Observational Specifications and the Indistinguishability Assumption

Gilles Bernot **Michel Bidoit** **Teodor Knapik**

LIENS C.N.R.S. U.R.A. 1327
Ecole Normale Supérieure
45 Rue d'Ulm
F – 75230 PARIS Cedex 05 France
e-mail: [bernot, bidoit, knapik] @dmi.ens.fr (Internet) or @frulm63.bitnet (Earn)

Abstract

To establish the correctness of some software w.r.t. its formal specification is widely recognized as a difficult task. A first simplification is obtained when the semantics of an algebraic specification is defined as the class of all algebras which correspond to the correct realizations of the specification. A software is then declared correct if it corresponds to some algebra of this class. We approach this goal by defining an **observational satisfaction relation** which is less restrictive than the usual satisfaction relation. Based on this notion we provide an institution for observational specifications. The idea is that the validity of an equational axiom should depend on an **observational equality**, instead of the usual equality. We show that it is not reasonable to expect an observational equality to be a congruence. We define an **observational algebra** as an algebra equipped with an observational equality which is an equivalence relation but not necessarily a congruence.

We assume that two values can be declared indistinguishable when it is impossible to establish they are different using some available observations. This is what we call the **Indistinguishability Assumption**. Since term observation seems sufficient for data type specifications, we define an indistinguishability relation on the carriers of an algebra w.r.t. the observation of an arbitrary set of terms. From a careful case study it follows that this requires to take into account the **continuations** of suspended evaluations of observable terms. Since our indistinguishability relation is not transitive, it is only an intermediate step to define an observational equality. Our approach is motivated by numerous examples.

Keywords: algebraic specification, observability, software correctness

1 Introduction

A main purpose of formal specifications is to provide a rigorous basis for establishing software correctness. Indeed, it is well known that proving the correctness of some piece of software without any formal reference makes no sense. Algebraic specifications are widely advocated as being one of the most promising formal specification techniques. However, to be provided with some algebraic specification is not sufficient per se. A precise (and adequate) definition of software correctness is mandatory. This crucial prerequisite must be first fulfilled before one can develop the relevant verification methods, and try to mechanize them.

The adequacy of the chosen definition of software correctness has a great practical impact, and we should therefore define software correctness according to the actual needs. In

the framework of algebraic specifications, straightforward definitions of correctness turn out to be oversimplified: most programs that should be considered as being correct (from a practical point of view) are rejected. The first thing is then to formally define the class of algebras which correspond to the correct implementations of a given specification. It is well known that this class contains not only all the models of the specification but also some algebras which do not satisfy (in the usual sense) all of the axioms of the specification. In fact, this class should rather correspond to the algebras which satisfy them "up to observations". For this reason, in our approach, we loosen this too restrictive usual satisfaction relation, in order to obtain an observational satisfaction relation "$\underline{\models}$", more permissive than "$\models$" in the sense that $\underline{\models}$ contains $\models$.

Assume now that the elements of some data type can only be observed via some available observations. In this situation, it is impossible to distinguish some data type elements from the others. This fact can be reflected by an indistinguishability relation, written "$\sim$", defined on a carrier of an algebra according to the following **Indistinguishability Assumption**:

> *Two values are indistinguishable with respect to some observations when it is impossible to establish that they are different, using these observations.*

Now, the idea to loosen the satisfaction relation is to use "$\sim$" instead of "=" in the definition of the satisfaction relation. The usual satisfaction $A \models (t = t')$ of an equational axiom is based on the set-theoretical equality "=" of the results of the evaluation of both t and t' in A, while an observational satisfaction should be based on whether these results are indistinguishable (i.e. related by "$\sim$") or not. Then the crucial point is to define the "$\sim$" relation, according to the Indistinguishability Assumption. Obviously, such a relation does not coincide with "=". Unlike in [16], [17] or [10] but similarly to [1] and [5] we want to consider more general observations than sort observation since sort observation does not provide the satisfactory expressive power (as shown in [2]). Unfortunately, an indistinguishability relation defined w.r.t. such general observations is not a congruence in general (see [5]). It may even not be an equivalence relation. As a matter of fact, according to the Indistinguishability Assumption, the observations only allow to decide that two elements should be distinct but not to decide that they are equal. We overcome this problem by introducing an observational equality "$\cong$" included in "$\sim$". This leads us to the concept of observational algebras which are of the form $\langle A, \cong \rangle$ where A is an algebra (in the usual sense) equipped with an equivalence relation $\cong$.

We discuss the conditions which make our formalism provide an institution [8], [9]. A first obvious condition is to attach the observations to some institution component. Since the observations act on the semantics of a specification in the same way as the axioms, we believe that the observations should be attached to the formulae part. Beside observational algebras, we also introduce observational formulae which are of the form $\langle \varphi, \mathrm{W} \rangle$ with φ a (usual) formula and W a set of observable terms attached to it. In order to define an institution in such an approach, we investigate the relations between the variance (translation) of observational formulae and the covariance ("σ-reduct") of observational algebras.

In [2], the existing observational techniques have been classified in decreasing order of expressive power as follows: formula, atom, term, operation and sort observation. Thus we should justify why we restrict now to term observation, while formula observation is the most powerful. The reason is that it is hard to define an indistinguishability relation w.r.t. formula or atom observation and requires a more elaborated framework [14]. In our opinion this is due to the fact that formula and atom observations have no direct meaning at the (imple-

menting) software level. On the contrary, observing some chosen terms may be viewed at this level as observing the results of some computations, since the evaluation of an instantiated term clearly corresponds to a computation. This is probably the reason why we did not find practical examples which would motivate the necessity of formula or atom observations.

The approach we develop in this paper attempts to extend the class of the models of an algebraic specification by loosening the satisfaction relation. On the other hand there are approaches where this extension is made by means of an equivalence relation $\equiv_{\mathrm{Obs}}$ on algebras (called **behavioural equivalence**) depending on some observations Obs. In these approaches, the class of "observational models" (also called behaviours), denoted by $\mathbf{Beh}[\mathbf{SP}, \mathbf{Obs}]$, which should correspond to the correct realization of a specification SP, is usually defined in the following way:

$$\mathrm{Beh}[\mathrm{SP}, \mathrm{Obs}] \quad = \quad \{B \in \mathrm{Alg}[\mathrm{Sig}[\mathrm{SP}]] \mid \exists\ A \in \mathrm{Alg}[\mathrm{SP}], A \equiv_{\mathrm{Obs}} B\} \qquad (1.\mathrm{i})$$

Based on this notion, in [19] Sannella and Tarlecki have developed an institution independent formalism.

Even if very general, in our opinion, these approaches do not provide a satisfactory observational semantics. It turns out that in some cases, we know of some realizations that we would like to consider as being correct, but unfortunately these realizations cannot be shown to be behaviourally equivalent to any of the (usual) models of the specification at hand. A typical example of such a situation, namely when $\mathrm{Alg}[\mathrm{SP}] = \emptyset$, is given in the next section.

2 A Motivating Example

Let SWC (see Figure 2.1) be a usual specification of sets of natural numbers with an additional operation $\mathsf{choose} : \mathsf{Set} \to \mathsf{Nat}$, defined by the axiom $\mathsf{s} \neq \emptyset \Rightarrow \mathsf{choose}(\mathsf{s}) \in \mathsf{s} = \mathsf{true}$. By this axiom we require choose to return an arbitrary element of an nonempty set. Consider a usual algebra L of lists of natural numbers. Clearly, lists behaves like sets provided that we do not observe them directly but only via the membership operation. For this reason we can consider L as an "observational model" of SWC, choose being realized by car. In this realization the lists nm and mn (with $n \neq m$) are observationally equal, since they are viewed as the same set $\{\mathrm{n}, \mathrm{m}\}$. However $choose(nm)$ and $choose(mn)$ produces two Nat values which should not be observationally equal. Accordingly, we should not request the indistinguishability relation to be a congruence. This opens new perspectives in writing specifications because some inconsistent specifications (in the usual sense) can be "observationally consistent" provided that the inconsistencies are not observed. This allows some data types to be specified in a straightforward way with less risk of introducing unexpected inconsistencies. For instance in Figure 2.1, sets of natural numbers with an operation enum, which enumerates a set to a list, have been specified in a very natural way. Unfortunately this specification is inconsistent in the usual sense. Thus in the approaches based on behavioural equivalence, from (1.i), we have $\mathrm{Beh}[\mathrm{SP}, \mathrm{Obs}] = \emptyset$ for any set of observations Obs. On the contrary, in an approach with an observational satisfaction relation this specification can have models (sets can be realized by list, enum being the identity), provided that the inconsistencies are not observed (i.e. the terms in which enum occurs are not observable). Notice by the way that sort observation is not sufficient in this case.

As a summary we state the following claims:

1. *An observational equality depends on observations. Since they are proper to a data type, each data type owns its proper observational equality.*

spec : SWE
  use : LIST, NAT, BOOL
sort : Set
generated by :
  $\emptyset$: $\rightarrow$ Set
  ins: Nat Set $\rightarrow$ Set
operations :
  $\_\in\_$: Nat Set $\rightarrow$ Bool
  del : Nat Set $\rightarrow$ Set
  enum : Set $\rightarrow$ List
axioms :
  ψ_1: ins(x,ins(x,s)) = ins(x,s)
  ψ_2: ins(x,ins(y,s)) = ins(y,ins(x,s))
  ψ_3: del(x,$\emptyset$) = $\emptyset$
  ψ_4: del(x,ins(x,s)) = del(x,s)
  ψ_5: x $\neq$ y $\Rightarrow$ del(x,ins(y,s)) = ins(y,del(x,s))
  ψ_6: x $\in$ $\emptyset$ = false
  ψ_7: x $\in$ ins(x,s) = true
  ψ_8: x $\neq$ y $\Rightarrow$ x $\in$ ins(y,s) = x $\in$ s
  ψ_9: enum($\emptyset$) = nil
ψ_{10}: enum(ins(x,s)) = cons(x,enum(s))
	spec : SWC
	  use : NAT, BOOL
	sort : Set
	generated by :
	  $\emptyset$: $\rightarrow$ Set
	  ins: Nat Set $\rightarrow$ Set
	operations :
	  $\_\in\_$: Nat Set $\rightarrow$ Bool
	  del : Nat Set $\rightarrow$ Set
	  choose : Set $\rightarrow$ Nat
	axioms :
	  ins(x,ins(x,s)) = ins(x,s)
	  ins(x,ins(y,s)) = ins(y,ins(x,s))
	  del(x,$\emptyset$) = $\emptyset$
	  del(x,ins(x,s)) = del(x,s)
	  x $\neq$ y $\Rightarrow$ del(x,ins(y,s)) = ins(y,del(x,s))
	  x $\in$ $\emptyset$ = false
	  x $\in$ ins(x,s) = true
	  x $\neq$ y $\Rightarrow$ x $\in$ ins(y,s) = x $\in$ s
	  s $\neq$ $\emptyset$ $\Rightarrow$ choose(s) $\in$ s = true

Figure 2.1: Specification of sets with enum and with choose

2. *The operations do not necessarily preserve observational equalities (i.e. "$\sim$ " is not necessarily a congruence).*

3. *Two distinguishable elements cannot be equal. Two indistinguishable elements are not necessarily equal.*

3 Basic Definitions

We assume that the reader is familiar with algebraic specifications (see e.g. [7] or [11]). A **signature Σ** consists of a finite set S of **sort symbols** and a finite set of **operation names with arities** ambiguously denoted by Σ. We assume that each signature Σ is provided with an S-sorted set of variables X such that X_s is countable for each $s \in S$. We use the following conventions. Given a signature Σ (resp. Σ'), S (resp. S$'$) denotes the sorts of Σ (resp. of Σ') and X (resp. X$'$) denotes the variables of Σ (resp. of Σ'). A **signature morphism** $\sigma : \Sigma \rightarrow \Sigma'$ maps each sort of S to a sort of S$'$, each operation $(f : s_1 \ldots s_n \rightarrow s) \in \Sigma$ to an operation $\sigma(f)$ of Σ' with the arity $\sigma(s_1) \ldots \sigma(s_n) \rightarrow \sigma(s)$ and each variable of X_s to a variable of $X'_{\sigma(s)}$. Moreover, we assume that a signature morphism is always injective on variables[1]. Signatures with signature morphisms form the usual category of signatures, written **Sig**.

From $T_\Sigma(X)$, the "=" symbol, connectives ($\neg$, $\vee$, $\wedge$, $\Rightarrow$, etc.) and quantifiers ($\forall$, $\exists$) we construct the set **Wff[Σ]** of **well formed Σ-formulae**. The definition of **(total) Σ-algebras** and **Σ-morphisms** is the standard one, as well as the satisfaction relation between Σ-algebras

[1] Without this assumption, which under a stronger form appears in [9] (page 36, Definition 55), it would be impossible to establish the satisfaction condition for most institutions.

and Σ-formulae. The **category of all Σ-algebras** is denoted by $\mathbf{Alg[\Sigma]}$. 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 **Σ-algebra of ground terms** (resp. **terms with variables**), $\mathbf{T_\Sigma}(\boldsymbol{A})$ (resp. $\mathbf{T_\Sigma}(\boldsymbol{A}\cup\mathbf{X})$) denotes the **$\Sigma$-algebra of ground terms** (resp. **terms with variables**) **over the carriers of a Σ-algebra $\boldsymbol{A}$**. Given a signature morphism $\sigma : \Sigma \to \Sigma'$ the **σ-reduct** of a Σ'-algebra A', written $\boldsymbol{A'}_{|\sigma}$ is defined in the usual way and extending it on Σ'-morphisms we obtain the **forgetful functor** $-_{|\sigma} : \mathrm{Alg}[\Sigma'] \to \mathrm{Alg}[\Sigma]$. In the particular case of an inclusion $\Sigma \subseteq \Sigma'$, the corresponding forgetful functor is written $-_{|\Sigma}$.

A **valuation** is a morphism $\nu : \mathrm{X} \to A$ which maps each $\mathrm{x} \in \mathrm{X_s}$ to a value $\mathrm{x}\nu \in A_\mathrm{s}$. The set of all valuations from X to A is written $\mathbf{Val[X,}\boldsymbol{A}\mathbf{]}$. A **partial valuation** is a valuation preceded by an inclusion $\mathrm{X_0} \subseteq \mathrm{X}$. 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 $\overline{\tau}$.

A **position** p in a term t is a sequence of integers which describe the path from the topmost position of t (denoted by the empty sequence) to the **subterm of t at position p** written $\mathbf{t}|_\mathbf{p}$. The set of all the positions of t is denoted by $\mathbf{Pos(t)}$. The replacement of $\mathrm{t}|_\mathrm{p}$ by a term r in t is written $\mathbf{t[r]_p}$. The multiple replacement at parallel positions $\mathrm{p_1}, \ldots, \mathrm{p_n}$ is written $\mathbf{t[r_1 \ldots r_n]_{p_1 \ldots p_n}}$.

Definition 3.1

Given sorts $\mathrm{S} = \{\mathrm{s_1}, \ldots, \mathrm{s_n}\}$ *the* **set of contextual variables** *is the (S-indexed) set* $\Diamond = \{\Diamond_{\mathrm{s_1}}, \ldots \Diamond_{\mathrm{s_n}}\}$ *with* $\{\Diamond_{\mathrm{s_i}}\}$ *called the* **contextual variable of sort $\mathbf{s_i}$**. *A* **multicontext** *(resp.* **context***) over a Σ-algebra A is a partially valued term η with only one (resp. only one occurrence of a) contextual variable. Consequently, the set of all multicontexts over A, written* $\mathbf{MC_\Sigma}(\boldsymbol{A})$ *(the set of all contexts over A is written* $\mathbf{C_\Sigma}(\boldsymbol{A})$*) is defined as follows:*

$$\mathrm{MC}_\Sigma(A) = \bigcup_{\mathrm{s}\in\mathrm{S}} \mathrm{T}_\Sigma(A \cup \{\Diamond_\mathrm{s}\})$$

Given $\eta \in \mathrm{MC}_\Sigma(A)$ (resp. $\eta \in \mathrm{C}_\Sigma(A)$) we can write $\eta : \mathrm{s} \to \mathrm{s}'$ instead of $\eta \in (\mathrm{T}_\Sigma(A \cup \{\Diamond_\mathrm{s}\}))_{\mathrm{s}'}$. Application of $\eta : \mathrm{s} \to \mathrm{s}'$ on $a \in A_\mathrm{s}$ is written $\boldsymbol{\eta}[\boldsymbol{a}]$.

The following definitions and results are very technical and can be skipped at first reading.

Definition 3.2

Given a signature morphism $\sigma : \Sigma \to \Sigma'$ and a Σ'-algebra A', we define $\overline{\sigma_{A'}}$ as the unique application from $A'_{|\sigma}$ to A', which maps any element of $(A'_{|\sigma})_\mathrm{s}$ to the equal element of $A'_{\sigma(\mathrm{s})}$.

Definition 3.3

Let $\sigma : \Sigma \to \Sigma'$ be a signature morphism, A' be a Σ'-algebra. We define $\boldsymbol{\sigma}_{A'} : \mathrm{T}_\Sigma(A'_{|\sigma}) \to \mathrm{T}_{\Sigma'}(A')$ as the unique extension of both $\overline{\sigma_{A'}} : A'_{|\sigma} \to A'$ and $\sigma : \mathrm{T}_\Sigma \to \mathrm{T}_{\Sigma'}$.

