Theoretical Computer Science 111 (1993) 191–210
Elsevier

Modal logic and algebraic specifications

Lawrence S. Moss

Department of Mathematics, Indiana University, Bloomington, IN 47405, USA

Satish R. Thatte

Department of Mathematics and Computer Science, Clarkson University, Potsdam, NY 13676, USA

Abstract

Moss, L.S. and S.R. Thatte, Modal logic and algebraic specifications, Theoretical Computer Science 111 (1993) 191–210.

The established approaches to the semantics of algebraic (equational) specifications are based on a category-theoretic perspective. When possible interpretations are viewed as a category, the extreme points – the initial and final algebras – present themselves as natural candidates for the canonical interpretation. However, neither choice provides a satisfactory solution for incomplete specifications of abstract data types – the initial algebra is not abstract enough and the final algebra often does not exist.

We argue that in much of the work on algebraic specifications, the categorical viewpoint is simply a convenient technical device to capture semantically the modalities of necessity and possibility. It is actually more natural to consider the semantic problem from the perspective of modal logic, gathering possible interpretations into a Kripke model. When necessity and possibility are added as modal operators in the logical language, a new candidate for the canonical interpretation – which we call the *optimal* algebra[1] – arises naturally. The optimal algebra turns out to be a natural generalization of the final algebra, and provides a satisfactory semantics in situations where the *spirit* of final algebra semantics is desired but a final algebra does not exist.

Optimal semantics has a topological flavor. Our Kripke models are topological spaces in a natural way. In most (but not all) of the interesting cases, the Baire category theorem holds for the topology of a Kripke model, in which case the optimal semantics validates exactly those equational properties which hold in *dense open* subsets of the Kripke model. In analogy with many similar situations, we may regard these as properties that hold *almost everywhere* in the model.

Correspondence to: L.S. Moss, Department of Mathematics, Indiana University, Bloomington, IN 47405, USA. Email: lmoss@indiana.edu.

[1] The term "optimal algebra" was suggested to us by Vaughan Pratt, who also independently arrived at some of the related intuitions. Francesco Parisi-Pressice has informed us that, in an unpublished work, he considered optimality several years ago, also as a generalization of final algebra semantics.

1. Introduction

Many properties of abstract data types can be specified *algebraically*, i.e., with sets of universally quantified equations. For instance, a simple specification for sets may use the operations

$$\mathsf{add}: \mathsf{item} \times \mathsf{set} \to \mathsf{set}$$

$$\mathsf{empty}: \to \mathsf{set}$$

$$\mathsf{member}: \mathsf{item} \times \mathsf{set} \to \mathsf{bool}$$

$$\mathsf{subset}: \mathsf{set} \times \mathsf{set} \to \mathsf{bool}$$

with the equations

$$\mathsf{member}(x, \mathsf{add}(y, s)) = \mathsf{equal}(x, y) \vee \mathsf{member}(x, s)$$

$$\mathsf{subset}(\mathsf{empty}, s) = \mathsf{true}$$

$$\mathsf{subset}(\mathsf{add}(x, s_1), s_2) = \mathsf{member}(x, s_2) \ \& \ \mathsf{subset}(s_1, s_2)$$

Obviously, an abstract type specified is thus expected to possess many more equational properties than the ones stated above. The *semantics* of the specification characterizes these *implied* properties by associating a canonical model with the specification – the semantics determines how "complete" the specification has to be in order to capture the intended model and its properties. The most conservative characterization of implied properties is the *equational theory* of the specification, which is the set of equations that hold in all models of the specification. By Birkhoff's well-known completeness theorem for equational logic, this is also the set of all equations deducible (equationally) from the specification. This characterization is closely related to the (slightly more liberal) *initial algebra semantics* because the *ground* equations in the equational theory are precisely those which hold in the initial model in the natural category of all models for a specification. The equational theory often does not capture all the expected properties of an abstract type since many such properties are *inductive*. For instance, the equation

$$\mathsf{subset}(s, s) = \mathsf{true}$$

is not a consequence of the above specification without further stipulation that all values of the sort set are generated by the constructors empty and add. This restriction narrows the class of permissible models and gives rise to a notion of *inductive theories* [1]. One can go a step further, and consider all equations that can be used as program transformations without any *observable* consequences. In fact, this is natural since abstract data types are normally viewed as black boxes whose users are to be concerned only with their observable behavior. In a many-sorted specification such as the one above for sets, the sorts can be naturally divided into the observable and nonobservable ones. Suppose the sort of booleans (bool) is observable (because

truth values can be used in conditionals, say), while that of sets is not. Suppose further that the usual equations for boolean operations such as $\vee$ and & have been provided. Now the equations

$$\mathsf{add}(x, \mathsf{add}(y, s)) = \mathsf{add}(y, \mathsf{add}(x, s))$$

$$\mathsf{add}(x, \mathsf{add}(x, s)) = \mathsf{add}(x, s)$$

are both usable as program transformations since there is no way to observe the difference between the two sides of either equation by "plugging" them into any context of observable sort. However, they are *not* inductive properties in any reasonable sense. We shall refer to such equational properties as *abstract* properties and the collection of such properties as the *abstract theory* of a specification. These names are inspired by the similarity in spirit between abstract theories and the *fully abstract* semantics of programming languages [8].

The main purpose of this paper is to formalize and study abstract theories and the corresponding characteristic models which we call the *optimal* algebras. The best existing formalization of abstract theories is found in final algebra semantics [10, 4]. However, this formalization has a serious flaw – it is applicable only to specifications that are *complete* in some sense. For instance, the specification given above is incomplete because it does not specify the result of expressions of the form $\mathsf{member}(x, \mathsf{empty})$. Final algebra semantics is not applicable to such specifications. Real specifications in the process of development are rarely complete. To say that they possess no abstract properties during their entire development but suddenly acquire them all upon adding the last equation needed for completeness does not seem satisfactory. We show in this paper that, in a natural sense, the existence of abstract theories and the corresponding characteristic models (optimal algebras) is independent of completeness. It turns out that the ideas underlying these results arise naturally when the semantics of equational specifications is considered from a modal logic perspective, rather than the category-theoretic one which gave rise to initial and final algebra semantics. We now turn to a discussion of this new perspective.

2. A new perspective on semantics

The point of any semantic approach is to capture a notion of validity. In the context of equational specifications, the notion of validity depends on two parameters:

(1) A modality attached implicitly to equational assertions.

(2) A class of interesting (or as we shall say in the sequel, *proper*) interpretations.

