In the context of $\mathcal{D}^{\downarrow}_{\tau}$-logic, the first condition (BA1) expresses a modal invariance property with respect to weak bisimulation between labelled transition systems and behavioural satisfaction. For (BA2), we define the black-box structure of a labelled transition system M in terms of its quotient $M/{\approx_M}$ and show that both are weakly bisimilar. For getting (BA3) we show that for quotients standard satisfaction and behavioural satisfaction of formulas is the same. Thus we get a behaviour-abstractor framework and can apply the results in [7] to $\mathcal{D}^{\downarrow}_{\tau}$-logic which show that behavioural semantics is included in abstractor semantics (of specifications) and both are the same if and only if standard semantics is included in behavioural semantics.

Our results extend both, the behaviour-abstractor relationships investigated for $\mathcal{D}^{\downarrow}$-logic in [7, Section 5] and the Hennessy-Milner style instantiation of the behaviour-abstractor framework in [7, Section 6]. In contrast to [7, Section 6] we do not use in formulas the special empty action ε but the invisible action τ instead. Though both are equivalent in the observational interpretations of the logic $\mathcal{D}_{\tau}^{\downarrow}$ they are not in the standard interpretation of $\mathcal{D}_{\tau}^{\downarrow}$. Compared to [7, Section 6] this leads to a significant simplification and generalisation since we do not need to restrict our results to weakly deterministic models.

The remainder of this paper is structured as follows: In Sect. 2 we present $\mathcal{D}_{\tau}^{\downarrow}$-logic, the basis of our approach. Then, in Sect. 3, we consider two observational interpretations of $\mathcal{D}_{\tau}^{\downarrow}$ in terms of abstractor and behavioural specifications. In Sect. 4 we recall the general concept of a behaviour-abstractor framework and we show how it can be instantiated with $\mathcal{D}_{\tau}^{\downarrow}$-logic and its observational interpretations. Thus we get the semantic relationships between abstractor and behavioural specifications for free. All investigations are accompanied by examples. Concluding remarks are given in Sect. 5.

2 A Dynamic Logic with Binders and Silent Transitions

Dynamic logic with binders, called $\mathcal{D}^{\downarrow}$-logic, has been introduced in [9] 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. Thus $\mathcal{D}^{\downarrow}$-logic supports a stepwise refinement methodology for the formal development of reactive systems. The logic combines modalities indexed by regular expressions of actions, as in Dynamic Logic [3], and state variables with binders, as in Hybrid Logic [2]. In this section we extend $\mathcal{D}^{\downarrow}$-logic by splitting atomic actions into observable actions and the invisible action τ. The new logic, denoted by $\mathcal{D}_{\tau}^{\downarrow}$, is technically only a small modification of $\mathcal{D}^{\downarrow}$ but, as we will see in the forthcoming sections, the differentiation between observable and invisible actions provides a powerful basis for observational interpretations.

Signatures and sentences. A *$\mathcal{D}_{\tau}^{\downarrow}$-signature* is a set $A = O \cup \{\tau\}$ of *atomic actions* comprising *observable actions* O and the *invisible action* τ. The class of $\mathcal{D}_{\tau}^{\downarrow}$-signatures is denoted by $\mathbb{S}^{\mathcal{D}_{\tau}^{\downarrow}}$. The set of *composed actions* $Act(A)$ over A is given by

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

where $a \in A$ and ; represents the sequential composition of actions, $+$ the choice between actions, and * the iteration of an action.

For any $A \in \mathbb{S}^{\mathcal{D}_{\tau}^{\downarrow}}$, the set of *$A$-formulas* is given by

$$\varphi ::= \mathbf{tt} \mid \neg\varphi \mid \varphi \vee \varphi \mid \langle\alpha\rangle\varphi \mid x \mid \downarrow x\,.\,\varphi \mid (@x)\varphi$$

where $\alpha \in Act(A)$ is a composed action and $x \in X$ is a variable belonging to a universal set X of state variables. We use the usual abbreviations $\mathbf{ff} = \neg\mathbf{tt}$,

$\varphi \wedge \psi = \neg(\neg\varphi \vee \neg\psi)$, $[\alpha]\varphi = \neg\langle\alpha\rangle\neg\varphi$, etc. An *A-sentence* is an A-formula φ containing no free variables, where free variables are defined as usual with $\downarrow$ being the only operator binding variables. The set of A-sentences is denoted by $\mathrm{Sen}^{\mathcal{D}^{\downarrow}_{\tau}}(A)$.

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. $\mathcal{D}^{\downarrow}_{\tau}$ 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.

Structures. The semantic structures of $\mathcal{D}^{\downarrow}_{\tau}$ are reachable, labelled transition systems (LTS) with initial state. For an $A \in \mathbb{S}^{\mathcal{D}^{\downarrow}_{\tau}}$, an *A-structure* $M = (W, R, w_0)$ consists of a *set of states* W, a family of *transition relations* $R = (R_a \subseteq W \times W)_{a\in A}$, and the *initial state* $w_0 \in W$ such that, for each $w \in W$, either $w = w_0$ or there is a finite sequence of transitions $(w_{k-1}, w_k) \in R_{a_k}$, $1 \leq k \leq n$, with $a_k \in A$, such that $w_n = w$. Transitions in R_τ are called *silent transitions*. The class of A-structures is denoted by $Str^{\mathcal{D}^{\downarrow}_{\tau}}(A)$.

Satisfaction relation. To define the satisfaction relation we extend, as usual, the interpretation of actions over a structure $M = (W, R, w_0) \in Str^{\mathcal{D}^{\downarrow}_{\tau}}(A)$ to composed actions from $Act(A)$ 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 $y \in X \setminus \{x\}$. For any A-structure $M = (W, R, w_0) \in Str^{\mathcal{D}^{\downarrow}_{\tau}}(A)$, valuation $g : X \to W$ and state $w \in W$,

- $M, g, w \models^{\mathcal{D}^{\downarrow}_{\tau}}_{A} \mathbf{tt}$ is true;
- $M, g, w \models^{\mathcal{D}^{\downarrow}_{\tau}}_{A} \neg\varphi$ iff it is false that $M, g, w \models^{\mathcal{D}^{\downarrow}_{\tau}}_{A} \varphi$;
- $M, g, w \models^{\mathcal{D}^{\downarrow}_{\tau}}_{A} \varphi \vee \varphi'$ iff $M, g, w \models^{\mathcal{D}^{\downarrow}_{\tau}}_{A} \varphi$ or $M, g, w \models^{\mathcal{D}^{\downarrow}_{\tau}}_{A} \varphi'$;
- $M, g, w \models^{\mathcal{D}^{\downarrow}_{\tau}}_{A} \langle\alpha\rangle\varphi$ iff there is a $v \in W$ with $(w, v) \in R_\alpha$ and $M, g, v \models^{\mathcal{D}^{\downarrow}_{\tau}}_{A} \varphi$;
- $M, g, w \models^{\mathcal{D}^{\downarrow}_{\tau}}_{A} x$ iff $g(x) = w$;
- $M, g, w \models^{\mathcal{D}^{\downarrow}_{\tau}}_{A} \downarrow x\,.\,\varphi$ iff $M, g\{x \mapsto w\}, w \models^{\mathcal{D}^{\downarrow}_{\tau}}_{A} \varphi$;
- $M, g, w \models^{\mathcal{D}^{\downarrow}_{\tau}}_{A} (@x)\varphi$ iff $M, g, g(x) \models^{\mathcal{D}^{\downarrow}_{\tau}}_{A} \varphi$.

