Specifications with Observable Formulae and Observational Satisfaction Relation

Teodor KNAPIK

Laboratoire d'Informatique, URA 1327 du CNRS
Département de Mathématiques et d'Informatique
Ecole Normale Supérieure

LIENS - 92 - 14

June 1992

Specifications with Observable Formulae and Observational Satisfaction Relation

Teodor Knapik

LIENS CNRS URA 1327
45 Rue d'Ulm
F – 75230 PARIS Cedex 05 France

e-mail: knapik@dmi.ens.fr or knapik@frulm63.bitnet

Abstract

We consider algebraic specifications with observational features. Axioms as well as observations are formulae of full (Many-Sorted) First Order Logic with Equality. The associated semantics is based on a non standard interpretation of equality called **observational equality**. We study the adequacy of this semantics for software specification and the relationship with **behavioural equivalence of algebras**. We show that this framework defines an **institution**.

Keywords: algebraic specification, observability, semantics.

1 Introduction

Within an observational approach the loose semantics of a specification may either be defined as a class of algebras **observationally equivalent to models** satisfying the specification in the usual sense or as a class of algebras **observationally satisfying** the specification. The former way has already been deeply explored in [13] while in the latter one, the following problems remains open:

1. How to define an observational satisfaction relation w.r.t. more sophisticated observation techniques than sort observation ?

2. How to generalize the observational satisfaction relation of equational axioms of [10], positive conditional axioms of [14], [8] or [11], first order

axioms without existential quantifier nor predicate symbols of [1] or [3] to the full (Many Sorted) First Order Logic with Equality ?

3. Is it possible to provide an observational institution[1] in such a general framework ?

All these questions are investigated in the present paper. For the first one the answer was partially given in [14] and [1] where observable signatures are considered[2] and in [3] where observable terms (possibly with variables) are considered. In the present paper, observable (first order) formulae are considered. More precisely, a set of formulae represents available experiments. An experiment consists of checking the validity of a formula in an algebra for a given assignment of variables. Thus each value is involved only in some experiments. We assume that only the results of such experiments provide an information on what an algebra resembles. It is then impossible to distinguish some values from the others. This is represented by an indistinguishability relation defined according to the following **Indistinguishability Assumption**:

> *Two values are indistinguishable with respect to some experiments when it is impossible to see if they are different using the results of these experiments.*

We show that our indistinguishability relation is neither a congruence nor an equivalence relation. We do not think that this is unfortunate. This fact seems rather necessary in order to model the real situations in a better way, for instance the following ones:

1. A specification of sets of natural numbers may be additionally equipped with an operation *choose* which takes a set as argument and returns an element of the set. Sequences over $\mathbb{N}$ should clearly be considered as a correct realization of this specification, *choose* being for instance an operation which returns the head of a sequence. Then the sequences mn and nm are indistinguishable since they represent the same set $\{m, n\}$. But when $n \neq m$ we want the results of $choose(nm)$ and $choose(mn)$ (i.e. n and m) to be distinguishable.

2. Given a specification of something like a metric space, we may want to consider as indistinguishable two elements which are very close, (let

[1] See [7] for more details about institutions.

[2] In fact these approaches combine signature and sort observations.

us say a and b indistinguishable iff $||\mathsf{a} - \mathsf{b}|| \leq \varepsilon$, for some fixed ε). Such a relation is clearly non transitive.

Another surprising fact is that the indistinguishability relation is not compatible with the predicates as illustrated by the following example:

spec : OPT-SET **use :** CONST **sort :** set **generated by :** $\emptyset$: $\rightarrow$ set add: Const set $\rightarrow$ set **predicates :** $\_ \in \_$: Const set **axioms :** $\mathsf{optional(e)} \Rightarrow \mathsf{add(e,s)} = \mathsf{s}$ $\neg(\mathsf{e} \in \emptyset)$ $\neg\mathsf{optional(e)} \Rightarrow$ $(\mathsf{e} \in \mathsf{add(e',s)} \Leftrightarrow$ $\mathsf{e} = \mathsf{e'} \vee \mathsf{e} \in \mathsf{s})$ **observations :** $\mathsf{optional(e)} \vee \mathsf{e} \in \mathsf{s}$	**spec :** CONST **sort :** Const **generated by :** $\mathsf{a}_1, \ldots, \mathsf{a}_\mathsf{n}$: $\rightarrow$ Const $\mathsf{b}_1, \ldots, \mathsf{b}_\mathsf{m}$: $\rightarrow$ Const **predicates :** optional : Const particular : Const **axioms :** $\mathsf{optional(a_1)}, \ldots$ $\ldots, \mathsf{optional(a_n)}$ $\neg\mathsf{optional(b_1)}, \ldots$ $\ldots, \neg\mathsf{optional(b_m)}$ *“Some axioms about* particular” **observations :** x=y

Figure 1.1: Specification OPT-SET

Example 1.1

Figure 1.1 is an attempt to specify a data type (sort set*) whose elements are sets of some constants (sort* Const*). Some of these constants should be considered as optional in the sense that if* optional(c) *holds then add*$(c, \{c_1, \ldots, c_n\})$ *does not necessarily returns* $\{c, c_1, \ldots, c_n\}$*; it may also return* $\{c_1, \ldots, c_n\}$*. We may then consider a realization by the sets with the usual membership but unusual* add*: non optional constants are always added while the optional ones are added only if some other properties are satisfied (e.g.* particular(c)*). We will show later that in this realization two sets are indistinguishable if they have the same non optional elements. Consequently, the indistinguishability relation is not compatible with “*$\in$*” since,* *for instance, $\emptyset$ and any singleton set $\{e\}$ with an optional e are indistinguishable, whereas the realization under consideration satisfies $e \in \{e\}$ but not $e \in \emptyset$.*

In contrast to the non transitivity and the non compatibility with operations or with predicate symbols, another property causes a serious problem for the indistinguishability relation. In general, the indistinguishability relation is not "transported" through the forgetful functor. This, in part, provides an answer for the third question mentioned at the beginning of the introduction: an institution may be established under some restrictions on the category of signatures. Our institution for observational specifications requires signature morphisms to be injective. However **without such a restriction** our formalism is still a "semi-institution" (only the if part of the Satisfaction Condition holds). This is probably our main contribution since with all the definitions of observational satisfaction relation preceding [3], such a result requires at least the restriction to positive conditional axioms with observable preconditions. In our approach such a restriction is not necessary anymore, due to the following idea. We define observational algebras as usual algebras equipped with an additional equivalence relation called **observational equality** which is used as a non standard interpretation of equality. Moreover, we require an observational equality to be included in the indistinguishability relation. (Thus, in our example of metric-like space, observational equality provides a tiling of space such that the longest distance between two points in a same tile is less than ε.) Unlike the indistinguishability relation, an observational equality is of course "transported" by the forgetful functor.

It is important to notice that, similarly to the indistinguishability relation, an observational equality is not necessarily a congruence. This choice allows more realistic realizations of observational specifications and may be motivated by examples such as sets with choose or similar to 1.1. Consequently with our observational semantics, if in a specification one writes the axiom a = b together with f(a) $\neq$ f(b), such a specification may have a model. This points out that approaches with an observational satisfaction relation may have the advantage to be fully observational over the approaches based on the observational equivalence of algebras, where unfortunately some observational features are directly based on the usual ones. In particular, in these approaches observational consistency always coincide with the usual one whereas in ours, a specification being inconsistent (in the usual sense) may still have observational models. (An example of such specifications may be found in [3] or [2].)

In this paper some proofs have been presented in a reduced form. Complete proofs may be found in [2].

2 Algebraic and Logic Preliminaries

We assume that the reader is familiar with algebraic specifications (see e.g. [6] or [9]). A **signature $\boldsymbol{\Sigma}$** consists of a finite set S of **sorts** and a finite set of **operation** and **predicate** names with **arities**, ambiguously denoted by $\boldsymbol{\Sigma}$. We assume that each signature Σ is provided with an S-sorted set of variables X such that $\mathrm{X_s}$ is countable for each $\mathrm{s} \in \mathrm{S}$. We use the following conventions. Given a signature Σ (resp. Σ'), S (resp. S') denotes the sorts of Σ (resp. Σ') and X (resp. X') denotes the variables of Σ (resp. Σ'). A **signature morphism** $\sigma : \Sigma \to \Sigma'$ maps each sort of S to a sort of S', each operation $(\mathrm{f} : \mathrm{s_1} \ldots \mathrm{s_n} \to \mathrm{s}) \in \Sigma$ to an operation $\sigma(\mathrm{f})$ of Σ' with the arity $\sigma(\mathrm{s_1}) \ldots \sigma(\mathrm{s_n}) \to \sigma(\mathrm{s})$, each predicate $(\mathrm{q} : \mathrm{s_1} \ldots \mathrm{s_n}) \in \Sigma$ to a predicate $\sigma(\mathrm{q})$ of Σ' with the arity $\sigma(\mathrm{s_1}) \ldots \sigma(\mathrm{s_n})$ and each variable of $\mathrm{X_s}$ to a variable of $\mathrm{X}'_{\sigma(\mathrm{s})}$. Moreover, we assume that a signature morphism is always injective on variables[1].

Remark 2.1

Our approach to variables is slightly different than the one of [7] *(page* 36*, Definition* 55 *of* [7]*) where the authors consider an* S*-sorted set of variables as a map* $\mathrm{X} : \mathcal{X} \to \mathrm{S}$ *from a fixed set* $\mathcal{X}$ *of variable symbols to sorts. In presence of* $\sigma : \Sigma \to \Sigma'$*, variables used for* Σ'*-formulae are defined in* [7] *as* $\mathrm{X}' = \mathrm{X};\sigma$*. In other words, the authors of* [7] *assume that signature morphisms are always bijective on variables. Consequently, in their approach, there are no variables of sorts* $\mathrm{S}' \setminus \sigma(\mathrm{S})$*. This seems to us a bit restrictive.*

Since we deal with predicate symbols, our Σ-algebras are usual **(total)** Σ-algebras equipped additionally with relations $q^A \subseteq A_{\mathrm{s_1}} \times \ldots \times A_{\mathrm{s_n}}$ for each predicate symbol $(\mathrm{q} : \mathrm{s_1} \ldots \mathrm{s_n}) \in \Sigma$. Consequently, a **$\boldsymbol{\Sigma}$-morphism** in our sense is any usual Σ-morphism $\mu : A \to B$ which additionally satisfies

[1] Without this assumption, which in a stronger form appears in [7], it would be impossible to establish that $A' \models \sigma(\mathrm{x} = \mathrm{y})$ iff $A'|_{\sigma} \models \mathrm{x} = \mathrm{y}$, for instance with $\sigma(\mathrm{x} = \mathrm{y}) = (\mathrm{x}' = \mathrm{x}')$.

the following condition:

$$\forall\ a_1 \in A_{\mathrm{s}_1}, \ldots, a_{\mathrm{n}} \in A_{\mathrm{s}_{\mathrm{n}}}\ \ \langle a_1, \ldots, a_{\mathrm{n}}\rangle \in q^A\ \Rightarrow\ \langle \mu(a_1), \ldots, \mu(a_{\mathrm{n}})\rangle \in q^B$$

The **category of $\boldsymbol{\Sigma}$-algebras** is denoted by **Alg[$\boldsymbol{\Sigma}$]**. Given a signature morphism $\sigma : \Sigma \rightarrow \Sigma'$ the **$\boldsymbol{\sigma}$-reduct** of a Σ'-algebra A', written $\boldsymbol{A'}_{|_\sigma}$ is defined in the usual way (with $q^{A'_{|\sigma}} = \sigma(q)^{A'}$ for each predicate symbol q $\in \Sigma$) and extending it on Σ'-morphisms we obtain the **forgetful functor** $\_{|_\sigma} : \mathrm{Alg}[\Sigma'] \rightarrow \mathrm{Alg}[\Sigma]$.

