Under consideration for publication in Math. Struct. in Comp. Science

Behavioral Reasoning for Conditional Equations[†]

MANUEL A. MARTINS[1] and DON PIGOZZI[2]

[1] *Department of Mathematics, University of Aveiro, 3810-193 Aveiro, Portugal*
martins@mat.ua.pt
[2] *Department of Mathematics, Iowa State University, Ames, IA 50011, USA*
dpigozzi@iastate.edu

Received 23 April 2003; Revised 12 April 2007

Abstract. Object oriented (OO) programming techniques can be applied to equational specification logics by distinguishing *visible* data from *hidden* data (i.e., by distinguishing the output of methods from the objects to which the methods apply), and then focusing on the behavioral equivalence of hidden data in the sense introduced by H. Reichel in 1984. Equational specification logics structured in this way are called *hidden equational logics*, HEL's. The central problem is how to extend the specification of a given HEL to a specification of behavioral equivalence in a computationally effective way. S. Buss and G. Roşu showed in 2000 that this is not possible in general, but much work has been done on the partial specification of behavioral equivalence for a wide class of HEL's. The OO connection suggests the use of coalgebraic methods, and J. Goguen and his collaborators have developed coinductive processes that depend on an appropriate choice of a *cobasis*, a special set of contexts that generates a subset of the behavioral equivalence relation. In this paper the theoretical aspects of coinduction are investigated, specifically its role as a supplement to standard equational logic for determining behavioral equivalence. Various forms of coinduction are explored. A simple characterization is given of those HEL's that are behaviorally specifiable. Those sets of conditional equations that constitute a complete, finite cobasis for a HEL are characterized in terms of the HEL's specification. Behavioral equivalence, in the form of logical equivalence, is also an important concept for single-sorted logics, e.g., sentential logics such as the classical propositional logic. The paper is an application of the methods of the extensive work that has been done in this area to HEL's, and to a broader class of logics that encompasses both sentential logics and HEL's.

Keywords: Specification logic, behavioral equivalence, behavioral validity, hidden algebra, equational logic, abstract algebraic logic, Leibniz congruence.

[†] Research partially supported by *Fundação para a Ciência e a Tecnologia* (Portugal) through *Unidade de Investigação Matemática e Aplicações* of University of Aveiro and NSF grant CCR-9803843.

1. Introduction

Equational logic serves as the underlying logic in many formal approaches to program specification. The algebraic data types specified in this formal way can be viewed as abstract machines on which the programs are to be run. This is one way of giving a precise algebraic semantics for programs, against which the correctness of a program can be tested. Object oriented (OO) programs however present a special challenge for equational methods. A more appropriate model for the abstract machine in the case of an OO program is, arguably, a state transition system: like a state of such a system, a state of an OO program can be viewed as encapsulating all pertinent information about the abstract machine when it reaches the state during execution of the program. As a way of meeting this challenge the standard equality predicate can be augmented by *behavioral equivalence*; in this way many of the characteristic properties of state transition systems can be grafted onto equational logic.

In this approach the data are partitioned into *visible* and *hidden* parts, with the latter representing the objects in the object-oriented paradigm. Procedures that take hidden data as input (the methods associated with an object) are assumed to output only visible data. Hidden data can be only indirectly compared by comparing the outputs of the procedures. Two hidden data elements are *behaviorally equivalent* if every procedure returns the same value when executed with either of the data elements as input. In formalizing the equational logic intended to specify behavioral equivalence, only equations and conditional equations between visible terms are used in axiomatizing the logic since only visible data are used to define behavioral equivalence. Such logics are referred to as *hidden equational logics*, or HEL's. Here we follow (Goguen and Malcolm 2000) in the choice of the descriptive term "hidden".

The central problem is how to specify behavioral equivalence in a computationally effective way, more precisely, how to do this for behavioral validity. An equation is said to be *behaviorally valid* over a given HEL $\mathcal{L}$ if its left- and right-hand sides are behaviorally equivalent under all possible interpretations in the models of $\mathcal{L}$. A natural extension of this idea gives a corresponding notion of the behavioral validity of a conditional equation. It is known that this problem is not solvable in general. More specifically, (Buss and Roşu 2000) give an example of a hidden equational logic defined by a finite number of equations and conditional equations with the property that the set of behaviorally valid equations (and hence in particular the set of behaviorally valid conditional equations) fails to be either recursively enumerable (RE) or co-RE. So attention has been focused on partial solutions to the problem.

The analogy between hidden equational logic and state-transition systems suggests the use of coalgebraic methods in the verification of behavioral validity, and indeed various forms of coinduction in combination with standard techniques of equational logic have been developed for this purpose. See (Bouhoula and Rusinowitch 2002; Goguen and Malcolm 1999; Goguen and Malcolm 2000; Roşu 2000; Roşu and Goguen 2000; Roşu and Goguen 2001; Goguen et al. 2002). More abstract studies of the behavioral equivalence and validity relations can be found in (Bidoit and Hennicker 1996; Hennicker 1997).

Research in the area has generally focused on computationally effective coinductive

and specialized rewriting techniques that can serve as the basis of special languages that support automated behavioral reasoning. (Bouhoula and Rusinowitch 2002) propose an automatic method for proving behavioral validity of conditional equations in conditional specifications based on the fact that there are specifications for which a small set of contexts, called *critical contexts* is sufficient to determine behavioral validity. This is the genesis of the SPIKE language (Berreged et al. 1998), which uses context induction (see `http://www.loria.fr/bouhoula/spike.html`). The language CafeOBJ was developed by (Diaconescu and Futatsugi 1998) (`http://www.ldl.jaist.ac.jp/Research/CafeOBJ/`). It implements behavioral rewriting to make behaviorally sound reductions of terms, and is based on a behavioral version of the well known efficient method of rewriting for automated theorem proving.

Joseph Goguen and his collaborators have developed coinductive algorithms that depend on an appropriate choice of a *cobasis*, a special set of contexts that generates a subset of the behavioral equivalence relation. Those algorithms have been implemented in the language BOBJ (Lin et. al. 2000). (Roşu and Goguen 2001) present a new technique which combines behavioral rewriting and coinduction (see also (Lin et. al. 2000)). The most recent version is CCCRW, called *conditional circular coinductive rewriting with case analysis* (Goguen et al. 2002).

In contrast our work is more theoretical, like that of (Buss and Roşu 2000; Bidoit and Hennicker 1996; Hennicker 1997). We investigate the theoretical aspects of coinduction and its role as a supplement to standard equational logic for determining behavioral equivalence. We explore the various forms coinduction can assume and how they interact with the deductive process of standard equational logic. In order to do this properly we must first describe in some detail the underlying logical formalism and precisely define within that context what behavioral equivalence is. Although the work here may eventually lead to computationally effective ways of determining behavioral equivalence in practical situations, this is not one of our goals and we do not explore the possibility.

There are some consequences of this aspect of our work, setting it apart from others in the area, that we feel compelled to mention because they have proved somewhat controversial. Various examples of HEL's and other kinds of logics are given illustrating our theoretical results, and we have purposely chosen simple, some would say trivial, examples because these best serve our purpose. The example of stacks of natural numbers is one whose familiarity seems to have bred contempt in some quarters, but it is just this familiarity that makes it well suited for our purpose. More complex examples would be appropriate only if we were presenting case studies for specific deductive algorithms.

Another controversial aspect of our work is the requirement that axioms refer only to visible data. For example, in axiomatizing stacks of natural numbers we chose the infinite set of visible axioms $top(pop^{n+1}(push(x,s))) \approx top(pop^n(s))$, for all natural numbers n, instead of the familiar single, hidden axiom $pop(push(x,s) \approx s$. Given the object oriented paradigm guiding us, this is the only coherent choice. Hidden objects can only be specified in terms of the data the applicable methods return, and these are necessarily visible. A simpler axiomatization can of course be obtained by replacing the infinitely many hidden equations with the single hidden one, but to assure this replacement is

sound, the behavioral validity of $pop(push(x, s) \approx s$ must first be verified by some means using the original axiom system.

The authors came to this project with a background in algebraic logic, more precisely abstract algebraic logic, an area of mathematical logic that has been quite active recently. (For surveys of the subject see (Font et al. 2003; Pigozzi 2001).) Roughly speaking *abstract algebraic logic* (AAL) is the study of the relation between logical *assertion* (i.e, asserting that a sentence is logically *true*) and logical *equivalence* (asserting that two sentences are logically equivalent). Historically logics, like the classical propositional logic (CPL), have been formalized as one-sorted assertional systems, i.e., *sentential logics*, and it turns out that in such systems logical equivalence can be characterized precisely as behavioral equivalence. In CPL behavioral (i.e., logical) equivalence is defined by a explicit logical connective, the biconditional $\leftrightarrow$, but in arbitrary sentential logics it has to be captured by other means, and this essentially is the subject matter of AAL. In this paper we apply the methods of AAL to HEL's and to a broader class of logics that encompasses both sentential logics and HEL's.

The special feature of this approach is the characterization of behavioral equivalence as a congruence relation on the term algebra of a special kind (called the *Leibniz congruence* in AAL). This congruence has been used before in hidden equational logic (Roşu and Goguen 2000; Roşu and Goguen 2001), but plays a greatly expanded role in our work. The role that algebraic data structures traditionally play in hidden equational logic is in large part supplanted by the theory of the Leibniz congruence. This this gives our work a distinctive combinatorial flavor that, in our view, adds much to the understanding of the subject.

1.1. *Description of contents of paper*

A large part of our theory applies to a much more general class of logical systems than hidden equational logics. In the first part of Section 2 we define the notion of a hidden k-logic. The elementary part of its semantics is developed in Section 2.2.

Hidden k-logics encompass not only the hidden and standard equational logics, but also Boolean logics (i.e., multi-sorted logics with a Boolean sort in place of equality predicates). They also comprehend sentential logics, the purview of abstract algebraic logic. In Section 2.3 we specialize to the hidden equational logics (HEL's) and present several representative examples of HEL's and an example of a hidden 3-logic (Example 2.11).

The standard definition of behavioral equivalence of elements of an hidden algebra (in terms of contexts), is given in Section 2.4, and followed by the generalization of the notion to k-data structures, the natural models of hidden k-logics. The next section, 2.5, is a brief detour into abstract algebraic logic where we define the Leibniz congruence and develop some of its basic properties. We also present in this section a general version of the completeness theorem for HEL's that involves some special hidden algebras that are defined in terms of the Leibniz congruence.

The core of the paper is found in Section 3. We give precise definitions of behaviorally valid equations and conditional equations over a hidden k-logic and as a special case a HEL. In the main lemma of the paper, (Theorem 3.4), behavioral validity is characterized

in terms of combinatorial properties of Leibniz congruences on the term algebra; this characterization can be viewed as the most abstract form of coinduction for conditional equations, and all subsequent results of the paper derive from it.

In Section 3.1 we prove that all members of a set of conditional equations E are behaviorally valid over a HEL if and only if every conditional equation with visible consequent that is derivable using E as a set of additional inference rules is already derivable without the aid of E (Theorem 3.10). This gives an alternative form of coinduction for conditional equations that uses only standard equational logic. It generalizes in a natural way a similar result in (Leavens and Pigozzi 2002, Theorem 3.18) for equations. As a consequence (Corollary 3.13) we get that the set of conditional equations that are behaviorally valid over a HEL is closed under equational consequence in the sense that any conditional equation that is derivable using any set of behaviorally valid conditional equations as additional rules is itself behaviorally valid. Thus coinduction (in either one of its two alternative forms mentioned above) remains sound as well as complete with respect to behavioral validity when augmented by the standard deductive apparatus of equational logic. This turns out to be especially useful in the case of behaviorally specifiable HEL's (see following paragraph) for which there are just a few behaviorally valid equations and conditional equations that, once their behavioral validity is verified in some way, for example by coinduction, can be used to derive all other behavioral validities by means of standard equational logic. An example of the use of this technique for establishing the behavioral validity of equations can be found in (Leavens and Pigozzi 2002).

In Section 3.2 we apply the results of the previous sections to the theory of cobases. Roughly speaking, a *cobasis* (in the sense of (Roşu and Goguen 2001)) is a collection of possibly infinite conditional equations (i.e., each conditional equation has possibly an infinite number of conditions), that when adjoined as new inference rules to those of a specifiable HEL is sound with regard to behavioral validity; a cobasis is called *finite* if each conditional equation has only a finite number of conditions. As indicated earlier in the Introduction, the search for effective cobases has played an important part in the research on behavioral equivalence. We call a HEL, more generally any hidden k-logic, *behaviorally specifiable* if there is a finite cobasis that is complete, as well as sound, for the HEL. According to (Buss and Roşu 2000), not every specifiable HEL is behaviorally specifiable. The main result of Section 3.2 is a simple characterization of those HEL's that are behaviorally specifiable. More specifically, we characterize, entirely in terms of the underlying equational logic of the HEL, those sets of conditional equations that constitute a complete, finite cobasis. (See Theorems 3.19, 3.20, and the remarks following Definition 3.21.) These such cobases turn out to be the analogue of so-called *finite equivalence systems* of abstract algebraic logic.

If $\mathcal{L}$ has an equivalence system, then every conditional equation can be transformed into a set of visible conditional equations with possibly infinitely many conditions such that the original conditional equation is behaviorally valid if and only if each of its transforms is derivable in $\mathcal{L}$; in the case of a finite equivalence system, the set of transforms is finite and each is a standard conditional equation (Theorem 3.22). This result can be useful in practice since many HEL's have equivalence systems and even finite equivalence systems.

2. Hidden Logics

From the beginning, we distinguish visible and hidden data by separating the set of sorts in two parts, visible and hidden, in the definition of signature.

A *hidden* (*sorted*) *signature* is a triple

$$\Sigma = \big\langle \mathrm{SORT}, \mathrm{VIS}, \langle \mathrm{OP}_\tau : \tau \in \mathrm{TYPE} \rangle \big\rangle,$$

where SORT is a nonempty, countable set whose elements are called *sorts*, VIS is a subset of SORT, called the set of *visible sorts*, TYPE is a set of nonempty sequences $S_0, \ldots, S_n$ of sorts, called *types*, and, for each $\tau \in \mathrm{TYPE}$, OP_τ is a countable set of operation symbols of type τ. Those sorts in $\mathrm{SORT} \setminus \mathrm{VIS}$, that are not visible, are called *hidden sorts*. The set of hidden sorts is denoted by HID. A hidden signature Σ is said to be *standard* if there is a ground term of every sort.

From each hidden signature Σ we obtain the associated *un-hidden* signature Σ^{UH} by making all sorts of Σ visible.

$$\Sigma^{\mathrm{UH}} = \big\langle \mathrm{SORT}, \mathrm{SORT}, \langle \mathrm{OP}_\tau : \tau \in \mathrm{TYPE} \rangle \big\rangle.$$

By a SORT-*sorted set*, or just a *sorted set* when SORT is clear from context, we mean a sequence $A = \langle\, A_S : S \in \mathrm{SORT} \,\rangle$ indexed by SORT. A sorted set A is *locally countable* (*finite*), if for every sort S, A_S is a countable (finite) set.

A Σ-*algebra* is a pair

$$\big\langle\, A, \langle\, \sigma^A : \tau \in \mathrm{TYPE}, \sigma \in \mathrm{OP}_\tau \rangle \,\big\rangle,$$

where A is SORT-sorted set and σ^A is an operation on A of type τ. As customary we use the same symbol to denote an algebra and the the carrier of the algebra. We assume in addition that the domain A_S is nonempty for each sort S. This simplifies the logical arguments, and all results of the paper extend *mutatis mutandis* to the more general case. An algebra A is *locally countable* (*finite*) if its carrier set is locally countable (finite). To simplify notation and terminology we occasionally identify, when no confusion seems likely, an sorted set such as $\langle A_S : S \in \mathrm{SORT} \,\rangle$ with the corresponding unsorted set $\bigcup_{S \in \mathrm{SORT}} A_S$.

Let $X = \langle X_S : S \in \mathrm{SORT} \rangle$ be a fixed locally countable sorted set of variables. We define the sorted set $\mathrm{Te}_\Sigma(X)$ of terms over the signature Σ as usual. We use the lower case Greek letters $\varphi, \psi, \vartheta, \ldots$ to represent terms, possibly with annotations to indicated sort and variables. Specifically, writing φ in the form

$$\varphi(x_1{:}T_1, \ldots, x_n{:}T_n){:}S \tag{1}$$

indicates that φ is of sort S and that the variables that actually occur in φ are included in the list $x_1, \ldots, x_n$ of sort $T_1, \ldots, T_n$, respectively.

We define, in the usual way, operations over $\mathrm{Te}_\Sigma(X)$ to obtain the *term algebra* over the signature Σ (also denoted by $\mathrm{Te}_\Sigma(X)$). It is well known that $\mathrm{Te}_\Sigma(X)$ has the *universal mapping property* over X in the sense that, for every Σ-algebra A and every sorted map $h : X \to A$, called an *assignment*, there is a unique sorted homomorphism $h^* : \mathrm{Te}_\Sigma(X) \to A$, which extends h. In the sequel we will not distinguish between these two maps. If φ

is the term (1), and $a_i \in A_{T_i}$, we write $\varphi^A(a_1, \ldots, a_n)$ for the image $h(\varphi)$ under any homomorphism h such that $h(x_i) = a_i$ for all i.

A map from X to the set of terms, and its unique extension to an endomorphism of $\mathrm{Te}_\Sigma(X)$, is called a *substitution*. Substitutions are represented by the Greek letters $\sigma, \tau, \ldots$. Since X is assumed fixed throughout the paper, we normally write Te_Σ in place of $\mathrm{Te}_\Sigma(X)$.

