Observational Approaches in Algebraic Specifications : a Comparative Study

Gilles BERNOT Michel BIDOIT
Teodor KNAPIK

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

LIENS - 91 - 6

April 1992

Observational Approaches in Algebraic Specifications: A Comparative Study *

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

L. I. E. N. S.
C.N.R.S. U.R.A 1327
Ecole Normale Supérieure
45 Rue d'Ulm
F – 75230 PARIS Cedex 05 France

Abstract

This paper focuses on observability issues in the framework of loose algebraic specifications. It is well known that some correct realizations of an algebraic specification do not satisfy all the axioms of the specification. They remain correct provided that the differences between the properties of the realization and the properties required by the specification are not "observable". We compare various observational approaches developed so far. We point out their respective advantages and limitations. Expressive power is our main criterion for the discussion.

Keywords: algebraic specification, observability, implementation

1 Introduction

Since the pioneering work of [6], algebraic specifications have been advocated as being one of the most promising approach to enhance software quality and reliability. Algebraic specifications proved to be useful not only to formally describe complex software systems, but also to prototype them (e.g. by transforming axioms into an equivalent set of rewrite rules, or by resolution as in SLOG [3] or RAP [9]), and to prove the correctness of these software systems (w.r.t. their formal, algebraic specification). More recently, it has also been shown that algebraic specifications provide suitable means to compute adequate test sets for the described software systems, and that they provide also a formal basis to promote software reusability. An important aim of the research activity in the area of algebraic specifications is to provide adequate concepts, languages and tools to cover the whole software development process and to establish their mathematical foundations.

In this paper we shall focus on problems arising when one tries to establish the correctness of some software w.r.t. its specification. To better understand the very nature of the problems involved, we shall first briefly recall the main underlying paradigm of the loose approach:

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

- A specification is supposed to describe a future or existing system in such a way that the properties of the system (**what** the system does) are expressed, and the implementation details (**how** it is done) are omitted. Thus a specification language aims at describing *classes* of correct (w.r.t. the intended purposes) realizations. In contrast a programming language aims at describing *specific* realizations.

- In a loose framework, the semantics of some specification SP is a class Alg[SP] of (non-isomorphic) algebras. Given some realization (program) P, its correctness w.r.t. the specification SP can then be established by relating the program P with one of the algebras of the class Alg[SP]. Roughly speaking, the program P will be correct w.r.t. the specification SP if and only if the algebra defined by P belongs to the class Alg[SP].

This understanding of program correctness w.r.t. algebraic specifications is however an over-simplified picture. Indeed, if correctness is defined in such a way, then most realizations that we would like to consider as being correct (from a practical point of view) turn out to be incorrect ones. This is illustrated by the following example:

spec : SET
  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
axioms :
  $\mathrm{ins}(x,\mathrm{ins}(x,s)) = \mathrm{ins}(x,s)$
  $\mathrm{ins}(x,\mathrm{ins}(y,s)) = \mathrm{ins}(y,\mathrm{ins}(x,s))$
  $\mathrm{del}(x, \emptyset) = \emptyset$
  $\mathrm{del}(x, \mathrm{ins}(x, s)) = \mathrm{del}(x, s)$
  $x \neq y \Rightarrow \mathrm{del}(x, \mathrm{ins}(y, s)) = \mathrm{ins}(y, \mathrm{del}(x, s))$
  $x \in \emptyset = \mathrm{false}$
  $x \in \mathrm{ins}(x,s) = \mathrm{true}$
  $x \neq y \Rightarrow x \in \mathrm{ins}(y,s) = x \in s$

If we consider a standard realization of SET by e.g. lists, we do not obtain a correct realization: this is due to the axioms expressing the commutativity of the insertion operation, which do not hold for lists. However, if we notice that indeed we are only interested in the result of some computations (e.g. membership), then it is clear that our realization "behaves" correctly. This leads to a refined understanding of program correctness: a program P should be considered as being correct w.r.t. its specification SP if and only if the algebra defined by P is a "behaviourally correct realization" of SP. In other words, the differences between the specification and the program should not be "observable", w.r.t. some appropriate notion of "observability".

The problem is now to specify the "observations" to be associated to some specification, and to define the semantics of such "observations" in order to obtain a framework that will capture the essence of program correctness. Up to now, various notions of observability have been introduced, involving observation techniques based on sorts [5], [21], [10], [4], [18], [11], [19], [14], [13], operations [1], terms [17], [7] or formulae [16], [17]. It is unfortunately difficult to compare these various notions of observability and to decide which one is better suited to solve the problem described above. The aim of this paper is to provide grounds for such a comparative study. To achieve this goal we shall use the notion of "observational equivalence" of Sannella and Tarlecki, first introduced in [16] and further developed in [17]. The expressive power of the various observation techniques mentioned above will be our main criterion for the discussion.

This paper is organized as follows. In Section 2 we summarize some basic notations that will be used later on and we introduce various observation techniques. In Section 3 we briefly recall the observational-equivalence-based semantics. Then we use this semantics in Section 4 to establish a classification of the various observation techniques and some other results. In Section 5 we point out some limitations of observational-equivalence-based approaches.

2 Observational Specifications

We assume that the reader is familiar with algebraic specifications (see e.g. [6] and [2]).

A **signature $\boldsymbol{\Sigma}$** consists of a finite set of **sort** symbols **Sorts[$\boldsymbol{\Sigma}$]** (also denoted by **S**) and a finite set of **operation names with arities Ops[$\boldsymbol{\Sigma}$]** (also denoted by Σ). We denote by $\mathbf{T}_{\boldsymbol{\Sigma}}$ (resp. $\mathbf{T}_{\boldsymbol{\Sigma}(\mathbf{X})}$) the Σ-algebra of **ground terms** (resp. **terms with variables**) over Σ. We use **At[$\boldsymbol{\Sigma}$]** to denote the set of **atoms** over Σ (i.e. $\mathrm{At}[\Sigma] = \{\mathrm{t} = \mathrm{t}' \mid \mathrm{t}, \mathrm{t}' \in \mathrm{T}_{\Sigma(\mathrm{X})}\}$) and **At[W]** to denote the set of all atoms built only with a set W of terms (i.e. $\mathrm{At}[\mathrm{W}] = \{\mathrm{t} = \mathrm{t}' \mid \mathrm{t}, \mathrm{t}' \in \mathrm{W}\}$). From atoms, **connectives** ($\vee$, $\wedge$, $\neg$ etc.) and **quantifiers** ($\exists$, $\forall$) we construct the set of all **well formed formulae** over Σ, written **Wff[$\boldsymbol{\Sigma}$]**, in the usual way. The definition of a **(total) $\boldsymbol{\Sigma}$-algebra** is the standard one, as well as the satisfaction relation between Σ-algebras and Σ-formulae. The **class of all $\boldsymbol{\Sigma}$-algebras** is denoted by **Alg[$\boldsymbol{\Sigma}$]**. The **restriction** (by the forgetful functor) of a Σ-algebra A to a subsignature Σ' of Σ is denoted by $\boldsymbol{A}_{|_{\boldsymbol{\Sigma}'}}$.

An **algebraic specification SP** is a pair $\langle \boldsymbol{\Sigma}, \boldsymbol{\Theta} \rangle$ where Σ is its signature (also written **Sig[SP]**) and $\Theta \subseteq \mathrm{Wff}[\Sigma]$ is a finite set of axioms. We denote by **Alg[SP]** the **class of the models** of SP, which by definition is the class of all Σ-algebras for which Θ is satisfied.

"To rely on some observational technique" means "to choose which kind of objects we observe and how we observe them". In this paper, for a given signature Σ (with $\mathrm{S} = \mathrm{Sorts}[\Sigma]$), we will consider observation techniques based on:

- **sorts**
  We consider some set of observable sorts $\mathrm{S}_{\mathrm{Obs}}$ which is a subset of the sorts of the signature ($\mathrm{S}_{\mathrm{Obs}} \subseteq \mathrm{S}$).
- **operations**
  We consider some set of observable operations Σ_{Obs} which is a subset of the operations of the signature ($\Sigma_{\mathrm{Obs}} \subseteq \Sigma$).
- **terms**
  We consider some set of observable terms W ($\mathrm{W} \subseteq \mathrm{T}_{\Sigma(\mathrm{X})}$).
- **atoms**
  We consider some set of observable Σ-atoms $\mathcal{E}$ ($\mathcal{E} \subseteq \mathrm{At}[\Sigma]$).
- **formulae**
  We consider some set of observable Σ-formulae $\boldsymbol{\Phi}$ ($\boldsymbol{\Phi} \subseteq \mathrm{Wff}[\Sigma]$).

Once we have chosen some observation technique, we can specify, using this technique, that some parts of an algebraic specification are observable. An observational specification is formed by adding a specification of the objects to be observed to a usual algebraic specification, as precised by the following definition.

