Towards an adequate notion of observation *

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

One can attempt to solve the problem of establishing the correctness of some software w.r.t. a formal specification at the semantical level. For this purpose, the semantics of an algebraic specification should be the class of all algebras which correspond to the correct realizations of the specification. We approach this goal by defining an **observational satisfaction relation** which is less restrictive than the usual satisfaction relation. 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, hence we define an **observational algebra** as an algebra equipped with an observational equality which is an equivalence relation but not necessarily a congruence. Since terms may represent computations, our notion of observation depends on a set of observable terms. From a careful case study it follows that this requires to take into account the **continuations** of suspended evaluations of observable terms. The bridge between observations and observational equality is provided by an **indistinguishability relation** defined on the carriers of an algebra according to the observations. In the general case, this relation is neither transitive nor a congruence.

1 Introduction

A fundamental aim of formal specifications is to provide a rigorous basis to establish software correctness. Intuitively, a program P is a correct realization of a specification SP if P satisfies all properties required by SP. On the other hand SP should be some description of all its correct realizations. These notions can be, probably in the best

*This work is partially supported by ESPRIT Working Group COMPASS and C.N.R.S. GDR de Programmation.

way, handled within an observational framework. Consequently, the aim of this paper is to provide an observational semantics of algebraic specifications so that the class of observational models of SP matches as well as possible the class of its correct realizations.

We may follow one of at least two directions in the development of an observational approach. The first of them was opened by Sannella and Tarlecki [16] (but also independently by Pepper [14]) and further generalized in [17]. The authors of these papers define the class of observational models (*behaviours* in their terminology) as an extension of the class of the usual models by an equivalence relation (called *observational equivalence*) between algebras, according to some observations Obs. This leads to a somewhat heterogeneous framework where the observational features are directly based on the usual ones. In particular the "observational consistency" always coincides with the usual one. These shortcomings can be avoided in an observational approach developed according to the second direction which mainly aims at defining a true observational satisfaction relation as in [8], [13] or [15]. Consequently, our paper follows this direction.

spec : SWE
use : LIST, NAT
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))

Figure 1.1: Specification of sets with enum

In our approach, an equation $t = t'$ is observationally satisfied by an algebra if for any assignment ν of variables, the results of the evaluations of both $t\nu$ and $t'\nu$ are observationally equal. Unlike in similar approaches, we do not require an observational equality to be a congruence. This allows to better capture the correct realizations of specifications with some "loose" (underspecified) operations such as choose : Set $\rightarrow$ Nat: this operation, when applied to a nonempty set, should return an element of the set. For instance the realization of sets by lists such that choose returns the head of a list, should be considered

as a correct realization of this specification. In this realization the lists $\langle n, m\rangle$ and $\langle m, n\rangle$ are observationally equal, since they are viewed as the same set. However $choose(\langle n, m\rangle)$ and $choose(\langle m, n\rangle)$ produces two **Nat** values which should not be observationally equal. The use of an observational equality being non necessarily a congruence allows to have an observational consistency which does not coincide with the usual one. For instance, the inconsistent specification **SWE** of sets with **enum** (see Figure 1.1) can be declared observationally consistent, provided that the inconsistencies are not observed. This is impossible within the approach of [17] since **SWE** has no behaviours whatever observations are. An observational model of this specification will be described in the following sections. This example points out that in our approach, some data types can be specified in a more straightforward way with less risk of introducing unexpected inconsistencies.

Our main contribution is to provide a suitable notion of observation. We claim that this notion should reflect at the specification level the following paradigm: a user observes the results of some specific computations. Since computations may be represented as evaluations of terms, the part of a specification devoted to observations should be some description of a set of (observable) terms. As soon as only some computations can be observed, it is impossible to distinguish some values from some others. For this reason our approach fully agrees with the following **Indistinguishability Assumption:**

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

The bridge between observations and the observational equality is provided by an indistinguishability relation which is defined further according to the above assumption. From a careful case study it follows that this requires to take into account the **continuations** of suspended evaluations of observable terms. Even if very reasonable, we show that this assumption has some surprising consequences.