To provide a context that allows us to deal simultaneously with specification logics that are assertional (for example ones with a Boolean sort but no equality) and equational, we introduce the notion of a k-formula for any nonzero natural number k. A *k-formula* of sort S over Σ is a sequence of k Σ-terms all of the same sort S. We indicate k-formulas by overlining, so $\bar{\varphi}{:}S = \langle \varphi_0{:}S, \ldots, \varphi_{k-1}{:}S \rangle$. When we do not need to make the common sort S of each term of $\bar{\varphi}{:}S$ explicit, we simply write it as $\bar{\varphi}$. Te^k_Σ is the sorted set of all k-formulas over Σ. Thus $\mathrm{Te}^k_\Sigma = \langle (\mathrm{Te}_\Sigma)^k_S : S \in \mathrm{SORT} \rangle$. The set of all visible k-formulas $(\mathrm{Te}^k_\Sigma)_{\mathrm{VIS}}$ is the VIS-sorted set $\langle (\mathrm{Te}_\Sigma)^k_V : V \in \mathrm{VIS} \rangle$. More generally, for any subset $\mathcal{S}$ of sorts and any sorted set A, $A_\mathcal{S}$ denotes the $\mathcal{S}$-sorted set $\langle A_S : S \in \mathcal{S} \rangle$.

The paradigm for 1-formulas are Boolean terms over an arbitrary hidden signature with a Boolean sort (the only visible sort). The main examples of 2-formulas are the equations of free hidden equational logic over any hidden signature Σ (free HEL_Σ) considered below (Definition 2.6); here the equation $\phi \approx \psi$ is identified with the 2-formula $\langle \phi, \psi \rangle$. Higher dimension formulas are less common but not unnatural. For example, in a signature for reasoning about certain kinds of sets, the set containment relation $\vartheta \in [\varphi, \psi]$ can be identified with the 3-formula $\langle \vartheta, \varphi, \psi \rangle$.

If A is a Σ-algebra and $\bar{\varphi}(x_1{:}T_1, \ldots, x_n{:}T_n)$ is a k-formula and $a_1 \in A_{T_1}, \ldots, a_n \in A_{T_n}$, then we denote by $\bar{\varphi}^A(a_1, \ldots, a_n)$ the value $\bar{\varphi}$ takes in A when the variables $x_1, \ldots, x_n$ are interpreted respectively by $a_1, \ldots, a_n$. More precisely, if

$$\bar{\varphi}(x_1, \ldots, x_n) = \langle \varphi_1(x_1, \ldots, x_n), \ldots, \varphi_k(x_1, \ldots, x_n) \rangle,$$

then $\bar{\varphi}^A(a_1, \ldots, a_n) = h(\bar{\varphi}) = \langle h(\varphi_1), \ldots, h(\varphi_k) \rangle$, where h is any homomorphism from Te_Σ to A such that $h(x_i) = a_i$ for all $i \leq n$.

Definition 2.1. A *visible k-data structure* over the hidden signature Σ is a pair $\mathcal{A} = \langle A, F \rangle$, where A is a Σ-algebra and $F \subseteq A^k_{\mathrm{VIS}} := \langle A^k_V : V \in \mathrm{VIS} \rangle$.

In the sequel, we normally omit the term "visible" and we simply say a k-data structure. An example of a 2-data structure is any model of the free hidden equational logic over Σ. The standard model of the free HEL_Σ is of the form $\langle A, \mathrm{id}_{A_{\mathrm{VIS}}} \rangle$, where A is a Σ-algebra and $\mathrm{id}_{A_{\mathrm{VIS}}}$ is the identity relation on the visible part of A, but one gets more general 2-data structures as models by taking any congruence relation on the visible part of A in place of $\mathrm{id}_{A_{\mathrm{VIS}}}$. By a *congruence relation on the visible part of A*, or simply a VIS-*congruence*, we mean a VIS-sorted set $\langle F_V : V \in \mathrm{VIS} \rangle$ such that, for every $V \in \mathrm{VIS}$, F_V is an equivalence relation on A_V, and for every term $\varphi(x_1{:}V_1, \ldots, x_n{:}V_n, y_1{:}H_1, \ldots, y_m{:}H_m){:}V$ with $V_1, \ldots, V_n, V \in \mathrm{VIS}$ and $H_1, \ldots, H_m, \in \mathrm{HID}$, if $\langle a_i, b_i \rangle \in F_{V_i}$ for all $i \leq n$, then for all $c_j \in A_{H_j}$ $j \leq m$

$$\langle \varphi^A(a_1, \ldots, a_n, c_1, \ldots, c_m), \varphi^A(b_1, \ldots, b_n, c_1, \ldots, c_m) \in F_V.$$

The admission of equality, or more generally equivalence, only between visible elements in the specification of the data structure reflects the basic premise of hidden logic, namely that only properties of visible elements can be known *a priori*: hidden data elements are equal or equivalent just when they have the same visible properties in a sense made precise below.

We can also consider the free Boolean logic over Σ, provided Σ has a Boolean sort. Here the standard models are the 1-data structures $\langle A, \{true\}\rangle$, where A is a Σ-algebra such that A_{VIS} is the two-element Boolean algebra. In a general model, A_{VIS} is an arbitrary Boolean algebra and $\{true\}$ is replaced by an arbitrary Boolean filter on A_{VIS}.

2.1. *Consequence*

For our purposes it is convenient to define a hidden k-logic as an abstract consequence relation on the set of k-formulas, independently of any specific choice of axioms and rules of inference. Let $\mathcal{S}$ be a subset of SORT. By a *consequence relation*, or *closure relation*, on $(\mathrm{Te}^k_\Sigma)_\mathcal{S}$ we mean a binary relation $\vdash \subseteq \mathcal{P}(\mathrm{Te}^k_\Sigma)_\mathcal{S} \times (\mathrm{Te}^k_\Sigma)_\mathcal{S}$ between subsets of k-formulas and individual k-formulas of sort $S \in \mathcal{S}$ satisfying the following conditions. (a) $\Gamma \vdash \bar\gamma$ for each $\bar\gamma \in \Gamma$; (b) $\Gamma \vdash \bar\varphi$, and $\Delta \vdash \bar\gamma$ for each $\bar\gamma \in \Gamma$, imply $\Delta \vdash \bar\varphi$.

The consequence relation is *finitary* (or *compact*) if $\Gamma \vdash \bar\varphi$ implies $\Delta \vdash \bar\varphi$ for some globally finite subset Δ of Γ (note that a set Δ of formulas is said to be globally finite if $\bigcup_{S\in\mathrm{SORT}} \Delta_S$ is finite). It is *substitution-invariant* if $\Gamma \vdash \bar\varphi$ implies $\sigma(\Gamma) \vdash \sigma(\bar\varphi)$ for every substitution $\sigma : X \to \mathrm{Te}_\Sigma$. The relation $\vdash$ has a natural extension to a relation, also denoted by $\vdash$, between subsets of $(\mathrm{Te}^k_\Sigma)_\mathcal{S}$. It is defined by $\Gamma \vdash \Delta$ if $\Gamma \vdash \bar\varphi$ for each $\bar\varphi \in \Delta$ (i.e., $\bar\varphi \in \Delta_S$, for some $S \in \mathcal{S}$).

Definition 2.2. A *hidden k-logic* over a hidden signature Σ is a pair $\mathcal{L} = \langle \Sigma, \vdash_\mathcal{L}\rangle$, where $\vdash_\mathcal{L}$ is a substitution-invariant consequence relation on the set $(\mathrm{Te}^k_\Sigma)_{\mathrm{VIS}}$ of visible k-formulas. A hidden k-logic is *specifiable* if $\vdash_\mathcal{L}$ is finitary (this terminology will soon be justified).

By a *un-hidden k-logic over* Σ we mean a hidden k-logic over Σ^{UH}. A *hidden k-logic* (without reference to a signature) can mean either a hidden or un-hidden logic over some unspecified hidden signature Σ.

Meseguer (Meseguer 1989) presents a similar general notion of logic, which is also defined as a consequence relation. Meseguer's system is called *entailment system* and combines a consequence relation with the notion of institution (see also (Fiadeiro and Sernadas 1988)).

Hidden k-logics are useful mainly because they encompass not only the 2-dimensional hidden and un-hidden equational logics, but also *Boolean logics*; these are 1-dimensional multisorted logics with Boolean as the only visible sort, and with equality-test operations for some of the hidden sorts in place of equality predicates. They also include all assertional logics, the purview of abstract algebraic logic. By this way we obtain a unified theory for a variety of logical systems. In this paper we are mainly concerned with a special hidden 2-logic, the *hidden equational logic* (see Section 2.3).

Normally a specifiable hidden k-logic is presented by a set of axioms (visible k-formulas)

and inference rules of the general form

$$\frac{\bar{\varphi}_0{:}V_0, \ldots, \bar{\varphi}_{n-1}{:}V_{n-1}}{\bar{\varphi}_n{:}V_n}, \tag{2}$$

where $\bar{\varphi}_0, \ldots, \bar{\varphi}_n$ are all visible k-formulas. A visible k-formula $\bar{\psi}$ is *directly derivable* from a set Γ of visible k-formulas by a rule such as (2) if there is a substitution $h : X \to \mathrm{Te}_\Sigma$ such that $h(\bar{\varphi}_n) = \bar{\psi}$ and $h(\bar{\varphi}_0), \ldots, h(\bar{\varphi}_{n-1}) \in \Gamma$. $\bar{\psi}$ is *derivable* from Γ by a given set of axioms and rules of inference if there is a finite sequence of k-formulas $\bar{\psi}_0, \ldots, \bar{\psi}_{n-1}$ such that $\bar{\psi}_{n-1} = \bar{\psi}$, and for each $i < n$ either (a) $\bar{\psi}_i \in \Gamma$, or (b) $\bar{\psi}_i$ is a substitution instance of an axiom, or (c) $\bar{\psi}_i$ is directly derivable from $\{\bar{\psi}_j : j < i\}$ by one of the rules of inference.

It is well known, and straightforward to show, that a hidden k-logic $\mathcal{L}$ is specifiable if and only if there exists a (possibly) infinite set of axioms and rules of inference such that, for any visible k-formula $\bar{\psi}$ and any set Γ of visible k-formulas, $\Gamma \vdash_{\mathcal{L}} \bar{\psi}$ iff $\bar{\psi}$ is derivable from Γ by the given set of axioms and rules.

Let $\mathcal{L}$ be a (not necessarily specifiable) hidden k-logic. By a *theorem of* $\mathcal{L}$, we mean a (necessarily visible) k-formula $\bar{\varphi}$ such that $\vdash_{\mathcal{L}} \bar{\varphi}$, i.e., $\emptyset \vdash_{\mathcal{L}} \bar{\varphi}$. The set of all theorems is denoted by $\mathrm{Thm}(\mathcal{L})$. A rule such as (2) is said to be a *derivable rule* of $\mathcal{L}$ if $\{\bar{\varphi}_0, \ldots, \bar{\varphi}_{n-1}\} \vdash_{\mathcal{L}} \bar{\varphi}_n$.

A set of visible k-formulas T closed under the consequence relation, i.e., $T \vdash_{\mathcal{L}} \bar{\varphi}$ implies $\bar{\varphi} \in T$, is called a *theory* of $\mathcal{L}$. The set of all theories is denoted by $\mathrm{Th}(\mathcal{L})$. It is closed under arbitrary intersection, i.e., $\{\, T_i : i \in I \,\} \subseteq \mathrm{Th}(\mathcal{L})$ implies $\bigcap_{i\in I} T_i \in \mathrm{Th}(\mathcal{L})$. Moreover, if $\mathcal{L}$ is specifiable, then $\mathrm{Th}(\mathcal{L})$ is closed under unions of upward directed sets, i.e., if $\{\, T_i : i \in I \,\} \subseteq \mathrm{Th}(\mathcal{L})$ and for every $i, i' \in I$, there is a $j \in I$ such that $T_i \cup T_{i'} \subseteq T_j$, then $\bigcup_{i\in I} T_i \in \mathrm{Th}(\mathcal{L})$.

The set of all $\mathcal{L}$-consequences of $\Gamma \subseteq (\mathrm{Te}^k_\Sigma)_{\mathrm{VIS}}$, $\{\, \bar{\varphi} \in (\mathrm{Te}^k_\Sigma)_{\mathrm{VIS}} : \Gamma \vdash_{\mathcal{L}} \bar{\varphi}\}$, is the smallest theory that includes Γ. It is denoted by $\mathrm{Cn}_{\mathcal{L}}(\Gamma)$. So a hidden k-logic is completely determined by its set of theories.

The restriction to axioms and rules of inference involving only visible k-formulas is natural in view of the special role visible data play in hidden logic. Axioms and rules involving hidden data can also play an important part as well, as we shall see, but only in an auxiliary role.

2.2. *Semantics*

Definition 2.3. Let K be a class of k-data structures over a hidden signature Σ.

(i) A visible k-formula $\bar{\varphi}{:}V$ is said to be a *valid consequence* of a set of visible k-formulas Γ in K, in symbols $\Gamma \models_K \bar{\varphi}$, if,

$$(\forall\, \langle A, F\rangle \in K)(\forall\, h{:}X \to A)\big[\big((\forall\, \bar{\psi}{:}W \in \Gamma)\,(h(\bar{\psi}) \in F_W)\big) \Rightarrow h(\bar{\varphi}) \in F_V\big].$$

(ii) A visible k-formula $\bar{\varphi}$ is *valid* in K if $h(\bar{\varphi}) \in F_V$ for every $\langle A, F\rangle \in K$ and every assignment $h{:}X \to A$, i.e., if it is a valid consequence of the empty set of k-formulas, in symbols $\models_K \bar{\varphi}$.

(iii) A rule such as (2) is a *valid rule* of K, if $\{\bar{\varphi}_0, \ldots, \bar{\varphi}_{n-1}\} \models_K \bar{\varphi}_n$.

For simplicity, we write $\Gamma \models_{\mathcal{A}} \varphi$ in place of $\Gamma \models_{\{\mathcal{A}\}} \varphi$ for a single k-data structure $\mathcal{A}$.

It is easy to see that $\models_K$ is a substitution-invariant consequence relation on the set of k-formulas. It is not however in general finitary; hence the associated hidden k-logic $\langle \Sigma, \models_K \rangle$ is not in general specifiable.

Definition 2.4. A k-data structure $\mathcal{A}$ is a *model* of a hidden k-logic $\mathcal{L}$ if every $\mathcal{L}$-consequence is a semantic consequence of $\mathcal{A}$, i.e., $\Gamma \vdash_{\mathcal{L}} \bar{\varphi}$ always implies $\Gamma \models_{\mathcal{A}} \bar{\varphi}$. The class of all models of $\mathcal{L}$ is denoted by $\mathrm{Mod}(\mathcal{L})$.

If $\mathcal{L}$ is a specifiable hidden k-logic, then $\mathcal{A}$ is a model of $\mathcal{L}$ iff every axiom is valid in $\mathcal{A}$ and every inference rule is a valid rule of $\mathcal{A}$.

The proof of the following theorem is straightforward and can be found in (Martins 2004). For sentential logics the result is well known; see for example (Wójcicki 1988).

Theorem 2.5 (Completeness of Hidden k-logics (Martins 2004)). For any hidden k-logic $\mathcal{L}$,

$$\vdash_{\mathcal{L}} \; = \; \models_{\mathrm{Mod}(\mathcal{L})},$$

i.e., for every set of k-formulas Γ and any k-formula $\bar{\varphi}$, $\Gamma \vdash_{\mathcal{L}} \bar{\varphi}$ iff $\Gamma \models_{\mathrm{Mod}(\mathcal{L})} \bar{\varphi}$.

Strictly speaking, this completeness theorem only holds when the models of $\mathcal{L}$ are restricted to k-data structures with a nonempty domain of each sort. In the sequel we assume all k-data structures have this property.

2.3. *Hidden equational logic*

In the present context hidden equational logic is a special class of 2-logics in which a 2-formula $\langle t, s \rangle$ is intended to represent an equation, which we denote by $t \approx s$, and a rule $\dfrac{\langle t_0, s_0 \rangle, \ldots, \langle t_{n-1}, s_{n-1} \rangle}{\langle t_n, s_n \rangle}$ represents a conditional equation, denoted by

$$t_0 \approx s_0, \ldots, t_{n-1} \approx s_{n-1} \to t_n \approx s_n.$$

Since the basic premise of hidden logics is that only visible data can be compared directly, in hidden equational logic there is no way of directly asserting the quality of terms of hidden sort. In fact no representation of the equality predicate between elements of the hidden domains exists in the object language, and in reasoning about hidden data, only visible properties expressible in the form of conditional equations are admitted. The rationale behind this restriction was discussed in the introduction. Of course the equality of hidden elements can be inferred indirectly by comparing their visible behavior, and it is convenient for this purpose to consider an expanded class of equational logics, the so-called *un-hidden equational logics* admitting equality predicates over hidden domains.

Definition 2.6 (Free hidden and un-hidden equational logic). Let Σ be a hidden signature and VIS its set of visible sorts.

(i) The *free hidden equational logic* over Σ (or the *free* HEL_Σ) is the specifiable hidden 2-logic presented as follows.
Axioms:

$x{:}V \approx x{:}V$, for all $V \in \mathrm{VIS}$

Inference rules: for each $V, W \in \mathrm{VIS}$,

(IR_1) $\quad x{:}V \approx y{:}V \to y{:}V \approx x{:}V$,

(IR_2) $\quad x{:}V \approx y{:}V, y{:}V \approx z{:}V \to x{:}V \approx z{:}V$,

(IR_3) $\quad \varphi{:}V \approx \psi{:}V \to \vartheta(x/\varphi){:}W \approx \vartheta(x/\psi){:}W$, for every $\vartheta \in \mathrm{Te}_W$ and every $x \in X_V$.

(ii) The *free un-hidden equational logic* over Σ (or the *free* UHEL_Σ) contains an equality predicate for each sort, visible and hidden. The axioms and inference rules are the same as those of the free HEL_Σ, except that V and W are now allowed to range over all sorts. Thus $\mathrm{UHEL}_\Sigma = \mathrm{HEL}_{\Sigma^{\mathrm{UH}}}$.

We assume here that the set of variables associated with each term coincides with the set of variables that actually occur in the term. As a consequence, in Theorem 2.25 below we must assume that all the sort domains of each model are nonempty.

