Finitary Observations in Regular Algebras

Sławomir Lasota*

Institute of Informatics, Warsaw University
Banacha 2, 02-097 Warszawa, Poland
email: sl@mimuw.edu.pl

Abstract. We investigate *regular algebras*, admitting infinitary regular terms interpreted as least upper bounds of suitable approximation chains. We prove that finitary observable contexts are sufficient for observational indistinguishability in a regular algebra. Moreover, assumed all observable sorts to be essentially flat, observational equivalence is also completely characterized by finitary contexts. As a corollary, methods of proving behavioural properties and observational equivalence of standard algebras can be reused in the setting of regular algebras.

1 Introduction

Behavioural semantics of algebraic specifications is widely accepted to capture properly the "black box" character of data abstraction. As a nontrivial example of an algebraic framework where behavioural ideas may be applied, we consider regular algebras, differing from the standard algebras in one respect: they allow one to additionally model infinite regular datatypes, like streams. Regular algebras were introduced in [11, 12], and then studied e.g. in [3]. Our starting point here is a more recent paper [2], investigating observational equivalence of regular algebras and the induced behavioural semantics of specification. Regular algebras contain properly continuous algebras [10], intended usually to model infinite datatypes. However continuous algebras are not well suited for behavioural semantics, in particular the requirement of existence of lubs of all (countable) chains seems to be too restrictive (cf. e.g. discussion in [2]).

Our motivation is to analyze applicability of regular algebras as models of behavioural specifications in the process of step-wise development of software systems [7, 8]. A crucial role is played here by the concept of observational equivalence: it allows one to consider possibly large class of acceptable realizations of a specification, under the only assumption that the observable behavior of the implementation conforms to the specification requirements. Observational equivalence of regular algebras is defined analogously as in the case of standard algebras, using observational indistinguishability by means of all observable contexts (cf. [2]). However, compared with standard algebras, in regular algebras infinitary contexts are involved too, since the structure is substantially richer: carrier sets are partially ordered and all term-definable mappings have fixed

* The work reported here was partially supported by the KBN grant 8 T11C 019 19.

points, given by the least upper bounds of appropriate approximation chains. This has a serious impact on complexity of proofs of behavioural properties of regular algebras, including proofs of correctness of implementation step.

In Section 3 we prove that observational indistinguishability in a regular algebra is actually induced by only finitary observable contexts – surprisingly, even when non-trivial approximation chains exist in carrier sets of observable sorts. This makes proofs of behavioural properties of regular algebras substantially easier, and allows one to use proof methods known for standard algebras, like context induction [4] or methods developed in [1].

Finitary contexts are not sufficient for observational equivalence in general. In the following Section 4 we extend the setting of regular algebras with a possibility to have carriers of some sorts essentially unordered (*essentially flat*), which is strongly required in practical examples. We prove that when carrier sets of all observable sorts are essentially flat, the notion of observational equivalence can be characterized by only finitary contexts too. Hence one can prove equivalence of regular algebras e.g. using standard observational correspondences [9].

Results reported here are used in [6] for adaptation of constructor implementation methodology [8] for regular algebras; the results are also contained in Chapter 5 of [5].

Acknowledgements The author is grateful to Andrzej Tarlecki for many fruitful discussions and valuable comments during this work.

2 Preliminaries

Regular algebras Let Σ, Σ' be fixed many-sorted algebraic signatures throughout this paper. We omit introducing classical notions of standard Σ-algebra, homomorphism, subalgebra, congruence, quotient. By $t_{A[v]}$ we denote the value of Σ-term t in algebra A under valuation v. By $|A|$ we denote the many-sorted carrier set of A; by $|A|_s$ the carrier of sort s. For a subset S of sorts of Σ, by $|A|_S$ we denote the carrier sets of sorts from S. All sets are implicitly meant to be many-sorted in the sequel. An *ordered Σ-algebra* is a standard Σ-algebra whose carrier set on each sort s is partially ordered (let $\leq_s^A$ denote the partial order in $|A|_s$) and has a distinguished element $\perp_s^A \in |A|_s$.