Given an S-sorted set E, we denote by $\mathbf{T_\Sigma(E)}$ the free Σ-algebra over E. For instance $\mathbf{T_\Sigma}$ (resp. $\mathbf{T_\Sigma(X)}$) denotes the **$\boldsymbol{\Sigma}$-algebra of ground terms** (resp. **terms with variables**), $\mathbf{T_\Sigma}(\boldsymbol{A})$ (resp. $\mathbf{T_\Sigma}(\boldsymbol{A}\cup\mathbf{X})$) denotes the **$\boldsymbol{\Sigma}$-algebra of ground terms** (resp. **terms with variables**) **over the carriers of a $\boldsymbol{\Sigma}$-algebra $\boldsymbol{A}$.** Notice that if A is a free algebra then we have necessarily $q^A = \emptyset$ for any predicate symbol q.

A **valuation** is a morphism $\nu : \mathrm{X} \rightarrow A$ which maps each $\mathrm{x} \in \mathrm{X_s}$ to a value $\mathrm{x}\nu \in A_{\mathrm{s}}$. A **partial valuation** is a valuation preceded by an inclusion $\mathrm{X}_0 \subseteq \mathrm{X}$. The set of all valuations (resp. partial valuations) from X to A is written **Val[X,$\boldsymbol{A}$]** (resp. **PVal[X,$\boldsymbol{A}$]**). From the freeness of $\mathrm{T}_\Sigma(\mathrm{X})$ any valuation (resp. partial valuation) ν followed by the inclusion $A \subseteq \mathrm{T}_\Sigma(A)$ (resp. $A \subseteq \mathrm{T}_\Sigma(A \cup \mathrm{X})$) extends to a unique morphism (written ambiguously ν) from $\mathrm{T}_\Sigma(\mathrm{X})$ to $\mathrm{T}_\Sigma(A)$ (resp. $\mathrm{T}_\Sigma(A \cup \mathrm{X})$) which maps each term $\mathrm{t} \in (\mathrm{T}_\Sigma(\mathrm{X}))_{\mathrm{s}}$ to a **valued term** $\mathrm{t}\nu \in (\mathrm{T}_\Sigma(A))_{\mathrm{s}}$ (resp. **partially valued term** $\mathrm{t}\nu \in (\mathrm{T}_\Sigma(A \cup \mathrm{X}))_{\mathrm{s}}$). The **evaluation morphism** from $\mathrm{T}_\Sigma(A)$ to A is defined as the unique Σ-morphism which maps each element of $(\mathrm{T}_\Sigma(A))_{\mathrm{s}} \cap A_{\mathrm{s}}$ to itself. This morphism maps a valued term τ to its **evaluation result** written $\overline{\boldsymbol{\tau}}$.

From $\mathrm{T}_\Sigma(\mathrm{X})$, predicate symbols (including equality), connectives $(\neg, \wedge, \vee, \Rightarrow$, etc.) and quantifiers $(\forall, \exists)$, we construct the **set $\mathbf{Wff_\Sigma(X)}$** of **well formed $\boldsymbol{\Sigma}$-formulae**. Given $\varphi \in \mathrm{Wff}_\Sigma(\mathrm{X})$ among the variables of φ (written **Var[$\boldsymbol{\varphi}$]**) we distinguish between **free** and **bound variables**, both being defined in the usual way. We assume that there are no clashes between them in a formula (otherwise variables are properly renamed). A valuation $\nu : \mathrm{X} \rightarrow A$ may also be applied to a formula φ. We then define valued formulae (resp. partially valued formulae) as follows

$$\begin{array}{rrcl} & \mathrm{Wff}_\Sigma(A) & = & \{\varphi\nu \mid \varphi \in \mathrm{Wff}_\Sigma(\mathrm{X}),\ \nu \in \mathrm{Val}[\mathrm{X}, A]\} \\ (\text{resp.} & \mathrm{Wff}_\Sigma(A \cup \mathrm{X}) & = & \{\varphi\nu \mid \varphi \in \mathrm{Wff}_\Sigma(\mathrm{X}),\ \nu \in \mathrm{PVal}[\mathrm{X}, A]\}) \end{array}$$

Satisfaction relation between Σ-algebras and Σ-formulae is the usual one of (Many Sorted) First Order Logic with Equality. We may also write $A \models \vartheta$ for $\vartheta \in \mathrm{Wff}_\Sigma(A)$ and $A \in \mathrm{Alg}[\Sigma]$, that is we extend the usual notion of satisfaction relation on valued formulae in the following way: elements of A appearing in ϑ are considered as constants interpreted by themselves. The extension of a signature morphism $\sigma : \Sigma \to \Sigma'$ on formulae is ambiguously denoted by $\boldsymbol{\sigma}$. Given a Σ'-algebra A' we also use σ to denote the extension of a signature morphism on valued formulae, namely $\sigma : \mathrm{T}_\Sigma(A'_{|\sigma}) \to \mathrm{T}_{\Sigma'}(A')$.

Definition 2.2

Given a signature morphism $\sigma : \Sigma \to \Sigma'$ *and a* Σ'*-algebra* A'*, we define a* **$\boldsymbol{\sigma}$-reduct of a valuation** $\nu' : \mathrm{X}' \to A'$ *as a valuation* $\nu'_{|\sigma} : \mathrm{X} \to A'_{|\sigma}$ *satisfying:*

$$\forall\ \mathrm{x} \in \mathrm{X} \quad \sigma(\mathrm{x})\nu' = \mathrm{x}\nu'_{|\sigma}$$

Moreover given $\nu : \mathrm{X} \to A'_{|\sigma}$ *we denote by* $\boldsymbol{\sigma(\nu)}$ *the class of all valuations* $\nu' : \mathrm{X}' \to A'$ *such that* $\nu'_{|\sigma} = \nu$.

Remark 2.3

Since our approach to variables is slightly different than the one of [7] *(see Remark* 2.1*) we do not have a one to one map between* $\mathrm{Val}[\mathrm{X}, A'_{|\sigma}]$ *and* $\mathrm{Val}[\mathrm{X}', A']$*. In order to reuse the results of* [7] *about Satisfaction Condition in various institutions we translate our approach to variables in the Goguen's and Burstall's one as follows: we consider the quotient of* $\mathrm{Val}[\mathrm{X}', A']$ *by the equivalence relation determined by* $\nu'_{|\sigma} = \mu'_{|\sigma}$*. Consequently there is a one to one map between* $\mathrm{Val}[\mathrm{X}, A'_{|\sigma}]$ *and this quotient. Thus any "logical system" which is an institution in a* [7]*-like approach to variables is also an institution in our approach to variables due to the following lemma:*

Lemma 2.4

Let φ *be a* Σ*-formula with* $\mathrm{Var}[\varphi] = \mathrm{X}_0$ *and* A *be a* Σ*-algebra. Two valuations which differ on* $\mathrm{X} \setminus \mathrm{X}_0$ *have the same effect on the truth of* φ*. In particular for a signature morphism* $\sigma : \Sigma \to \Sigma'$ *and a* Σ'*-algebra* A'*,* *any valuations $\nu', \mu' \in \mathrm{Val}[\mathrm{X}', A']$ such that $\mu'|_{\sigma} = \nu'|_{\sigma}$ are both solutions (that is valuations which make the formula true) of the same formulae of $\sigma(\mathrm{Wff}_{\Sigma}(\mathrm{X}))$. In other words for any $\nu : \mathrm{X} \to A'|_{\sigma}$ and any $\varphi \in \mathrm{Wff}_{\Sigma}(\mathrm{X})$ we have that either all elements of the class $\sigma(\nu)$ are solutions of $\sigma(\varphi)$ or none of them are.* □

Also the following result may be deduced from Goguen's and Burstall's proof of Satisfaction Condition for (Many-Sorted) Equational Logic:

Fact 2.5

Let $\sigma : \Sigma \to \Sigma'$ be a signature morphism and A' be a Σ'-algebra. For any valued term $\tau \in \mathrm{T}_{\Sigma}(A'|_{\sigma})$ we have $\overline{\sigma(\tau)} = \overline{\tau}$. □

3 Indistinguishable Elements

As mentioned in the introduction we need to define an indistinguishability relation on the carriers of an algebra in order to loosen the satisfaction relation. Usually this is done using the concept of observable contexts. Since we observe formulae, we consider **contextual formulae** instead of contexts. The definition of contextual formula requires some additional notations. We assume that a formula φ can be represented by a tree. A **term position** p in φ is a sequence of integers which describe the path from the topmost position of φ to the considered term in φ written $\boldsymbol{\varphi|_{\mathrm{p}}}$. The replacement of $\varphi|_{\mathrm{p}}$ by a term t in φ is written $\boldsymbol{\varphi[\mathrm{t}]_{\mathrm{p}}}$.

Definition 3.1

Given sorts $\mathrm{S} = \{\mathrm{s}_1, \ldots, \mathrm{s}_\mathrm{n}\}$ the **set of contextual variables** *is the (S-indexed) set $\Diamond = \{\diamond_{\mathrm{s}_1}, \ldots \diamond_{\mathrm{s}_\mathrm{n}}\}$ with $\{\diamond_{\mathrm{s}_\mathrm{i}}\}$ being called the* **contextual variable of sort $\mathbf{s_i}$**. *A* **contextual formula** *over a Σ-algebra A is a partially valued formula ϑ with only one variable being both contextual and free. Consequently, the set of all contextual formulae over A, written $\mathbf{Cf}_{\boldsymbol{\Sigma}}(\boldsymbol{A})$ is defined as follows:*

$$\mathrm{Cf}_{\Sigma}(A) = \bigcup_{\mathrm{s}\in\mathrm{S}} \mathrm{Wff}_{\Sigma}(A \cup \{\diamond_{\mathrm{s}}\})$$

The application of $\xi \in \mathrm{Wff}_{\Sigma}(A \cup \{\diamond_{\mathrm{s}}\})$ on $a \in A_{\mathrm{s}}$ is written $\boldsymbol{\xi[a]}$.