As indicated earlier, the models of the free HEL_Σ are the 2-data structures $\mathcal{A} = \langle A, F\rangle$ where A is an arbitrary Σ-algebra and F is a VIS-*congruence* on A, i.e., a congruence on the visible part of A. The theories of the free HEL_Σ are the VIS-congruences on the term algebra.

The models of the free UHEL_Σ are the 2-data structures $\langle A, F\rangle$ where F is a congruence on the entire algebra A; the theories are the congruences on the term algebra.

For every congruence F of A, whether on the visible part or entire algebra, we write $a \equiv a' \mod F_S$, or simply $a \equiv a'\ (F_S)$ or $a \equiv_{F_S} a'$, alternatively for $\langle a, a'\rangle \in F_S$; we also may omit explicit reference to the sort S in these expressions if no confusion is possible. If A is the term algebra and φ, φ' are terms, we might also write $\varphi \approx \varphi' \in F_S$.

An *applied hidden equational logic over* Σ, called simply a HEL_Σ, is any hidden 2-logic $\mathcal{L}$ over Σ that satisfies all axioms and rules of inference of the free hidden equational logic over Σ; an *applied un-hidden equational logic over* Σ is defined similarly and it is simply called an UHEL_Σ; the subscript Σ may be omitted if it is clear from the context. We almost always are interested exclusively in those applied hidden equational logics $\mathcal{L}$ that are specifiable, that is, that are obtained from the free logic by adding new, so-called *extra-logical* axioms and inference rules to the *logical* axioms and rules of Definition 2.6. In view of the completeness theorem (Theorem 2.25 below) they correspond respectively to the identities and conditional identities of the class of models of $\mathcal{L}$. In particular, the visible conditional equation

$$t_0(\bar{x}) \approx s_0(\bar{x}), \ldots, t_{n-1}(\bar{x}) \approx s_{n-1}(\bar{x}) \to t_n(\bar{x}) \approx s_n(\bar{x}) \tag{3}$$

is a valid rule of a model $\mathcal{A} = \langle A, F\rangle$ of the free HEL_Σ (free UHEL_Σ) if, for every assignment $\bar{a}$ of the elements of A to $\bar{x}$ (of the appropriate sorts),

$$t_n^A(\bar{a}) \equiv_F s_n^A(\bar{a}) \quad \text{if} \quad t_0^A(\bar{a}) \equiv_F s_0^A(\bar{a}), \ldots, t_{n-1}^A(\bar{a}) \equiv_F s_{n-1}^A(\bar{a}).$$

The applied un-hidden equational logics we deal with are, on the contrary, normally

unspecifiable since they come from the behavioral equivalence of hidden equational logics and more general hidden k-logics.

We give several examples of specifiable hidden logics. We have purposely chosen simple, well-known ones that allow us to illustrate the basic ideas without burdening the reader with irrelevant detail. The first two illustrate how the logic of a particular data structure can be alternatively formalized as a Boolean 1-logic and as an equational 2-logic, a HEL. The flag logics provide two different ways of specifying semaphores, which are commonly used in scheduling resources (Goguen and Malcolm 1999).

Example 2.7. (**Flags** as a Boolean 1-logic)
Consider the hidden signature Σ_{flag}:

SORT $= \{\mathit{flag}, \mathit{bool}\}$, with bool the unique visible sort and the following operation symbols:

$$\begin{array}{ll} \mathit{up} : \mathit{flag} \to \mathit{flag}; & \mathit{rev} : \mathit{flag} \to \mathit{flag}; \\ \mathit{dn} : \mathit{flag} \to \mathit{flag}; & \mathit{up?} : \mathit{flag} \to \mathit{bool}, \end{array}$$

and the operation symbols for the Boolean part: $\neg, \wedge, \vee, \mathit{true}, \mathit{false}$. The Boolean biconditonal $\varphi \leftrightarrow \psi$ is an abbreviation for the compound operation $(\neg\varphi \vee \psi) \wedge (\neg\psi \vee \varphi)$.

The Boolean logic of flags, $\mathcal{L}_{\mathit{bflag}}$, is the 1-logic with the following extra-logical axioms:

$$\begin{array}{ll} \mathit{up?}(\mathit{up}(F)) & \mathit{up?}(\mathit{rev}(F)) \leftrightarrow \neg(\mathit{up?}(F)) \\ \neg\mathit{up?}(\mathit{dn}(F)) & \end{array}$$

and including usual logical axioms for the classical propositional logic. There are no extra-logical rules of inference. ♢

Example 2.8. (**Flags** as a HEL) The signature is the same as above.

The equational logic of flags, $\mathcal{L}_{\mathit{eflag}}$, is the $\mathrm{HEL}_{\Sigma_{\mathit{flag}}}$ with the following extra-logical axioms:

$$\begin{array}{ll} \mathit{up?}(\mathit{up}(F)) \approx \mathit{true} & \mathit{up?}(\mathit{rev}(F)) \approx \neg(\mathit{up?}(F)) \\ \mathit{up?}(\mathit{dn}(F)) \approx \mathit{false} & \end{array}$$

and including the usual logical axioms for Boolean algebra. There are no extra-logical rules of inference. ♢

As expected, $\mathcal{L}_{\mathit{bflag}}$ and $\mathcal{L}_{\mathit{eflag}}$ are equivalent. Precisely, $\dfrac{\varphi_1 \leftrightarrow \varphi'_1, \ldots, \varphi_n \leftrightarrow \varphi'_n}{\psi \leftrightarrow \psi'}$ is a derivable rule of $\mathcal{L}_{\mathit{bflag}}$ iff $\dfrac{\varphi_1 \approx \varphi'_1, \ldots, \varphi_n \approx \varphi'_n}{\psi \approx \psi'}$ is a derivable rule of $\mathcal{L}_{\mathit{eflag}}$.

Example 2.9. (**Stacks of Natural Numbers** as a HEL) As in the standard specification of the logic of stacks, only the natural numbers are visible. Consequently, the axioms and rules of inference can only reference "numerical behavior" of stacks rather than the stacks themselves. In particular there can be no axiom or rule involving equality between stacks. Because of this we get an infinite number of axioms, where in the standard formalizations, where assertions about the equality of stacks are allowed, the

axiomatization is finite and on its face conceptually simpler. We have more to say about this later.

The specification differs from the usual one in another regard. The top of the empty stack is zero and pushing zero on the empty stack gives the empty stack. This is done to simplify the specification logic and agrees with what is done in (Goguen and Malcolm 2000).

Consider the hidden signature Σ_{stacks}:

SORT $= \{nat, stack\}$, with nat the unique visible sort and the following operation symbols:

$$\begin{array}{ll} empty : \quad \rightarrow stack & top : stack \rightarrow nat \\ zero : \quad \rightarrow nat & pop : stack \rightarrow stack \\ push : nat, stack \rightarrow stack & s : nat \rightarrow nat \end{array}$$

The specification logic of stacks, $\mathcal{L}_{stacks}$, is the logic with hidden signature Σ_{stacks} and the following axioms and inference rules:

Extra-logical axioms:

$top(pop^n(empty)) \approx zero$, for all n;

$top(push(x, y)) \approx x$;

$top(pop^{n+1}(push(x, y))) \approx top(pop^n(y))$, for all n.

Extra-logical inference rule:

$s(x) \approx s(y) \rightarrow x \approx y$. ♢

Example 2.10. (**Sets**) This example is the usual specification of sets (see (Bouhoula and Rusinowitch 2002)). There are three sorts: *set*, *elt* and *bool*, with *elt* and *bool* as the visible sorts. The visible operations are the operations for the Booleans: *true*, *false*, $\neg$, $\wedge$ and $\vee$. And the hidden operations are the constant *empty* to represent the empty set; and $\cup$, & and *neg* to represent the set theoretical union, intersection and complement, respectively. The action of adding an element to a set is represented by *add*, and *in* is the operation symbol used to test whether an element belongs to a set, i.e., $in(e, X)$ expresses that "e is in X".

Consider the hidden signature Σ_{sets}:

SORT $= \{set, bool, elt\}$, with $\{bool, elt\}$ the set of visible sorts and the following operation symbols:

$$\begin{array}{llll} empty : & \rightarrow set; & neg : & set \rightarrow set \\ \& : & set, set \rightarrow set; & add : & elt, set \rightarrow set. \end{array} \qquad in : \quad elt, set \rightarrow bool;$$

and the operation symbols for the Boolean part: $\neg, \wedge, \vee, true, false$.

The extralogical axioms are the axioms of the Boolean algebra and the following ones:

$$\begin{array}{ll} in(n, empty) \approx false & in(n, (\cup(x, y))) \approx in(n, x) \ \vee \ in(n, y) \\ in(n, neg(x)) \approx \neg(in(n, x)) & in(n, (\&(x, y)) \approx in(n, x) \ \wedge \ in(n, y) \end{array}$$

And the extralogical inference rules are:

$in(z,x) \approx in(z,y) \to in(z,add(n,x)) \approx in(z,add(n,y))$;

$m \approx n \to in(z,add(m,x)) \approx in(z,add(n,x))$. ♢

Example 2.11 (Interval Sets). We now give an example of a hidden 3-logic that formalizes the sets of intervals of an abstract ordered set. The 3-formula $\langle x,y,z\rangle$ may be thought of as the ternary partial ordering relation $x \leq y \leq z$, although there is no formal representation of the binary relation $\leq$. A set s is the interval $[\,\mathrm{n},\mathrm{m}\,] = \{\, x : n \leq x \leq m \,\}$ of numbers in the partial ordering, where n, m are respectively the *lower bound* ($lb(s)$) and the *upper bound* ($ub(s)$) of the interval.
SORT $= \{set, num\}$, where num is the only visible sort.

Operations.

$lub, glb : num, num \to num$,

$ub, lb : set \to num$,

$elt\text{-}of : set \to num$,

$\cup, \& : set, set \to set$.

Axioms.

$\langle x,x,x\rangle$,

$\langle glb(x,y),\ x,\ lub(x,y)\rangle$,

$\langle glb(x,y),\ y,\ lub(x,y)\rangle$,

$\langle lb(s),\ elt\text{-}of(s),\ ub(s)\rangle$,

$\langle glb(lb(s),\ lb(t)),\ elt\text{-}of(\cup(s,t)),\ lub(up(s),\ ub(t)\rangle$,

$\langle lub(lb(s),\ lb(t)),\ elt\text{-}of(\&(s,t)),\ glb(up(s),\ ub(t)\rangle$.

Rules of Inference.

$$\frac{\langle x,\ y,\ w\rangle,\ \langle y,\ z,\ w'\rangle}{\langle x,\ y,\ z\rangle},$$

$$\frac{\langle w,\ x,\ y\rangle,\ \langle w',\ y,\ z\rangle}{\langle x,\ y,\ z\rangle},$$

$$\frac{\langle x,\ z,\ x'\rangle,\ \langle y,\ z,\ y'\rangle}{\langle lub(x,\ y),\ z,\ glb(x',y')\rangle}.$$

♢

A theory of a HEL $\mathcal{L}$ is also called an *$\mathcal{L}$-congruence* on the term algebra. For any set E of equations, the theory of $\mathcal{L}$ generated by E, $\mathrm{Cn}_{\mathcal{L}}(E)$, is the smallest $\mathcal{L}$-congruence that contains the pair $\langle t,t'\rangle$ for each equation $t \approx t'$ in E.

A visible conditional equation (3) is a *quasi-identity* of a Σ-algebra A if it is a valid rule of $\langle A, \mathrm{id}_{A_{\mathrm{VIS}}}\rangle$, or of $\langle A, \mathrm{id}_A\rangle$ if it is of arbitrary sort. Models of the free HEL_Σ (the free UHEL_Σ) of the form $\langle A, \mathrm{id}_{A_{\mathrm{VIS}}}\rangle$ ($\langle A, \mathrm{id}_A\rangle$) are called *equality models*. The class of all equality models of a HEL_Σ (or an UHEL_Σ) $\mathcal{L}$ is denoted by $\mathrm{Mod}^{=}(\mathcal{L})$. Since every equality model is uniquely determined by its algebraic reduct, we shall not bother distinguishing them in the sequel. Thus, for every HEL_Σ $\mathcal{L}$ we identify $\mathrm{Mod}^{=}(\mathcal{L})$ with $\{\, A : \langle A, \mathrm{id}_{A_{\mathrm{VIS}}}\rangle \in \mathrm{Mod}^{=}(\mathcal{L}) \,\}$, and similarly for the equality models of an UHEL_Σ.

2.4. *Behavioral equivalence*

In hidden equational logic, two hidden data elements of the same sort are *behaviorally equivalent* if, roughly speaking, any visible procedure returns the same value when executed with either of the two objects as input. The notion arises from the alternative view of a data structure as a transition system in which the hidden data elements represent states of the system and the operations (i.e., the *methods*) that return hidden, as opposed to visible, elements induce transitions between states.

In the formalism of HEL, the concept of procedure takes the form of a context. Formally, a *S-context* over a hidden signature Σ is a term

$$\varphi(z{:}S, u_1{:}T_1, \ldots, u_m{:}T_m){:}U \tag{4}$$

with a distinguished variable z of sort S and parametric variables $u_1, \ldots, u_m$ of arbitrary (visible or hidden) sort. It is a *visible context* if the sort U of φ is visible.

Definition 2.12. Let A be a Σ-algebra and let S be a arbitrary sort. Then, $a, a' \in A_S$ are *behaviorally equivalent in* A, in symbols $a \equiv_A^{\text{beh}} a'$, if for every visible S-context $\varphi(z{:}S, u_1{:}T_1, \ldots, u_m{:}T_m)$ and for all $b_1 \in A_{T_1}, \ldots, b_m \in A_{T_m}$,

$$\varphi^A(a, b_1, \ldots, b_m) = \varphi^A(a', b_1, \ldots, b_m).$$

Variants of this notion of behavioral equivalence have occurred in the literature. For example, Goguen and Malcolm (Goguen and Malcolm 2000) restrict the set of contexts to the ones built from a predefined set of observational operational symbols (see the Conclusion section for more details).

To generalize the notion of behavioral equivalence to apply to hidden k-logics we first generalize the notion of context. A (k, S)-*context* over a hidden signature Σ is a k-term

$$\begin{aligned}\bar{\varphi}(z{:}S, u_1{:}T_1, \ldots, u_m{:}T_m){:}U \\ = \big\langle \varphi_1(z{:}S, u_1{:}T_1, \ldots, u_m{:}T_m), \ldots, \varphi_k(z{:}S, u_1{:}T_1, \ldots, u_m{:}T_m)\big\rangle{:}U\end{aligned} \tag{5}$$

with a distinguished variable z of sort S and parametric variables $u_1, \ldots, u_m$. It is a *visible context* if the sort U of $\bar{\varphi}$ is visible.

Definition 2.13. Let $\mathcal{A} = \langle A, F\rangle$ be a k-data structure over a hidden signature Σ. Two elements a, a' of A of arbitrary sort S are said to be *behaviorally equivalent* in $\mathcal{A}$, in symbols $a \equiv_{\mathcal{A}}^{\text{beh}} a'$, if for every visible (k, S)-context $\bar{\varphi}(z{:}S, u_1{:}T_1, \ldots, u_m{:}T_m){:}V$ and for all $b_1 \in A_{T_1}, \ldots, b_m \in A_{T_m}$,

$$\bar{\varphi}^A(a, b_1, \ldots, b_m) \in F_V \quad \text{iff} \quad \bar{\varphi}^A(a', b_1, \ldots, b_m) \in F_V. \tag{6}$$

This notion does indeed generalize behavior equivalence in equational logic, since, as a consequence of Theorem 2.23 below, we have that a and a' are behaviorally equivalent in a Σ-algebra A iff they are behaviorally equivalent in the 2-dimensional equality data structure $\langle A, \mathrm{id}_{A_{\text{VIS}}}\rangle$ in the sense of Definition 2.13.

2.5. *Leibniz congruence*

Behavioral equivalence over a k-data structure turns out to be a congruence relation on the underlying algebra of the data structure with special properties. In the 1-sorted, 1-data structures (called *matrices*) that constitute the natural models of sentential logic, the detailed combinatorial analysis of this congruence constitutes the basis of a branch of mathematical logic called *abstract algebraic logic*. Our intention here is to extend this analysis to the behavioral congruences of arbitrary multi-sorted k-data structures and in particular to the models of hidden equational logic.

Let $\mathcal{A} = \langle A, F\rangle$ be a k-data structure. A congruence relation Θ on A is VIS-*compatible* (or simply *compatible*) with F if for all $V \in \mathrm{VIS}$ and for all $\bar{a}, \bar{a}' \in A_V^k$ the following condition holds.

$$\text{if } a_i \equiv a_i'(\Theta_V) \text{ for all } i \leq k \text{ then, } \bar{a} \in F_V \text{ iff } \bar{a}' \in F_V;$$

that is, each F_V is the union of a cartesian product of Θ_V-classes i.e.,

$$F_V = \bigcup_{\bar{a} \in F_V} (a_1/\Theta_V) \times (a_2/\Theta_V) \times \cdots \times (a_k/\Theta_V).$$

Lemma 2.14. Let $\mathcal{A} = \langle A, F\rangle$ be a k-data structure. There is a largest congruence relation on A compatible with F.

Proof. Let Φ and Ψ be two congruences on A compatible with F. The relative product $\Phi \circ \Psi$, defined for each $S \in \mathrm{SORT}$ by

$$(\Phi \circ \Psi)_S := \big\{\langle a, b\rangle \in A_S^2 : \exists c \in A_S \ \big(\langle a, c\rangle \in \Phi_S \text{ and } \langle c, b\rangle \in \Psi_S\big)\big\},$$

is also compatible with F. Since the join $\Phi \vee \Psi$, in the lattice of congruences, is defined by $\bigcup_{i<\omega} \Phi \circ^i \Psi$, where $\Phi \circ^0 \Psi = \Delta_A$ and $\Phi \circ^{i+1} \Psi = (\Phi \circ^i \Psi) \circ (\Phi \circ \Psi)$, we have that $\Phi \vee \Psi$ is also compatible with F. Hence, the set of all congruence relations on A compatible with F is directed in the sense that, for any pair of congruences compatible with F, there is a third congruence with the same property that includes both of them. We can conclude from this that the union of all compatible congruences is again a compatible congruence. Therefore, the largest congruence compatible with F always exists. □

Definition 2.15. Let $\mathcal{A} = \langle A, F\rangle$ be a k-data structure. The largest congruence relation on A compatible with F is called the *Leibniz congruence of F on A* and is denoted by $\Omega_A(F)$.