The set of *regular Σ-terms* $T_\Sigma^\mu(X)$ over X is defined inductively as usual, with the only additional case: for any $t \in T_\Sigma^\mu(X \cup \{z : s\})_s$ and a distinguished variable z of the same sort s, there is a *μ-term* $\mu z.t$ in $T_\Sigma^\mu(X)_s$. Similarly, the inductive definition of the value $t_{A[v]}$ of a term under a valuation $v : X \to |A|$ in an ordered algebra A needs one more case. For $t \in T_\Sigma^\mu(X \cup \{z : s\})_s$, put:

- $t^0_{A[v]}(\perp) := \perp_s^A$,
- for $i \in \omega$, $t^{i+1}_{A[v]}(\perp) := t_{A[v_i]}$, where $v_i : X \cup \{z : s\} \to |A|$ extends v by $v_i(z) = t^i_{A[v]}(\perp)$.

Now, $(\mu z.t)_{A[v]}$ is defined if $t^i_{A[v]}(\perp)$ are defined, for all $i \in \omega$, $t^i_{A[v]}(\perp) \leq_s^A t^{i+1}_{A[v]}(\perp)$, and the least upper bound $\bigsqcup_{i \in \omega} t^i_{A[v]}(\perp)$ exists in $|A|_s$; if so, then

$(\mu z.t)_{A[v]} = \bigsqcup_{i\in\omega} t^i_{A[v]}(\bot)$. An ordered Σ-algebra A is *regular* if it satisfies the following conditions:

- *completeness*: for all $t \in T^{\mu}_{\Sigma}(X)$ and $v : X \to |A|$, the value $t_{A[v]}$ is defined,
- *continuity*: for all $t \in T^{\mu}_{\Sigma}(X \cup \{y : s\})_{s'}$, $q \in T^{\mu}_{\Sigma}(X \cup \{z : s\})_s$ and valuations $v : X \to |A|$, $t_{A[v_i]} \leq^A_s t_{A[v_{i+1}]}$, for $i \in \omega$, and $t_{A[v']} = \bigsqcup_{i\geq 0} t_{A[v_i]}$, where valuation $v' : X \cup \{y : s\} \to |A|$ extends v by $v'(y) = (\mu z.q)_{A[v]}$ and $v_i : X \cup \{y : s\} \to |A|$ extends v by $v_i(y) = q^i_{A[v]}(\bot)$, for $i \geq 0$.

As it was proved in [5], continuity can be equivalently required only for *finitary* terms $t \in T_{\Sigma}(X \cup \{y : s\})_{s'}$, i.e., those not containing symbol μ. Notice that continuity, as stated above, does not imply even monotonicity of operations in a regular algebra.

By completeness, $\bot^A_s$ is the least element in $|A|_s$.

A regular subalgebra of A is any regular algebra B the carrier of which is a subset of A and such that for all terms $t \in T^{\mu}_{\Sigma}(X)$ and valuations $v : X \to |B|$, $t_{B[v]} = t_{A[v]}$. It is easy to see that all operations of B are restrictions of operations of A to $|B|$ and moreover $\bot^B_s = \bot^A_s$ for each sort s. For $Y \subseteq |A|$, by *the subalgebra of A generated by Y* we mean the least regular subalgebra of A whose carrier includes Y.

By a regular Σ-homomorphism $h : A \to B$ we mean any function h such that for all terms $t \in T^{\mu}_{\Sigma}(X)$ and valuations $v : X \to |A|$, $h(t_{A[v]}) = t_{B[h\circ v]}$. A regular congruence on A is a kernel of any regular Σ-homomorphism $h : A \to B$ (i.e., $\{(x, x') \mid h(x) = h(x')\}$).