The categorical viewpoint gives a convenient technical device to capture semantically the modalities of *necessity* and *possibility*. That is, if C is a collection of models of an equational specification considered as a preorder category in the natural way, the ground equations true in an initial C-object are exactly those which are *necessarily*

true, i.e., true in all C-objects. Similarly, the ground equations true in a final C-model are exactly those which are *possibly true*.

The *usefulness* of a semantic method is judged by asking how closely the choices of modality and class correspond to some predetermined intuition. The *applicability* of the method is gauged by determining for which choices is there a *single* algebra which captures the semantics. Under this rubric, initial algebra semantics (the semantics of necessary truth under all reasonable interpretations) is always applicable. On the other hand, we have seen that final algebra semantics (the semantics of possible truth in all reasonable interpretations) is not always applicable. The reason is that two assertions can both be possible, yet together they might be inconsistent. For the specification of abstract data types, final algebra semantics is much more useful in capturing *abstract* properties than initial algebra semantics, but also much less applicable.

Returning to our discussion of the existing semantic approaches, we note that even though the modalities are conceptually primary, they have been mathematically secondary – it just so happens that initiality and finality capture the right modalities, but the modalities are implicit rather than explicit. It is hard to see how to generate more complicated modalities from these tools.

Our central idea is to add modal operators necessity ($\Box$) and possibility ($\Diamond$) to the *language* of equational logic (rather than the metalanguage), and we call the result *modal equational logic*. We interpret this logic on categories of proper interpretations, considered as Kripke structures under the quotient relation. The preorder property of quotients implies that every formula is equivalent to one of the following three forms: $\Box e$, $\Diamond e$, and $\Box \Diamond e$.

This paper introduces the third of these modalities into work on data type specification. If $\Box \Diamond e$ is true in a (Kripke) model, we say that e is *densely true*, because when the model is given the natural topology, e is true on a dense open set. The semantics of the modalities implies that an equation is densely true exactly when it is *consistent* with *all* algebras in the model. Furthermore, dense truths are always collectively consistent. As a result, given *any* choice of the class of proper algebras, there is an algebra that captures dense truth relative to that class. This is the algebra we call the *optimal* algebra of a specification.

It is not obvious from the foregoing that optimal algebras have anything to do with the abstract theories we set out to formalize. In fact, there is a very close connection. For one thing, dense truth coincides with possible truth whenever the set of all possible truths is consistent. Thus, optimal algebra semantics coincides with final algebra semantics whenever the latter is well-defined, independent of the choice of the class of proper interpretations. Moreover, an equation is an abstract property of a specification exactly when it is *consistent* with *all* algebras in the class of proper interpretations, since consistency in this context means exactly the lack of observable contradiction. The notion of abstract property, therefore, coincides with the notion of dense truth. The only flaw in this picture is that a nonground equation that holds in the optimal algebra may not, in general, be densely true in the corresponding Kripke

structure when the Kripke structure is *incomplete* in some sense. This and other undesirable properties of incomplete Kripke structures suggest that they should not be used in constructing optimal semantics.

We now make these ideas precise. Preliminary definitions are given in the next section. Section 4 describes a simple modal equational logic in which there are exactly three fundamental modalities – necessary, possible and dense truth. The optimal semantics is determined by dense truth and a collection of structures; it is described in Section 5. This section is the heart of the technical part of the paper, and contains the easy proof that the optimal model always exists. Section 5 also discusses the topological connections of the ideas of density. Section 6 formalizes what we mean by "complete" Kripke models, and proves the connection between dense truth and the alternative formulation of abstract properties in such models. The semantic ideas of this paper are illustrated with several examples in Section 7.

3. Preliminaries

Our technical machinery is based on the work of the ADJ group. An excellent tutorial introduction to this material can be found in [2]. We assume familiarity with the basic notions therein.

Given an S-sorted signature Σ, we use T_Σ to denote both the initial (free) Σ-algebra, and the (many-sorted) set of all Σ-terms. Given a Σ-algebra A, the unique homomorphism from T_Σ to A evaluates terms according to their interpretation in A; it too will be denoted by A. All of the Σ-algebras in this paper are *reachable*, i.e., the function A will be surjective. By implication, we assume that the *signature* of the specification is complete – few interesting abstract properties can be derived without such an assumption. A theory E consists of a signature Σ_E and a set (also called) E of (Σ_E)-equations. The equations might contain variables, but in this paper we will not consider conditional equations.

If e is a Σ-equation and the signature Σ_A of an algebra A includes Σ, then we write $A \models e$ to mean that every substitution instance of e is true in A. An equation e determines a congruence $|e|$ on A; $|e|$ is the least congruence containing all substitution instances of e. The quotient $A/|e|$ then satisfies e. Both notations extend to sets E of equations in the obvious way. We write I_E for $T_{\Sigma_E}/|E|$. One of the basic results of algebraic semantics is that I_E is initial in the category of Σ_E-algebras which satisfy E. For all ground terms t and u of the appropriate signature, $I_E(t) = I_E(u)$ iff the equation "$t = u$" is deducible from E using simple equational deduction. We write $t =_E u$ as an abbreviation for $I_E(t) = I_E(u)$.

When considering abstract semantics, a specification is naturally divided into a base specification and its extension, which we denote by the pair (BASE, EXT). Intuitively, the BASE specifies observability – the carriers of I_{BASE} are the observable values. The sorts of BASE are, therefore, called the *observable sorts*. The extension EXT usually adds new operations, possibly on the same sort set and possibly adding new

sorts. We assume that EXT is well-formed in the sense that $\Sigma_{\text{EXT}} \supseteq \Sigma_{\text{BASE}}$ and the equational theory of EXT is a *conservative extension* of the equational theory of BASE, i.e., $I_{\text{EXT}}|\Sigma_{\text{BASE}} \cong I_{\text{BASE}}$, where a reduct $A|\Sigma$ of A is just the algebra A considered as a Σ-algebra and forgetting everything else – assuming, of course, that $\Sigma_A \supseteq \Sigma$. This condition does not require that EXT $\supseteq$ BASE; it allows EXT to contain a different set of axioms for I_{BASE}.

We write T_{BASE} for the set of all Σ_{BASE}-terms, and similarly for T_{EXT}.

Definition. A Σ_{EXT}-algebra A is an EXT-*algebra* if

(1) $A \models$ EXT,

(2) $A|\Sigma_{\text{BASE}} \cong I_{\text{BASE}}$.

An EXT-algebra A is said to *respect* the BASE since it must satisfy condition (2). An algebra which respects the BASE neither implies new identifications nor new distinctions in the observable values created by the BASE. It is important to note that the condition restricts only the interpretation of Σ_{BASE}-terms, not that of other Σ_{EXT}-terms of observable sort.