Our meta-concept of observation is that for each element a of an algebra, there is a set of experiments in which a may be involved. We call such a set

observers of $\boldsymbol{a}$. Here, an observer of a is some contextual formulae ξ and the corresponding experiment is the truth of $\xi[a]$. In order to define what the observers of a are, we first need two auxiliary definitions:

Definition 3.2

Let A be a Σ-algebra. We define the **partial evaluation relation**, *written* $\underset{\mathbf{pEv}}{\rightarrow}$, *on* $\mathrm{Wff}_\Sigma(A)$ *as follows. We say that a formula* $\vartheta_2 \in \mathrm{Wff}_\Sigma(A)$ *is the result of the partial evaluation of* $\vartheta_1 \in \mathrm{Wff}_\Sigma(A)$, *written* $\boldsymbol{\vartheta_1 \underset{\mathbf{pEv}}{\rightarrow} \vartheta_2}$, *if there is a term position* p *in* ϑ_1 *satisfying* $\mathrm{Var}[\vartheta_1|_\mathrm{p}] = \emptyset$ *and such that* $\vartheta_1[\overline{\vartheta_1|_\mathrm{p}}]_\mathrm{p} = \vartheta_2$.

The requirement $\mathrm{Var}[\vartheta_1|_\mathrm{p}] = \emptyset$ may seem strange. This is necessary, since given $\varphi \in \mathrm{Wff}_\Sigma(\mathrm{X})$ only the free variables of φ can be mapped to A. Consequently we assume that when applied to φ, a valuation ν is implicitly preceded by the inclusion "free variables of φ" $\subseteq$ X. For instance if ν which maps x to a and y to b is applied on a formula $\exists\ \mathrm{y}\ \mathrm{x} \leq \mathrm{y}$ we obtain $\exists\ \mathrm{y}\ a \leq \mathrm{y}$ and not $\exists\ b\ a \leq b$. Thus given a valued formula ϑ, in general we do not have $\mathrm{Var}[\vartheta] = \emptyset$.

Definition 3.3

Let $\Phi \subseteq \mathrm{Wff}_\Sigma(\mathrm{X})$ *be a set of formulae and* A *be a* Σ*-algebra. The* **closure by partial evaluations of $\boldsymbol{\Phi}$ in $\boldsymbol{A}$**, *written* $\boldsymbol{\widetilde{\Phi}^A}$, *is defined as follows:*

$$\widetilde{\Phi}^A = \{\vartheta \in \mathrm{Wff}_\Sigma(A) \ \mid\ \exists\ \varphi \in \Phi\ \ \exists\ \nu : \mathrm{X} \rightarrow A \quad \varphi\nu \overset{*}{\underset{\mathrm{pEv}}{\rightarrow}} \vartheta\}$$

where $\overset{*}{\underset{\mathbf{pEv}}{\rightarrow}}$ *denotes the reflexive-transitive closure of* $\underset{\mathrm{pEv}}{\rightarrow}$.

Now if Φ is a set of observable formulae, $\widetilde{\Phi}^A$ provides an information about experiments in which a may by involved:

Definition 3.4

Let $\Phi \subseteq \mathrm{Wff}_\Sigma(\mathrm{X})$ *be a set of formulae which we call* **observable formulae** *and* a *be an element of a* Σ*-algebra* A*. We say that a contextual formula* $\xi \in \mathrm{Cf}_\Sigma(A)$ *is a* **$\boldsymbol{\Phi}$-observer of $\boldsymbol{a}$** *(an observer of* a*, in short) if* $\xi[a] \in \widetilde{\Phi}^A$*. The set of* Φ*-observers of* a *is written* $\mathbf{obs}_\Phi(\boldsymbol{a})$.

Once we know which experiments can be made on a value a, we want to know how to compare their results with the ones made on another value b. We claim that only common observers of a and b (called comparators) may be used for this purpose:

Definition 3.5

A **Φ-comparator** *(comparator, in short) of elements a and b of a given carrier of a Σ-algebra, is any Φ-observer of a and b. The set of all comparators of both a and b is denoted by* $\mathbf{cmp}_{\Phi}(\boldsymbol{a}, \boldsymbol{b})$. *We say that a Φ-comparator ξ* **distinguishes** *a and b iff $A \not\models \xi[a] \Leftrightarrow \xi[b]$.*

We can now state the following definition of indistinguishability:

Definition 3.6

We say that two elements a and b of a given carrier of a Σ-algebra are **indistinguishable** *w.r.t. a set of formulae $\Phi \in \mathrm{Wff}_{\Sigma}(\mathrm{X})$ (or* **Φ-indistinguishable***) written $\boldsymbol{a} \sim_{\Phi} \boldsymbol{b}$, if there is no Φ-comparator which distinguishes them.*

We illustrate these concepts by the following example:

Example 3.7

Consider an algebra $\boldsymbol{L}$ of sets over the signature of OPT-SET *(see Figure* 1.1*) with the usual membership test and with the following* add*:*

$$add^L(c, \{c_1, \ldots, c_n\}) = \begin{cases} \{c, c_1, \ldots, c_n\} & \text{if } c \in particular^L \text{ or } c \notin optional^L \\ \{c_1, \ldots, c_n\} & \text{otherwise} \end{cases}$$

that is any non optional constant is always added to a set and optional ones are added only if they are particular. The set of observable formulae Opt *of this specification is* $\{\mathsf{optional(x)} \vee \mathsf{x} \in \mathsf{s}\}$. *Applying the definition we obtain*

$$\widetilde{\mathsf{Opt}}^L = \{\mathsf{optional}(c) \ \vee \ c \in l \mid c \in L_{\mathsf{Const}}, l \in L_{\mathsf{Set}}\}$$

Consequently any $l \in L_{\mathsf{Set}}$ has the same observers $\{\mathsf{optional}(c) \vee c \in \diamond \mid c \in L_{\mathsf{Const}}\}$. Such an observer may only distinguish two sets which differ on non optional elements.

As mentioned in Introduction, we would like to present an institution for observational specifications. Since our observational satisfaction relation (which will be defined further) strongly depends on observers we must first study their properties w.r.t. the forgetful functor and the translation of observable formulae. In this way, we shall provide tools which will be useful to show that the Satisfaction Condition holds in our formalism. Below we give the first important theorem. It is a good occasion to establish some interesting lemmas about partial evaluation.

Theorem 3.8

Let $\sigma : \Sigma \to \Sigma'$ be a signature morphism, $\Phi \subseteq \mathrm{Wff}_{\Sigma}(\mathrm{X})$ and $\Phi' \subseteq \mathrm{Wff}_{\Sigma'}(\mathrm{X}')$ be sets of formulae such that $\sigma(\Phi) \subseteq \Phi'$ and A' be a Σ'-algebra. For any element $a \in A'_{|\sigma}$ and any contextual formula $\xi \in \mathrm{Cf}_{\Sigma(A'_{|\sigma})}$ we have

$$\xi \in \mathrm{obs}_{\Phi}(a) \quad \Rightarrow \quad \sigma(\xi) \in \mathrm{obs}_{\Phi'}(a)$$

We need the following lemmas for the proof:

Lemma 3.9

Let $\sigma : \Sigma \to \Sigma'$ be a signature morphism, and A' be a Σ'-algebra. For any $\vartheta_1, \vartheta_2 \in \mathrm{Wff}_{\Sigma}(A'_{|\sigma})$ we have:

$$\vartheta_1 \underset{\mathrm{pEv}}{\overset{*}{\rightarrow}} \vartheta_2 \quad \Rightarrow \quad \sigma(\vartheta_1) \underset{\mathrm{pEv}}{\overset{*}{\rightarrow}} \sigma(\vartheta_2)$$

Proof

Follows directly from Definition 3.2 and Fact 2.5. □

Lemma 3.10

Let $\sigma : \Sigma \to \Sigma'$ be a signature morphism, $\Phi \subseteq \mathrm{Wff}_{\Sigma}(\mathrm{X})$ and $\Phi' \subseteq \mathrm{Wff}_{\Sigma'}(\mathrm{X}')$ be sets of formulae such that $\sigma(\Phi) \subseteq \Phi'$ and A' be a Σ'-algebra. For any $\vartheta \in \mathrm{Wff}_{\Sigma}(A'_{|\sigma})$ we have:

$$\vartheta \in \widetilde{\Phi}^{A'_{|\sigma}} \quad \Rightarrow \quad \sigma(\vartheta) \in \widetilde{\Phi'}^{A'}$$

Proof

Assume $\vartheta \in \widetilde{\Phi}^{A'_{|\sigma}}$. By Definition 3.3 we have $\exists\, \varphi \in \Phi \;\; \exists\, \nu : \mathrm{X} \to A'_{|\sigma} \quad \varphi\nu \underset{\mathrm{pEv}}{\overset{*}{\rightarrow}} \vartheta$. By Lemma 3.9 we obtain

$$\exists\, \varphi \in \Phi \;\; \exists\, \nu : \mathrm{X} \to A'_{|\sigma} \quad \sigma(\varphi\nu) \underset{\mathrm{pEv}}{\overset{*}{\rightarrow}} \sigma(\vartheta) \qquad \text{(i)}$$

It is obvious from Definition 2.2 that for any $\nu' \in \sigma(\nu)$ we have $\sigma(\varphi\nu) = \sigma(\varphi)\nu'$. Let $\varphi' = \sigma(\varphi)$ then from (i), we deduce: $\exists\, \varphi' \in \Phi' \;\; \exists\, \nu' : \mathrm{X} \to A' \quad \varphi'\nu' \underset{\mathrm{pEv}}{\overset{*}{\rightarrow}} \sigma(\vartheta)$. By Definition 3.3 this yields $\sigma(\vartheta) \in \widetilde{\Phi'}^{A'}$. □

Proof of Theorem 3.8

Let $\sigma : \Sigma \rightarrow \Sigma'$ be a signature morphism, $\Phi \subseteq \mathrm{Wff}_\Sigma(\mathrm{X})$ and $\Phi' \subseteq \mathrm{Wff}_{\Sigma'}(\mathrm{X}')$ be sets of formulae such that $\sigma(\Phi) \subseteq \Phi'$ and A' a be Σ'-algebra. Let $a \in A'_{|_\sigma}$ and assume $\xi \in \mathrm{obs}_\Phi(a)$. By Definition 3.4 we have $\xi[a] \in \widetilde{\Phi}^{A'_{|_\sigma}}$, hence by Lemma 3.10 we deduce $\sigma(\xi[a]) \in \widetilde{\Phi'}^{A'}$. By Definition 3.4 this yields $\sigma(\xi) \in \mathrm{obs}_{\Phi'}(a)$. □

Note that the converse of the above theorem does not hold even if $\sigma(\Phi) = \Phi'$:

Example 3.11

Consider the signatures $\Sigma = \{\mathrm{q}_1, \mathrm{q}_2 : \mathrm{s}\}$ and $\Sigma' = \{\mathrm{q}' : \mathrm{s}'\}$. Let $\Phi = \{\mathrm{q}_1(\mathrm{x})\}$. Consider $\sigma : \Sigma \rightarrow \Sigma'$ such that $\sigma(\mathrm{s}) = \mathrm{s}'$ and $\sigma(\mathrm{q}_1) = \sigma(\mathrm{q}_2) = \mathrm{q}'$. It is clear that for any Σ'-algebra A', $\mathrm{q}_2(\diamond)$ is not a Φ-observer of any element $a \in A'_{|_\sigma}$, whereas $\sigma(\mathrm{q}_2(\diamond)) = \mathrm{q}'(\diamond)$ and $\mathrm{q}'(\diamond) \in \mathrm{obs}_{\sigma(\Phi)}(a)$.