Observational equivalence In the following we concentrate on an observational equivalence induced by a subset of observable sorts; hence throughout this paper let us fix a subset OBS of *observable sorts* of Σ.

In the following, let X denote some OBS-sorted set of variables. By a *Σ-context* of sort s' on sort s we mean any term $\gamma \in T^{\mu}_{\Sigma}(X \cup \{z_s : s\})_{s'}$, where z_s is a special, distinguished variable of sort s such that $z_s \notin X$. Note that z_s, for $s \notin OBS$, are the only variables of non-observable sorts appearing in contexts. A special role is played by *observable contexts*, i.e., contexts of observable sort ($s' \in OBS$). For any regular Σ-algebra A, Σ-context γ on sort s, valuation $v : X \to |A|_{OBS}$ and value $a \in |A|_s$, we will write $\gamma_{A[v]}(a)$ for $\gamma_{A[v_a]}$ where v_a extends v by $v(z_s) = a$.

For any A, let A_{OBS} denote its subalgebra generated by (carrier sets of) observable sorts; we call A_{OBS} an *observational subalgebra* of A. The regular congruence $\sim^{OBS}_A$ on A_{OBS} is defined as follows: for any $a, a' \in |A_{OBS}|_s$, $a \sim^{OBS}_A a'$ if and only if for all valuations v into carriers of observable sorts of A_{OBS} and all observable contexts γ, $\gamma_{A[v]}(a) = \gamma_{A[v]}(a')$. The congruence $\sim^{OBS}_A$ is a called *observational indistinguishability* in A; $\sim^{OBS}_A$ is the greatest congruence on A_{OBS} being identity on observable sorts (cf. [2]). The quotient of A_{OBS} by $\sim^{OBS}_A$ represents the observable behaviour of A; $A_{OBS}/{\sim^{OBS}_A}$ is *fully abstract* in the sense that its indistinguishability is identity. Two regular algebras are taken as equivalent when their behaviours are isomorphic:

Definition 1 *Observational equivalence $\equiv_{OBS}$ of regular Σ-algebras is defined by:*

$$A \equiv_{OBS} B \quad \textit{iff} \quad A_{OBS}/_{\sim_A^{OBS}} \cong B_{OBS}/_{\sim_B^{OBS}}.$$

$A_{OBS}/{\sim_A^{OBS}}$ will be written shortly $A/{\sim^{OBS}}$, when no confusion can occur.

All definitions concerning observational equivalence are still valid when standard algebras are taken into account instead of regular ones – the only modification required is to restrict contexts γ to only finitary terms $T_\Sigma(X)$ in definition of indistinguishability. We will deliberately overload notation and use symbols $\equiv_{OBS}$, $(\_)_{OBS}$ also for standard algebras. On the other hand, observational indistinguishability in standard algebras will be denoted by $\approx^{OBS}$.

3 Finitary Observations

Roughly, finitary observational contexts are powerful enough for indistinguishability in a regular algebra; the only infinitary regular terms really needed are to denote bottoms $\bot$. The proof of this fact is based on the property that each value of a μ-term is approximated by values of appropriate finitary terms.

For fixed OBS, Let $\mathcal{F}^{OBS}$ denote the set of all observable contexts $\gamma \in T_\Sigma^\mu(X \cup \{z_s : s\})$, such that the only possible μ-subterms of γ are of the form $\mu x.x$. Let $\sim_A^{\mathcal{F}^{OBS}}$ denote the contextual indistinguishability induced in A by only contexts from $\mathcal{F}^{OBS}$.

Theorem 2 *In a regular algebra A, $\sim_A^{OBS} \; = \; \sim_A^{\mathcal{F}^{OBS}}$.*

Proof. Assume that two values $a, a' \in |A|_s$ of sort s are distinguished by some regular context $\gamma \in T_\Sigma^\mu(X \cup \{z_s : s\})$ and a valuation v into carriers of observable sorts, i.e., $\gamma_{A[v]}(a) \neq \gamma_{A[v]}(a')$.