If φ is an A-sentence, then the valuation is irrelevant, i.e., $M, g, w \models^{\mathcal{D}^{\downarrow}_{\tau}}_{A} \varphi$ iff $M, w \models^{\mathcal{D}^{\downarrow}_{\tau}}_{A} \varphi$. *M satisfies* an A-sentence φ, denoted by $M \models^{\mathcal{D}^{\downarrow}_{\tau}}_{A} \varphi$, if $M, w_0 \models^{\mathcal{D}^{\downarrow}_{\tau}}_{A} \varphi$.

A specification $Sp = (A, \Phi)$ over $\mathcal{D}^{\downarrow}_{\tau}$ consists of a signature $A \in \mathbb{S}^{\mathcal{D}^{\downarrow}_{\tau}}$ and a set $\Phi \subseteq \mathrm{Sen}^{\mathcal{D}^{\downarrow}_{\tau}}(A)$ of A-sentences, also called *axioms*, specifying required properties. The semantics of Sp is given by its *model class* $\mathrm{Mod}^{\mathcal{D}^{\downarrow}_{\tau}}(Sp)$, which is the class of all A-structures satisfying the axioms of Sp, i.e.,

$$\mathrm{Mod}^{\mathcal{D}^{\downarrow}_{\tau}}(Sp) = \{M \in Str^{\mathcal{D}^{\downarrow}_{\tau}}(A) \mid \forall \varphi \in \Phi\,.\, M \models^{\mathcal{D}^{\downarrow}_{\tau}}_{A} \varphi\}\ .$$

3 Abstractor and Behavioural Specifications over $\mathcal{D}^{\downarrow}_{\tau}$

3.1 Motivation and Example

Though $\mathcal{D}^{\downarrow}_{\tau}$ extends $\mathcal{D}^{\downarrow}$ with its distinction between observable and invisible actions, its satisfaction relation does not take this difference into account. It interprets the invisible action τ in the same way as observable actions: $M, g, w \models^{\mathcal{D}^{\downarrow}_{\tau}}_{A} \langle\tau\rangle\varphi$ iff there is a $v \in W$ with $(w, v) \in R_\tau$ and $M, g, v \models^{\mathcal{D}^{\downarrow}_{\tau}}_{A} \varphi$. A proper integration of the invisible action τ should make clear that this action is in fact not observable: performing or not performing just τ actions should be equivalent from the observational point of view. The following example motivates the need for observational interpretations in the presence of silent transitions.

Example 1. We consider a specification *2Buf* for buffers of size 2. There are two observable actions *in* and *out*. For simplicity, we do not specify the nature of the elements inserted by *in* or removed by *out* from the buffer. It is assumed that the specification *2Buf* has the following sentence φ as an axiom[4]:

$$\varphi = \downarrow x_0 \,.\, \langle in\rangle\downarrow x_1 \,.\, (\langle out\rangle x_0 \wedge \langle in\rangle\downarrow x_2 \,.\, \langle out\rangle x_1)$$

Obviously, the LTS M shown in Fig. 1 satisfies φ and hence $M \in \mathrm{Mod}(\mathit{2Buf})$.

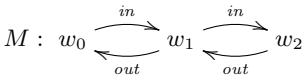

Fig. 1. A model of *2Buf*

Now we want to construct an implementation of a two element buffer by composing two one element buffers. The composition should be achieved in a way such that the first (one element) buffer inputs an element from the outside, then it synchronises its output with the input of the second (one element) buffer and thus transmits the received element to the second buffer. Then either the first buffer can input another element or the second buffer outputs its element to the outside, etc. Figure 2 shows an LTS I which models the (behaviour of the) synchronous composition of two one element buffers. Shifting an element from the first to the second buffer is invisible to the outside and thus modelled by a silent τ-transition.

Note that the LTS I does not satisfy the axiom φ since after an *in*-action an *out* is not possible (and also another *in* is not possible). Hence $I \notin \mathrm{Mod}(\mathit{2Buf})$. Nevertheless I should be regarded as a correct implementation of *2Buf*. It has the expected observable behaviour of a two element buffer since the shift of elements is not visible. Hence we are faced with the question: How can we formally justify

[4] In general there could be other axioms as well specifying, e.g., disallowed behaviours.

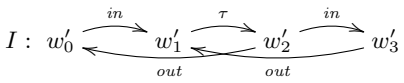

Fig. 2. LTS of two composed one element buffers

the correctness of the implementation I? There are, in principle, two possible solutions.

First, we notice that I is weakly bisimilar (for the formal definition see below) to the model M of *2Buf*. A weak bisimulation relation between the states of M and I is given by the set $B = \{(w_0, w'_0), (w_1, w'_1), (w_1, w'_2), (w_2, w'_3)\}$. Thus, by constructing the closure of the model class of *2Buf* under weak bisimulation the LTS I will be an element of this "abstracted" model class and therefore can be considered as a correct implementation of *2Buf*. Another possibility is to relax the satisfaction relation for modal formulas $\langle\alpha\rangle\varphi$ (and hence $[\alpha]\varphi$) by abstracting from silent transitions (for the formal definition of behavioural satisfaction see below). Then the LTS I does behaviourally satisfy the axiom φ and therefore I can be considered again as a correct implementation of *2Buf*. □

In the sequel we will formalise the two approaches to observational interpretations of $\mathcal{D}^{\downarrow}_{\tau}$ illustrated in Ex. 1 and we will study relationships between them.

3.2 Abstractor Specifications over $\mathcal{D}^{\downarrow}_{\tau}$

Abstractor specifications are based on weak bisimulation equivalence. For its definition (cf. [10]), we first define the τ-closure of transition relations with observable actions. For $A = O \cup \{\tau\} \in \mathbb{S}^{\mathcal{D}^{\downarrow}_{\tau}}$, let $M = (W, R, w_0)$ be an A-structure with transition relations $R = (R_a \subseteq W \times W)_{a \in A}$. For each $o \in O$, the τ-closure of R_o is the relation $\widehat{R}_o \subseteq W \times W$ such that $(w, v) \in \widehat{R}_a$ if and only if there is a finite sequence of transitions in R from w to v containing exactly one transition labelled with observable action a surrounded by arbitrarily many τ-transitions. The relation $\widehat{R}_\tau \subseteq W \times W$ contains all pairs (w, v) such that there is a finite, possibly empty, sequence of τ-transitions from w to v, i.e., either $w = v$ or there are $(w_k, w_{k+1}) \in R_\tau$ for $1 \leq k \leq n$ with $n \geq 1$, such that $w_1 = w$ and $w_{n+1} = v$. The τ-closure for atomic actions extends to composed actions by $\widehat{R}_{\alpha;\alpha'} = \widehat{R}_\alpha \cdot \widehat{R}_{\alpha'}$, $\widehat{R}_{\alpha+\alpha'} = \widehat{R}_\alpha \cup \widehat{R}_{\alpha'}$, and $\widehat{R}_{\alpha^*} = (\widehat{R}_\alpha)^\star$.