However, for injective signature morphisms the converse of Theorem 3.8 holds:

Theorem 3.12

Let $\sigma : \Sigma \rightarrow \Sigma'$ be an injective signature morphism, $\Phi \subseteq \mathrm{Wff}_\Sigma(\mathrm{X})$ be a set of formulae and A' be a Σ'-algebra. For any $a \in A'_{|_\sigma}$ and any $\xi \in \mathrm{Cf}_\Sigma(A'_{|_\sigma})$ we have:

$$\xi \in \mathrm{obs}_\Phi(a) \quad \Leftrightarrow \quad \sigma(\xi) \in \mathrm{obs}_{\sigma(\Phi)}(a)$$

Proof sketch

Since σ is injective, the implications in lemmas 3.9, 3.10 become equivalences when $\Phi' = \sigma(\Phi)$. Consequently, we obtain the proof we are looking for, by replacing the implications in the proof of 3.8 by equivalences. □

The former example shows the real source of problems in our approach. More generally a signature morphism $\sigma : \Sigma \rightarrow \Sigma'$ may map two (or more) different sorts $\mathrm{s}_1, \mathrm{s}_2 \in \mathrm{S}$ to the same sort $\mathrm{s}' \in \mathrm{S}'$. By definition of σ-reduct we then have $(A'_{|_\sigma})_{\mathrm{s}_1} = (A'_{|_\sigma})_{\mathrm{s}_2} = A_{\mathrm{s}'}$ but the indistinguishability relations may be different on these three carrier sets even if $\sigma(\Phi) = \Phi'$. Consequently, given $\sim_\Phi$ on an algebra $A'_{|_\sigma}$, we often need to mention the carrier we are working on. This makes the statements of some theorems and their proofs unusually complicated.

4 Properties of the Indistinguishability Relation

The definition 3.6 expresses a situation in which two elements of a Σ-algebra are indistinguishable. Indeed, it defines an S-sorted relation $\sim_\Phi = (\sim_\Phi)_{s \in S}$ on an algebra, called the **indistinguishability relation**. Since this relation is the next step toward a complete description of our institution for observational specifications, we must study its properties w.r.t. the forgetful functor and the translation of observable formulae. This will be subsequently necessary for establishing the Satisfaction Condition (see [7]). The following proposition is devoted to this purpose and next we study other interesting properties of the indistinguishability relation.

Proposition 4.1

Let $\sigma : \Sigma \to \Sigma'$ be a signature morphism, let $\Phi \subseteq \mathrm{Wff}_\Sigma(\mathrm{X})$ and $\Phi' \subseteq \mathrm{Wff}_{\Sigma'}(\mathrm{X}')$ be sets of formulae such that $\sigma(\Phi) \subseteq \Phi'$ and A' be a Σ'-algebra. For any $\mathrm{s}' \in \sigma(\mathrm{S})$, for all $\mathrm{a}, \mathrm{b} \in A'_{\mathrm{s}'}$ we have that if $a \sim_{\Phi'} b$ then for any $\mathrm{s} \in \sigma^{-1}(\mathrm{s}')$, a and b are Φ-indistinguishable in $(A'_{|\sigma})_\mathrm{s}$.

We need the following lemma for the proof:

Lemma 4.2

Let $\sigma : \Sigma \to \Sigma'$ be a signature morphism and A' be a Σ'-algebra. For any valued formula $\vartheta \in \mathrm{Wff}_\Sigma(A'_{|\sigma})$ we have $A'_{|\sigma} \models \vartheta$ iff $A' \models \sigma(\vartheta)$.

Proof sketch

This lemma is a slightly modified version of the Satisfaction Condition (see [7]) for (Many Sorted) First Order Logic with Equality and is proved similarly. □

Proof of Proposition 4.1

Assume by contradiction that there exists $\mathrm{s} \in \mathrm{S}$ and $a, b \in A'_{\sigma(\mathrm{s})}$ such that $a \sim_{\Phi'} b$ and $a \not\sim_\Phi b$ in $(A'_{|\sigma})_\mathrm{s}$. By Definition 3.5 there exists $\xi \in \mathrm{cmp}_\Phi(a, b)$ such that $A'_{|\sigma} \not\models \xi[a] \Leftrightarrow \xi[b]$. Hence from Lemma 4.2 we have:

$$A' \not\models \sigma(\xi)[a] \Leftrightarrow \sigma(\xi)[b] \qquad \text{(i)}$$

But according to Theorem 3.8, $\sigma(\xi)$ is a Φ'-observer for both a and b. Thus according to (i), $\sigma(\xi)$ distinguishes a and b. This is in contradiction with the assumption $a \sim_{\Phi'} b$. □

As mentioned at the end of the previous section the converse of this proposition does not hold even if $\sigma(\Phi) = \Phi'$. But once again this converse holds for injective signature morphisms.

The following fact is obvious from the definition of the indistinguishability relation.

Fact 4.3

The indistinguishability relation is reflexive and symmetric. □

The next fact fully agrees with our claims:

Fact 4.4

The indistinguishability relation is neither compatible with operations nor with predicates.

Proof sketch

It is enough to consider the examples given in Introduction. □

We have already announced the following fact which is a consequence of our Indistinguishability Assumption together with general form observations we use:

Fact 4.5

The indistinguishability relation is not transitive in general.

Proof

Consider $\Sigma = \{\mathsf{a}, \mathsf{b}, \mathsf{c} :\rightarrow \mathsf{Trans}; \mathsf{q} : \mathsf{Trans}\}$, $\Phi = \{\mathsf{q}(\mathsf{a}), \mathsf{q}(\mathsf{c})\}$ *and a* Σ*-algebra* A *such that* $q^A = \{a^A\}$. *In this algebra we have* $\mathrm{obs}_\Phi(a^A) = \mathrm{obs}_\Phi(c^A) = \{\mathsf{q}(\diamond)\}$ *and* $\mathrm{obs}_\Phi(b^A) = \emptyset$. *Since* a^A *and* b^A *(resp.* b^A *and* c^A*) have no comparator they are indistinguishable. On the other hand,* a^A *and* c^A *are distinguished by* $\mathsf{q}(\diamond)$. *Consequently, in this example the indistinguishability relation is not transitive.* □

More generally, the above result has the following explanation: since we did not impose any restriction on the set of observable formulae, nothing ensures that all the elements of a given data type can be observed in the same way. On the contrary, when all the elements of a carrier set have the same observers, the indistinguishability relation is transitive on this carrier set. This may be illustrated as follows:

Example 4.6

The indistinguishability relation from Example 3.7 *is transitive.*

One may think that Fact 4.5 is quite unfortunate and claim that two elements should be indistinguishable if they are in the sense of Definition 3.6 and if additionally they have the same observers. But in our opinion such definition would not be adequate, due to the reason detailed in the following example:

Example 4.7

Consider a signature Σ and assume that we need to provide a set Φ of observable formulae which induces on any Σ-algebra A the following indistinguishability relation

$$\forall\ a, b \in A \quad a \sim_\Phi b \ \text{ iff } \quad \nexists\ \mathrm{t} \in \mathrm{T}_\Sigma \ \ \overline{\mathrm{t}} = a$$

With Definition 3.6 we obtain this relation by taking $\Phi = \{\mathrm{l} = \mathrm{r} \mid \mathrm{l}, \mathrm{r} \in (\mathrm{T}_\Sigma)_\mathrm{s}, \mathrm{s} \in \mathrm{S}\}$. Now if we add to this definition the additional requirement mentioned above, we do not obtain the desired indistinguishability relation whatever Φ we consider.

This example points out that the discussed modification of the Definition 3.6 would decrease the expressive power of our approach. Consequently we are not enthusiastic about such a modification. Moreover, as we will see in the sequel (Definition 6.4), Fact 4.5 raises no particular problem.

5 Observational Algebras

As mentioned in the introduction, in this paper, an observational equality does not necessarily coincide with the indistinguishability relation. This choice was dictated by the fact that the indistinguishability relation is not "transported" by the forgetful functor (the converse of Proposition 4.1 does not hold even if $\Phi' = \sigma(\Phi)$) whereas an observational equality should be "transported" through the forgetful functor as the usual equality does. For this reason we introduce in this section a flexible concept of observational algebras.

Definition 5.1

Given a signature Σ, an **observational Σ-algebra** *is a pair $\langle A, \cong \rangle$ where A is a Σ-algebra and $\cong$ is an S-sorted equivalence relation on A, called* **observational equality on A**. *We denote the class of all observational Σ-algebras by* **OAlg[Σ]**.

According to the above definition we consider the equality symbol "=" as a particular predicate symbol. This symbol is explicitly interpreted in an algebra by a particular relation, namely an observational equality.

Example 5.2

Let L and $\sim_{\mathsf{Opt}}$ be respectively the algebra and the indistinguishability relation described in Example 3.7*. Since $\sim_{\mathsf{Opt}}$ is an equivalence relation (c.f.* 4.6*), the pair $\langle L, \sim_{\mathsf{Opt}}\rangle$ is an observational algebra.*

Definition 5.3

An **observational Σ-morphism** *$\mu : \langle A, \cong^A\rangle \rightarrow \langle B, \cong^B\rangle$ is any Σ-morphism from A to B which preserves observational equalities i.e:*

$$\forall a, b \in A_{\mathrm{s}} \quad a \cong^A b \Rightarrow \mu(a) \cong^B \mu(b)$$

It is obvious that OAlg[Σ] equipped with the observational Σ-morphisms forms a category.