Definition 2.1

An **observational specification** *is a pair* $\langle \mathrm{SP}, \mathrm{Obs} \rangle$*, where* SP *is a usual algebraic specification and* Obs *is a set of observations over* Sig[SP]*, which can be either a set of sorts, operations, terms, atoms or formulae, according to the observation technique in use.*

The next step is to define the semantics of such observational specifications.

3 Observational Semantics

As already mentioned in the introduction, the usual satisfaction relation is not sufficient to reflect the paradigm: "the class of the models of a specification represents all its acceptable realizations." Some correct programs could correspond to algebras which do not satisfy all the axioms of the specification, provided that the differences between the properties of the algebra and the properties required by the specification are not observable. Thus, a correct realization of an algebraic specification SP may correspond to an algebra which is outside of Alg[SP]. The aim of an observational semantics is to define the class of "observational models" (or "behaviours") of SP, denoted by **Beh[⟨SP, Obs⟩]**, which better matches the class of correct realizations of SP (w.r.t. Obs).

There are mainly two possible ways to define an observational semantics of SP. We could extend Alg[SP] by including some additional algebras which are "observationally equivalent" to a model of Alg[SP] w.r.t. Obs (**extension by observational equivalence**, see [16], [17], [7]). We could also directly relax the satisfaction relation (**extension by relaxing the satisfaction relation**, see [18], [14], [1]). Our comparative study of observation techniques will be based on the notion of "observational equivalence".

First we need an appropriate equivalence relation $\equiv_{\mathrm{Obs}}$ on $\mathrm{Alg}[\Sigma]$, also called observational equivalence of algebras w.r.t. Obs (cf. [16], [17]). The choice of $\equiv_{\mathrm{Obs}}$ depends on the observational technique in use. For each observational technique we give below a definition of the corresponding observational equivalence $\equiv_{\mathrm{Obs}}$.

Definition 3.1

Given a set of observations Obs*, an observational equivalence w.r.t.* Obs*, written* $\equiv_{\mathrm{Obs}}$*, is an equivalence relation on* $\mathrm{Alg}[\Sigma]$ *defined (depending on the observation technique used to express* Obs*) as follows:*

- $\mathrm{Obs} = \mathrm{S}_{\mathrm{Obs}}$ *(observable sorts)*[1]

$$A \equiv_{\mathrm{S}_{\mathrm{Obs}}} B \quad \textit{iff} \quad \forall\ \mathrm{t}, \mathrm{t}' \in (\mathrm{T}_{\Sigma(\mathrm{X})})_{\mathrm{s}},\ \ \mathrm{s} \in \mathrm{S}_{\mathrm{Obs}} \quad A \models \mathrm{t} = \mathrm{t}' \ \Leftrightarrow\ B \models \mathrm{t} = \mathrm{t}'$$

  In other words, A and B are observationally equivalent w.r.t. a set of observable sorts, if A and B satisfy the same equalities between terms of observable sorts.

- $\mathrm{Obs} = \Sigma_{\mathrm{Obs}}$ *(observable operations)*[1]

$$\begin{array}{l} A \equiv_{\Sigma_{\mathrm{Obs}}} B \quad \textit{iff} \\ \quad \forall\ \mathrm{f}, \mathrm{g} \in \Sigma_{\mathrm{Obs}}, \quad \textit{with the same target sort} \\ \quad \forall\ \sigma : \mathrm{X} \rightarrow \mathrm{T}_{\Sigma(\mathrm{X})} \\ \qquad A \models \mathrm{f}(\mathrm{x}_1, \ldots, \mathrm{x}_\mathrm{n})\sigma = \mathrm{g}(\mathrm{y}_1, \ldots \mathrm{y}_\mathrm{m})\sigma \ \Leftrightarrow\ B \models \mathrm{f}(\mathrm{x}_1, \ldots, \mathrm{x}_\mathrm{n})\sigma = \mathrm{g}(\mathrm{y}_1, \ldots \mathrm{y}_\mathrm{m})\sigma \end{array}$$

In other words, A and B are observationally equivalent w.r.t. a set of observable operations, if A and B satisfy the same equalities between terms with observable head.

- $\mathrm{Obs} = \mathrm{W}$ *(observable terms)*[1]

$$A \equiv_{\mathrm{W}} B \quad \textit{iff} \quad \forall\, \mathrm{l}, \mathrm{r} \in \mathrm{W} \quad \forall\, \sigma, \rho : \mathrm{X} \to \mathrm{T}_{\Sigma(\mathrm{X})} \quad A \models \mathrm{l}\sigma = \mathrm{r}\rho \quad \Leftrightarrow \quad B \models \mathrm{l}\sigma = \mathrm{r}\sigma$$

In other words, A and B are observationally equivalent w.r.t. a set of observable terms, if A and B satisfy the same equalities between observable terms and their (non necessarily ground) instantiations.[2]

- $\mathrm{Obs} = \mathcal{E}$ *(observable atoms)*

$$A \equiv_{\mathcal{E}} B \quad \textit{iff} \quad \forall\, \mathrm{e} \in \mathcal{E} \quad A \models \mathrm{e} \quad \Leftrightarrow \quad B \models \mathrm{e}$$

In other words, A and B are observationally equivalent w.r.t. a set of observable atoms, if A and B satisfy the same observable atoms.

- $\mathrm{Obs} = \Phi$ *(observable formulae)*

$$A \equiv_{\Phi} B \quad \textit{iff} \quad \forall \varphi \in \Phi \quad A \models \varphi \quad \Leftrightarrow \quad B \models \varphi$$

In other words, A and B are observationally equivalent w.r.t. a set of observable formulae, if A and B satisfy the same observable formulae.

An observational model of $\langle \mathrm{SP}, \mathrm{Obs} \rangle$ is an algebra observationally equivalent to a model of SP as defined below:

Definition 3.2

The class of observational models of $\langle \mathrm{SP}, \mathrm{Obs} \rangle$, written $\mathbf{Beh}[\langle \mathbf{SP}, \mathbf{Obs} \rangle]$ *is defined as follows:*

$$\mathrm{Beh}[\langle \mathrm{SP}, \mathrm{Obs} \rangle] = \{ B \in \mathrm{Alg}[\Sigma] \;\mid\; \exists\, A \in \mathrm{Alg}[\mathrm{SP}] \quad B \equiv_{\mathrm{Obs}} A \}$$

It should be noted that ordinary specifications can be considered as observational specifications in a straightforward way. For a given observation technique α we just have to consider a set $\mathrm{Obs}_{\alpha}^{\mathrm{all}}$ which makes "everything" observable. Then for all SP

$$\mathrm{Beh}[\langle \mathrm{SP}, \mathrm{Obs}_{\alpha}^{\mathrm{all}} \rangle] = \mathrm{Alg}[\mathrm{SP}]$$

For instance if we consider observable operations then the set $\Sigma_{\mathrm{Obs}}^{\mathrm{all}}$ which makes everything observable is just the whole signature Σ. Then we have:

$$\mathrm{Beh}[\langle \mathrm{SP}, \Sigma \rangle] = \mathrm{Alg}[\mathrm{SP}]$$

This correctly reflects the fact that the class of observational models associated to an ordinary specification SP is exactly Alg[SP].

---

[1] There is a variant of these techniques which consists on observation of ground objects (i.e. ground terms of sorts S in the case of sort observation, ground terms with observable head in the case of operation observation etc).

[2] We consider the atoms formed by substituted terms $\mathrm{l}\sigma = \mathrm{r}\rho$ rather than $\mathrm{l} = \mathrm{r}$ only. For instance, when $\mathrm{W} = \{\mathrm{t}\}$, the observational equivalence $\equiv_{\mathrm{W}}$ does not rely only on the satisfaction of the unique (trivial) atom $\mathrm{t} = \mathrm{t}$, but also on the satisfaction of all atoms $\mathrm{t}\sigma = \mathrm{t}\rho$.

4 Expressive Power of Observation Techniques

It is of first importance to have a precise understanding of the respective expressiveness of various observation techniques for the following reason. The observation technique will be the basis of a correctness notion (of some software w.r.t. its specification). If the observation technique is not "powerful enough", then it may be impossible to take into account some realizations that we would like to consider as being relevant (because they will still be incorrect). The crucial point here is that when the observation technique is not powerful enough, then the set of "observed properties" (i.e. those properties that are used to decide the correctness of the realization) is too large, hence the class of correct realizations is too small.

In this section we compare the expressive power of observation techniques introduced in Section 2. The criterion for this comparison is provided by following two definitions.