Henceforth, we shall simply write *algebra* instead of EXT-*algebra* and *equation* instead of Σ_{EXT}-*equation* whenever possible without creating confusion.

The (reachable) algebras with Σ_{EXT}-morphisms comprise a category which we denote by $\mathscr{R}_{\text{EXT}}$. (Again, we generally omit the subscript.) Identifying isomorphic algebras, $\mathscr{R}$ is a partial order category – $A \leqslant B$ in $\mathscr{R}$ iff there is a morphism from A to B. Often, we will forget the category-theoretic aspects of $\mathscr{R}$ and instead emphasize the order.

The notion of a "complete" specification can be made precise in terms of the following property.

Definition (*Standardness*). An EXT-algebra A is said to be *standard* if for all observable sorts s, and $\forall u \in A_s$, $\exists v \in (T_{\text{BASE}})_s$ such that $u = A(v)$.

Standardness essentially *extends* the notion of respecting the base to all Σ_{EXT}-terms of observable sort, i.e., it guarantees that the carriers of observable sorts will be exactly those in I_{BASE}. A specification (BASE, EXT) is said to be *sufficiently complete* iff I_{EXT} is standard [3]. The main theorem of final algebra semantics is the following.

Theorem 3.1 (Wand [10]). *For every sufficiently complete specification* (BASE, EXT), *the category* $\mathscr{R}_{\text{EXT}}$ *has a final object.*

4. Three fundamental modalities

We show in this section that if the ideas of necessity and possibility are applied as modal operators to define a modal equational logic, then they give rise to exactly one new fundamental modality.

Fix a specification (BASE, EXT), and let the class of proper interpretations of EXT be an *arbitrary* full subcategory $\mathscr{K}$ of $\mathscr{R}_{\text{EXT}} - \mathscr{K}$ is a Kripke model of EXT. The modal formulas use the traditional necessity ($\Box$) and possibility ($\Diamond$) operators. The notion of satisfaction uses the natural order on the algebras in $\mathscr{K}$.

Definition. The set of (*modal equational*) *formulas* is the smallest set S containing every equation, and such that if $\phi \in S$, then both $\Box\phi$ and $\Diamond\phi$ belong to S. The *ground formulas* are formulas which do not contain variables.

The *satisfaction* relation $\models_{\mathscr{K}}$ (relative to a Kripke model $\mathscr{K}$) is the unique relation on $\mathscr{K} \times S$ such that for all $A \in \mathscr{K}$

- $A \models_{\mathscr{K}} e$ if $A \models e$,
- $A \models_{\mathscr{K}} \Diamond\phi$ if for some $B \geqslant A$ in $\mathscr{K}$, $B \models_{\mathscr{K}} \phi$,
- $A \models_{\mathscr{K}} \Box\phi$ if for all $B \geqslant A$ in $\mathscr{K}$, $B \models_{\mathscr{K}} \phi$.

Two formulas ϕ and ψ are considered *equivalent* (written $\phi \equiv \psi$) if for all $\mathscr{K}$, and all $A \in \mathscr{K}$, $A \models_{\mathscr{K}} \phi$ iff $A \models_{\mathscr{K}} \psi$. Satisfaction in $\mathscr{K}$ as a whole is represented by the assertion $\models_{\mathscr{K}} \phi$, where ϕ is a modal formula. This would be most naturally defined as "$\models_{\mathscr{K}} \phi$ iff $\perp \models_{\mathscr{K}} \phi$" if $\mathscr{K}$ had an *initial* object $\perp$. However, the categories $\mathscr{K}$ which arise naturally in applications do not always have an initial object; so, we make the definition more explicit.

Definition. Given a Kripke structure $\mathscr{K}$,

- $\models_{\mathscr{K}} \Box\phi \Leftrightarrow \forall A \in \mathscr{K}.\ A \models_{\mathscr{K}} \phi$,
- $\models_{\mathscr{K}} \Diamond\phi \Leftrightarrow \exists A \in \mathscr{K}.\ A \models_{\mathscr{K}} \phi$,
- $\models_{\mathscr{K}} e \Leftrightarrow \models_{\mathscr{K}} \Box e$.

The main result of this section is that, although S includes complicated formulas like $\Diamond\Box\Diamond\Diamond\Box e$, every formula is, in fact, equivalent to a formula of one of three special forms.

Lemma 4.1. *For every formula ϕ there is an equivalent formula ψ of one of the following forms:*

- *An equational necessity*: $\Box e$.
- *An equational possibility*: $\Diamond e$.
- *A density formula*: $\Box\Diamond e$.

Proof. Recall that the truth of equations is preserved as we go up the order $\leqslant$, and the ordering on $\mathscr{K}$ is transitive. Therefore, for all ϕ, $\Box\phi \equiv \Box\Box\phi$ and $\Diamond\phi \equiv \Diamond\Diamond\phi$. Further, it is easy to see that if $\phi \equiv \psi$, then $\Diamond\phi \equiv \Diamond\psi$ and $\Box\phi \equiv \Box\psi$, and, moreover, $\Box e \equiv e$ and $\Diamond\Box\Diamond e \equiv \Diamond e$. This proves the proposition for all ϕ with at most three modalities. The general case now follows by a simple induction on ϕ. □

Lemma 4.1 implies that in modal equational logic, there are exactly three senses in which an equation e can "hold" in a Kripke model $\mathscr{K}$ as a whole. These, therefore, are

the three alternatives available for the first choice mentioned at the beginning of Section 2. Of the three, the first two alternatives lead to familiar results.

Proposition 4.2. *Let A be an algebra in $\mathscr{K}$. A is initial in $\mathscr{K}$ iff for all (ground) equations e, $A \models e$ iff $\models_{\mathscr{K}} \Box e$ and A is final in $\mathscr{K}$ iff for all such e, $A \models e$ iff $\models_{\mathscr{K}} \Diamond e$.*

The third and novel alternative is explored below.

5. Dense truth and optimal semantics

We begin by stating the topology that justifies calling the third category of formulas in Lemma 4.1 the "density formulas". This is just the natural topology on posets. On a partial order $\langle X, \leqslant_X \rangle$, the family of upper intervals $U_A = \{B\colon A \leqslant_X B\}$ forms the base for a topology on X; a set is open iff it is upward-closed. For instance, the standard algebras form an open subset of $\mathscr{R}$. This idea can be applied to $\mathscr{R}$ and also to any full suborder $\mathscr{K} \subseteq \mathscr{R}$. In this topology, a set $\mathscr{Y} \subseteq \mathscr{K}$ is *dense* in $\mathscr{K}$ if for all $A \in \mathscr{K}$, there is some $B \in \mathscr{Y}$ such that $A \leqslant B$.