Definition 3.4

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

$$\forall\ \mathrm{x} \in \mathrm{X}\quad \sigma(\mathrm{x})\nu' = \overline{\sigma_{A'}}(\mathrm{x}\nu'_{|\sigma}) \tag{3.i}$$

Notice that this definition makes sense, since σ and $\overline{\sigma_{A'}}$ are well defined. The notation $\nu'|_\sigma$ suggests that the relation $-|_\sigma$ defined on the valuations by Equation (3.i) is a function. The following lemma points out this fact.

Lemma 3.5

Let $\sigma : \Sigma \to \Sigma'$ be a signature morphism and A' be a Σ'-algebra. The relation $-|_\sigma$ defined by Equation (3.i) is a total and surjective function $-|_\sigma : \mathrm{Val}[\mathrm{X}', A'] \to \mathrm{Val}[\mathrm{X}, A'|_\sigma]$.

Proof is given in the Appendix.

Lemma 3.6

Let $\sigma : \Sigma \to \Sigma'$ be a signature morphism and A' be a Σ'-algebra. For any valuation $\nu' : \mathrm{X}' \to A'$ and any term $\mathrm{t} \in \mathrm{T}_\Sigma(\mathrm{X})$ we have:

$$\overline{\sigma(\mathrm{t})\nu'} = \overline{\sigma_{A'}}(\overline{\mathrm{t}\nu'|_\sigma})$$

Proof is given in the Appendix.

Corollary 3.7

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:

$$\overline{\sigma_{A'}(\tau)} = \overline{\sigma_{A'}}(\overline{\tau})$$

Proof

It is a trivial consequence of Lemma 3.6 since τ can always be written $\mathrm{t}\nu'|_\sigma$ with $\mathrm{t} \in \mathrm{T}_\Sigma(\mathrm{X})$ and $\nu' : \mathrm{X}' \to A'$ (c.f. Lemma 3.5). □

4 How to Observe and How to Compare

As mentioned in the introduction we need to define an indistinguishability relation on the carriers of an algebra in order to relax the satisfaction relation. Usually this is done using the concept of observable contexts. Since this concept was only defined for sort ([10], [12], [16]) or signature[1] ([1], [5]) observations, we should start by defining it in the situation when we observe an arbitrary set of terms.

In the most usual framework one considers a set of observable sorts $\mathrm{S}_{\mathrm{Obs}}$ which is a subset of the sorts of a specification. Then an observable context is any context $\eta : \mathrm{s} \to \mathrm{s}'$ with $\mathrm{s}' \in \mathrm{S}_{\mathrm{Obs}}$. Given an element $a \in A_\mathrm{s}$ we can observe it via η by evaluating $\eta[a]$. Hence we have the following trivial fact:

Fact 4.1

For sort observation, all the elements of a carrier of an algebra have the same observable contexts w.r.t. a set of observable sorts.

Notice that it is unreasonable to hope that this fact could be extended to term observation. This affirmation is justified by the specification THREE (c.f. Figure 4.1). Let A be a Sig[THREE]-algebra. It is clear that $\mathsf{g}(a^A)$ does not produce an observable value, since $\mathsf{g}(\mathsf{a})$ is not an observable term. Consequently, we should consider $\mathsf{g}(\diamond)$ as an observable context of b^A and c^A only and, for a similar reason, $\mathsf{f}(\diamond)$ as an observable context of a^A and b^A (but not of c^A). It follows from the above that observable contexts cannot be taken into

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

account independently of the elements on which they apply. Therefore, we need to define the observable contexts of a given **element of an algebra**. Notice that such a definition is superfluous for observable sorts.

spec : THREE **sort :** Three, Visible **generated by :** a, b, c : $\rightarrow$ Three **operations :** f, g: Three $\rightarrow$ Visible **axioms :** a = b b = c **observations :** f(a), f(b), g(b), g(c)	**spec :** AD-HOC **use :** Bool **sort :** Hoc **generated by :** a, b, c : $\rightarrow$ Hoc **operations :** f : Hoc Hoc $\rightarrow$ Bool g : Hoc $\rightarrow$ Hoc **observations :** f(a, c), f(b, g(c))

Figure 4.1: Two exotic specifications

Since Fact 4.1 cannot be extended to term observation we have a little trouble to declare some $a, b \in A_s$ indistinguishable. It seems reasonable to compare a and b with the same observable contexts. Thus in the previous example we compare a^A and b^A (resp. b^A and c^A) only via the context $\mathsf{f}(\diamond)$ (resp. $\mathsf{g}(\diamond)$). We also notice that a^A and c^A have no common observable context. Consequently, these two values cannot be compared. However, according to our Indistinguishability Assumption, we do not consider that two elements can either be indistinguishable, distinguishable or incomparable. Our point of view is close to final semantics ([3], [13], [20]): we consider indistinguishable these pairs of elements, for which we do not observe the contrary. This is stated in the undermentioned definition.

For a while assume already defined the notion of observable contexts w.r.t. a set W of observable terms.

Definition (comparator, version 1)
We call **W-comparator** *(or shortly comparator) of elements a and b of a Σ-algebra, an observable context of a and b w.r.t. a set* W *of Σ-terms. We say that a W-comparator η* **distinguishes** *a and b iff $\overline{\eta[a]} \neq \overline{\eta[b]}$.*

We can now state the following definition of indistinguishability:

Definition 4.2
We say that two elements a and b of a given carrier of a Σ-algebra are **indistinguishable** *w.r.t. a set of terms $\mathrm{W} \subseteq \mathrm{T}_\Sigma(\mathrm{X})$ (or* **W-indistinguishable***) written $\boldsymbol{a \sim_{\mathrm{w}} b}$, if there is no* W*-comparator which distinguishes them.*

Now, the crucial point is to define the observable contexts of an element of an algebra. Below we make a first attempt of such a definition. Next, this definition will be progressively refined. In this way we are going to introduce the concept of **continuations** which is one of the originalities of our approach.

Definition (observable contexts version 1)
Let $\mathrm{W} \subseteq \mathrm{T}_\Sigma(\mathrm{X})$ be a set of terms and $a \in A$ be an element of a Σ-algebra. We say that a context $\eta \in \mathrm{C}_\Sigma(A)$ is an **observable context of $\boldsymbol{a}$***, if there is a term $\mathrm{w} \in \mathrm{W}$ and a valuation*

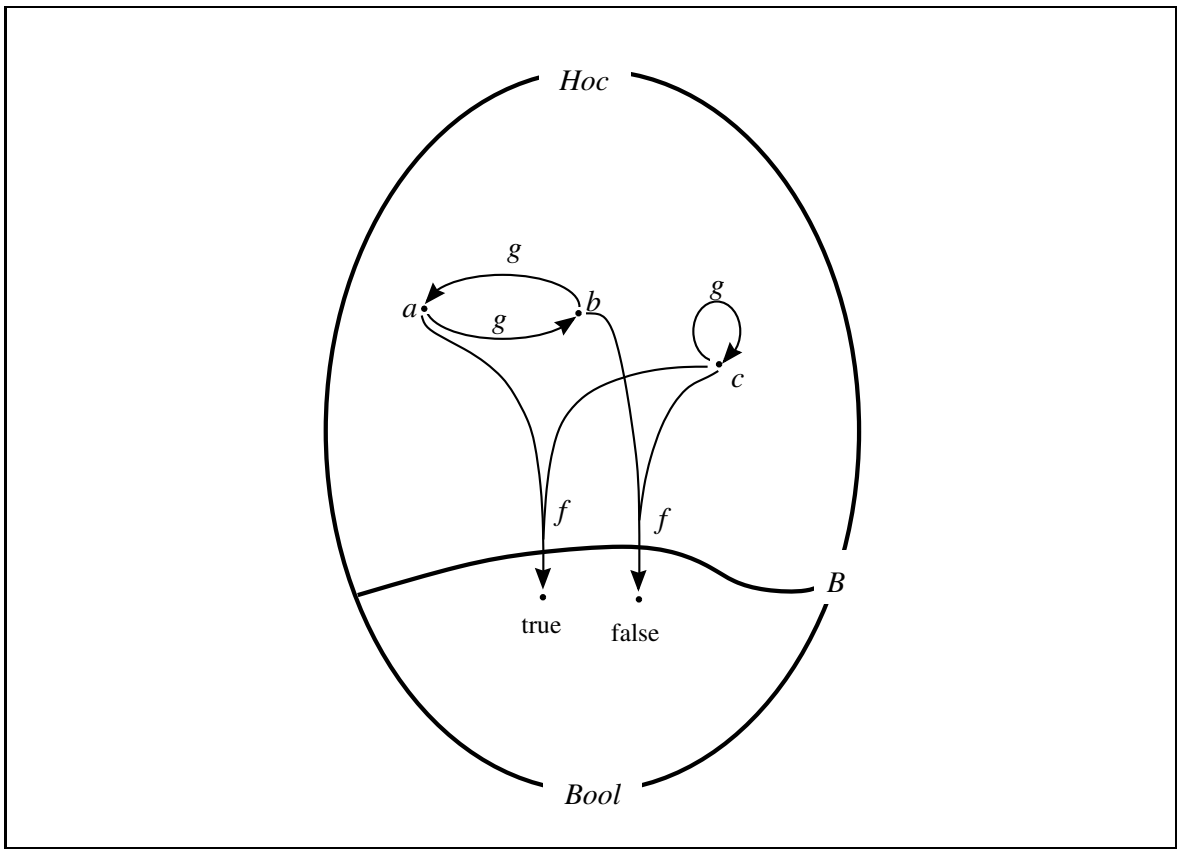


Figure 4.2: A model of the specification AD-HOC

$\nu : \mathrm{X} \to A$ *such that* $\mathrm{w}\nu$ *has a leaf* l *verifying* $\eta[\mathrm{l}] = \mathrm{w}\nu$ *and such that* l *is either the constant of* Σ *interpreted by* A *as* a *or* l *is already* a *itself.*

The underlying intuition of this definition is that an instantiated observable term $\mathrm{w}\nu$ denotes an "observable calculus" i.e. a calculus whose result can be directly observed. Consequently, an observable context η of a, instantiated by a represents an observable calculus with input a. Unfortunately, it is not adequate enough to rely only on input values. For instance consider the specification AD-HOC (c.f. Figure 4.1). According to the current definition, the unique observable context of a^A (resp. b^A) is $\mathsf{f}(\diamond, \mathsf{c})$ (resp. $\mathsf{f}(\diamond, \mathsf{g}(\mathsf{c}))$) independently of the Sig[AD-HOC]-algebra A under consideration. Consequently, a^A and b^A are indistinguishable (no comparator) in any algebra A. Consider now the algebra B given in Figure 4.2 and try to partially evaluate in b the observable contexts of a^B and b^B. Since $\mathsf{g}(\mathsf{c})$ evaluates to c^B, the evaluations of both $\mathsf{f}(\diamond, \mathsf{c})$ and $\mathsf{f}(\diamond, \mathsf{g}(\mathsf{c}))$ yield $\mathsf{f}(\diamond, c^B)$. Then the question whether it is not preferable to consider $\mathsf{f}(\diamond, c^B)$ as a comparator of a^B and b^B clearly arises. Notice that this comparator distinguishes these two values.

Our first version of the definition of observable contexts has also another drawback: the entire carriers of some sorts can be, in an unreasonable way, devoid of observable context, as in the case of the specification PASS-BY (c.f. Figure 4.3). Here the elements of A_{Hidden} have no observable contexts in any algebra A. Thus they are all indistinguishable. Consequently, the algebras with the carrier of Hidden reduced to a singleton should be present among the observational models of PASS-BY. However, this could prevent from preserving the observable properties of Nat. In fact, the specification PASS-BY requires all reachable elements of Nat to

spec : PASS-BY **sort :** Nat, Hidden, Visible **generated by :** 0: $\rightarrow$ Nat succ: Nat $\rightarrow$ Nat **operations :** stage-one: Nat $\rightarrow$ Hidden stage-two: Hidden $\rightarrow$ Visible **axioms :** $0 \neq \mathrm{succ}(x)$ $x \neq \mathrm{succ}(x) \Rightarrow \mathrm{succ}(x) \neq \mathrm{succ}(\mathrm{succ}(x))$ **observations :** stage-two(stage-one(x))	**spec :** SYM **use :** BOOL **sort :** Sym **generated by :** a, b : $\rightarrow$ Sym **operations :** f : Sym Sym $\rightarrow$ Bool **observations :** f(a, a), f(b, b)

Figure 4.3: Yet other exotic specifications

be distinguishable i.e.

$$\mathrm{stage\text{-}two}(\mathrm{stage\text{-}one}(\mathrm{succ}^{\mathrm{i}}(0))) \neq \mathrm{stage\text{-}two}(\mathrm{stage\text{-}one}(\mathrm{succ}^{\mathrm{j}}(0))) \quad \text{for} \quad \mathrm{i} \neq \mathrm{j}$$

should hold in any observational model. Of course, this is impossible when the carrier of Hidden is a singleton. We conclude that in the above example we should consider stage-two($\diamond$) as an observable context of any element which is reachable by the evaluation of stage-one(x) properly instantiated.

The examples PASS-BY and AD-HOC suggest that a better version of the definition of observable contexts should somehow take into account the super-terms of observable terms as well as their partial evaluations. Before to state this version, we need some reminders about partial evaluation.

Definition 4.3

Let A be a Σ-algebra. We define the **partial evaluation relation**, *written $\underset{\mathbf{pEv}}{\rightarrow}$, on $\mathrm{T}_\Sigma(A)$ as follows. We say that a term $\tau_2 \in \mathrm{T}_\Sigma(A)$ is the result of the partial evaluation of $\tau_1 \in \mathrm{T}_\Sigma(A)$, written $\tau_1 \underset{\mathbf{pEv}}{\rightarrow} \tau_2$, if there is a position p in τ_1 such that $\tau_1[\overline{\tau_1|_\mathrm{p}}]_\mathrm{p} = \tau_2$.*

Fact 4.4

The reflexive-transitive closure of $\underset{\mathrm{pEv}}{\rightarrow}$, written $\underset{\mathbf{pEv}}{\overset{*}{\rightarrow}}$, is an order. □

Definition 4.5

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

$$\widetilde{\mathrm{W}}^A = \{\tau \in \mathrm{T}_\Sigma(A) \mid \exists\, \mathrm{w} \in \mathrm{W} \;\; \exists\, \nu : \mathrm{X} \rightarrow A \quad \mathrm{w}\nu \underset{\mathrm{pEv}}{\overset{*}{\rightarrow}} \tau\}$$

This definition can be used to state a better definition of observable contexts:

Definition (observable contexts, version 2)

Let $\mathrm{W} \subseteq \mathrm{T}_\Sigma(\mathrm{X})$ be a set of observable terms and A be a Σ-algebra. We say that $\eta \in \mathrm{C}_\Sigma(A)$ is an **observable context of $a \in A_\mathrm{s}$** *if $\eta[a] \in \widetilde{\mathrm{W}}^A$.*

According to this definition, an observable context η of $a \in A_s$ is obtained from some valued observable term $w\nu$ ($\nu : X \to A$), if a is an intermediate result of its evaluation. In fact, the above definition requires the term $\eta[a]$ to be obtained from $w\nu$ as a result of its partial evaluation. Thus the context η represents a calculus waiting for an input. If the value a is given as input, then the carrying out of this calculus corresponds exactly to a "continuation" of the evaluation of $w\nu$. However, the case of the specification SYM (c.f. Figure 4.3) shows that this approach is not yet satisfactory. For instance, let A be a Sig[SYM]-algebra such that $f^A(a^A, a^A) = true^A$ and $f^A(b^A, b^A) = false^A$. Applying the last definition we obtain:

$$\begin{array}{ll} \text{observable contexts of } a^A : & \mathsf{f}(\diamond, \mathsf{a}), \mathsf{f}(\mathsf{a}, \diamond) \\ \text{observable contexts of } b^A : & \mathsf{f}(\diamond, \mathsf{b}), \mathsf{f}(\mathsf{b}, \diamond) \end{array}$$

Since the elements a^A and b^A have no comparator, they are declared indistinguishable. Nevertheless, the evaluation of the terms f(a, a) and f(b, b) allows to distinguish a^A and b^A. This motivates to consider $\mathsf{f}(\diamond, \diamond)$ as a comparator of a^A and b^A. Consequently, **an adequate definition of continuation should be based on multicontexts instead of contexts**:

Definition 4.6

Let $W \subseteq T_\Sigma(X)$ be a set of observable terms and a be an element of a Σ-algebra A. We say that a multicontext $\eta \in MC_\Sigma(A)$ is a **W-continuation via a** *(a continuation via a, for short) if $\eta[a] \in \widetilde{W}^A$. The set of W-continuations via a is written* $\mathbf{cont_W(a)}$. *(If there is no ambiguity we omit the index W in this notation.)*

The definition of indistinguishability (c.f. 4.2) remains unchanged provided that we modify the definition of comparator which must be based on the notion of continuation.

Definition 4.7

A **W-comparator** *(comparator, for short) of elements a and b of a given carrier of Σ-algebra, is any W-continuation via a and b. The set of all comparators of a and b is denoted by* $\mathbf{cmp_W(a, b)}$. *(If there is no ambiguity we omit the index W in this notation.) We say that a W-comparator η* **distinguishes** *a and b iff $\overline{\eta[a]} \neq \overline{\eta[b]}$.*

We illustrate the concepts introduced so far by means of the specification SWE (see Figure 2.1).