Definition 5.4

Let $\sigma : \Sigma \rightarrow \Sigma'$ be a signature morphism. The **σ-reduct** *of an observational Σ′-algebra $\langle A', \cong'\rangle$ is the observational Σ-algebra*

$$\langle A', \cong'\rangle_{|_\sigma} = \langle A'_{|_\sigma}, \cong'_{|_\sigma}\rangle$$

where $A'_{|_\sigma}$ is the usual σ-reduct of the Σ′-algebra A' and $(\cong'_{|_\sigma})_{\mathrm{s}} = (\cong')_{\sigma(\mathrm{s})}$.

The mapping $\_{|_\sigma}$ extends to observational morphisms as in the usual framework. Consequently, it defines the **forgetful functor** from OAlg[Σ′] to OAlg[Σ] associated to σ. Thus OAlg is a functor from the category of signatures Sig to the dual of the category of all categories $\mathrm{Cat}^{\mathrm{op}}$. OAlg maps an object Σ of Sig to the category of the observational Σ-algebras and a signature morphism σ to the corresponding forgetful functor $\_{|_\sigma}$. This provides components upon which an institution can be built.

6 Validity of Observational Formulae

Before introducing observational formulae and defining their validity in observational algebras we give some additional definitions and results.

Definition 6.1

A **solution** *of an equation* $\mathrm{l} = \mathrm{r}$ *(resp. atomic formula* $\mathrm{q}(\mathrm{t}_1, \ldots, \mathrm{t}_n)$*) in an observational* Σ*-algebra* $\langle A, \cong\rangle$ *is a valuation* $\nu : \mathrm{X} \to A$ *such that* $\overline{\mathrm{l}\nu} \cong \overline{\mathrm{r}\nu}$ *(resp.* $\langle\overline{\mathrm{t}_1\nu}, \ldots, \overline{\mathrm{t}_n\nu}\rangle \in q^A$*). The set of solutions of a formula* φ*, written* $[\varphi]_{\langle A,\cong\rangle}$*, is defined recursively as follows:*

- *if* $\varphi = \neg\psi$ *then* $[\varphi]_{\langle A,\cong\rangle} = \mathrm{Val}[\mathrm{X}, A] \smallsetminus [\psi]_{\langle A,\cong\rangle}$
- *if* $\varphi = \psi \wedge \psi'$ *then* $[\varphi]_{\langle A,\cong\rangle} = [\psi]_{\langle A,\cong\rangle} \cap [\psi']_{\langle A,\cong\rangle}$
- *if* $\varphi = \forall \mathrm{x}\psi$ *then* $[\varphi]_{\langle A,\cong\rangle} =$

  $= \{\nu \in \mathrm{Val}[\mathrm{X}, A] \mid \forall\, \mu \in \mathrm{Val}[\mathrm{X}, A]\ (\forall\, \mathrm{y} \in \mathrm{X} \smallsetminus \{\mathrm{x}\}\ \ \mathrm{y}\mu = \mathrm{y}\nu) \Rightarrow \mu \in [\psi]_{\langle A,\cong\rangle}\}$

where ψ, ψ' *are* Σ*-formulae.*

Since all the connectives of the classical logic as well as the existential quantifier can be expressed by means of $\neg$, $\wedge$ and $\forall$, the solutions of an arbitrary first order logic Σ-formula are well defined by the above definition.

Before putting our formalism into an institutional framework we need to investigate the solutions across the forgetful functor and the translation of formulae. This is done in the following theorem:

Theorem 6.2

Let $\sigma : \Sigma \to \Sigma'$ *be a signature morphism and* $\langle A', \cong'\rangle$ *be an observational* Σ'*-algebra. For any* Σ*-formula* φ *we have:*

$$\nu \in [\varphi]_{\langle A',\cong'\rangle_{|\sigma}} \quad \textit{iff} \quad \sigma(\nu) \subseteq ([\sigma(\varphi)]_{\langle A',\cong'\rangle})_{|\sigma} \qquad \text{(i)}$$

Proof sketch

The proof is based on the fact that (Many-Sorted) First Order Logic is an institution. The Goguen's and Burstall's proof of this fact establishes a one to one map between $\mathrm{Val}[\mathrm{X}, A'_{|\sigma}]$ *and* $\mathrm{Val}[\mathrm{X}', A']$ *which is shown to be solution preserving w.r.t. formula translation, that is* (i) *holds (replacing* $\subseteq$ *by* $\in$*) in the usual framework of (Many-Sorted) First Order Logic. According to Remark* 2.3 *which is justified by Lemma* 2.4*,* (i) *also holds for (Many-Sorted) First Order Logic with our approach to variables. Our "logical system" is not exactly (Many-Sorted) First Order Logic but may be mapped into this in the following way:*

- *We consider the equality symbol as an S-indexed family of ordinary predicate symbols* $=_\mathrm{s}$*.*

- *Since in our approach* $(=_\mathrm{s})_{\mathrm{s}\in\mathrm{S}}$ *are interpreted by equivalence relations we consider an S-indexed set of axioms* $\mathcal{E} = \{\mathrm{x} =_\mathrm{s} \mathrm{x},\ \ \mathrm{x} =_\mathrm{s} \mathrm{y} \ \Rightarrow\ \mathrm{y} =_\mathrm{s} \mathrm{x},\ \ \mathrm{x} =_\mathrm{s} \mathrm{y} \wedge \mathrm{y} =_\mathrm{s} \mathrm{z} \ \Rightarrow\ \mathrm{x} =_\mathrm{s} \mathrm{z}\}$.

Since (i) *holds in the usual framework of (Many-Sorted) First Order Logic, it also holds for a particular class of first order* Σ*-formulae of the form* $\psi \wedge \mathcal{E}$. *Consequently, in the axiomatic theory* $\mathcal{E}$ *underlying our "logical system"* (i) *holds for any first order* Σ*-formula* φ. □

An elementary and complete proof of this theorem may be found in [2].

Definition 6.3

An **observational Σ-formula** *is a pair* $\langle \theta, \Phi \rangle$ *where* $\theta \in \mathrm{Wff}_\Sigma(\mathrm{X})$ *is a* Σ*-formula and* $\Phi \subseteq \mathrm{Wff}_\Sigma(\mathrm{X})$ *is a set of formulae. We note* **OWff**$[\mathbf{\Sigma}]$ *the set of all observational* Σ*-formulae.*

Notice that observational formulae are only atomic ones. We have neither "observational connectives" nor "observational quantifiers". It may be interesting to investigate the possibility of including such features to our approach.

As in the usual framework, OWff is extended to a functor from the category of signatures Sig to Set (the category of sets). This functor maps an objet Σ of Sig to the set of all observational Σ-formulae. An arrow σ of $\mathrm{Sig}(\Sigma, \Sigma')$ is mapped by OWff to the corresponding translation of observational formula: $\mathrm{OWff}[\sigma](\langle \theta, \Phi \rangle) = \langle \sigma(\varphi), \sigma(\Phi) \rangle$. (We write shortly σ instead of $\mathrm{OWff}[\sigma]$.)

We have already all the elements necessary to define an observational satisfaction relation:

Definition 6.4

We say that an observational Σ*-algebra* $\langle A, \cong \rangle$ **satisfies** *an observational formula* $\langle \psi, \Phi \rangle$, *written* $\langle \boldsymbol{A}, \cong \rangle \ \Box\!\!\models\ \langle \boldsymbol{\psi}, \boldsymbol{\Phi} \rangle$, *iff:*

$$\begin{array}{rcll} [\psi]_{\langle A, \cong \rangle} & = & \mathrm{Val}[\mathrm{X}, A] & \text{(i)} \\ \cong & \subseteq & \sim_\Phi & \text{(ii)} \end{array}$$

Notice that in the above we have defined a family of relations $\{\Box\!\!\models_\Sigma\}_{\Sigma:\mathrm{Sig}}$ with

$$\Box\!\!\models_\Sigma \ \subseteq \ \mathrm{OAlg}[\Sigma] \times \mathrm{OWff}[\Sigma]$$

We examine now how our satisfaction relation behaves w.r.t. the variance of observational formulae (translation) and the covariance of algebras (σ-reduct). We start by the first requirement of Definition 6.4:

Proposition 6.5

Let $\sigma : \Sigma \rightarrow \Sigma'$ be a signature morphism. For any set of formulae $\Phi \subseteq \mathrm{Wff}_\Sigma(\mathrm{X})$, any observational Σ'-algebra $\langle A', \cong' \rangle$ and any Σ-formula φ we have:

$$[\sigma(\varphi)]_{\langle A', \cong' \rangle} = \mathrm{Val}[\mathrm{X}', A'] \quad \textit{iff} \quad [\varphi]_{\langle A', \cong' \rangle_{|\sigma}} = \mathrm{Val}[\mathrm{X}, A'_{|\sigma}]$$

Proof

We have $[\sigma(\varphi)]_{\langle A', \cong' \rangle} = \mathrm{Val}[\mathrm{X}', A']$ *which is equivalent to* $([\sigma(\varphi)]_{\langle A', \cong' \rangle})_{|\sigma} = (\mathrm{Val}[\mathrm{X}', A'])_{|\sigma}$*, which by Theorem 6.2 is equivalent to:*

$$[\varphi]_{\langle A', \cong' \rangle_{|\sigma}} = (\mathrm{Val}[\mathrm{X}', A'])_{|\sigma} \qquad \text{(i)}$$

Since $\_{|\sigma}$ *is surjective on valuations we have* $(\mathrm{Val}[\mathrm{X}', A'])_{|\sigma} = \mathrm{Val}[\mathrm{X}, A'_{|\sigma}]$*. Thus, the formula* (i) *is equivalent to* $[\varphi]_{\langle A', \cong' \rangle_{|\sigma}} = \mathrm{Val}[\mathrm{X}, A'_{|\sigma}]$. □

The next step is to study the second condition of Definition 6.4 w.r.t. formula translation and the forgetful functor.

Proposition 6.6

Let $\sigma : \Sigma \rightarrow \Sigma'$ be a signature morphism. For all sets of formulae $\Phi \subseteq \mathrm{Wff}_\Sigma(\mathrm{X})$, $\Phi' \subseteq \mathrm{Wff}_{\Sigma'}(\mathrm{X}')$ such that $\sigma(\Phi) \subseteq \Phi'$ and for any observational Σ'-algebra $\langle A', \cong' \rangle$ we have:

$$\cong' \subseteq \sim_{\Phi'} \quad \Rightarrow \quad \cong'_{|\sigma} \subseteq \sim_\Phi$$

where $\sim_{\Phi'}$ and $\sim_\Phi$ are the indistinguishability relations on A' and $A'_{|\sigma}$ respectively.