Definition. A (not necessarily ground) equation e is *densely true in* $\mathscr{K}$ if there is a dense subset $\mathscr{Y} \subseteq \mathscr{K}$ such that for every $C \in \mathscr{Y}$, $C \models e$.

Recall the informal notion of an *abstract property* we started with in the introduction. There are various ways to interpret the statement 'there is no way to observe the difference between the two sides of an equation by "plugging" them into any context of observable sort' relative to a specification and a Kripke model for it. We use it to mean that the equation must be consistent with every proper interpretation of the specification. The assertion that e is densely true in $\mathscr{K}$ captures exactly this intuition: even though e might not be *true* in every proper algebra, given any $A \in \mathscr{K}$, e is *consistent* with A in the sense that there is some $B \geqslant A \in \mathscr{K}$ such that $B \models e$ – since B respects the BASE, the addition of e does not cause a contradiction. We shall, henceforth, use the terms "densely true equation" and "abstract property" interchangeably. The connection between densely true equations and the density formulas of Lemma 4.1 is simple.

Proposition 5.1. *An equation e is densely true in $\mathscr{K}$ iff $\models_{\mathscr{K}} \Box \Diamond e$.*

We note also that for every equation e, the set $\{A \in \mathscr{K}\colon A \models e\}$ is open since the truth of equations persists upwards. So, if e is densely true, then in fact e holds in a dense *open* set.

Just as necessary and possible truths yield initial and final algebra semantics, dense truth yields a corresponding semantics which we call optimal algebra semantics. To be more precise, a *ground* equation is densely true iff it holds in the optimal algebra

defined below. For non-ground equations it is necessary to add a completeness condition on Kripke structures (see Section 6).

Definition. An algebra A is *optimal* for $\mathscr{K}$ if for all ground equations e, $A \models e \Leftrightarrow e$ is densely true in $\mathscr{K}$.

In many interesting cases, the optimal algebra will exist but not belong to $\mathscr{K}$. For this reason, we do not require $A \in \mathscr{K}$ as part of the definition of optimality for $\mathscr{K}$. From the definition, it follows easily that optimal algebra semantics is a generalization of final algebra semantics. First of all, a final algebra is always optimal.

Theorem 5.2. *If $\mathscr{K}$ has a final object F then F is optimal for $\mathscr{K}$.*

Proof. Suppose A is optimal for $\mathscr{K}$. The set $\{F\}$ is dense in $\mathscr{K}$. Therefore, by the definition of dense truth, every ground equation in F is densely true. However, by the definition of optimality, every densely true ground equation holds in the optimal algebra A. Therefore, $F \leqslant A$. Conversely, if $A \models e$ for a ground equation e then e is densely true in $\mathscr{K}$ and, hence, $F \models e$. Therefore, $A \leqslant F$. □

The fact that an optimal algebra always exists follows from the simple topological fact that the intersection of a finite collection of dense open sets is dense and open in any space [6].

Proposition 5.3. *Given a finite set $e_1, \ldots, e_k$ of densely true ground equations, and an equation e such that*

$$e_1, \ldots, e_k \vdash e,$$

by equational deduction, e is densely true.

Proof. Let $\mathscr{U} = \{A \in \mathscr{K} : A \models e_i \text{ for } 1 \leqslant i \leqslant k\}$. Then $\mathscr{U}$ is a finite intersection of open dense sets. Hence, $\mathscr{U}$ is dense and open. By the soundness of equational deduction, e holds everywhere in $\mathscr{U}$ and is, therefore, densely true. □

The main existence theorem for optimal algebras is a corollary of Proposition 5.3.

Theorem 5.4. *There is a unique optimal algebra for every $\mathscr{K}$.*

Proof. Let $\equiv$ be the relation on ground terms defined by

$$x \equiv y \text{ iff } x = y \text{ is densely true in } \mathscr{K}.$$

To see that $\equiv$ is a congruence, note that the congruence closure of an equational relation like $\equiv$ is the same as its deductive closure. The latter is $\equiv$ itself by Proposition 5.3 and by compactness, i.e., by the finiteness of proofs. Let $A = I_{\mathrm{EXT}}/\equiv$.

To show that A is optimal for $\mathscr{K}$, we only need to show that A respects the BASE. Let v_1 and v_2 be two T_{BASE} terms. If $A \models v_1 = v_2$, then the equation $v_1 = v_2$ is densely true. Therefore, there is a $B \in \mathscr{K}$ such that $B \models v_1 = v_2$. Since B respects the BASE, we see that $I_{\text{BASE}} \models v_1 = v_2$. Going the other way, if $I_{\text{BASE}} \models v_1 = v_2$ then, by the definition of an EXT-algebra, this equation is densely true (in fact, necessarily true) and, thus, $A \models v_1 = v_2$.

The uniqueness of A is immediate, since the definition of optimality completely specifies the true ground facts of the reachable Σ_{EXT}-algebra A. □

This result is quite "robust" in the sense that it depends only on the finiteness of equational proofs. Optimal models always exist, not only for purely equational specifications, but also for first-order specifications of any kind whatsoever for which a semantics based on ordered Kripke structures is appropriate. A simple example is specifications which use *conditional* equations. We have not explored other situations, but the results in the equational setting suggest that optimal models will be good vehicles for reasoning about many types of incomplete specifications.

Examples of optimal semantics for different choices of $\mathscr{K}$ are presented in Section 7. Before turning to examples, we discuss the question of adequacy of Kripke models. We have placed no restrictions on $\mathscr{K}$ whatsoever in the definition of optimal semantics or in Theorem 5.4. We show in the next section that a "completeness" condition is needed for $\mathscr{K}$ to establish a satisfactory connection between abstract properties and optimal models.