2 Basic Definitions

We assume that the reader is familiar with algebraic specifications (see e.g. [9] and [5]). A **signature** Σ consists of a finite set of **sort** symbols **Sorts**$[\Sigma]$ and a finite set of **operation names with arities Ops**$[\Sigma]$ (also 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 Sorts$[\Sigma]$ (resp. Sorts$[\Sigma']$) and X (resp. X') denotes the variables of Σ (resp. of Σ'). A **signature morphism** $\sigma : \Sigma \to \Sigma'$ maps each sort of S to a sort of S', each operation $(f : s_1 \dots s_n \to s) \in \Sigma$ to an operation $\sigma(f)$ of Σ' with the arity $\sigma(s_1) \dots \sigma(s_n) \to \sigma(s)$ 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]. The signatures with the signature morphisms form the usual category of signatures, written **Sig**.

The definition of **(total) Σ-algebras** and **Σ-morphisms** is the standard one. The **category of all Σ-algebras** is denoted by **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**), $\mathbf{T}_{\Sigma(A)}$ (resp. $\mathbf{T}_{\Sigma(A \cup X)}$) denotes the **$\Sigma$-algebra of ground terms** (resp. **terms with variables**) **over the carriers of a Σ-algebra**

[1] Without this assumption, which in a stronger form appears in [7] (page 36, Definition 55), it would be impossible to establish the satisfaction condition for most institutions.

A. Given a signature morphism $\sigma : \Sigma \to \Sigma'$ the **σ-reduct** of a Σ'-algebra A', written $A'|_\sigma$ 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 $-|_\Sigma$.

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

A **valuation** is a morphism $\nu : X \to A$ which maps each $x \in X_s$ to a value $x\nu \in A_s$. The set of all valuations from X to A is written **Val[X,A]**. A **partial valuation** is a valuation preceded by an inclusion $X_0 \subseteq X$. From the freeness of $T_{\Sigma(X)}$ any valuation (resp. partial valuation) ν followed by the inclusion $A \subseteq T_{\Sigma(A)}$ (resp. $A \subseteq T_{\Sigma(A \cup X)}$) extends to a unique morphism (written ambiguously ν) from $T_{\Sigma(X)}$ to $T_{\Sigma(A)}$ (resp. $T_{\Sigma(A \cup X)}$) which maps each term $t \in (T_{\Sigma(X)})_s$ to a **valued term** $t\nu \in (T_{\Sigma(A)})_s$ (resp. **partially valued term** $t\nu \in (T_{\Sigma(A \cup X)})_s$). The **evaluation morphism** from $T_{\Sigma(A)}$ to A is defined as the unique Σ-morphism which maps each element of $(T_{\Sigma(A)})_s \cap A_s$ 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 $\mathbf{t|_p}$. The set of all the positions of t is denoted by **Pos(t)**. The replacement of $t|_p$ by a term r in t is written $\mathbf{t[r]_p}$. The multiple replacement at parallel positions $p_1, \ldots, p_n$ is written $\mathbf{t[r_1 \ldots r_n]_{p_1 \ldots p_n}}$.

Definition 2.1 *An (S-indexed)* **set of contextual variables** *is written $\Diamond$, where each $\Diamond_s$ is a singleton $\{\diamond_s\}$. 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 $\mathbf{MC_{\Sigma(A \cup \Diamond)}}$ (the set of all contexts over A is written $\mathbf{C_{\Sigma(A \cup \Diamond)}}$) is defined as follows:*

$$\mathrm{MC}_{\Sigma(A \cup \Diamond)} = \bigcup_{s \in S} T_{\Sigma(A \cup \{\diamond_s\})}$$

Given $\eta \in \mathrm{MC}_{\Sigma(A \cup \Diamond)}$ (resp. $\eta \in \mathrm{C}_{\Sigma(A \cup \Diamond)}$) we can write $\eta : s \to s'$ instead of $\eta \in (T_{\Sigma(A \cup \{\diamond_s\})})_{s'}$. Application of η on $a \in A_s$ is written $\eta[a]$.

3 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 given only for sort ([8], [10], [13]) or signature[1] ([1], [4]) observation, 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 S_{Obs} which is a subset of the sorts of a specification. Then an observable context is any context $\eta : s \to s'$ with $s' \in S_{Obs}$. Given an element $a \in A_s$ we can observe it via η by evaluating $\eta[a]$. Hence we have the following trivial fact:

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

Fact 3.1 *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 motivated by the specification THREE (c.f. Figure 3.1). Let A be a Sig[THREE]-algebra. It is clear that $\mathbf{g}(a^A)$ does not produce an observable value, since $\mathbf{g(a)}$ is not an observable term. Consequently, we should consider $\mathbf{g}(\diamond)$ 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 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 : → Three **operations :** f, g: Three → 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 : → Hoc **operations :** f : Hoc Hoc → Bool g : Hoc → Hoc **observations :** f(a, c), f(b, g(c))