Proof

Assume that $\forall\ a, b \in A' \quad a \cong' b \quad \Rightarrow \quad a \sim_{\Phi'} b$*. Applying Definition 5.4 we obtain*

$$\forall\ a, b \in A'_{|\sigma} \quad a \cong'_{|\sigma} b \quad \Rightarrow \quad a \sim_{\Phi'} b$$

But from Proposition 4.1 it follows that $a \sim_{\Phi'} b \quad \Rightarrow \quad a \sim_\Phi b$*. Consequently* $\cong'_{|\sigma} \subseteq \sim_\Phi$. □

The next step would be to prove the converse of the above proposition when restricted to $\Phi' = \sigma(\Phi)$. Unfortunately this is not true in general. The following example illustrates this fact:

Example 6.7

Consider $\Sigma = \{\mathrm{a}, \mathrm{b} :\rightarrow \mathrm{s};\ \mathrm{p}, \mathrm{q} : \mathrm{s}\}$ *and* $\Sigma' = \{\mathrm{c}, \mathrm{d} :\rightarrow \mathrm{s};\ \mathrm{r} : \mathrm{s}\}$. *Let* $\Phi = \{\mathrm{p}(\mathrm{a}), \mathrm{q}(\mathrm{b})\}$. *Notice that in any* Σ*-algebra* A *we have*

$$a^A \sim_\Phi b^A \tag{i}$$

because a^A *and* b^A *have no comparator. Consider* $\sigma : \Sigma \rightarrow \Sigma'$ *defined by:* $\sigma(\mathrm{s}) = \mathrm{s}$, $\sigma(\mathrm{a}) = \mathrm{c}$, $\sigma(\mathrm{b}) = \mathrm{d}$, $\sigma(\mathrm{p}) = \sigma(\mathrm{q}) = \mathrm{r}$. *Notice that in any* Σ'*-algebra* A' *we have*

$$\mathrm{cmp}_{\sigma(\Phi)}(c^{A'}, d^{A'}) = \{\mathrm{r}(\diamond)\} \tag{ii}$$

since $\sigma(\Phi) = \{\mathrm{r}(\mathrm{c}), \mathrm{r}(\mathrm{d})\}$. *Consider then a reachable observational* Σ'*-algebra* $\langle A', \cong' \rangle$ *such that*

$$A' \not\models r^{A'}(c^{A'}) \Leftrightarrow r^{A'}(d^{A'}) \tag{iii}$$

$$c^{A'} \cong' d^{A'} \tag{iv}$$

Notice that $\cong'|_\sigma = \{(a^{A|_\sigma}, b^{A|_\sigma})\}$. *Therefore, according to* (i) *we have* $\cong'|_\sigma \subseteq \sim_\Phi$ *but* $\cong' \not\subseteq \sim_{\sigma(\Phi)}$ *since from* (ii) *and* (iii) *we have* $c^{A'} \not\sim_{\sigma(\Phi)} d^{A'}$ *while* (iv) *holds.*

From this negative result we may conclude that, in order to define institutions within our approach, we will be constrained to restrict somehow our formalism. This will be the subject of Section 9.

7 Observational Specifications

This section is devoted to some general notions about observational specifications.

Definition 7.1

An **observational specification** OSP *is a triplet* $\langle \Sigma, \Theta, \Phi \rangle$, *where* Σ *is the signature of* OSP, Θ *the (finite) set of its axioms and* Φ *is a set of formulae,* $\Phi \subseteq \mathrm{Wff}_\Sigma(\mathrm{X})$, *called* **observations** *of* OSP.

The models are defined as in the usual approach except that we use the observational satisfaction instead of the usual one:

Definition 7.2

Let $\mathrm{OSP} = \langle \Sigma, \{\theta_1, \ldots, \theta_n\}, \Phi \rangle$ *be an observational specification. We say that an observational* Σ*-algebra* $\langle A, \cong \rangle$ *is a* **model** *of* OSP *iff:*

$$\langle A, \cong \rangle \;\square\!\!\models \langle \theta_1 \wedge \ldots \wedge \theta_n, \Phi \rangle$$

We note **OAlg[OSP]** *the class of all observational models of* OSP.

OAlg[OSP] with observational Σ-morphisms is a full subcategory of OAlg[Σ].

Fact 7.3

The observational algebra $\langle L, \sim_{\mathsf{Opt}} \rangle$*, described in Example* 5.2*, is a model of the observational specification* OPT-SET.

Proof

Since the observational equality on $\langle L, \sim_{\mathsf{Opt}} \rangle$ *is just the indistinguishability relation, we only need to prove that for any axiom* θ *of* OPT-SET *we have*

$$[\theta]_L = \mathrm{Val}[\mathrm{X}, L] \qquad \text{(i)}$$

- *For the first axiom the requirement* (i) *is satisfied because for any set* $\{c_1, \ldots, c_n\} \in L_{\mathsf{Set}}$ *and any optional constant* c *the result of* $add^L(c, \{c_1, \ldots, c_n\})$ *is either* $\{c, c_1, \ldots, c_n\}$ *or* $\{c_1, \ldots, c_n\}$ *(depending on whether* c *is particular or not) and we know (see* 3.7*) that* $\{c, c_1, \ldots, c_n\}$ *and* $\{c_1, \ldots, c_n\}$ *are in the same equivalence class of the observational equality* $\sim_{\mathsf{Opt}}$.

- *Since* $\in^L$ *is the usual membership, it is clear that the requirement* (i) *is also satisfied by the second and the third axiom.* □

The next result points out that our observational specifications generalize the usual approach. On one hand an algebra A can be viewed as the observational algebra $\langle A, = \rangle$. On the other hand, an algebraic specification $\langle \Sigma, \Theta \rangle$ can be considered as an observational one in the straightforward way:

Proposition 7.4

Let $\langle \Sigma, \Theta \rangle$ *be an algebraic specification. Each model of* $\langle \Sigma, \Theta, \Phi \rangle$ *with* $\Phi = \{\mathrm{x_s} = \mathrm{y_s} \mid \mathrm{s} \in \mathrm{S}\}$ *is of the form* $\langle A, = \rangle$ *with* $A \in \mathrm{Alg}[\langle \Sigma, \Theta \rangle]$.

Proof

Note first that $\sim_\Phi$ is the identity relation on any Σ-algebra. This is obvious since all $a, b \in A_{\mathrm{s}}$, $a \neq b$, are distinguished by e.g. $(\diamond = a) \in \mathrm{cmp}_\Phi(a, b)$. According to Definition 6.4 for any $\langle A, \cong\rangle \in \mathrm{OAlg}[\langle\Sigma, \Theta, \Phi\rangle]$ we should have $\cong \subseteq \sim_\Phi$. Thus $\cong$ is just the usual equality. From the requirement $[\Theta]_{\langle A,=\rangle} = \mathrm{Val}[\mathrm{X}, A]$ we deduce that $A \in \mathrm{Alg}[\langle\Sigma, \Theta\rangle]$. Conversely, it is clear that for any $B \in \mathrm{Alg}[\langle\Sigma, \Theta\rangle]$ we have $\langle B, =\rangle \in \mathrm{OAlg}[\langle\Sigma, \Theta, \Phi\rangle]$. □

Up to now, we have not been studying modularity issues. We have only defined the semantics of "flat" specifications. In fact, as in [1], our semantics extends to an observational **stratified loose semantics** [4] without additional assumptions. For instance, the next theorem shows that our approach fulfills the requirement of "reusing by restriction" of [4].

Theorem 7.5

Let $\sigma : \Sigma \to \Sigma'$ be a signature morphism. For all observational specifications $\mathrm{OSP} = \langle\Sigma, \Theta, \Phi\rangle$ and $\mathrm{OSP}' = \langle\Sigma', \Theta', \Phi'\rangle$ such that $\sigma(\Theta) \subseteq \Theta'$ and $\sigma(\Phi) \subseteq \Phi'$ we have:

$$\mathrm{OAlg}[\mathrm{OSP}']_{|_\sigma} \subseteq \mathrm{OAlg}[\mathrm{OSP}]$$

Proof

From definitions 7.2 and 6.4 it is enough to prove:

$$[\Theta']_{\langle A',\cong'\rangle} = \mathrm{Val}[\mathrm{X}', A'] \quad\Rightarrow\quad [\Theta]_{\langle A',\cong'\rangle_{|_\sigma}} = \mathrm{Val}[\mathrm{X}, A'_{|_\sigma}] \tag{i}$$

and

$$\cong' \subseteq \sim_{\Phi'} \quad\Rightarrow\quad \cong'_{|_\sigma} \subseteq \sim_\Phi \tag{ii}$$

for all $\langle A', \cong'\rangle \in \mathrm{OAlg}[\Sigma']$.

- **Proof of (i)**

Let $\langle A', \cong'\rangle \in \mathrm{OAlg}[\Sigma']$ such that $[\Theta']_{\langle A',\cong'\rangle} = \mathrm{Val}[\mathrm{X}', A']$. Since $\sigma(\Theta)$ is included in Θ', by definition of solution of a conjunction of formulae (c.f. 6.1) we have $\sigma(\Theta)_{\langle A',\cong'\rangle} \supseteq \Theta'_{\langle A',\cong'\rangle}$. Hence $[\sigma(\Theta)]_{\langle A',\cong'\rangle} = \mathrm{Val}[\mathrm{X}', A']$ which according to Proposition 6.5 implies that $[\Theta]_{\langle A',\cong'\rangle_{|_\sigma}} = \mathrm{Val}[\mathrm{X}, A'_{|_\sigma}]$.

- **Proof of (ii)** *follows directly from Proposition 6.6.* □

This result corresponds to a very fundamental property which holds in most non observational frameworks. With all the definitions of observational satisfaction relation preceding [3], such a result holds only for equational axioms or positive-conditional axioms with observable preconditions which is a rather strong restriction. It may be then surprising that in our approach the former theorem holds without restrictions even if the axioms are arbitrary first order formulae. The reason is that our observational equality is not fixed by observations, even though the indistinguishability relation is fixed. Unlike [1], [14], [8], [10] and [11], our observational equality does not coincide with the indistinguishability relation. This choice was dictated by the fact that the indistinguishability relation is "disconnected" from the forgetful functor. On the contrary, our observational equality, similarly to the usual equality, is always "transported" through the forgetful functor. In short, the main difference of our approach with the above-mentioned works is that our satisfaction relation is based on an observational equality which does not coincide with the indistinguishability relation. This situation (in part) guarantees such a general result as Theorem 7.5.