Definition 4.1
An observation technique α *is* **finer** *than another one* β*, written* $\boldsymbol{\alpha \succeq \beta}$*, if and only if: For any specification* SP *and any set* Obs_β *of observations defined using technique* β*, there exists a set of observations* Obs_α *(defined using technique* α*) such that both* $\langle \mathrm{SP}, \mathrm{Obs}_\alpha \rangle$ *and* $\langle \mathrm{SP}, \mathrm{Obs}_\beta \rangle$ *have the same observational models, i.e.* $\mathrm{Beh}[\langle \mathrm{SP}, \mathrm{Obs}_\alpha \rangle] = \mathrm{Beh}[\langle \mathrm{SP}, \mathrm{Obs}_\beta \rangle]$.

Definition 4.2
An observation technique α *is* **strictly finer** *than another one* β*, written* $\boldsymbol{\alpha \succ \beta}$ *if it is finer and if:*
There exists a specification SP *and a set* Obs_α *of observations defined using technique* α*, such that there is no set of observations* Obs_β *(defined using technique* β*) for which both* $\langle \mathrm{SP}, \mathrm{Obs}_\alpha \rangle$ *and* $\langle \mathrm{SP}, \mathrm{Obs}_\beta \rangle$ *have the same observational models, i.e.*

$$\alpha \succeq \beta \quad \textit{and} \quad \exists\ \mathrm{SP}\ \ \exists\ \mathrm{Obs}_\alpha\ \ \forall\ \mathrm{Obs}_\beta \quad \mathrm{Beh}[\langle \mathrm{SP}, \mathrm{Obs}_\alpha \rangle] \neq \mathrm{Beh}[\langle \mathrm{SP}, \mathrm{Obs}_\beta \rangle]$$

In the following we use the definitions above to compare the expressive power of the observation techniques introduced in Section 2.

Proposition 4.3
Fineness orders observation techniques as follows:

$$\textit{formulae} \succeq \textit{atoms} \succeq \textit{terms} \succeq \textit{operations} \succeq \textit{sorts}$$

Proof
In order to prove that $\alpha \succeq \beta$*, from Definitions* 3.1, 3.2 *and* 4.1 *it is enough to construct a set* Obs_α *corresponding to the given* Obs_β *such that*

$$\forall\ A, B \in \mathrm{Alg}[\Sigma] \quad A \equiv_{\mathrm{Obs}_\alpha} B \ \ \textit{iff}\ \ A \equiv_{\mathrm{Obs}_\beta} B$$

- **formulae $\succeq$ atoms**
  This is clear since each set of atomic formulae is a set of formulae as well.
- **atoms $\succeq$ terms**
  Given a set W *of terms the corresponding set of atomic observations is given by*

  $$\mathcal{E} \;=\; \{\mathrm{l}\sigma = \mathrm{r}\rho \;\mid\; \mathrm{l}, \mathrm{r} \in \mathrm{W},\ \sigma, \rho : \mathrm{X} \to \mathrm{T}_{\Sigma(\mathrm{X})}\}$$

- **terms $\succeq$ operations**
  Term observation corresponding to an operation observation Σ_{Obs} *is given by the set:*

  $$\mathrm{W} \;=\; \{\mathrm{f}(\mathrm{t}_1, \ldots, \mathrm{t}_\mathrm{n}) \;\mid\; (\mathrm{f} : \mathrm{s}_1 \ldots \mathrm{s}_\mathrm{n} \to \mathrm{s}) \in \Sigma_{\mathrm{Obs}},\ \ \mathrm{t}_1 \in (\mathrm{T}_{\Sigma(\mathrm{X})})_{\mathrm{s}_1}, \ldots, \mathrm{t}_\mathrm{n} \in (\mathrm{T}_{\Sigma(\mathrm{X})})_{\mathrm{s}_\mathrm{n}}\}$$

- **operations $\succeq$ sorts**
  Given a set of observable sorts $\mathrm{S_{Obs}}$ *we construct the corresponding set of observable operations as follows:*
$$\Sigma_{\mathrm{Obs}} = \{\mathrm{f} : \mathrm{s}_1 \dots \mathrm{s}_\mathrm{n} \to \mathrm{s} \in \Sigma \;\mid\; \mathrm{s} \in \mathrm{S_{Obs}}\}$$

□

The above result is not very surprising. Indeed it is even possible to show that the ordering between the observation techniques is a strict one:

Proposition 4.4

Strict fineness orders observation techniques as follows:
$$\textit{formulae} \succ \textit{atoms} \succ \textit{terms} \succ \textit{operations} \succ \textit{sorts}$$

Proof

We consider the following specification

spec : SP
sort : s
generated by :
  a, b, c, d : $\to$ s
axioms :
  a = b
  b = c
  c = d

From the axioms of SP *and the fact that* $\Sigma = \mathrm{Sig[SP]}$ *is reduced to constants, we have: for any algebra* $A \in \mathrm{Alg[SP]}$ *and for any atom* $\mathrm{e} \in \mathrm{At}[\Sigma]$*:* $A \models \mathrm{e}$*. Therefore:*
$$\forall\, \mathcal{E} \subseteq \mathrm{At}[\Sigma] \quad \mathrm{Beh}[\langle \mathrm{SP}, \mathcal{E}\rangle] = \mathrm{Alg}[\langle \Sigma, \mathcal{E}\rangle]$$

- **formulae $\succ$ atoms**
  Assume that the set of observable formulae is the singleton $\Phi = \{\mathrm{a} = \mathrm{b} \vee \mathrm{c} = \mathrm{d}\}$*. Since any* $A \in \mathrm{Alg[SP]}$ *satisfies* Φ *we have*
$$\mathrm{Beh}[\langle \mathrm{SP}, \Phi\rangle] = \mathrm{Alg}[\langle \Sigma, \Phi\rangle]$$
  Assume now that there exists $\mathcal{E} \subseteq \mathrm{At}[\Sigma]$ *such that*
$$\mathrm{Beh}[\langle \mathrm{SP}, \mathcal{E}\rangle] = \mathrm{Beh}[\langle \mathrm{SP}, \Phi\rangle]$$
  Thus
$$\mathrm{Alg}[\langle \Sigma, \mathcal{E}\rangle] = \mathrm{Alg}[\langle \Sigma, \Phi\rangle]$$
  But this is in contradiction with the fact that $\mathrm{Alg}[\langle \Sigma, \Phi\rangle]$ *has no initial object while, for any* $\mathcal{E} \subseteq \mathrm{At}[\Sigma]$, $\mathrm{Alg}[\langle \Sigma, \mathcal{E}\rangle]$ *does.*
- **atoms $\succ$ terms**
  Consider the previous specification SP with the set $\mathcal{E}_0 = \{\mathrm{a} = \mathrm{b}, \mathrm{c} = \mathrm{d}\}$ *of atomic observations. Assume that there exists* $\mathrm{W} \subseteq \mathrm{T}_\Sigma$ *such that*
$$\mathrm{Beh}[\langle \mathrm{SP}, \mathrm{W}\rangle] = \mathrm{Beh}[\langle \mathrm{SP}, \mathcal{E}_0\rangle] \tag{i}$$
  For the same reason as before (i) *is equivalent to*
$$\mathrm{Alg}[\langle \Sigma, \mathrm{At[W]}\rangle] = \mathrm{Alg}[\langle \Sigma, \mathcal{E}_0\rangle] \tag{ii}$$
  Since Σ *is reduced to constants, we must therefore have* $\mathrm{At[W]} \supseteq \mathcal{E}_0$*. Thus* $\mathrm{W} \supseteq \{\mathrm{a}, \mathrm{b}, \mathrm{c}, \mathrm{d}\}$*, hence* $(\mathrm{b} = \mathrm{c}) \in \mathrm{At[W]}$*. Consider* $B \in \mathrm{Alg}[\Sigma]$ *such that* $\mathrm{a}^B = \mathrm{b}^B \neq \mathrm{c}^B = \mathrm{d}^B$*. Then*
$$\begin{array}{rl} & B \in \mathrm{Alg}[\langle \Sigma, \mathcal{E}_0\rangle] \\ \textit{and} & B \notin \mathrm{Alg}[\langle \Sigma, \mathrm{At[W]}\rangle] \end{array}$$
  which contradicts (ii).

It is easy to construct analogous examples which prove **terms $\succ$ operations $\succ$ sorts**. $\square$

When $\mathrm{Obs}_\alpha \succ \mathrm{Obs}_\beta$, in general for a given SP_1 and Obs_α there is no set of observations Obs_β such that $\langle \mathrm{SP}_1, \mathrm{Obs}_\beta\rangle$ has the same behaviour as $\langle \mathrm{SP}_1, \mathrm{Obs}_\alpha\rangle$. However some systematic transformations can be performed on $\langle \mathrm{SP}_1, \mathrm{Obs}_\alpha\rangle$ in order to obtain $\langle \mathrm{SP}_2, \mathrm{Obs}_\beta + \Delta\Theta\rangle$ which "simulates" the behaviour of $\langle \mathrm{SP}_1, \mathrm{Obs}_\alpha\rangle$, where $\Delta\Theta$ is a particularly simple set of formulae.

