ECOLE NORMALE SUPERIEURE

Regular Algebras
A Framework for Observational Specifications with Recursive Definitions

Michel BIDOIT
Andrzej TARLECKI

LIENS - 95 - 12

Département de Mathématiques et Informatique

CNRS URA 1327

Regular Algebras
A Framework for Observational Specifications with Recursive Definitions

Michel BIDOIT
Andrzej TARLECKI*

LIENS - 95 - 12

May 1995

Laboratoire d'Informatique de l'Ecole Normale Supérieure
45 rue d'Ulm 75230 PARIS Cedex 05

Tel : (33)(1) 44 32 00 00
Adresse électronique : bidoit@dmi.ens.fr

*Institute of Informatics
Warsaw University and Institute of Computer Science,
Polish Academy of Sciences, Warsaw, Poland

Regular algebras
A framework for observational specifications with recursive definitions

Michel Bidoit [1] and Andrzej Tarlecki [2]

[1] LIENS, C.N.R.S. U.R.A. 1327 & Ecole Normale Supérieure
45, Rue d'Ulm, F-75230 Paris Cedex 05, France
[2] Institute of Informatics, Warsaw University and
Institute of Computer Science, Polish Academy of Sciences, Warsaw, Poland

Abstract

We present a possible framework for specifications of data types with infinitary data, which can be defined by recursive equations. The basic tool is that, as usual, a recursive definition determines an element given as the least fixed point of the corresponding *recursor*, constructed naturally as the least upper bound of the usual chain of approximations. Somewhat unusually, we limit the prerequisite assumptions about the underlying ordering to the necessary minimum, arriving at the notion of a regular algebra as introduced by Tiuryn (1978, 79). It follows then that the framework of regular algebras can be naturally equipped with the notions permitting behavioural interpretation of specifications.

1 Introduction

Behavioural semantics for specification plays a crucial role in the formalisation of the development process, where a specification need not be implemented exactly but so that the required system *behaviour* is achieved — the idea goes back to [GGM76], [Hoa72]; see e.g. [ST95] for the context in which we view it now. There have been two basic approaches to behavioural equivalence to achieve this effect. One introduces a new notion of a *behavioural satisfaction* of formulae, based on the interpretation of equality as an internal indistinguishability relation in each model defined so that two elements are considered equal if they are indistinguishable to the user of the data type given by the model. The other is based on an external notion of a *behavioural equivalence* of models, where two models are considered equivalent if they cannot be distinguished by any computation the user can perform. For example, see [NO88] for a technical presentation of the former and [ST87] of the latter approach. There have also been attempts to unify the two views [Rei85], recently concluded in [BHW94], where it has been shown that the class of models that behaviourally satisfy a specification coincides with the class of models behaviourally equivalent to a fully abstract model (in the usual sense) of the specification. One goal of this paper is to show how these ideas work in the framework permitting recursive definitions of data.

A well-know framework which facilitates such definitions and has been extensively studied in the literature is that of continuous algebras (as presented e.g. in [GTWW77], [TW86]). Unfortunately, under a closer scrutiny from the point of view of the machinery needed for behavioural semantics, some technicalities of the continuous algebra framework turn out to be rather cumbersome. In particular, we were not quite able to explicate some standard examples (like implementation of streams of sets by streams of some lists) in a convincing way. The technical source of the trouble was the need for limits of all (countable) chains in continuous algebras, which led to the ideal closure construction [Nel81], [BN82] in the process of behavioural quotienting of a continuous (implementation) algebra to obtain a continuous (implemented) algebra. The resulting extra elements can of course enjoy different properties from the ones present in the implementation (even in the presence of the usual continuity requirements), and hence render the idea of implementation via quotienting by an indistinguishability relation intuitively questionable.

Instead of trying to bend our general views to cover this somewhat unintuitive case, we have decided to explore another possibility and check whether ideal closure is in fact really needed. The starting point for these considerations was that we tried to minimize the assumptions under which we can meaningfully deal with recursively defined data in continuous algebras. The key observation here is that limits of all the chains that can be formed in the partially ordered carrier of the algebra are not needed for this: all we need are limits of the chains of subsequent "finitary" approximations of the data defined by recursive equations. Similarly, continuity of operations of the algebras is not needed: the operations need not preserve limits of all the chains, but only limits of such definable chains of approximations.

In this way the ordering relation on the algebra carriers becomes just a technical tool to describe solutions of recursive equations, rather than a central element of the algebra structure to be specified and argued about by means of logical axioms, as is the case in the continuous algebra framework.

In this paper we present some of the resulting technicalities. These will cover formal definitions of basic algebraic concepts as well as some most standard facts, familiar from the standard universal algebra, restated in this framework. We view this paper as a technical note reporting the technical progress made and largely recalling the technical developments presented in [Tiu78], [Tiu79], much more than as an adequate presentation of the framework proposed. For this, more work would be needed, both on the technical side, to complete the algebraic picture we have in mind (see [Tiu78], [Tiu79] for some further technical developments we omit here), and on the more practical side, where examples should be provided to check whether what we propose applies to the situations typically studied.

2 Regular algebras and their homomorphisms

Let S be an arbitrary set (of *sorts*). By an S-sorted set we mean any family $X = \langle X_s \rangle_{s \in S}$ of sets. The usual category of S-sorted sets will be denoted by $\mathbf{Set}^S$. We generalise all the standard set-theoretic notions and notations to S-sorted sets. Moreover, the explicit qualifications by the set S of sorts and by specific sorts $s \in S$ will often be omitted whenever they are clear from the context. For example, we write $x \in X$ meaning $x \in X_s$ if $s \in S$ is clear (or unimportant); for

$R \subseteq X \times Y$ (that is, $R = \langle R_s \subseteq X_s \times Y_s \rangle_{s \in S}$) and $x \in X_s$, $y \in Y_s$, we will write $x\,R\,y$ meaning $x\,R_s\,y$; for $f\colon X \to Y$ and $x \in X$ we will write $f(x)$ meaning $f_s(x)$ for the appropriate $s \in S$; etc.

An *algebraic signature* $\Sigma = \langle S, \Omega \rangle$ consists of a set S (of sorts) and of a family $\Omega = \langle \Omega_{s,w} \rangle_{s \in S, w \in S^*}$ of sets (of operation names). When Σ is clear from the context, we will write $f\colon s_1 \times \ldots \times s_n \to s$ for $s_1, \ldots, s_n, s \in S$ and $f \in \Omega_{s,s_1 \ldots s_n}$.

Let $\Sigma = \langle S, \Omega \rangle$ be an algebraic signature, fixed throughout the rest of the paper.

Definition 2.1

An *ordered* Σ*-algebra* A consists of

- an S-sorted set $|A| \in |\mathbf{Set}^S|$,
- for each sort $s \in S$, a partial order $\leq_s^A \subseteq |A|_s \times |A|_s$ on $|A|_s$,
- for each sort $s \in S$, a distinguished element $\bot_s^A \in |A|_s$,
- for each operation name $f\colon s_1 \times \ldots \times s_n \to s$, a function $f_A\colon |A|_{s_1} \times \ldots \times |A|_{s_n} \to |A|_s$.

□

As usual, we will omit the formally given above sort and algebra decorations (subscripts s and superscripts A) when no confusion is likely.

The above notion of an ordered algebra departs essentially from the more usual definitions known in the literature, see e.g. [Möl85]. All we assume here is that some ordering relation, with a distinguished point, is given on the algebra carriers. This is quite orthogonal to the usual structure of algebraic operations, which are not even assumed here to be monotone w.r.t. the ordering.

Definition 2.2

For any S-sorted set $X \in |\mathbf{Set}^S|$ (of variables), we define the set $T_\Sigma^\mu(X)$ of Σ*-terms* with variables X as the least S-sorted set such that:

- $X \subseteq T_\Sigma^\mu(X)$,
- for $f\colon s_1 \times \ldots \times s_n \to s$ and $t_1 \in T_\Sigma^\mu(X)_{s_1}, \ldots, t_n \in T_\Sigma^\mu(X)_{s_n}$, $f(t_1, \ldots, t_n) \in T_\Sigma^\mu(X)_s$,
- for any $t \in T_\Sigma^\mu(X \cup \{z{:}s\})_s$, where $z{:}s$ is a distinguished variable of sort $s \in S$, $\mu z.t \in T_\Sigma^\mu(X)$.

A term is *algebraic* if it does not contain any subterm of the form $\mu z.t$; the set of all algebraic Σ-terms with variables X will be denoted by $T_\Sigma(X)$.

For each term $t \in T_\Sigma^\mu(X)$ the (finite) set $\mathsf{FV}(t) \subseteq X$ of variables that occur freely in t is defined as usual (z does not occur freely in $\mu z.t$). □

The idea is of course that terms of the form $\mu z.t$ are to denote elements `el` defined recursively by

```
val rec el = t[el]
```

where `t[el]` is t with `el` substituted for all the free occurrences of z. Terms $t \in T^{\mu}_{\Sigma}(X \cup \{z{:}s\})_s$ with indicated "recursion variable" $z{:}s$ will be called *recursors on sort* s (a bit ambiguously, we will also use this name for the function on an algebra carrier such a recursor implicitly denotes).

Note that we do not equip the set of terms $T^{\mu}_{\Sigma}(X)$ with the structure of an ordered algebra: no term is distinguished as $\bot$, no partial order is given, no operations on terms are defined, terms of the form $\mu z.t$ are just formal symbols here, not least fixed points, etc.

Definition 2.3

Given an ordered Σ-algebra A, a term $t \in T^{\mu}_{\Sigma}(X)_s$ and a valuation of variables $v{:}\, X \to |A|$, we define the *value of* t *in* A *under* v, written as $t_{A[v]} \in |A|_s$, by induction on the structure of t as follows:

- for $x \in X$, $x_{A[v]} = v(x)$,
- for $f{:}\, s_1 \times \ldots \times s_n \to s$ and $t_1 \in T^{\mu}_{\Sigma}(X)_{s_1}$, $\ldots$, $t_n \in T^{\mu}_{\Sigma}(X)_{s_n}$, $(f(t_1, \ldots, t_n))_{A[v]}$ is defined if and only if all $(t_1)_{A[v]}$, $\ldots$, $(t_n)_{A[v]}$ are defined and then $(f(t_1, \ldots, t_n))_{A[v]} = f_A((t_1)_{A[v]}, \ldots, (t_n)_{A[v]})$,
- for any $t \in T^{\mu}_{\Sigma}(X \cup \{z{:}s\})_s$, where z is a distinguished variable of the sort $s \in S$, put
  - $t^0_{A[v]}(\bot) = \bot_s$,
  - for $i \geq 0$, $t^{i+1}_{A[v]}(\bot) = t_{A[v_i]}$, where $v_i{:}\, (X \cup \{z{:}s\}) \to |A|$ extends v by $v_i(z) = t^i_{A[v]}(\bot)$.