We may also consider a particular case of this theorem with $\Theta' = \sigma(\Theta)$. This points out that observations act on the semantics of a specification in a similar way as the axioms do: by adding observations we diminish the class of the observational models. This is yet another reason for introducing observational formulae, especially in context of the next section. We argue that in any approach with an observational satisfaction relation, the Satisfaction Condition may hold only if the translation of observations is considered at the same level as the translation of axioms.

8 Relationship with Behavioural Equivalence

In this section we investigate deeper the relationship of our approach with behavioural equivalence of algebras.

Several papers dealing with an observational satisfaction relation provide also a definition of a **behavioural equivalence** $\equiv_{\mathrm{Obs}}$ of algebras which aims at reflecting the situation when algebras behave in the same way w.r.t. some observations Obs. One may then define the class of **behaviours** of a specification SP, written $\mathrm{Beh}_{\mathrm{Obs}}[\mathrm{SP}]$ as the closure of the usual class of the models of SP by the equivalence $\equiv_{\mathrm{Obs}}$:

$$\mathrm{Beh}_{\mathrm{Obs}}[\mathrm{SP}] \quad = \quad \{A \in \mathrm{Alg}[\Sigma] \mid \exists \ \mathrm{B} \in \mathrm{Alg}[\mathrm{SP}],\ \mathrm{A} \equiv_{\mathrm{Obs}} \mathrm{B}\} \qquad (8\text{–i})$$

In such a framework it is interesting to establish that the class of the behaviours of $\mathrm{SP} = \langle \Sigma, \Theta \rangle$ coincides with the class of observational models of

SP:

$$\mathrm{Beh}_{\mathrm{Obs}}[\langle \Sigma, \Theta \rangle] = \mathrm{OAlg}[\langle \Sigma, \Theta, \mathrm{Obs} \rangle]$$

This result cannot hold in our approach since, according to (8–i), for an inconsistent specification SP ($\mathrm{Alg}[\mathrm{SP}] = \emptyset$) we have always $\mathrm{Beh}_{\mathrm{Obs}}[\mathrm{SP}] = \emptyset$, whereas the class of the observational models of SP may be nonempty. This is due to the fact that our observational satisfaction relation is based on an observational equality which is not necessarily a congruence. But this phenomenon disappears when we restrict to observational equalities being congruences. It is then interesting to investigate the relationship between behavioural equivalence on algebras and our approach in this restricted framework.

> We assume for the scope of this section that **observational equalities are congruences.** Consequently, in this section an element of $\mathrm{OAlg}[\Sigma]$ is any pair $\langle A, \cong \rangle$ such that A is a Σ-algebra and $\cong$ is a congruence.

Under this assumption it is always possible to consider the quotient $A_{/\cong}$. This allows to provide an adequate to our approach definition of behavioural equivalence of observational algebras w.r.t. a set of formulae.

Definition 8.1

We say that two observational Σ-algebras $\langle A, \cong^A \rangle$ and $\langle B, \cong^B \rangle$ are behaviourally equivalent w.r.t. a set of Σ-fromulae Φ, written $\langle A, \cong^A \rangle \equiv_\Phi \langle B, \cong^B \rangle$, iff

$$\cong^A \subseteq \sim^A_\Phi \quad \Leftrightarrow \quad \cong^B \subseteq \sim^B_\Phi \qquad \text{(i)}$$

$$A_{/\cong^{\mathrm{A}}} \quad = \quad B_{/\cong^{\mathrm{B}}} \qquad \text{(ii)}$$

where $\sim^A_\Phi$ and $\sim^B_\Phi$ are the indistinguishability relations on A and B respectively.

The formula (8–i) which defines the class of behaviours is adapted to observational algebras:

Definition 8.2

Given an observational specification $\langle \Sigma, \Theta, \Phi \rangle$, the class of its behaviours, written $\mathbf{Beh}_{\mathbf{\Phi}}[\langle \mathbf{\Sigma}, \mathbf{\Theta} \rangle]$, is defined as follows

$$\mathrm{Beh}_\Phi[\langle \Sigma, \Theta \rangle] \;=\; \{\langle A, \cong \rangle \in \mathrm{OAlg}[\Sigma] \mid \exists\, B \in \mathrm{Alg}[\langle \Sigma, \Theta \rangle],\ \langle A, \cong \rangle \equiv_\Phi \langle \mathrm{B}, = \rangle\}$$

The result we are interested in may be stated as follows:

Theorem 8.3

For any observational specification $\langle\Sigma, \Theta, \Phi\rangle$ *we have*

$$\mathrm{Beh}_\Phi[\langle\Sigma, \Theta\rangle] = \mathrm{OAlg}[\langle\Sigma, \Theta, \Phi\rangle]$$

We need an auxiliary definition as well as some lemmas for the proof.

Lemma 8.4

For any specification $\langle\Sigma, \Theta, \Phi\rangle$ *and any observational* Σ*-algebra* $\langle A, \cong\rangle$ *we have* $\langle A, \cong\rangle \in \mathrm{Beh}_\Phi[\langle\Sigma, \Theta\rangle]$ *iff* $A_{/\cong} \models \Theta$ *and* $\cong \subseteq \sim^A_\Phi$.

Proof

Let $\langle A, \cong\rangle \in \mathrm{Beh}_\Phi[\langle\Sigma, \Theta\rangle]$. *By Definition* 8.2 *this is equivalent to*

$$\exists\ B \in \mathrm{Alg}[\langle\Sigma, \Theta\rangle]\ \ \langle A, \cong\rangle \equiv_\Phi \langle B, =\rangle$$

Since $= \subseteq \sim^B_\Phi$ *by Definition* 8.1 *this is equivalent to*

$$\exists\ B \in \mathrm{Alg}[\Sigma]\ \ A_{/\cong} = B,\ \ B \models \Theta\ \ \mathit{and}\ \ \cong \subseteq \sim^A_\Phi$$

which is equivalent to $A_{/\cong} \models \Theta$ *and* $\cong \subseteq \sim^A_\Phi$. □

Definition 8.5

Let $\cong$ *be a congruence on a* Σ*-algebra* A *and let* $\nu : \mathrm{X} \to A$ *be a valuation. Then* $\boldsymbol{\nu}_{/\cong} : \mathrm{X} \to A_{/\cong}$ *is defined as a valuation such that if* $\mathrm{x}\nu = a$ *then* $\mathrm{x}\nu_{/\cong} = [a]_\cong$ *where* $[a]_\cong$ *is the equivalence class of* a *w.r.t.* $\cong$.

Lemma 8.6

Let $\cong$ *be a congruence on a* Σ*-algebra* A *and let* $\nu : \mathrm{X} \to A$ *and* $\mu : \mathrm{X} \to A_{/\cong}$ *be valuations such that* $\mu = \nu_{/\cong}$. *For any* $\varphi \in \mathrm{Wff}_\Sigma(\mathrm{X})$ *we have*

$$\nu \in [\varphi]_{\langle A, \cong\rangle}\ \ \mathit{iff}\ \ \mu \in [\varphi]_{\langle A_{/\cong},\, =\rangle}$$

Proof

Obvious from the fact that if $\nu_{1/\cong} = \nu_{2/\cong}$ *then* $\nu_1 \in [\varphi]_{\langle A, \cong\rangle} \Leftrightarrow \nu_2 \in [\varphi]_{\langle A, \cong\rangle}$ *for any formula* φ. □

Lemma 8.7

Let $\cong$ be a congruence on a Σ-algebra A. For any $\varphi \in \mathrm{Wff}_\Sigma(\mathrm{X})$ we have

$$[\varphi]_{\langle A,\cong\rangle} = \mathrm{Val}[\mathrm{X}, A] \quad \textit{iff} \quad [\varphi]_{\langle A_{/\cong},\, =\rangle} = \mathrm{Val}[\mathrm{X}, A_{/\cong}]$$

Proof

Obvious from the previous lemma. □

Proof of Theorem 8.3

Let $\langle A, \cong\rangle \in \mathrm{Beh}_\Phi[\langle\Sigma, \Theta\rangle]$. By Lemma 8.4 *this is equivalent to*

$$[\Theta]_{\langle A_{/\cong},\, =\rangle} = \mathrm{Val}[\mathrm{X}, A_{/\cong}] \quad \textit{and} \quad \cong\subseteq\sim_\Phi^A$$

which by Lemma 8.7 *and Definition* 7.2 *is equivalent to $\langle A, \cong\rangle \in \mathrm{OAlg}[\langle\Sigma, \Theta, \Phi\rangle]$.*
□

Theorem 8.3 shows that, when observational equalities are restricted to congruences, the class of such observational models may be characterized as the closure of the usual class of the models by an appropriate behavioural equivalence.

9 Towards an Institution of Observational Specifications

In this section, based on the formalism we have developed so far, we propose an institution for observational specifications. As mentioned in Section 6, this task requires to introduce some restrictions in our general formalism.

According to the definition of [7] the quadruple $\langle \mathrm{Sig}, \mathrm{OWff}, \mathrm{OAlg}, \Box\!\!\models\rangle$ could be an institution provided that it would fulfill the Satisfaction Condition which in our formalism is expressed by the following property:

Property 9.1

For any $\sigma : \Sigma \to \Sigma'$, any observational Σ-formula $\langle\theta, \Phi\rangle$ and any observational Σ'-algebra we have:

$$\langle A', \cong'\rangle \mathrel{\Box\!\!\models} \sigma(\langle\theta, \Phi\rangle) \quad \textit{iff} \quad \langle A', \cong'\rangle_{|_\sigma} \mathrel{\Box\!\!\models} \langle\theta, \Phi\rangle$$

To show that this property holds, by definition 6.4, it is enough to prove that for any observational Σ'-algebra the following conditions hold:

$$[\sigma(\varphi)]_{\langle A', \cong' \rangle} = \mathrm{Val}[\mathrm{X}', A'] \quad \Leftrightarrow \quad [\varphi]_{\langle A', \cong' \rangle_{|_\sigma}} = \mathrm{Val}[\mathrm{X}, A'_{|_\sigma}] \qquad \text{(i)}$$

and

$$\cong' \subseteq \sim_{\sigma(\Phi)} \quad \Leftrightarrow \quad \cong'_{|_\sigma} \subseteq \sim_\Phi \qquad \text{(ii)}$$

for all $\langle A', \cong' \rangle \in \mathrm{OAlg}[\Sigma']$. The first requirement is guaranteed by 6.5. From Proposition 6.6 we have the if part of the second requirement. Unfortunately, we know from Example 6.7 that its converse part does not hold without additional assumptions. The following is the necessary and sufficient condition of the converse part of (ii).