Proposition 4.5 (Term observation can be simulated by operation observation)
Let $\mathrm{SP}_1 = \langle \Sigma_1, \Theta_1\rangle$. *Let* W *be a set of* Σ_1*-terms. For each term* $\mathrm{t} \in \mathrm{W}$*, let* s *be the sort of* t*, and* $\mathrm{x}_1, \ldots, \mathrm{x}_\mathrm{n}$ *be the variables occurring in* t *(of sorts* $\mathrm{s}_1, \ldots, \mathrm{s}_\mathrm{n}$ *respectively); we introduce a new operation* $\mathrm{f}_\mathrm{t} : \mathrm{s}_1 \ldots \mathrm{s}_\mathrm{n} \rightarrow \mathrm{s}$*, and a new axiom* $\mathrm{e}_\mathrm{t} : \mathrm{f}_\mathrm{t}(\mathrm{x}_1, \ldots, \mathrm{x}_\mathrm{n}) = \mathrm{t}$. *Let then*

$$\begin{aligned} \Delta\Sigma &= \{\mathrm{f}_\mathrm{t} \mid \mathrm{t} \in \mathrm{W}\} \\ \Delta\Theta &= \{\mathrm{e}_\mathrm{t} \mid \mathrm{t} \in \mathrm{W}\} \\ \textit{and}\quad \mathrm{SP}_2 &= \langle \Sigma_1 + \Delta\Sigma, \Theta_1 + \Delta\Theta\rangle \end{aligned}$$

The observational specification $\langle \mathrm{SP}_1, \mathrm{W}\rangle$ *is "simulated" by the observational specification* $\langle \mathrm{SP}_2, \Delta\Sigma + \Delta\Theta\rangle$ *in the sense that:*

$$\mathrm{Beh}[\langle \mathrm{SP}_2, \Delta\Sigma + \Delta\Theta\rangle]_{|\Sigma_1} = \mathrm{Beh}[\langle \mathrm{SP}_1, \mathrm{W}\rangle]$$

Proof is given in Appendix A.

This transformation can be rather impractical when W is large since we need to enrich SP_1 with $|\mathrm{W}|$ operations and $|\mathrm{W}|$ axioms in order to obtain SP_2.

Proposition 4.6 (Operation observation can be simulated by sort observation)
Let $\mathrm{SP}_1 = \langle \Sigma_1, \Theta_1\rangle$. *Let* $\Sigma_{\mathrm{Obs}} \subseteq \Sigma_1$ *be a set of observable operations. For each target sort* s *of the observable operations we introduce a new sort* $\mathrm{s}_{\mathrm{new}}$. *Let then*

$$\mathrm{S}_{\mathrm{Obs}} = \{\mathrm{s}_{\mathrm{new}} \mid \exists\ (\mathrm{f} : \mathrm{s}_1 \ldots \mathrm{s}_\mathrm{n} \rightarrow \mathrm{s}) \in \Sigma_{\mathrm{Obs}}\}$$

For each $\mathrm{f} : \mathrm{s}_1 \ldots \mathrm{s}_\mathrm{n} \rightarrow \mathrm{s} \in \Sigma_{\mathrm{Obs}}$ *we introduce a new operation* $\mathrm{f}_{\mathrm{new}} : \mathrm{s}_1 \ldots \mathrm{s}_\mathrm{n} \rightarrow \mathrm{s}_{\mathrm{new}}$. *Let*

$$\Delta\Sigma = \langle \mathrm{S}_{\mathrm{Obs}}, \{\mathrm{f}_{\mathrm{new}} \mid \mathrm{f} \in \Sigma_{\mathrm{Obs}}\}\rangle$$

Next, for each $\mathrm{g} : \mathrm{p}_1 \ldots \mathrm{p}_\mathrm{n} \rightarrow \mathrm{s} \in \Sigma_{\mathrm{Obs}}$ *and* $\mathrm{h} : \mathrm{r}_1 \ldots \mathrm{r}_\mathrm{m} \rightarrow \mathrm{s} \in \Sigma_{\mathrm{Obs}}$ *we introduce a new axiom* $\mathrm{a}_{\mathrm{g,h}} :\ \mathrm{g}(\mathrm{x}_1, \ldots, \mathrm{x}_\mathrm{n}) = \mathrm{h}(\mathrm{y}_1, \ldots, \mathrm{y}_\mathrm{m}) \quad \Leftrightarrow \quad \mathrm{g}_{\mathrm{new}}(\mathrm{x}_1, \ldots, \mathrm{x}_\mathrm{n}) = \mathrm{h}_{\mathrm{new}}(\mathrm{y}_1, \ldots, \mathrm{y}_\mathrm{m})$ *with pairwise distinct variables* $\mathrm{x}_1, \ldots, \mathrm{x}_\mathrm{n}, \mathrm{y}_1, \ldots, \mathrm{y}_\mathrm{m}$. *Let then*

$$\Delta\Theta = \{\mathrm{a}_{\mathrm{g,h}} \mid \mathrm{g}, \mathrm{h} \in \Sigma_{\mathrm{Obs}} \ \ \textit{with the same target sort}\}$$

and let $\mathrm{SP}_2 = \langle \Sigma_1 + \Delta\Sigma, \Theta_1 + \Delta\Theta\rangle$.

Under the hypothesis above, the observational specification $\langle \mathrm{SP}_1, \Sigma_{\mathrm{Obs}}\rangle$ *is "simulated" by the observational specification* $\langle \mathrm{SP}_2, \mathrm{S}_{\mathrm{Obs}} + \Delta\Theta\rangle$ *in the sense that:*

$$\mathrm{Beh}[\langle \mathrm{SP}_2, \mathrm{S}_{\mathrm{Obs}} + \Delta\Theta\rangle]_{|\Sigma_1} = \mathrm{Beh}[\langle \mathrm{SP}_1, \Sigma_{\mathrm{Obs}}\rangle]$$

Proof is given in Appendix B.

The two last propositions demonstrate that observations based on terms can be "simulated" by observations based on operations, with additional observation of some particular atoms (axioms e_t), and that observations based on operations can as well be simulated by observations based on sorts, with additional observation of some particular formulae (axioms $a_{g,h}$).

It should be noted that the additional observable atoms, for the first simulation, as well as the additional observable formulae, for the second one, have a particularly simple form. Thus one could hope to lift proofs from the sort observation level to the term observation level.

Therefore, one could hope that Hennicker's proof method (see [8]), which works mainly for observable sorts, could be used to prove properties expressed with observable terms. However, we want to prevent the reader from such a quick conclusion, which requires further investigation, especially w.r.t. the following points:

1. Hennicker's observational semantics is slightly different from Sannella's and Tarlecki's observational semantics, that we used to establish our simulation results.
2. Hennicker's proof method requires observable preconditions for every conditional axiom of the specification, but in the transformation described in Proposition 4.6, we add axioms ($a_{g,h}$) with non observable preconditions.
3. Even if possible, such translations of proofs would result in rather illegible proofs.

Consequently, the problem of the proof translation remains an open question.

5 Some Limitations of Extension by Observational Equivalence

The observational semantics based on an equivalence on $Alg[\Sigma]$ provides a general framework enabling us to discuss the power of observational techniques. Nevertheless, there are some cases where this observational semantics seems too restrictive. Sometimes, there clearly exists some relevant realizations which are not observationally equivalent to a (usual) model of the specification. This fact is particularly clear when $Alg[SP]$ is empty. For instance, let us consider the following specification

spec : SET-WITH-ENUM
    use : NAT, BOOL, LIST
sort : Set
generated by :
    $\emptyset : \to$ Set
    ins: Nat Set $\to$ Set
operations :
    $\_\in\_$: Nat Set $\to$ Bool
    del : Nat Set $\to$ Set
    enum : Set $\to$ List
axioms :
    $ins(x,ins(x,s)) = ins(x,s)$
    $ins(x,ins(y,s)) = ins(y,ins(x,s))$
    $del(x, \emptyset) = \emptyset$
    $del(x, ins(x, s)) = del(x, s)$
    $x \neq y \Rightarrow del(x, ins(y, s)) = ins(y, del(x, s))$
    $x \in \emptyset = false$

$$\mathsf{x \in ins(x,s) = true}$$
$$\mathsf{x \neq y \Rightarrow x \in ins(y,s) = x \in s}$$
$$\mathsf{enum(\emptyset) = nil}$$
$$\mathsf{enum(ins(x,s)) = cons(x,enum(s))}$$

What we really need for this example is to observe

$$W \ = \ \{x \in s\} \cup \{t \in T_{\mathsf{Sig[LIST]}} \mid t \text{ is of sort } \mathsf{Nat} \text{ or } \mathsf{Bool}\}$$

In other words, we observe membership and some LIST terms but we do not observe those LIST terms where enum occurs.