Figure 3.1: Two exotic specifications

Since Fact 3.1 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 context $\mathsf{f}(\diamond)$ (resp. $\mathbf{g}(\diamond)$). 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], [11], [18]): we consider indistinguishable these pairs of elements, for which we do not observe the contrary. This is stated in the definition below (for a while assume already defined the notion of observable contexts):

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 3.2 *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 $W \in T_{\Sigma(X)}$ (or* **W-indistinguishable***) written $a \sim_W b$, if there is no W-comparator which distinguishes them.*

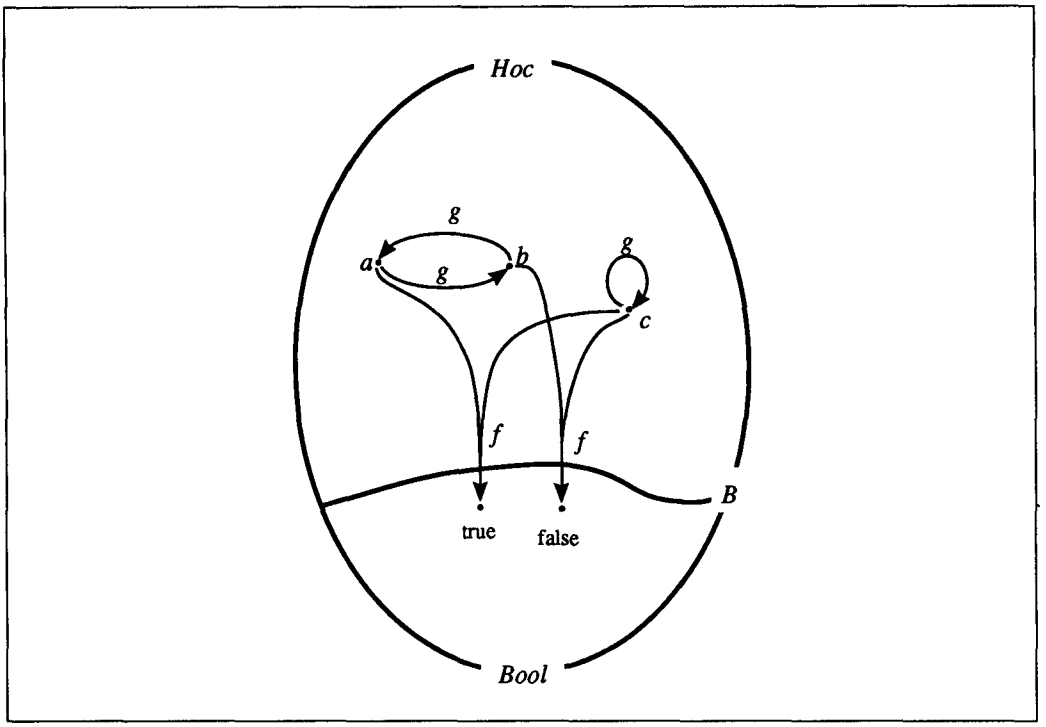

Figure 3.2: A model of the specification AD-HOC

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* $W \subseteq T_{\Sigma(X)}$ *be a set of terms and* $a \in A$ *be an element of a* Σ*-algebra. We say that a context* $\eta \in C_{\Sigma(A \cup \diamond)}$ *is an* **observable context of** a*, if there is a term* $w \in W$*, with valuation* $\nu : X \rightarrow A$ *such that* $w\nu$ *has a leaf* l *verifying* $\eta[l] = w\nu$ *and such that* l *is either the constant of* Σ *interpreted in* A *as* a *or* l *is already* a *itself.*

The underlying intuition of this definition is that an instantiated observable term $w\nu$ 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 only rely on input values. For instance consider the specification AD-HOC (c.f. Figure 3.1). According to the definition, the unique observable context of a^A (resp. b^A) is $f(\diamond, c)$ (resp. $f(\diamond, g(c))$) 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 3.2 and try to partially evaluate in b the observable contexts of a^B and b^B. Since $g(c)$ evaluates to c^B, the evaluations of both $f(\diamond, c)$ and $f(\diamond, g(c))$ yield $f(\diamond, c^B)$. Then the question whether it is not preferable to consider $f(\diamond, c^B)$ as a comparator of a^B and b^B clearly arises. Notice that this comparator distinguishes these two values.