Example 4.8

Let Γ_{SWE} be the signature of SWE *except the* enum *operation. Consider the following set of observable terms $Obs_{SWE} = (T_{\Gamma_{SWE}}(X))_{Bool} \cup (T_{\Gamma_{SWE}}(X))_{Nat}$. Assume that we enrich* SWE *with the operation* idl : List → List *defined by the axiom* idl(l) = l. *(This operation, without any practical interest, aims at precisely define an algebra as a σ-reduct of another one.) Since* SWE *is an enrichment of* LIST *we can write*

$$Sig[SWE] = Sig[LIST] + \Delta\Sigma$$

Then we consider the following signature morphism:

$$\begin{array}{lllll} \sigma = \sigma_{LIST} + \Delta\sigma \quad \textit{with} & \sigma_{LIST} : & Sig[LIST] & \to & Sig[LIST] \\ & \Delta\sigma : & \Delta\Sigma & \to & Sig[LIST] \end{array}$$

where σ_{LIST} is the identity morphism and

$$\begin{array}{llllll} \Delta\sigma(Set) = List & \Delta\sigma(\emptyset) = nil & \Delta\sigma(ins) = cons \\ \Delta\sigma(\in) = member & \Delta\sigma(del) = remove & \Delta\sigma(enum) = idl \end{array}$$

Consider the Sig[LIST]*-algebra* L *being the usual realization of lists. Then the* Sig[SWE]*-algebra we are interested in is* $L_{|\sigma}$*. The continuations of* $l \in (L_{|\sigma})_{\mathsf{List}}$ *are the following ones:*

$$\mathrm{cont}(l) \quad = \quad \{\mathsf{car}(\eta), \mathsf{member}(n, \eta) \ \mid \ n \in (L_{|\sigma})_{\mathsf{Nat}},\ \eta \in (\mathrm{MC}_{\Gamma_{\mathsf{SWE}}}(L_{|\sigma}))_{\mathsf{List}}\}$$

Therefore, $\sim_{\mathrm{Obs}_{\mathsf{SWE}}}$ *is the set-theoretical equality on* $(L_{|\sigma})_{\mathsf{List}}$*. The continuations of* $s \in (L_{|\sigma})_{\mathsf{Set}}$ *are the following ones:*

$$\mathrm{cont}(s) \quad = \quad \{n{\in}\eta \ \mid \ n \in (L_{|\sigma})_{\mathsf{Nat}},\ \eta \in (\mathrm{MC}_{\Gamma_{\mathsf{SWE}}}(L_{|\sigma}))_{\mathsf{Set}}\}$$

Thus $s, s' \in (L_{|\sigma})_{\mathsf{Set}}$ *are indistinguishable if they contain the same elements.*

We would like to propose an institution for observational specifications. Since our observational satisfaction relation (which will be defined further) strongly depends on continuations, we must first study their properties w.r.t. the forgetful functor and the translation of observable terms. In this way, we are going to 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 opportunity to establish some interesting lemmas about partial evaluation.

Theorem 4.9

Let $\sigma : \Sigma \to \Sigma'$ *be a signature morphism,* $\mathrm{W} \subseteq \mathrm{T}_{\Sigma}(\mathrm{X})$ *and* $\mathrm{W}' \subseteq \mathrm{T}_{\Sigma'}(\mathrm{X}')$ *be sets of terms such that* $\sigma(\mathrm{W}) \subseteq \mathrm{W}'$ *and* A' *be a* Σ'*-algebra. For any element* $a \in A'_{|\sigma}$ *and any multicontext* $\eta \in \mathrm{MC}_{\Sigma}(A'_{|\sigma})$ *we have:*

$$\eta \in \mathrm{cont}_{\mathrm{W}}(a) \quad \Rightarrow \quad \sigma_{A'}(\eta) \in \mathrm{cont}_{\mathrm{W}'}(\overline{\sigma_{A'}}(a))$$

We need the following lemmas for the proof:

Lemma 4.10

Let $\sigma : \Sigma \to \Sigma'$ *be a signature morphism, and* A' *be a* Σ'*-algebra. For all* $\tau_1, \tau_2 \in \mathrm{T}_{\Sigma}(A'_{|\sigma})$ *we have:*

$$\tau_1 \underset{\mathrm{pEv}}{\to} \tau_2 \quad \Rightarrow \quad \sigma_{A'}(\tau_1) \underset{\mathrm{pEv}}{\to} \sigma_{A'}(\tau_2)$$

Proof

By Definition 4.3 *there exists a position* $\mathrm{p} \in \mathrm{Pos}(\tau_1)$ *such that* $\tau_1[\overline{\tau_1|_{\mathrm{p}}}]_{\mathrm{p}} = \tau_2$*. By Corollary* 3.7 *we have*

$$\overline{\sigma_{A'}}(\overline{\tau_1|_{\mathrm{p}}}) = \overline{\sigma_{A'}(\tau_1|_{\mathrm{p}})} = \overline{\sigma_{A'}(\tau_1)|_{\mathrm{p}}}$$

Hence

$$\sigma_{A'}(\tau_2) = \sigma_{A'}(\tau_1[\overline{\tau_1|_{\mathrm{p}}}]_{\mathrm{p}}) = \sigma_{A'}(\tau_1)[\overline{\sigma_{A'}}(\overline{\tau_1|_{\mathrm{p}}})]_{\mathrm{p}} = \sigma_{A'}(\tau_1)[\overline{\sigma_{A'}(\tau_1)|_{\mathrm{p}}}]_{\mathrm{p}}$$

This proves $\sigma_{A'}(\tau_1) \underset{\mathrm{pEv}}{\to} \sigma_{A'}(\tau_2)$*.* □

Lemma 4.11

Let $\sigma : \Sigma \to \Sigma'$ *be a signature morphism, and* A' *be a* Σ'*-algebra. For any* $\tau_1, \tau_2 \in \mathrm{T}_{\Sigma}(A'_{|\sigma})$ *we have:*

$$\tau_1 \underset{\mathrm{pEv}}{\overset{*}{\to}} \tau_2 \quad \Rightarrow \quad \sigma_{A'}(\tau_1) \underset{\mathrm{pEv}}{\overset{*}{\to}} \sigma_{A'}(\tau_2)$$

Proof

Follows directly from the previous lemma. □

Lemma 4.12

Let $\sigma : \Sigma \to \Sigma'$ be a signature morphism, $\mathrm{W} \subseteq \mathrm{T}_\Sigma(\mathrm{X})$ and $\mathrm{W}' \subseteq \mathrm{T}_{\Sigma'}(\mathrm{X}')$ be sets of terms such that $\sigma(\mathrm{W}) \subseteq \mathrm{W}'$ and A' be a Σ'-algebra. For any $\tau \in \mathrm{T}_\Sigma(A'_{|\sigma})$ we have:

$$\tau \in \widetilde{\mathrm{W}}^{A'_{|\sigma}} \quad \Rightarrow \quad \sigma_{A'}(\tau) \in \widetilde{\mathrm{W}'}^{A'}$$

Proof

Assume $\tau \in \widetilde{\mathrm{W}}^{A'_{|\sigma}}$. By Definition 4.5 we have

$$\exists\ \mathrm{w} \in \mathrm{W}\ \ \exists\ \nu : \mathrm{X} \to A'_{|\sigma} \quad \mathrm{w}\nu \xrightarrow[\mathrm{pEv}]{*} \tau$$

By Lemma 4.11 we obtain

$$\exists\ \mathrm{w} \in \mathrm{W}\ \ \exists\ \nu : \mathrm{X} \to A'_{|\sigma} \quad \sigma_{A'}(\mathrm{w}\nu) \xrightarrow[\mathrm{pEv}]{*} \sigma_{A'}(\tau) \qquad \text{(i)}$$

By Lemma 3.5 we know that there exists a valuation $\nu' : \mathrm{X}' \to A'$ such that $\nu'_{|\sigma} = \nu$. It is obvious from Definition 3.4 that $\sigma_{A'}(\mathrm{w}\nu) = \sigma(\mathrm{w})\nu'$. Consequently, from (i)*, we deduce:*

$$\exists\ \mathrm{w} \in \mathrm{W}\ \ \exists\ \nu' : \mathrm{X} \to A' \quad \sigma(\mathrm{w})\nu' \xrightarrow[\mathrm{pEv}]{*} \sigma_{A'}(\tau)$$

Now $\sigma(\mathrm{w}) \in \mathrm{W}'$, hence

$$\exists\ \mathrm{w}' \in \mathrm{W}'\ \ \exists\ \nu' : \mathrm{X} \to A' \quad \mathrm{w}'\nu' \xrightarrow[\mathrm{pEv}]{*} \sigma_{A'}(\tau)$$

By Definition 4.5 this yields $\sigma_{A'}(\tau) \in \widetilde{\mathrm{W}'}^{A'}$. □

Proof of Theorem 4.9

Let $\sigma : \Sigma \to \Sigma'$ be a signature morphism, $\mathrm{W} \subseteq \mathrm{T}_\Sigma(\mathrm{X})$ and $\mathrm{W}' \subseteq \mathrm{T}_{\Sigma'}(\mathrm{X}')$ be sets of terms such that $\sigma(\mathrm{W}) \subseteq \mathrm{W}'$ and A' a be Σ'-algebra. Let $a \in A'_{|\sigma}$.

Assume $\eta \in \mathrm{cont}_{\mathrm{W}}(a)$. By Definition 4.6 we have $\eta[a] \in \widetilde{\mathrm{W}}^{A'_{|\sigma}}$, hence by Lemma 4.12 we deduce $\sigma_{A'}(\eta[a]) \in \widetilde{\mathrm{W}'}^{A'}$. By Definition 4.6 this yields $\sigma_{A'}(\eta) \in \mathrm{cont}_{\mathrm{W}'}(\overline{\sigma_{A'}}(a))$. □

Notice that the converse of the above theorem does not hold even if $\sigma(\mathrm{W}) = \mathrm{W}'$:

Example 4.13

Consider the following signatures:

$$\Sigma = \{\mathrm{f}_1, \mathrm{f}_2 : \mathrm{s} \to \mathrm{s}\} \qquad \Sigma' = \{\mathrm{f}' : \mathrm{s}' \to \mathrm{s}'\}$$

Let $\mathrm{W} = \{\mathrm{f}_1(\mathrm{x})\}$. Let $\sigma : \Sigma \to \Sigma'$ be the following signature morphism:

$$\sigma(\mathrm{s}) = \mathrm{s}' \qquad \sigma(\mathrm{f}_1) = \sigma(\mathrm{f}_2) = \mathrm{f}'$$

It is clear that for any Σ'-algebra A', $\mathrm{f}_2(\diamond)$ is not a W-continuation via any element $a \in A'_{|\sigma}$, whereas $\sigma(\mathrm{f}_2(\diamond)) = \mathrm{f}'(\diamond) \in \mathrm{cont}_{\sigma(\mathrm{W})}(\overline{\sigma_{A'}}(a))$.

However, for injective signature morphisms the converse of Theorem 4.9 holds:

Theorem 4.14

Let $\sigma : \Sigma \to \Sigma'$ be an injective signature morphism, $\mathrm{W} \subseteq \mathrm{T}_\Sigma(\mathrm{X})$ be a set of terms and A' be a Σ'-algebra. For any $a \in A'_{|\sigma}$ and any $\eta \in \mathrm{MC}_\Sigma(A'_{|\sigma})$ we have:

$$\eta \in \mathrm{cont}_{\mathrm{W}}(a) \quad \Leftrightarrow \quad \sigma_{A'}(\eta) \in \mathrm{cont}_{\sigma(\mathrm{W})}(\overline{\sigma_{A'}}(a))$$

Proof sketch

Since σ is injective, $\sigma_{A'}$ is too. Then, for $\mathrm{W}' = \sigma(\mathrm{W})$, the implications in lemmas 4.10, 4.11, 4.12 become equivalences. Consequently, we obtain the proof we are looking for, by replacing the implications in the proof of 4.9 by equivalences. □

5 Properties of the Indistinguishability Relation

The definition 4.2 express in which situations two elements of a Σ-algebra are indistinguishable. Indeed, it defines an S-sorted relation $\sim_{\mathrm{W}} = (\sim_{\mathrm{W}})_{s\in S}$ 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 terms. This will be necessary for establishing the satisfaction condition (see [9]) in a further section. After the following proposition devoted to this aim, we study other interesting properties of the indistinguishability relation.

Proposition 5.1

Let $\sigma : \Sigma \to \Sigma'$ be a signature morphism, let $\mathrm{W} \subseteq \mathrm{T}_\Sigma(\mathrm{X})$ and $\mathrm{W}' \subseteq \mathrm{T}_{\Sigma'}(\mathrm{X}')$ be sets of terms such that $\sigma(\mathrm{W}) \subseteq \mathrm{W}'$ and A' be a Σ'-algebra. For all $a', b' \in {A'}_{\sigma(s)}$ and $a, b \in (A'_{|\sigma})_s$ verifying $\overline{\sigma_{A'}}(a) = a'$ and $\overline{\sigma_{A'}}(b) = b'$ we have:

$$a' \sim_{\mathrm{W}'} b' \quad \Rightarrow \quad a \sim_{\mathrm{W}} b$$

Proof of Proposition 5.1

Let $a', b' \in {A'}_{\sigma(s)}$ such that $a' \sim_{\mathrm{W}'} b'$. Assume by contradiction that there exist $a, b \in (A'_{|\sigma})_s$ such that

$$\overline{\sigma_{A'}}(a) = a' \quad \overline{\sigma_{A'}}(b) = b' \quad \text{and} \quad a \not\sim_{\mathrm{W}} b$$

According to Definition 4.2 there exists $\eta \in \mathrm{cmp}_{\mathrm{W}}(a, b)$ such that

$$\overline{\eta[a]} \neq \overline{\eta[b]} \tag{i}$$

By definition of comparator (c.f. 4.7) η is an element of $\mathrm{cont}_{\mathrm{W}}(a)$ and $\mathrm{cont}_{\mathrm{W}}(b)$. On the other hand, it is clear that

$$\sigma_{A'}(\eta)[a'] = \sigma_{A'}(\eta[a]) \quad \text{and} \quad \sigma_{A'}(\eta)[b'] = \sigma_{A'}(\eta[b]) \tag{ii}$$

From Corollary 3.7 we have therefore

$$\overline{\sigma_{A'}(\eta[a])} = \overline{\sigma_{A'}}(\overline{\eta[a]}) \quad \text{and} \quad \overline{\sigma_{A'}(\eta[b])} = \overline{\sigma_{A'}}(\overline{\eta[b]}) \tag{iii}$$

From (i), (ii) *and* (iii) *we obtain*

$$\overline{\sigma_{A'}(\eta)[a']} \neq \overline{\sigma_{A'}(\eta)[b']} \tag{iv}$$

Now, from Theorem 4.9 we know that $\sigma_{A'}(\eta)$ is an element of $\mathrm{cont}_{\mathrm{W}'}(a')$ (resp. $\mathrm{cont}_{\mathrm{W}'}(b')$). Accordingly, it is a comparator of a' and b' and by (iv) *it distinguishes a' and b'. This is in contradiction with the starting hypothesis.* □

As a corollary of this proposition, we have the following fact which makes clear the decreasing character of the indistinguishability relation w.r.t. the inclusion sets of observable terms.

Corollary 5.2

Let $\mathrm{W}_1, \mathrm{W}_2$ be two sets of Σ-terms such that $\mathrm{W}_1 \subseteq \mathrm{W}_2$. On any Σ-algebra, the indistinguishability relations $\sim_{\mathrm{W}_1}$ and $\sim_{\mathrm{W}_2}$ satisfy $\sim_{\mathrm{W}_2} \subseteq \sim_{\mathrm{W}_1}$.

Proof

It is enough to consider the previous proposition with $\Sigma = \Sigma'$, $\mathrm{W} = \mathrm{W}_1$, $\mathrm{W}' = \mathrm{W}_2$ and σ the identity. □

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

Fact 5.3

The indistinguishability relation is reflexive and symmetric. □

The next fact fully agrees with our claims:

Fact 5.4

The indistinguishability relation is not a congruence in general.