  (Notation $t^i_{A[v]}(\bot)$, as introduced here, will be used throughout the paper.)

  Now, $(\mu z.t)_{A[v]}$ is defined if
  - $t^i_{A[v]}(\bot)$ are defined for all $i \geq 0$,
  - $t^i_{A[v]}(\bot) \leq_s t^{i+1}_{A[v]}(\bot)$ for all $i \geq 0$, and
  - the least upper bound $\bigsqcup_{i \geq 0} t^i_{A[v]}(\bot)$ w.r.t. $\leq_s$ exists in $|A|_s$.

  Then $(\mu z.t)_{A[v]} = \bigsqcup_{i \geq 0} t^i_{A[v]}(\bot)$.

□

As follows from the above definition, the value of a term in an ordered algebra need not be defined.

It is easy to check that the usual substitution properties for the values of terms hold:

Lemma 2.4

Consider an ordered Σ-algebra A, and a term $t \in T^{\mu}_{\Sigma}(X)$.

- The value of a term depends only on the valuation of its free variables: for any two valuations $v, v'{:}\, X \to |A|$ such that $v(x) = v'(x)$ for all $x \in \mathsf{FV}(t)$, $t_{A[v]}$ is defined if and only if $t_{A[v']}$ is defined and if this is the case then $t_{A[v]} = t_{A[v']}$.
- For any substitution $\theta{:}\, X \to T^{\mu}_{\Sigma}(Y)$ and valuation $v'{:}\, Y \to |A|$ such that for all $x \in X$, $\theta(x)_{A[v']}$ is defined, $t_{A[v]}$ is defined if and only if $\theta(t)_{A[v']}$ is defined and if this is the case then $t_{A[v]} = \theta(t)_{A[v']}$, where $\theta(t) \in T^{\mu}_{\Sigma}(Y)$ is the term resulting from t by substituting all free occurrences of $x \in X$ by $\theta(x)$ (substitution is defined so that unintended clashes of variables are avoided) and $v{:}\, X \to |A|$ is defined by $v(x) = \theta(x)_{A[v']}$.

Proof: Follows by induction on the structure of t. □

One consequence of the above lemma is that the subsequent iterations of a recursor, defined semantically in Definition 2.3, may in fact be redefined syntactically as follows.

Lemma 2.5

Consider an ordered Σ-algebra A and a recursor $t \in T^{\mu}_{\Sigma}(X \cup \{z{:}s\})_s$. Define $t^{(0)} = z$ and for $i \geq 0$, $t^{(i+1)} = \theta_i(t^{(i)})$, where $\theta_i{:}\,(X \cup \{z{:}s\}) \to T^{\mu}_{\Sigma}(X \cup \{z{:}s\})$ extends the identity on X by $\theta_i(z) = t^{(i)}$. Then for any valuation $v{:}\,X \to |A|$, for $i \geq 0$, $t^{i}_{A[v]}(\bot)$ is defined if and only if $t^{(i)}_{A[v_\bot]}$ is defined and if this is the case then $t^{i}_{A[v]}(\bot) = t^{(i)}_{A[v_\bot]}$, where $v_\bot{:}\,(X \cup \{z{:}s\}) \to |A|$ extends v by $v_\bot(z) = \bot_s$.

Proof: Follows by an easy induction on $i \geq 0$ using Lemma 2.4. □

Definition 2.6

An ordered Σ-algebra A is called a *regular Σ-algebra* if it satisfies the following two conditions:

(*completeness condition*): For all terms $t \in T^{\mu}_{\Sigma}(X)$ and valuations $v{:}\,X \to |A|$, the value $t_{A[v]}$ of t in A under v is defined.

(*continuity condition*): For all terms $t \in T^{\mu}_{\Sigma}(X \cup \{y{:}s\})_{s'}$, recursors $q \in T^{\mu}_{\Sigma}(X \cup \{z{:}s\})_s$ and valuation $v{:}\,X \to |A|$,

- $t_{A[v_i]} \leq t_{A[v_{i+1}]}$, for $i \geq 0$, and
- $t_{A[v']} = \bigsqcup_{i \geq 0} t_{A[v_i]}$,

where $v'{:}\,(X \cup \{y{:}s\}) \to |A|$ extends v by $v'(y) = (\mu z.q)_{A[v]}$ and for $i \geq 0$, $v_i{:}\,(X \cup \{y{:}s\}) \to |A|$ extends v by $v_i(y) = q^{i}_{A[v]}(\bot)$.

□

More intuitively, regular algebras permit any recursive definitions of their elements, ensuring that any recursor defined using their operations has a least fixed point given as the least upper bound of the usual chain of approximations. The first requirement of the above definition gives the sufficient completeness condition on the (partially ordered) carrier of the algebra. It is easy to see that for each sort $s \in S$, $\bot_s$ is the least element in $|A|_s$ (since $\mu z.x$ has a value under any valuation of the free variable x). Notice however that not all the chains in $|A|$ need to have least upper bounds. Thus, the carriers of a regular algebra need not form complete posets in the usual sense. The second condition ensures that the operations of the algebra are continuous w.r.t. to the approximation chains involved in the definition of the meaning of such recursively defined data. This implies that the denotation of a recursive term of the form $\mu z.t$ is indeed the least fixed point of the recursor t:

Proposition 2.7

Consider any regular Σ-algebra A, recursor $t \in T^{\mu}_{\Sigma}(X \cup \{z{:}s\})_s$ and valuation $v{:}\,X \to |A|$. Then $t_{A[v']} = (\mu z.t)_{A[v]}$, where $v'{:}\,(X \cup \{z{:}s\}) \to |A|$ extends v by $v'(z) = (\mu z.t)_{A[v]}$. Moreover, if for some $a \in |A|$, $t_{A[v_a]} = a$, where $v_a{:}\,(X \cup \{z{:}s\}) \to |A|$ extends v by $v_a(z) = a$, then $(\mu z.t)_{A[v]} \leq a$.

Proof: The first part follows directly from the continuity condition of Definition 2.6. For the second part, first notice that again from the continuity condition, considering the term $\mu z'.z$, we have $t^1_{A[v]}(\bot) = t_{A[v_\bot]} \leq t_{A[v_a]} = a$, where $v_\bot : (X \cup \{z{:}s\}) \to |A|$ extends v by $v_\bot(z) = \bot = (z)^0_{A[v_a]}(\bot)$, since $v_a(z) = a = (z)^1_{A[v_a]}$. In fact, for any $i > 0$, using the same argument and Lemma 2.5, $t^i_{A[v]}(\bot) = t^{(i)}_{A[v_\bot]} \leq t^{(i)}_{A[v_a]} = a$ (since $t^{(i)}_{A[v_a]} = a$ follows from $t_{A[v_a]} = a$ by an easy induction on $i > 0$ using Lemma 2.4). This directly implies that $(\mu z.t)_{A[v]} = \bigsqcup_{i \geq 0} t^i_{A[v]}(\bot) \leq a$. □

The operations of a regular algebra need not be continuous, nor even monotone, since they in general do not preserve all least upper bounds of chains which may happen to exist in the carriers of A. However, as the proof of the above proposition indicates, the image of $\bot$ under all algebraic operations in A (including those denoted by complex recursive terms) is smaller than the image of any other value under this operation. Therefore, our definition of regular algebra does indeed coincide with the definition of a regular algebra as given in [Tiu78], [Tiu79].

Definition 2.8

Given two regular Σ-algebras A and B, by a regular Σ-homomorphism $h : A \to B$ from A to B we mean any function $h : |A| \to |B|$ such that for all terms $t \in T^\mu_\Sigma(X)$ and valuations $v : X \to |A|$, $h(t_{A[v]}) = t_{B[v;h]}$. □

Again, one can check that regular homomorphisms as defined above coincide with the regular homomorphisms of [Tiu78], [Tiu79].

It follows that regular homomorphisms preserve the distinguished elements and the values of operations, as expected:

Proposition 2.9

Let $h : A \to B$ be a regular Σ-homomorphisms.

- $h(\bot^A) = \bot^B$, and
- for $f : s_1 \times \ldots \times s_n \to s$ and $a_1 \in |A|_{s_1}, \ldots, a_n \in |A|_{s_n}$, $h(f_A(a_1, \ldots, a_n)) = f_B(h(a_1), \ldots, h(a_n))$.
- for $t \in T^\mu_\Sigma(X \cup \{z{:}s\})_s$ and $v : X \to |A|$, for all $i \geq 0$, $h(t^i_{A[v]}(\bot^A)) = t^i_{B[v;h]}(\bot^B)$.

Proof: $\bot^A = (\mu z.z)_A$ and $f_A(a_1, \ldots, a_n) = (f(x_1, \ldots, x_n))_{A[v]}$, where $v(x_i) = a_i$ for $i = 1, \ldots, n$. The last part follows by an easy induction on $i \geq 0$. □

In general, regular homomorphisms need not be continuous or even monotone. They do, however, preserve the limits of approximation chains that may occur in recursive definitions.

It is easy to check that regular homomorphisms are closed under composition and that identities are regular homomorphisms. This yields a category $\mathbf{RAlg}(\Sigma)$ of regular Σ-algebras and their homomorphisms.

Proposition 2.10

Let $h : A \to B$ be a regular Σ-homomorphisms. Then h is an isomorphism (in $\mathbf{RAlg}(\Sigma)$) if and only if it is a bijection.

Proof: The "only if" part is trivial. For the "if" part, assume that the regular homomorphism is bijective. Let $h^{-1}\colon |B| \to |A|$ be the inverse of h. We have to show that $h^{-1}\colon B \to A$ is a regular homomorphism. Consider $t \in T^{\mu}_{\Sigma}(X)$ and $v\colon X \to |B|$. Then $h^{-1}(t_{B[v]}) = h^{-1}(t_{B[v;h^{-1};h]}) = h^{-1}(h(t_{A[v;h^{-1}]})) = t_{A[v;h^{-1}]}$. □

Consequently, in $\mathbf{RAlg}(\Sigma)$ there exist exact isomorphisms (that is, isomorphisms which are identities as functions between carrier sets) that are not identities of $\mathbf{RAlg}(\Sigma)$.

Lemma 2.11

Let $\mathcal{B}$ be a nonempty family of exactly isomorphic regular Σ-algebras. Then an ordered Σ-algebra A given by:

- $|A| = |B|$ for any (and hence all) $B \in \mathcal{B}$,
- $\bot^A = \bot^B$ for any (and hence all) $B \in \mathcal{B}$,
- for each operation name f in Σ, $f_A = f_B$ for any (and hence all) $B \in \mathcal{B}$,
- $\leq^A = \bigcap_{B \in \mathcal{B}} \leq_B$

is a regular Σ-algebra exactly isomorphic to those in $\mathcal{B}$.

Proof: First, we have to show that all recursive terms have values in A. By induction on the structure of a term $t \in T^{\mu}_{\Sigma}(X)$ we show that for all valuations $v\colon X \to |A|$, $t_{A[v]}$ is defined and moreover $t_{A[v]} = t_{B[v]}$ for any (and hence for all) $B \in \mathcal{B}$.