This 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 3.3). Here the elements of

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 :** $0 \neq succ(x)$ $x \neq succ(x) \Rightarrow succ(x) \neq succ(succ(x))$ **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 3.3: Yet other exotic specifications

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 be distinguishable i.e.

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

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

Fact 3.4 *The reflexive-transitive closure of $\underset{\mathbf{pEv}}{\rightarrow}$, written $\overset{*}{\underset{\mathbf{pEv}}{\rightarrow}}$ is an order.* □

Definition 3.5 *Let $W \subseteq T_{\Sigma(X)}$ be a set of terms and A be a Σ-algebra. The* **closure by partial evaluations of W in A,** *written $\widetilde{W}^A$, is defined as follows:*

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

The last notion can be used to state a better definition of observable contexts:

Definition (observable contexts, version 2) *Let* $W \in T_{\Sigma(X)}$ *be a set of observable terms and* A *be a* Σ*-algebra. We say that* $\eta \in C_{\Sigma(A \cup \diamond)}$ *is an* **observable context of** $a \in A_s$ *if* $\eta[a] \in \widetilde{W}^A$.

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 3.3) 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.**

4 The Indistinguishability Relation

According to the previous discussion, we define continuations as follows:

Definition 4.1 *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* $\eta \in MC_{\Sigma(A \cup \diamond)}$ *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. 3.2) from the last section remains unchanged provided that we modify the definition of comparator which must be based on the notion of continuation.

Definition 4.2 *A* **W-comparator** *(comparator, for short) of elements* a *and* b *of a given carrier of a* 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 these concepts by means of the specification SWE (see Figure 1.1).

Example 4.3 *We equip the specification* SWE *with the following set of observable terms*

$$Obs_{SWE} = \{x \in X\} \cup (T_{Sig[LIST](X)})_{Bool} \cup (T_{Sig[LIST](X)})_{Nat}$$

The algebra L *which we would like to consider as a correct realization of* SWE *admits two copies of the carrier of the usual realization of lists: one for lists and the other for sets.*

Consequently, $enum^L$ is the bijection between these two copies preserving axioms ψ_9 and ψ_{10}. In other words $L_{|\mathsf{Sig[LIST]}}$ and $L_{|\mathsf{Sig[SET]}}$ are equal up to some appropriate renaming of operations. The continuations of $l \in L_{\mathsf{List}}$ are the following ones:

$$\mathrm{cont}(l) \quad = \quad \{\mathsf{car}(\eta), \mathsf{member}(n, \eta) \mid n \in L_{\mathsf{Nat}},\ \eta \in (\mathrm{MC}_{\mathsf{Sig[LIST]}(L \cup \diamond)})_{\mathsf{List}}\}$$

Therefore, $\sim_{\mathsf{Obs_{SWE}}}$ is the set theoretical equality on L_{List}. The continuations of $s \in L_{\mathsf{Set}}$ are the following ones:

$$\mathrm{cont}(s) \quad = \quad \{n \in \diamond_{\mathsf{Set}} \mid n \in L_{\mathsf{Nat}}\}$$

Thus $s, s' \in L_{\mathsf{Set}}$ are indistinguishable if they contain the same elements.

We give below the first important theorem which will be useful in establishing some results about observational specifications w.r.t. the specification-building primitives.

Theorem 4.4 *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 all elements $a \in (A'_{|\sigma})_s$ and any multicontext $\eta \in \mathrm{MC}_{\Sigma(A'_{|\sigma} \cup \diamond)}$ we have:*

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

The proof (omitted here) may be found in [12]. Notice that the converse of the above theorem does not hold even if $\sigma(\mathrm{W}) = \mathrm{W}'$.

The definition 3.2 express in which situation two elements of a Σ-algebra are indistinguishable. By the way, it defines an S-sorted relation $\sim_{\mathrm{W}} = (\sim_{\mathrm{W}})_{s \in \mathrm{S}}$ on an algebra, called **indistinguishability relation**. Since this relation is a step toward our observational semantics, we must study its properties w.r.t. at least the forgetful functor and the translation of observable terms in order to be able to cope with specification-building primitives.

Proposition 4.5 *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 $a, b \in (A'_{|\sigma})_s$ we have that if a and b are W'-indistinguishable (in $A'_{\sigma(s)}$) then a and b are also W-indistinguishable (in $(A'_{|\sigma})_s$).*

The proof (omitted here) may be found in [12]. Again, the converse result does not hold even if $\sigma(\mathrm{W}) = \mathrm{W}'$. The following fact is obvious from the definition of the indistinguishability relation.