Obviously, this specification is inconsistent (i.e. $\mathrm{Alg[SP]} = \emptyset$). Consequently the extension by the observational equivalence w.r.t. the set W yields an empty class of observational models. Moreover, for any observation technique α, the specification SET-WITH-ENUM with observations Obs_α has its observational model class empty. Nevertheless, a realization which represents sets by lists, enum being the identity, should clearly be considered as a correct one.

In a semantical framework based on the extension by observational equivalence, the existence of observational models depends on the existence of usual models. Indeed, the extension by observational equivalence is based on the usual satisfaction relation. This leads to a somewhat heterogeneous framework where the observational features are based on the usual ones. In particular the "observational consistency" ($\mathrm{Beh}[\langle \mathrm{SP}, \mathrm{Obs}\rangle] \neq \emptyset$) always coincides with the usual one ($\mathrm{Alg[SP]} \neq \emptyset$). An approach where the satisfaction relation is directly redefined according to observability (extension by relaxing the satisfaction relation) seems more promising. This would allow to give a homogeneous observational definition for all the usual notions depending on the satisfaction relation (such as e.g. consistency).

Note also that this example points out a situation where we want to observe an infinite set of terms.

6 Conclusion

When we want to include observability features into algebraic specifications, two aspects have to be taken into account. First, we have to ensure a good expressive power which for instance gives rise to a usable specification language. Second, we must provide simple proof techniques since this point is crucial to establish software correctness. Clearly, the complexity of proving software correctness increases with the fineness of the observation technique. Consequently, the choice of an observation technique should be a compromise between its fineness and the existence of proof facilities. Therefore we should, as far as possible, choose the lower level of observation with a satisfactory expressive power. From our experiments it seems that this level corresponds to term observation. Terms allow the expression of any composition of operations. Intuitively, a term denotes a "computation" and software specification needs at most to define the computations that we want to observe and those that we do not want to observe. Conversely, there are examples where term observation seems necessary (c.f. SET-WITH-ENUM).

Of course, the choice of even the finest observation technique does not ensure, by itself, a satisfactory expressive power of the observational approach. The specification SET-WITH-ENUM points out some limitations of semantics based on the extension by observational equivalence. For this reason we believe that a promising direction for further investigations is an approach which associates term observation with a semantics based on the extension by relaxing the satisfaction relation.

References

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

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

[3] **Fribourg L.** SLOG, a Logic Programming Language Interpreter Based on Clausal Superposition and Rewriting *International Symposium on Logic Programming, Boston, July 1985.*

[4] **Ganzinger H.** Parameterized Specifications: Parameter Passing and Implementation with Respect to Observability *ACM Transactions on Programming Languages and Systems, Vol 5, No 3, 318-354 (1983)*

[5] **Girratana V., Gimona F., Montanari U.** Observability Concepts in Abstract Data Type Specification *MFCS, Gdańsk 1976, LNCS 45, 576-587*

[6] **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)*

[7] **Hennicker R.** Implementation of Parameterized Observational Specifications, *TapSoft, Barcelona 1989, LNCS 351, vol. 1, 290-305*

[8] **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)*

[9] **Hussmann H.** Unification in Conditional-Equational Theories *Fakultät für Mathematik und Informatik Universität Passau, January 1985 (Internal Report MIP-8502) and short version in Proc. EUROCAL 85 Conf., Linz.*

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

[11] **Meseguer J., Goguen J.A.** Initiality, Induction and Computability *(Nivat M., Reynolds J.C. eds.) Algebraic Methods in Semantics, Cambridge Univ. Press, 459-540 (1985)*

[12] **Moss L.S., Meseguer J., Goguen J.A.** Final Algebras, Cosemicomputable Algebras and Degrees of Unsolvability *(Pitt D.H., Poigné A., Rydeheard D.E. eds.), Category Theory and Computer Science, Edinburgh, September 1987, LNCS 283, 158-181*

[13] **Moss L.S., Thate 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*

[14] **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*

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

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

[19] **Schoett O.** Data Abstraction and the Correctness of Modular Programming *Ph. D. Thesis, Univ. of Edinburgh, 1986*

[20] **Schoett O.** An Observational Subset of First-Order Predicate Logic Cannot Specify the Behaviour of a Counter (Extended Abstract) *STACS, Hamburg 1991, LNCS 480, 499-510*

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

A Proof of the Proposition 4.5

Proposition 4.5 was stated in Section 4 as follows:

Proposition 4.5
Let $\mathrm{SP}_1 = \langle\Sigma_1, \Theta_1\rangle$. *Let* W *be a set of* Σ_1*-terms. For each term* $\mathrm{t} \in \mathrm{W}$, *let* s *be the sort of* t, *and* $\mathrm{x}_1, \ldots, \mathrm{x}_n$ *be the variables occurring in* t *(of sorts* $\mathrm{s}_1, \ldots, \mathrm{s}_n$ *respectively); we introduce a new operation* $\mathrm{f}_t : \mathrm{s}_1 \ldots \mathrm{s}_n \to \mathrm{s}$, *and a new axiom* $\mathrm{e}_t : \mathrm{f}_t(\mathrm{x}_1, \ldots, \mathrm{x}_n) = \mathrm{t}$. *Let then*

$$\begin{aligned} \Delta\Sigma &= \{\mathrm{f}_t \mid \mathrm{t} \in \mathrm{W}\} \\ \Delta\Theta &= \{\mathrm{e}_t \mid \mathrm{t} \in \mathrm{W}\} \\ \textit{and}\quad \mathrm{SP}_2 &= \langle\Sigma_1 + \Delta\Sigma, \Theta_1 + \Delta\Theta\rangle \end{aligned}$$

The observational specification $\langle\mathrm{SP}_1, \mathrm{W}\rangle$ *is "simulated" by the observational specification* $\langle\mathrm{SP}_2, \Delta\Sigma + \Delta\Theta\rangle$ *in the sense that:*

$$\mathrm{Beh}[\langle\mathrm{SP}_2, \Delta\Sigma + \Delta\Theta\rangle]_{|\Sigma_1} = \mathrm{Beh}[\langle\mathrm{SP}_1, \mathrm{W}\rangle]$$

To prove Proposition 4.5 we will use the following lemmas.

Lemma A.1
Let $\Sigma_1 \subseteq \Sigma_2$. *For any* Σ_2*-algebra* A_2 *and any* Σ_1*-formula* φ *we have:*

$$A_{2|\Sigma_1} \models \varphi \quad \textit{iff} \quad A_2 \models \varphi$$

(Well known) □

Lemma A.2
With the notations of Proposition 4.5, *for any* Σ_1*-algebra* B_1 *there exists* $B_2 \in \mathrm{Alg}[\langle\Sigma_1 + \Delta\Sigma, \Delta\Theta\rangle]$ *such that* $B_{2|\Sigma_1} = B_1$.

Proof
Obvious from the definition of $\Delta\Sigma$ *and* $\Delta\Theta$. *Indeed* B_2 *is unique and its carrier is the one of* B_1. □

Lemma A.3
Given SP_1 *and* SP_2 *as defined in Proposition* 4.5, *for any* Σ_1*-algebra* A_1 *there exists* $A_2 \in \mathrm{Alg}[\mathrm{SP}_2]$ *such that* $A_{2|\Sigma_1} = A_1$.

Proof

Follows directly from Lemmas A.2 and A.1. □

Lemma A.4

Given SP_1 *and* SP_2 *as defined in Proposition 4.5, for any model* $A_2 \in \mathrm{Alg}[\mathrm{SP}_2]$ *and any model* $B_2 \in \mathrm{Alg}[\langle \Sigma_1 + \Delta\Sigma, \Delta\Theta \rangle]$*, we have:*

$$A_2 \equiv_{\Delta\Sigma + \Delta\Theta} B_2 \quad \textit{iff} \quad A_2 \equiv_{\Delta\Sigma} B_2$$

Proof

Results from the fact that

$$A_2 \equiv_{\Delta\Sigma + \Delta\Theta} B_2 \quad \textit{iff} \quad A_2 \equiv_{\Delta\Sigma} B_2 \ \wedge \ A_2 \equiv_{\Delta\Theta} B_2$$

The second member of this last conjunction is true since from the hypothesis we have $A_2 \models \Delta\Theta$ *and* $B_2 \models \Delta\Theta$*, and we know that*

$$\forall \Phi \quad (A \models \Phi \ \wedge \ B \models \Phi) \quad \Rightarrow \quad A \equiv_{\Phi} B$$

□

Lemma A.5

With the notations of Proposition 4.5, for any $\mathrm{t} \in \mathrm{W}$ *, any* $\sigma : \mathrm{X} \to \mathrm{T}_{(\Sigma_1 + \Delta\Sigma)(\mathrm{X})}$*, there exists* $\mu : \mathrm{X} \to \mathrm{T}_{\Sigma_1(\mathrm{X})}$ *such that*

$$\mathrm{f_t}(\mathrm{x}_1, \ldots, \mathrm{x_n})\sigma \underset{\Delta\Theta}{=} \mathrm{t}\mu$$

i.e. $\mathrm{f_t}(\mathrm{x}_1, \ldots, \mathrm{x_n})\sigma$ *and* $\mathrm{t}\mu$ *are equal in the theory presented by* $\Delta\Theta$.