- For variables the thesis is trivial.
- For terms of the form $f(t_1, \ldots, t_n)$, the thesis follows easily by the inductive assumption.
- Consider $q \in T^{\mu}_{\Sigma}(X \cup \{z{:}s\})_s$ and a valuation $v\colon X \to |A|$. Using the inductive assumption, we show that for any (and hence all) $B \in \mathcal{B}$
  - $q^0_{A[v]}(\bot) = \bot^A = \bot^B = q^0_{B[v]}$, and
  - by induction on $i \geq 0$, $q^{i+1}_{A[v]}(\bot) = q_{A[v_i]} = q_{B[v_i]} = q^{i+1}_{B[v]}$, where $v_i\colon (X \cup \{z{:}s\}) \to |A|$ extends v by $v_i(z) = q^i_{A[v]} = q^i_{B[v]}$.

  It follows now that for all $B \in \mathcal{B}$, $q^i_{A[v]}(\bot) \leq^B q^{i+1}_{A[v]}(\bot)$, and so $q^i_{A[v]}(\bot) \leq^A q^{i+1}_{A[v]}(\bot)$. Let now $a = (\mu z.q)_{B[v]}$ for any (hence all) $B \in \mathcal{B}$. Since a is the least upper bound of the chain $\langle q^i_{A[v]}(\bot)\rangle_{i\geq 0}$ w.r.t. the ordering $\leq^B$ for each $B \in \mathcal{B}$, $a = \bigsqcup_{i\geq 0} q^i_{A[v]}(\bot)$ w.r.t. the ordering $\leq^A$, which shows $(\mu z.q)_{A[v]} = (\mu z.q)_{B[v]}$.

Then, we have to show that the continuity condition holds for A. So, consider $t \in T^{\mu}_{\Sigma}(X \cup \{y{:}s\})_{s'}$, $q \in T^{\mu}_{\Sigma}(X \cup \{z{:}s\})_s$ and $v\colon X \to |A|$. Since we have already proved the completeness condition for A, by an easy induction on $i \geq 0$ it follows that $t_{A[v_i]} = t_{B[v_i]}$ for any (hence all) $B \in \mathcal{B}$, where $v_i\colon (X \cup \{y{:}s\}) \to |A|$ extends v by $v(y) = q^i_{A[v]}(\bot) = q^i_{B[v]}(\bot)$. Let now $a = t_{B[v']}$ for any (hence all) $B \in \mathcal{B}$, where $v'\colon (X \cup \{y{:}s\}) \to |A|$ extends v by $v(y) = (\mu z.q)_{B[v]}$. Since $\langle t_{A[v_i]}(\bot)\rangle_{i\geq 0}$ is a chain with the least upper bound a w.r.t. each ordering $\leq^B$, $B \in \mathcal{B}$, $\langle t_{A[v_i]}(\bot)\rangle_{i\geq 0}$ is a chain with the least upper bound a w.r.t. the ordering $\leq^A$, which proves the continuity condition for A.

Finally, we have already shown that for all terms $t \in T^{\mu}_{\Sigma}(X)$ and valuations $v: X \to |A|$, $t_{A[v]} = t_{B[v]}$ for each $B \in \mathcal{B}$, which completes the proof that A is a regular Σ-algebra exactly isomorphic to all the regular algebras in $\mathcal{B}$. □

Corollary 2.12

Let A be a regular Σ-algebra. Then in the class of regular Σ-algebras exactly isomorphic to A there exists a regular Σ-algebra $\mu(A)$ with the smallest ordering relation.

Proof: Follows directly from Lemma 2.11. □

3 Regular subalgebras

Definition 3.1

Given two regular Σ-algebras A and B, we say that B is a regular Σ-subalgebra of A if $|B| \subseteq |A|$ and moreover, for each term $t \in T^{\mu}_{\Sigma}(X)$ and valuation $v: X \to |B|$, $t_{B[v]} = t_{A[v]}$, that is, if the inclusion $\iota: |B| \hookrightarrow |A|$ is in fact a regular Σ-homomorphism $\iota: B \to A$. □

It is easy to see that if B is a regular subalgebra of A then $\bot^B = \bot^A$ and for each operation name f in Σ, f_B is the restriction of f_A to $|B|$. However, this is certainly not the sufficient condition for B to be a regular subalgebra of A.

Example 3.2

Consider a signature Σ_0 with a single sort s and a unary operation name $suc: s \to s$. Let then B be an ordered algebra with the carrier $|B| = \{\bot, b_0, b_1, \ldots, b_\infty\}$, the ordering induced by $\bot \leq^B b_i \leq^B b_\infty$ for $i \geq 0$ and $b_i \leq^B b_j$ for $j \geq i \geq 0$, and the operation suc_B given by $suc_B(\bot) = b_0$, $suc_B(b_i) = b_{i+1}$ for $i \geq 0$, and $suc_B(b_\infty) = b_\infty$. B is a regular Σ_0-algebra, with $(\mu z.suc(z))_B = b_\infty$.

Then, let A be an ordered algebra with the carrier $|A| = |B| \cup \{b'_\infty\}$, the least ordering $\leq^A$ such that $\leq^B \subseteq \leq^A$ and $\bot \leq^A b_i \leq^A b'_\infty \leq^A b_\infty$ for $i \geq 0$, and the operation suc_A that extends suc_B by $suc_A(b'_\infty) = b'_\infty$. Then A is a regular Σ_0-algebra, $|B| \subseteq |A|$, suc_B is a restriction of suc_A, $\leq^B = \leq^A \cap\, |B| \times |B|$, but $(\mu z.suc(z))_A = b'_\infty \neq b_\infty = (\mu z.suc(z))_B$. □

If B is a regular subalgebra of A, the ordering on B need not in general be included in the ordering on A — this is obvious, since a part of the ordering is irrelevant, as Proposition 2.10 indicates. When the minimal ordering as given by Corollary 2.12 is considered, the expected inclusion holds:

$$\leq^{\mu(B)} \subseteq \leq^{\mu(A)} \cap\, |B| \times |B|$$

This follows easily from Lemma 3.4 below. First, let us point out though that, perhaps surprisingly, the above inclusion may be proper.

Example 3.3

Consider a signature Σ_1 with one sort s and a binary operation $f: s \times s \to s$.

Let B be an ordered Σ_1-algebra with the carrier $|B| = \{\bot, b_0, b_1, \ldots\}$ and the trivial ordering (induced by the requirement $\bot \leq^B b_i$ for $i \geq 0$). Let then $f_B(x, \bot) = f_B(\bot, x) = x$ and $f_B(b_i, b_j) = b_{max(i,j)}$ (this does not really matter for the example, as long as some simple continuity requirements are satisfied). Then B is a regular algebra (with no non-trivial recursively defined elements) and $\mu(B) = B$.

Let then A be an ordered Σ_1-algebra with the carrier $|A| = |B| \cup \{a, b_\infty\}$ and the ordering induced by $\leq^B$ and $\bot \leq^A a$, $b_i \leq^A b_j$ for $j \geq i \geq 0$, and $b_i \leq^A b_\infty$ for $i \geq 0$. Moreover, let f_A extends f_B as follows: $f_A(x, \bot) = f_A(\bot, x) = x$, $f_A(a, b_i) = f_A(b_i, a) = b_{i+1}$ for $i \geq 0$, and $f_A(x, b_\infty) = f_A(b_\infty, x) = b_\infty$. Then A is a regular algebra, with $b_\infty = (\mu z.f(x, z))_{A[\{x \mapsto a\}]}$, and here $\mu(A) = A$.

Finally, B is a regular Σ-subalgebra of A, $\leq^{\mu(B)} \subseteq \leq^{\mu(A)} \cap |B| \times |B|$, but clearly $\leq^{\mu(B)} \neq \leq^{\mu(A)} \cap |B| \times |B|$. □

We will see, however, that if B is a regular Σ-subalgebra of A then up to an exact isomorphism, the ordering on B is (may be chosen to be) the restriction of the ordering on A to the carrier $|B|$.

Lemma 3.4

Let A be a regular Σ-algebra, and let $K \subset |A|$ be a subset of its carrier that is closed under the values of terms in A, that is such that for all terms $t \in T^\mu_\Sigma(X)$ and valuations $v: X \to K \subseteq |A|$, $t_{A[v]} \in K$.

Then an ordered Σ-algebra B given by

- $|B| = K$,
- $\bot^B = \bot^A$,
- f_B is the restriction of f_A to K, for each operation name f in Σ,
- $\leq^B = \leq^A \cap K \times K$,

is a regular Σ-subalgebra of A.

Proof: We have to show that for each term $t \in T^\mu_\Sigma(X)$ and valuation $v: X \to K$, $t_{B[v]} = t_{A[v]}$ (and so in particular $t_{B[v]}$ is defined). This follows by an easy induction on the structure of t, by the assumption that $t_{A[v]} \in K$. Then, the continuity condition for B follows easily from the continuity condition for A. □

Lemma 3.5

Let A be a regular Σ-algebra and $K \subseteq |A|$. Then the set $\langle K \rangle_A = \{t_{A[v]} \mid t \in T^\mu_\Sigma(X), v: X \to K\}$ is closed under the values of terms in A. Moreover, $\langle K \rangle_A$ is the least subset of $|A|$ which has this property and includes K.

Proof: Obviously, whenever a subset of $|A|$ is closed under values of terms in A and includes K, it includes $\langle K \rangle_A$ as well.

Consider now a term $t \in T^\mu_\Sigma(X)$ and a valuation $v: X \to \langle K \rangle_A$. By definition, for each $x \in X$ there exists a set Y_x, term $t^x \in T^\mu_\Sigma(Y_x)$ and valuation $v_x: Y_x \to K$ such that $v(x) = t^x_{A[v_x]}$. We can assume that for $x \neq x'$, $Y_x \cap Y_{x'} = \emptyset$. Put now $Y = \biguplus_{x \in X} Y_x$ and $\bar{v} = (\biguplus_{x \in X} v_x): Y \to K$. Let $\theta: X \to T^\mu_\Sigma(Y)$ be the substitution given by $\theta(x) = t^x$ for $x \in X$. Then, by Lemma 2.4 $t_{A[\bar{v}]} = \theta(t)_{A[\bar{v}]} \in \langle K \rangle_A$, which proves that indeed $\langle K \rangle_A$ is closed under the values of terms in A and completes the proof of the lemma. □

We will say that $\langle K \rangle_A$ is the *regular Σ-subalgebra of A generated by K*. If $|\langle K \rangle_A| = |A|$ then we say that A *is generated by K*.

Theorem 3.6

Let A be a regular Σ-algebra. Up to exact isomorphism, regular Σ-subalgebras of A are given by all subsets of $|A|$ closed under values of terms in A and only by such subsets. Moreover, for any set $K \subset |A|$ there exists the least regular Σ-subalgebra $\langle K \rangle_A$ of A that (has the carrier that) includes K.