Proof

It is enough to go back to Example 4.8. *Recall that in the algebra* $L_{|_\sigma}$, *sets are represented by lists. Let then* $\langle n, m\rangle$ *and* $\langle m, n\rangle$ *be two representations of the set* $\{n, m\}$ *in this algebra. On one hand we have* $\langle n, m\rangle \sim_{\mathrm{Obs_{SWE}}} \langle m, n\rangle$ *but on the other hand* $enum^{L}{}_{|\sigma}(\langle n, m\rangle) \not\sim_{\mathrm{Obs_{SWE}}} enum^{L}{}_{|\sigma}(\langle m, n\rangle)$ *because of the comparator* $\mathsf{car}(\diamond)$ *which distinguishes them.* □

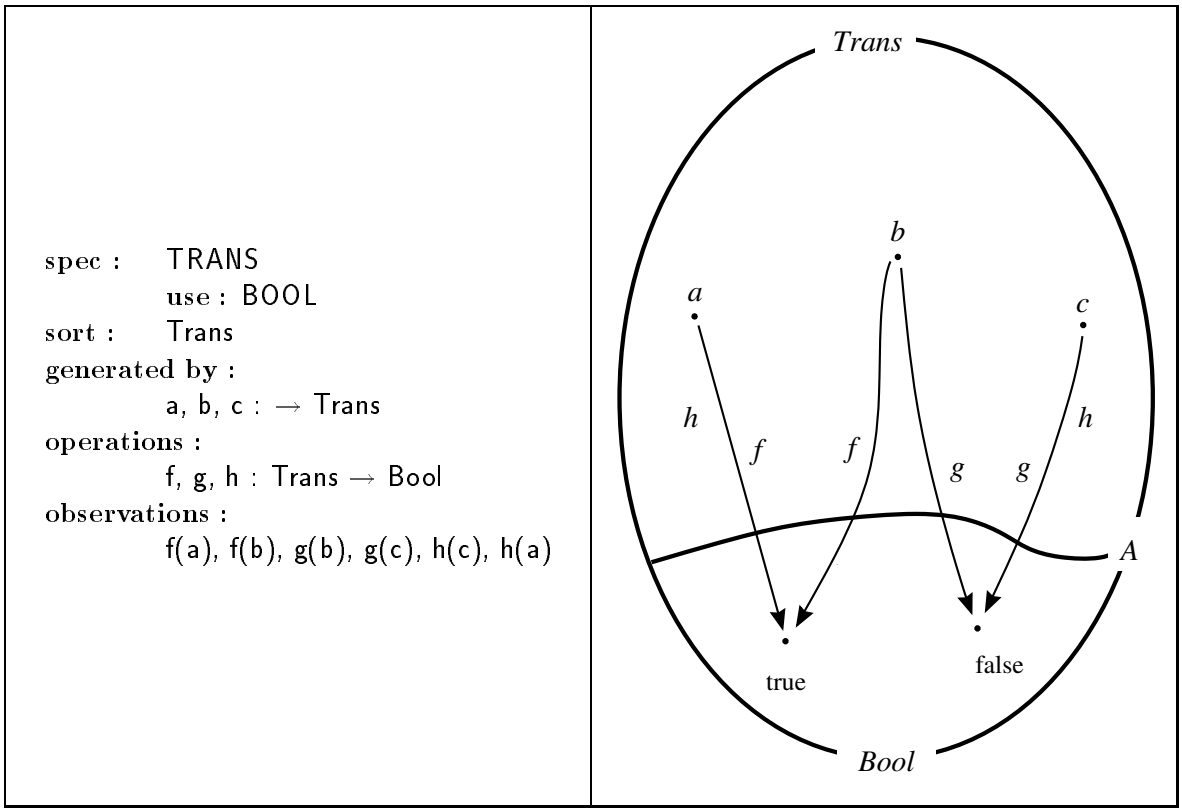


Figure 5.1: Specification TRANS and one of its models

We have also an unexpected negative result:

Fact 5.5

The indistinguishability relation is not transitive in general.

Consider the model A (see Figure 5.1) of the specification TRANS. In this algebra we have $a^A \sim_{\mathrm{W}} b^A$ and $b^A \sim_{\mathrm{W}} c^A$, but not $a^A \sim_{\mathrm{W}} c^A$. The reason is that we did not impose any restriction on the set of observable terms. Consequently, nothing ensures that all the elements of a given data type can be observed in the same way. In the algebra A each of the elements a^A, b^A, c^A is observed differently, each pair among this elements is compared in some proper way, different from the others. This is the reason why the indistinguishability relation is not transitive. In fact, this surprising property results directly from our Indistinguishability Assumption according to which we have built definitions 4.2, 4.6 and 4.7. However, when all the elements of a given carrier of an algebra have the same continuations, the indistinguishability relation is transitive:

Fact 5.6

Let A *be a* Σ*-algebra and* W *be a set of* Σ*-terms. If* $\mathrm{cont_W}(a) = \mathrm{cont_W}(b)$ *for all* $a, b \in A_{\mathrm{s}}$ *then the relation* $\sim_{\mathrm{W}}$ *is transitive on* A.

Proof

Obvious. □

It is possible to have a definition of "$\sim_{\mathrm{W}}$" which is always transitive. One may state that a and b are W-indistinguishable if they do in the sense of Definition 4.2 and if additionally $\mathrm{cont}_{\mathrm{W}}(a) = \mathrm{cont}_{\mathrm{W}}(b)$. In our opinion, such a definition will distinguish too much. For instance, if in a specification we observe only some **ground** terms then, according to Definition 4.2, a non reachable value will never be distinguished from any other value, whereas with the modified version of this definition, a non reachable value will always be distinguished from any reachable value. Consequently we are not enthusiastic about such a modification.

Fact 5.7

The relation $\sim_{\mathrm{Obs_{SWE}}}$ *from Example* 4.8 *is transitive.*

Proof

Follows directly from the above proposition, since in Example 4.8 *we have shown that the elements of the same carrier of* $L_{|\sigma}$ *have the same continuations.* □

Fact 5.6 provides a semantical transitivity criterion of the indistinguishability relation. There exist also some syntactical criteria. We describe them in the next section.

6 A Particular Case of Term Observation

An interesting case arises when the set of observable terms is described by a *partial subsignature* defined precisely by the following definition:

Definition 6.1

Let Σ *be a signature. A* **partial subsignature of** Σ *(partial signature for short) is a pair* $\langle \mathrm{S}_1, \Sigma_0 \rangle$ *such that* Σ_0 *is a subsignature of* Σ *and* S_1 *is a subset of sorts of* Σ_0*. The set of terms* $\mathrm{T}_{\langle \mathrm{S}_1, \Sigma_0 \rangle}(\mathrm{X})$ *of a partial signature* $\langle \mathrm{S}_1, \Sigma_0 \rangle$ *(the set of* $\langle \mathrm{S}_1, \Sigma_0 \rangle$*-terms) is defined as follows:*

$$\mathrm{T}_{\langle \mathrm{S}_1, \Sigma_0 \rangle}(\mathrm{X}) = \coprod_{\mathrm{s} \in \mathrm{S}_1} (\mathrm{T}_{\Sigma_0}(\mathrm{X}))_{\mathrm{s}}$$

This kind of sets of terms is interesting because the indistinguishability relation generated by such a set is transitive on any algebra. In order to make this point clear, we first introduce an auxiliary definition of $\langle \mathrm{S}_1, \Sigma_0 \rangle$*-indistinguishability*. This is a transitive relation. We show then that this relation is the same that the $\mathrm{T}_{\langle \mathrm{S}_1, \Sigma_0 \rangle}(\mathrm{X})$-indistinguishability (in the sense of Definition 4.2). This last result allows to conclude that any $\mathrm{T}_{\langle \mathrm{S}_1, \Sigma_0 \rangle}(\mathrm{X})$-indistinguishability is transitive on all Σ-algebras.

Definition 6.2

Let $\langle \mathrm{S}_1, \Sigma_0 \rangle$ *be a partial subsignature of* Σ *and* A *be a* Σ*-algebra. We say that* $a, b \in A_{\mathrm{s}}$ *are* $\langle \mathrm{S}_1, \Sigma_0 \rangle$*-indistinguishable, written* $a \sim_{\langle \mathrm{S}_1, \Sigma_0 \rangle} \mathrm{b}$*, if for any term* $\mathrm{t} \in \mathrm{T}_{\langle \mathrm{S}_1, \Sigma_0 \rangle}(\mathrm{X})$ *with at least one variable* x_{s} *of sort* s *and for all the valuations* $\nu_1, \nu_2 \in \mathrm{Val}[\mathrm{X}, A]$ *which coincide everywhere except at* x_{s} *where* $\mathrm{x}_{\mathrm{s}}\nu_1 = a$ *and* $\mathrm{x}_{\mathrm{s}}\nu_2 = b$*, we have*

$$\overline{\mathrm{t}\nu_1} = \overline{\mathrm{t}\nu_2}$$

Proposition 6.3

Let $\langle \mathrm{S}_1, \Sigma_0 \rangle$ *a partial subsignature of* Σ*. The relation of* $\langle \mathrm{S}_1, \Sigma_0 \rangle$*-indistinguishability is transitive on all* Σ*-algebras.*

Proof

Consider $a, b, c \in A_s$ *such that* $a \sim_{\langle S_1, \Sigma_0\rangle} b$ *and* $b \sim_{\langle S_1, \Sigma_0\rangle} c$. *From Definition* 6.2, *this amounts to say that* $\overline{t\nu_1} = \overline{t\nu_2} = \overline{t\nu_3}$ *for any term* $t \in T_{\langle S_1, \Sigma_0\rangle}(X)$ *and all the valuations* $\nu_1, \nu_2, \nu_3 \in \mathrm{Val}[X, A]$ *which coincide everywhere except at an* $x_s \in \mathrm{Var}[t]$ *where* $x_s\nu_1 = a$, $x_s\nu_2 = b$ *and* $x_s\nu_3 = c$. *Hence, we deduce immediately that*

$$a \sim_{\langle S_1, \Sigma_0\rangle} c$$

□

Theorem 6.4

Let $\langle S_1, \Sigma_0\rangle$ *be a partial subsignature of* Σ *and* A *be a* Σ*-algebra. For all* $a, b \in A_s$ *we have*

$$a \sim_{\langle S_1, \Sigma_0\rangle} b \quad \textit{iff} \quad a \sim_{T_{\langle S_1, \Sigma_0\rangle}(X)} b$$

The proof of this theorem requires a technical definition as well as some additional results.

Definition 6.5

Let A *be a* Σ*-algebra and* $\tau \in T_\Sigma(A)$ *be a valued term. Consider the following set of positions.*

$$\{p_1, \ldots, p_n\} = \{p \in \mathrm{Pos}(\tau) \mid \tau|_p \in A\}$$

We call τ**-derived**, *a term* $t \in T_\Sigma(X)$ *obtained from* τ *by replacement of all its leaves at positions* $p_1, \ldots p_n$ *by distinct variables. In other words* $t = \tau[x_1, \ldots, x_n]_{p_1 \ldots p_n}$ *with* $x_i \neq x_j$ *when* $i \neq j$. *We note* $\mathbf{der}(\tau)$ *the set of all* τ*-derived terms.*

Lemma 6.6

Let $\langle S_1, \Sigma_0\rangle$ *be a partial subsignature of* Σ, t *be a term of* $T_{\langle S_1, \Sigma_0\rangle}(X)$, A *be a* Σ*-algebra and* $\nu : X \to A$ *be a valuation. If* $t\nu \xrightarrow[pEv]{*} \tau$, *where* $\tau \in T_\Sigma(A)$, *then* $\mathrm{der}(\tau) \subseteq T_{\langle S_1, \Sigma_0\rangle}(X)$.

Proof

Obvious, since the sort of any term of $\mathrm{der}(\tau)$ *is in* S_1 *and each operation occurring in it is in* Σ_0. □

Lemma 6.7

Let $\langle S_1, \Sigma_0\rangle$ *be a partial subsignature of* Σ *and* A *be a* Σ*-algebra. For all* $\tau \in \widetilde{T_{\langle S_1, \Sigma_0\rangle}(X)}^A$ *we have*

$$\mathrm{der}(\tau) \subseteq T_{\langle S_1, \Sigma_0\rangle}(X)$$

Proof

Assume $\tau \in \widetilde{T_{\langle S_1, \Sigma_0\rangle}(X)}^A$. *By Definition* 4.5 *we have*

$$\exists\, t \in T_{\langle S_1, \Sigma_0\rangle}(X) \;\; \exists\, \nu : X \to A \quad t\nu \xrightarrow[pEv]{*} \tau$$

Hence, by Lemma 6.6 *we deduce that* $\mathrm{der}(\tau) \subseteq T_{\langle S_1, \Sigma_0\rangle}(X)$. □

Lemma 6.8

Let $\langle S_1, \Sigma_0\rangle$ *be a partial subsignature of* Σ *and* a *be an element of a* Σ*-algebra* A. *For any* $\eta \in \mathrm{cont}_{T_{\langle S_1, \Sigma_0\rangle}(X)}(a)$ *we have*

$$\mathrm{der}(\eta[a]) \subseteq T_{\langle S_1, \Sigma_0\rangle}(X)$$

Proof

Assume $\eta \in \mathrm{cont}_{\mathrm{T}_{\langle \mathrm{S}_1,\Sigma_0\rangle}(\mathrm{X})}(a)$. *By Definition* 4.6 $\eta[a]$ *is an element of* $\widetilde{\mathrm{T}_{\langle \mathrm{S}_1,\Sigma_0\rangle}(\mathrm{X})}^{A}$. *Hence, applying Lemma* 6.7, *we obtain the result we are looking for.* □

Lemma 6.9

Let $\langle \mathrm{S}_1, \Sigma_0\rangle$ *be a partial subsignature of* Σ, A *be a* Σ*-algebra and let* $a, b \in A_{\mathrm{s}}$. *For any* $\eta \in \mathrm{cmp}_{\mathrm{T}_{\langle \mathrm{S}_1,\Sigma_0\rangle}(\mathrm{X})}(a, b)$ *there exists a term* $\mathrm{t} \in \mathrm{T}_{\langle \mathrm{S}_1,\Sigma_0\rangle}(\mathrm{X})$, *and valuations* $\nu_1, \nu_2 \in \mathrm{Val}[\mathrm{X}, A]$ *which coincide everywhere except at* $\mathrm{x_s} \in \mathrm{Var}[\mathrm{t}]$ *where* $\mathrm{x_s}\nu_1 = a$ *and* $\mathrm{x_s}\nu_2 = b$ *and such that* $\eta[a] = \mathrm{t}\nu_1$ *and* $\eta[b] = \mathrm{t}\nu_2$

Proof

Let $\eta \in \mathrm{cmp}_{\mathrm{T}_{\langle \mathrm{S}_1,\Sigma_0\rangle}(\mathrm{X})}(a, b)$ *and* $\mathrm{t}_0 \in \mathrm{der}(\eta[a])$. *It is obvious that* $\mathrm{der}(\eta[a]) = \mathrm{der}(\eta[b])$, *therefore* $\mathrm{t}_0 \in \mathrm{der}(\eta[b])$. *Let* $\{\mathrm{p}_1, \ldots, \mathrm{p}_{\mathrm{n}}\}$ *be all positions of* $\diamond_{\mathrm{s}}$ *in* η *and let* $\mathrm{x_s} \notin \mathrm{Var}[\mathrm{t}_0]$. *Notice that* $\mathrm{Pos}(\eta) = \mathrm{Pos}(\mathrm{t}_0)$. *Consequently, we can consider a term* $\mathrm{t} = \mathrm{t}_0[\mathrm{x_s}]_{\mathrm{p}_1 \ldots \mathrm{p}_{\mathrm{n}}}$. *Since by Lemma* 6.8 t_0 *is in* $\mathrm{T}_{\langle \mathrm{S}_1,\Sigma_0\rangle}(\mathrm{X})$, *we have also* $\mathrm{t} \in \mathrm{T}_{\langle \mathrm{S}_1,\Sigma_0\rangle}(\mathrm{X})$. *By construction of* t, *there exists a valuation* $\nu_1 : \mathrm{X} \to A$ *such that* $\mathrm{t}\nu_1 = \eta[a]$. *Hence* $\mathrm{x_s}\nu_1 = a$. *It is obvious that there exists a valuation* $\nu_2 : \mathrm{X} \to A$ *which coincides with* ν_1 *everywhere except at* $\mathrm{x_s}$ *where* $\mathrm{x_s}\nu_2 = b$. *Then we are done since* $\mathrm{t}\nu_2 = \eta[b]$. □

Proof of Theorem 6.4

Let $\langle \mathrm{S}_1, \Sigma_0\rangle$ *be a partial subsignature of* Σ *and* A *be a* Σ*-algebra. We will proceed by an indirect proof. We show that for all* $a, b \in A_{\mathrm{s}}$ *we have* $a \not\sim_{\langle \mathrm{S}_1,\Sigma_0\rangle} b$ *iff* $a \not\sim_{\mathrm{T}_{\langle \mathrm{S}_1,\Sigma_0\rangle}(\mathrm{X})} b$

- ⇒

Let $a, b \in A_{\mathrm{s}}$ *such that* $a \not\sim_{\langle \mathrm{S}_1,\Sigma_0\rangle} b$. *By definition* 6.2, *there exists a term* $\mathrm{t} \in \mathrm{T}_{\langle \mathrm{S}_1,\Sigma_0\rangle}(\mathrm{X})$ *and valuations* $\nu_1, \nu_2 \in \mathrm{Val}[\mathrm{X}, A]$ *which coincide everywhere except at* $\mathrm{x_s} \in \mathrm{Var}[\mathrm{t}]$ *where* $\mathrm{x_s}\nu_1 = a$ *and* $\mathrm{x_s}\nu_2 = b$, *such that*

$$\overline{\mathrm{t}\nu_1} \neq \overline{\mathrm{t}\nu_2} \tag{i}$$

Let $\{\mathrm{p}_1, \ldots, \mathrm{p}_{\mathrm{n}}\}$ *be the set of positions where* $\mathrm{x_s}$ *occurs in* t. *Consider then a multicontext* $\eta = \mathrm{t}\nu_1[\diamond]_{\mathrm{p}_1 \ldots \mathrm{p}_{\mathrm{n}}}$. *It is obvious that* $\eta = \mathrm{t}\nu_2[\diamond]_{\mathrm{p}_1 \ldots \mathrm{p}_{\mathrm{n}}}$ *and that* $\eta[a] = \mathrm{t}\nu_1$ *and* $\eta[b] = \mathrm{t}\nu_2$. *Now, by Definition* 4.5 *we have* $\mathrm{t}\nu_1, \mathrm{t}\nu_2 \in \widetilde{\mathrm{T}_{\langle \mathrm{S}_1,\Sigma_0\rangle}(\mathrm{X})}^{A}$. *So* $\eta \in \mathrm{cmp}_{\mathrm{T}_{\langle \mathrm{S}_1,\Sigma_0\rangle}(\mathrm{X})}(a, b)$ *and according to* (i), η *distinguishes* a *and* b, *hence* $a \not\sim_{\mathrm{T}_{\langle \mathrm{S}_1,\Sigma_0\rangle}(\mathrm{X})} b$ *by Definition* 4.2.