Proof

It is obvious from the definition of $\Delta\Sigma$ *and* $\Delta\Theta$ *that for any* $\mathrm{l} \in \mathrm{T}_{(\Sigma_1 + \Delta\Sigma)(\mathrm{X})}$ *there exists* $\mathrm{r} \in \mathrm{T}_{\Sigma_1(\mathrm{X})}$ *such that* $\mathrm{l} \underset{\Delta\Theta}{=} \mathrm{r}$*. In particular, for* $\mathrm{i} = 1, \ldots, \mathrm{n}$ *there exists* $\mathrm{d_i} \in \mathrm{T}_{\Sigma_1(\mathrm{X})}$ *such that* $\mathrm{x_i}\sigma \underset{\Delta\Theta}{=} \mathrm{d_i}$*. Consequently*

$$\mathrm{f_t}(\mathrm{x}_1\sigma, \ldots, \mathrm{x_n}\sigma) \underset{\Delta\Theta}{=} \mathrm{f_t}(\mathrm{d}_1, \ldots, \mathrm{d_n})$$

Therefore we can consider $\mu : \mathrm{X} \to \mathrm{T}_{\Sigma_1(\mathrm{X})}$ *such that* $\mu = \{\mathrm{x_i} \mapsto \mathrm{d_i}\}_{\mathrm{i} \in \{1, \ldots, \mathrm{n}\}}$*. Then*

$$\mathrm{f_t}(\mathrm{x}_1, \ldots, \mathrm{x_n})\sigma \underset{\Delta\Theta}{=} \mathrm{f_t}(\mathrm{x}_1, \ldots, \mathrm{x_n})\mu$$

But since $\mathrm{f_t}(\mathrm{x}_1, \ldots, \mathrm{x_n}) = \mathrm{t}$ *belongs to* $\Delta\Theta$*, we conclude*

$$\mathrm{f_t}(\mathrm{x}_1, \ldots, \mathrm{x_n})\sigma \underset{\Delta\Theta}{=} \mathrm{t}\mu$$

□

Lemma A.6

With the notations of Proposition 4.5, for all $A_2, B_2 \in \mathrm{Alg}[\langle \Sigma_1 + \Delta\Sigma, \Delta\Theta \rangle]$ *the following holds:*

$$A_2 \equiv_{\Delta\Sigma} B_2 \quad \textit{iff} \quad A_2|_{\Sigma_1} \equiv_{\mathrm{W}} B_2|_{\Sigma_1}$$

Proof

- $\Rightarrow$
  Given $A_2, B_2 \in \mathrm{Alg}[\langle\Sigma_1+\Delta\Sigma, \Delta\Theta\rangle]$ *such that* $A_2 \equiv_{\Delta\Sigma} B_2$*; given* $\mathrm{l}, \mathrm{r} \in \mathrm{W}$ *and* $\sigma, \rho : \mathrm{X} \rightarrow \mathrm{T}_{\Sigma_1(\mathrm{X})}$*, we have to prove that*
  $$A_2|_{\Sigma_1} \models \mathrm{l}\sigma = \mathrm{r}\rho \quad \textit{iff} \quad B_2|_{\Sigma_1} \models \mathrm{l}\sigma = \mathrm{r}\rho$$
  Since $\mathrm{f_l}(\mathrm{x}_1, \ldots, \mathrm{x_n}) = \mathrm{l}$ *and* $\mathrm{f_r}(\mathrm{y}_1, \ldots, \mathrm{y_m}) = \mathrm{r}$ *belong to* $\Delta\Theta$ *we have*
  $$A_2 \ (\textit{resp. } B_2) \ \models \ \mathrm{l}\sigma = \mathrm{f_l}(\mathrm{x}_1\sigma, \ldots, \mathrm{x_n}\sigma) \ \wedge \ \mathrm{r}\rho = \mathrm{f_r}(\mathrm{y}_1\rho, \ldots, \mathrm{y_m}\rho)$$
  Hence
  $$\begin{array}{rl} & A_2 \models \mathrm{l}\sigma = \mathrm{r}\rho \quad \textit{iff} \quad A_2 \models \mathrm{f_l}(\mathrm{x}_1\sigma, \ldots, \mathrm{x_n}\sigma) = \mathrm{f_r}(\mathrm{y}_1\rho, \ldots, \mathrm{y_m}\rho) \\ \textit{and} & B_2 \models \mathrm{l}\sigma = \mathrm{r}\rho \quad \textit{iff} \quad B_2 \models \mathrm{f_l}(\mathrm{x}_1\sigma, \ldots, \mathrm{x_n}\sigma) = \mathrm{f_r}(\mathrm{y}_1\rho, \ldots, \mathrm{y_m}\rho) \end{array}$$
  But since $A_2 \equiv_{\Delta\Sigma} B_2$*, we have*
  $$A_2 \models \mathrm{f_l}(\mathrm{x}_1\sigma, \ldots, \mathrm{x_n}\sigma) = \mathrm{f_r}(\mathrm{y}_1\rho, \ldots, \mathrm{y_m}\rho) \quad \textit{iff} \quad B_2 \models \mathrm{f_l}(\mathrm{x}_1\sigma, \ldots, \mathrm{x_n}\sigma) = \mathrm{f_r}(\mathrm{y}_1\rho, \ldots, \mathrm{y_m}\rho)$$
  Hence
  $$A_2 \models \mathrm{l}\sigma = \mathrm{r}\rho \quad \textit{iff} \quad B_2 \models \mathrm{l}\sigma = \mathrm{r}\rho$$
  and from Lemma A.1*, this is equivalent to*
  $$A_2|_{\Sigma_1} \models \mathrm{l}\sigma = \mathrm{r}\rho \quad \textit{iff} \quad B_2|_{\Sigma_1} \models \mathrm{l}\sigma = \mathrm{r}\rho$$

- $\Leftarrow$
  Given $A_2, B_2 \in \mathrm{Alg}[\langle\Sigma_1 + \Delta\Sigma, \Delta\Theta\rangle]$ *such that* $A_2|_{\Sigma_1} \equiv_{\mathrm{W}} B_2|_{\Sigma_1}$*; given* $\mathrm{f_t}(\mathrm{x}_1, \ldots, \mathrm{x_n})\sigma$ *and* $\mathrm{f_u}(\mathrm{y}_1, \ldots, \mathrm{y_m})\rho$ *(with* $\sigma, \rho : \mathrm{X} \rightarrow \mathrm{T}_{(\Sigma_1+\Delta\Sigma)(\mathrm{X})}$ *and* $\mathrm{f_t}, \mathrm{f_u} \in \Delta\Sigma$*) we have to prove that*
  $$A_2 \models \mathrm{f_t}(\mathrm{x}_1, \ldots, \mathrm{x_n})\sigma = \mathrm{f_u}(\mathrm{y}_1, \ldots, \mathrm{y_m})\rho \quad \textit{iff} \quad B_2 \models \mathrm{f_t}(\mathrm{x}_1, \ldots, \mathrm{x_n})\sigma = \mathrm{f_u}(\mathrm{y}_1, \ldots, \mathrm{y_m})\rho$$
  By Lemma A.5 *there exist* $\mu, \nu : \mathrm{X} \rightarrow \mathrm{T}_{\Sigma_1(\mathrm{X})}$ *such that*
  $$\begin{array}{rrcl} & A_2, B_2 & \models & \mathrm{f_t}(\mathrm{x}_1, \ldots, \mathrm{x_n})\sigma = \mathrm{t}\mu \\ \textit{and} & A_2, B_2 & \models & \mathrm{f_u}(\mathrm{y}_1, \ldots, \mathrm{y_m})\rho = \mathrm{u}\nu \end{array}$$
  Thus:
  $$\begin{array}{rl} & A_2 \models \mathrm{f_t}(\mathrm{x}_1, \ldots, \mathrm{x_n})\sigma = \mathrm{f_u}(\mathrm{y}_1, \ldots, \mathrm{y_m})\rho \quad \textit{iff} \\ & A_2 \models \mathrm{t}\mu = \mathrm{u}\nu \quad \textit{iff} \\ (\textit{by Lemma } \mathrm{A.1}) & A_2|_{\Sigma_1} \models \mathrm{t}\mu = \mathrm{u}\nu \quad \textit{iff} \\ (\textit{by hypothesis } A_2|_{\Sigma_1} \equiv_{\mathrm{W}} B_2|_{\Sigma_1}) & B_2|_{\Sigma_1} \models \mathrm{t}\mu = \mathrm{u}\nu \quad \textit{iff} \\ (\textit{by Lemma } \mathrm{A.1}) & B_2 \models \mathrm{t}\mu = \mathrm{u}\nu \quad \textit{iff} \\ & B_2 \models \mathrm{f_t}(\mathrm{x}_1, \ldots, \mathrm{x_n})\sigma = \mathrm{f_u}(\mathrm{y}_1, \ldots, \mathrm{y_m})\rho \end{array}$$