6. Complete Kripke models

There is a serious flaw in the connection between optimal semantics and abstract properties established in the last section. Most abstract properties of interest are *not* ground equations, and a nonground equation that holds in the optimal algebra is *not* guaranteed to be densely true in the corresponding Kripke structure. For instance, suppose e is a nonground equation such that an infinite number of its instances do not hold in I_{EXT}, but e is consistent with EXT. A good example is the "missing" equation

$$\mathsf{member}(x, \mathsf{empty}) = \mathsf{false}$$

for sets as specified in the introduction. Let $e_1, e_2, \ldots$ be an enumeration of the ground instances of e, and let

$$\mathscr{K} = \{I_{\text{EXT}}, I_{\text{EXT}}/|e_1|, I_{\text{EXT}}/|e_1, e_2|, \ldots, I_{\text{EXT}}/|e_1, \ldots, e_k|, \ldots\}$$

where $|e_1, \ldots, e_k|$ is the least congruence generated by the equations $e_1, \ldots, e_k$. Now, obviously, every ground instance of e is densely true in $\mathscr{K}$, but e itself holds in none of the algebras in $\mathscr{K}$. Proposition 5.3 guarantees that for any *finite* set of densely true ground equations, there is a dense set where all of the equations hold. For a proper connection between optimal semantics and abstract properties, we need a dense set of

algebras in which *all* the densely true ground equations hold. Specifically, one would expect the intersection of the truth sets for all densely true ground equations to be dense in $\mathscr{K}$.

Definition. A Kripke structure $\mathscr{K}$ is said to be *complete* exactly when the set

$$D_{\mathscr{K}} = \{A \in \mathscr{K} : \text{for all ground } e, \text{ if } \models_{\mathscr{K}} \Box \Diamond e, \text{ then } A \models e\}$$

is dense in $\mathscr{K}$.

This leads immediately to the desired connection between optimal algebras and abstract properties:

Lemma 6.1. *Suppose A is the optimal algebra for a complete Kripke model $\mathscr{K}$, and let e be an equation possibly containing variables. Then $A \models e$ iff e is densely true in $\mathscr{K}$.*

Proof. Every ground instance of e holds in every $B \in D_{\mathscr{K}}$ if $A \models e$. Since $\mathscr{K}$ is complete, $D_{\mathscr{K}}$ is dense in $\mathscr{K}$ and, so, e is densely true in $\mathscr{K}$. The converse is immediate from the definition of optimality. □

$D_{\mathscr{K}}$ is a countable intersection of dense open sets, but there is no reason to believe that this intersection is nonempty. As someone familiar with the Baire category theorem (BCT) might suspect, the example at the beginning of this section suggests a sufficient topological condition for this.

Definition. A poset $\langle X, \leqslant_X \rangle$ is *countably bounded* if every ω-sequence from X has an upper bound in X.

Countable boundedness is a rather weak hypothesis for a poset. It is trivially implied by directed completeness or even ω-chain completeness.

Proposition 6.2. *Every countably bounded X satisfies the BCT: the intersection of countably many dense open subsets of X is dense.*

Proof. The proof is a standard argument modeled on that of the BCT. Let D_i be dense open subsets for $i \in \omega$, and let $A \in X$. Define a sequence $\langle A_i : i \in \omega \rangle$ by recursion as follows: Let $A_0 = A$. Given A_i, let A_{i+1} be such that $A_i \leqslant A_{i+1}$ and $A_{i+1} \in D_i$. Let $B \geqslant A_i$ for all i. Then $B \geqslant A_0$. By construction, $B \in D_i$ for all i. Hence, $B \in \bigcap_i D_i$. □

Theorem 6.3. *Every countably bounded Kripke model is complete.*

Proof. This follows from the Proposition 6.2, since $D_{\mathscr{K}}$ is the intersection of the countable collection of sets where the densely true equations hold.

As a slight digression, countable boundedness also allows us to formalize the notion of an "approximation" for final algebras. A final algebra (when it exists) is the *maximal* point of $\mathscr{K}$, i.e., the algebra B such that for all $C \geqslant B$ from $\mathscr{K}$, $c \cong B$. Since an abstract (equational) property of a *complete* specification is exactly the one which holds in its unique maximal interpretation, it is natural to generalize by saying that an abstract property of an *arbitrary* specification is the one which holds in *all* its maximal interpretations. A *dense* set of maximal algebras is, therefore, an approximation for a final algebra since such a set captures the abstract properties of a specification in every sense. The next result shows that if $\mathscr{K}$ is countably bounded, then the set of maximal algebras is dense.

Lemma 6.4. *Let $\mathscr{K}$ be countably bounded, and let $A \in \mathscr{K}$. Then there exists some (not necessarily unique) $B \in \mathscr{K}$ such that $B \geqslant A$ and B is maximal.*

The proof is similar to that of Proposition 6.2. Note that every maximal algebra belongs to $D_{\mathscr{K}}$; so, Lemma 6.4 is a strengthening of Theorem 6.3. The maximal algebras in some sense form the *kernel* of $D_{\mathscr{K}}$ and the optimal algebra can be thought of as the intersection of the maximal algebras.

It is useful to consider another characterization of the relationship between optimality and completeness based directly on abstract properties. Consider the interpretations of EXT which have the property that all of the (not necessarily ground) equations true in them are abstract properties of EXT. The following is an equivalent definition.

Definition. An algebra A is *compatible (with $\mathscr{K}$)* is U_A is dense in $\mathscr{K}$.

Compatible algebras are in some sense "partial" optimal algebras. This intuition is confirmed by the following theorem.

Theorem 6.5. *Suppose A is compatible with $\mathscr{K}$. A is optimal for $\mathscr{K}$ iff A is final in the category of algebras which are compatible with $\mathscr{K}$.*

Proof. Assume that A is final among the algebras which are compatible with $\mathscr{K}$. Suppose also that a ground equation e is densely true in $\mathscr{K}$. Let $B = I_{\mathrm{EXT}}/|e|$. We show that B is compatible. Let $C \in \mathscr{K}$. By density, there is some $D \geqslant C$ such that $D \models e$. By initiality of B among the models of $\mathrm{EXT} \cup \{e\}$, $B \leqslant D$. This shows that B is compatible. By the finality of A, $B \leqslant A$. Therefore, $A \models e$.

Going the other way, suppose that A is optimal for $\mathscr{K}$. We want to show that A is a quotient of every algebra which is compatible with $\mathscr{K}$. Let B be compatible with $\mathscr{K}$. The morphism from B to A will be $B(t) \mapsto A(t)$. This is well-defined since $B \models t_1 = t_2$ implies that $(t_1 = t_2)$ is densely true (for ground t_1, t_2), as we have seen. Since our overall hypothesis is that A is compatible, this shows that A is the final compatible algebra. □

The reason why compatibility is interesting is the following result.

Theorem 6.6. *A Kripke structure $\mathscr{K}$ is complete iff the optimal algebra for $\mathscr{K}$ is compatible with $\mathscr{K}$.*

Proof. Let A be optimal for a complete $\mathscr{K}$. To see that A is compatible with $\mathscr{K}$, let B be any algebra in $\mathscr{K}$. Since $\mathscr{K}$ is complete, $D_{\mathscr{K}}$ is dense in $\mathscr{K}$. By density, there is a $C \in D_{\mathscr{K}}$ such that $B \leqslant C$. Then, by the definition of $D_{\mathscr{K}}$, $A \leqslant C$.