Fact 4.6 *The indistinguishability relation is reflexive and symmetric.* □

The next fact fully agrees with our claims:

Fact 4.7 *The indistinguishability relation is not a congruence in general.*

Proof *It is enough to go back to Example 4.3. Recall that in the algebra L, 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 $\langle n, m\rangle \sim_{\mathsf{Obs_{SWE}}} \langle m, n\rangle$ but on the other hand $enum^L(\langle n, m\rangle) \not\sim_{\mathsf{Obs_{SWE}}} enum^L(\langle m, n\rangle)$ because of the comparator $\mathsf{car}(\diamond)$ which distinguishes them.* □

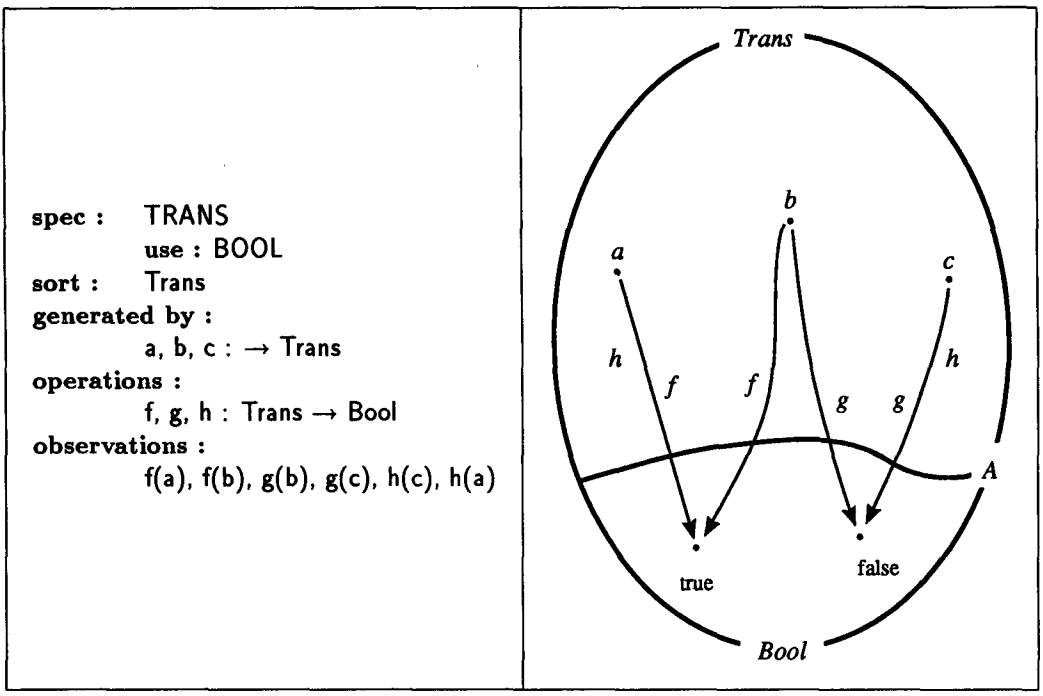

Figure 4.1: Specification TRANS and one of its models

We have also an unexpected negative result:

Fact 4.8 *The indistinguishability relation is not transitive in general.*

Consider the model A (see Figure 4.1) of the specification TRANS. In this algebra we have $a^A \sim_W b^A$ and $b^A \sim_W c^A$, but not $a^A \sim_W c^A$. 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 these 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 3.2, 4.1 and 4.2 but in certain cases this could be explained by an "inconsistent" choice of observations and sometimes should be avoided. The next fact gives a sufficient condition to avoid this problem.

Fact 4.9 *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 $a, b \in A_s$ then the relation $\sim_W$ is transitive on A.*

Proof *Obvious.* □

Fact 4.10 *The relation $\sim_{\mathrm{Obs}_{SWE}}$ from Example 4.3 is transitive.*

Proof *Follows directly from the above proposition, since in Example 4.3 we have shown that the elements of the same carrier set of L have the same continuations.* □

It is possible to have a definition of "$\sim_W$" which is always transitive. One may state that a and b are W-indistinguishable if they do in the sense of Definition 3.2 and if additionally $\mathrm{cont}_W(a) = \mathrm{cont}_W(b)$. 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 3.2, 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.