Proof: The fact that the carriers of regular subalgebras of A are closed under the values of terms in A follows directly from definition. Then Lemma 3.4 shows that every subset of $|A|$ closed under the values of terms in A is the carrier of a regular subalgebra of A. Moreover, it is easy to check that any two regular subalgebras of A with the same carrier are exactly isomorphic. Finally, for any set $K \subseteq |A|$, Lemma 3.5 gives the least (carrier of a) regular subalgebra of A which contains K. □

Another consequence of the characterisation of regular subalgebras is that the image and coimage of a regular subalgebra under a regular homomorphism is a regular subalgebra:

Corollary 3.7

Let $h: A \to B$ be a regular Σ-homomorphism, and let C be a regular Σ-subalgebra of A. Then $h(|C|) = \{h(a) \mid a \in |C|\}$ is (the carrier of) a regular Σ-subalgebra of B.

Proof: Consider $t \in T^{\mu}_{\Sigma}(X)$ and $v: X \to h(|C|)$. Let $\tilde{v}: X \to |C|$ be such that $\tilde{v}; h = v$. Then $t_{A[v]} = t_{A[\tilde{v};h]} = h(t_{B[\tilde{v}]}) = h(t_{C[\tilde{v}]}) \in h(|C|)$ since $t_{C[\tilde{v}]} \in |C|$. □

Corollary 3.8

Let $h: A \to B$ be a regular Σ-homomorphism, and let C be a regular Σ-subalgebra of B. Then $h^{-1}(|C|) = \{a \in |A| \mid h(a) \in |C|\}$ is (the carrier of) a regular Σ-subalgebra of A.

Proof: Consider $t \in T^{\mu}_{\Sigma}(X)$ and $v: X \to h^{-1}(|C|)$. Then $h(t_{A[v]}) = t_{B[v;h]} = t_{C[v;h]}$ since $v; h: X \to |C|$ and C is a regular subalgebra of B. Hence, $h(t_{A[v]}) \in |C|$, and so $t_{A[v]} \in h^{-1}(|C|)$. The result then follows from Lemma 3.5. □

Finally, it may be interesting to notice that all regular subalgebras are *full* in the following sense:

Proposition 3.9

If B is a regular Σ-subalgebra of A and $h: C \to A$ is a regular Σ-homomorphism such that $h: |C| \to |B|$, then $h: C \to B$ is a regular Σ-homomorphism as well.

Proof: We have to check that h, given as a map from $|C|$ to $|B|$, preserves the values of terms. Let $t \in T^{\mu}_{\Sigma}(X)$, $v: X \to |C|$. Then $h(t_{C[v]}) = t_{A[v;h]} = t_{B[v;h]}$, which completes the proof. □

4 Regular congruences and quotients

By a *kernel* of an S-sorted function $f: X \to Y$ we mean an S-sorted (equivalence) relation $\mathsf{ker}(f) \subseteq X \times X$ given by $\mathsf{ker}(f) = \{\langle x, x' \rangle \mid f(x) = f(x')\}$.

Definition 4.1

Given a regular Σ-algebra A, by a *regular congruence* on A we mean the kernel of any regular Σ-homomorphism $h: A \to B$. □

To give a more explicit characterisation of regular congruences, we need one more technical concept:

Definition 4.2

By a *pre-congruence* on a regular Σ-algebra A we mean a preorder $\sqsubseteq \subseteq |A| \times |A|$ (that is, $\sqsubseteq$ is a transitive, reflexive, but not necessarily anti-symmetric relation) such that the following conditions hold:

- For all recursors $t \in T^{\mu}_{\Sigma}(X \cup \{z{:}s\})_s$ and valuations $v{:}\, X \to |A|$, $\langle t^i_{A[v]}(\bot)\rangle_{i\geq 0}$ is a chain w.r.t. $\sqsubseteq$ with the least upper bound $(\mu z.t)_{A[v]}$, that is:
  - $t^i_{A[v]}(\bot) \sqsubseteq t^{i+1}_{A[v]}(\bot)$, for $i \geq 0$,
  - $t^i_{A[v]}(\bot) \sqsubseteq (\mu z.t)_{A[v]}$, for $i \geq 0$,
  - for all $a \in |A|$, if $t^i_{A[v]}(\bot) \sqsubseteq a$ for $i \geq 0$, then $(\mu z.t)_{A[v]} \sqsubseteq a$.
- For all $t \in T^{\mu}_{\Sigma}(X \cup \{y{:}s\})_{s'}$, $q \in T^{\mu}_{\Sigma}(X \cup \{z{:}s\})_s$ and $v{:}\, X \to |A|$, $\langle t_{A[v_i]}\rangle_{i\geq 0}$ forms a chain w.r.t. $\sqsubseteq$ with the least upper bound $t_{A[v']}$, where for $i \geq 0$, $v_i{:}\,(X \cup \{y{:}s\}) \to |A|$ extends v by $v_i(y) = q^i_{A[v]}(\bot)$ and $v'{:}\,(X \cup \{y{:}s\}) \to |A|$ extends v by $v'(y) = (\mu z.q)_{A[v]}$, that is
  - $t_{A[v_i]} \sqsubseteq t_{A[v_{i+1}]}$ for $i \geq 0$,
  - $t_{A[v_i]} \sqsubseteq t_{A[v']}$ for $i \geq 0$,
  - for all $a \in |A|$, if $t_{A[v_i]} \sqsubseteq a$ for $i \geq 0$ then $t_{A[v']} \sqsubseteq a$,
- The equivalence generated by $\sqsubseteq$ is preserved by the operations: for all $f{:}\, s_1 \times \ldots \times s_n \to s$ and $a_1, b_1 \in |A|_{s_1}$, $\ldots$, $a_n, b_n \in |A|_{s_n}$ such that $a_1 \sqsubseteq b_1$ and $b_1 \sqsubseteq a_1$, $\ldots$, $a_n \sqsubseteq b_n$ and $b_n \sqsubseteq a_n$, we also have $f_A(a_1, \ldots, a_n) \sqsubseteq f_A(b_1, \ldots, b_n)$ and $f_A(b_1, \ldots, b_n) \sqsubseteq f_A(a_1, \ldots, a_n)$.

□

Lemma 4.3

The family of pre-congruences on a regular Σ-algebra A forms a complete lattice, with greatest lower bounds given by set-theoretic intersection.

Proof: First notice that the total relation on $|A|$ is a pre-congruence on A. Then, to complete the proof it is enough to check that the intersection of any non-empty family of pre-congruences on A is a pre-congruence on A as well — which is rather obvious since all the requirements imposed on pre-congruences are "implicational". □

Lemma 4.4

Let $\sqsubseteq \subseteq |A| \times |A|$ be a pre-congruence on a regular Σ-algebra A, and let $\approx = \sqsubseteq \cap \sqsubseteq^{-1}$ be the equivalence relation induced by the preordering $\sqsubseteq$.

An ordered Σ-algebra $B = A/\sqsubseteq$ given by

- $|B| = |A|/\approx$,
- $\bot^B = [\bot^A]_{\approx}$,
- for all $a, a' \in |A|$, $[a]_{\approx} \leq^B [a']_{\approx} \iff a \sqsubseteq a'$,

- for $f: s_1 \times \ldots \times s_n \to s$ and $a_1 \in |A|_{s_1}, \ldots, a_n \in |A|_{s_n}$, $f_B([a_1]_\approx, \ldots, [a_n]_\approx) = [f_A(a_1, \ldots, a_n)]_\approx$

is a regular Σ-algebra.

Moreover, the natural map $a \mapsto [a]_\approx$, $a \in |A|$, is a regular Σ-homomorphism from A to B.

Proof: The properties of pre-congruences ensure that $\approx$ is indeed an equivalence relation, that $\leq^B$ is well-defined (i.e., the definition of $[a]_\approx \leq^B [a']_\approx$ does not depend on the choice of the representants of the equivalence classes) and is an ordering relation on $|B|$, and that the operations are well-defined functions on $|B|$. Thus, B as defined above is indeed an ordered Σ-algebra.

To show the completeness condition of Definition 2.6, consider $t \in T^\mu_\Sigma(X)$ and $\bar{v}: X \to |B|$ where for $x \in X$, $\bar{v}(x) = [v(x)]_\approx$ for some $v: X \to |A|$. By induction on the structure of t we show that $t_{B[\bar{v}]} = [t_{A[v]}]_\approx$ and so in particular $t_{B[\bar{v}]}$ is defined.

- For variables the thesis is trivial.
- For terms of the form $f(t_1, \ldots, t_n)$, the thesis follows easily by the inductive assumption.
- Consider a term t of the form $\mu z.q$, where $q \in T^\mu_\Sigma(X \cup \{z{:}s\})_s$. Using the inductive assumption, by easy induction on $i \geq 0$ we can show that $q^i_{B[\bar{v}]}(\bot) = [q^i_{A[v]}(\bot)]_\approx$. Then $\langle q^i_{B[\bar{v}]}(\bot)\rangle_{i\geq 0}$ form a chain w.r.t. $\leq^B$ with the least upper bound $[(\mu z.q)_{A[v]}]_\approx$:
  - for $i \geq 0$, $q^i_{B[\bar{v}]}(\bot) \leq^B q^{i+1}_{B[\bar{v}]}(\bot)$, since $q^i_{A[v]}(\bot) \sqsubseteq q^{i+1}_{A[v]}(\bot)$ (by the definition of a pre-congruence),
  - for $i \geq 0$, $q^i_{B[\bar{v}]}(\bot) \leq^B [(\mu z.q)_{A[v]}]_\approx$, since $q^i_{A[v]}(\bot) \sqsubseteq (\mu z.q)_{A[v]}$ (by the definition of a pre-congruence),
  - for any $[a]_\approx \in |B|$, $a \in |A|$, if for all $i \geq 0$, $q^i_{B[\bar{v}]}(\bot) \leq^B [a]_\approx$ then for all $i \geq 0$, $q^i_{A[v]}(\bot) \sqsubseteq a$, and so by the definition of a pre-congruence, $(\mu z.q)_{A[v]} \sqsubseteq a$, which yields $[(\mu z.q)_{A[v]}]_\approx \leq^B [a]_\approx$.

  This shows that indeed $(\mu z.q)_{B[\bar{v}]}$ is defined and $(\mu z.q)_{B[\bar{v}]} = [(\mu z.q)_{A[v]}]_\approx$, which completes the proof of the completeness condition for B.