Lemma 3 formulated below will be crucial in what follows. Let t_0 be an arbitrary regular Σ-term and let w be an arbitrary valuation. Without loss of generality we can assume that if the same variable x is bound in two different subterms $\mu x.t_1$ and $\mu x.t_2$ of t_0, then these subterms are disjoint and terms $\langle t_1 \rangle_\mu$ and $\langle t_2 \rangle_\mu$ are identical; where for any regular term t, $\langle t \rangle_\mu$ denotes the term obtained from t by replacing each μ-subterm $\mu x'.t'$ with the variable x'. Let $\mu x_1.t_1, \ldots, \mu x_n.t_n$ be all different μ-subterms of t_0, $n \geq 0$. We define inductively $n+1$ sequences of terms, $\{t_i^j\}_{j \in \omega}$, for $0 \leq i \leq n$, as follows:

$$\begin{array}{lll} t_i^0 & := \mu x_i.x_i, & \text{for } i \geq 1; \\ t_i^{j+1} & := \langle t_i \rangle_\mu [t_1^j/x_1, \ldots, t_n^j/x_n], & \text{for } i \geq 1; \\ t_0^j & := \langle t_0 \rangle_\mu [t_1^j/x_1, \ldots, t_n^j/x_n]; & \end{array}$$

square brackets denote simultaneous substitution. (Notice that if $t_0 = \mu x_i.t_i$ for some i, then $\langle t_0 \rangle_\mu = x_i$ and $t_0^j = t_i^j$, for $j \geq 0$.) From Theorem 5.2.2 in Section 5.2 in [5] directly follows:

Lemma 3 *Value $(t_0)_{A[w]}$ is the l.u.b. of the chain $\{(t_0^j)_{A[w]}\}_{j \in \omega}$.*

Terms t_i^j have no μ-subterms except $\mu x_i.x_i$. Applying the lemma to $t_0 = \gamma$ and $w = v_a$ (i.e., v_a extends v by $v_a(z_s) = a$), we conclude that $\gamma_{A[v]}(a)$ is necessarily the least upper bound of the sequence $\{(\gamma_j)_{A[v]}(a)\}_{j\in\omega}$ and that contexts γ_j are in $\mathcal{F}^{OBS}$. Moreover, for $w = v_{a'}$ we conclude that also $\gamma_{A[v]}(a')$ is the least upper bound of the sequence $\{(\gamma_j)_{A[v]}(a')\}_{j\in\omega}$ induced by the same contexts. Since least upper bounds are different, $\gamma_{A[v]}(a) \neq \gamma_{A[v]}(a')$, the chains differ necessarily on some j, $(\gamma_j)_{A[v]}(a) \neq (\gamma_j)_{A[v]}(a')$; this completes the proof. $\square$

We can easily eliminate each term $\mu x.x$ of observable sort by replacing it with a fresh variable y and extending the valuation by $y \mapsto \perp$. Hence we only need terms $\mu x.x$ of non-observable sorts.

As a corollary, methods of proving behavioural properties of standard algebras (like context induction [4] or methods developed in [1]) can be reused in the framework of regular algebras.

Let $\Sigma(\perp)$ denote signature Σ enriched by a constant symbol $\perp_s$ in each sort s. For a regular Σ-algebra A, let $|A|_{\Sigma(\perp)}$ denote the standard $\Sigma(\perp)$-algebra with carrier sets and operations as in A and with $\perp_s$ interpreted as $\perp_s^A$ in each sort (i.e., by passing from A to $|A|_{\Sigma(\perp)}$, the partial order is forgotten and consequently also the information about values of non-trivial μ-terms). In the sequel, all $\Sigma(\perp)$-terms are called *finitary*.