Property 9.2

Let $\sigma : \Sigma \to \Sigma'$ be a signature morphism and $\Phi \subseteq \mathrm{Wff}_\Sigma(\mathrm{X})$ be a set of formulae. For any Σ'-algebra A', any $\mathrm{s}' \in \sigma(\mathrm{S})$ and all $a, b \in A'_{\mathrm{s}'}$ $\sigma(\Phi)$-distinguishable, there exist $\mathrm{s} \in \sigma^{-1}(\mathrm{s}')$ such that a and b are Φ-distinguishable when considered as elements of $(A'_{|_\sigma})_\mathrm{s}$.

Proposition 9.3

Let $\sigma : \Sigma \to \Sigma'$ be a signature morphism. The property 9.2 holds for a set Φ of Σ-formulae if and only if

$$\cong'_{|_\sigma} \subseteq \sim_\Phi \quad \Rightarrow \quad \cong' \subseteq \sim_{\sigma(\Phi)}$$

holds on all $\langle A', \cong' \rangle \in \mathrm{OAlg}[\Sigma']$.

Proof

- $\Rightarrow$

Let $\langle A', \cong' \rangle \in \mathrm{OAlg}[\Sigma']$. Assume that

$$\forall\ a, b \in A'_{|_\sigma} \quad a \cong'_{|_\sigma} b \quad \Rightarrow \quad a \sim_\Phi b \qquad \text{(i)}$$

By contradiction assume that there exist $a_0, b_0 \in A'_{\sigma(\mathrm{s})}$ such that $a_0 \not\sim_{\sigma(\Phi)} b_0$ and

$$a_0 \cong' b_0 \qquad \text{(ii)}$$

Using Property 9.2, we find that there exist $\mathrm{s}_0 \in \sigma^{-1}(\sigma(\mathrm{s}))$ such that $a_0 \not\sim_\Phi b_0$ in $(A'_{|_\sigma})_{\mathrm{s}_0}$. But according to (ii) we conclude that $a_0 \cong'_{|_\sigma} b_0$. Therefore $a_0 \cong'_{|_\sigma} b_0 \quad \not\Rightarrow \quad a_0 \sim_\Phi b_0$ which is a contradiction to the assumption (i).

- $\Leftarrow$ (We use the contrapositive method for the proof.)

Let $\sigma : \Sigma \rightarrow \Sigma$ and $\Phi \subseteq \mathrm{Wff}_{\Sigma}(\mathrm{X})$ for which the property 9.2 does not hold. Consequently, there is a Σ'-algebra A' with elements $a, b \in A'_{\sigma(\mathrm{s}_0)}$ (for some $\mathrm{s}_0 \in \mathrm{S}$) $\sigma(\Phi)$-distinguishable, such that for any $\mathrm{s} \in \mathrm{S}$ satisfying $\sigma(\mathrm{s}) = \sigma(\mathrm{s}_0)$, a and b are Φ-indisintguishable in $(A'|_{\sigma})_{\mathrm{s}}$. Let A' be provided with $\cong'$ so that $c \cong' d \Rightarrow c \sim_{\sigma(\Phi)} d$ for all $c, d \in A'$ except for a, b where $a \cong' b$ and as assumed $a \not\sim_{\sigma(\Phi)} b$. It is clear from the proof of 6.6 that for all of these c, d we have also:

$$c \cong'|_{\sigma} d \Rightarrow c \sim_{\Phi} d$$

It follows from the above formula that $\cong'|_{\sigma} \subseteq \sim_{\Phi}$, since by Definition 5.4 we have $a \cong'|_{\sigma} b$ and we assumed that $a \sim_{\Phi} b$. Now $\cong' \not\subseteq \sim_{\sigma(\Phi)}$ because $a \cong' b$ and we have assumed that $a \not\sim_{\sigma(\Phi)} b$. □

We can conclude from the above that in our approach, the Satisfaction Condition does not hold in general. Only the if part of Property 9.1 holds. Consequently, according to [12], our approach defines a reduction-preserving pre-institution. The converse part of 9.1 holds only for the signature morphisms and the observations which preserve 9.2. Therefore our approach is another motivation for more liberal formalizations than institutions of the notion of "logical system" such as e.g. specification logic [5] or pre-institutions [12].

Since the Satisfaction Condition holds only for some signature morphisms, in order to define an institution in our framework, one could ignore the problematic arrows of Sig and consider as a category of signatures a category which has the same objects as Sig but less arrows. Then the question is which signature morphisms we should eliminate in order to obtain an institution. It is easy to see that examples similar to 6.7 can be constructed, as soon as we have an non injective signature morphism. We conclude that an observational institution can be provided within our formalism under the restriction of the arrows of Sig to injective morphisms only.

Proposition 9.4

Consider the quadruple $\mathrm{OAlgSpec} = \langle \mathrm{ISig}, \mathrm{OWff}, \mathrm{OAlg}, \mathrel{\mathrm{O}\!\!\models} \rangle$ *where ISig is the category whose objects are the usual signatures and whose arrows are the injective signature morphisms. Then* OAlgSpec *is an institution.*

Proof

It is sufficient to prove that Property 9.2 holds for injective signature morphisms.

Let $\sigma : \Sigma \longrightarrow \Sigma'$ be an injective signature morphism, let $\Phi \subseteq \mathrm{Wff}_\Sigma(\mathrm{X})$ be a set of formulae, A' a Σ'-algebra and let $a, b \in {A'}_{\sigma(\mathrm{s})}$ $\sigma(\Phi)$-distinguishable. Let $\xi' \in \mathrm{cmp}_{\sigma(\Phi)}(a, b)$ be a comparator which distinguishes a from b. Since σ is injective, there is a unique $\xi \in \mathrm{Cf}_\Sigma(A'_{|_\sigma})$ such that $\sigma(\xi) = \xi'$. According to Theorem 3.12, *ξ is an observer of a and b. So $\xi \in \mathrm{cmp}_\Phi(a, b)$. Since $A' \not\models \xi'[a] \Leftrightarrow \xi'[b]$, from Lemma* 4.2 *we deduce that $A'_{|_\sigma} \not\models \xi[a] \Leftrightarrow \xi[b]$. Therefore, by Definition* 3.5 *we have $a \not\sim_\Phi b$.* □

A drawback of our approach is the necessity to restrict the category of signatures to ISig, in order to have an institution. However, except for some particular examples of parameter-passing morphisms, non injective signature morphisms seem to be not very useful. In spite of this restriction, OAlgSpec may be used for modular specifications with no parameterized modules. (Observational semantics of parameterized specifications is one of our current research topics.)

10 Conclusions

We have presented an observational semantics of algebraic specifications supporting full first order axioms and full first order formulae as observations. This has been achieved by defining an observational satisfaction relation whose cornerstone is the use of a non standard interpretation of equality. We have shown that our formalism is a reduction-preserving pre-institution and may, under some restrictions, even provide an institution.

This work may continue along different lines. Since our observational formulae are in some sense only atomic ones, one may want to define some observational connectives or quantifiers together with their semantics. This may lead to an "Observational Model Theory". A much more problematic, still missing contribution, would be the corresponding "Observational Proof Theory". However, the results of this research area are crucial for most applications of observational specifications in software engineering.

Acknowledgments I gratefully acknowledge Gilles Bernot, Michel Bidoit and Fernando Orejas for their extensive comments and numerous fruitful discussions. I also wish to thank particularly Regina Yillah for the careful proof reading of this paper. This work is partially supported by ESPRIT Working Group COMPASS and CNRS GDR de Programmation.

References

[1] G. Bernot and M. Bidoit. Proving the correctness of algebraically specified software: Modularity and observability issues. In *Proceedings of Second International Conference on Algebraic Methodology and Software Technology*, pages 139–161, Iowa City, May 1991.

[2] G. Bernot, M. Bidoit, and T. Knapik. Observational approaches and indistinguishability assumption. Technical Report LIENS–92–3, Laboratoire d'Informatique de l'Ecole Normale Supérieure, 1992.

[3] G. Bernot, M. Bidoit, and T. Knapik. Towards an adequate notion of observation. In B. Krieg-Brückner, editor, *European Syposium on Programming*, LNCS 582, pages 39–55, Rennes, Feb. 1992.

[4] M. Bidoit. The stratified loose approach: A generalization of initial and loose semantics. In D. Sannella and A. Tarlecki, editors, *Recent Trends in Data Type Specification*, LNCS 332, pages 1–22, Gullane, Sept. 1987. Selected papers from 5th Workshop on Specification of Abstract Data Types.

[5] H. Ehrig, M. Baldamus, and F. Orejas. New concepts for amalgamation and extension in the framework of specification logics. Technical Report 91/05, Technische Universität Berlin, May 1991.

[6] H. Ehrig and B. Mahr. *Fundamentals of Algebraic Specifications*, volume 6 of *EATCS Monographs on Theoretical Computer Science*. Springer-Verlag, 1985.

[7] J. A. Goguen and R. Burstall. Institutions: Abstract model theory for specification and programming. Technical Report ECS–LFCS–90–106, Department of Computer Science, University of Edinburgh, Jan. 1990.

[8] J. A. Goguen and J. Meseguer. Persistent interconnection and implementation of abstract modules. In M. Nielsen and E. M. Schmidt, editors, *ICALP*, LNCS 140, pages 256–281, Aarhus, May 1982.

[9] J. A. Goguen, J. W. Thatcher, and E. G. Wagner. An initial approach to the specification, correctness and implementation of abstract data types. In R. T. Yeh, editor, *Data Structuring*, volume 4 of *Current Trends in Programming Methodology*, pages 80–149. Prentice Hall, 1978.

[10] P. Nivela and F. Orejas. Initial behaviour semantics for algebraic specification. In D. Sannella and A. Tarlecki, editors, *Recent Trends in Data Type Specification*, LNCS 332, pages 184–207, Gullane, Sept. 1987. Selected papers from 5th Workshop on Specification of Abstract Data Types.

[11] H. Reichel. Behavioural validity of conditional equations in abstract data types. In *Contributions to General Algebra 3*, pages 301–324, 1984. Proceedings of the Vienna Conference.

[12] A. Salibra and G. Scollo. A soft stairway to institutions. In M. Bidoit and C. Choppy, editors, *Recent Trends in Data Type Specification*, Dourdan, Sept. 1991. Selected papers from 8th Workshop on Specification of Abstract Data Types.

[13] D. Sannella and A. Tarlecki. On observational equivalence and algebraic specification. *J. Comput. Syst. Sci.*, (34):150–178, 1987.

[14] N. W. P. van Diepen. Implementation of modular algebraic specifications. In H. Ganzinger, editor, *European Syposium on Programming*, LNCS 300, pages 64–78, Nancy, Mar. 1988.