To show the continuity condition, consider $t \in T^\mu_\Sigma(X \cup \{y{:}s\})_{s'}$, $q \in T^\mu_\Sigma(X \cup \{z{:}s\})_s$, $\bar{v}: X \to |B|$ such that for $x \in X$, $\bar{v}(x) = [v(x)]_\approx$ for $v: X \to |A|$. By the above proof of the completeness condition for B, we have that for $i \geq 0$, $q^i_{B[\bar{v}]}(\bot) = [q^i_{A[v]}(\bot)]_\approx$, $t_{B[\bar{v}_i]} = [t_{A[v_i]}]_\approx$, where $\bar{v}_i: (X \cup \{y{:}s\}) \to |B|$ extends $\bar{v}$ by $\bar{v}_i(y) = q^i_{B[\bar{v}]}(\bot)$ and $v_i: (X \cup \{y{:}s\}) \to |A|$ extends v by $v_i(y) = q^i_{A[v]}(\bot)$. Moreover, $t_{B[\bar{v}']} = [t_{A[v']}]_\approx$, where $\bar{v}': (X \cup \{y{:}s\}) \to |B|$ extends $\bar{v}$ by $\bar{v}'(y) = (\mu z.q)_{B[\bar{v}]}$ and $v': (X \cup \{y{:}s\}) \to |A|$ extends v by $v'(y) = (\mu z.q)_{A[v]}$. This is enough to show that $\langle t_{B[\bar{v}_i]}\rangle_{i\geq 0}$ forms a chain w.r.t. $\leq^B$ with the least upper bound $t_{B[\bar{v}']}$:

- for $i \geq 0$, $t_{B[\bar{v}_i]} \leq^B t_{B[\bar{v}_{i+1}]}$, since $t_{A[v_i]} \sqsubseteq t_{A[v_{i+1}]}$ by the definition of a pre-congruence,
- for $i \geq 0$, $t_{B[\bar{v}_i]} \leq^B t_{B[\bar{v}']}$, since $t_{A[v_i]} \sqsubseteq t_{A[v']}$ by the definition of a pre-congruence,
- for any $[a]_\approx \in |B|$, $a \in |A|$, if for all $i \geq 0$, $t_{B[\bar{v}_i]} \leq^B [a]_\approx$ then for all $i \geq 0$, $t_{A[v_i]} \sqsubseteq a$, hence by the definition of a pre-congruence, $t_{A[v']} \sqsubseteq a$ and so $t_{B[\bar{v}']} \leq^B [a]_\approx$.

This completes the proof of the continuity condition for B, and thus of the lemma as well. $\Box$

In the following, given a regular Σ-algebra A and a pre-congruence $\sqsubseteq$ on A, we will refer to the regular Σ-algebra $A/\sqsubseteq$ as the *quotient* of A by $\sqsubseteq$.

Theorem 4.5

A relation $\approx \subseteq |A| \times |A|$ is a regular congruence on a regular Σ-algebra A if and only if $\approx = \sqsubseteq \cap \sqsubseteq^{-1}$ for some pre-congruence $\sqsubseteq \subseteq |A| \times |A|$ on A.

Proof: For the "only if" part, consider any regular Σ-homomorphism $h: A \to B$. Define now a relation $\sqsubseteq \subseteq |A| \times |A|$ by

$$a \sqsubseteq a' \quad \Longleftrightarrow \quad h(a) \leq^B h(a').$$

It is easy to see that $\sqsubseteq$ is a preorder relation and that $\mathsf{ker}(h) = \sqsubseteq \cap \sqsubseteq^{-1}$. We still have to show that $\sqsubseteq$ is a pre-congruence on A.

- Consider $t \in T^{\mu}_{\Sigma}(X \cup \{z{:}s\})_s$ and $v: X \to |A|$. By Proposition 2.9, for $i \geq 0$, $h(t^i_{A[v]}(\bot)) = t^i_{B[v;h]}(\bot)$. Then clearly:
  - for $i \geq 0$, $t^i_{A[v]}(\bot) \sqsubseteq t^{i+1}_{A[v]}(\bot)$, since $t^i_{B[v;h]}(\bot) \leq^B t^{i+1}_{B[v;h]}(\bot)$,
  - for $i \geq 0$, $t^i_{A[v]}(\bot) \sqsubseteq (\mu z.t)_{A[v]}$, since $t^i_{B[v;h]}(\bot) \leq^B (\mu z.t)_{B[v;h]} = h((\mu z.t)_{A[v]})$,
  - for $a \in |A|$, if for all $i \geq 0$, $t^i_{A[v]}(\bot) \sqsubseteq a$ then for all $i \geq 0$, $t^i_{B[v;h]}(\bot) \leq^B h(a)$. Therefore $h(\mu z.t_{A[v]}) = (\mu z.t)_{B[v;h]} \leq^B h(a)$, which proves $(\mu z.t)_{A[v]} \sqsubseteq a$.
- Consider $t \in T^{\mu}_{\Sigma}(X \cup \{y{:}s\})_{s'}$, $q \in T^{\mu}_{\Sigma}(X \cup \{z{:}s\})$ and $v: X \to |A|$. Then for $i \geq 0$, $h(q^i_{A[v]}(\bot)) = q^i_{B[v;h]}(\bot)$, and so for $v_i: (X \cup \{y{:}s\}) \to |A|$ that extends v by $v_i(y) = q^i_{A[v]}(\bot)$, $v_i; h: (X \cup \{y{:}s\}) \to |B|$ extends $v; h$ by $(v_i; h)(y) = q^i_{B[v;h]}(\bot)$. Similarly, for $v': (X \cup \{y{:}s\}) \to |A|$ that extends v by $v'(y) = (\mu z.q)_{A[v]}$, $v'; h: (X \cup \{y{:}s\}) \to |B|$ extends $v; h$ by $(v'; h)(y) = (\mu z.q)_{B[v;h]}$. Given this:
  - for $i \geq 0$, $t_{A[v_i]} \sqsubseteq t_{A[v_{i+1}]}$, since $t_{B[v_i;h]} \leq^B t_{B[v_{i+1};h]}$,
  - for $i \geq 0$, $t_{A[v_i]} \sqsubseteq t_{A[v']}$, since $t_{B[v_i;h]} \leq^B t_{B[v';h]}$,
  - for $a \in |A|$, if for all $i \geq 0$, $t_{A[v_i]}(\bot) \sqsubseteq a$ then for all $i \geq 0$, $t_{B[v_i;h]}(\bot) \leq^B h(a)$. Therefore $h(t_{A[v']}) = t_{B[v';h]} \leq^B h(a)$, which proves $t_{A[v']} \sqsubseteq a$.
- Finally, for all $f: s_1 \times \ldots \times s_n \to s$ and $a_1, a'_1 \in |A|_{s_1}$, $\ldots$, $a_n, a'_n \in |A|_{s_n}$ such that $a_1 \sqsubseteq a'_1$ and $a'_1 \sqsubseteq a_1$, $\ldots$, $a_n \sqsubseteq a'_n$ and $a'_n \sqsubseteq a_n$, that is $h(a_1) = h(a'_1)$, $\ldots$, $h(a_n) = h(a'_n)$, we have $h(f_A(a_1, \ldots, a_n)) = f_B(h(a_1), \ldots, h(a_n)) = f_B(h(a'_1), \ldots, h(a'_n)) = h(f_A(a'_1, \ldots, a'_n))$, which proves that $f_A(a_1, \ldots, a_n) \sqsubseteq f_A(a'_1, \ldots, a'_n)$ and $f_A(a'_1, \ldots, a'_n) \sqsubseteq f_A(a_1, \ldots, a_n)$.

This completes the proof of the "only if" part of the theorem.

For the "if" part, consider a pre-congruence $\sqsubseteq \subseteq |A| \times |A|$ and let $\approx = \sqsubseteq \cap \sqsubseteq^{-1}$. Then $\approx = \mathsf{ker}(h)$, where $h: A \to A/\sqsubseteq$ is the natural regular Σ-homomorphism from A to its quotient by $\sqsubseteq$ (as constructed in Lemma 4.4) given by $h(a) = [a]_{\approx}$, for $a \in |A|$. □

Corollary 4.6

Let $\approx$ be a regular congruence on a regular Σ-algebra A. Then for any term $t \in T^{\mu}_{\Sigma}(X)$ and valuations $v_1, v_2: X \to |A|$ such that for all $x \in X$, $v_1(x) \approx v_2(x)$, $t_{A[v_1]} \approx t_{A[v_2]}$.

Proof: Let $\approx = \sqsubseteq \cap \sqsubseteq^{-1}$ for some pre-congruence $\sqsubseteq$ on A. Let then $\bar{v}: X \to |A/\sqsubseteq|$ be given by $\bar{v}(x) = [v_1(x)]_{\approx} = [v_2(x)]_{\approx}$. Then, by Lemma 4.4, $[t_{A[v_1]}]_{\approx} = t_{A/\sqsubseteq[\bar{v}]} = [t_{A[v_2]}]_{\approx}$, which completes the proof. □

Corollary 4.7

Let A be a regular Σ-algebra. For any relation $R \subseteq |A| \times |A|$ there exists the smallest regular congruence $\approx$ on A such that $R \subseteq \approx$.

Proof: By Lemma 4.3 there exists the smallest pre-congruence $\sqsubseteq$ on A such that $R \cup R^{-1} \subseteq \sqsubseteq$. Then $\approx = \sqsubseteq \cap \sqsubseteq^{-1}$ is the smallest congruence on A which contains R. □

Theorem 4.8

Let A be a regular Σ-algebra, and $R \subseteq |A| \times |A|$. Let then $\approx$ be the least congruence on A that contains R, and let $\sqsubseteq$ be any pre-congruence on A such that $\approx = \sqsubseteq \cap \sqsubseteq^{-1}$. Then $A/\sqsubseteq$ is a categorical quotient of A by R in the following sense: for any regular Σ-homomorphism $h: A \to C$ such that $R \subseteq \mathsf{ker}(h)$ there exists a (unique) regular Σ-homomorphism $g: A/\sqsubseteq \to C$ such that for all $a \in |A|$, $h(a) = g([a]_{\approx})$.

Proof: Under the assumptions of the theorem, the requirement that for all $a \in |A|$, $h(a) = g([a]_{\approx})$ determines unambiguously a function $g: |A/\sqsubseteq| \to |C|$. We have to check that it preserves the values of terms.

Consider $t \in T^{\mu}_{\Sigma}(X)$ and $\bar{v}: X \to |A/\sqsubseteq|$ where for $x \in X$, $\bar{v}(x) = [v(x)]_{\approx}$ for some $v: X \to |A|$. By Lemma 4.4, $t_{A/\sqsubseteq[\bar{v}]} = [t_{A[v]}]_{\approx}$. Therefore, $g(t_{A/\sqsubseteq[\bar{v}]}) = h(t_{A[v]}) = t_{C[v;h]} = t_{C[\bar{v};g]}$, which completes the proof. □

Corollary 4.9

Let $\sqsubseteq_1$ and $\sqsubseteq_2$ be two regular pre-congruences on a regular Σ-algebra A such that $\sqsubseteq_1 \cap \sqsubseteq_1{}^{-1} = \sqsubseteq_2 \cap \sqsubseteq_2{}^{-1}$. Then $A/\sqsubseteq_1$ and $A/\sqsubseteq_2$ are exactly isomorphic.