By Theorem 2 we conclude that observational indistinguishability in a regular algebra A is roughly the indistinguishability in $|A|_{\Sigma(\perp)}$. But observational equivalence of regular algebras is not reducible to observational equivalence of standard $\Sigma(\perp)$-algebras: it *does not* hold

$$A \equiv_{OBS} B \quad \Leftrightarrow \quad |A|_{\Sigma(\perp)} \equiv_{OBS} |B|_{\Sigma(\perp)} \tag{1}$$

(note that on the right-hand side $\equiv_{OBS}$ denotes observational equivalence of standard $\Sigma(\perp)$-algebras). Intuitively, finitary contexts have more distinguishing power in regular algebras than in standard algebras, since the observational subalgebra A_{OBS} of a regular algebra A may be larger than the observational subalgebra $(|A|_{\Sigma(\perp)})_{OBS}$ of the standard $\Sigma(\perp)$-algebra $|A|_{\Sigma(\perp)}$.

Let us find out where the difficulties appear. Since $\sim_A^{OBS}$ is standard $\Sigma(\perp)$-congruence, the forgetful functor $|\_|_{\Sigma(\perp)}$ commutes with observational quotient:

$$|A_{OBS}|_{\Sigma(\perp)}/_{\sim_A^{OBS}} \;=\; |A_{OBS}/_{\sim_A^{OBS}}|_{\Sigma(\perp)}. \tag{2}$$

The observational (standard, regular) subalgebras are generated by (finitary, regular) terms, hence $(|A|_{\Sigma(\perp)})_{OBS} = (|A_{OBS}|_{\Sigma(\perp)})_{OBS}$. Moreover $(|A|_{\Sigma(\perp)})_{OBS}$ may be a *proper* subalgebra of $|A_{OBS}|_{\Sigma(\perp)}$ in general – this is why we need another symbol $\approx_A^{OBS}$ to stand for the indistinguishability (by means of $\Sigma(\perp)$-contexts) in $(|A|_{\Sigma(\perp)})_{OBS}$. However, by Theorem 2 $\approx_A^{OBS}$ and $\sim_A^{OBS}$ agree on $(|A|_{\Sigma(\perp)})_{OBS}$, so the implication from left to right holds in (1). On the other hand, from $|A|_{\Sigma(\perp)} \equiv_{OBS} |B|_{\Sigma(\perp)}$, i.e. $(|A|_{\Sigma(\perp)})_{OBS}/_{\approx^{OBS}} \cong (|B|_{\Sigma(\perp)})_{OBS}/_{\approx^{OBS}}$ we cannot even conclude (e.g. using (2)) that $|A/_{\sim^{OBS}}|_{\Sigma(\perp)} \cong |B/_{\sim^{OBS}}|_{\Sigma(\perp)}$. But even if we could, this would not guarantee $A/_{\sim^{OBS}} \cong B/_{\sim^{OBS}}$ in general.

Example 4 *As a counterexample to (1) (confirming also the last statement), consider two regular algebras, A and A', over Σ containing two sorts, $\{o, n\}$, and two operations: $f : o \to o$, $g : n \to o$; the only observable sort is o.*

$$\begin{array}{ll} A_o = \{a_0 = \bot_o, a_\infty, a'_\infty\} \cup \{a_i\}_{i=1,2,\ldots} & f^A(a_i) = a_{i+1},\ i \geq 0 \\ A_n = \{a = \bot_n\} & f^A(a_\infty) = a_\infty,\ f^A(a'_\infty) = a'_\infty \\ \bot_o \leq a_1 \leq \ldots,\ (\bigsqcup_{i=0,1,\ldots} a_i) = a_\infty \leq a'_\infty & g^A(a) = a_\infty \end{array}$$

A' differs from A only by $g^{A'}(a) = a'_\infty$ (i.e., in particular $|A'| = |A|$). Both A and A' are fully abstract, i.e., their indistinguishabilities are identities. This implies that they are not observationally equivalent, since they are non-isomorphic (e.g. because the equation: $\forall x.\ g(x) = \mu y.f(y)$ is satisfied only in one of them). On the other hand, evidently, $|A|_{\Sigma(\bot)} \cong |A'|_{\Sigma(\bot)}$; an isomorphisms $\sim$ is given by: $\sim_o = \{(a_i, a_i)\}_{i=0,1,\ldots} \cup \{(a_\infty, a'_\infty), (a'_\infty, a_\infty)\}$, $\sim_n = \{(a, a)\}$.