Definition 1 (Weak bisimulation). *Let $M = (W, R, w_0)$ and $M' = (W', R', w'_0)$ be two A-structures. A* weak bisimulation relation *between M and M' is a relation $B \subseteq W \times W'$ that contains (w_0, w'_0) and satisfies*

(weak-zig) *for any $a \in A$, $w, v \in W$, $w' \in W'$ such that $(w, w') \in B$:*
if $(w, v) \in R_a$, then there is a $v' \in W'$ such that $(w', v') \in \widehat{R}'_a$ and $(v, v') \in B$;
(weak-zag) *for any $a \in A$, $w \in W$, $w', v' \in W'$ such that $(w, w') \in B$:*
if $(w', v') \in R'_a$, then there is a $v \in W$ such that $(w, v) \in \widehat{R}_a$ and $(v, v') \in B$.

Two A-structures $M, M' \in Str^{\mathcal{D}^{\downarrow}_{\tau}}(A)$ are weakly bisimulation equivalent*, denoted by $M \equiv_A^{\mathcal{D}^{\downarrow}_{\tau}} M'$, if there exists a weak bisimulation relation between M and M'.*

Weak bisimulation relations extend to composed actions and their τ-closures:

Lemma 1. *Let M and M' be two A-structures and $B \subseteq W \times W'$ be a weak bisimulation. Then the following holds:*

(weak-zig*) *for any $\alpha \in Act(A)$, $w, v \in W$, $w' \in W'$ such that $(w, w') \in B$:*
if $(w, v) \in \widehat{R}_\alpha$, then there is a $v' \in W'$ such that $(w', v') \in \widehat{R}'_\alpha$ and $(v, v') \in B$;
(weak-zag*) *for any $\alpha \in Act(A)$, $w \in W$, $w', v' \in W'$ such that $(w, w') \in B$:*
if $(w', v') \in \widehat{R}'_\alpha$, then there is a $v \in W$ such that $(w, v) \in \widehat{R}_\alpha$ and $(v, v') \in B$.

It is well known that, for any $A \in \mathbb{S}^{\mathcal{D}^{\downarrow}_{\tau}}$, weak bisimulation equivalence $\equiv_A^{\mathcal{D}^{\downarrow}_{\tau}}$ is an equivalence relation on the class of A-structures. An *abstractor specification* (over $\mathcal{D}^{\downarrow}_{\tau}$) is an expression **abstract** Sp **wrt** $\equiv_A^{\mathcal{D}^{\downarrow}_{\tau}}$ where $Sp = (A, \Phi)$ is a specification over $\mathcal{D}^{\downarrow}_{\tau}$. The semantics of an abstractor specification is given by the closure of the model class of Sp under weak bisimulation, i.e.,

$$\mathrm{Mod}^{\mathcal{D}^{\downarrow}_{\tau}}(\textbf{abstract } Sp \textbf{ wrt } \equiv_A^{\mathcal{D}^{\downarrow}_{\tau}}) = \{M \in Str^{\mathcal{D}^{\downarrow}_{\tau}}(A) \mid \exists N \in \mathrm{Mod}^{\mathcal{D}^{\downarrow}_{\tau}}(Sp) \,.\, M \equiv_A^{\mathcal{D}^{\downarrow}_{\tau}} N\} \,.$$

Example 2. Let I be the LTS in Fig. 2. Then, as discussed in Ex. 1, $I \in \mathrm{Mod}^{\mathcal{D}^{\downarrow}_{\tau}}(\textbf{abstract } 2Buf \textbf{ wrt } \equiv_A^{\mathcal{D}^{\downarrow}_{\tau}})$. □

3.3 Behavioural Specifications over $\mathcal{D}^{\downarrow}_{\tau}$

Behavioural specifications rely on a behavioural satisfaction relation. The crucial idea of behavioural satisfaction in the context of $\mathcal{D}^{\downarrow}_{\tau}$ is twofold: first, we relax the satisfaction of the diamond modality (and hence of the derived box operator) by abstracting from invisible τ-transitions as done for observable modal logic in [17]. Secondly, we interpret state variables x by states which are not necessarily identical but only observationally equal to the current value of x. For the latter purpose, we recall that for any A-structure $M = (W, R, w_0)$ there exists a greatest weak bisimulation relation between the states of M. We denote this relation by $\approx_M \subseteq W \times W$ and call it *observational equality*. Note that $\approx_M$ is an equivalence relation.

Definition 2 (Behavioural satisfaction). *Let $M = (W, R, w_0)$ be an A-structure, $g : X \to W$ a valuation and $w \in W$. The* behavioural satisfaction *of an A-formula φ w.r.t. valuation g in state w, denoted by $M, g, w \models\!\!\approx_A^{\mathcal{D}^{\downarrow}_{\tau}} \varphi$, is defined analogously to the satisfaction relation for $\mathcal{D}^{\downarrow}$ (see Sect. 2) with the exception of diamond and state variable formulas:*

– *$M, g, w \models\!\!\approx_A^{\mathcal{D}^{\downarrow}_{\tau}} \langle\alpha\rangle\varphi$ iff there is a $v \in W$ with $(w, v) \in \widehat{R}_\alpha$ and $M, g, v \models\!\!\approx_A^{\mathcal{D}^{\downarrow}_{\tau}} \varphi$;*

– $M, g, w \models\!\approx_A^{\mathcal{D}_\tau^\downarrow} x$ *iff* $g(x) \approx_M w$.

For an A-sentence $\varphi \in \mathrm{Sen}^{\mathcal{D}_\tau^\downarrow}(A)$*, the valuation is irrelevant and* M satisfies behaviourally φ*, denoted by* $M \models\!\approx_A^{\mathcal{D}_\tau^\downarrow} \varphi$*, iff* $M, w_0 \models\!\approx_A^{\mathcal{D}_\tau^\downarrow} \varphi$.