- ⇐

Let $a, b \in A_{\mathrm{s}}$ *such that* $a \not\sim_{\mathrm{T}_{\langle \mathrm{S}_1,\Sigma_0\rangle}(\mathrm{X})} b$. *By Definition* 4.2, *there exists* $\eta \in \mathrm{cmp}_{\mathrm{T}_{\langle \mathrm{S}_1,\Sigma_0\rangle}(\mathrm{X})}(a, b)$ *such that*

$$\overline{\eta[a]} \neq \overline{\eta[b]} \tag{ii}$$

But according to Lemma 6.9 *there exists a term* $\mathrm{t} \in \mathrm{T}_{\langle \mathrm{S}_1,\Sigma_0\rangle}(\mathrm{X})$, *and valuations* $\nu_1, \nu_2 \in \mathrm{Val}[\mathrm{X}, A]$ *which coincide everywhere except at* $\mathrm{x_s} \in \mathrm{Var}[\mathrm{t}]$ *where* $\mathrm{x_s}\nu_1 = a$ *and* $\mathrm{x_s}\nu_2 = b$ *and such that* $\eta[a] = \mathrm{t}\nu_1$ *and* $\eta[b] = \mathrm{t}\nu_2$. *From* (ii) *we deduce that* $\overline{\mathrm{t}\nu_1} \neq \overline{\mathrm{t}\nu_2}$. *Hence* $a \not\sim_{\langle \mathrm{S}_1,\Sigma_0\rangle} b$, *by Definition* 6.2. □

Corollary 6.10

Let $\langle \mathrm{S}_1, \Sigma_0\rangle$ *be a partial subsignature of* Σ. *The relation of indistinguishability w.r.t. a set of terms* $\mathrm{T}_{\langle \mathrm{S}_1,\Sigma_0\rangle}(\mathrm{X})$ *is transitive on all* Σ*-algebras.*

Proof

Follows immediately from Theorem 6.4 *and Proposition* 6.3. □

We give below an example of an observation of a partial signature:

Example 6.11

Consider the observations $\mathrm{Obs}_{\mathsf{SWE}}$ *from Example* 4.8. *Recall that* $\mathrm{Obs}_{\mathsf{SWE}} = (\mathrm{T}_{\Gamma_{\mathsf{SWE}}}(\mathrm{X}))_{\mathsf{Bool}} \cup (\mathrm{T}_{\Gamma_{\mathsf{SWE}}}(\mathrm{X}))_{\mathsf{Nat}}$. *In fact, this is an observation of a partial subsignature of* $\mathrm{Sig}[\mathsf{SWE}]$, *namely* $\langle \Gamma_{\mathsf{SWE}}, \{\mathsf{Bool}, \mathsf{Nat}\}\rangle$.

Partial signatures are used as observations in [1]. Observational equality w.r.t. $\langle S_1, \Sigma_0 \rangle$ defined in this paper coincides with our $\langle S_1, \Sigma_0 \rangle$-indistinguishability on all reachable algebras. However these two relations do not coincide on non reachable algebras, not even on their reachable parts. If two elements are $\langle S_1, \Sigma_0 \rangle$-indistinguishable then they are also observationally equal w.r.t. $\langle S_1, \Sigma_0 \rangle$ (in the sense of [1]) but the converse is true only for reachable algebras. This is due to the fact that our comparators are elements of $MC_\Sigma(A)$ while these used in [1] can be viewed as elements of MC_Σ. Since $MC_\Sigma \subseteq MC_\Sigma(A)$ we have more possibilities than [1] to distinguish two elements.

7 Observational Algebras

In Section 5 we have shown that the indistinguishability relation is not transitive in general. For this reason, an observational satisfaction relation cannot be directly based on the indistinguishability relation in contrast with the usual satisfaction relation based on the usual equality (of the elements of an algebra). Its non-transitive character (see 5.5) would make impossible the replacement of equals by equals. On the contrary, the non-congruence property (see 5.4) does not reject this possibility, provided that such exotic operations as enum (see Figure 2.1) are treated with care. For instance in some term t of SWE we can replace its subterm $t|_p = \mathsf{ins}(\mathsf{s}(\mathsf{0}), \mathsf{ins}(\mathsf{0}, \emptyset))$ by $\mathsf{ins}(\mathsf{0}, \mathsf{ins}(\mathsf{s}(\mathsf{0}), \emptyset))$ except when there is some enum in t over the position p.[1] In addition we believe that there is no reason to expect an "observational equality" to be a congruence (as in [5]). This happens only in a particular case of sort observation (see [10], [16]).

We can conclude that at this moment the only problem is due to the non-transitive character of the indistinguishability relation. For this reason, we introduce in this section the notion of observational equality which, being transitive, is a step toward an observational satisfaction relation.

At the end of Section 2 we have stated some claims as the result of the former discussion. They lead us now to the following conclusions:

- Because of the second claim, an observational equality cannot be a congruence for the same reason that the indistinguishability relation is not (c.f. 5.4).
- The last claim suggests that on a given algebra, an observational equality is not unique.
- The first claim suggests that observational equality should be an S-sorted relation.

Putting these conclusions together, we state the following definition:

Definition 7.1
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 note* **OAlg[Σ]** *the class of all observational* Σ*-algebras.*

Notice that:

- A Σ-algebra A can be considered in a straightforward way as an observational Σ-algebra $\langle A, = \rangle$.

[1] More precisely, this replacement is impossible only if each node on the path from p to the closest enum over p (if there is one) is of sort Set.

- In general we can form an infinity of observational algebras from a Σ-algebra. For this reason we use the notation $\cong^{\alpha}$ or $\cong^{\beta}$ in order to distinguish between two relations which can form two observational algebras $\langle A, \cong^{\alpha} \rangle$ and $\langle A, \cong^{\beta} \rangle$ from a given algebra A.

The reader certainly realizes that our definition of observational algebras is similar to the one of structures in First Order Logic where each predicate symbol is interpreted by a relation. We consider the equality symbol "=" in the axioms as a particular predicate symbol. This symbol is explicitly interpreted in an algebra by a particular relation, namely an observational equality.

Example 7.2

Consider $L_{|\sigma}$ *and* $\mathrm{Obs}_{\mathsf{SWE}}$ *both defined in Example* 4.8. *Since* $\sim_{\mathrm{Obs}_{\mathsf{SWE}}}$ *is an equivalence relation (c.f.* 5.7*), the pair* $\langle L_{|\sigma}, \sim_{\mathrm{Obs}_{\mathsf{SWE}}} \rangle$ *is an observational* Sig[SWE]*-algebra.*

Definition 7.3

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

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

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

Definition 7.4

Let $\sigma : \Sigma \to \Sigma'$ *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* $(\cong'_{|\sigma})_{\mathrm{s}} = \cong'_{\sigma(\mathrm{s})}$ *for all* $\mathrm{s} \in \mathrm{S}$.

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 we can also view OAlg as 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 $-_{|\sigma}$. Notice that in the above we have provided components upon which an institution can be built.

8 Validity of Observational Formulae

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

Definition 8.1

A **solution** *of an equation* $\mathrm{l} = \mathrm{r}$ *in an observational* Σ*-algebra* $\langle A, \cong \rangle$ *is a valuation* $\nu : \mathrm{X} \to A$ *such that* $\overline{\mathrm{l}\nu} \cong \overline{\mathrm{r}\nu}$. *The set of all the solutions of an equation is written* $\mathbf{[l=r]}_{\langle A, \cong \rangle}$. *The set of solutions of a formula* φ *is defined recursively as follows:*

- *if* $\varphi = \neg\psi$ *then* $[\varphi]_{\langle A, \cong \rangle} = \mathrm{Val}[\mathrm{X}, A] \setminus [\psi]_{\langle A, \cong \rangle}$
- *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* $[\varphi]_{\langle A, \cong \rangle} =$

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

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 (without predicate symbols) are well defined by the above definition.

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

Theorem 8.2

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:

$$[\varphi]_{\langle A', \cong' \rangle}\big|_\sigma = ([\sigma(\varphi)]_{\langle A', \cong' \rangle})\big|_\sigma$$

The proof of this theorem requires the following lemmas:

Lemma 8.3

Let $\sigma : \Sigma \to \Sigma'$ be a signature morphism, $\langle A', \cong' \rangle$ be an observational Σ'-algebra and $\nu \in \mathrm{Val}[\mathrm{X}, A'\big|_\sigma]$ be a valuation. For any Σ-formula ψ we have:

$$\begin{array}{rl} \textit{either} & \{\nu' \in \mathrm{Val}[\mathrm{X}', A'] \mid \nu'\big|_\sigma = \nu\} \subseteq [\sigma(\psi)]_{\langle A', \cong' \rangle} \\ \textit{or} & \{\nu' \in \mathrm{Val}[\mathrm{X}', A'] \mid \nu'\big|_\sigma = \nu\} \cap [\sigma(\psi)]_{\langle A', \cong' \rangle} = \emptyset \end{array}$$

Proof

Consider two valuations $\nu'_1, \nu'_2 \in \mathrm{Val}[\mathrm{X}', A']$ such that $\nu'_1\big|_\sigma = \nu'_2\big|_\sigma = \nu$. According to Definition 3.4, ν'_1 and ν'_2 differ only on values they assign to variables of $\mathrm{X}' \setminus \sigma(\mathrm{X})$. This difference cannot have any effect on the fact whether these valuations are solutions of $\sigma(\psi)$, because $\mathrm{Var}[\sigma(\psi)] \subseteq \sigma(\mathrm{X})$. Consequently, either ν'_1 and ν'_2 are both solutions of $\sigma(\psi)$, or both are not. □

Lemma 8.4

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

$$\mathrm{Val}[\mathrm{X}', A']\big|_\sigma \setminus ([\sigma(\psi)]_{\langle A', \cong' \rangle})\big|_\sigma = (\mathrm{Val}[\mathrm{X}', A'] \setminus [\sigma(\psi)]_{\langle A', \cong' \rangle})\big|_\sigma$$

Proof

- $\subseteq$

This is an obvious set-theoretical inclusion.

- $\supseteq$

Let $\nu \in (\mathrm{Val}[\mathrm{X}', A'] \setminus [\sigma(\psi)]_{\langle A', \cong' \rangle})\big|_\sigma$. From Lemma 8.3 we have

$$\{\nu' \in \mathrm{Val}[\mathrm{X}', A'] \mid \nu'\big|_\sigma = \nu\} \cap [\sigma(\psi)]_{\langle A', \cong' \rangle} = \emptyset$$

Hence $\nu \notin ([\sigma(\psi)]_{\langle A', \cong' \rangle})\big|_\sigma$ □

Lemma 8.5

Let $\sigma : \Sigma \to \Sigma'$ be a signature morphism, $\langle A', \cong' \rangle$ an observational Σ'-algebra and $\nu \in \mathrm{Val}[\mathrm{X}, A'\big|_\sigma]$ be a valuation. For all Σ-formulae φ, ψ we have:

$$([\sigma(\varphi)]_{\langle A', \cong' \rangle})\big|_\sigma \cap ([\sigma(\psi)]_{\langle A', \cong' \rangle})\big|_\sigma = ([\sigma(\varphi]_{\langle A', \cong' \rangle} \cap [\sigma(\psi)]_{\langle A', \cong' \rangle})\big|_\sigma$$

Proof

• $\subseteq$
Let $\nu \in ([\sigma(\varphi]_{\langle A',\cong'\rangle})\big|_\sigma \cap ([\sigma(\psi)]_{\langle A',\cong'\rangle})\big|_\sigma$. *From lemma* 8.3 *we have*

$$\{\nu' \in \mathrm{Val}[\mathrm{X}', A'] \mid \nu'\big|_\sigma = \nu\} \subseteq [\sigma(\varphi)]_{\langle A',\cong'\rangle}$$
$$\text{and} \quad \{\nu' \in \mathrm{Val}[\mathrm{X}', A'] \mid \nu'\big|_\sigma = \nu\} \subseteq [\sigma(\psi)]_{\langle A',\cong'\rangle}$$

Thus

$$\{\nu' \in \mathrm{Val}[\mathrm{X}', A'] \mid \nu'\big|_\sigma = \nu\} \subseteq [\sigma(\varphi)]_{\langle A',\cong'\rangle} \cap [\sigma(\psi)]_{\langle A',\cong'\rangle}$$

Hence

$$\nu \in ([\sigma(\varphi)]_{\langle A',\cong'\rangle} \cap [\sigma(\psi)]_{\langle A',\cong'\rangle})\big|_\sigma$$

• $\supseteq$
This is an obvious set-theoretical inclusion. □

Lemma 8.6

Let $\sigma : \Sigma \to \Sigma'$ *be a signature morphism,* $\langle A', \cong'\rangle$ *be an observational* Σ'*-algebra,* x *be a variable of* X *and* ψ *be a* Σ*-formula. For any valuation* $\nu' \in \mathrm{Val}[\mathrm{X}', A']$ *we have:*

$$\forall\ \mu' \in \mathrm{Val}[\mathrm{X}', A']\ \ (\forall\ \mathrm{y}' \in \sigma(\mathrm{X}) \setminus \{\sigma(\mathrm{x})\}\ \ \mathrm{y}'\mu' = \mathrm{y}'\nu') \ \Rightarrow\ \mu' \in [\sigma(\psi)]_{\langle A',\cong'\rangle} \qquad \text{(i)}$$
$$\textit{iff}\quad \forall\ \mu' \in \mathrm{Val}[\mathrm{X}', A']\ \ (\forall\ \mathrm{y}' \in \mathrm{X}' \setminus \{\sigma(\mathrm{x})\}\ \ \mathrm{y}'\mu' = \mathrm{y}'\nu') \ \Rightarrow\ \mu' \in [\sigma(\psi)]_{\langle A',\cong'\rangle} \qquad \text{(ii)}$$

Proof

We use the following notations in the proof:

$$\mathcal{M}_{\nu'} = \{\mu' \in \mathrm{Val}[\mathrm{X}', A'] \mid \forall\ \mathrm{y}' \in \sigma(\mathrm{X}) \setminus \{\sigma(\mathrm{x})\}\ \ \mathrm{y}'\mu' = \mathrm{y}'\nu'\}$$
$$\mathcal{P}_{\nu'} = \{\mu' \in \mathrm{Val}[\mathrm{X}', A'] \mid \forall\ \mathrm{y}' \in \mathrm{X}' \setminus \{\sigma(\mathrm{x})\}\ \ \mathrm{y}'\mu' = \mathrm{y}'\nu'\}$$

It is obvious that

$$\mathcal{M}_{\nu'} \subseteq [\sigma(\psi)]_{\langle A',\cong'\rangle} \qquad \text{(iii)}$$

is equivalent to (i). *It is also obvious that*

$$\mathcal{P}_{\nu'} \subseteq [\sigma(\psi)]_{\langle A',\cong'\rangle} \qquad \text{(iv)}$$

is equivalent to (ii). *Consequently, it is enough to prove the equivalence between* (iii) *and* (iv).

• (iii) $\Rightarrow$ (iv)
Since in $\mathcal{P}_{\nu'}$ *the quantification domain corresponding to* $\sigma(\mathrm{X}) \setminus \{\sigma(\mathrm{x})\}$ *of* $\mathcal{M}_{\nu'}$ *is extended to* $\mathrm{X}' \setminus \{\sigma(\mathrm{x})\}$, *we have* $\mathcal{P}_{\nu'} \subseteq \mathcal{M}_{\nu'}$, *hence* $\mathcal{P}_{\nu'} \subseteq [\sigma(\psi)]_{\langle A',\cong'\rangle}$.