As the example suggests, the reason why (1) does not hold is presence of infinite chains in carrier sets of observable sorts. This will be more apparent in the next section, as our assumption there rules out such chains.

In consequence, the concept of observational correspondence [9] cannot be adopted here using only finitary contexts.

4 Flat Observable Sorts

In many practical situations we need only some sorts of a regular algebra to have upper bounds of approximation chains. In [5] it was argued that the best way to achieve this is to require carrier sets of algebraic sorts to be *essentially flat*. Formally, we say that the carrier set of sort s of a regular Σ-algebra is essentially flat if this algebra is isomorphic (i.e., related via a bijective regular homomorphism) to a regular algebra A whose carrier set of sort s has flat ordering with the least element $\bot_s^A$ ($a \leq b$ iff $a = \bot_s^A$ or $a = b$).[1] In consequence, all chains imposed by completeness and continuity in an essentially flat carrier set collapse, namely contain at most two different values.

In practical examples all observable sorts are usually intended to be essentially flat. Besides practical advantages, essentially flat carriers of observable sorts imply that finitary observational contexts (and consequently standard correspondences) are sufficient for observational equivalence of regular algebras, in contrast to the negative statement (1) above.

Theorem 5 *For regular algebras A and B with essentially flat carrier sets of observable sorts, $A \equiv_{OBS} B \ \Leftrightarrow\ |A|_{\Sigma(\bot)} \equiv_{OBS} |B|_{\Sigma(\bot)}$.*

Proof. Recall from the previous section that the implication from left to right holds for any regular A and B. For the opposite direction, assume $|A|_{\Sigma(\bot)} \equiv_{OBS} |B|_{\Sigma(\bot)}$, i.e., $(|A|_{\Sigma(\bot)})_{OBS}/_{\approx_A^{OBS}}$ and $(|B|_{\Sigma(\bot)})_{OBS}/_{\approx_A^{OBS}}$ are related by an isomorphism of standard $\Sigma(\bot)$-algebras, say i. The proof proceeds in two steps.

[1] Evidently, isomorphic regular algebras may have different orders.

First, we show that i can be extended to isomorphism between $|A_{OBS}|_{\Sigma(\bot)}/_{\sim_A^{OBS}}$ and $|B_{OBS}|_{\Sigma(\bot)}/_{\sim_B^{OBS}}$.

Recall that $\sim_A^{OBS}$ and $\approx_A^{OBS}$ agree on $(|A|_{\Sigma(\bot)})_{OBS}$ and that observational subalgebra A_{OBS} (resp. $(|A|_{\Sigma(\bot)})_{OBS}$) is generated by regular (resp. finitary) terms with variables of observable sorts. Hence we only need to extend i to abstraction classes of $\sim_A^{OBS}$ of values denoted by infinitary terms in A_{OBS}. We define an isomorphism $i' : |A_{OBS}|_{\Sigma(\bot)}/_{\sim_A^{OBS}} \to |B_{OBS}|_{\Sigma(\bot)}/_{\sim_B^{OBS}}$ as follows: for an arbitrary regular term t with variables of observable sorts and valuation w into carrier sets of observable sorts of A,

$$i'([t_{(A_{OBS})[w]}]_{\sim_A^{OBS}}) = [t_{(B_{OBS})[i\circ w]}]_{\sim_B^{OBS}}. \tag{3}$$

(On observable sorts, i is treated in (3) as if its domain is A, since $\approx_A^{OBS}$ is necessarily identity on OBS.) We need to show the following:

- i' is a well defined function, i.e., its value according to (3) does not depend on a representative of an abstraction class of $\sim_A^{OBS}$;
- i' is a bijective $\Sigma(\bot)$-homomorphism.