Now suppose that A is compatible with $\mathscr{K}$. Let B be any algebra in $\mathscr{K}$. By compatibility, there is a $C \in \mathscr{K}$ such that $A \leqslant C$ and $B \leqslant C$. By the optimality of A, $C \in D_{\mathscr{K}}$; so, $D_{\mathscr{K}}$ is dense in $\mathscr{K}$. □

We conclude this section with an example which demonstrates that there are "natural" Kripke models that turn out to be incomplete. Our example is the Kripke model consisting of the "finitary" algebras.

Definition. An algebra A is *finitary* iff there is a *finite* set E of Σ_A-equations such that $A \cong I_E$. Let $\mathscr{F}_{\text{EXT}}$ be the collection of finitary EXT-algebras.

Finitariness seems a natural condition since implementations must after all be computable, and in this context equational computation is the natural choice. Of course, finite axiomatization guarantees only semicomputability for the word problem, but allows all *necessary* observable results to be computed, which is what one really needs in an implementation.

Our negative result rests on the fact that there are algebras which can be specified as final algebras of finite specifications, but for which the word problem is not semicomputable; such an algebra is not finitary. More precisely, we state this as follows.

Lemma 6.7. *There is a specification* (BASE, EXT) *such that the category of* EXT*-algebras has a final object which is not semicomputable and, hence, not finitary.*

The standard example is a specification of polynomials in n variables (with $n \geqslant 14$). The result makes essential use of the celebrated theorem of Matijasevich, which proves that all recursively enumerable sets of natural numbers are diophantine, and, therefore, there are polynomials $p(x_0, x_1, \ldots, x_n)$ and $q(x_0, x_1, \ldots, x_n)$, with coefficients from N, such that the set of natural numbers

$$\{m: \forall a_1, \ldots, a_n,\ p(m, a_1, \ldots, a_n) \neq q(m, a_1, \ldots, a_n)\}$$

is not recursively enumerable. Since the details are quite complex and have no bearing on our argument, they are omitted here. The interested reader can find this and other related results in [7, 9].

The proof of the following lemma uses the connection between compatibility and completeness established in Theorem 6.6.

Lemma 6.8. *There is a specification* (BASE, EXT) *such that* $\mathscr{F}^{2}_{\text{EXT}}$ *is not complete.*

Proof. Let (BASE, EXT) be as in Lemma 6.7, and let F be the final EXT-algebra. We first show that F is not compatible with $\mathscr{F}_{\text{EXT}}$. If it were, there would be some $C \in \mathscr{F}_{\text{EXT}}$ such that $I_{\text{EXT}} \leqslant C$ and $F \leqslant C$, since I_{EXT} is finitary. But since F is final, $F \cong C$. Thus, F is finitary, and this contradicts Lemma 6.7.

We now claim that F is optimal for $\mathscr{F}_{\text{EXT}}$. Since F is final, it suffices to show that $F \models e$ implies that e is densely true. Suppose $F \models e$. Consider an arbitrary $B \in \mathscr{F}_{\text{EXT}}$, and let E be the finite axiomatization of B. Let $C = B/|e|$. C respects the BASE since $C \leqslant F$. Moreover, C is finitary since $E \cup \{e\}$ is a finite axiomatization of it. Therefore, $C \in \mathscr{F}_{\text{EXT}}$ and $C \models e$. This shows that the optimal algebra for $\mathscr{F}_{\text{EXT}}$ is not compatible with $\mathscr{F}_{\text{EXT}}$. Therefore, by Theorem 6.6, $\mathscr{F}_{\text{EXT}}$ is not complete. □

In fact, it is not hard to see that $D_{\mathscr{K}}$ is empty if $\mathscr{K} = \mathscr{F}_{\text{EXT}}$ for the specification (BASE, EXT) mandated by Lemma 6.7.

7. Examples

In this section we consider two Kripke models which have been used in observable semantics [10, 5]: the classes of all and all *standard* algebras. The class of all (reachable) algebras is perhaps the most obvious Kripke structure for observable semantics, as reflected in the fact that the traditional final algebra approach is based on this class. However, in more recent work, the smaller class of standard algebras has been found to be a useful basis for reasoning methods for incomplete specifications [5]. In particular, as we illustrate with examples below, a class of "inductive theorems" arises naturally relative to the standard algebras but not in the larger structure of all reachable algebras. In some ways, therefore, the standard algebras yield a "better" Kripke model in that the corresponding optimal semantics appears to validate more of the natural properties of a specification (when it is reasonable to assume that all implementations must be standard). It is conceivable that other classes will be found to be useful in future work. This was the reason why we chose to work with the natural parameterization of optimal semantics with respect to Kripke structures.

7.1. Optimal normal semantics

Our first example of a Kripke structure for optimal semantics is the class $\mathscr{R}$ of all EXT-algebras – the class usually used in final algebra semantics. $\mathscr{R}$ is complete. We call the corresponding optimal model the *optimal normal algebra.*

[2] It can be shown that Lemma 6.8 also holds for the Kripke model of "recursive" algebras (in a recursive algebra the "word problem" is recursive). The proof is much more complicated, and beyond our scope.

Lemma 7.1. *For every specification pair* (BASE, EXT), *the structure* $\mathscr{R}_{\text{EXT}}$ *is complete.*

Proof. Apply Theorem 6.3. It is no easier to check countable boundedness than the stronger property of directed completeness; so let $\mathscr{D}$ be any nonempty directed subset of $\mathscr{R}$. Let $\equiv$ be the following congruence on T_{EXT}:

$$t \equiv u \text{ iff for some } B \in \mathscr{D},\ B(t) = B(u).$$

The fact that $\mathscr{D}$ is directed implies that this relation $\equiv$ is indeed a congruence. Since $\mathscr{D}$ is nonempty, the equations EXT are satisfied.