Since the problem of software correctness is the main motivation of our work, we want to provide a semantical framework which could be further extended with adequate theorem proving features. Incontestably, proving software correctness w.r.t. an algebraic specification requires at least equational reasoning. 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 set-theoretic equality (of the elements of an algebra). Its non-transitive character would eliminate all possibility of equational reasoning. On the contrary, the non-congruence property does not disallow this possibility, subject to beware on some exotic operations such as **enum** (see Figure 1.1). For instance we can replace in some term t of SWE its subterm $t|_p = \mathsf{ins}(\mathsf{s}(0), \mathsf{ins}(0, \emptyset))$ by $\mathsf{ins}(0, \mathsf{ins}(\mathsf{s}(0), \emptyset))$ except when there is some occurrence of **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 [4]). This holds only in the particular case of sort observation (see [8], [13]).

5 Observational Algebras

At this moment we have a little trouble with the non-transitive character of the indistinguishability relation. Since this aspect seems to be crucial for establishing some proof methods, we introduce in this section a flexible concept of observational algebras.

Definition 5.1 *Given a signature* Σ, *an* **observational Σ-algebra** *is a pair* $\langle A, \cong \rangle$ *where* A *is a* Σ*-algebra and* $\cong$ *is an* S*-sorted equivalence relation on* A, *called* **observational equality on** A. *We note* $\mathbf{OAlg}[\Sigma]$ *the class of all observational* Σ*-algebras.*

Notice that any Σ-algebra A can be considered in a straightforward way as an observational Σ-algebra $\langle A, = \rangle$. 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 5.2 *Consider* L *and* $\mathrm{Obs}_{\mathsf{SWE}}$ *both defined in Example* 4.3. *Since* $\sim_{\mathrm{Obs}_{\mathsf{SWE}}}$ *is an equivalence relation (c.f.* 4.10*), the pair* $\langle L, \sim_{\mathrm{Obs}_{\mathsf{SWE}}} \rangle$ *is an observational* $\mathrm{Sig}[\mathsf{SWE}]$*-algebra.*

Definition 5.3 *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 observational equalities i.e:*

$$\forall a, b \in A_s \quad a \cong^A b \Rightarrow \mu(a) \cong^B \mu(b)$$

[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.

Obviously OAlg[Σ] provided with the observational Σ-morphisms forms a category.

Definition 5.4 *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 $(\cong'_{|\sigma})_s = \cong'_{\sigma(s)}$ for all $s \in S$.

The mapping $-_{|\sigma}$ extends on observational morphisms as in the usual framework. Consequently, it defines the corresponding **forgetful functor** from OAlg[Σ'] to OAlg[Σ].

Definition 5.5 *A* **solution** *of an equation $l = r$ in an observational Σ-algebra $\langle A, \cong \rangle$ is a valuation $\nu : X \to A$ such that $\overline{l\nu} \cong \overline{r\nu}$. The set of all the solutions of an equation is written $[l{=}r]_{\langle A, \cong \rangle}$. The set of solutions of a formula φ is defined recursively w.r.t. the connectives $\neg$ and $\wedge$:*

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

where ψ, ψ' are Σ-formulae.

Since all the connectives of the classical logic can be expressed by means of the connectives $\neg$ and $\wedge$, the solutions of an arbitrary formula without quantifiers (i.e. implicitly universally quantified) are well defined by the above definition.

The following theorem relates solutions of a formula and its translation, on an observational algebra and on its σ-reduct:

Theorem 5.6 *Let $\sigma : \Sigma \to \Sigma'$ be a signature morphism, $\langle A', \cong' \rangle$ be an observational Σ'-algebra and φ be a Σ-formula. Let $\nu : X \to A'_{|\sigma}$ and $\nu' : X' \to A'_{|\sigma}$ be valuations such that $x\nu = \sigma(x)\nu'$ for all $x \in X$. Then*

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

A slightly different version of this theorem as well as its proof may be found in [12].