For fixed t and w as before, by Lemma 3 in Section 3, $a := t_{(A_{OBS})[w]}$ is the l.u.b. of $\{a_j := t^j{}_{(|A_{OBS}|_{\Sigma(\bot)})[w]}\}_{j\in\omega}$, for appropriate $\Sigma(\bot)$-terms t^j. Similarly, $b := t_{(B_{OBS})[i\circ w]}$ is the l.u.b. of $\{b_j := t^j{}_{(|B_{OBS}|_{\Sigma(\bot)})[i\circ w]}\}_{j\in\omega}$. Consider an arbitrary observable context γ (by virtue of Theorem 2 we assume γ to be a finitary $\Sigma(\bot)$-context) together with a valuation v into carrier sets of observable sorts of A. Since carrier sets of observable sorts of A and B are essentially flat, all relevant chains in these sorts are collapsed in A_{OBS} and B_{OBS}. In particular $\{\gamma_{(|A_{OBS}|_{\Sigma(\bot)})[v]}(a_j)\}_{j\in\omega}$ is constant starting from some position. Hence, the value of $\gamma_{(A_{OBS})[v]}(a)$ is equal to a' iff starting from some position, values $\{\gamma_{(|A_{OBS}|_{\Sigma(\bot)})[v]}(a_j)\}_{j\in\omega}$ in the approximation chain are all equal to a'. In a similar way, the value of $\gamma_{(B_{OBS})[i\circ v]}(b)$ is determined by $\{\gamma_{(|B_{OBS}|_{\Sigma(\bot)})[i\circ v]}(b_j)\}_{j\in\omega}$. Moreover, for $j\in\omega$, $b_j = i(a_j)$ and $\gamma_{(|B_{OBS}|_{\Sigma(\bot)})[i\circ v]}(b_j) = i(\gamma_{(|A_{OBS}|_{\Sigma(\bot)})[v]}(a_j))$, since all t^j and γ are finitary. Finally, quotient by the observational indistinguishability $\sim_A^{OBS}$ ($\sim_B^{OBS}$) preserves values of observable contexts, e.g.

$$\gamma_{\left(|A_{OBS}|_{\Sigma(\bot)}/\sim_A^{OBS}\right)[v]}([a]_{\sim_A^{OBS}}) = \gamma_{(A_{OBS})[v]}(a)$$

(since $\sim^{OBS}$ is identity on OBS, we treat here v as a function into the quotient algebra and moreover we identify carriers of observable sorts of A_{OBS} and $|A_{OBS}|_{\Sigma(\bot)}/\sim_A^{OBS}$). Due to the mentioned facts and since $i'([a]_{\sim_A^{OBS}}) = [b]_{\sim_B^{OBS}}$ by (3), we conclude that i' preserves (up to i) values of observable contexts, i.e.,

$$\gamma_{\left(|B_{OBS}|_{\Sigma(\bot)}/\sim_B^{OBS}\right)[i\circ v]}\big(i'([a]_{\sim_A^{OBS}})\big) = i\big(\gamma_{\left(|A_{OBS}|_{\Sigma(\bot)}/\sim_A^{OBS}\right)[v]}([a]_{\sim_A^{OBS}})\big) \tag{4}$$

Now, consider two indistinguishable values a_1, a_2 in A_{OBS}, $a_1 \sim_A^{OBS} a_2$. By (4) $i'([a_1]_{\sim_A^{OBS}})$ and $i'([a_2]_{\sim_A^{OBS}})$ are also indistinguishable in $|B_{OBS}|_{\Sigma(\bot)}/_{\sim_B^{OBS}}$. But the quotient algebra $|B_{OBS}/_{\sim_B^{OBS}}|_{\Sigma(\bot)}$ is necessarily fully abstract, i.e., any two indistinguishable elements are equal. By (2), $|B_{OBS}|_{\Sigma(\perp)}/_{\sim_B^{OBS}}$ is fully abstract too, hence $i'([a_1]_{\sim_A^{OBS}}) = i'([a_2]_{\sim_A^{OBS}})$ and i' is well defined in (3).