Proof: By the construction in Lemma 4.4, $|A/\sqsubseteq_1| = |A/\sqsubseteq_2|$. Moreover, by Theorem 4.8, the identity function is a regular Σ-homomorphism from $A/\sqsubseteq_1$ to $A/\sqsubseteq_2$ and from $A/\sqsubseteq_2$ to $A/\sqsubseteq_1$. □

By this corollary, we can define up to an isomorphism a quotient of a regular algebra by a regular congruence as the quotient of the algebra by any pre-congruence that determines the regular congruence:

Definition 4.10

Given a regular Σ-algebra A and a regular congruence $\approx$ on A, the *quotient of A by $\approx$*, written $A/\approx$, is defined up to an (exact) isomorphism as $A/\sqsubseteq$, where $\sqsubseteq$ is any pre-congruence on A such that $\approx = \sqsubseteq \cap \sqsubseteq^{-1}$. □

5 Observational indistinguishability and behavioural equivalence of regular algebras

In this section we will present a definition of an observational indistinguishability relation between elements of a regular algebra. We will show that this indistinguishability relation is a congruence and characterise explicitly the behavioural equivalence relation between regular algebras "factorized" [BHW94] by the observational indistinguishability congruence. In this way we will provide a basis for the further, rather standard now, development of behavioural semantics for specification in its two well-known versions: via observational satisfaction of formulae and via behavioural closure of the usual model class of a specification.

As usual, let $\Sigma = \langle S, \Omega \rangle$ be an algebraic signature fixed for the rest of this section. Moreover, let $OBS \subseteq S$ be a distinguished set of *observable sorts*.

For any S-sorted set X, by X_{OBS} we will denote an S-sorted set such that

$$(X_{OBS})_s = \begin{cases} X_s & \text{for } s \in OBS \\ \emptyset & \text{for } s \notin OBS \end{cases}$$

Following this notation, X_{OBS} will denote any S-sorted set (of variables) such that $(X_{OBS})_s = \emptyset$ for all $s \notin OBS$.

By an *observational context* on sort $s \in S$ we mean any term $\gamma \in T^{\mu}_{\Sigma}(X_{OBS} \cup \{x{:}s\})_o$, where $o \in OBS$ and $x \notin X_{OBS}$ is a special new variable.

Given any regular Σ-algebra A, observational context $\gamma \in T^{\mu}_{\Sigma}(X_{OBS} \cup \{x{:}s\})_o$, valuation $\alpha{:}\, X_{OBS} \to |A|$ and value $a \in |A|_s$ we will write $\gamma_{A[\alpha]}(a)$ for $\gamma_{A[\alpha_a]}$, where $\alpha_a{:}\,(X_{OBS} \cup \{x{:}s\}) \to |A|$ extends α by $\alpha_a(x) = a$.

Definition 5.1

Let A be a regular Σ-algebra generated by $|A|_{OBS}$. An *observational indistinguishability relation* $\sim^{OBS}_A$ on A is defined so that for $s \in S$, for $a, b \in |A|_s$, $a \sim^{OBS}_A b$ if for all observable contexts $\gamma \in T^{\mu}_{\Sigma}(X_{OBS} \cup \{x{:}s\})$ and valuations $\alpha{:}\, X \to |A|$, $\gamma_{A[\alpha]}(a) = \gamma_{A[\alpha]}(b)$. □

Theorem 5.2

Let A be a regular Σ-algebra generated by $|A|_{OBS}$. Then the observational indistinguishability relation $\sim^{OBS}_A$ is the largest regular congruence on A that is the identity on the carriers of observable sorts.

Proof: First, notice that since for any observable sort $o \in OBS$, $x \in T^{\mu}_{\Sigma}(\{x{:}o\})_o$ is an observable context, $(\sim^{OBS}_A)_o$ is indeed the identity on $|A|_o$.

To prove that $\sim^{OBS}_A$ as defined above is a congruence on A, define a relation $\sqsubseteq^{OBS}_A \subseteq |A| \times |A|$ so that for $s \in S$ and $a, b \in |A|_s$, $a \sqsubseteq^{OBS}_A b$ if for all observable contexts $\gamma \in T^{\mu}_{\Sigma}(X_{OBS} \cup \{x{:}s\})$ and valuations $\alpha{:}\, X \to |A|$, $\gamma_{A[\alpha]}(a) \leq^A \gamma_{A[\alpha]}(b)$. Since clearly $\sim^{OBS}_A = \sqsubseteq^{OBS}_A \cap (\sqsubseteq^{OBS}_A)^{-1}$, and $\sqsubseteq^{OBS}_A$ is a pre-order, it is enough to prove now that $\sqsubseteq^{OBS}_A$ is a pre-congruence on A:

- Consider $t \in T^{\mu}_{\Sigma}(Y \cup \{y{:}s\})_s$ and $v{:}\, Y \to |A|$. We have to show that $\langle t^i_{A[v]}(\bot)\rangle_{i \geq 0}$ is a chain w.r.t. $\sqsubseteq^{OBS}_A$ with the least upper bound $(\mu y.t)_{A[v]}$. Consider any $\gamma \in T^{\mu}_{\Sigma}(X_{OBS} \cup \{x{:}s\})$ and valuation $\alpha{:}\, X_{OBS} \to |A|$. We can assume $(X_{OBS} \cup \{x{:}s\}) \cap (Y \cup \{y{:}s\}) = \emptyset$, hence $t \in T^{\mu}_{\Sigma}(Z \cup \{y{:}s\})_s$ and $\gamma \in T^{\mu}_{\Sigma}(Z \cup \{x{:}s\})$ where $Z = X_{OBS} \uplus Y$. Then, by the continuity condition of Definition 2.6, $\langle \gamma_{A[\alpha \uplus v]}(t^i_{A[\alpha \uplus v]}(\bot))\rangle_{i \geq 0}$ forms a chain w.r.t. $\leq^A$ with the least upper bound $\gamma_{A[\alpha \uplus v]}((\mu y.t)_{A[\alpha \uplus v]})$. Therefore, relying on the fact that a value of a term depends on the valuation of its free variables only (Lemma 2.4):

  - for $i \geq 0$, $t^i_{A[v]}(\bot) \sqsubseteq^{OBS}_A t^{i+1}_{A[v]}(\bot)$, since for all γ and α as above,

    $$\gamma_{A[\alpha]}(t^i_{A[v]}(\bot)) = \gamma_{A[\alpha \uplus v]}(t^i_{A[\alpha \uplus v]}(\bot)) \leq^A \gamma_{A[\alpha \uplus v]}(t^{i+1}_{A[\alpha \uplus v]}(\bot)) = \gamma_{A[\alpha]}(t^{i+1}_{A[v]}(\bot)),$$

  - for $i \geq 0$, $t^i_{A[v]}(\bot) \sqsubseteq^{OBS}_A (\mu y.t)_{A[v]}$, since for all γ and α as above,

    $$\gamma_{A[\alpha]}(t^i_{A[v]}(\bot)) = \gamma_{A[\alpha \uplus v]}(t^i_{A[\alpha \uplus v]}(\bot)) \leq^A \gamma_{A[\alpha \uplus v]}((\mu y.t)_{A[\alpha \uplus v]}) = \gamma_{A[\alpha]}((\mu y.t)_{A[v]}),$$

– for $a \in |A|$, if for all $i \geq 0$, $t^i_{A[v]}(\bot) \sqsubseteq^{OBS}_A a$ then for all γ and α as above, for all $i \geq 0$, $\gamma_{A[\alpha \uplus v]}(t^i_{A[\alpha \uplus v]}(\bot)) \leq^A \gamma_{A[\alpha \uplus v]}(a)$, and so $\gamma_{A[\alpha]}((\mu y.t)_{A[v]}) = \gamma_{A[\alpha \uplus v]}((\mu y.t)_{A[\alpha \uplus v]}) \leq^A \gamma_{A[\alpha \uplus v]}(a) = \gamma_{A[\alpha]}(a)$, which proves that $(\mu y.t)_{A[v]} \sqsubseteq^{OBS}_A a$.

- Consider $t \in T^\mu_\Sigma(Y \cup \{y{:}s\})_{s'}$, $q \in T^\mu_\Sigma(Y \cup \{z{:}s\})_s$ and $v{:}\, X \to |A|$. We have to show that $\langle t_{A[v_i]} \rangle_{i \geq 0}$, where $v_i{:}\,(Y \cup \{y{:}s\}) \to |A|$ extends v by $v_i(y) = q^i_{A[v]}(\bot)$, forms a chain w.r.t. $\sqsubseteq^{OBS}_A$ with a least upper bound $t_{A[v']}$, where $v'{:}\,(Y \cup \{y{:}s\}) \to |A|$ extends v by $v'(y) = (\mu z.q)_{A[v]}$. Consider any $\gamma \in T^\mu_\Sigma(X_{OBS} \cup \{x{:}s'\})$ and valuation $\alpha{:}\, X_{OBS} \to |A|$. We can assume $(X_{OBS} \cup \{x{:}s'\}) \cap (Y \cup \{y, z{:}s\}) = \emptyset$, hence $t \in T^\mu_\Sigma(Z \cup \{y{:}s\})_{s'}$, $q \in T^\mu_\Sigma(Z \cup \{z{:}s\})_s$ and $\gamma \in T^\mu_\Sigma(Z \cup \{x{:}s'\})$ where $Z = X_{OBS} \uplus Y$. Let then $\gamma[t/x] \in T^\mu_\Sigma(Z \cup \{y{:}s\})$ be the result of substituting the term t for all free occurrences of x in γ. By the continuity condition of Definition 2.6, $\langle \gamma[t/x]_{A[\alpha \uplus v_i]} \rangle_{i \geq 0}$ forms a chain w.r.t. $\leq^A$ with the least upper bound $\gamma[t/x]_{A[\alpha \uplus v']}$. Therefore, using Lemma 2.4 a few times:

  – for $i \geq 0$, $t_{A[v_i]} \sqsubseteq^{OBS}_A t_{A[v_{i+1}]}$, since for all γ and α as above,

$$\gamma_{A[\alpha]}(t_{A[v_i]}) = (\gamma[t/x])_{A[\alpha \uplus v_i]} \leq^A (\gamma[t/x])_{A[\alpha \uplus v_{i+1}]} = \gamma_{A[\alpha]}(t_{A[v_{i+1}]}),$$

  – for $i \geq 0$, $t_{A[v_i]} \sqsubseteq^{OBS}_A t_{A[v']}$, since for all γ and α as above,

$$\gamma_{A[\alpha]}(t_{A[v_i]}) = (\gamma[t/x])_{A[\alpha \uplus v_i]} \leq^A (\gamma[t/x])_{A[\alpha \uplus v']} = \gamma_{A[\alpha]}(t_{A[v']}),$$

  – for $a \in |A|$, if for all $i \geq 0$, $t_{A[v_i]} \sqsubseteq^{OBS}_A a$ then for all γ and α as above, for all $i \geq 0$,

$$(\gamma[t/x])_{A[\alpha \uplus v_i]} = \gamma_{A[\alpha]}(t_{A[v_i]}) \leq^A \gamma_{A[\alpha]}(a),$$

    and so

$$\gamma_{A[\alpha]}(t_{A[v']}) = (\gamma[t/x])_{A[\alpha \uplus v']} \leq^A \gamma_{A[\alpha]}(a),$$

    which proves that $t_{A[v']} \sqsubseteq^{OBS}_A a$.