6 Observational Specifications

Definition 6.1 *An* **observational Σ-formula** *is a pair $\langle \varphi, W \rangle$ where $\varphi \in \mathrm{Wff}[\Sigma]$ is a Σ-formula and $W \in T_{\Sigma(X)}$ is a set of terms. We note* **OWff[Σ]** *the set of all observational Σ-formulae.*

In a straightforward way we consider a set $\Phi = \{\varphi_1, \ldots, \varphi_n\}$ of formulae as a conjunction of formulae $\Phi = \varphi_1 \wedge \ldots \wedge \varphi_n$. Thus any pair $\langle \Phi, W \rangle$ can be viewed as a single observational formula and consequently, any observational specification can be viewed as composed by a single observational formula:

Definition 6.2 *An* **observational specification** OSP *is a triple $\langle \Sigma, \Theta, W \rangle$, where Σ is the signature of* OSP *and $\langle \Theta, W \rangle \in \mathrm{OWff}[\Sigma]$.*

One may also define an observational specification as a pair $\langle \Sigma, \mathrm{OAx} \rangle$ with $\mathrm{OAx} = \{\langle \theta_1, \mathrm{W}_1 \rangle, \ldots, \langle \theta_i, \mathrm{W}_i \rangle, \ldots\}$. 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.

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

Definition 6.3 *We say that an observational Σ-algebra $\langle A, \cong \rangle$* **satisfies** *an observational formula $\langle \psi, \mathrm{W} \rangle$, written $\langle A, \cong \rangle \dot{\models} \langle \psi, \mathrm{W} \rangle$, iff:*

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

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

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

Definition 6.4 *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:*

$$\langle A, \cong \rangle \dot{\models} \langle \Theta, \mathrm{W} \rangle$$

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

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

Fact 6.5 *The observational algebra $\langle L, \sim_{\mathrm{Obs_{SWE}}} \rangle$ described in Example 5.2, is a model of the observational specification* SWE.

Proof sketch *Since the observational equality on $\langle L, \sim_{\mathrm{Obs_{SWE}}} \rangle$ is just the indistinguishability relation, we only need to prove that for any axiom θ of* SWE *we have*

$$[\theta]_{\langle L, \sim_{\mathrm{Obs_{SWE}}} \rangle} = \mathrm{Val}[\mathrm{X}, L]$$

This is obvious for the axioms of LIST *since $L_{|\mathrm{Sig[LIST]}}$ is the usual realization of lists and since from Example 4.3 we know that $\sim_{\mathrm{Obs_{SWE}}}$ is the usual equality on $L_{|\mathrm{Sig[LIST]}}$.*

Since the elements observationally equal on L_{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 1.1), we have

$$[\psi_i]_{\langle L, \sim_{\mathrm{Obs_{SWE}}} \rangle} = \mathrm{Val}[\mathrm{X}, L]$$

In matters of ψ_9 and ψ_{10}, it is not difficult to show that $[\psi_9]_{\langle L, = \rangle} = [\psi_{10}]_{\langle L, = \rangle} = \mathrm{Val}[\mathrm{X}, L]$ Then we can conclude that

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

This 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 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 $\langle A, \sim_W \rangle$. Of course, this is possible only when $\sim_W$ 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 [11]. Notice that when $\sim_W$ is not transitive this category has often no terminal object. For instance, the category of observational models of TRANS based on the algebra A (see Figure 4.1) has no terminal object.

We examine now how our satisfaction relation behaves w.r.t. the variance of observational formulae (translation) and the covariance of algebras (σ-reduct). We start by the first requirement of Definition 6.3:

Proposition 6.6 *Let $\sigma : \Sigma \to \Sigma'$ be a signature morphism. For any set of terms $W \subseteq T_{\Sigma(X)}$, any observational Σ'-algebra $\langle A', \cong' \rangle$ and any Σ-formula φ we have:*

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

The proof (omitted here) mainly uses Theorem 5.6 and may be found in [12]. The next step is to study the second condition of Definition 6.3 w.r.t. term translation and the forgetful functor. We examine first the if part of this condition.

Proposition 6.7 *Let $\sigma : \Sigma \to \Sigma'$ be a signature morphism. For all sets of terms $W \subseteq T_{\Sigma(X)}$, $W' \subseteq T_{\Sigma'(X')}$ such that $\sigma(W) \subseteq W'$ and for any observational Σ'-algebra $\langle A', \cong' \rangle$ we have:*

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

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

The proof may be found in [12].

The next step should be to prove the converse of the above proposition restricted to $W' = \sigma(W)$. Unfortunately this does not hold in general[1]. Consequently the **satisfaction condition** (see [6] or [7]) does not hold in our approach without additional assumptions. Nevertheless an institution can be defined within this framework, under some restrictions on either signature morphisms or the set of observable terms (see [12]).