$\square$

Proof of Proposition 4.5

We have to prove
$$\mathrm{Beh}[\langle \mathrm{SP}_2, \Delta\Sigma + \Delta\Theta\rangle]|_{\Sigma_1} = \mathrm{Beh}[\langle \mathrm{SP}_1, \mathrm{W}\rangle]$$
We have:

$$\begin{aligned} &\mathrm{Beh}[\langle \mathrm{SP}_2, \Delta\Sigma + \Delta\Theta\rangle] \overset{\text{(by definition of Beh)}}{=} \\ &= \{B_2 \in \mathrm{Alg}[\Sigma_1 + \Delta\Sigma] \mid \exists A_2 \in \mathrm{Alg}[\mathrm{SP}_2], B_2 \equiv_{\Delta\Sigma+\Delta\Theta} A_2\} \overset{\text{(by Lemma A.4)}}{=} \\ &= \{B_2 \in \mathrm{Alg}[\langle\Sigma_1 + \Delta\Sigma, \Delta\Theta\rangle] \mid \exists A_2 \in \mathrm{Alg}[\mathrm{SP}_2], B_2 \equiv_{\Delta\Sigma} A_2\} \overset{\text{(by Lemma A.6)}}{=} \\ &= \{B_2 \in \mathrm{Alg}[\langle\Sigma_1 + \Delta\Sigma, \Delta\Theta\rangle] \mid \exists A_2 \in \mathrm{Alg}[\mathrm{SP}_2], B_2|_{\Sigma_1} \equiv_{\mathrm{W}} A_2|_{\Sigma_1}\} \end{aligned}$$

Therefore,

$\mathrm{Beh}[\langle \mathrm{SP}_2, \Delta\Sigma + \Delta\Theta\rangle]_{|\Sigma_1} =$

$= \{B_2 \in \mathrm{Alg}[\langle \Sigma_1 + \Delta\Sigma, \Delta\Theta\rangle] \mid \exists A_2 \in \mathrm{Alg}[\mathrm{SP}_2], {B_2}_{|\Sigma_1} \equiv_{\mathrm{W}} {A_2}_{|\Sigma_1}\}_{|\Sigma_1} =$

(by Lemma A.2)

$= \{B_1 \in \mathrm{Alg}[\Sigma_1] \mid \exists A_2 \in \mathrm{Alg}[\mathrm{SP}_2], B_1 \equiv_{\mathrm{W}} {A_2}_{|\Sigma_1}\} =$

(by Lemma A.3)

$= \{B_1 \in \mathrm{Alg}[\Sigma_1] \mid \exists A_1 \in \mathrm{Alg}[\mathrm{SP}_1], B_1 \equiv_{\mathrm{W}} A_1\} =$

(by definition of Beh)

$= \mathrm{Beh}[\langle \mathrm{SP}_1, \mathrm{W}\rangle]$.

□

B Proof of Proposition 4.6

Proposition 4.5 was stated in Section 4 as follows:

Proposition 4.6

Let $\mathrm{SP}_1 = \langle \Sigma_1, \Theta_1\rangle$. *Let* $\Sigma_{\mathrm{Obs}} \subseteq \Sigma_1$ *be a set of observable operations. For each target sort* s *of the observable operations we introduce a new sort* $\mathrm{s_{new}}$. *Let then*

$$\mathrm{S_{Obs}} = \{\mathrm{s_{new}} \mid \exists\ (\mathrm{f} : \mathrm{s_1} \ldots \mathrm{s_n} \to \mathrm{s}) \in \Sigma_{\mathrm{Obs}}\}$$

For each $\mathrm{f} : \mathrm{s_1} \ldots \mathrm{s_n} \to \mathrm{s} \in \Sigma_{\mathrm{Obs}}$ *we introduce a new operation* $\mathrm{f_{new}} : \mathrm{s_1} \ldots \mathrm{s_n} \to \mathrm{s_{new}}$. *Let*

$$\Delta\Sigma = \langle \mathrm{S_{Obs}}, \{\mathrm{f_{new}} \mid \mathrm{f} \in \Sigma_{\mathrm{Obs}}\}\rangle$$

Next, for each $\mathrm{g} : \mathrm{p_1} \ldots \mathrm{p_n} \to \mathrm{s} \in \Sigma_{\mathrm{Obs}}$ *and* $\mathrm{h} : \mathrm{r_1} \ldots \mathrm{r_m} \to \mathrm{s} \in \Sigma_{\mathrm{Obs}}$ *we introduce a new axiom* $\mathrm{a_{g,h}} :\ \mathrm{g}(\mathrm{x_1}, \ldots, \mathrm{x_n}) = \mathrm{h}(\mathrm{y_1}, \ldots, \mathrm{y_m}) \quad \Leftrightarrow \quad \mathrm{g_{new}}(\mathrm{x_1}, \ldots, \mathrm{x_n}) = \mathrm{h_{new}}(\mathrm{y_1}, \ldots, \mathrm{y_m})$ *with pairwise distinct variables* $\mathrm{x_1}, \ldots, \mathrm{x_n}, \mathrm{y_1}, \ldots, \mathrm{y_m}$. *Let then*

$$\Delta\Theta = \{\mathrm{a_{g,h}} \mid \mathrm{g}, \mathrm{h} \in \Sigma_{\mathrm{Obs}} \ \ \textit{with the same target sort}\}$$

and let $\mathrm{SP}_2 = \langle \Sigma_1 + \Delta\Sigma, \Theta_1 + \Delta\Theta\rangle$.

Under the hypothesis above, the observational specification $\langle \mathrm{SP}_1, \Sigma_{\mathrm{Obs}}\rangle$ *is "simulated" by the observational specification* $\langle \mathrm{SP}_2, \mathrm{S_{Obs}} + \Delta\Theta\rangle$ *in the sense that:*

$$\mathrm{Beh}[\langle \mathrm{SP}_2, \mathrm{S_{Obs}} + \Delta\Theta\rangle]_{|\Sigma_1} = \mathrm{Beh}[\langle \mathrm{SP}_1, \Sigma_{\mathrm{Obs}}\rangle]$$

To prove Proposition 4.6 we will use the following lemmas.

Lemma B.1

With the notations of Proposition 4.6, for any Σ_1*-algebra* B_1 *there exists* $B_2 \in \mathrm{Alg}[\langle \Sigma_1 + \Delta\Sigma, \Delta\Theta\rangle]$ *such that* ${B_2}_{|\Sigma_1} = B_1$.

Proof

Let $\mathcal{F}$ *be the free synthesis functor associated with the presentation* $\langle \Delta\Sigma, \Delta\Theta\rangle$ *over* SP_1. *Then:*

$$\mathcal{F}(B_1)_{|\Sigma_1} = B_1$$

because $\Delta\Sigma$ *only contains operations with target in the new sorts (i.e. in* $\mathrm{S_{Obs}}$*) and* $\Delta\Theta$ *only concerns the new sorts. Thus we can take* $B_2 = \mathcal{F}(B_1)$. □

Lemma B.2

Given SP_1 *and* SP_2 *as defined in Proposition* 4.6, *for any* Σ_1*-algebra* A_1 *there exists* $A_2 \in \mathrm{Alg}[\mathrm{SP}_2]$ *such that* $A_{2|_{\Sigma_1}} = A_1$.