• (iii) $\Leftarrow$ (iv)
Assume $\mu' \in \mathcal{M}_{\nu'}$ *and show that* $\mu' \in [\sigma(\psi)]_{\langle A',\cong'\rangle}$. *It is clear that there exists* $\varrho' \in \mathcal{P}_{\nu'}$ *which coincides with* μ' *on* $\sigma(\mathrm{X})$. *Since* $\mathrm{Var}[\sigma(\phi)] \subseteq \sigma(\mathrm{X})$, *either* μ' *and* ϱ' *are solutions of* $\sigma(\psi)$ *or none of the both is. Now, by the hypothesis* ϱ' *is a solution of* $\sigma(\psi)$, *therefore* μ' *is also.* □

Lemma 8.7

Let $\sigma : \Sigma \to \Sigma'$ *be a signature morphism,* $\langle A', \cong'\rangle$ *be an observational* Σ'*-algebra,* x *be a variable of* X *and* ψ *be a* Σ*-formula. For any valuation* $\nu' \in \mathrm{Val}[\mathrm{X}', A']$ *we have:*

$$\forall\ \mu' \in \mathrm{Val}[\mathrm{X}', A']\ \ (\forall\ \mathrm{y} \in \mathrm{X} \setminus \{\mathrm{x}\}\ \ \mathrm{y}'\mu'\big|_\sigma = \mathrm{y}'\nu'\big|_\sigma) \ \Rightarrow\ \mu'\big|_\sigma \in ([\sigma(\psi)]_{\langle A',\cong'\rangle})\big|_\sigma \qquad \text{(i)}$$
$$\textit{iff}\quad \forall\ \mu' \in \mathrm{Val}[\mathrm{X}', A']\ \ (\forall\ \mathrm{y}' \in \mathrm{X}' \setminus \{\sigma(\mathrm{x})\}\ \ \mathrm{y}'\mu' = \mathrm{y}'\nu') \ \Rightarrow\ \mu' \in [\sigma(\psi)]_{\langle A',\cong'\rangle} \qquad \text{(ii)}$$

Proof

Notice first that the subformula $\mathrm{y}'\mu'_{|_\sigma} = \mathrm{y}'\nu'_{|_\sigma}$ *of* (i) *is equivalent to* $\overline{\sigma_{A'}}(y'\mu'_{|_\sigma}) = \overline{\sigma_{A'}}(y'\nu'_{|_\sigma})$ *since* $\overline{\sigma_{A'}}$ *is injective, when restricted to the carrier of a given sort. By definition* 3.4 *the last equation is equivalent to* $\sigma(\mathrm{y})\mu' = \sigma(\mathrm{y})\nu'$. *We can therefore replace the left hand side of the implication in* (i) *by* $\forall\ \mathrm{y} \in \mathrm{X} \setminus \{\mathrm{x}\}\ \ \sigma(\mathrm{y})\mu' = \sigma(\mathrm{y})\nu'$. *Since* σ *is injective on variables we can change the quantification domain and variable in order to obtain an equivalent formula:*

$$\forall\ \mathrm{y}' \in \sigma(\mathrm{X}) \setminus \{\sigma(\mathrm{x})\}\ \ \mathrm{y}'\mu' = \mathrm{y}'\nu' \tag{iii}$$

From Lemma 8.3, *we can deduce that the right hand side of the implication in* (i) *is equivalent to* $\mu' \in [\sigma(\psi)]_{\langle A, \cong\rangle}$. *By substituting it as well as formula* (iii) *into* (i) *we obtain the following formula equivalent to* (i)

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

By lemma 8.6 *this last formula is equivalent to* (ii). □

Proof of Theorem 8.2

By structural induction on a formula $\varphi \in \mathrm{Wff}[\Sigma]$ *under the induction hypothesis that the theorem holds for all subformula of* φ.

- **Base step**: φ *is an equation* $\mathrm{l} = \mathrm{r}$

From Definition 8.1 *we have* $\nu \in [\mathrm{l} = \mathrm{r}]_{\langle A', \cong'\rangle_{|_\sigma}}$ *if and only if* $\nu : \mathrm{X} \to A'_{|_\sigma}$ *and*

$$\overline{\mathrm{l}\nu} \cong'_{|_\sigma} \overline{\mathrm{r}\nu} \tag{iv}$$

From Lemma 3.5 *we know that any* $\nu : \mathrm{X} \to A'_{|_\sigma}$ *has the form* $\nu'_{|_\sigma}$ *with* $\nu' : \mathrm{X}' \to A'$ *and that* $\mu'_{|_\sigma}$ *exists for any* $\mu' : \mathrm{X}' \to A'$. *So* (iv) *is equivalent to* $\overline{\mathrm{l}\nu'_{|_\sigma}} \cong'_{|_\sigma} \overline{\mathrm{r}\nu'_{|_\sigma}}$, *by Definition* 7.4 *is equivalent to* $\overline{\sigma_{A'}}(\overline{\mathrm{l}\nu'_{|_\sigma}}) \cong' \overline{\sigma_{A'}}(\overline{\mathrm{r}\nu'_{|_\sigma}})$ *and by Lemma* 3.6 *is equivalent to* $\overline{\sigma(\mathrm{l})\nu'} \cong' \overline{\sigma(\mathrm{r})\nu'}$. *This last formula holds if and only if* $\nu' \in [\sigma(\mathrm{l}) = \sigma(\mathrm{r})]_{\langle A', \cong'\rangle}$.

- **Induction step**

- $\varphi\ =\ \neg\psi$

$$\begin{aligned}
[\neg\psi]_{\langle A', \cong'\rangle_{|_\sigma}} &= \mathrm{Val}[\mathrm{X}, A'_{|_\sigma}] \setminus [\psi]_{\langle A', \cong'\rangle_{|_\sigma}} = && \text{(By the induction hypothesis)}\\
&= \mathrm{Val}[\mathrm{X}, A'_{|_\sigma}] \setminus ([\sigma(\psi)]_{\langle A', \cong'\rangle})_{|_\sigma} = && \text{(By the injectivity of } -_{|_\sigma})\\
&= (\mathrm{Val}[\mathrm{X}', A'])_{|_\sigma} \setminus ([\sigma(\psi)]_{\langle A', \cong'\rangle})_{|_\sigma} = && \text{(By Lemma 8.4)}\\
&= (\mathrm{Val}[\mathrm{X}', A'] \setminus [\sigma(\psi)]_{\langle A', \cong'\rangle})_{|_\sigma} = && \text{(By Definition 8.1)}\\
&= ([\neg\sigma(\psi)]_{\langle A', \cong'\rangle})_{|_\sigma} =\\
&= ([\sigma(\neg\psi)]_{\langle A', \cong'\rangle})_{|_\sigma}
\end{aligned}$$

- $\varphi\ =\ \psi_1 \wedge \psi_2$

$$\begin{aligned}
[\psi_1 \wedge \psi_2]_{\langle A', \cong'\rangle_{|_\sigma}} &= [\psi_1]_{\langle A', \cong'\rangle_{|_\sigma}} \cap\ [\psi_2]_{\langle A', \cong'\rangle_{|_\sigma}} = && \text{(By the induction hypothesis)}\\
&= ([\sigma(\psi_1)]_{\langle A', \cong'\rangle})_{|_\sigma} \cap\ ([\sigma(\psi_2)]_{\langle A', \cong'\rangle})_{|_\sigma} = && \text{(By Lemma 8.4)}\\
&= ([\sigma(\psi_1)]_{\langle A', \cong'\rangle} \cap\ [\sigma(\psi_2)]_{\langle A', \cong'\rangle})_{|_\sigma} = && \text{(By Definition 8.1)}\\
&= ([\sigma(\psi_1) \wedge \sigma(\psi_2)]_{\langle A', \cong'\rangle})_{|_\sigma} =\\
&= ([\sigma(\psi_1 \wedge \psi_2)]_{\langle A', \cong'\rangle})_{|_\sigma}
\end{aligned}$$

- $\varphi\ =\ \forall \mathrm{x}\ \psi$

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

(by the induction hypothesis)

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

(by injectivity of $-_{|\sigma}$ on valuations)

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

(by Lemma 8.7)

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

(by Definition 8.1)

$$= ([\forall\sigma(\mathrm{x})\ \sigma(\psi)]_{\langle A', \cong'\rangle})_{|\sigma} = ([\sigma(\forall \mathrm{x}\ \psi)]_{\langle A', \cong'\rangle})_{|\sigma}$$ □

Definition 8.8

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

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 cartesian product of its usual extensions on $\mathrm{Wff}[\Sigma]$ and $\mathrm{T}_\Sigma(\mathrm{X})$. In other words:

$$\mathrm{OWff}[\sigma](\langle \varphi, \mathrm{W}\rangle) = \langle \sigma(\varphi), \sigma(\mathrm{W})\rangle$$

(We write ambiguously σ instead of $\mathrm{OWff}[\sigma]$.)

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

Definition 8.9

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

$$[\psi]_{\langle A, \cong\rangle} = \mathrm{Val}[\mathrm{X}, A] \quad \text{(i)}$$

$$\cong \ \subseteq\ \sim_{\mathrm{W}} \quad \text{(ii)}$$

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

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

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 8.9:

Proposition 8.10

Let $\sigma : \Sigma \to \Sigma'$ *be a signature morphism. For any set of terms* $\mathrm{W} \subseteq \mathrm{T}_\Sigma(\mathrm{X})$*, 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 $[\sigma(\varphi)]_{\langle A', \cong'\rangle} = \mathrm{Val}[\mathrm{X}', A']$ *equivalent to* $([\sigma(\varphi)]_{\langle A', \cong'\rangle})_{|\sigma} = (\mathrm{Val}[\mathrm{X}', A'])_{|\sigma}$*, which by Theorem* 8.2 *is equivalent to:*

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

According to Lemma 3.5, $-_{|\sigma}$ *is surjective on the valuations. Consequently, 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 8.9 w.r.t. term translation and forgetful functor. We examine first the if part and then the converse part of this condition.

Proposition 8.11

Let $\sigma : \Sigma \to \Sigma'$ be a signature morphism. For all sets of terms $\mathrm{W} \subseteq \mathrm{T}_\Sigma(\mathrm{X})$, $\mathrm{W}' \subseteq \mathrm{T}_{\Sigma'}(\mathrm{X}')$ such that $\sigma(\mathrm{W}) \subseteq \mathrm{W}'$ and for any observational Σ'-algebra $\langle A', \cong' \rangle$ we have:

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

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

Proof

Assume that

$$\forall\ a', b' \in A' \quad a' \cong' b' \quad \Rightarrow \quad a' \sim_{\mathrm{W}'} b' \tag{i}$$

This holds particularly for $a', b' \in A'_{\sigma(\mathrm{s})}$ (for some $\mathrm{s} \in \mathrm{S}$). Since $\overline{\sigma_{A'}} : A'_{|\sigma} \to A'$ with range $\coprod_{\mathrm{s} \in \mathrm{S}} A'_{\sigma(\mathrm{s})}$, from (i) *we deduce that*

$$\forall\ a, b \in A'_{|\sigma} \quad \overline{\sigma_{A'}}(a) \cong' \overline{\sigma_{A'}}(b) \quad \Rightarrow \quad \overline{\sigma_{A'}}(a) \sim_{\mathrm{W}'} \overline{\sigma_{A'}}(b)$$

By Definition 7.4, $\overline{\sigma_{A'}}(a) \cong' \overline{\sigma_{A'}}(b)$ is equivalent to $a \cong'_{|\sigma} b$. Hence

$$\forall\ a, b \in A'_{|\sigma} \quad a \cong'_{|\sigma} b \quad \Rightarrow \quad \overline{\sigma_{A'}}(a) \sim_{\mathrm{W}'} \overline{\sigma_{A'}}(b)$$

But from Proposition 5.1 it follows that $\overline{\sigma_{A'}}(a) \sim_{\mathrm{W}'} \overline{\sigma_{A'}}(b) \ \Rightarrow \ a \sim_{\mathrm{W}} b$. Consequently

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

□

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

Example 8.12

Consider the following signatures

$$\Sigma = \left\{ \begin{array}{rcl} \mathrm{a}, \mathrm{b} & : & \to \mathrm{s} \\ \mathrm{true}, \mathrm{false} & : & \to \mathrm{Bool} \\ \mathrm{f}, \mathrm{g} & : & \mathrm{s} \to \mathrm{Bool} \end{array} \right\} \qquad \Sigma' = \left\{ \begin{array}{rcl} \mathrm{c}, \mathrm{d} & : & \to \mathrm{s} \\ \mathrm{true}, \mathrm{false} & : & \to \mathrm{Bool} \\ \mathrm{h} & : & \mathrm{s} \to \mathrm{Bool} \end{array} \right\}$$

Let $\mathrm{W} = \{\mathrm{f(a)}, \mathrm{g(b)}\}$. Notice that in any Σ-algebra A we have

$$a^A \sim_{\mathrm{W}} b^A \tag{i}$$

because a^A and b^A have no comparator. Consider $\sigma : \Sigma \to \Sigma'$ defined by:

$$\begin{array}{rclrclrcl} \sigma(\mathrm{Bool}) & = & \mathrm{Bool} & \sigma(\mathrm{true}) & = & \mathrm{true} & \sigma(\mathrm{a}) & = & \mathrm{c} \\ \sigma(\mathrm{s}) & = & \mathrm{s} & \sigma(\mathrm{false}) & = & \mathrm{false} & \sigma(\mathrm{b}) & = & \mathrm{d} \\ & & & & & & \sigma(\mathrm{f}) & = & \sigma(\mathrm{g}) = \mathrm{h} \end{array}$$

Notice that in any Σ'-algebra A',

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

since $\sigma(\mathrm{W}) = \{\mathrm{h(c)}, \mathrm{h(d)}\}$

Consider a reachable observational Σ'-algebra $\langle A', \cong' \rangle$ such that

$$h^{A'}(c^{A'}) \quad \neq \quad h^{A'}(d^{A'}) \tag{iii}$$

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

Notice that $\cong'_{|_\sigma} = \{(a^{A_{|\sigma}}, b^{A_{|\sigma}})\}$. *Therefore, according to* (i) *we have*

$$\cong'_{|_\sigma} \subseteq \sim_{\mathrm{W}}$$

but we have not $\cong' \subseteq \sim_{\sigma(\mathrm{W})}$ *since from* (ii) *and* (iii) *we have* $c^{A'} \not\sim_{\sigma(\mathrm{W})} d^{A'}$ *whereas from* (iv) *we have* $c^{A'} \cong' d^{A'}$.

From this negative result we may already conclude that, in order to establish institutions within our approach, we will be constrained to restrict somehow our formalism. This will be the subject of Section 10.

9 Observational Specifications

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

Definition 9.1

An **observational specification** OSP *is a triplet* $\langle \Sigma, \Theta, \mathrm{W} \rangle$, *where* Σ *is the signature of* OSP, Θ *the set of its axioms and* W *is a set of terms with variables,* $\mathrm{W} \subseteq \mathrm{T}_\Sigma(\mathrm{X})$, *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 9.2

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

$$\langle A, \cong \rangle \; \square\!\!= \langle \Theta, \mathrm{W} \rangle$$

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

In the above definition we have considered a set $\Phi = \{\varphi_1, \ldots, \varphi_\mathrm{n}\}$ of formulae as a conjunction of formulae $\Phi = \varphi_1 \wedge \ldots \wedge \varphi_\mathrm{n}$. Thus any pair $\langle \Phi, \mathrm{W} \rangle$ can be viewed as a single observational formula. One may also define an observational specification as a pair $\langle \Sigma, \mathrm{OAx} \rangle$ with $\mathrm{OAx} = \{\langle \theta_1, \mathrm{W}_1 \rangle, \ldots, \langle \theta_\mathrm{i}, \mathrm{W}_\mathrm{i} \rangle, \ldots\}$. The possibility to associate observations separately to each axiom would increase the expressive power. (In particular, it allows an infinite set OAx.) However, in all examples it seems preferable to attach a unique set of observable terms to the whole specification.

Fact 9.3

The observational algebra $\langle L_{|_\sigma}, \sim_{\mathrm{Obs}_{\mathsf{SWE}}} \rangle$, *described in Example* 7.2, *is a model of the observational specification* SWE.

Proof

Since the observational equality on $\langle L_{|_\sigma}, \sim_{\mathrm{Obs}_{\mathsf{SWE}}} \rangle$ *is just the indistinguishability relation, we only need to prove that for any axiom* θ *of* SWE *we have*

$$[\theta]_{\langle L_{|_\sigma}, \sim_{\mathrm{Obs}_{\mathsf{SWE}}} \rangle} = \mathrm{Val}[\mathrm{X}, L_{|_\sigma}]$$

• *Notice that* $(L_{|\sigma})_{|\mathrm{Sig[LIST]}} = L$. *On the other hand from Example* 4.8 *we know that* $\sim_{\mathrm{Obs_{SWE}}}$ *is the usual equality on* $(L_{|\sigma})_{|\mathrm{Sig[LIST]}}$. *We have therefore:*

$$(\langle L_{|\sigma}, \sim_{\mathrm{Obs_{SWE}}}\rangle)_{|\mathrm{Sig[LIST]}} = \langle L, =\rangle$$

and since L *is a model of* LIST, $\langle L_{|\sigma}, \sim_{\mathrm{Obs_{SWE}}}\rangle$ *satisfies all the axioms of* LIST.