By the very definition, i' is a standard $\Sigma(\perp)$-homomorphism. Moreover, since i is a bijection (hence surjective) on OBS, it follows immediately that i' is surjective. For injectivity, notice that whenever $i'([a_1]_{\sim_A^{OBS}}) = i'([a_2]_{\sim_A^{OBS}})$, by (4) $[a_1]_{\sim_A^{OBS}}$ and $[a_2]_{\sim_A^{OBS}}$ are indistinguishable in $|A|_{\Sigma(\perp)}/_{\sim_A^{OBS}}$, hence equal due to full abstractness of the quotient algebra, similarly as above.

Now we come to the second step of the proof, which fortunately turns out to be immediate. By (2) we conclude that the isomorphism i' relates $|A/_{\sim^{OBS}}|_{\Sigma(\perp)}$ and $|B/_{\sim^{OBS}}|_{\Sigma(\perp)}$. Moreover, by the very definition (3), i' is also a regular Σ-homomorphism. Hence $A/_{\sim^{OBS}}$ and $B/_{\sim^{OBS}}$ are isomorphic. □

Unlike in Theorem 2, the whole signature $\Sigma(\perp)$ is actually needed in the proof, in order to guarantee that $\perp$'s in all observable sorts are related by i.

As a conclusion, we obtain an effective complete proof technique for observational equivalence of regular algebras:

Corollary 6 *Regular algebras with essentially flat carrier sets of observable sorts are observationally equivalent iff they are related by an observational $\Sigma(\perp)$-correspondence [9].*

References

1. Bidoit, M., Hennicker, R. Behavioural theories and the proof of behavioural properties. *Theoretical Computer Science* 165(1): 3-55, 1996.
2. Bidoit, M., Tarlecki, A. Regular algebras: a framework for observational specifications with recursive definitions. Report LIENS-95-12, ENS, 1995.
3. Guessarian, I., Parisi-Presicce, F. Iterative vs. regular factor algebras. SIGACT News 15(2), 32-44, 1983.
4. Hennicker, R. Context induction: A proof principle for behavioural abstractions and algebraic implementations. *Formal Aspects of Computing*, 3(4):326-345, 1991.
5. Lasota, S. Algebraic observational equivalence and open-maps bisimilarity. Ph.D. Thesis in Institute of Informatics of Warsaw University, March 2000. Accessible at `http://www.mimuw.edu.pl/~sl/work/phd.ps.gz`.
6. Lasota, S. Behavioural constructor implementation for regular algebras. To appear in *Proc. 7th International Conference on Logic for Programming and Automated Reasoning LPAR'2000*, Springer-Verlag LNAI series.
7. Sannella, D., Tarlecki, A. Towards formal development of programs from algebraic specifications: implementations revisited. *Acta Informatica* 25:233-281, 1988.
8. Sannella, D., Tarlecki, A. Essential Concepts of Algebraic Specification and Program Development. *Formal Aspects of Computing* 9:229-269, 1997.
9. Schoett, O. *Data abstraction and correctness of modular programming.* PhD thesis, CST-42-87, Department of Computer Science, University of Edinburgh, 1987.
10. Tarlecki, A., Wirsing, M. Continuous abstract data types. *Fundamenta Informaticae* 9(1986), 95-126.
11. Tiuryn, J. Fixed-points and algebras with infinitely long expressions. Part I. Regular algebras. *Fundamenta Informaticae* 2(1978), 102-128.
12. Tiuryn, J. Fixed-points and algebras with infinitely long expressions. Part II. Muclones of regular algebras. *Fundamenta Informaticae* 2(1979), 317-336.