A *behavioural specification* (over $\mathcal{D}_\tau^\downarrow$) is an expression **behaviour** Sp **wrt** $\models\!\approx_A^{\mathcal{D}_\tau^\downarrow}$ where $Sp = (A, \Phi)$ is a specification over $\mathcal{D}_\tau^\downarrow$. The semantics of a behavioural specification is given by the class of all A-structures which satisfy behaviourally the axioms of the specification, i.e.,

$$\mathrm{Mod}^{\mathcal{D}_\tau^\downarrow}(\textbf{behaviour } Sp \textbf{ wrt } \models\!\approx_A^{\mathcal{D}_\tau^\downarrow}) = \{M \in Str^{\mathcal{D}_\tau^\downarrow}(A) \mid \forall \varphi \in \Phi \,.\, M \models\!\approx_A^{\mathcal{D}_\tau^\downarrow} \varphi\} \ .$$

Example 3. Let I be the LTS in Fig. 2. Then I behaviourally satisfies the specification *2Buf*, i.e., $I \in \mathrm{Mod}^{\mathcal{D}_\tau^\downarrow}(\textbf{behaviour } \textit{2Buf} \textbf{ wrt } \models\!\approx_A^{\mathcal{D}_\tau^\downarrow})$. For instance, after an *in*-action an *out*-action preceded by a silent transition and also an *in*-action preceded by a silent transition is possible. □

In the remainder of this section we show that under certain conditions behavioural satisfaction and standard satisfaction coincide. The first condition is full abstraction; it expresses that observational equality and set-theoretic equality of elements are the same.

Definition 3 (Full abstraction). *An A-structure* $M = (W, R, w_0)$ *is* fully abstract *if for all* $w, w' \in W$ *it holds that* $w \approx_M w'$ *if and only if* $w = w'$.

The second condition is observational saturation; it expresses that all elements which are related by the τ-closure of an action a are already related by the action a itself. While the idea of full abstraction is well-known, we are not aware of a notion related to observational saturation.

Definition 4 (Observational saturation). *An A-structure* $M = (W, R, w_0)$ *is* observationally saturated *if for all* $a \in A$ *it holds that* $\widehat{R}_a = R_a$.

Obviously, observational saturation extends to composed actions $\alpha \in Act(A)$ (which can be shown by structural induction on the form of α).

Lemma 2. *Let* $M = (W, R, w_0)$ *be an observationally saturated A-structure. Then for all* $\alpha \in Act(A)$ *it holds that* $\widehat{R}_\alpha = R_\alpha$.

The following lemma is used to show that for fully abstract and observationally saturated structures there is no difference between behavioural and standard satisfaction.

Lemma 3. *Let* $M = (W, R, w_0) \in Str^{\mathcal{D}_\tau^\downarrow}(A)$ *be a fully abstract and observationally saturated A-structure. Then for any* $w \in W$*, valuation* $g : X \to W$ *and for any A-formula* φ*, we have*

$$M, g, w \models\!\approx_A^{\mathcal{D}_\tau^\downarrow} \varphi \iff M, g, w \models_A^{\mathcal{D}_\tau^\downarrow} \varphi \ .$$

Proof. The proof is performed by structural induction over the form of the formula φ. The only interesting cases are diamond and state variable formulas.

Case $\varphi = \langle\alpha\rangle\psi$: $M, g, w \mathrel{|\!\approx}_A^{\mathcal{D}_\tau^\downarrow} \langle\alpha\rangle\psi$ iff there is a $v \in W$ with $(w, v) \in \widehat{R}_\alpha$ and $M, g, v \mathrel{|\!\approx}_A^{\mathcal{D}_\tau^\downarrow} \psi$. Since M is observationally saturated, this is, by Lem. 2, equivalent to $(w, v) \in R_\alpha$ and $M, g, v \mathrel{|\!\approx}_A^{\mathcal{D}_\tau^\downarrow} \psi$. By induction hypothesis this is equivalent to $(w, v) \in R_\alpha$ and $M, g, v \models_A^{\mathcal{D}_\tau^\downarrow} \psi$ which is in turn equivalent to $M, g, w \models_A^{\mathcal{D}_\tau^\downarrow} \langle\alpha\rangle\psi$.

Case $\varphi = x$: $M, g, w \mathrel{|\!\approx}_A^{\mathcal{D}_\tau^\downarrow} x$ iff $g(x) \approx_M w$. Since M is fully abstract this is equivalent to $g(x) = w$ which is in turn equivalent to $M, g, w \models_A^{\mathcal{D}_\tau^\downarrow} x$. □

As a direct consequence of Lem. 3 we obtain the following theorem.

Theorem 1. *Let* $M = (W, R, w_0) \in Str^{\mathcal{D}_\tau^\downarrow}(A)$ *be a fully abstract and observationally saturated* A*-structure. Then, for all* $\varphi \in \mathrm{Sen}^{\mathcal{D}_\tau^\downarrow}(A)$*, we have that*

$$M \mathrel{|\!\approx}_A^{\mathcal{D}_\tau^\downarrow} \varphi \iff M \models_A^{\mathcal{D}_\tau^\downarrow} \varphi \ .$$

4 Behaviour-Abstractor Framework for $\mathcal{D}_\tau^\downarrow$-logic

Having defined abstractor and behavioural specifications over $\mathcal{D}_\tau^\downarrow$ an obvious question is whether their semantics can be related. For this purpose we will show that $\mathcal{D}_\tau^\downarrow$-logic and its observational interpretations give rise to an instantiation of the behaviour-abstractor framework introduced in [7].

4.1 Behaviour-Abstractor Framework

The concept of a behaviour-abstractor framework identifies a small but significant set of abstract requirements which are enough to define behavioural and abstractor specifications independently of a concrete logic and to study relationships between their semantics.

Definition 5 ([7]). *A* behaviour-abstractor framework $\mathrm{BA} = (\mathbb{S}, Str, \mathrm{Sen}, \models, \equiv, \mathrel{|\!\approx}, \mathcal{BB})$ *consists of*

- *a class* $\mathbb{S}$ *of* signatures*,*
- *a family* $Str = (Str(\Sigma))_{\Sigma\in\mathbb{S}}$ *of classes* $Str(\Sigma)$ *of* Σ-structures*,*
- *a family* $\mathrm{Sen} = (\mathrm{Sen}(\Sigma))_{\Sigma\in\mathbb{S}}$ *of sets* $\mathrm{Sen}(\Sigma)$ *of* Σ-sentences*,*
- *a family* $\models = (\models_\Sigma)_{\Sigma\in\mathbb{S}}$ *of* satisfaction relations $\models_\Sigma \subseteq Str(\Sigma) \times \mathrm{Sen}(\Sigma)$*,*
- *a family* $\equiv = (\equiv_\Sigma)_{\Sigma\in\mathbb{S}}$ *of* abstraction equivalences $\equiv_\Sigma \subseteq Str(\Sigma) \times Str(\Sigma)$*,*
- *a family* $\mathrel{|\!\approx} = (\mathrel{|\!\approx}_\Sigma)_{\Sigma\in\mathbb{S}}$ *of* behavioural satisfaction relations $\mathrel{|\!\approx}_\Sigma \subseteq Str(\Sigma) \times \mathrm{Sen}(\Sigma)$*, and*
- *a family* $\mathcal{BB} = (\mathcal{BB}_\Sigma)_{\Sigma\in\mathbb{S}}$ *of* black-box *functions* $\mathcal{BB}_\Sigma : Str(\Sigma) \to Str(\Sigma)$*,*

such that the following conditions (BA1–BA3) are satisfied for each signature $\Sigma \in \mathbb{S}$ *and for all* Σ*-structures* $M, M' \in Str(\Sigma)$*:*

(BA1) *if* $M \equiv_\Sigma M'$, *then* $M \models\!\!\approx_\Sigma \varphi \iff M' \models\!\!\approx_\Sigma \varphi$ *for all* $\varphi \in \mathrm{Sen}(\Sigma)$*;*
(BA2) $M \equiv_\Sigma \mathcal{BB}_\Sigma(M)$*;*
(BA3) $\mathcal{BB}_\Sigma(M) \models\!\!\approx_\Sigma \varphi \iff \mathcal{BB}_\Sigma(M) \models_\Sigma \varphi$ *for all* $\varphi \in \mathrm{Sen}(\Sigma)$.