The Leibniz congruence plays a central role in abstract algebraic logic when restricted to single-sorted, k-data structures; see for example (Pigozzi 2001) and (Font et al. 2003). The term was introduced in (Blok and Pigozzi 1989), but the concept appeared much earlier. The motivation behind the choice of the term *Leibniz* will become clear after the next theorem.

A systematic study of the Leibniz congruence in hidden k-logics can be found in (Martins 2004) — in particular a proof of the following characterization. In the case of single-sorted 1-data structures, this result was well known in the literature of sentential logic; see for example (Blok and Pigozzi 1989).

Theorem 2.16. Let Σ be a hidden signature and let $\mathcal{A} = \langle A, F\rangle$ be a k-data structure over Σ. Then, $\equiv_{\mathcal{A}}^{\mathrm{beh}} = \Omega_A(F)$, i.e., for every $S \in \mathrm{SORT}$ and for all $a, a' \in A_S$, $a \equiv_{\mathcal{A}}^{\mathrm{beh}} a'$ iff $a \equiv a'\ (\Omega_A(F)_S)$.

Proof. It is easy to see that $\equiv_{\mathcal{A}}^{\mathrm{beh}}$ is an equivalence relation on A. To see that it is a congruence relation, let O be an operation symbol of type $T_1, \ldots, T_n \to S$ and suppose $a_i \equiv_{\mathcal{A}}^{\mathrm{beh}} a_i'$, $1 \le i \le n$. We must show that, for any visible (k,T)-context $\bar\varphi(z{:}S, \bar u{:}\bar Q){:}V$, with the designated variable $z{:}S$, and for all parameters $\bar b \in A_{\bar Q}$, we have

$$\bar\varphi^A\big(O^A(\bar a), \bar b\big) \in F_V \quad \text{iff} \quad \bar\varphi^A\big(O^A(\bar a'), \bar b\big) \in F_V. \tag{7}$$

Consider any $i \le n$. Using the assumption $a_i \equiv_{\mathcal{A}}^{\mathrm{beh}} a_i'$, and taking x_i as the designated variable, $x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n, u_1, \ldots, u_n$ as parametric variables, and $a_1, \ldots, a_{i-1}$, $a_{i+1}', \ldots, a_n', b_1, \ldots, b_m$ as parameters we have

$$\bar\varphi^A\big(O^A(a_1, \ldots, a_{i-1}, a_i, a_{i+1}', \ldots, a_n'), \bar b\big) \in F_V \\ \text{iff} \quad \bar\varphi^A\big(O^A(a_1, \ldots, a_{i-1}, a_i', a_{i+1}', \ldots, a_n'), \bar b\big) \in F_V.$$

Since this equivalence holds for all $i \le n$, (7) holds, and hence $\equiv_{\mathcal{A}}^{\mathrm{beh}}$ is a congruence on A.

To see that $\equiv_{\mathcal{A}}^{\mathrm{beh}}$ is compatible with F, consider $\bar a, \bar a' \in A_V^k$ such that $\bar a \left(\equiv_{\mathcal{A}}^{\mathrm{beh}}\right)_V^k \bar a'$. Consider the k-sequence of pairwise distinct variables $\bar x = \langle x_1{:}V, \ldots, x_k{:}V\rangle$ (called a *k-variable*, a special k-formula). For each i, $1 \le i \le k$, view $\bar x$ as a (k,V)-context with designated variable x_i and treat $a_1, \ldots, a_{i-1}, a_{i+1}', \ldots, a_k'$ as parameters. Then from the assumption $a_i \left(\equiv_{\mathcal{A}}^{\mathrm{beh}}\right)_V a_i'$ we conclude that

$$\langle a_1, \ldots, a_{i-1}, a_i, a_{i+1}', \ldots, a_n'\rangle \in F_V \quad \text{iff} \quad \langle a_1, \ldots, a_{i-1}, a_i', a_{i+1}', \ldots, a_n'\rangle \in F_V.$$

So $\bar a \in F_V$ iff $\bar a' \in F_V$. Thus $\equiv_{\mathcal{A}}^{\mathrm{beh}}$ is compatible with F.

Finally, we must show that $\equiv_{\mathcal{A}}^{\mathrm{beh}}$ is the largest congruence on A compatible with F. Let Θ be any congruence on A that is compatible with F. Assume $a \equiv a'\ (\Theta_S)$. Let $\bar\varphi(z{:}S, \bar u{:}\bar Q){:}V$ be a visible (k,S)-formula with designated variable $z{:}S$, and let $\bar b \in A_{\bar Q}$ be a system of parameters. By the congruence property, $\bar\varphi^A(a, \bar b) \equiv \bar\varphi^A(a', \bar b)\ \big(\Theta^k\big)$. So by the compatibility of Θ with F we have $\bar\varphi^A(a, \bar b) \in F_V$ iff $\bar\varphi^A(a', \bar b) \in F_V$. Thus $\Theta \subseteq \equiv_{\mathcal{A}}^{\mathrm{beh}}$. □

So $\equiv_{\mathcal{A}}^{\mathrm{beh}}$ is a congruence relation on the whole algebra A. Thus, for any k-data structure $\mathcal{A}$ over the hidden signature Σ, the associated 2-data structure $\langle A, \equiv_{\mathcal{A}}^{\mathrm{beh}}\rangle$ is a model of the free UHEL_Σ.

According to Leibniz's famous criterion, two objects in the universe of discourse are equal if they share all properties that can be expressed in the language of discourse. In the universe represented by a k-data structure $\mathcal{A} = \langle A, F\rangle$, the condition that two elements a, a' of A have the same properties is expressed exactly by the equivalence (6), and hence, in view of the last theorem, by the equivalence $a \equiv_{\Omega_A(F)} a'$. This is the motivation for the choice of the term *Leibniz congruence* for $\Omega_A(F)$.

Definition 2.17.

(i) A k-data structure $\mathcal{A} = \langle A, F\rangle$ is *reduced* if two elements are behaviorally equivalent only if they are equal, i.e. (in view of Theorem 2.16), if $\Omega_A(F) = \mathrm{id}_A$.

(ii) The class of all reduced models of a hidden k-logic $\mathcal{L}$ is denoted by $\mathrm{Mod}^*(\mathcal{L})$.

The reduced models of one-sorted k-logics, in particular sentential logics, play an important role in abstract algebraic logic. For instance, the reduced models of the classical propositional calculus are exactly the Boolean algebras, which constitute just a small part of the class of all models.

The reduced models of a hidden k-logic can be obtained by taking the quotient of an arbitrary model by its Leibniz congruence. If $\mathcal{A} = \langle A, F\rangle$ is a k-data structure over Σ, we can form the quotient structure $\mathcal{A}/\Omega_A(F) = \langle A, F\rangle/\Omega_A(F) = \langle A/\Omega_A(F),\, F/\Omega_A(F)\rangle$, where $A/\Omega_A(F)$ is the quotient of A by $\Omega_A(F)$, and $F/\Omega_A(F) = \{\, \langle a_1/\Omega_A(F), \ldots, a_k/\Omega_A(F)\rangle : \langle a_1, \ldots, a_k\rangle \in F \,\}$. The quotient $\mathcal{A}/\Omega_A(F)$ is called the *reduction* of $\mathcal{A}$ and is denoted by $\mathcal{A}^* = \langle A^*, F^*\rangle$.

$\mathcal{A}^*$ is indeed always reduced. To see this we will need the following technical lemma. But first we introduce some convenient shorthand notation. Let $h : B \to A$ be a mapping between sets. For every k-sequence $\bar{b} = \langle b_1, \ldots, b_k\rangle$ over B, we write $h(\bar{b})$ for the k-sequence $\langle h(b_1), \ldots, h(b_k)\rangle$ over A; and for every k-sequence $\bar{a} = \langle a_1, \ldots, a_k\rangle$ over A, $h^{-1}(\bar{a})$ denotes the set of all k-sequences over B that map onto $\bar{a}$, i.e, $h^{-1}(\bar{a}) = \{\, \bar{b} \in B^k : h(\bar{b}) = \bar{a} \,\}$.

Lemma 2.18. Let $\mathcal{A} = \langle A, F\rangle$ be a k-data structure over Σ, and let B be a Σ algebra and $h : B \to A$ a surjective homomorphism (i.e., a homomorphism such that $h(B_S) = A_S$ for every sort S of Σ. Then

$$h^{-1}(\Omega_A(F)) = \Omega_B(h^{-1}(F)). \tag{8}$$

Proof. It is not difficult to see that $h^{-1}(\Omega_A(F))$ is a congruence on B. It is an equivalence relation since the inverse image of any equivalence relation is one. To verify the congruence property, let $\varphi(x_1{:}S_1, \ldots, x_n{:}S_n){:}T$ be a Σ-term, and let $b_i, b_i' \in B_{S_i}$ such that $b_i \equiv_{h^{-1}(\Omega_A(F))} b_i'$, for all i, $1 \le i \le n$. Then $h(b_i) \equiv_{\Omega_A(F)} h(b_i')$ for all i, and hence, since h is a homomorphism and $\Omega_A(F)$ is a congruence,

$$h(\varphi^B(b_1, \ldots, b_n)) = \varphi^A(h(b_1), \ldots, h(b_n)) \equiv_{\Omega_A(F)} \varphi^A(h(b_1'), \ldots, h(b_n')) = h(\varphi^B(b_1', \ldots, b_n')).$$

Moreover, $h^{-1}(\Omega_A(F))$ is compatible with $h^{-1}(F)$. To see this suppose $\bar{b} = \langle b_1, \ldots, b_k\rangle \in h^{-1}(F)$ and $\bar{b} \equiv \bar{b}' \left(h^{-1}(\Omega_A(F)^k)\right)$. Then $h(\bar{b}) \in F$ and $h(\bar{b}) \equiv h(\bar{b}') \left(\Omega_A(F)^k\right)$. Thus $h(\bar{b}') \in F$, since $\Omega_A(F)$ is compatible with F, and hence $\bar{b}' \in h^{-1}(\Omega_A(F))$.

So $h^{-1}(\Omega_A(F)) \subseteq \Omega_B(h^{-1}(F))$, by definition of the Leibniz congruence. To prove the reciprocal inclusion, it suffices to prove that $h(\Omega_B(h^{-1}(F))) \subseteq \Omega_A(F)$. For if this inclusion holds, then $\Omega_B(h^{-1}(F)) \subseteq h^{-1}h(\Omega_B(h^{-1}(F))) \subseteq h^{-1}(\Omega_A(F))$. Let Θ be the congruence generated by $h(\Omega_B(h^{-1}(F)))$. Since h is surjective, Θ is the transitive closure of $h(\Omega_B(h^{-1}(F)))$. Hence it is enough to prove that $h(\Omega_B(h^{-1}(F)))$ is compatible with F.

Let $\bar{a}, \bar{a}' \in A_S^k$ such that $\bar{a} \in F_S$ and $\bar{a} \equiv \bar{a}' \left(h(\Omega_B(h^{-1}(F))_S^k\right)$. Let $\bar{b}, \bar{b}' \in B_S^k$ such

that $\bar{b} \equiv \bar{b}' \big(\Omega_B(h^{-1}(F))^k_S\big)$ and $h(\bar{b}) = \bar{a}$ and $h(\bar{b}') = \bar{a}'$ Then $\bar{b} \in h^{-1}(F_S)$. Hence $\bar{b}' \in h^{-1}(F_S)$ since $\Omega_B(h^{-1}(F))$ is compatible with $h^{-1}(F)$. So $\bar{a}' \in F_S$. □

Theorem 2.19. The reduction of any k-data structure is reduced.

Proof. Let $\langle A, F\rangle$ be a k-data structure. Let $h : A \to A/\Omega_A(F)$ be the natural homomorphism and note that $\Omega_A(F)$ is the kernel of h. By Lemma 2.18, $h^{-1}\big(\Omega_{A/\Omega_A(F)}(F/\Omega_A(F))\big) = \Omega_A\big(h^{-1}(F/\Omega_A(F))\big) = \Omega_A(F)$. So $\Omega\big(F/\Omega_A(F)\big)$ is the identity congruence on $A/\Omega_A(F)$. □

As a corollary we have that, if $\mathcal{A}$ is reduced, then $\mathcal{A}^*$ is isomorphic to $\mathcal{A}$, and, up to isomorphism, $\mathrm{Mod}^*(\mathcal{L}) = \{\, \mathcal{A}^* : \mathcal{A} \in \mathrm{Mod}(\mathcal{L}) \,\}$.

In the next theorem we see that $\mathrm{Mod}^*(\mathcal{L})$ forms a complete set of models of $\mathcal{L}$. This is a consequence of a more general result that proves useful in other contexts.

Definition 2.20. Let $\mathcal{A} = \langle A, F\rangle$ and $\mathcal{B} = \langle B, G\rangle$ be k-data structures over the same hidden signature Σ. $\mathcal{B}$ is said to be a *strict homomorphic image of* $\mathcal{A}$, in symbols $\mathcal{A} \succcurlyeq \mathcal{B}$, if there exists a surjective homomorphism $h\colon A \to B$ of algebras such that $h^{-1}(G) = F$.

Theorem 2.21. Let $\mathcal{A} = \langle A, F\rangle$ and $\mathcal{B} = \langle B, G\rangle$ be two k-data structures. If $\mathcal{A} \succcurlyeq \mathcal{B}$, then $\models_{\mathcal{A}} = \models_{\mathcal{B}}$, i.e., for any set $\Gamma \cup \{\bar{\varphi}\}$ of visible k-formulas, we have $\Gamma \models_{\mathcal{A}} \bar{\varphi}$ iff $\Gamma \models_{\mathcal{B}} \bar{\varphi}$.

Proof. Let $h\colon \mathcal{A} \to \mathcal{B}$ be a strict homomorphism. Since $h^{-1}(G) = F$, we have that, for every visible k-formula $\bar{\psi}(\bar{x}\colon \bar{S})$,

$$\text{for all } \bar{a} \in A_{\bar{S}}, \quad \bar{\psi}^A(\bar{a}) \in F \quad \text{iff} \quad \bar{\psi}^B(h(\bar{a})) = h\big(\bar{\psi}^A(\bar{a})\big) \in G.$$

Then, letting $\bar{S}$ be the list of all variables occurring in $\Gamma \cup \{\bar{\varphi}\}$, we have that, for all $\bar{a} \in A_{\bar{S}}$,

$$\big(\forall\, \bar{\gamma} \in \Gamma\, (\bar{\gamma}^A(\bar{a}) \in F)\big) \Longrightarrow \bar{\varphi}^A(\bar{a}) \in F \quad \text{iff} \quad \big(\forall\, \bar{\gamma} \in \Gamma\, (\bar{\gamma}^B(h(\bar{a})) \in G\big) \Longrightarrow \bar{\varphi}^B(h(\bar{a})) \in G.$$

Since h is surjective, $h(\bar{a})$ ranges over all $\bar{b} \in B_{\bar{S}}$ as $\bar{a}$ ranges over all of $A_{\bar{S}}$. Thus $\Gamma \models_{\mathcal{A}} \bar{\varphi}$ iff $\Gamma \models_{\mathcal{B}} \bar{\varphi}$. □

As in the case of Theorem 2.5, the following theorem, and the completeness theorem for hidden equational logic given below (Theorem 2.25), are valid in general only under the assumption that all sort domains of all models are nonempty.

Theorem 2.22 (Reduced Completeness of Hidden k-logics). For any hidden k-logic $\mathcal{L}$,

$$\vdash_{\mathcal{L}} \;=\; \models_{\mathrm{Mod}^*(\mathcal{L})},$$

i.e., for every set of k-formulas Γ and any k-formula $\bar{\varphi}$, $\Gamma \vdash_{\mathcal{L}} \bar{\varphi}$ iff $\Gamma \models_{\mathrm{Mod}^*(\mathcal{L})} \bar{\varphi}$.

Proof. In view the Completeness Theorem (2.5) and the fact that, by Theorem 2.19, $\mathrm{Mod}^*(\mathcal{L}) = \{\, \mathcal{A}^* : \mathcal{A} \in \mathrm{Mod}(\mathcal{L}) \,\}$, it suffices to prove that, for any k-data structure $\mathcal{A} = \langle A, F\rangle$, $\models_{\mathcal{A}} = \models_{\mathcal{A}^*}$. Thus, by Theorem 2.21, it suffices to show that $\mathcal{A}^*$ is a strict homomorphic image of $\mathcal{A}$.

Let $h\colon A \to A^*$ be the natural homomorphism. We must show $h^{-1}(F^*) = F$, so suppose

$\bar{a} \in A$ and $h(\bar{a}) \in F^* = F/\Omega_A(F)$. This means that $\bar{a} \equiv \bar{a}' \, (\Omega_A(F)^k)$ for some $\bar{a}' \in F$. Thus, since $\Omega_A(F)$ is compatible with F, $\bar{a} \in F$. □

When applied to hidden equational logics, Theorem 2.16 takes a more natural form in terms of 1-dimensional contexts as we now see.