Let $L = T_{\text{EXT}}/\equiv$. We need to show that L respects the BASE. This is a compactness argument, almost identical to the one found in the proof of Theorem 5.4. □

Example 7.2. Consider an extended version of the incomplete specification for sets in Section 1. Suppose we have the operations

$$\mathsf{add}: \mathsf{item} \times \mathsf{set} \to \mathsf{set}$$

$$\mathsf{union}: \mathsf{set} \times \mathsf{set} \to \mathsf{set}$$

$$\mathsf{empty}: \to \mathsf{set}$$

$$\mathsf{universe}: \to \mathsf{set}$$

$$\mathsf{member}: \mathsf{item} \times \mathsf{set} \to \mathsf{bool}$$

$$\mathsf{subset}: \mathsf{set} \times \mathsf{set} \to \mathsf{bool}$$

with the equations

$$\mathsf{member}(x, \mathsf{add}(y, s)) = \mathsf{equal}(x, y) \vee \mathsf{member}(x, s)$$

$$\mathsf{subset}(\mathsf{empty}, s) = \mathsf{true}$$

$$\mathsf{subset}(\mathsf{add}(x, s_1), s_2) = \mathsf{member}(x, s_2)\ \&\ \mathsf{subset}(s_1, s_2)$$

This specification is seriously incomplete because the observable behavior of three operations (empty, universe and union) is not specified. Nonetheless, every ground instance of the equations

$$\mathsf{add}(x, \mathsf{add}(y, s)) = \mathsf{add}(y, \mathsf{add}(x, s))$$

$$\mathsf{add}(x, \mathsf{add}(x, s)) = \mathsf{add}(x, s)$$

is consistent with every reachable algebra for the specification (and, therefore, densely true in $\mathscr{R}$). This is a consequence of the single equation for the member operation and the usual properties (commutativity and idempotence) of the boolean $\vee$ operation. These two abstract properties, therefore, hold in the optimal normal algebra. In the optimal algebra, ground terms of the form member(x, empty), member(x, universe) and member(x, union(s_1, s_2)) (among others) are interpreted as new values of sort bool. The optimal normal algebra is, therefore, not standard (it respects but does not

preserve the base sort bool). This is neither surprising nor problematic. The optimal algebra is not an ideal implementation – it is the repository of abstract properties that will hold no matter how the specification is implemented. As in the introduction, it is best to think of such properties as program transformations guaranteed to produce no observable effects. The optimal semantics can also be represented by the dense subset of $\mathscr{R}$ consisting of the final algebras corresponding to every possible *complete* set of decisions regarding the observable behavior of the three unspecified operations. If the equation "member(3, empty) = true" is added to EXT, the algebras in which the contrary equation holds will drop out of $\mathscr{R}$ and the dense set of candidate final algebras will be thinned accordingly. The incremental accretion of abstract properties can be illustrated by adding equations to the specification above. For instance, if the equation

$$\mathsf{member}(x, \mathsf{universe}) = \mathsf{true}$$

is added, then the property

$$\mathsf{add}(x, \mathsf{universe}) = \mathsf{universe}$$

holds in the corresponding optimal normal algebra. Similarly, if the equation

$$\mathsf{member}(x, \mathsf{union}(s_1, s_2)) = \mathsf{member}(x, s_1) \vee \mathsf{member}(x, s_2)$$

is added then the property

$$\mathsf{union}(\mathsf{add}(x, s_1), s_2) = \mathsf{add}(x, \mathsf{union}(s_1, s_2))$$

holds in the optimal normal algebra. Note that the specification is still incomplete because it lacks a specification for the behavior of empty.

7.2. Optimal standard semantics

Next we consider the Kripke model $\mathscr{S}_{\text{EXT}}$ of all *standard* EXT-algebras. Its main interest is in validating additional "inductive" properties (often in single-sorted specifications) which are based on the assumption that all observable values in a model must be reachable with BASE operators alone. $\mathscr{S}_{\text{EXT}}$ inherits bounded completeness (and directed completeness) from $\mathscr{R}$, since it is an open subset of $\mathscr{R}$. The completeness of $\mathscr{S}_{\text{EXT}}$ (Lemma 7.3) is, therefore, a consequence of Theorem 6.3 and the proof of Lemma 7.1. The optimal algebra for $\mathscr{S}_{\text{EXT}}$ is called the *optimal standard algebra.*

Lemma 7.3. *For every specification pair* (BASE, EXT), *the structure* $\mathscr{S}_{\text{EXT}}$ *is complete.*

We illustrate the applications of the optimal standard model with two examples. The specifications in the first part of Examples 7.4 and 7.5 are taken from [1].

Example 7.4. Suppose $\Sigma_{\text{BASE}} = \{\text{true}, \text{false}\}$ and BASE $= \emptyset$. Let EXT add a new operator not and the equation

$$\text{not}(\text{true}) = \text{false}$$

The value of not(false) is left unspecified. It is easy to see that the equation

$$\text{not}(\text{not}(\text{not}(x))) = \text{not}(x)$$

holds in the optimal standard algebra. The "induction" here is simple – there are only two standard algebras corresponding to the two choices for not(false). The equation does *not* hold in the optimal normal algebra which contains an infinite number of new "truth values" corresponding to multiple applications of not to false. Note that the optimal standard algebra is not itself standard – not(false) is interpreted as a new boolean value since neither standard choice is densely true. To repeat a point made in the context of Example 7.2, an optimal algebra is not an implementation. The point of choosing the $\mathscr{S}_{\text{EXT}}$ structure is that it is possible to validate additional properties when an implementation is required to be standard, and the optimal standard algebra captures these properties.

As a more complex example of the same kind, consider the case where $\Sigma_{\text{BASE}} = \{\text{true}, \text{false}, \wedge, \vee\}$. Let BASE contain the ground equations for the classical two-valued truth table for conjunction and disjunction. Suppose that EXT adds a single truth value U of sort bool, but no new equations. There is no final object in $\mathscr{S}_{\text{EXT}}$ (or in $\mathscr{R}$) since the specification of U is incomplete. If it is reasonable to make the assumption that U is "actually" one of the two standard truth values, then $\mathscr{S}_{\text{EXT}}$ is the appropriate Kripke model. There are again only two standard algebras; so, it is easy to compute the optimal standard semantics, which turns out to be the usual strong three-valued logic (without negation). That is, the interpretation of bool is exactly the set $\{\text{true}, \text{false}, \text{U}\}$, and the usual operations are extended by the equations

$$\text{true} \wedge \text{U} = \text{U}, \qquad \text{false} \wedge \text{U} = \text{false}, \qquad \text{U} \wedge \text{U} = \text{U}$$

$$\text{true} \vee \text{U} = \text{true}, \qquad \text{false} \vee \text{U} = \text{U}, \qquad \text{U} \vee \text{U} = \text{U}$$

In addition, $\wedge$ and $\vee$ are commutative. The equations above hold in the optimal standard algebra because they are independent of whichever truth value U may turn out to be. $\mathscr{S}_{\text{EXT}}$ is not adequate to capture the traditional idea (following Kleene) that U represents *divergent* computation. For instance, if the BASE contains negation ($\neg$) with its usual truth table, the expected equation $\text{U} = \neg\,\text{U}$ fails to hold in the optimal standard model. A proper representation of divergence seems to require a Kripke model of *ordered* algebras rather than standard ones.