The idea of an abstraction equivalence is to relate structures 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 (BA1) relates abstraction equivalence and behavioural satisfaction by requiring that abstraction equivalence preserves behavioural satisfaction of sentences. This means that behavioural satisfaction of sentences is invariant under abstraction equivalence. The black-box function constructs, for each Σ-structure M, a so-called *black-box view* of M. The intuitive idea is that $\mathcal{BB}_\Sigma(M)$ shows the observable behaviour of M abstracting away implementation details which are not visible for the user of a system. Of course, the black-box view of M should be equivalent to M according to the abstraction equivalence, and this is expressed by condition (BA2). Condition (BA3) formalises an intrinsic property of black-box views, for which behavioural satisfaction of sentences should be the same as ordinary satisfaction.

Given a behaviour-abstractor framework BA, a specification $Sp = (\Sigma, \Phi)$ over BA consists of a signature $\Sigma \in \mathbb{S}$ and a set $\Phi \subseteq \mathrm{Sen}(\Sigma)$ of Σ-sentences. The (ordinary) semantics of Sp is given by $\mathrm{Mod}(Sp) = \{M \in Str(\Sigma) \mid \forall \varphi \in \Phi \,.\, M \models_\Sigma \varphi\}$. On top of Sp an abstractor specification **abstract** Sp **wrt** $\equiv$ and a behavioural specification **behaviour** Sp **wrt** $\models\!\!\approx$ can be constructed with their model classes defined as follows:

$$\mathrm{Mod}(\textbf{abstract } Sp \textbf{ wrt } \equiv) = \{M \in Str(\Sigma) \mid \exists N \in \mathrm{Mod}(Sp) \,.\, M \equiv_\Sigma N\} \,,$$
$$\mathrm{Mod}(\textbf{behaviour } Sp \textbf{ wrt } \models\!\!\approx) = \{M \in Str(\Sigma) \mid \forall \varphi \in \Phi \,.\, M \models\!\!\approx_\Sigma \varphi\} \,.$$

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[5].

Theorem 2 ([7]). *Let* $\mathrm{BA} = (\mathbb{S}, Str, \mathrm{Sen}, \models, \equiv, \models\!\!\approx, \mathcal{BB})$ *be a behaviour-abstractor framework and* Sp *a specification over* BA.

1. $\mathrm{Mod}(\textbf{behaviour } Sp \textbf{ wrt } \models\!\!\approx) \subseteq \mathrm{Mod}(\textbf{abstract } Sp \textbf{ wrt } \equiv)$.
2. $\mathrm{Mod}(Sp) \subseteq \mathrm{Mod}(\textbf{behaviour } Sp \textbf{ wrt } \models\!\!\approx) \iff$
   $\mathrm{Mod}(\textbf{behaviour } Sp \textbf{ wrt } \models\!\!\approx) = \mathrm{Mod}(\textbf{abstract } Sp \textbf{ wrt } \equiv)$.

[5] It may sound strange that ordinary satisfaction does not always imply behavioural satisfaction but there are indeed some cases where this can happen; see Ex. 6.

4.2 Instantiation of the Behaviour-Abstractor Framework with $\mathcal{D}_\tau^\downarrow$

We can instantiate the behaviour-abstractor framework with the notions of $\mathcal{D}_\tau^\downarrow$-logic as follows. Signatures, structures, sentences and the (ordinary) satisfaction relation of $\mathcal{D}_\tau^\downarrow$ have been defined in Sect. 2; black-box functions are discussed below. As abstraction equivalences we use weak bisimulation (Def. 1) and the behavioural satisfaction relation is the one of Def. 2.

In the context of $\mathcal{D}_\tau^\downarrow$-logic, condition (BA1) of a behaviour-abstractor framework (cf. Def. 5) expresses modal invariance of A-sentences w.r.t. weak bisimulation equivalence and behavioural satisfaction. The proof of this modal invariance property relies on the following lemma which can be shown by structural induction over formulas (using Lem. 1 for the case of diamond formulas).

Lemma 4. *Let $M = (W, R, w_0)$ and $M' = (W', R', w_0')$ be two A-structures and $B \subseteq W \times W'$ a weak bisimulation. Then for any $w \in W, w' \in W'$ with $(w, w') \in B$, for any valuations $g : X \to W$, $g' : X \to W'$ with $(g(x), g'(x)) \in B$ for all $x \in X$, and for any A-formula φ, we have*

$$M, g, w \models\!\approx_A^{\mathcal{D}_\tau^\downarrow} \varphi \iff M', g', w' \models\!\approx_A^{\mathcal{D}_\tau^\downarrow} \varphi \ .$$

As a direct consequence of Lem. 4 we obtain the following theorem that verifies the first condition of a behaviour-abstractor framework.

Theorem 3. *For any $A \in \mathbb{S}^{\mathcal{D}_\tau^\downarrow}$ and for all $M, M' \in Str^{\mathcal{D}_\tau^\downarrow}(A)$,*

$(\mathrm{BA1}^{\mathcal{D}_\tau^\downarrow})$ *if $M \equiv_A^{\mathcal{D}_\tau^\downarrow} M$, then $\forall \varphi \in \mathrm{Sen}^{\mathcal{D}_\tau^\downarrow}(A) \,.\, M \models\!\approx_A^{\mathcal{D}_\tau^\downarrow} \varphi \iff M' \models\!\approx_A^{\mathcal{D}_\tau^\downarrow} \varphi$.*

Black-box function. To define the black-box view of an A-structure M we use the following quotient construction. It identifies observationally equal states and relates equivalence classes $[w]_{\approx_M}$ and $[v]_{\approx_M}$ by an action a if there are elements w' in $[w]_{\approx_M}$ and v' in $[v]_{\approx_M}$ which are related by the τ-closure of a (w.r.t. the transitions of M).