Theorem 2.23. Let Σ be an hidden signature and let $\mathcal{A} = \langle A, F \rangle$ be a model of the free HEL_Σ, i.e., F is a VIS-congruence on A. Then, for every $S \in \mathrm{SORT}$ and all $a, a' \in A_S$, $a \equiv_{\Omega(F)_S} a'$ iff, for every visible S-context $\varphi(z{:}S, u_1{:}Q_1, \ldots, u_m{:}Q_m){:}V$ and for all $b_1 \in A_{Q_1}, \ldots, b_m \in A_{Q_m}$,

$$\varphi^A(a, b_1, \ldots, b_m) \equiv \varphi^A(a', b_1, \ldots, b_m) \mod F_V. \tag{9}$$

Proof. By Theorem 2.16, $a \equiv_{\Omega(F)_S} a'$ iff, for every (2,S)-context $\langle \varphi(z{:}S,\ \bar{u}{:}\bar{Q}), \psi(z{:}S,\ \bar{u}{:}\bar{Q}) \rangle$ of sort V, and every $\bar{b} \in A_{\bar{Q}}$,

$$\varphi^A(a,\ \bar{b}) \equiv \psi^A(a,\ \bar{b}) \mod F_V \quad \text{iff} \quad \varphi^A(a',\ \bar{b}) \equiv \psi^A(a',\ \bar{b}) \mod F_V. \tag{10}$$

Suppose (9) holds for every S context $\varphi(z, \bar{u})$ and every $\bar{b} \in A_{\bar{Q}}$. If $\varphi^A(a,\ \bar{b}) \equiv_{F_V} \psi^A(a,\ \bar{b})$, then

$$\varphi^A(a',\ \bar{b}) \equiv \varphi^A(a,\ \bar{b}) \equiv \psi^A(a,\ \bar{b}) \equiv \psi^A(a', \bar{b}) \mod F_V$$

(the first and third equivalences hold because F is a VIS-congruence). Thus (10) holds for every pair of S-contexts and every sequence of parameters $\bar{b}$, i.e., $a \equiv_{\Omega(F)_V} a'$.

Conversely, assume $a \equiv_{\Omega(F)_V} a'$. Let $\varphi(z{:}S,\ \bar{u}{:}\bar{Q}){:}V$ be an arbitrary visible S-context, where $\bar{u}{:}\bar{Q} = \langle u_1{:}Q_1, \ldots, u_m{:}Q_m \rangle$. Let u_{n+1} be a new parametric variable of sort V; the single term u_{n+1} can be viewed as a visible S-context with designated variable z (which does not actually occur) and parametric variables $\bar{u}^+ := \langle u_1, \ldots, u_n, u_{n+1} \rangle$. φ can also be viewed as an S-context with the same parametric variables. Let $\langle b_1, \ldots, b_n \rangle$ be any system of parameters of sort $\bar{Q}$, and extend it to a system $\bar{b}^+ := \langle b_1, \ldots, b_{n+1} \rangle$, where $b_{n+1} = \varphi^A(a, \bar{b})$. Thus $\varphi^A(a, \bar{b}^+) = b_{n+1} = u^A_{n+1}(a, \bar{b}^+)$. So by (10), $\varphi^A(a', \bar{b}^+) \equiv_{F_V} u^A_{n+1}(a', \bar{b}^+)$. But $u^A_{n+1}(a', \bar{b}^+)$ also equals b_{n+1}. So $\varphi^A(a, \bar{b}) \equiv_{F_V} \varphi^A(a', \bar{b})$. Thus (9) holds for every S context $\varphi(z, \bar{u})$ and every $\bar{b} \in A_{\bar{Q}}$. □

Applying this result to equality models, we get that a and a' are behaviorally equivalent in the sense of Definition 2.12 iff $a \equiv a' \, \big(\Omega_A(\mathrm{id}_{A_{\mathrm{VIS}}})\big)$; hence behavioral equivalence over k-data structures does indeed generalize the familiar notion of behavioral equivalence over a sorted algebra. This result was obtained independently by Goguen and Malcolm (Goguen and Malcolm 2000).

For hidden equational logics the Leibniz relation has the following useful property; this also can be found in (Goguen and Malcolm 1999; Goguen and Malcolm 2000) for the case of equality models.

Corollary 2.24. Let $\mathcal{A} = \langle A, F \rangle$ be a model of the free HEL_Σ. Then $\Omega_A(F)$ is the largest congruence in A whose visible part is F.

Proof. Suppose $a \equiv a' \, \big(\Omega_A(F)_V\big)$ with $V \in \mathrm{VIS}$. Let z be a variable of sort V. Then z is a visible V-context and hence $a = z^A(a) \equiv z^A(a') = a' \mod F_V$. Thus $\Omega_A(F)_{\mathrm{VIS}} \subseteq F$. Conversely, assume $a \equiv a' \mod F_V$. Then for every V-context $\varphi(z, \bar{u})$ and every choice

of parameters $\bar{b} \in A_{\bar{Q}}$, we have $\varphi^A(a, \bar{b}) \equiv \varphi^A(a', \bar{b}) \mod F_V$. Thus $a \equiv a' (\Omega_A(F)_V)$ and hence $\Omega_A(F)_{\mathrm{VIS}} = F$. If Θ is any other congruence on A such that $\Theta_{\mathrm{VIS}} = F$, then Θ is compatible with F, and hence $\Theta \subseteq \Omega_A(F)$. □

As a special case we have that $\Omega_A(\mathrm{id}_{A_{\mathrm{VIS}}})_{\mathrm{VIS}} = \mathrm{id}_{A_{\mathrm{VIS}}}$, i.e., two visible elements of a Σ-algebra are behaviorally equivalent only if they are equal.

The following completeness theorem for hidden and unrestricted equational logic is special case of Theorems 2.5 and 2.22. Recall that $\mathrm{Mod}^{=}(\mathcal{L})$ is the set of all equality models of a HEL or UHEL $\mathcal{L}$.

Theorem 2.25 (Completeness Theorem for Equational Logic). Let $\mathcal{L}$ be a HEL_Σ or a UHEL_Σ. Then the following are equivalent for every visible conditional equation ξ in the HEL case and every arbitrary conditional equation ξ in the UHEL case.

(i) ξ is a derivable rule of $\mathcal{L}$;
(ii) ξ is a valid rule of $\mathrm{Mod}(\mathcal{L})$;
(iii) ξ is a quasi-identity of $\mathrm{Mod}^{=}(\mathcal{L})$;
(iv) ξ is a quasi-identity of $\mathrm{Mod}^{*}(\mathcal{L})$.

In particular, a visible or unrestricted equation ψ is a theorem of $\mathcal{L}$ iff it is a validity of $\mathrm{Mod}(\mathcal{L})$ iff it is an identity of $\mathrm{Mod}^{=}(\mathcal{L})$ iff it is an identity of $\mathrm{Mod}^{*}(\mathcal{L})$.

Proof. The equivalence of items (i), (ii), and (iv) follows immediately from Theorem 2.5. The equivalence of these with (iii) is an immediate consequence of the fact that $\mathrm{Mod}^{*}(\mathcal{L}) \subseteq \mathrm{Mod}^{=}(\mathcal{L})$ which follows from Corollary 2.24. □

As in the case of the completeness theorems for hidden k-logic, this theorem is valid in general only under the assumption that all sort domains of models are nonempty. If this restriction is lifted, then a more complex formalization of equational logic is required; see for example (Ehrig and Mahr 1985). For single-sorted equational logics the theorem is well known; see for example (Gorbunov 1998).

It is commonplace in the literature of hidden equational logic to restrict attention exclusively to equality models that are not necessarily reduced; see for instance (Goguen and Malcolm 2000). The completeness theorem shows that this is justified.

3. Behavioral Reasoning

The concept of a *behaviorally valid consequence* (Definition 3.1 below) was introduced in order to reason effectively about behavioral equivalence. It has been a useful device for importing the techniques and intuitions of transition systems into the equational paradigm. In the present context it takes the form of an un-hidden and normally non-specifiable HEL associated with every k-logic. The basis of behaviorally valid consequence proof theory has been coinduction, in some form, in combination with ordinary equational deduction.

The behavioral validity for equations and conditional equations was introduced by Reichel in 1984 (Reichel 1985). These notions and their proof theory have been studied by a number of researchers: Goguen, Malcolm and Roşu (Goguen and Malcolm 1999;

Goguen and Malcolm 2000; Roşu and Goguen 2000; Roşu 2000; Roşu and Goguen 2001); Bidoit and Hennicker (Bidoit and Hennicker 1996; Hennicker 1997); Leavens and Pigozzi (Leavens and Pigozzi 2002).We concentrate here on the behavioral validity of conditional equations and the methods by which this validity can be established. Following the abstract algebraic logic approach, we take as the basis for our investigations Leibniz congruences on the term algebra and their combinatorial properties.

Our particular characterization of behavioral validity of a conditional equation is given in Theorem 3.4. The use of un-hidden equational logic in verifying behavioral validity of conditional equations is addressed in Theorem 3.10. As a corollary we get that the set of all behaviorally valid conditional equations is closed under un-hidden equational deduction (Corollary 3.13).

In the last part of the section we consider the important problem of determining when a HEL $\mathcal{L}$ has specifiable behavior, i.e, when there exists a set of axioms and rules in the form of equations and conditional equations respectively such that an equation $t \approx s$ (of arbitrary sort) is a behaviorally valid consequence of a set E of equations iff $t \approx s$ is derivable from E in standard equational using the given axioms and rules. Several characterizations of this property are obtained. Possibly the most interesting deals with the notion of a *cobasis*. This concept, introduced in (Roşu and Goguen 2001), has served as the principal method of partially verifying the behavioral validity of hidden equations in a large class of HEL's. We show that the behavior of a HEL is specifiable just in case it has a cobasis of a very special kind (Theorem 3.20).

The definition of a behaviorally specifiable HEL is given in Definition 3.14. In Theorem 3.19 those HEL's that are behaviorally specifiable are characterized in terms of the consequence of the HEL. As a consequence, in Theorem 3.22 we obtain for behaviorally specifiable HEL's a characterization of behaviorally valid conditional equations.

Definition 3.1. Let K be a class of k-data structure over the hidden signature Σ.

(i) An equation $t \approx t'$ of arbitrary sort is said to be a *behaviorally valid consequence* of a set E of equations (of arbitrary sorts) over K, in symbols $E \models^{\mathrm{beh}}_K t \approx t'$, if, for every $\mathcal{A} \in K$ and every assignment $h : X \to A$, $h(t) \equiv^{\mathrm{beh}}_{\mathcal{A}} h(t')$ whenever $h(s) \equiv^{\mathrm{beh}}_{\mathcal{A}} h(s')$ for every equation $s \approx s'$ in E.

(ii) An equation $t \approx t'$ is *behaviorally valid* over K if $\models^{\mathrm{beh}}_K t \approx t'$, and a conditional equation $t_0 \approx t'_0, \ldots, t_{n-1} \approx t'_{n-1} \to t_n \approx t'_n$ is *behaviorally valid* over K if $\{t_0 \approx t'_0, \ldots, t_{n-1} \approx t'_{n-1}\} \models^{\mathrm{beh}}_K t_n \approx t'_n$.

We write $\models^{\mathrm{beh}}_{\mathcal{A}}$ for $\models^{\mathrm{beh}}_{\{\mathcal{A}\}}$.

By Theorem 2.16 the behavioral equivalence relation over a k-data structure $\mathcal{A} = \langle A, F\rangle$ coincides with the Leibniz congruence $\Omega_A(F)$. So the 2-data structure $\langle A, \equiv^{\mathrm{beh}}_{\mathcal{A}}\rangle$ is a model of the free UHEL_Σ. Moreover, $\models^{\mathrm{beh}}_K$ coincides with the valid consequence relation $\models_{K'}$ (Definition 2.3), where $K' = \{\, \langle A, \Omega_A(F)\rangle : \langle A, F\rangle \in K \,\}$. So $\langle \Sigma, \models^{\mathrm{beh}}_K\rangle$ is an UHEL_Σ. In this way we can associate a generally un-specifiable UHEL with every hidden k-logic $\mathcal{L}$ by taking the behavioral consequence relation determined by the class of models of $\mathcal{L}$.

Definition 3.2. Let $\mathcal{L}$ be a hidden k-logic over a hidden signature Σ.

(i) An equation $t \approx t'$ is said to be a *behaviorally valid consequence* of a set E of equations over $\mathcal{L}$, in symbols $E \models^{\text{beh}}_{\mathcal{L}} t \approx t'$, if $E \models^{\text{beh}}_{\text{Mod}(\mathcal{L})} t \approx t'$.
(ii) An equation or conditional equation is *behaviorally valid over* $\mathcal{L}$ if it is behaviorally valid over $\text{Mod}(\mathcal{L})$.

One of the central problems of hidden k-logic is specifying in some effective way the behavioral validities of a given $\mathcal{L}$. This can sometimes be facilitated by isolating a subclass K of $\text{Mod}(\mathcal{L})$ with special properties such that is *behaviorally complete* for $\mathcal{L}$ in the sense that $\equiv^{\text{beh}}_{\mathcal{L}} = \equiv^{\text{beh}}_{K}$. A *Lindenbaum model* of $\mathcal{L}$ (the term comes from abstract algebraic logic) is a model whose underlying algebra is the term algebra, i.e., a model of the form $\langle \text{Te}_\Sigma, T\rangle$ (so T is a theory of $\mathcal{L}$). In the sequel, the Leibniz congruence over a theory T on Te_Σ will be denoted by $\Omega(T)$ instead of $\Omega_{\text{Te}_\Sigma}(T)$. To show that the Lindenbaum models are behaviorally complete for $\mathcal{L}$ we require the following technical lemma.

A k-data structure $\mathcal{B} = \langle B, G\rangle$ is a *substructure* of a k-data structure $\mathcal{A} = \langle A, F\rangle$ over the hidden signature Σ if B is a subalgebra of A and $G = F \cap B^k$, that is, the sorted intersection of $F = \langle\, F_S : S \in \text{SORT}\,\rangle$ and $B^k = \langle\, B^k_S : S \in \text{SORT}\,\rangle$. It is easy to see that $\mathcal{B} \in \text{Mod}(\mathcal{L})$ whenever $\mathcal{A} \in \text{Mod}(\mathcal{L})$. It is also easy to see that the inverse image of a model under an algebra homomorphism is also a model. More precisely, if $\mathcal{L} \in \text{Mod}(\mathcal{L})$ and $h{:}B \to A$ is a homomorphism of algebras, then $\langle B, h^{-1}(F)\rangle \in \text{Mod}(\mathcal{L})$. In particular, $\sigma^{-1}(T)$ is a theory of $\mathcal{L}$ for every theory T and every substitution $\sigma{:}X \to \text{Te}_\Sigma$. This fact is used in the proof of Corollary 3.6 below.

Lemma 3.3. Let $\mathcal{A} = \langle A, F\rangle$ be an arbitrary k-data structure over a hidden signature Σ. Let $t \approx t'$ be any equation and E any set of equations (all of arbitrary sort). If $E \models^{\text{beh}}_{\mathcal{B}} t \approx t'$ for every locally countable substructure $\mathcal{B}$ of $\mathcal{A}$, then $E \models^{\text{beh}}_{\mathcal{A}} t \approx t'$.

In particular, if a conditional equation is behaviorally valid in every locally countable substructure of $\mathcal{A}$, then it is behaviorally valid in $\mathcal{A}$.

Proof. Assume $E \not\models^{\text{beh}}_{\mathcal{A}} t \approx t'$. Then there is an assignment $g : X \to A$ such that $g(s) \equiv^{\text{beh}}_{\mathcal{A}} g(s')$ for all $s \approx s'$ in E, but $g(t) \not\equiv^{\text{beh}}_{\mathcal{A}} g(t')$. Let S be the common sort of t and t'. Then by the definition of behavioral equivalence there is a visible (k, S)-context $\bar\varphi(z{:}S, \bar u{:}\bar T){:}U$, with $\bar u{:}\bar T = \langle u_1{:}T_1, \ldots, u_m{:}T_m\rangle$ and $\bar b \in A_{T_1} \times \cdots \times A_{T_m}$ such that $\bar\varphi^A(g(t), \bar b) \in F_U$ and $\bar\varphi^A(g(t'), \bar b) \notin F_U$ or vise-versa.

Let $\mathcal{B} = \langle B, F \cap B^k\rangle$ be the subalgebra of A generated by $g(X) \cup \bar b$; $\mathcal{B}$ is locally countable since X is locally countable and $\bar b$ is finite. Then $g(t), g(t') \in B$ for all $t \approx t'$ in E, and $\bar\varphi^B(g(t), \bar b) = \bar\varphi^A(g(t), \bar b) \in F \cap B^k$ and $\bar\varphi^A(g(t'), \bar b) = \bar\varphi^B(g(t'), \bar b) \notin F \cap B^k$, or vise-versa. So $g(t) \not\equiv^{\text{beh}}_{\mathcal{B}} g(t')$.

On the other hand, for each $s{:}S \approx s'{:}S$ in E, $g(s), g(s') \in B$ and hence, for every visible (k, S)-context $\bar\psi(z{:}S, \bar u{:}\bar U){:}W$ and all $\bar c \in B_{\bar U}$, we have $\bar\psi^B(g(s), \bar c) = \bar\psi^A(g(s), \bar c) \in F \cap B^k$ iff $\bar\psi^B(g(s'), \bar c) = \bar\psi^A(g(s'), \bar c) \in F \cap B^k$. So $g(s) \equiv^{\text{beh}}_{\mathcal{B}} g(s')$ for each $s \approx s'$ in E.

Thus $E \not\models^{\text{beh}}_{\mathcal{B}} t \approx t'$ □

The following theorem may be viewed of as a form of coinduction for conditional equations. It gives a characterization, in terms of combinatorial properties of Leibniz congruences on the term algebra, for a conditional equation to be behaviorally valid in

a given hidden k-logic. It should be compared with the coinduction rule in (Roşu and Goguen 2000) for verifying the behavioral validity of equations in HEL's.