- Consider $f{:}\, s_1 \times \ldots \times s_n \to s$ and $a_1, b_1 \in |A|_{s_1}$, $\ldots$, $a_n, b_n \in |A|_{s_n}$ such that $a_1 \sim^{OBS}_A b_1$, $\ldots$, $a_n \sim^{OBS}_A b_n$. We have to show that $f_A(a_1, \ldots, a_n) \sim^{OBS}_A f_A(b_1, \ldots, b_n)$, that is for all $\gamma \in T^\mu_\Sigma(X_{OBS} \cup \{x{:}s\})_o$ for $o \in OBS$ and $\alpha{:}\, X_{OBS} \to |A|$, $\gamma_{A[\alpha]}(f_A(a_1, \ldots, a_n)) = \gamma_{A[\alpha]}(f_A(b_1, \ldots, b_n))$.

  Since A is generated by $|A|_{OBS}$, by Lemma 3.5, there exist terms $t_1 \in T^\mu_\Sigma(Y^1_{OBS})$, $q_1 \in T^\mu_\Sigma(Z^1_{OBS})$, $\ldots$, $t_n \in T^\mu_\Sigma(Y^n_{OBS})$, $q_n \in T^\mu_\Sigma(Z^n_{OBS})$ and valuations $\alpha_1{:}\, Y^1_{OBS} \to |A|_{OBS}$, $\beta_1{:}\, Z^1_{OBS} \to |A|_{OBS}$, $\ldots$, $\alpha_n{:}\, Y^n_{OBS} \to |A|_{OBS}$, $\beta_n{:}\, Z^n_{OBS} \to |A|_{OBS}$, such that $a_1 = (t_1)_{A[\alpha_1]}$, $b_1 = (q_1)_{A[\beta_1]}$, $\ldots$, $a_n = (t_n)_{A[\alpha_n]}$, $b_n = (q_n)_{A[\beta_n]}$. Moreover, we can assume that the sets of variables involved are mutually disjoint.

  For $1 \leq j \leq n$ we have then:

$$\begin{aligned}
&\gamma_{A[\alpha]}(f_A(b_1, \ldots, b_{j-1}, a_j, a_{j+1}, \ldots, a_n)) \\
&\qquad = (\gamma[f(q_1, \ldots, q_{j-1}, x_j, t_{j+1} \ldots, t_n)/x])_{A[\alpha \uplus \beta_1 \uplus \ldots \uplus \beta_{j-1} \uplus \alpha_{j+1} \ldots \uplus \alpha_n]}(a_j) \\
&\qquad = (\gamma[f(q_1, \ldots, q_{j-1}, x_j, t_{j+1} \ldots, t_n)/x])_{A[\alpha \uplus \beta_1 \uplus \ldots \uplus \beta_{j-1} \uplus \alpha_{j+1} \ldots \uplus \alpha_n]}(b_j) \\
&\qquad = \gamma_{A[\alpha]}(f_A(b_1, \ldots, b_{j-1}, b_j, a_{j+1}, \ldots, a_n)).
\end{aligned}$$

  Thus, it follows by easy induction that $\gamma_{A[\alpha]}(f_A(a_1, \ldots, a_n)) = \gamma_{A[\alpha]}(f_A(b_1, \ldots, b_n))$.

The above proves that indeed $\sqsubseteq_A^{OBS}$ is a pre-congruence on A, and so $\sim_A^{OBS}$ is a regular congruence on A, which moreover is the identity on the observable sorts.

To show that $\sim_A^{OBS}$ is the largest regular congruence with this property, consider any regular congruence $\approx$ on A and assume that for $o \in OBS$, $\approx_o$ is the identity on $|A|_o$. Let $a, b \in |A|_s$ be such that $a \approx b$. Consider an observable context $\gamma \in T_\Sigma^\mu(X_{OBS} \cup \{x{:}s\})$ and valuation $\alpha{:}X_{OBS} \to |A|_{OBS}$. By Corollary 4.6, $\gamma_{A[\alpha]}(a) \approx \gamma_{A[\alpha]}(b)$, but since the result sort of γ is observable, this means that $\gamma_{A[\alpha]}(a) = \gamma_{A[\alpha]}(b)$. Hence, $a \sim_A^{OBS} b$, which proves $\approx \subseteq \sim_A^{OBS}$ and completes the proof of the theorem. □

Definition 5.3

Let A and B be regular Σ-algebras. We say that A and B are *behaviourally equivalent* if the quotients $A_O/{\sim_{A_O}^{OBS}}$ and $B_O/{\sim_{B_O}^{OBS}}$ are isomorphic, where $A_O = \langle |A|_{OBS} \rangle_A$ and $B_O = \langle |B|_{OBS} \rangle_B$ are the regular Σ-subalgebras of A and B, respectively, generated by the carriers of observable sorts. □

The following theorem gives a more explicit, expected characterisation of the behavioural equivalence of regular algebras.

Theorem 5.4

Two regular Σ-algebras A and B are behaviourally equivalent if and only if there exist a set X_{OBS} (of variables of observable sorts only) and surjective valuations $v_A{:}X_{OBS} \to |A|_{OBS}$ and $v_B{:}X_{OBS} \to |B|_{OBS}$ such that for all terms $t, t' \in T_\Sigma^\mu(X_{OBS})_o$ with $o \in OBS$,

$$t_{A[v_A]} = t'_{A[v_A]} \iff t_{B[v_B]} = t'_{B[v_B]}.$$

Proof: Let $A_O = \langle |A|_{OBS} \rangle_A$ and $B_O = \langle |B|_{OBS} \rangle_B$ be the regular Σ-subalgebras of A and B, respectively, generated by the carriers of observable sorts.

For the proof of the "only if" part of the theorem, consider an isomorphism $i{:}A_O/{\sim_{A_O}^{OBS}} \to B_O/{\sim_{B_O}^{OBS}}$. Recall that by Proposition 2.10, i is bijective. Let X_{OBS} be any set of the same cardinality as $|A|_{OBS}$ (and $|B|_{OBS}$) and let $v_A{:}X_{OBS} \to |A|_{OBS}$ and $v_B{:}X_{OBS} \to |B|_{OBS}$ be bijections such that $\tilde{v}_A; i = \tilde{v}_B$, where $\tilde{v}_A{:}X_{OBS} \to |A_O/{\sim_{A_O}^{OBS}}|$ and $\tilde{v}_B{:}X_{OBS} \to |B_O/{\sim_{B_O}^{OBS}}|$ are valuations defined by $\tilde{v}_A = [v_A(x)]_{\sim_{A_O}^{OBS}} = \{v_A(x)\}$ and $\tilde{v}_B = [v_B(x)]_{\sim_{B_O}^{OBS}} = \{v_B(x)\}$ for all $x \in X_{OBS}$. Then for any term $t \in T_\Sigma^\mu(X_{OBS})$,

$$[t_{B[v_B]}]_{\sim_{B_O}^{OBS}} = t_{B_O/{\sim_{B_O}^{OBS}}[\tilde{v}_B]} = i(t_{A_O/{\sim_{A_O}^{OBS}}[\tilde{v}_A]}) = i([t_{A[v_A]}]_{\sim_{A_O}^{OBS}}).$$

Therefore, since i is bijective, for any two terms $t, t' \in T_\Sigma^\mu(X_{OBS})_s$,

$$t_{A[v_A]} \sim_{A_O}^{OBS} t'_{A[v_A]} \iff t_{B[v_B]} \sim_{B_O}^{OBS} t'_{B[v_B]},$$

Thus, for $s \in OBS$, in which case $(\sim_{A_O}^{OBS})_s$ is the identity on $|A|_s$ and $(\sim_{B_O}^{OBS})_s$ is the identity on $|B|_s$,

$$t_{A[v_A]} = t'_{A[v_A]} \iff t_{B[v_B]} = t'_{B[v_B]},$$

which completes the proof on the "only if" part.

For the proof of the "if" part, first note that since all variables $x \in X_{OBS}$ are terms of observable sorts, under the assumptions for this part of the theorem, $\mathsf{ker}(v_A) = \mathsf{ker}(v_B)$. Hence, for any set Y_{OBS} of variables of observable sorts we can define a bijection $to_B(\_\_)$ between valuations of Y_{OBS} into $|A|_{OBS}$ and valuations of Y_{OBS} into $|B|_{OBS}$ as follows: for $v\colon Y_{OBS} \to |A|_{OBS}$, $to_B(v)\colon Y_{OBS} \to |B|_{OBS}$ is given by $to_B(v)(y) = v_B(x)$ for $y \in Y_{OBS}$ and any $x \in X_{OBS}$ such that $v_A(x) = v(y)$. Then, for any terms $t, t' \in T^{\mu}_{\Sigma}(Y_{OBS})_o$, $o \in OBS$, and valuation $v\colon Y_{OBS} \to |A|_{OBS}$, by the assumptions for the "if" part of the theorem

$$t_{A[v]} = t'_{A[v]} \iff t_{B[to_B(v)]} = t'_{B[to_B(v)]},$$

since by Lemma 2.4 we have $t_{A[v]} = (\theta_v(t))_{A[v_A]}$, $t'_{A[v]} = (\theta_v(t'))_{A[v_A]}$, $t_{B[to_B(v)]} = (\theta_v(t))_{B[v_B]}$, and $t'_{B[to_B(v)]} = (\theta_v(t'))_{B[v_B]}$, where $\theta_v(y) = x$ for $y \in Y_{OBS}$ and any $x \in X_{OBS}$ such that $v_A(x) = v(y)$.