Definition 6 (Quotient structure). *Let $M = (W, R, w_0) \in Str^{\mathcal{D}_\tau^\downarrow}(A)$ be an A-structure. The* quotient of M *w.r.t. $\approx_M$ is the A-structure $M/\!\approx_M = (W/\!\approx_M, R/\!\approx_M, [w_0]_{\approx_M})$, where*

- $W/\!\approx_M = \{[w]_{\approx_M} \mid w \in W\}$ *with* $[w]_{\approx_M} = \{w' \mid w' \approx_M w\}$;
- $R/\!\approx_M = ((R/\!\approx_M)_a)_{a \in A}$ *with*

$$(R/\!\approx_M)_a = \{([w]_{\approx_M}, [v]_{\approx_M}) \mid \exists w' \in [w]_{\approx_M}, v' \in [v]_{\approx_M} \,.\, (w', v') \in \hat{R}_a\}$$

for any $a \in A$.

Since $\approx_M$ is an equivalence relation, $M/\!\approx_M$ is well-defined and any state $[w]$ is reachable from the initial one. For any $M \in Str^{\mathcal{D}_\tau^\downarrow}(A)$, the *black-box view* of M is defined by $\mathcal{BB}_A^{\mathcal{D}_\tau^\downarrow}(M) =_{\mathrm{def}} M/\!\approx_M$.

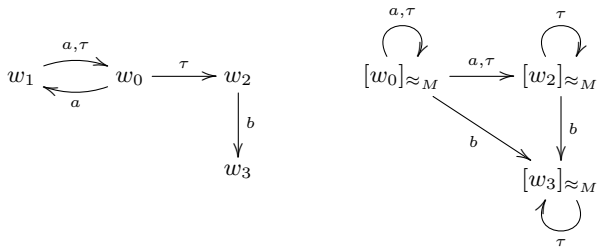

Fig. 3. A structure M and its quotient $M/{\approx_M}$

Example 4. Figure 3 shows an LTS M and its quotient $M/{\approx_M}$. By definition of quotients there is a τ-loop for each state $[w]_{\approx_M} \in M/{\approx_M}$. The states w_0 and w_2 of M are not observationally equivalent since the silent τ-transition from w_0 to w_2 removes the possibility to execute a. Hence the τ-transition remains in the quotient, now between the different states $[w_0]_{\approx_M}$ and $[w_2]_{\approx_M}$. □

The next theorem verifies the second condition of a behaviour-abstractor framework.

Theorem 4. *For any A-structure $M \in Str^{\mathcal{D}^{\downarrow}_{\tau}}(A)$, it holds*

$(\mathrm{BA2}^{\mathcal{D}^{\downarrow}_{\tau}})$ $M \equiv^{\mathcal{D}^{\downarrow}_{\tau}}_{A} \mathcal{BB}^{\mathcal{D}^{\downarrow}_{\tau}}_{A}(M)$.

Proof. It is straightforward, though somewhat technical, to show that the relation $B \subseteq W \times W/{\approx_M}$ with $B = \{(w, [w]_{\approx_M}) \mid w \in W\}$ is a weak bisimulation relation between M and $M/{\approx_M}$, and hence between M and $\mathcal{BB}^{\mathcal{D}^{\downarrow}_{\tau}}_{A}(M)$. □

Let us now consider the third condition of a behaviour-abstractor framework requiring that behavioural and standard satisfaction coincide for black-box structures in $\mathcal{D}^{\downarrow}_{\tau}$. For the proof we use the next two lemmas. The first one says that quotient structures, and hence black-box structures, are fully abstract.

Lemma 5. *For any $M = (W, R, w_0) \in Str^{\mathcal{D}^{\downarrow}_{\tau}}(A)$, $\mathcal{BB}^{\mathcal{D}^{\downarrow}_{\tau}}_{A}(M)$ is fully abstract, i.e., for all $w, w' \in W$ it holds that $[w]_{\approx_M} \approx_{\mathcal{BB}^{\mathcal{D}^{\downarrow}_{\tau}}_{A}(M)} [w']_{\approx_M}$ iff $[w]_{\approx_M} = [w']_{\approx_M}$.*

Proof. Only the direction "⇒" is not trivial. It is straightforward, but technical, to show that the relation $B \subseteq W \times W$ with

$$B = \{(w, w') \mid [w]_{\approx_M} \approx_{\mathcal{BB}^{\mathcal{D}^{\downarrow}_{\tau}}_{A}(M)} [w']_{\approx_M}\}$$

is a weak bisimulation relation between the states of M. Now, let $w, w' \in W$ such that $[w]_{\approx_M} \approx_{\mathcal{BB}^{\mathcal{D}^{\downarrow}_{\tau}}_{A}(M)} [w']_{\approx_M}$ holds. Then $(w, w') \in B$. Since $\approx_M$ is the greatest weak bisimulation relation on M we have $w \approx_M w'$ and therefore $[w]_{\approx_M} = [w']_{\approx_M}$. □

The second lemma says that quotient structures, and hence black-box structures, are observationally saturated.

Lemma 6. *For any $M = (W, R, w_0) \in Str^{\mathcal{D}^{\downarrow}_{\tau}}(A)$, $\mathcal{BB}^{\mathcal{D}^{\downarrow}_{\tau}}_{A}(M)$ is observationally saturated, i.e., for each $a \in A$,*

$$(\widehat{R/{\approx_M}})_a = (R/{\approx_M})_a.$$

Proof. Let us write $\widetilde{R}$ for $R/{\approx_M}$; $\widehat{\widetilde{R}}$ for $\widehat{R/{\approx_M}}$; and $\widetilde{w}$ for $[w]_{\approx_M}$. The claim then reads $\widehat{\widetilde{R}} = \widetilde{R}$. $\widetilde{R} \subseteq \widehat{\widetilde{R}}$ is obvious. For the converse inclusion, we first show for every $a \in A = O \cup \{\tau\}$

$(*)$ if $(\widetilde{w}_1, \widetilde{w}_2) \in \widetilde{R}_\tau$ and $(\widetilde{w}_2, \widetilde{w}_3) \in \widetilde{R}_a$, then $(\widetilde{w}_1, \widetilde{w}_3) \in \widetilde{R}_a$;

$(**)$ if $(\widetilde{w}_1, \widetilde{w}_2) \in \widetilde{R}_a$ and $(\widetilde{w}_2, \widetilde{w}_3) \in \widetilde{R}_\tau$, then $(\widetilde{w}_1, \widetilde{w}_3) \in \widetilde{R}_a$.

Indeed, for $(*)$, $(\widetilde{w}_1, \widetilde{w}_2) \in \widetilde{R}_\tau$ and $(\widetilde{w}_2, \widetilde{w}_3) \in \widetilde{R}_a$ imply that there are $v_1 \in \widetilde{w}_1$, $v_2, v_2' \in \widetilde{w}_2$, and $v_3' \in \widetilde{w}_3$ with $(v_1, v_2) \in \widehat{R}_\tau$ and $(v_2', v_3') \in \widehat{R}_a$. Since $v_2, v_2' \in \widetilde{w}_2$, we have $v_2 \approx_M v_2'$, and thus, by applying (weak-zig*) of Lem. 1 to $(v_2', v_3') \in \widehat{R}_a$, there is a $v_3 \in W$ with $(v_2, v_3) \in \widehat{R}_a$ and $v_3' \approx_M v_3$. Now $(v_1, v_2) \in \widehat{R}_\tau$ and $(v_2, v_3) \in \widehat{R}_a$ and hence $(v_1, v_3) \in \widehat{R}_a$. By $v_3 \approx_M v_3' \in \widetilde{w}_3$ we obtain $v_3 \in \widetilde{w}_3$ and thus $(\widetilde{w}_1, \widetilde{w}_3) \in \widetilde{R}_a$. The proof for $(**)$ is symmetric.