Theorem 3.4. Let $\mathcal{L}$ be a hidden k-logic. Then the Lindenbaum models of $\mathcal{L}$ are behaviorally complete for $\mathcal{L}$. More precisely:

(i) Let $t \approx t'$ be an equation and E a set of equations (all of arbitrary sort). Then $E \models^{\text{beh}}_{\mathcal{L}} t \approx t'$ iff

$$\forall\, T \in \mathrm{Th}(\mathcal{L})\, \big(\big(\forall\, (s \approx s' \in E)\, (s \equiv_{\Omega(T)} s')\big) \Rightarrow t \equiv_{\Omega(T)} t'\big). \tag{11}$$

(ii) A conditional equation

$$t_0 \approx t'_0, \ldots, t_{n-1} \approx t'_{n-1} \to t_n \approx t'_n. \tag{12}$$

is behaviorally valid over $\mathcal{L}$ iff

$$\forall\, T \in \mathrm{Th}(\mathcal{L})\big(\big(\forall\, i < n\ (t_i \equiv_{\Omega(T)} t'_i)\big) \Rightarrow t_n \equiv_{\Omega(T)} t'_n\big).$$

Proof. (i): Assume $E \models^{\text{beh}}_{\mathcal{L}} t \approx t'$. Let $T \in \mathrm{Th}(\mathcal{L})$ such that $s \equiv_{\Omega(T)} s'$ for all $s \approx s'$ in E. Let $\mathcal{A} = \langle \mathrm{Te}_\Sigma, T\rangle$; $\mathcal{A} \in \mathrm{Mod}(\mathcal{L})$ by definition of theory. Thus $s \equiv^{\text{beh}}_{\mathcal{A}} s'$ for all $s \approx s'$ in E by Theorem 2.16. It follows that $t \equiv^{\text{beh}}_{\mathcal{A}} t'$ by the assumption $E \models^{\text{beh}}_{\mathcal{L}} t \approx t'$. So the condition (11) holds

Conversely, assume (11) holds. By Lemma 3.3(ii) it suffices to show that $E \models^{\text{beh}}_{\mathcal{A}} t \approx t'$ for every locally countable model of $\mathcal{L}$.

Without loss of generality we assume that, for each sort S there are a countable number of variables of sort S that are not contained in $t \approx t'$ or in any of the equations in E; if this were not the case, then by replacing variables uniformly on a one-to-one basis we can obtain $\hat{t} \approx \hat{t}'$ and $\widehat{E} = \{\, \hat{s} \approx \hat{s}' : (s \approx s') \in E \,\}$ with this property and such that $\widehat{E} \models^{\text{beh}}_{\mathcal{L}} \hat{t} \approx \hat{t}'$ iff $E \models^{\text{beh}}_{\mathcal{L}} t \approx t'$.

Let $\mathcal{A} = \langle A, F\rangle \in \mathrm{Mod}(\mathcal{L})$ be locally countable, and let $h : X \to A$ be an arbitrary assignment such that $h(s)$ and $h(s')$ are behaviorally equivalent in $\mathcal{A}$, i.e., $h(s) \equiv_{\Omega_A(F)} h(s')$, for every $s \approx s'$ in E. If h (more precisely, its unique extension $h^* : \mathrm{Te}_\Sigma \to A$) is not surjective, it is clear that it can be replaced by an assignment that is surjective and such that t and t' take the same value, and also s and s' take the same value for each $s \approx s'$ in E. (This uses the assumption that for each sort S there are a countable number of variables of sort S that are not contained in $t \approx t'$ or in any of the equations in E.) Thus we may assume h itself is surjective without loss of generality.

Let $T = h^{-1}(F)$. Then T is a theory of $\mathcal{L}$ and, by Lemma 2.18, $\Omega_{\mathrm{Te}_\Sigma}(T) = h^{-1}(\Omega_A(F))$. Thus, $s \equiv_{\Omega(T)} s'$ for each $s \approx s'$ in E. So by hypothesis, $t \equiv_{\Omega(T)} t'$. Hence, $h(t) \equiv_{\Omega(F)} h(t')$, by Lemma 2.18.

(ii) is an immediate consequence of part (i). □

In application to hidden equational logic, this result takes a simpler form, but this requires the notion of an extension of a k-logic by additional axioms and rules of inference.

Definition 3.5. Let $\mathcal{L}$ be a HEL_Σ and E a set of equations and conditional equations of arbitrary, possibly un-hidden, sort. We define $\mathcal{L}^{\text{UH}}[E]$ as the natural extension of $\mathcal{L}$ by E to a UHEL over the same signature.

If $\mathcal{L}$ is specifiable, $\mathcal{L}^{\text{UH}}[E]$ is the specifiable UHEL whose extra-logical axioms and inference rules are obtained by adjoining E to those of $\mathcal{L}$. For an arbitrary $\mathcal{L}$, $\mathcal{L}^{\text{UH}}[E]$ is the UHEL whose theories are the congruence relations Θ on the entire term algebra Te_Σ such that

- $\Theta_{\text{VIS}} \in \text{Th}(\mathcal{L})$;
- Θ is closed under the equations and conditional equations of E in the following sense. For every equation $t \approx t' \in E$ and substitution $\sigma{:}X \to \text{Te}_\Sigma$, $\sigma(t) \approx \sigma(t') \in \Theta$, and for every conditional equation $t_0 \approx t'_0, \ldots, t_{n-1} \approx t'_{n-1} \to t_n \approx t'_n$ in E and every $\sigma{:}X \to \text{Te}_\Sigma$, if $h(t_i) \approx \sigma(t'_i) \in \Theta$ for all $i < n$, then $\sigma(t_n) \approx \sigma(t'_n) \in \Theta$.

$\mathcal{L}^{\text{UH}}$ is the extension of $\mathcal{L}$ to a UHEL with no additional axioms and rules of inference; its theories are the congruences on Te_Σ whose visible part is a theory of $\mathcal{L}$. If E is a set of visible equations and conditional equations, then $\mathcal{L}[E]$ is the HEL obtained by adjoining E as new axioms and rules of inference.

For each theory T of $\mathcal{L}$ we have $\Omega(T)_{\text{VIS}} = T$ by Corollary 2.24. Thus $\Omega(T) \in \text{Th}(\mathcal{L}^{\text{UH}})$. More generally, it follows easily from Corollary 2.24 that, if $\langle A, F\rangle \in \text{Mod}(\mathcal{L})$, then $\langle A, \Omega(F)\rangle \in \text{Mod}(\mathcal{L}^{\text{UH}})$.

Corollary 3.6. Let $\mathcal{L}$ be a HEL, and let E be a set of equations and conditional equations of arbitrary type. Then every equation and conditional equation in E is behaviorally valid over $\mathcal{L}$ iff for every $T \in \text{Th}(\mathcal{L})$, $\Omega(T) \in \text{Th}(\mathcal{L}^{\text{UH}}[E])$.

Proof. Assume each conditional equation of E is behaviorally valid over $\mathcal{L}$. (For simplicity we treat equations as conditional equations with an empty set of antecedents.) Let $T \in \text{Th}(\mathcal{L})$. As we have previously observed, $\Omega(T) \in \text{Th}(\mathcal{L}^{\text{UH}})$. Thus to show $\Omega(T) \in \text{Th}(\mathcal{L}^{\text{UH}}[E])$ it suffices to show that $\Omega(T)$ is closed under each conditional equation in E. Let $\xi \in E$ be of the form (12) and let $\sigma : X \to \text{Te}_\Sigma$ be a substitution such that, for all $i < n$, $\sigma(t_i) \equiv \sigma(t'_i)\,\big(\Omega(T)\big)$, i.e., $t_i \equiv t'_i\,\big(\sigma^{-1}(\Omega(T))\big)$. Assume for the time being that σ is surjective (as an endomorphism of the term algebra). Then, for each $i < n$, $t_i \equiv t'_i\,\big(\Omega(\sigma^{-1}(T))\big)$ by Lemma 2.18. Thus, since $\sigma^{-1}(T) \in \text{Th}(\mathcal{L})$ and ξ is behaviorally valid over $\mathcal{L}$ by assumption, we have by Theorem 3.4 that $t_n \equiv t'_n\,\big(\sigma^{-1}(\Omega(T))\big)$, i.e., $\sigma(t_n) \equiv \sigma(t'_n)\,\big(\Omega(T)\big)$.

Suppose now that σ is not surjective. Let $\tau : X \to \text{Te}_\Sigma$ be a surjective substitution such that $\tau(x) = \sigma(x)$ for each variable occurring in ξ; this is possible since there are only finitely many of these variables. Then $\tau(t_i) \equiv \tau(t'_i)\,\big(\Omega(T)\big)$ for each $i < n$, since $\tau(t_i) = \sigma(t_i)$ and $\tau(t'_i) = \sigma(t'_i)$. So by the first part of the proof, $\sigma(t_n) = \tau(t_n) \equiv_{\Omega(T)} \tau(t'_n) = \tau(t_n)$. Thus $\Omega(T)$ is closed under ξ for every $\xi \in E$, and hence $\Omega(T) \in \text{Th}(\mathcal{L}^{\text{UH}}[E])$.

For the implication in the other direction, assume $\Omega(T) \in \text{Th}(\mathcal{L}^{\text{UH}}[E])$ for each $T \in \text{Th}(\mathcal{L})$. Let $T \in \text{Th}(\mathcal{L})$, and let ξ be a conditional equation in E of the form (12). Suppose that, for all $i < n$, $t_i \equiv t'_i\,\big(\Omega(T)\big)$. Then $t_n \equiv t'_n\,\big(\Omega(T)\big)$ since $\Omega(T) \in \text{Th}\big(\mathcal{L}^{\text{UH}}[E]\big)$ by assumption. So ξ is behaviorally valid over $\mathcal{L}$ by Theorem 3.4. □

As a special case of this result we have that an equation $t \approx t'$ is behaviorally valid over $\mathcal{L}$ iff $t \equiv t'\,\big(\Omega(\text{Thm}(\mathcal{L}))\big)$.

In the following corollaries we give two simpler characterizations for conditional equa-

tions of a special kind to be behaviorally valid in a HEL $\mathcal{L}$; in the first case the antecedents are all visible and in the second it is the consequent that is visible.

If the antecedents of the conditional equation (12) are all visible then condition (ii) of Theorem 3.4 can be simplified since, in this case, $t_i \equiv t'_i\,(\Omega(T))$ iff $t_i \equiv t'_i\,(T)$ by Corollary 2.24. Thus we get the following result. Recall that, for any set of E equations, $\mathrm{Cn}_{\mathcal{L}}(E)$ is the intersection of all theories of $\mathcal{L}$ that include E.

Corollary 3.7. Let $\mathcal{L}$ be a HEL. A conditional equation (12) with visible antecedents is behaviorally valid over $\mathcal{L}$ iff $t_n \equiv t'_n\,(\Omega(\mathrm{Cn}_{\mathcal{L}}\{\, t_i \approx t'_i : i < n \,\}))$.

Furthermore, if the antecedents of the conditional equation are visible ground terms, then condition (ii) of Theorem 3.4 can be written in the form

$$t_n \equiv t'_n\,(\Omega(\mathrm{Thm}(\mathcal{L}[\{\, t_i \approx t'_i : i < n \,\}]))). \tag{13}$$

For this it is enough to note that $\mathrm{Cn}_{\mathcal{L}}\{\, t_i \approx t'_i : i \leq n\}$ is the set of all theorems of the HEL $\mathcal{L}[\{\, t_i \approx t'_i : i < n \,\}]$. This result can be found in (Roşu 2000), where it is called the *Deduction Theorem*.

If the consequent $t_n \approx t'_n$ of the conditional equation (12) is visible, then the characterization of behavioral validity given in Theorem 3.4 can be simplified in the following way.

Corollary 3.8. Let $\mathcal{L}$ be a HEL. A conditional equation (12) with a visible consequent is behaviorally valid over $\mathcal{L}$ iff

$$t_n \equiv t'_n\,(\mathrm{Cn}_{\mathcal{L}}(\textstyle\bigcup_{i<n}\{\, \varphi(t_i, \bar{x}) \approx \varphi(t'_i, \bar{x}) : \varphi \text{ an appropriate context for } t_i, t'_i \,\})).$$

Proof. Let

$$G = \mathrm{Cn}_{\mathcal{L}}(\textstyle\bigcup_{i<n}\{\, \varphi(t_i, \bar{x}) \approx \varphi(t'_i, \bar{x}) : \varphi \text{ an appropriate context for } t_i, t'_i \,\}).$$

Assume (12) is not behaviorally valid over $\mathcal{L}$. Then by Theorem 3.4 there is a theory T of $\mathcal{L}$ such that

$$t_i \equiv t'_i\,(\Omega(T)), \text{ for all } i < n, \quad \text{and} \quad t_n \not\equiv t'_n\,(\Omega(T)). \tag{14}$$

From the first condition we conclude by Theorem 2.23 that $\varphi(t_i, \bar{x}) \equiv \varphi(t'_i, \bar{x})\,(T)$ for each $i < n$, and hence, by definition of G, that $G \subseteq T$. Since t_n, t'_n are visible, from the second condition of (14) we conclude that $t_n \not\equiv t'_n\,(T)$. So $t_n \not\equiv t'_n\,(G)$.

Assume now that (12) is behaviorally valid over $\mathcal{L}$. $G \in \mathrm{Th}(\mathcal{L})$ and, by definition of G, $t_i \equiv t'_i\,(\Omega(G))$. Hence, by Theorem 3.4, we get that $t_n \equiv t'_n\,(\Omega(G))$. Thus $t_n \equiv t'_n\,(G)$ since t_n, t'_n are visible. □

The next corollary states another straightforward consequence of Theorem 3.4, the theorems of the UHEL-expansion $\mathcal{L}^{\mathrm{UH}}$ of $\mathcal{L}$ are all behaviorally valid over $\mathcal{L}$, and, what is more interesting, the same is true for any extension of $\mathcal{L}^{\mathrm{UH}}$ obtained by adjoining a behaviorally valid conditional equation as a new inference rule.

Corollary 3.9. Let $\mathcal{L}$ be a HEL_{Σ}, and let ξ be a conditional equation (of arbitrary sort)

which is behaviorally valid over $\mathcal{L}$. Then for every Σ-equation $s \approx s'$ (of arbitrary sort), $\vdash_{\mathcal{L}^{\mathrm{UH}}[\xi]} s \approx s'$ implies that $s \approx s'$ is behaviorally valid over $\mathcal{L}$.

Proof. We want to show that $s \equiv s' \big(\mathrm{Thm}(\mathcal{L}^{\mathrm{UH}}[\xi])\big)$ implies $s \equiv s' \big(\Omega(\mathrm{Thm}(\mathcal{L}))\big)$. But $\mathrm{Thm}(\mathcal{L}^{\mathrm{UH}}[\xi]) \subseteq \Omega(\mathrm{Thm}(\mathcal{L}))$ because $\Omega(\mathrm{Thm}(\mathcal{L}))$ is a theory of $\mathcal{L}^{\mathrm{UH}}$, and hence also a theory of $\mathcal{L}^{\mathrm{UH}}[\xi]$ since, by Theorem 3.4 , it is closed under ξ as an inference rule. □

3.1. *Closure of behavioral validity under equational consequence*

Intuitively, since the terms of a behaviorally valid equation have exactly the same visible properties, adjoining it as a new axiom should not result in the provability of any new visible equations. And it was shown (Leavens and Pigozzi 2002, Theorem 3.18) that, not only is this indeed the case, but the property serves to actually characterize behaviorally valid equations. In the next theorem this result is generalized in a natural way to conditional equations. This gives another characterization of the conditional equations that are behaviorally valid over a given HEL entirely by means of standard equational logic, and it can be viewed as an alternative form of coinduction for conditional equations.

Theorem 3.10. Let $\mathcal{L}$ be a HEL, and let E be a set of (unrestricted) conditional equations. Then every rule in E is behaviorally valid over $\mathcal{L}$ iff every conditional equation with visible consequent that is a derivable rule of $\mathcal{L}^{\mathrm{UH}}[E]$ is already a derivable rule of $\mathcal{L}^{\mathrm{UH}}$, i.e., for every conditional equation $s_0 \approx s'_0, \ldots, s_{m-1} \approx s'_{m-1} \to s_m \approx s'_m$ with a visible consequent,

$$\{s_0 \approx s'_0, \ldots, s_{m-1} \approx s'_{m-1}\} \vdash_{\mathcal{L}^{\mathrm{UH}}[E]} s_m \approx s'_m \quad \text{implies} \quad \{s_0 \approx s'_0, \ldots, s_{m-1} \approx s'_{m-1}\} \vdash_{\mathcal{L}^{\mathrm{UH}}} s_m \approx s'_m. \tag{15}$$

Proof. Assume that each rule in E is behaviorally valid over $\mathcal{L}$. Assume in addition that

$$\{s_0 \approx s'_0, \ldots, s_{m-1} \approx s'_{m-1}\} \vdash_{\mathcal{L}^{\mathrm{UH}}[E]} s_m \approx s'_m \tag{16}$$

with $s_m \approx s'_m$ visible. Let G be any theory of $\mathcal{L}^{\mathrm{UH}}$ such that $s_i \equiv s'_i\,(G)$ for all $i < m$. G_{VIS} is a theory of $\mathcal{L}$ and $\Omega(G_{\mathrm{VIS}})$ is a theory of $\mathcal{L}^{\mathrm{UH}}[E]$ by Corollary 3.6, and since $G \subseteq \Omega(G_{\mathrm{VIS}})$, we have that $s_i \equiv s'_i\,(\Omega(G_{\mathrm{VIS}}))$ for each $i < m$. So by the assumption (16), $s_m \equiv s'_m\,(\Omega(G_{\mathrm{VIS}}))$. But then $s_m \equiv s'_m\,(G_{\mathrm{VIS}})$ since $s_m \approx s'_m$ is visible. Thus $\{s_0 \approx s'_0, \ldots, s_{m-1} \approx s'_{m-1}\} \vdash_{\mathcal{L}^{\mathrm{UH}}} s_m \approx s'_m$. This verifies (15).