Consider now two arbitrary terms $q \in T^{\mu}_{\Sigma}(Y_{OBS})_s$ and $q' \in T^{\mu}_{\Sigma}(Y'_{OBS})_s$ of the same sort $s \in S$, and two valuations $v\colon Y_{OBS} \to |A|_{OBS}$ and $v'\colon Y'_{OBS} \to |A|_{OBS}$. Assume that $Y_{OBS} \cap Y'_{OBS} = \emptyset$. For any observable context $\gamma \in T^{\mu}_{\Sigma}(Z_{OBS} \cup \{z{:}s\})$, with $Z_{OBS} \cup \{z{:}s\}$ disjoint from Y_{OBS} and Y'_{OBS}, and valuation $\alpha\colon Z_{OBS} \to |A|_{OBS}$, we have then:

$$\gamma_{A[\alpha]}(q_{A[v]}) = \gamma_{A[\alpha]}(q'_{A[v']}) \iff \gamma_{B[to_B(\alpha)]}(q_{B[to_B(v)]}) = \gamma_{B[to_B(\alpha)]}(q'_{B[to_B(v')]})$$

since by Lemma 2.4 again,

$$\begin{array}{rcl} \gamma_{A[\alpha]}(q_{A[v]}) = (\gamma[q/z])_{A[\alpha \uplus v \uplus v']} & & \gamma_{B[to_B(\alpha)]}(q_{B[to_B(v)]}) = (\gamma[q/z])_{B[to_B(\alpha \uplus v \uplus v')]} \\ \gamma_{A[\alpha]}(q'_{A[v']}) = (\gamma[q'/z])_{A[\alpha \uplus v \uplus v']} & \text{and} & \gamma_{B[to_B(\alpha)]}(q'_{B[to_B(v')]}) = (\gamma[q'/z])_{B[to_B(\alpha \uplus v \uplus v')]}. \end{array}$$

Since $to_B(\_\_)$ is a bijection between valuations, this shows that

$$q_{A[v]} \sim^{OBS}_{A_O} q'_{A[v']} \iff q_{B[to_B(v)]} \sim^{OBS}_{B_O} q'_{B[to_B(v')]}.$$

Define now a map $i\colon |A_O/{\sim}^{OBS}_{A_O}| \to |B_O/{\sim}^{OBS}_{B_O}|$ by $i([q_{A[v]}]_{\sim^{OBS}_{A_O}}) = [q_{B[to_B(v)]}]_{\sim^{OBS}_{B_O}}$. By Lemma 3.5, since A_O is generated by $|A|_{OBS}$, i is defined on all equivalence classes in $|A_O/{\sim}^{OBS}_{A_O}|$ and the above argument shows that its definition does not depend on the choice of representants for the equivalence classes. Moreover, again by the above argument, i is injective, and by Lemma 3.5, since B_O is generated by $|B|_{OBS}$ and $to_B(\_\_)$ is a bijection between the sets of valuations, i is surjective as well.

It remains to be proved that i as defined above is indeed a regular Σ-homomorphism $i\colon A_O/{\sim}^{OBS}_{A_O} \to B_O/{\sim}^{OBS}_{B_O}$, that is, that i preserves values of terms. For this, consider any term $q \in T^{\mu}_{\Sigma}(Z)$ and valuation $\tilde{v}\colon Z \to |A_O/{\sim}^{OBS}_{A_O}|$. Let then $v\colon Z \to |A|$ be such that $\tilde{v}(z) = [v(z)]_{\sim^{OBS}_{A_O}}$ for all $z \in Z$. Moreover, by Lemma 3.5, for all $z \in Z$ there exist a term $q^z \in T^{\mu}_{\Sigma}(Z^z_{OBS})$ and a valuation $\alpha^z\colon Z^z_{OBS} \to |A|_{OBS}$ such that $v(z) = q^z_{A[\alpha^z]}$. Define now $v'\colon Z \to |B|$ by $v'(z) = q^z_{B[to_B(\alpha^z)]}$. We can assume that the sets Z^z_{OBS}, $z \in Z$, are mutually disjoint. Define $\theta(z) = q^z$ and $\alpha = \biguplus_{z \in Z} \alpha^z$. We have then, by Lemmas 2.4 and 4.4:

$$\begin{array}{rcl} i(q_{A_O/{\sim}^{OBS}_{A_O}[\tilde{v}]}) & = & i([q_{A[v]}]_{\sim^{OBS}_{A_O}}) = i([\theta(q)_{A[\alpha]}]_{\sim^{OBS}_{A_O}}) = [\theta(q)_{B[to_B(\alpha)]}]_{\sim^{OBS}_{B_O}} = [q_{B[v']}]_{\sim^{OBS}_{B_O}} \\ & = & q_{B_O/{\sim}^{OBS}_{B_O}[\tilde{v};i]} \end{array}$$

where the last identity follows by the homomorphism property of the natural quotient map (Lemma 4.4) since for $z \in Z$ we have

$$i(\tilde{v}(z)) = i([v(z)]_{\sim^{OBS}_{A_O}}) = i([q^z_{A[\alpha^z]}]_{\sim^{OBS}_{A_O}}) = [q^z_{B[to_B(\alpha^z)]}]_{\sim^{OBS}_{B_O}} = [v'(z)]_{\sim^{OBS}_{B_O}}.$$

This shows that indeed $i: A_O/\sim^{OBS}_{A_O} \to B_O/\sim^{OBS}_{B_O}$ is a regular isomorphism, and thus completes the proof of the theorem. □

6 Final remarks and further work

In this paper we have re-introduced the framework of regular algebras, which we want to propose as an algebraic framework for specification of algebras with infinitary data defined by recursive equations. Following [Tiu78], [Tiu79], we have introduced the basic concept of a regular algebra, the related notions of regular homomorphism, subalgebra, congruence and quotient, and presented some expected relationships between these notions (only some of those can be found in [Tiu78], [Tiu79]). In particular we have defined the natural notion of an observational indistinguishability of elements in regular algebra, proved that it is a regular congruence, and shown that it factorizes the expected natural notion of behavioural equivalence between regular algebras. Of course, this is but a preliminary proposal, and much work remains to be done.

First, we have not introduced in this report any formal notion of a logical formula and satisfaction: for equations this is trivial, and so is an extension to first-order logic. It would be much less trivial to try to develop some proof calculus for the equational logic, even admitting infinitary rules which seem to be necessary here to handle infinitary data.

Then, all these definitions should be put together to define an institution of equational logic for regular algebras: we do not expect any trouble here either, with the reduct functors and translation of sentences along algebraic signature morphisms defined in the standard way; the satisfaction condition should follow as usual.

In [Tiu79] the existence of initial (and more generally, free) regular algebras is proved. This should be generalised to the existence of left adjoints to all reduct functors induced by signature morphisms, and the institution of equations in regular algebras should be proved to admit initial models. Again, we expect no troubles here. One consequence of the existence of free regular algebras is the Birkhoff-style characterisation of equationally definable classes of regular algebras given in [Tiu79].

Corollary 3.7 shows that all dense epimorphisms in $\mathbf{RAlg}(\Sigma)$ are surjective (a regular homomorphism is dense if the least full subobject of the target algebra that contains the image of the source algebra is the whole target algebra). It is an interesting open question whether all epimorphisms in $\mathbf{RAlg}(\Sigma)$ are dense (i.e., in this framework, surjective). This is known not to be the case for continuous algebras, and perhaps the well-known example due to Lehman and Pasztor [LP82] can be adapted to the framework of regular algebras as well.

Section 5 gives the preliminaries for the study of observational satisfaction and behavioural equivalence in regular algebras. We expect this can be done along the general lines we try to develop for an arbitrary (concrete) institution. But a lot of work specific for regular algebras would be needed here as well. Some (infinitary) proof system in the style of context induction or finitary proof techniques could perhaps be developed following the pattern known for the standard algebraic framework.

Finally, there is a lot of polishing to be done on the proofs already reported here. For example, many of the proofs have a similar character and one would hope that there should be a way to simplify them by extracting the intuitively common induction scheme. Indeed, some

proofs of elementary facts in [Tiu78], [Tiu79] seem simpler than those given here (Lemma 2.5 as used in the proof of Proposition 2.7 may be crucial in this context).

However, even before all this technical and mathematical analysis is attempted, it is necessary to make sure that the proposed framework is indeed useful. Some typical examples of the use of continuous algebras (like in specifications based on streams) should be checked to be meaningful in this framework (we can see no reason why not). It is important to make sure that the resulting observational satisfaction implicit in the developments in Section 5 applies in such specific examples. Is it really the case that a regular algebra with an observational quotient (i.e., the quotient by the observational indistinguishability congruence) satisfying the specification is intuitively an admissible realisation of this specification? And vice versa, do admissible realisations of a specification have quotients which satisfy the axioms in the standard way (at least to the same extent as in the standard algebraic case)?

References

[BN82] Banaschewski, B., Nelson, E. Completions of partially ordered sets. *SIAM J. on Computing* 11(1982), 521–528.

[BHW94] Bidoit, M., Hennicker, R., Wirsing, M. Behavioural and abstractor specifications. *Proc. European Symposium on Programming*, ESOP'94, Edinburgh 1994, LNCS 788, 105–119, Springer-Verlag 1994; full version to appear in *Science of Computer Programming*.

[GGM76] Giarratana, V., Gimona, F., Montanari, U. Observability concepts in abstract data type specification. *Proc. 5th Intl. Symp. Mathematical Foundations of Computer Science*, Gdańsk 1976, LNCS 45, 576–587, Springer-Verlag 1976.

[GTWW77] Goguen, J.A., Thatcher, J.W., Wagner, E.G. Initial algebra semantics and continuous algebras. *Journal of the ACM* 24(1977), 68–95.

[Hoa72] Hoare, C.A.R. Proofs of correctness of data representations. *Acta Informatica* 1(1972), 271–281.

[LP82] Lehman, D.J., Pasztor, A. Epis need not be dense. *Theoretical Computer Science* 17(1982), 151–161.

[Möl85] Möller, B. On the algebraic specification of infinite objects: ordered and continuous algebraic types. *Acta Informatica* 22(1985), 537–578.

[Nel81] Nelson, E. Free Z-continuous algebras. *Proc. Workshop on Continuous Lattices*, Lecture Notes Math. 871, 315–334, Springer-Verlag 1981.

[NO88] Nivela, P., Orejas, F. Initial behaviour semantics for algebraic specifications. *Recent Trends in Data Type Specification, Selected Papers from the 5th Workshop on Specification of Abstract Data Types*, Gullane 1987, LNCS 332, 184–207, Springer-Verlag 1988.

[Rei85] Reichel, H. Behavioural validity of conditional equations in abstract datat types. *Proc. Vienna Conference on Contributions to General Algebra*, 301–324, Treubner-Verlag 1985.

[ST87] Sannella, D., Tarlecki, A. On observational equivalence and algebraic specification. *J. Computer and System Sciences* 34(1987), 150–178.

[ST95] Sannella, D., Tarlecki, A. Model–theoretic foundations for formal program development: basic concepts and motivation. Technical report, February 1995; an earlier short version: Toward formal development of programs from algebraic specifications: model-theoretic foundations. *Proc. Intl. Colloq. on Automata, Languages and Programming*, ICALP'92, Vienna 1992, LNCS 623, 656–671, Springer-Verlag 1992.

[TW86] Tarlecki, A., Wirsing, M. Continuous abstract data types. *Fundamenta Informaticae* 9(1986), 95–126.

[Tiu78] Tiuryn, J. Fixed-points and algebras with infinitely long expressions. Part I. Regular algebras. *Fundamenta Informaticae* 2(1978), 103–128.

[Tiu79] Tiuryn, J. Fixed-points and algebras with infinitely long expressions. Part II. mu-clones of regular algebras. *Fundamenta Informaticae* 2(1979), 317–336.