With these auxiliary facts we obtain, for $o \in O$ and writing the relation in infix notation,

$$\begin{aligned} \widetilde{w}_1 \mathrel{\widehat{\widetilde{R}}_o} \widetilde{w}_2 &\implies \widetilde{w}_1 \mathrel{\widetilde{R}_\tau} \cdot \ldots \cdot \mathrel{\widetilde{R}_\tau} \cdot \mathrel{\widetilde{R}_o} \cdot \mathrel{\widetilde{R}_\tau} \cdot \ldots \cdot \mathrel{\widetilde{R}_\tau} \widetilde{w}_2 \\ &\overset{(*)}{\implies} \widetilde{w}_1 \mathrel{\widetilde{R}_o} \cdot \mathrel{\widetilde{R}_\tau} \cdot \ldots \cdot \mathrel{\widetilde{R}_\tau} \widetilde{w}_2 \overset{(**)}{\implies} \widetilde{w}_1 \mathrel{\widetilde{R}_o} \widetilde{w}_2 \ . \end{aligned}$$

For $\widetilde{w}_1 \mathrel{\widehat{\widetilde{R}}_\tau} \widetilde{w}_2$ either $\widetilde{w}_1 = \widetilde{w}_2$ or there is a non-empty sequence $\widetilde{w}_1 \mathrel{\widetilde{R}_\tau} \cdot \ldots \cdot \mathrel{\widetilde{R}_\tau} \widetilde{w}_2$. In the first case, we note that $w_1 \hat{R}_\tau w_1$ and hence, by definition of quotients, $\widetilde{w}_1 \mathrel{\widetilde{R}_\tau} \widetilde{w}_1$. Since $\widetilde{w}_1 = \widetilde{w}_2$ we have $\widetilde{w}_1 \mathrel{\widetilde{R}_\tau} \widetilde{w}_2$. In the second case, either the sequence has length one and we are done or

$$\widetilde{w}_1 \mathrel{\widehat{\widetilde{R}}_\tau} \widetilde{w}_2 \implies \widetilde{w}_1 \mathrel{\widetilde{R}_\tau} \cdot \ldots \cdot \mathrel{\widetilde{R}_\tau} \widetilde{w}_2 \overset{(*)}{\implies} \widetilde{w}_1 \mathrel{\widetilde{R}_\tau} \widetilde{w}_2 \ . \qquad \square$$

Since $\mathcal{BB}^{\mathcal{D}^{\downarrow}_{\tau}}_{A}(M)$ is fully abstract and observationally saturated we can apply Thm. 5 such that we obtain the third condition of a behaviour-abstractor framework in the context of $\mathcal{D}^{\downarrow}_{\tau}$.

Theorem 5. *Let $M \in Str^{\mathcal{D}^{\downarrow}_{\tau}}(A)$. Then, for all $\varphi \in \mathrm{Sen}^{\mathcal{D}^{\downarrow}_{\tau}}(A)$, we have that*

$(\mathrm{BA3}^{\mathcal{D}^{\downarrow}_{\tau}})$ $\mathcal{BB}^{\mathcal{D}^{\downarrow}_{\tau}}_{A}(M) \mathrel{|\!\approx^{\mathcal{D}^{\downarrow}_{\tau}}_{A}} \varphi \iff \mathcal{BB}^{\mathcal{D}^{\downarrow}_{\tau}}_{A}(M) \mathrel{|\!=^{\mathcal{D}^{\downarrow}_{\tau}}_{A}} \varphi$.

Corollary 1. $\mathrm{BA}^{\mathcal{D}^{\downarrow}_{\tau}} = (\mathbb{S}^{\mathcal{D}^{\downarrow}_{\tau}}, \mathrm{Sen}^{\mathcal{D}^{\downarrow}_{\tau}}, Str^{\mathcal{D}^{\downarrow}_{\tau}}, \models^{\mathcal{D}^{\downarrow}_{\tau}}, \equiv^{\mathcal{D}^{\downarrow}_{\tau}}, \mathrel{|\!\approx^{\mathcal{D}^{\downarrow}_{\tau}}}, \mathcal{BB}^{\mathcal{D}^{\downarrow}_{\tau}})$ *is a behaviour-abstractor framework.*

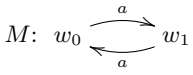

Fig. 4. $M \models_A^{\mathcal{D}_\tau^\downarrow} \downarrow x\,.\,\langle a\rangle\neg x$ but $M \not\approx_A^{\mathcal{D}_\tau^\downarrow} \downarrow x\,.\,\langle a\rangle\neg x$

We thus can instantiate Thm. 2 and get the respective relationships between behavioural and abstractor specifications in the context of $\mathcal{D}_\tau^\downarrow$-logic.

Corollary 2. *Let Sp be a specification over* $\mathcal{D}_\tau^\downarrow$.

1. $\mathrm{Mod}^{\mathcal{D}_\tau^\downarrow}(\textbf{behaviour } Sp \textbf{ wrt } \approx_A^{\mathcal{D}_\tau^\downarrow}) \subseteq \mathrm{Mod}^{\mathcal{D}_\tau^\downarrow}(\textbf{abstract } Sp \textbf{ wrt } \equiv_A^{\mathcal{D}_\tau^\downarrow})$
2. $\mathrm{Mod}^{\mathcal{D}_\tau^\downarrow}(Sp) \subseteq \mathrm{Mod}^{\mathcal{D}_\tau^\downarrow}(\textbf{behaviour } Sp \textbf{ wrt } \approx_A^{\mathcal{D}_\tau^\downarrow}) \iff$
$\mathrm{Mod}^{\mathcal{D}_\tau^\downarrow}(\textbf{behaviour } Sp \textbf{ wrt } \approx_A^{\mathcal{D}_\tau^\downarrow}) = \mathrm{Mod}^{\mathcal{D}_\tau^\downarrow}(\textbf{abstract } Sp \textbf{ wrt } \equiv_A^{\mathcal{D}_\tau^\downarrow})$