• *Since the elements observationally equal on* $(L_{|\sigma})_{\mathsf{Set}}$ *are different representations of the same set, it is clear that for the "standard" axioms* $\psi_1, \psi_2, \ldots, \psi_8$ *of sets (c.f. Figure* 2.1*), we have*

$$[\psi_{\mathrm{i}}]_{\langle L_{|\sigma}, \sim_{\mathrm{Obs_{SWE}}}\rangle} = \mathrm{Val[X}, L_{|\sigma}]$$

• *Notice that* ψ_9 *and* ψ_{10} *are translated by* σ *(c.f.* 4.8*) in the following way:*

$$\begin{array}{lrcl} \sigma(\psi_9): & \mathsf{idl(nil)} & = & \mathsf{nil} \\ \sigma(\psi_{10}): & \mathsf{idl(cons(x,l))} & = & \mathsf{cons(x, idl(l))} \end{array}$$

We have therefore

$$[\sigma(\psi_9)]_{\langle L, =\rangle} = [\sigma(\psi_{10})]_{\langle L, =\rangle} = \mathrm{Val[X}, L]$$

Then, according to the theorem 8.2*, we obtain*

$$[\psi_9]_{\langle L_{|\sigma}, =\rangle} = [\psi_{10}]_{\langle L_{|\sigma}, =\rangle} = \mathrm{Val[X}, L_{|\sigma}]$$

Hence we can conclude that

$$[\psi_9]_{\langle L_{|\sigma}, \sim_{\mathrm{Obs_{SWE}}}\rangle} = [\psi_{10}]_{\langle L_{|\sigma}, \sim_{\mathrm{Obs_{SWE}}}\rangle} = \mathrm{Val[X}, L_{|\sigma}]$$

The last step is justified by the fact that the axioms ψ_9 *and* ψ_{10} *are equations and that* $= \subseteq \sim_{\mathrm{Obs_{SWE}}}$. *Obviously, for any* Σ*-equation* $\mathrm{t} = \mathrm{t}'$*, any* Σ*-algebra* A *and the observational equalities* $\cong^{\alpha} \subseteq \cong^{\beta}$ *on* A*, we have* $[\mathrm{t} = \mathrm{t}']_{\langle A, \cong^{\alpha}\rangle} \subseteq [\mathrm{t} = \mathrm{t}']_{\langle A, \cong^{\beta}\rangle}$ □

In the above example we have considered a model of the form $\langle A, \sim_{\mathrm{W}}\rangle$. Of course, this is possible only when $\sim_{\mathrm{W}}$ is transitive. Moreover this model has a particular status: it is a terminal object in the category of all observational models formed with a given algebra A. (This is quite analogous to the final data type of [13].) Notice that when $\sim_{\mathrm{W}}$ is not transitive this category has often no terminal object. For instance the category of observational models of TRANS formed with the algebra A (see Figure 5.1) has no terminal object.

The next result points out that our observational specifications together with their semantics 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: we just take $\langle \Sigma, \Theta, \mathrm{X}\rangle$. The relationship between the both is stated by the following proposition:

Proposition 9.4

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

Proof

Notice first that $\sim_{\mathrm{x}}$ *is the identity relation on any* Σ*-algebra. This is obvious since a variable* $\mathrm{x} \in \mathrm{X_s}$ *gives rise to an empty comparator* $\diamond_{\mathrm{s}}$ *which distinguishes all distinct* $a, b \in A_{\mathrm{s}}$ *and we have assumed that* $\mathrm{X_s}$ *is nonempty for any sort* s. *By Definition* 8.9*, for any* $\langle A, \cong\rangle \in \mathrm{OAlg}[\langle \Sigma, \Theta, \mathrm{X}\rangle]$ *we have* $\cong \subseteq \sim_{\mathrm{x}}$*, thus* $\cong$ *is just the usual equality. From the requirement* $[\Theta]_{\langle A, =\rangle} = \mathrm{Val[X}, A]$ *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* $\langle B, =\rangle \in \mathrm{OAlg}[\langle \Sigma, \Theta, \mathrm{X}\rangle]$. □

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 without additional assumptions. For instance, the next theorem shows that our approach fulfills the requirement of "reusing by restriction" [4].

Theorem 9.5

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

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

Proof

From definitions 9.2 *and* 8.9 *it is enough to prove:*

$$\forall\, \langle A', \cong' \rangle \in \mathrm{OAlg}[\Sigma'] \quad [\Theta']_{\langle A', \cong' \rangle} = \mathrm{Val}[\mathrm{X}', A'] \;\Rightarrow\; [\Theta]_{\langle A', \cong' \rangle_{|\sigma}} = \mathrm{Val}[\mathrm{X}, A'_{|\sigma}] \quad \text{(i)}$$

$$\text{and} \quad \forall\, \langle A', \cong' \rangle \in \mathrm{OAlg}[\Sigma'] \quad \cong' \subseteq \sim_{\mathrm{W}'} \;\Rightarrow\; \cong'_{|\sigma} \subseteq \sim_{\mathrm{W}} \quad \text{(ii)}$$

- **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 $\sigma(\Theta) \subseteq \Theta'$, *by definition of solution of a conjunction of formulae (c.f.* 8.1*) 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* 8.10 *implies that*

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

- **Proof of (ii)** *follows directly from Proposition* 8.11.

□

This result corresponds to a very fundamental property which holds in most non observational frameworks. **Except for our case, in the approaches with an observational satisfaction relation the corresponding property holds only for equational specifications.** It may also hold for positive-conditional axioms under the hypothesis of observable preconditions. However, this is a rather strong restriction. It may be then surprising that in our approach the former theorem holds without restriction even if the axioms are arbitrary first order formulae. The reason is that our observational equality is not fixed by observations as the indistinguishability relation does. Unlike [1], [5], [10], [16] and [17], 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. 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 (partly) guarantees such a general result as Theorem 9.5.

The following corollary of the former theorem formalizes the phenomenon: "more observations, less models".

Corollary 9.6

Let $\mathrm{OSP}_1 = \langle \Sigma, \Theta, \mathrm{W}_1 \rangle$ *and* $\mathrm{OSP}_2 = \langle \Sigma, \Theta, \mathrm{W}_2 \rangle$ *be observational specifications such that* $\mathrm{W}_1 \subseteq \mathrm{W}_2$. *Then:*

$$\mathrm{OAlg}[\mathrm{OSP}_2] \subseteq \mathrm{OAlg}[\mathrm{OSP}_1]$$

Proof

Follows directly from the previous theorem. □

We conclude from the above that observations acts on the semantics of a specification in a quite similar way than the axioms, since by adding axioms, we diminish the class of the models.

10 Towards an Institution of Observational Specifications

In this section, based on the formalism we have developed so far, we define an institution for observational specifications. As mentioned in Section 8, this task requires to put some restrictions on our general formalism.

Recall that an institution (see [9]) is a tuple $\langle \mathrm{Sign}, \mathrm{Wff}, \mathrm{Mod}, \models \rangle$ where

1. Sign is a category of "signatures",
2. $\mathrm{Wff} : \mathrm{Sign} \to \mathrm{Set}$ is a functor which maps a signature to the set of well formed formulae over the signature,
3. $\mathrm{Mod} : \mathrm{Sign} \to \mathrm{Cat}^{\mathrm{op}}$ is a functor which maps a signature to the category of the interpretation structures (models),
4. $\models$ is a ($|\mathrm{Sign}|$-sorted) satisfaction relation ($\models_\Sigma \subseteq \mathrm{Mod}[\Sigma] \times \mathrm{Wff}[\Sigma]$) such that for each $\sigma : \Sigma \to \Sigma$ in Sign, each $\varphi \in \mathrm{Wff}[\Sigma]$ and each $M' \in \mathrm{Mod}[\Sigma']$ the following **satisfaction condition** holds:
$$M' \models \mathrm{Wff}[\sigma](\varphi) \quad \text{iff} \quad \mathrm{Mod}[\sigma](M') \models \varphi$$

It is clear that the tuple $\langle \mathrm{Sig}, \mathrm{OWff}, \mathrm{OAlg}, \models\!\!\!\!\square \rangle$ could be an institution provided that it would fulfill the satisfaction condition which in our formalism is expressed by the following property:

Property 10.1

For any $\sigma : \Sigma \to \Sigma'$, any observational Σ-formula $\langle \varphi, \mathrm{W} \rangle$ and any observational Σ'-algebra we have:
$$\langle A', \cong' \rangle \models\!\!\!\!\square \sigma(\langle \varphi, \mathrm{W} \rangle) \quad \textit{iff} \quad \langle A', \cong' \rangle_{|_\sigma} \models\!\!\!\!\square \langle \varphi, \mathrm{W} \rangle$$

By definition 8.9 in order to show that this property holds, it is enough to prove

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

$$\text{and} \quad \forall\, \langle A', \cong' \rangle \in \mathrm{OAlg}[\Sigma'] \qquad \cong' \subseteq \sim_{\sigma(\mathrm{W})} \quad \Leftrightarrow \quad \cong'_{|_\sigma} \subseteq \sim_{\mathrm{W}} \qquad \text{(ii)}$$

The first requirement is guaranteed by 8.10. From Proposition 8.11 we have the if condition of the second requirement. Unfortunately, we know from Example 8.12 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 10.2

Let $\sigma : \Sigma \to \Sigma'$ be a signature morphism and $\mathrm{W} \subseteq \mathrm{T}_\Sigma(\mathrm{X})$ be a set of terms. For all Σ'-algebra A' and all $a', b' \in A'_{\sigma(\mathrm{s})}$ $\sigma(\mathrm{W})$-distinguishable, there exist $a, b \in (A'_{|_\sigma})_{\mathrm{s}}$ satisfying $\overline{\sigma_{A'}}(a) = a'$ and $\overline{\sigma_{A'}}(b) = b'$ such that:
$$a \not\sim_{\mathrm{W}} b$$

Proposition 10.3

Let $\sigma : \Sigma \to \Sigma'$ be a signature morphism. The property 10.2 *holds for a set* W *of* Σ*-terms if and only if*

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

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

Proof

• $\Rightarrow$

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

$$\forall\ a, b \in A'_{|_\sigma} \quad a \cong'_{|_\sigma} b \quad \Rightarrow \quad a \sim_{\mathrm{W}} b \tag{i}$$

By contradiction assume that there exist $a_1, b_1 \in A'_{|_\sigma}$ *such that*

$$\overline{\sigma_{A'}}(a_1) \quad \not\sim_{\sigma(\mathrm{W})} \quad \overline{\sigma_{A'}}(b_1) \tag{ii}$$
$$\overline{\sigma_{A'}}(a_1) \quad \cong' \quad \overline{\sigma_{A'}}(b_1) \tag{iii}$$

Using Property 10.2, *from* (ii) *we deduce that there exist* $a_2, b_2 \in A'_{|_\sigma}$ *such that*

$$\overline{\sigma_{A'}}(a_2) \quad = \quad \overline{\sigma_{A'}}(a_1) \tag{iv}$$
$$\overline{\sigma_{A'}}(b_2) \quad = \quad \overline{\sigma_{A'}}(b_1) \tag{v}$$
$$a_2 \quad \not\sim_{\mathrm{W}} \quad b_2 \tag{vi}$$

But according to (iii), (iv) *and* (v) *we conclude that* $a_2 \cong'_{|_\sigma} b_2$. *We have therefore*

$$a_2 \cong'_{|_\sigma} b_2 \quad \not\Rightarrow \quad a_2 \sim_{\mathrm{W}} b_2$$

which is in contradiction with the assumption (i).

• $\Leftarrow$

(We prove it in an indirect way.) Let $\sigma : \Sigma \to \Sigma$ *and* $\mathrm{W} \subseteq \mathrm{T}_\Sigma(\mathrm{X})$ *for which the property* 10.2 *does not holds. Consequently, there is a* Σ'*-algebra* A' *with elements* $a', b' \in A'_{\sigma(\mathrm{s}_0)}$ *(for some* $\mathrm{s}_0 \in \mathrm{S}$*)* $\sigma(\mathrm{W})$*-distinguishable, such that for any* $\mathrm{s} \in \mathrm{S}$ *satisfying* $\sigma(\mathrm{s}) = \sigma(\mathrm{s}_0)$, *all the elements* $a, b \in (A'_{|_\sigma})_s$ *which verify* $\overline{\sigma_{A'}}(a) = a'$ *and* $\overline{\sigma_{A'}}(b) = b'$ *are* W*-indistinguishable. Equip* A' *with* $\cong'$ *such that* $c' \cong' d' \Rightarrow c' \sim_{\sigma(\mathrm{W})} d'$ *for all* $c', d' \in A'$ *except for* a', b' *where* $a' \cong' b'$. *It is clear from the proof of* 8.11 *that for all these* c′, d′ *we have also that for all the elements* $c, d \in (A'_{|_\sigma})_s$ *which verify* $\overline{\sigma_{A'}}(c) = c'$ *and* $\overline{\sigma_{A'}}(d) = d'$ *the following holds*

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

It follows from the above formula that $\cong'_{|_\sigma} \subseteq \sim_{\mathrm{W}}$, *since by Definition* 7.4 *we have* $a \cong'_{|_\sigma} b$ *and we have assumed that* $a \sim_{\mathrm{W}} b$. *Now,* $\cong' \not\subseteq \sim_{\sigma(\mathrm{W})}$ *because* $a' \cong' b'$ *and we have assumed that* $a' \not\sim_{\sigma(\mathrm{W})} b'$. □

We can conclude from the above that in our approach, the satisfaction condition does not hold in general. Only the if part of Property 10.1 holds. Consequently, according to [18], our approach defines a reduction-preserving pre-institution. The converse part of 10.1 holds only for these signature morphisms and these observations which preserve 10.2. Consequently our approach could motivate more liberal formalizations than institutions of the notion of "logical system" as e.g. specification logic [6] or pre-institutions [18].

Since the satisfaction condition holds only for some signature morphisms, in order to define an institution in our framework, one could forget some problematic arrows of Sig and consider as a category of signatures a category which has the same objects as Sig but less

arrows. We retain this last solution. 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 8.12 can be constructed as soon as we have a non injective signature morphism. We conclude that an observational institution can be provided within our formalism under a restriction of the arrows of Sig to injective morphisms only.

Proposition 10.4

Consider the tuple $\mathrm{OAlgSpec} = \langle \mathrm{ISig}, \mathrm{OWff}, \mathrm{OAlg}, \not\models \rangle$ *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

According to the discussion of this section, it is enough to prove that Property 10.2 *holds for injective signature morphisms.*

Let $\sigma : \Sigma \to \Sigma'$ *be an injective signature morphism,* $\mathrm{W} \subseteq \mathrm{T}_\Sigma(\mathrm{X})$ *a set of terms,* A' *a* Σ'*-algebra and let* $a', b' \in {A'}_{\sigma(\mathrm{s})}$ $\sigma(\mathrm{W})$*-distinguishable. Let* $\eta' \in \mathrm{cmp}_{\sigma(\mathrm{W})}(a', b')$ *a comparator which distinguishes* a' *and* b'*.*

Since σ *is injective,* $\overline{\sigma_{A'}}$ *and* $\sigma_{A'}$ *are too, there exists a unique* $a \in A'|_\sigma$ *(resp.* $b \in A'|_\sigma$*) such that* $\overline{\sigma_{A'}}(a) = a'$ *(resp.* $\overline{\sigma_{A'}}(b) = b'$*) and a unique* $\eta \in \mathrm{MC}_\Sigma(A'|_\sigma)$ *such that* $\sigma_{A'}(\eta) = \eta'$*. According to Theorem* 4.14*,* η *is a continuation of* a *and* b*. So* $\eta \in \mathrm{cmp}_\mathrm{W}(a, b)$*. From Corollary* 3.7 *we have*

$$\begin{array}{rl} & \overline{\eta'[a']} = \overline{\sigma_{A'}(\eta[a])} = \overline{\sigma_{A'}}(\overline{\eta[a]}) \\ (\textit{resp.} & \overline{\eta'[b']} = \overline{\sigma_{A'}(\eta[b])} = \overline{\sigma_{A'}}(\overline{\eta[b]})) \end{array}$$

Since $\overline{\eta'[a']} \neq \overline{\eta'[b']}$*, we have* $\overline{\sigma_{A'}}(\overline{\eta[a]}) \neq \overline{\sigma_{A'}}(\overline{\eta[b]})$ *and since* $\overline{\sigma_{A'}}$ *is injective we conclude that* $\overline{\eta[\mathrm{a}]} \neq \overline{\eta[\mathrm{b}]}$*. Thus* a *and* b *are distinguishable.* □

Notice that OAlgSpec denotes in fact a family of institutions. Recall that

$$\mathrm{OWff}[\Sigma] \;=\; \{\langle \varphi, \mathrm{W} \rangle \mid \varphi \in \mathrm{Wff}[\Sigma],\ \mathrm{W} \subseteq \mathrm{T}_\Sigma(\mathrm{X})\}$$

Accordingly, OAlgSpec is in some sense "parameterized" by Wff. Recall that our approach does not take into account predicate symbols (other than $=$). Thus the Wff functors acceptable for our purposes must send signatures to any subset of the Many-Sorted First Order Logic with Equality without predicate symbols. Moreover, our approach can be easily enriched with predicate symbols without loss of the results (as shown in [14]).

11 Some Additional Examples

In this section we show on two examples how some (usual) algebraic specification $\langle \Sigma, \Theta \rangle$ can be completed with observations W, in order to get some interesting observational models corresponding to bounded realizations. Of course the examples of models we provide are only in $\mathrm{OAlg}[\langle \Sigma, \Theta, \mathrm{W} \rangle]$ and not in $\mathrm{Alg}[\langle \Sigma, \Theta \rangle]$. This motivates the use of an observational approach to handle bounded implementations of specifications which (in the usual sense) have no bounded models. In both examples we proceed as follows:

1. Given a specification $\langle \Sigma, \Theta \rangle$ we provide a Σ-algebra A which is not a model of $\langle \Sigma, \Theta \rangle$.
2. We equip A with an observational equivalence $\cong$ and we show that $\langle A, \cong \rangle$ fulfills the first requirement of the definition of our observational satisfaction relation 8.9, that is $[\theta]_{\langle A, \cong \rangle} = \mathrm{Val}[\mathrm{X}, A]$ for all $\theta \in \Theta$.