Assume now that (15) holds for every conditional equation $s_0 \approx s'_0, \ldots, s_{m-1} \approx s'_{m-1} \to s_m \approx s'_m$ with visible consequent. By Corollary 3.6 it suffices to show that

$$\Omega\big(\mathrm{Th}(\mathcal{L})\big) \subseteq \mathrm{Th}(\mathcal{L}^{\mathrm{UH}}[E]). \tag{17}$$

Suppose $T \in \mathrm{Th}(\mathcal{L})$, and let $G = \mathrm{Cn}_{\mathcal{L}^{\mathrm{UH}}[E]}\big(\Omega(T)\big)$, the $\mathcal{L}^{\mathrm{UH}}[E]$-theory generated by $\Omega(T)$. We claim that $G_{\mathrm{VIS}} = T$. To see the inclusion from left to right, assume s, s' are visible terms such that $s \equiv s'\,(G)$. Since G is generated as a $\mathcal{L}^{\mathrm{UH}}[E]$-theory by $\Omega(T)$, there are equations $s_0 \approx s'_0, \ldots, s_{m-1} \approx s_{m-1}$ such that $s_i \equiv s'_i\,\big(\Omega(T)\big)$, for $i < m$, and $\{s_0 \approx s'_0, \ldots, s_{m-1} \approx s'_{m-1}\} \vdash_{\mathcal{L}^{\mathrm{UH}}[E]} s \approx s'$. Thus, by assumption, $\{s_0 \approx s'_0, \ldots, s_{m-1} \approx s'_{m-1}\} \vdash_{\mathcal{L}^{\mathrm{UH}}} s \approx s'$. Hence $s \equiv s'\,\big(\Omega(T)\big)$, since $\Omega(T)$ is a $\mathcal{L}^{\mathrm{UH}}$-theory as previously

observed. But $s \approx s'$ is visible, so $s \equiv s'(T)$. Thus $G_{\mathrm{VIS}} \subseteq T$. Since the opposite inclusion is obvious, we have verified the claim. Then $\Omega(T) = \Omega(G_{\mathrm{VIS}}) \supseteq G$; but obviously $\Omega(T) \subseteq G$. So $\Omega(T) = G \in \mathrm{Th}\big(\mathcal{L}^{\mathrm{UH}}[E]\big)$. Hence (17) holds and thus every rule in E is behaviorally valid over $\mathcal{L}$ by Corollary 3.6. □

Considering the analogous characterization of behavioral validity of equations (see (Leavens and Pigozzi 2002)), one might expect to be able to characterize the behavioral equivalence of the set E of conditional equations by the condition that any completely visible conditional equation that is a derivable rule of $\mathcal{L}^{\mathrm{UH}}[E]$ is already a derivable rule of $\mathcal{L}^{\mathrm{UH}}$, i.e., by the weaker version of (15) where the antecedents $s_0 \approx s'_0, \ldots, s_{m-1} \approx s'_{m-1}$ are all required to be visible. However, the following counterexample shows that the condition (15) in its full strength is necessary.

Consider the Flags example and the conditional equation

$$rev(rev(F)) \approx F \to dn(F) \approx F. \tag{18}$$

On one hand, since $rev(rev(F)) \approx F$ is behaviorally valid while $dn(F) \approx F$ is not, this is not a behaviorally valid conditional equation. On the other hand, the weaker version of (15), where the conditional equations are restricted to be visible, holds. This follows from the easily verified fact that no substitution instance of $rev(rev(F)) \approx F$ can be deduced from a visible set of equations; this implies that in deducing a visible equation from a set of visible equations, the inference rule (18) can never be applied.

Note that if the set of derivable (visible) conditional equations of $\mathcal{L}$ is recursive, then the set of behaviorally valid conditional equations over $\mathcal{L}$ is co-RE. This gives:

Corollary 3.11. Let $\mathcal{L}$ be a HEL. If the set of derivable rules of $\mathcal{L}$ is recursively enumerable (RE) then the set of behaviorally valid conditional equations over $\mathcal{L}$ is at level $\prod_2^0$ in the arithmetical hierarchy.

It is shown in (Buss and Roşu 2000) that there are HEL's with a finite presentation for which the set of behavioral valid equations is $\prod_2^0$-complete.

The following obvious consequence of Theorem 3.10 shows that the converse of Corollary 3.9 holds for visible equations.

Corollary 3.12. Let $\mathcal{L}$ be a HEL and let ξ be a behaviorally valid conditional equation over $\mathcal{L}$. Then, for every $s, s' \in (\mathrm{Te}_\Sigma)_{\mathrm{VIS}}$,

$$\vdash_{\mathcal{L}^{\mathrm{UH}}[\xi]} s \approx s' \quad \text{iff} \quad \vdash_{\mathcal{L}} s \approx s'. \tag{19}$$

In the final result of this subsection we show that the set E of all conditional equations that are behaviorally valid over a HEL $\mathcal{L}$ is closed under equational consequence in the sense that any conditional equation that is a derivable rule of $\mathcal{L}^{\mathrm{UH}}[E]$ is already a member of E.

Corollary 3.13. Let $\mathcal{L}$ be a HEL and let E be the set of all conditional equations that are behaviorally valid over $\mathcal{L}$. Then any conditional equation that is a derivable rule of $\mathcal{L}^{\mathrm{UH}}[E]$ is itself behaviorally valid over $\mathcal{L}$ and hence a member of E.

Proof. Let ξ be a conditional equation that is a derivable rule of $\mathcal{L}^{\text{UH}}[E]$. Clearly then

$$\vdash_{\mathcal{L}^{\text{UH}}[\xi]} \subseteq \vdash_{\mathcal{L}^{\text{UH}}[E]} . \tag{20}$$

Then, applying Theorem 3.10, we get that ξ is behaviorally valid. In fact, let $s_0 \approx s'_0, \ldots, s_{m-1} \approx s'_{m-1} \rightarrow s_m \approx s'_m$ be any conditional equation with visible consequent, and suppose that $\{s_0 \approx s'_0, \ldots, s_{m-1} \approx s'_{m-1}\} \vdash_{\mathcal{L}^{\text{UH}}[\xi]} s_m \approx s'_m$. Then, by (20), $\{s_0 \approx s'_0, \ldots, s_{m-1} \approx s_{m-1}\} \vdash_{\mathcal{L}^{\text{UH}}[E]} s_m \approx s'_m$. Hence, applying Theorem 3.10 we get $\{s_0 \approx s'_0, \ldots, s_{m-1} \approx s_{m-1}\} \vdash_{\mathcal{L}} s_m \approx s'_m$. Applying the theorem again, this time in the other direction and with $\{\xi\}$ in place of E, we conclude that ξ is behaviorally valid over $\mathcal{L}$. □

This result can lead to a greatly simplified specification of a HEL $\mathcal{L}$ by allowing hidden equations and conditional equations in the specification. But one must first verify that the new hidden axioms and rules are behaviorally valid over $\mathcal{L}$ (with its original specification). Because only then can one be assured, by Corollary 3.13, that the new specification is sound in the sense that it does not lead to behaviorally invalid conditional equations. This process is illustrated in the canonical case of stacks where the infinite list of visible axioms can be replaced by a finite number of hidden axioms. It is shown below in Example 3.24 that the following equations are behaviorally valid over $\mathcal{L}_{stacks}$.

$$pop(push(x, S)) \approx S \quad \text{and} \quad pop(empty) \approx empty. \tag{21}$$

Thus these equations can be added to the specification of stacks, as new axioms, without having unexpected behavioral consequences. Moreover, each of the infinite number of the axioms of the original specification is an equational consequence of the equations $pop(push(x, S)) \approx S$ and $pop(empty) \approx empty$ together with $top(push(x, S)) \approx x$. Hence, they can be replaced by these three simple equations.

3.2. *The specification of behavioral validity*

Recall that a k-logic is behaviorally specifiable if its behavioral consequence relation can be axiomatized in standard equational logic by a possibly infinite set of equations and conditional equations. Several characterizations of the behavioral specifiability of HEL's are presented in this subsection, one of which (the existence of a *finite equivalence system*) can be useful in practice. The behavioral specification problem for arbitrary k-logics is more complicated and will not be treated here; see (Martins 2004).

Definition 3.14. Let $\mathcal{L}$ be a k-logic. We say that $\mathcal{L}$ is *behaviorally specifiable* if there is a specifiable UHEL $\mathcal{L}'$, over the same signature, such that $\models^{\text{beh}}_{\mathcal{L}} = \vdash_{\mathcal{L}'}$ i.e., for every set of equations $E \cup \{t \approx t'\}$ (of arbitrary sort) we have $E \models^{\text{beh}}_{\mathcal{L}} t \approx t'$ iff $E \vdash_{\mathcal{L}'} t \approx t'$. We call $\mathcal{L}'$ a *behavioral specification* of $\mathcal{L}$.

The theory off behavioral specifiability simplifies considerably when restricted to hidden equational logic, and that is what we shall do in this subsection, with only an occasional reference to general k-logics.

If a HEL $\mathcal{L}$ is behaviorally specifiable, then it must be specifiable in the standard sense, i.e., its consequence relation $\vdash_{\mathcal{L}}$ is finitary in the sense that $E \vdash_{\mathcal{L}} t \approx s$ implies

$E' \vdash_{\mathcal{L}} t \approx s$ for some finite subset E' of E. To see this let $\mathcal{L}$ be a behavioral specification of $\mathcal{L}$. Then, since the equations are all visible, $E \vdash_{\mathcal{L}} t \approx s$ iff $E \vDash^{\mathrm{beh}}_{\mathcal{L}} t \approx s$ iff $E \vdash_{\mathcal{L}'} t \approx s$ iff for a finite $E' \subseteq E$ such that $E \vdash_{\mathcal{L}'} t \approx s$ iff $E' \vdash_{\mathcal{L}} t \approx s$.

Theorem 3.15. Let $\mathcal{L}$ be a HEL. A UHEL $\mathcal{L}'$ over the same signature is a behavioral specification of $\mathcal{L}$ iff $\Omega\big(\mathrm{Th}(\mathcal{L})\big) = \mathrm{Th}(\mathcal{L}')$.

To prove this theorem it is useful to first establish some properties of Ω as an abstract mapping from the set of theories of $\mathcal{L}$ into the set of congruences of the term algebra Te_{Σ}.

- Ω *is monotonic, i.e., if* $T, G \in \mathrm{Th}(\mathcal{L})$ *and* $T \subseteq G$, *then* $\Omega(T) \subseteq \Omega(G)$.

Note that $\Omega(T)$ is compatible with G. Indeed, suppose t, t', s, s' are visible terms such that $t \equiv_G s$, $t \equiv_{\Omega(T)} t'$, and $s \equiv_{\Omega(T)} s'$. Since the terms are all visible and $\Omega(T)_{\mathrm{VIS}} = T \subseteq G$, we have that $t \equiv_G t'$ and $s \equiv_G s'$. Hence, $t' \equiv_G s'$. Consequently, $\Omega(T) \subseteq \Omega(G)$ since $\Omega(G)$ is the largest congruence of Te_{Σ} compatible with G.

In abstract algebraic logic a logical system with the property that Ω is monotonic is said to be *protoalgebraic*. Although every HEL is protoalgebraic, not every hidden k-logic is. The characterization of behaviorally specifiable HEL's given in Theorem 3.20 can only be naturally generalized to protoalgebraic k-logics.

- *For any, possibly infinite, set* $\{ T_i : i \in I \}$ *of* $\mathcal{L}$*-theories, we have* $\Omega\big(\bigcap_{i\in I} T_i\big) = \bigcap_{i\in I} \Omega(T_i)$.

In fact, we have that $\Omega\big(\bigcap_{i\in I} T_i\big) \subseteq \Omega(T_i)$ for each $i \in I$ by the monotonicity of Ω. Thus $\Omega\big(\bigcap_{i\in I} T_i\big) \subseteq \bigcap_{i\in I} \Omega(T_i)$. But $\bigcap_{i\in I} \Omega(T_i)$ is a congruence compatible with each T_i and hence with $\bigcap_{i\in I} T_i$. So $\Omega\big(\bigcap_{i\in I} T_i\big) \supseteq \bigcap_{i\in I} \Omega(T_i)$.

Proof of Theorem 3.15. By Theorem 3.4 the condition that $\Omega\big(\mathrm{Th}(\mathcal{L})\big) = \mathrm{Th}(\mathcal{L}')$ is clearly sufficient for $\mathcal{L}'$ to be a behavioral specification of $\mathcal{L}$. To see that it is necessary, assume $\mathcal{L}'$ is a behavioral specification of $\mathcal{L}$. By Theorem 3.4 we have that, for each $T \in \mathrm{Th}(\mathcal{L})$, $\Omega(T)$ is closed under behaviorally valid consequence in $\mathcal{L}$, and hence $\Omega(T) \in \mathrm{Th}(\mathcal{L}')$. Conversely, suppose $G \in \mathrm{Th}(\mathcal{L}')$. Let $K = \{ T \in \mathrm{Th}(\mathcal{L}) : G \subseteq \Omega(T) \}$. Then by Theorem 3.4 again we have $G = \bigcap_{T\in K} \Omega(T)$. Hence $G = \Omega\big(\bigcap_{T\in K} T\big)$. So $G \in \Omega\big(\mathrm{Th}(\mathcal{L})\big)$. □

Lemma 3.16. Let $\mathcal{L}$ be a behaviorally specifiable HEL and $\mathcal{L}'$ a behavioral specification. If $G \in \mathrm{Th}(\mathcal{L}')$ is finitely generated, then G_{VIS} is also finitely generated as an $\mathcal{L}$-theory.

Proof. Let $K = \{ T : T \in \mathrm{Th}(\mathcal{L})$, T is finitely generated, and $T \subseteq G_{\mathrm{VIS}} \}$. Since G_{VIS} is itself an $\mathcal{L}$-theory, $G_{\mathrm{VIS}} = \bigcup_{T\in K} T$. We show that $G = \bigcup_{T\in K} \Omega(T)$. We first show that $\bigcup_{T\in K} \Omega(T)$ is an $\mathcal{L}'$-theory. K is obviously upward directed since any finite subset K' of K is included in the theory generated by the union of the set of finite generating sets of the members of K'. Thus $\{ \Omega(T) : T \in K \}$ is an upward directed set of $\mathcal{L}'$-theories since Ω is monotonic. So $\bigcup_{T\in K} \Omega(T)$ is an $\mathcal{L}'$ theory, since $\mathcal{L}'$ is specifiable. $\big(\bigcup_{T\in K} \Omega(T)\big)_{\mathrm{VIS}} = \bigcup_{T\in K} \Omega(T)_{\mathrm{VIS}} = \bigcup_{T\in K} T = G_{\mathrm{VIS}}$. Thus, since $\bigcup_{T\in K} \Omega(T)$ is an $\mathcal{L}'$-theory, $\bigcup_{T\in K} \Omega(T) = \Omega\big((\bigcup_{T\in K} \Omega(T))_{\mathrm{VIS}}\big) = \Omega(G_{\mathrm{VIS}}) = G$.

Assume now that G is finitely generated, say by a finite set of equations E. So there

is a finite subset K' of K such that $E \subseteq \bigcup_{T \in K'} \Omega(T)$, and hence, since $\Omega(K)$ is upward directed, there is an $T^* \in K$ such that $E \subseteq \bigcup_{T \in K'} \Omega(T) \subseteq \Omega(T^*) \subseteq G$. Since $\Omega(T^*)$ is an $\mathcal{L}'$-theory and contains a generating set of G, it must equal G. Hence $G_{\mathrm{VIS}} = \Omega(T^*)_{\mathrm{VIS}} = T^*$, and G_{VIS} is finitely generated. □

Many HEL's that arise in practice are behaviorally specifiable, $\mathcal{L}_{eflag}$ for example (see Examples 2.7 and 2.8). However, many are not; for example, $\mathcal{L}_{stacks}$ is not behaviorally specifiable (see (Martins 2004)). Our characterization of those HEL's that are behaviorally specifiable is based on the concept of an *equivalence system*.

Let Σ be an arbitrary hidden signature. By a *pre-equivalence system* over Σ we mean a double sorted set

$$E := \big\langle \, \langle \, E_{S,H}(x{:}H, y{:}H, \bar{u}{:}\bar{Q}) : S \in \mathrm{SORT} \, \rangle : H \in \mathrm{HID} \, \big\rangle,$$

where $E_{S,H}(x{:}H, y{:}H, \bar{u}{:}\bar{Q})$ is a possibly infinite set of equations of the form

$$\varphi(x{:}H, \bar{u} : \bar{Q}) \approx \varphi(y{:}H, \bar{u} : \bar{Q}), \tag{22}$$

where $\varphi(z{:}H, \bar{u}{:}\bar{Q})$ is an S-context and x, y are variables distinct from the parametric variables $\bar{u}{:}\bar{Q} := u_1{:}Q_1, u_2{:}Q_2, u_3{:}Q_3, \ldots$. To simplify notation we assume that this sequence is the same for all of the equations of E, so it may be infinite since there may be an infinite number of equations; any given equation (22) can of course contain only a finite number of them. We also assume that the distinguished variables x and y of (22) and all variables substituted for them in the sequel are distinct from the parametric variables. To assure this is possible we assume that $\bar{u}{:}\bar{Q}$ excludes an infinite number of variables of each sort in SORT.

An pre-equivalence system E is *visible* if all the equations (22) of E are visible, i.e., $E_{S,H} = \emptyset$ for each $S \in \mathrm{HID}$. In this case we think of E_H as a VIS-sorted set and write E in the form

$$E := \big\langle \, \langle \, E_{V,H}(x{:}H, y{:}H, \bar{u}{:}\bar{Q}) : V \in \mathrm{VIS} \, \rangle : H \in \mathrm{HID} \, \big\rangle.$$

In the sequel all pre-equivalence systems are assumed to be visible unless explicitly indicated otherwise. If

$$E_H(x{:}H, y{:}H, \bar{u}{:}\bar{Q}) := \langle E_{V,H}(x{:}H, y{:}H, \bar{u}{:}\bar{Q}) : V \in \mathrm{VIS} \rangle$$

is globally finite for each $H \in \mathrm{HID}$ (i.e., $\bigcup_{V \in \mathrm{VIS}} E_{V,H}$ is finite), E is said to be *locally globally finite*. As we have done before in similar situations we sometimes abuse notation by identifying the VIS-sorted set E_H with its union $\bigcup_{V \in \mathrm{VIS}} E_{V,H}$.