Proof

Follows directly from Lemmas B.1 *and* A.1. □

Lemma B.3

Given SP_1 *and* SP_2 *as defined in Proposition* 4.6, *for any model* $A_2 \in \mathrm{Alg}[\mathrm{SP}_2]$ *and any model* $B_2 \in \mathrm{Alg}[\langle \Sigma_1 + \Delta\Sigma, \Delta\Theta \rangle]$, *we have:*

$$A_2 \equiv_{\mathrm{S_{Obs}} + \Delta\Theta} B_2 \quad \textit{iff} \quad A_2 \equiv_{\mathrm{S_{Obs}}} B_2$$

Proof

same as for Lemma A.4 □

Lemma B.4

With the notations of Proposition 4.6, *for all* $A_2, B_2 \in \mathrm{Alg}[\langle \Sigma_1 + \Delta\Sigma, \Delta\Theta \rangle]$ *the following holds:*

$$A_2 \equiv_{\mathrm{S_{Obs}}} B_2 \quad \textit{iff} \quad A_{2|_{\Sigma_1}} \equiv_{\Sigma_{\mathrm{Obs}}} B_{2|_{\Sigma_1}}$$

Proof

Let $A_2, B_2 \in \mathrm{Alg}[\langle \Sigma_1 + \Delta\Sigma, \Delta\Theta \rangle]$. *By definition of "*$\equiv_{\mathrm{S_{Obs}}}$*",* $A_2 \equiv_{\mathrm{S_{Obs}}} B_2$ *if and only if:*

$$\forall\, \mathrm{l}, \mathrm{r} \in (\mathrm{T}_{(\Sigma_1 + \Delta\Sigma)(\mathrm{X})})_{\mathrm{s}}, \quad \mathrm{s} \in \mathrm{S_{Obs}} \quad A_2 \models \mathrm{l} = \mathrm{r} \ \ \textit{iff} \ \ B_2 \models \mathrm{l} = \mathrm{r} \tag{i}$$

Since each proper subterm of l *(resp.* r*) is in* $\mathrm{T}_{\Sigma_1(\mathrm{X})}$ *(because no operation of* $\Sigma_1 + \Delta\Sigma$ *has an observable sort in its domain), the expression* (i) *is equivalent to*

$$\begin{aligned}\forall\, \mathrm{f}, \mathrm{g} \in \Sigma_{\mathrm{Obs}} \ \ \forall\, \sigma, \rho : \mathrm{X} \to \mathrm{T}_{\Sigma_1(\mathrm{X})} & \\ & A_2 \models \mathrm{f_{new}}(\mathrm{x}_1, \ldots \mathrm{x_n})\sigma = \mathrm{g_{new}}(\mathrm{y}_1, \ldots, \mathrm{y_m})\rho \\ \textit{iff} \ \ & B_2 \models \mathrm{f_{new}}(\mathrm{x}_1, \ldots \mathrm{x_n})\sigma = \mathrm{g_{new}}(\mathrm{y}_1, \ldots, \mathrm{y_m})\rho\end{aligned} \tag{ii}$$

where $\mathrm{x}_1, \ldots \mathrm{x_n}, \mathrm{y}_1, \ldots, \mathrm{y_m}$ *are pairwise distinct variables.*
By hypothesis both A_2 *and* B_2 *satisfy the axiom* $\mathrm{a_{f,g}}$. *Hence*

$$\begin{aligned} & A_2 \models \mathrm{f}(\mathrm{x}_1, \ldots \mathrm{x_n})\sigma = \mathrm{g}(\mathrm{y}_1, \ldots, \mathrm{y_m})\rho \ \ \textit{iff} \ \ A_2 \models \mathrm{f_{new}}(\mathrm{x}_1, \ldots \mathrm{x_n})\sigma = \mathrm{g_{new}}(\mathrm{y}_1, \ldots, \mathrm{y_m})\rho \\ \text{and} \ \ & B_2 \models \mathrm{f}(\mathrm{x}_1, \ldots \mathrm{x_n})\sigma = \mathrm{g}(\mathrm{y}_1, \ldots, \mathrm{y_m})\rho \ \ \textit{iff} \ \ B_2 \models \mathrm{f_{new}}(\mathrm{x}_1, \ldots \mathrm{x_n})\sigma = \mathrm{g_{new}}(\mathrm{y}_1, \ldots, \mathrm{y_m})\rho \end{aligned} \tag{iii}$$

From (iii) *we can deduce that* (ii) *is equivalent to*

$$\begin{aligned}\forall\, \mathrm{f}, \mathrm{g} \in \Sigma_{\mathrm{Obs}} \ \ \forall\, \sigma, \rho : \mathrm{X} \to \mathrm{T}_{\Sigma_1(\mathrm{X})} & \\ & A_2 \models \mathrm{f}(\mathrm{x}_1, \ldots \mathrm{x_n})\sigma = \mathrm{g}(\mathrm{y}_1, \ldots, \mathrm{y_m})\rho \\ \textit{iff} \ \ & B_2 \models \mathrm{f}(\mathrm{x}_1, \ldots \mathrm{x_n})\sigma = \mathrm{g}(\mathrm{y}_1, \ldots, \mathrm{y_m})\rho\end{aligned}$$

which by Lemma A.1 *is itself equivalent to*

$$\begin{aligned}\forall\, \mathrm{f}, \mathrm{g} \in \Sigma_{\mathrm{Obs}} \ \ \forall\, \sigma, \rho : \mathrm{X} \to \mathrm{T}_{\Sigma_1(\mathrm{X})} & \\ & A_{2|_{\Sigma_1}} \models \mathrm{f}(\mathrm{x}_1, \ldots \mathrm{x_n})\sigma = \mathrm{g}(\mathrm{y}_1, \ldots, \mathrm{y_m})\rho \\ \textit{iff} \ \ & B_{2|_{\Sigma_1}} \models \mathrm{f}(\mathrm{x}_1, \ldots \mathrm{x_n})\sigma = \mathrm{g}(\mathrm{y}_1, \ldots, \mathrm{y_m})\rho\end{aligned}$$

By definition of "$\equiv_{\Sigma_{\mathrm{Obs}}}$*" the last expression is equivalent to*

$$A_{2|_{\Sigma_1}} \equiv_{\Sigma_{\mathrm{Obs}}} B_{2|_{\Sigma_1}}$$

□

Proof of Proposition 4.6

We have to prove

$$\mathrm{Beh}[\langle \mathrm{SP}_2, \mathrm{S}_{\mathrm{Obs}} + \Delta\Theta \rangle]_{|\Sigma_1} = \mathrm{Beh}[\langle \mathrm{SP}_1, \Sigma_{\mathrm{Obs}} \rangle]$$

We have:

$$\begin{aligned}
&\mathrm{Beh}[\langle \mathrm{SP}_2, \mathrm{S}_{\mathrm{Obs}} + \Delta\Theta \rangle] \ \overset{\text{(by definition of Beh)}}{=} \\
&= \{ B_2 \in \mathrm{Alg}[\Sigma_1 + \Delta\Sigma] \ \mid \ \exists A_2 \in \mathrm{Alg}[\mathrm{SP}_2], B_2 \equiv_{\mathrm{S}_{\mathrm{Obs}}+\Delta\Theta} A_2 \} \overset{\text{(by Lemma B.3)}}{=} \\
&= \{ B_2 \in \mathrm{Alg}[\langle \Sigma_1 + \Delta\Sigma, \Delta\Theta \rangle] \ \mid \ \exists A_2 \in \mathrm{Alg}[\mathrm{SP}_2], B_2 \equiv_{\mathrm{S}_{\mathrm{Obs}}} A_2 \} \overset{\text{(by Lemma B.4)}}{=} \\
&= \{ B_2 \in \mathrm{Alg}[\langle \Sigma_1 + \Delta\Sigma, \Delta\Theta \rangle] \ \mid \ \exists A_2 \in \mathrm{Alg}[\mathrm{SP}_2], {B_2}_{|\Sigma_1} \equiv_{\Sigma_{\mathrm{Obs}}} {A_2}_{|\Sigma_1} \}
\end{aligned}$$

Therefore,

$$\begin{aligned}
&\mathrm{Beh}[\langle \mathrm{SP}_2, \mathrm{S}_{\mathrm{Obs}} + \Delta\Theta \rangle]_{|\Sigma_1} \ = \\
&= \{ B_2 \in \mathrm{Alg}[\langle \Sigma_1 + \Delta\Sigma, \Delta\Theta \rangle] \ \mid \ \exists A_2 \in \mathrm{Alg}[\mathrm{SP}_2], {B_2}_{|\Sigma_1} \equiv_{\Sigma_{\mathrm{Obs}}} {A_2}_{|\Sigma_1} \}_{|\Sigma_1} \overset{\text{(by Lemma B.1)}}{=} \\
&= \{ B_1 \in \mathrm{Alg}[\Sigma_1] \ \mid \ \exists A_2 \in \mathrm{Alg}[\mathrm{SP}_2], B_1 \equiv_{\Sigma_{\mathrm{Obs}}} {A_2}_{|\Sigma_1} \} \overset{\text{(by Lemma B.2)}}{=} \\
&= \{ B_1 \in \mathrm{Alg}[\Sigma_1] \ \mid \ \exists A_1 \in \mathrm{Alg}[\mathrm{SP}_1], B_1 \equiv_{\Sigma_{\mathrm{Obs}}} A_1 \} \overset{\text{(by definition of Beh)}}{=} \\
&= \mathrm{Beh}[\langle \mathrm{SP}_1, \Sigma_{\mathrm{Obs}} \rangle] \ .
\end{aligned}$$

□