Example 5. We consider the specification *2Buf* of Ex. 1 with axiom φ. Since φ is a positive formula (not containing negation), for all A-structures N, $N \models_A^{\mathcal{D}_\tau^\downarrow} \varphi$ implies $N \approx_A^{\mathcal{D}_\tau^\downarrow} \varphi$. Hence, $\mathrm{Mod}^{\mathcal{D}_\tau^\downarrow}(2Buf) \subseteq \mathrm{Mod}^{\mathcal{D}_\tau^\downarrow}(\textbf{behaviour } 2Buf \textbf{ wrt } \approx_A^{\mathcal{D}_\tau^\downarrow})$. Therefore, by Cor. 2(2),

$$\mathrm{Mod}^{\mathcal{D}_\tau^\downarrow}(\textbf{behaviour } 2Buf \textbf{ wrt } \approx_A^{\mathcal{D}_\tau^\downarrow}) = \mathrm{Mod}^{\mathcal{D}_\tau^\downarrow}(\textbf{abstract } 2Buf \textbf{ wrt } \equiv_A^{\mathcal{D}_\tau^\downarrow})\ .$$ □

Let us still point out that the condition $\mathrm{Mod}^{\mathcal{D}_\tau^\downarrow}(Sp) \subseteq \mathrm{Mod}^{\mathcal{D}_\tau^\downarrow}(\textbf{behaviour } Sp \textbf{ wrt } \approx_A^{\mathcal{D}_\tau^\downarrow})$ in Cor. 2(2) does not always hold.

Example 6. (i) Consider the signature of *2Buf* and the sentence $\varphi' = \langle in\rangle\neg\langle in\rangle\mathbf{tt}$. Then, for the structure I in Fig. 2, we have $I \models_A^{\mathcal{D}_\tau^\downarrow} \varphi'$ but $I \not\approx_A^{\mathcal{D}_\tau^\downarrow} \varphi'$.
(ii) The $\{a\}$-structure M in Fig. 4 gives another example where standard satisfaction does not imply behavioural satisfaction. The reason is that w_0 and w_1 are different but observationally equal states. □

5 Concluding Remarks

We have studied two observational interpretations of $\mathcal{D}_\tau^\downarrow$-logic, a dynamic logic with binders and silent transitions. The two approaches, behavioural and abstractor specifications, follow the lines of an intensive study of behavioural and abstractor semantics in the area of algebraic specifications which has been taken up for reactive systems in [5]. The major result is that behavioural semantics, based on a behavioural satisfaction relation, and abstractor semantics, based on observational abstraction of model classes by weak bisimulation, coincide if and only if any standard model of a specification is a behavioural model as well. To establish this result we have shown that our logic instantiates the general,

logic-independent requirements of a behaviour-abstractor framework proposed in [7]. As a side-effect we get that behavioural satisfaction of $\mathcal{D}_\tau^\downarrow$-sentences is modally invariant under weak bisimulation.

There are several interesting research questions for future work. We want to integrate $\mathcal{D}_\tau^\downarrow$-logic and its observational interpretations in the development methodology for reactive systems suggested in [9]. This would involve explicit implementation constructors, e.g., for information hiding and parallel composition. Larger case studies and tools for validating the observational interpretations of $\mathcal{D}_\tau^\downarrow$-logic would be another issue. This would include the investigation of proof methods for deriving observational consequences from specifications. As an extension of our work we would like to integrate data states following the ideas of [6]. Moreover it would be interesting to see what would happen if we replace weak bisimulation by other equivalence notions like, e.g., branching bisimulation.

Acknowledgement. We would like to thank the anonymous reviewers of this work for valuable suggestions.

References

1. Michel Bidoit, Rolf Hennicker, and Martin Wirsing. Behavioural and abstractor specifications. *Sci. Comput. Program.*, 25(2–3):149–186, 1995.
2. Torben Braüner. *Hybrid Logic and its Proof-Theory.* App. Logic Series. Springer, 2010.
3. David Harel, Dexter Kozen, and Jerzy Tiuryn. *Dynamic Logic.* MIT Press, 2000.
4. Rolf Hennicker. Context induction: A proof principle for behavioural abstractions and algebraic implementations. *Formal Asp. Comput.*, 3(4):326–345, 1991.
5. Rolf Hennicker and Alexandre Madeira. Observational semantics for dynamic logic with binders. In *Rev. Sel. Papers 23rd IFIP WG 1.3 Intl. Ws. Recent Trends in Algebraic Development Techniques (WADT 2016)*, volume 10644 of *Lect. Notes Comp. Sci.*, pages 135–152. Springer, 2017.
6. Rolf Hennicker, Alexandre Madeira, and Alexander Knapp. A hybrid dynamic logic for event/data-based systems. In Reiner Hähnle and Wil M. P. van der Aalst, editors, *Proc. 22nd Intl. Conf. Fundamental Approaches to Software Engineering*, volume 11424 of *Lect Notes Comp. Sci.*, pages 79–97. Springer, 2019.
7. Rolf Hennicker, Alexandre Madeira, and Martin Wirsing. Behavioural and abstractor specifications revisited. *Theor. Comput. Sci.*, 741:32–43, 2018.
8. Martin Hofmann and Donald Sannella. On behavioural abstraction and behavioural satisfaction in higher-order logic. *Theor. Comput. Sci.*, 167(1&2):3–45, 1996.
9. 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, *Proc. 13th Intl. Conf. Theoretical Aspects of Computing (ICTAC 2016)*, volume 9965 of *Lect. Notes Comp. Sci.*, pages 422–440, 2016.
10. Robin Milner. *Communication and Concurrency.* Prentice Hall, 1989.
11. Michal Misiak. Behavioural semantics of algebraic specifications in arbitrary logical systems. In *Rev. Sel. Papers 17th Intl. Ws. Recent Trends in Algebraic Development Techniques (WADT 2004)*, volume 3423 of *Lect. Notes Comp. Sci.*, pages 144–161. Springer, 2004.

12. Pilar Nivela and Fernando Orejas. Initial behaviour semantics for algebraic specifications. In Donald Sannella and Andrzej Tarlecki, editors, *Rev. Sel. Papers 5th Intl. Ws. Recent Trends in Data Type Specification (WADT 1987)*, volume 332 of *Lect. Notes Comp. Sci.*, pages 184–207. Springer, 1988.
13. Horst Reichel. Behavioural equivalence — a unifying concept for initial and final specifications. In M. Arato and L. Varga, editors, *Proc. 3rd Hungarian Computer Science Conf.*, pages 27–39. Akademiai Kiado, 1981.
14. Horst Reichel. Behavioural validity of conditional equations in abstract data types. In *Proc. 3rd Vienna Conf. Contributions to General Algebra*, pages 301–324. B.G. Teubner, 1985.
15. Donald Sannella and Andrzej Tarlecki. On observational equivalence and algebraic specification. *J. Comput. Syst. Sci.*, 34(2-3):150–178, June 1987.
16. Donald Sannella and Martin Wirsing. A kernel language for algebraic specifications and implementations. In *Proc. Coll. Foundations of Computation Theory*, volume 158 of *Lect. Notes Comp. Sci.*, pages 413–427. Springer, 1983.
17. Colin Stirling. *Modal and Temporal Properties of Processes.* Springer Science Business Media New York, 2001.