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 observational semantics easily extends to a stratified loose observational semantics without additional assumptions. The next theorem shows that our observational semantics is compatible w.r.t. enrichment and renaming:

Theorem 6.8 *Let $\sigma : \Sigma \to \Sigma'$ be a signature morphism. For all observational specifications $OSP = \langle \Sigma, \Theta, W \rangle$ and $OSP' = \langle \Sigma', \Theta', W' \rangle$ such that $\sigma(\Theta) \subseteq \Theta'$ and $\sigma(W) \subseteq W'$ we have:*

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

Proof *From definitions 6.4 and 6.3 it is enough to prove:*

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

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

[1] An example illustrating this fact may be found in [12].

- **Proof of (i)**
  Let $\langle A', \cong' \rangle \in \mathrm{OAlg}[\Sigma']$ *such that*

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

  Since $\sigma(\Theta) \subseteq \Theta'$, *by definition of solution of a conjunction of formulae (c.f.* 5.5*) we have* $\sigma(\Theta)_{\langle A', \cong' \rangle} \supseteq \Theta'_{\langle A', \cong' \rangle}$. *Hence* $[\sigma(\Theta)]_{\langle A', \cong' \rangle} = \mathrm{Val}[X', A']$ *which according to Proposition* 6.6 *implies that*

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

- **Proof of (ii)** *follows directly from Proposition* 6.7.

□

This last result deserves some comments. Indeed, it is somehow surprising that we obtain such a strong result, without any further hypotheses w.r.t. the axioms of the specification, while similar results hold for other observational approaches only when axioms are restricted to equations. It is quite important to note that, in our approach, observational algebras are algebras equipped with some observational equality. To obtain a model of a given observational specification, this observational equality should be "compatible" with the given axioms and observations. The point is that this observational equality is preserved by forgetful functors. In other approaches, one could define as well an observational equality, but this equality is **deduced** from the specified observations. Hence, when we apply some forgetful functor, the set of observations is modified (and so is the corresponding observational equality), and the result of Theorem 6.8 cannot be obtained without very strong restrictions on the axioms and on the observations.

7 Concluding Remarks

We have provided a suitable notion of observation based on terms. 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 in this framework requires to take into account multicontexts and partial evaluations of observable terms. In this way, we have introduced the concept of continuations which underlies 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 similar to the Nerode congruence [8]. However, unlike in [13], in our approach, two observational algebras differing on non observable junk do not necessarily satisfy the same observational formulae. We do not privilege reachable elements, since this is most suitable for defining the observational semantics of parameterized specifications in a loose framework (which is the topic of our current research). Moreover, one could think that our indistinguishability relation coincide with Reichel's I-indistinguishability [15] when we restrict our approach to sort observation and Reichel's one to total algebras. This is not true, since we use multicontexts from $\mathrm{MC}_{\Sigma(A \cup \Diamond)}$ instead of $\mathrm{MC}_{\Sigma(\Diamond)}$. Consequently, in our approach non observable junk can influence the indistinguishability of two elements of a carrier of an algebra while it cannot in other works. Thus the roles of reachable and non reachable values are symmetric w.r.t. our indistinguishability relation.

Being convinced of the necessity of equational reasoning in proving abstract implementation correctness, we have introduced in our semantics an additional stage over the indistinguishability relation, namely the observational equality. Then we have defined observational algebras, observational formulae and the corresponding satisfaction relation. In this way we have developed an observational approach which has all properties required to define the semantics of an algebraic specification language, even if it does not provide an institution.

The main disadvantage of our approach is that the logical formulae we use are always implicitly universally quantified. Consequently, the first improvement is to redefine our satisfaction relation and to prove once again some results in order to take into account existential quantifiers. Finally, the most important area of further research is the development of proof methods on top of our approach.

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 *Report LIENS-91-6, 1991*

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

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

[6] **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*

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

[8] **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*

[9] **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)*

[10] **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)*

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

[12] **Knapik T.** Sémantique Observationnelle des Spécifications Algébriques: application à la modularité et à l'implémentation *Ph. D. thesis in preparation, Université de Paris-Sud, Orsay 1992*

[13] **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*

[14] **Pepper P.** On the Correctness of Type Transformations *Talk at 2nd Workshop on Theory and Applications of Abstract Data Types, Passau, May 1983*

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

[16] **Sannella D., Tarlecki A.** On Observational Equivalence and Algebraic Specification, *TapSoft, Berlin 1985, LNCS 185, 308-322*

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

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