This example again illustrates the difference between optimal normal and optimal standard semantics. None of the equations of three-valued logic hold in the optimal *normal* algbebra. To show this, we employ a somewhat contrived EXT-algebra B. The universe of B has the three truth values $\{\text{true}, \text{false}, \text{U}\}$. The operations $\wedge$ and $\vee$ are defined according to Tables 1 and 2.

Table 1

$\wedge$	true	false	U
true	true	false	false
false	false	false	true
U	true	false	true

Table 2

$\vee$	true	false	U
true	true	true	false
false	true	false	false
U	true	true	false

Every equation e which is incompatible with B – in the sense that there is no algebra C such that $C \geqslant B$ and $C \models e$ – is false in the optimal normal algebra, and this includes all of the equations of three-valued logic. The associative and commutative laws also fail for both operations.

Example 7.5. For an example that requires true (structural) induction, consider $\Sigma_{\text{BASE}} = \{0, \text{succ}\}$ for sort Nat, and BASE $= \emptyset$. Let EXT add the sort set (of Nat) with the operations

$$\text{min} : \text{Nat} \times \text{Nat} \to \text{Nat}$$

$$\text{least} : \text{set} \to \text{Nat}$$

$$\text{empty} : \to \text{set}$$

$$\text{add} : \text{Nat} \times \text{set} \to \text{set}$$

and the equations

$$\text{min}(0, x) = 0$$

$$\text{min}(x, 0) = 0$$

$$\text{min}(\text{succ}(x), \text{succ}(y)) = \text{succ}(\text{min}(x, y))$$

$$\text{least}(\text{add}(x, \text{empty})) = x$$

$$\text{least}(\text{add}(x, \text{add}(y, s))) = \text{min}(x, \text{least}(\text{add}(y, s)))$$

The value of least(empty) is meaningless and, more importantly, unspecified. The specification is, therefore, incomplete. Nonetheless, the optimal standard semantics displays most of the properties the specification is intended to capture. For instance, the property

$$\text{least}(\text{add}(0, s)) = 0$$

holds in the optimal standard algebra since the choice of a natural number for the value of least(empty) has no effect. The equation can be proved mechanically by induction over s. This property actually holds in the optimal normal algebra as well. However, the equation

$$\text{min}(x, y) = \text{min}(y, x)$$

holds in the optimal standard but not in the optimal normal semantics. The reason is that the carrier of sort Nat is reachable with 0 and succ in any standard algebra;

hence, the property can be shown to hold in all such algebras by induction. However, it is perfectly possible for the equations

$$\mathsf{min}(\mathsf{succ}(\mathsf{least}(\mathsf{empty})), \mathsf{least}(\mathsf{empty})) = \mathsf{succ}(0)$$

$$\mathsf{min}(\mathsf{least}(\mathsf{empty}), x) = 0$$

to hold in some (unintended) reachable algebra where least(empty) is a nonstandard natural number. Consequently, equations such as

$$\mathsf{add}(x, \mathsf{add}(x, s)) = \mathsf{add}(x, s)$$

$$\mathsf{add}(x, \mathsf{add}(y, s)) = \mathsf{add}(y, \mathsf{add}(x, s))$$

hold in the optimal standard but not in the optimal normal algebra.

8. Conclusions

The main conceptual point of this paper is that natural concepts of modality are useful in giving semantics of algebraic specifications. We used the modality of *on a dense open set* to define the optimal semantics. This modality is analogous to *with probability 1* or *for all sufficiently large*; they all capture the intuition of *almost always*. There are many situations where this modality is more useful than *always*. There are many situations where this modality is more useful than *always*, and the semantics of incomplete specifications seems to be yet another one.

Optimal semantics arises naturally when modality is incorporated in the very language of specification. The basis is the classification of formulas in Lemma 4.1, which also suggests that there are no other semantic approaches based on explicit modalities besides the initial, the final, and the optimal. Our use of classes of models as Kripke structures is new though perhaps obvious because EXT-algebras are very much the possible worlds of a specification.

The contrast between initial and final semantics can be seen as a contrast between the extensional and intensional approaches to semantics. Optimal semantics is a complete realization of the intentional approach in that it is a universally applicable proper generalization of finality.

Although our results were based on the use of equational specifications, our conceptual points hold for more powerful semantic methods. The optimal model exists for specifications based on conditional equations, or even first-order logic.

Acknowledgment

We thank the (anonymous) referee for spotting a number of errors and infelicities, and for forcing us to improve the examples substantially. One of us (Satish Thatte) would like to thank Vaughan Pratt for an E-mail discussion that helped crystallize a very early version of some of the ideas presented here.

References

[1] S.J. Garland and J.V. Guttag, Inductive methods for reasoning about abstract data types, in: *Proc. 15th POPL Symp.* (ACM Press, New York, 1988) 219–228.
[2] J.A. Goguen, J.W. Thatcher, E.G. Wagner and J.B. Wright, An initial algebra approach to the specification, correctness, and implementation of abstract data types, in: R.T. Yeh, ed., *Current Trends in Programming Methodology IV* (Prentice-Hall, Englewood Cliffs, NJ, 1978).
[3] J.V. Guttag and J.J. Horning, The algebraic specification of abstract data types, *Acta Inform.* **10**(1) (1978) 27–52.
[4] S. Kamin, Final data types and their specifications, *ACM TOPLAS*, **5**(1) (1983) 97–121.
[5] D. Kapur and D.R. Musser, Inductive reasoning with incomplete specifications, in: *Proc. Symp. on Logic in Computer Science* (1986) 367–377.
[6] J.L. Kelley, *General Topology* (Springer-Verlag, Berlin, 1975).
[7] J. Meseguer and J.A. Goguen, Initiality, induction, and computability, in: M. Nivat and J.C. Reynolds, eds., *Algebraic Methods in Semantics* (Cambridge University Press, Cambridge, 1985) 184–197.
[8] R. Milner, Fully abstract models of typed λ-calculi, *Theoret. Comput. Sci.* **4** (1977) 1–22.
[9] L.S. Moss, J. Meseguer, and J.A. Goguen, Final algebras, cosemicomputable algebras, and degrees of unsolvability, *Theoret. Comput. Sci.* **100** (1992) 267–302.
[10] M. Wand, Final algebra semantics and data type extensions, *J. Comput. System Sci.* **19**(1) (1977) 27–44.