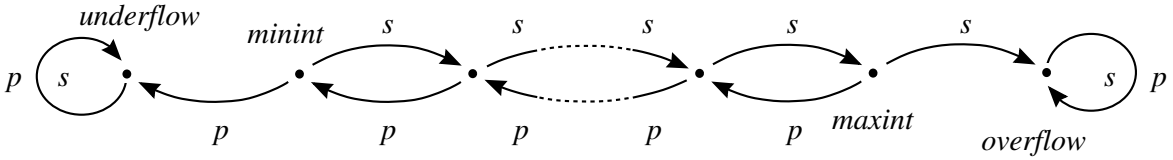
3. We give an appropriate set of observations W and we show that the second requirement of the definition of our satisfaction relation holds, that is $\cong \subseteq \sim_{W}$.

As a first example consider the specification INT= $\langle \Sigma_1, \Theta_1 \rangle$ of integers (see Figure 11.1). The only reachable models of this specification are $\mathbb{Z}$ and all the $\mathbb{Z}/n\mathbb{Z}$. Assume that

spec : INT **sort :** Int **generated by :** 0 : → Int s, p : Int → Int **axioms :** p(s(x)) = x s(p(x)) = x	**spec :** STACK **use :** NAT **sort :** Stack **generated by :** emptystack : → Stack push : Nat Stack → Stack **operations :** top : Stack → Nat pop : Stack → Stack **axioms :** top(push(x, s)) = x pop(push(x, s)) = s

Figure 11.1: Specifications INT and STACK

we need a realization of this specification which behaves like $\mathbb{Z}$ at least inside an interval between the constants minint and maxint. Consider the following Sig[INT]-algebra A:



Obviously, this algebra is not a model of INT.

Let us equip A with the observational equality "$\cong$" defined as the reflexive-symmetric-transitive closure of the relation

$$\{\langle minint, underflow\rangle, \langle maxint, overflow\rangle\}$$

It is easy to show that Val[X, A] is the set of solutions of both axioms of INT in $\langle A, \cong\rangle$. Assume now that we observe the set W_1 of all the ground terms which denote integers between minint and maxint. In this situation the contextual variable $\diamond_{\mathsf{Int}}$ is a continuation of all the elements of A between *minint* and *maxint*. On the contrary, *underflow* and *overflow* have no continuations. Consequently

$$\sim_{W_1} = \{\ \langle b, b\rangle, \langle c, d\rangle \mid\ b, c, d \in A_{\mathsf{Int}},\ \{c, d\} \cap \{underflow, overflow\} \neq \emptyset\ \}$$

Hence $\cong\ \subseteq\ \sim_{W_1}$ and we conclude that $\langle A, \cong\rangle$ is an observational model of $\langle \Sigma_1, \Theta_1, W_1\rangle$.

As a second example, we are going to study bounded stacks. Consider the specification STACK= $\langle \Sigma_2, \Theta_2\rangle$ (see Figure 11.1) and assume that we are only interested in stacks of a height bounded by a constant maxheight. Then the following algebra should be correct for our purposes: we consider an array-pointer realization with an array of length maxheight+1 starting at the index 0. A full stack is then represented by the couple $\langle t, maxheight\rangle$ and an

erroneous stack by $\langle t, s(maxheight)\rangle$ ($s(maxheight)$ points outside of t). For both erroneous and correct stacks, the operation top is always realized in the standard way:

$$top(\langle t, s(i)\rangle) = t[i]$$

On a correct stack the operations push and pop are also realized in the standard way:

$$i \neq s(maxheight) \Rightarrow push(x, \langle t, i\rangle) = \langle t[i]{:=}x, s(i)\rangle$$
$$i \neq maxheight \Rightarrow pop(\langle t, s(i)\rangle) = \langle t, i\rangle$$

These operations act on an erroneous stack in the following way:

$$push(x, \langle t, s(maxheight)\rangle) = \langle t[maxheight]{:=}x, s(maxheight)\rangle$$
$$pop(\langle t, s(maxheight)\rangle) = \langle t, s(maxheight)\rangle$$

It is important to notice that it is impossible in this realization to make correct an erroneous stack by means of combinations of pushes and pops only.

Let A be the above realization. We equip now the algebra A with the observational equality "$\cong$" defined as a the reflexive-symmetric-transitive closure of the following relation "ρ"

1. $\langle t, n\rangle\ \rho\ \langle t', n\rangle$ if $n \leq maxheight$ and $t[i] = t'[i]$ for all $i \leq n$
2. $\langle t, maxheight\rangle\ \rho\ \langle t', s(maxheight)\rangle$ if t and t' differ only at the index *maxheight.*

Let us show that the set of solutions of any axiom of STACK in the observational algebra $\langle A, \cong\rangle$ defined above is Val[X, A]. This is obvious for the non erroneous stacks. Consider then a full stack $\langle t, maxheight\rangle$. We check the axiom top(push(x, s)) = x:

$$\begin{aligned} top(push(a, \langle t, maxheight\rangle)) &= top(\langle t[maxheight]{:=}a, s(maxheight)\rangle) = \\ &= (t[maxheight]{:=}a)[maxheight] = a \end{aligned}$$

We check the axiom pop(push(x, s)) = s:

$$\begin{aligned} pop(push(a, \langle t, maxheight\rangle)) &= pop(\langle t[maxheight]{:=}a, s(maxheight)\rangle) = \\ &= \langle t[maxheight]{:=}a, s(maxheight)\rangle \end{aligned}$$

But according to 2: $\langle t[maxheight]{:=}a, s(maxheight)\rangle \cong \langle t, maxheight\rangle$.

We check now both axioms for an erroneous stack $\langle$t, s(maxheight)$\rangle$:

$$\begin{aligned} top(push(a, \langle t, s(maxheight)\rangle)) &= top(\langle t[maxheight]{:=}a, s(maxheight)\rangle) = \\ &= (t[maxheight]{:=}a)[maxheight] = a \end{aligned}$$

On the other hand:

$$\begin{aligned} pop(push(a, \langle t, s(maxheight)\rangle)) &= pop(\langle t[maxheight]{:=}a, s(maxheight)\rangle) = \\ &= \langle t[maxheight]{:=}a, s(maxheight)\rangle \end{aligned}$$

But according to 2 we have

$$\langle t, s(maxheight)\rangle\ \rho\ \langle t, maxheight\rangle\ \rho\ \langle t[maxheight]{:=}a, s(maxheight)\rangle$$

Since "$\cong$" is the reflexive-symmetric-transitive closure of "ρ", we have

$$\langle t, s(maxheight)\rangle \cong \langle t[maxheight]{:=}a, s(maxheight)\rangle$$

In this way we have shown that in $\langle A, \cong \rangle$, the solutions of both axioms of STACK are Val[X, A].

Assume now that we observe the set W_2 of all the ground terms of the form top(t) with t generated by emptystack, push and pop and representing a stack of height least or equal to maxheight. It is clear that for two non erroneous stacks $\langle t, n \rangle$ and $\langle t', n \rangle$ we have

$$\langle t, n \rangle \sim_{W_2} \langle t', n \rangle \quad \textit{iff} \quad \langle t, n \rangle \cong \langle t', n \rangle$$

Since an erroneous stack has no continuations, it is indistinguishable with any other stack. Consequently

$$\cong \subseteq \sim_{W_2}$$

and we have shown that $\langle A, \cong \rangle$ is an observational model of the specification $\langle \Sigma_2, \Theta_2, W_2 \rangle$.

The reader have certainly realized that in both examples the corresponding observations have been described in an informal way. In fact in this work we did not deal with a syntax for describing sets of observable terms. It is clear that no syntax may exist allowing to describe (in a finite way) an arbitrary subset of $T_\Sigma(X)$.[1] Consequently the choice of a particular syntax will impose strong restrictions on possible observations. Nevertheless, under such restrictions, we can expect some additional results within this framework.

12 Concluding Remarks

We have developed a loose observational semantics of algebraic specifications. We have shown that, under some restrictions, our formalism provides an institution. First, we have investigated how the elements of a carrier of an algebra should be observed through terms. We have pointed out that an adequate notion of observation requires to take into account multicontexts and partial evaluations of observable terms. In this way, we have introduced the concept of continuation underlying our definition of the indistinguishability relation. We have shown that this relation is neither a congruence nor an equivalence relation. These both results fully agree with our Indistinguishability Assumption. Notice that when we restrict to sort observation, our indistinguishability relation becomes a congruence. Consequently, this notion becomes close to the Nerode congruence [10]. However, unlike in [16], in our approach two observational algebras differing on non observable junk do not satisfy the same observational formulae. We do not privilege reachable elements, since this is most suitable for the observational semantics of parameterized specifications in the loose framework (which is one of the topics of further research). Moreover, one might think that our indistinguishability relation would coincide with the Reichel's I-indistinguishability (see [17]) when we restrict our approach to sort observation and the Reichel's one to total algebras. This is not true, since we use multicontexts from $MC_\Sigma(A)$ instead of MC_Σ. Consequently, in our approach, non observable junk can affect the indistinguishability of two elements of a carrier of an algebra while it cannot in other works with observational satisfaction relation. Thus he have fully followed our claim not to privilege reachable elements.

Being convinced that the possibility of replacements of equal by equal must be allowed, we have introduced in our semantics an additional stage over the indistinguishability relation, namely observational equality. Then we have defined the observational algebras, the observational formulae and the corresponding satisfaction relation. We have shown that the restriction to injective signature morphisms is a reasonably weak condition which enables our

[1] There exist non recursive subsets of $T_\Sigma(X)$.

formalism to be extended to an institution.

Acknowledgments We wish to thank Sungsoon Kim whose careful readings have contributed to improve the presentation of this paper. This work is partially supported by ESPRIT Working Group COMPASS and CNRS GDR de Programmation.

References

[1] **Bernot G., Bidoit M.** Proving the correctness of algebraically specified software: Modularity and Observability issues *Proceedings of International Conference AMAST, Iowa City, 1991, 139-161.*

[2] **Bernot G., Bidoit M., Knapik T.** Observational Approaches in Algebraic Specifications: a Comparative Study *Laboratoire de l'Informatique de l'Ecole Normale Supérieure, 1991, (Internal Report LIENS-91-6).*

[3] **Bergstra J.A., Tucker J.V.** Initial and Final Algebra Semantics for Data Type Specifications: Two Characterization Theorems. *SIAM Journal of Computing, vol 12 (1983), 366-387.*

[4] **Bidoit M.** The stratified loose approach: A generalization of initial and loose semantics. *(Sannella, Tarlecki eds.) Recent Trends in Data Type Specification, 5th Workshop on Specification of ADT, Gullane, September 1987, LNCS 332, 1-22.*

[5] **van Diepen N.W.P.** Implementation of Modular Algebraic Specifications *(Ganzinger H. ed.) ESOP 88, Nancy, March 1988, LNCS 300, 64-78.*

[6] **Ehrig H., Baldamus M., Orejas F.** New Concepts for Amalgamation and Extension in the Framework of Specification Logics *Tchnische Universität Berlin, May 1991 (Internal Report 91/05).*

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

[8] **Goguen J.A., Burstall R.** Introducing Institutions *(Clarke E., Kozen D. eds.) Proceedings of Logic of Programming Workshop, Carnegie Mellon, 1984, LNCS 164, 221-256.*

[9] **Goguen J.A., Burstall R.** Institutions: abstract model theory for specification and programming *LFCS report ECS-LFCS-90-106 (1990).*

[10] **Goguen J.A., Meseguer J.** Universal Realization, Persistent Interconnection and Implementation of Abstract Modules *(Nielsen M., Schmidt E.M. eds.) ICALP, Aarhus, 1982, LNCS 140, 265-281.*

[11] **Goguen J.A., Thatcher J.W., Wagner E.G.** An Initial Approach to the Specification, Correctness and Implementation of Abstract Data Types, *(Yeh R.T. ed.) Current Trends in Programming Methodology, Vol. 4: Data Structuring, Prentice Hall, 80-149 (1978).*

[12] **Hennicker R.** Context Induction: a Proof Principle for Behavioural Abstractions and Algebraic Implementations *Fakultät für Mathematik und Informatik Universität Passau, 1990 (Internal Report MIP-9001).*

[13] **Kamin S.** Final Data Types and Their Specification *ACM Transactions on Programming Languages and Systems, Vol 5, No 1, 97-123 (1983).*

[14] **Knapik T.** Observational Logic for Algebraic Specification: an Approach with Observational Satisfaction Relation and Formulae as Observations. *Laboratoire de l'Informatique de l'Ecole Normale Supérieure, 1992, (Internal Report LIENS-92).*

[15] **Moss L.S., Thatte S.R.** Generalization of Final Algebra Semantics by Relativization *(Main M., Melton A., Mislove M., Schmidt D. eds.) Mathematical Foundations of Programming Semantics, 5th Int. Conference, New Orleans, March/April 1989, LNCS 442, 284-300.*

[16] **Nivela P., Orejas F.** Initial Behaviour Semantics for Algebraic Specification *(Sannella, Tarlecki eds.) Recent Trends in Data Type Specification, 5th Workshop on Specification of ADT, Gullane, September 1987, LNCS 332, 184-207.*

[17] **Reichel H.** Behavioural Validity of Conditional Equations in Abstract Data Types *Contributions to General Algebra 3, Proceedings of the Vienna Conference, June 1984.*

[18] **Salibra A., Scollo G.** A soft stairway to institutions, *Talk at the 8th Workshop on Specifications of Abstract Data Types, Dourdan, September 1991.*

[19] **Sannella D., Tarlecki A.** Toward Formal Development of Programs from Algebraic Specification Revisited, *Acta Informatica 25, 233-281 (1988).*

[20] **Wand M.** Final Algebra Semantics and Data Type Extension *Journal of Computer and System Sciences, Vol 19, 27-44 (1979).*

Appendix

Proof of Lemma 3.5

- **Functionality**

Let $\nu' : \mathrm{Val}[\mathrm{X}', A']$. *We show that there exists the unique* $\nu : \mathrm{X} \to A'|_\sigma$ *such that* $\sigma(\mathrm{x})\nu' = \overline{\sigma_{A'}}(\mathrm{x}\nu)$.

Assume that $\sigma(\mathrm{x})\nu' = a'$ *for* $\mathrm{x} \in \mathrm{X_s}$. *Since* $\sigma(\mathrm{s})$ *is the sort of* $\sigma(\mathrm{x})$, *by definition of valuation* $a' \in A'_{\sigma(\mathrm{s})}$. *Since* σ *is not necessarily injective on the sorts,* ${\sigma_{A'}}^{-1}(a') = \{a_1, ..., a_n\}$, *each* a_i *having different sort of* $\sigma^{-1}(\sigma(\mathrm{s}))$. *Thus, there exists the unique* a_k *of the sort* s. *The valuation* ν, *we are looking for, exists and maps* x *into its unique value* a_k. *Consequently* ν *is unique.*

- **Surjectivity**

We show that for all $\nu : \mathrm{X} \to A$ *there exists* $\nu' : \mathrm{Val}[\mathrm{X}', A']$ *such that* $\nu'|_\sigma = \nu$.

Let a $\mathrm{x}' \in \mathrm{X}'$. *Since* σ *is injective on the variables there exists the unique* $\mathrm{x} \in \mathrm{X}$ *such that* $\sigma(\mathrm{x}) = \mathrm{x}'$. *Assume that* $\mathrm{x}\nu = a$, $a \in A'|_\sigma$. *Then the value that* ν' *should map to* x' *is* $\overline{\sigma_{A'}}(a)$. *This proves the existence of* ν'. □

Proof of Lemma 3.6

We prove it by induction on the size of t.

- **Induction hypothesis**
  Lemma holds for any term with size less than n
- **Base step**
  Obvious according to (3.i)
- **Induction step**
  Let $\mathrm{t}_1 \in (\mathrm{T}_\Sigma(\mathrm{X}))_{\mathrm{s}_1} \ldots \mathrm{t}_\mathrm{n} \in (\mathrm{T}_\Sigma(\mathrm{X}))_{\mathrm{s}_\mathrm{n}}$ *all of size less than* n *having at least one with size* n. *Let* $(\mathrm{f} : \mathrm{s}_1, \ldots, \mathrm{s}_\mathrm{n} \to \mathrm{s}) \in \Sigma$. *From induction hypothesis we have:*

$$\overline{\sigma(\mathrm{t}_1)\nu'} = \overline{\sigma_{A'}}(\overline{\mathrm{t}_1\nu'|_\sigma}) \qquad \ldots \qquad \overline{\sigma(\mathrm{t}_\mathrm{n})\nu'} = \overline{\sigma_{A'}}(\overline{\mathrm{t}_\mathrm{n}\nu'|_\sigma})$$

By definition ${\mathrm{f}^{A'}}|_\sigma = \sigma(\mathrm{f})^{A'}$. *Hence:* $\overline{\sigma(\mathrm{f}(\mathrm{t}_1, \ldots, \mathrm{t}_\mathrm{n}))\nu'} = \overline{\sigma_{A'}}(\overline{\mathrm{f}(\mathrm{t}_1, \ldots, \mathrm{t}_\mathrm{n})\nu'|_\sigma})$

□