The following definition of an equivalence system for hidden equational logics is a special case of a more general notion of arbitrary hidden k-logics given in (Martins 2004).

Definition 3.17. A (visible) pre-equivalence system $E = \langle E_H(x{:}H, y{:}H, \bar{u}{:}\bar{Q}) : H \in \mathrm{HID} \rangle$ is called an *equivalence system* for a HEL $\mathcal{L}$ if the following conditions hold for every $H \in \mathrm{HID}$.

(i) $\vdash_{\mathcal{L}} E_H(x{:}H, x{:}H, \bar{u}{:}\bar{Q})$;
(ii) $E_H(x{:}H, y{:}H, \bar{u}{:}\bar{Q}) \vdash_{\mathcal{L}} E_H(y{:}H, x{:}H, \bar{u}{:}\bar{Q})$;

(iii) $E_H(x{:}H, y{:}H, \bar{u}{:}\bar{Q}), E_H(y{:}H, z{:}H, \bar{u}{:}\bar{Q}) \vdash_{\mathcal{L}} E_H(x{:}H, z{:}H, \bar{u}{:}\bar{Q})$;
(iv) For each operation symbol O of type $S_0, \ldots, S_{n-1} \to S_n$,

(a) If $S_n \notin \text{VIS}$ then

$$\bigcup_{i<n} \{\, E_{S_i}(x_i{:}S_i, y_i{:}S_i, \bar{u}{:}\bar{Q}) : S_i \in \text{HID} \,\} \cup \{\, x_i \approx y_i : S_i \in \text{VIS} \,\} \vdash_{\mathcal{L}} E_{S_n}(O(x_0, \ldots, x_{n-1}){:}S_n, O(y_0, \ldots, y_{n-1}){:}S_n, \bar{u}{:}\bar{Q});$$

(b) If $S_n \in \text{VIS}$ then

$$\bigcup_{i<n} \{\, E_{S_i}(x_i{:}S_i, y_i{:}S_i, \bar{u}_i{:}\bar{Q}_i) : S_i \in \text{HID} \,\} \cup \{x_i \approx y_i : S_i \in \text{VIS} \,\} \vdash_{\mathcal{L}} O(x_0, \ldots, x_{n-1}) \approx O(y_0, \ldots, y_{n-1}).$$

For technical reasons it is convenient sometimes to think of an equivalence system as a SORT-sorted set E where $E_V = \{x{:}V \approx y{:}V\}$ for each visible sort V.

If a HEL $\mathcal{L}$ has an equivalence system then it is called *equivalential*. Moreover, if E is locally globally finite (i.e. $\bigcup_{V \in \text{VIS}} E_{V,H}$ is finite for each $H \in \text{HID}$), then $\mathcal{L}$ is called *finitely equivalential*.

Not every HEL is equivalential, a counter-example can be found in (Martins 2004). Also see this reference for details with regard to the following two examples.

Example 3.18.

I - Flags. The specification of flags $\mathcal{L}_{\mathit{eflag}}$ is finitely equivalential with finite system $E = \langle E_{\mathit{bool}}, E_{\mathit{flag}} \rangle$, where $E_{\mathit{bool}}(x{:}\mathit{bool}, y{:}\mathit{bool}) = \{x \approx y\}$ and

$$E_{\mathit{flag}}(x{:}\mathit{flag}, y{:}\mathit{flag}) = \{\mathit{up?}(x) \approx \mathit{up?}(y)\}.$$

II - Stacks. The specification of stacks $\mathcal{L}_{\mathit{stacks}}$ is equivalential with equivalence system $E = \langle E_{\mathit{nat}}, E_{\mathit{stack}} \rangle$ where $E_{\mathit{nat}}(x{:}\mathit{nat}, y{:}\mathit{nat}) = \{x \approx y\}$ and $E_{\mathit{stack}}(x{:}\mathit{stack}, y{:}\mathit{stack}) = \{\mathit{top}(\mathit{pop}^n(x)) \approx \mathit{top}(\mathit{pop}^n(y)) : n \geq 0\}$. However, $\mathcal{L}_{\mathit{stacks}}$ is not finitely equivalential.

♢

Note that neither of the two above equivalence systems contains a parametric variable. This is not an uncommon situation. If a HEL is (finitely) equivalential, then it has a (finite) equivalence system without parametric parameters, provided its signature has the property that every sort contains a ground term. For any (finite) equivalence system with parameters can be converted into one without parameters by replacing each parametric variable by an arbitrary ground term of the same sort.

Theorem 3.19. Let $\mathcal{L}$ be a HEL and E a pre-equivalence system over the same signature. Then E is an equivalence system for $\mathcal{L}$ iff, for every $H \in \text{HID}$ and every pair of H-terms t, t',

$$E_H(t, t', \bar{u}) \vDash^{\text{beh}}_{\mathcal{L}} t \approx t'. \tag{23}$$

Proof. Suppose E is an equivalence system for $\mathcal{L}$. Let T be an arbitrary $\mathcal{L}$-theory, and define $G(T) = \langle\, G(T)_S : S \in \mathrm{SORT} \,\rangle$ as follows.

$$G(T)_H := \{\, \langle t, t' \rangle : E_H(t, t', \bar{u}) \subseteq T \,\} \text{ for } H \in \mathrm{HID}, \text{ and } G(T)_{\mathrm{VIS}} := T.$$

The claim is that $G(T) = \Omega(T)$. It is easy to see directly from the definition of equivalence system that $G(T)$ is a congruence on Te_Σ. To see that it is the largest congruence with visible part T, let Θ be any congruence on Te_Σ whose visible part is T. Assume that $t \equiv t'\ (\Theta_H)$. Then for every $V \in \mathrm{VIS}$ and every equation $\varphi(x{:}H, \bar{u}{:}\bar{Q}){:}V \approx \varphi(y{:}H, \bar{u}{:}\bar{Q}){:}V$ in $E_{V,H}$, we have $\varphi(t, \bar{u}) \equiv \varphi(t', \bar{u})\ (\Theta_V)$ by the congruence property of Θ, and hence $\varphi(t, \bar{u}) \equiv \varphi(t', \bar{u})\ (T_V)$ since $\Theta_V = T_V$. Therefore, $E_H(t, t', \bar{u}) \subseteq T$, i.e., $t \equiv t'\ (G(T)_H)$. Thus $\Theta \subseteq G(T)$. Hence $G(T) = \Omega(T)$ as claimed.

We have shown that, for every $T \in \mathrm{Th}(\mathcal{L})$ and $H \in \mathrm{HID}$,

$$\Big(\big(\forall\, \varphi(t, \bar{u}) \approx \varphi(t', \bar{u}) \in E_H(t, t', \bar{u})\big)\ \big(\varphi(t, \bar{u}) \equiv_T \varphi(t', \bar{u})\big)\Big) \Longleftrightarrow t \equiv_{\Omega(T)} t'. \tag{24}$$

Thus $E_H(t, t', \bar{u}) \models^{\mathrm{beh}}_{\mathcal{L}} t \approx t'$ by Theorem 3.4.

Conversely, suppose now that (23) holds for all $H \in \mathrm{HID}$ and $t, t' \in (\mathrm{Te}_\Sigma)_H$. Applying Theorem 3.4 (and the fact the equations $\varphi(t, \bar{u}) \approx \varphi(t', \bar{u})$ are all visible) we get the equivalence (24) for every $T \in \mathrm{Th}(\mathcal{L})$, i.e.

$$\Omega(T)_H = \{\, \langle t, t' \rangle : E_H(t, t', \bar{u}) \subseteq T_H \,\} \text{ for every } H \in \mathrm{HID}.$$

The properties of $\Omega(T)$ as a congruence now translate directly into properties that define E as an equivalence system. For example, condition 3.17(iii) can be established in the following way. Let $T \in \mathrm{Th}(\mathcal{L})$ and suppose $E_H(t, t', \bar{u}), E_H(t', t'', \bar{u}) \subseteq T$. Then $t \equiv t' \equiv t''\ (\Omega(T))$. Hence $t \equiv t''\ (\Omega(T))$ by transitivity of $\Omega(T)$, i.e., $E_H(t, t'', \bar{u}) \subseteq T$. Since this is true for every T, 3.17(iii) holds □

Note that in the course of the proof it has been shown that, as a consequence of Theorem 3.4, the theorem can be alternatively expressed in the following way.

E is an equivalence system for $\mathcal{L}$ iff, for every $T \in \mathrm{Th}(\mathcal{L})$ and every sort $H \in \mathrm{HID}$,

$$\Omega(T)_H = \{\, \langle t, t' \rangle : E_H(t, t', \bar{u}) \subseteq T_H \,\}.$$

We are finally ready to give the promised characterization of behaviorally specifiable HEL's.

Theorem 3.20. A specifiable HEL $\mathcal{L}$ is behaviorally specifiable iff it is finitely equivalential.

Proof. Assume $E = \langle\, E_H(x{:}H, y{:}H, \bar{u}{:}\bar{Q} : H) \in \mathrm{HID} \,\rangle$ is an equivalence system for $\mathcal{L}$ such that E_H is globally finite for each $H \in \mathrm{HID}$. Define $\mathcal{L}'$ to be the UHEL obtained from $\mathcal{L}$ by adding, for each hidden sort H, the new inference rule

$$\varphi_1(x, \bar{u}) \approx \varphi_1(y, \bar{u}), \ldots, \varphi_n(x, \bar{u}) \approx \varphi_n(y, \bar{u}) \to x \approx y, \tag{25}$$

where $E_H(x{:}H, y{:}H, \bar{u}{:}\bar{Q}) = \{\varphi_1(x, \bar{u}) \approx \varphi_1(y, \bar{u}), \ldots, \varphi_n(x, \bar{u}) \approx \varphi_n(y, \bar{u})\}$, and x, y are variable of sort H distinct from all the variables in $\bar{u}$. To see $\mathcal{L}$ is a behavioral specification

of $\mathcal{L}$ it suffices by Theorem 3.15 to show that

$$\{\, \Omega(T) : T \in \mathrm{Th}(\mathcal{L}) \,\} = \mathrm{Th}(\mathcal{L}').$$

Let $T \in \mathrm{Th}(\mathcal{L})$. We have already seen that $\Omega(T) \in \mathrm{Th}(\mathcal{L}^{\mathrm{UH}})$, so in order to get $\Omega(T) \in \mathrm{Th}(\mathcal{L}')$ it is enough to show that $\Omega(T)$ is closed under the new inference rules (25). Let t, t' be H-terms such that $\varphi_i(t, \bar{u}) \equiv \varphi_i(t', \bar{u})$ $(\Omega(T))$ for $i \leq n$. Then $t \equiv t'$ $(\Omega(T))$ by Theorem 3.19.

To prove the other inclusion, let $G \in \mathrm{Th}(\mathcal{L}')$. Since $G \in \mathrm{Th}(\mathcal{L}^{\mathrm{UH}})$, $G_{\mathrm{VIS}} \in \mathrm{Th}(\mathcal{L})$, and hence $G \subseteq \Omega(G_{\mathrm{VIS}})$ because $\Omega(G_{\mathrm{VIS}})$ is the largest congruence whose visible part is G_{VIS}. Suppose $t \equiv t' \ \big(\Omega(G_{\mathrm{VIS}})_H\big)$. Then by the congruence property $\varphi_i(t, \bar{u}) \equiv \varphi_i(t', \bar{u})$ (G_{VIS}) for all $i \leq n$. Using the inference rule (25) we conclude that $t \equiv t'$ (G_H). Hence $\Omega(G_{\mathrm{VIS}}) \subseteq G$, and thus $G = \Omega(G_{\mathrm{VIS}})$.

Therefore, $\mathcal{L}'$ is the behavioral specification of $\mathcal{L}$.

Suppose that $\mathcal{L}$ is behaviorally specifiable and let $\mathcal{L}'$ be its behavioral specification. Let H be a fixed but arbitrary hidden sort, and let x, y be two distinct variables of sort H. Let G be the $\mathcal{L}'$-theory generated by the pair $\langle x, y \rangle$, i.e., $G = \mathrm{Cn}_{\mathcal{L}'}(\{\langle x, y \rangle\})$. Then G_{VIS} is generated by the set

$$\big\{\, \langle \psi(x{:}H, \bar{\vartheta}{:}\bar{R}),\ \psi(y{:}H, \bar{\vartheta}{:}\bar{R}) \rangle : \psi \in C_H, \bar{\vartheta} \in (\mathrm{Te}_\Sigma)_{\bar{R}} \,\big\}, \tag{26}$$

where C_H is the set of all visible H-contexts $\psi(z{:}H, \bar{u}{:}\bar{R})$. Indeed, if T is the $\mathcal{L}$-theory generated by this set of equations, then $x \equiv y$ $(\Omega(T))$ by Theorem 2.23, and hence, since $\Omega(T)$ is an $\mathcal{L}'$-theory (Theorem 3.15), we have $G \subseteq \Omega(T)$. It follows that $G_{\mathrm{VIS}} \subseteq \Omega(T)_{\mathrm{VIS}} = T$. On the other hand, $T \subseteq G_{\mathrm{VIS}}$ since G obviously includes the set of generators (26) of T. So $T = G_{\mathrm{VIS}}$.

G_{VIS} is finitely generated by Lemma 3.16 since G is finitely generated. So there is a finite subset of (26) that generates it. (If a theory is finitely generated, then any set of generators must include a finite generating subset.) Let

$$\big\{ \langle \psi_i(x{:}H, \bar{\vartheta}_i(\bar{u}{:}\bar{Q}){:}\bar{R}_i),\ \psi_i(y{:}H, \bar{\vartheta}_i(\bar{u}{:}\bar{Q}){:}\bar{R}_i) \rangle : i \leq m \,\big\}$$

be such a subset, where $\bar{u}{:}\bar{Q}$ is a finite list of all variables different from x or y that occur in this set of equations. For simplicity we write $\psi_i(x{:}H, \bar{\vartheta}_i(\bar{u}{:}\bar{Q}))$ in the form $\varphi_i(x{:}H, \bar{u}{:}\bar{Q})$. Then

$$\begin{aligned} &\big\{ \varphi_i(x{:}H,\ \bar{u}{:}\bar{Q}) \approx \varphi_i(y{:}H,\ \bar{u}{:}\bar{Q}) : i \leq m \,\big\} \\ &\qquad \vdash_{\mathcal{L}} \psi(x{:}H, \bar{\vartheta}{:}\bar{R}) \approx \psi(y{:}H, \bar{\vartheta}{:}\bar{R}) \quad \text{for every } \psi \in C_H \text{ and } \bar{\vartheta} \in (\mathrm{Te}_\Sigma)_{\bar{R}}. \end{aligned} \tag{27}$$

Consider any $t, t' \in (\mathrm{Te}_\Sigma)_H$ and any $\bar{\vartheta} \in (\mathrm{Te}_\Sigma)_{\bar{R}}$. By the substitution invariance of $\vdash_{\mathcal{L}}$ we have

$$\begin{aligned} &\big\{ \varphi_i(t{:}H,\ \bar{u}{:}\bar{Q}) \approx \varphi_i(t'{:}H,\ \bar{u}{:}\bar{Q}) : i \leq m \,\big\} \\ &\qquad \vdash_{\mathcal{L}} \psi(t{:}H, \bar{\vartheta}{:}\bar{R}) \approx \psi(t'{:}H, \bar{\vartheta}{:}\bar{R}) \quad \text{for every } \psi \in C_H \text{ and } \bar{\vartheta} \in (\mathrm{Te}_\Sigma)_{\bar{R}}. \end{aligned} \tag{28}$$

Let

$$E := \big\langle \big\{ \varphi_i(x{:}H,\ \bar{u}{:}\bar{Q}) \approx \varphi_i(y{:}H,\ \bar{u}{:}\bar{Q}) : i \leq m \,\big\} : H \in \mathrm{HID} \,\big\rangle.$$

E is an pre-equivalence system over Σ with E_H globally finite for each $H \in \mathrm{HID}$, and from (28) we conclude by Theorem 2.23 that, for every $H \in \mathrm{HID}$ and every pair of H-terms t, t',

$$E_H(t, t') \vDash^{\mathrm{beh}}_{\mathcal{L}} t \approx t'.$$

So E is a finitary equivalence system for $\mathcal{L}$ by Theorem 3.19. □

Roşu and Goguen in (Roşu and Goguen 2001) introduced the concept of cobasis that is closely related to our notion of equivalence system.

Definition 3.21. Let $\mathcal{L}$ be a HEL over the signature Σ. By a *cobasis* for $\mathcal{L}$ we mean a not necessarily visible pre-equivalence system

$$E := \big\langle\, \langle\, E_{S,H}(x{:}H, y{:}H, \bar{u}{:}\bar{Q}) : S \in \mathrm{SORT} \,\rangle : H \in \mathrm{HID} \,\big\rangle$$

with the following property. For every $H \in \mathrm{HID}$ and every pair of H-terms t, t',

$$E_H(t, t', \bar{u}) \vDash^{\mathrm{beh}}_{\mathcal{L}} t \approx t'.$$

Strictly speaking, a cobasis in the sense of Roşu and Goguen is the set of S-contexts $\varphi(z : H, \bar{u})$ that are used to form the equations of $E_{S,H}$.

In light of Theorem 3.19, an equivalence system is a cobasis where all the equations are visible. While a non-visible finite cobase can be useful in establishing behavioral equivalence, Theorem 3.20 shows that if it is complete in this regard, then it must be visible, or at least some visible finite cobasis must exist.

The following theorem gives us a method of verifying that a conditional equation is behaviorally valid over an equivalential HEL $\mathcal{L}$ entirely in terms of its consequence relation $\vdash_{\mathcal{L}}$.

Theorem 3.22. Let $\mathcal{L}$ be an equivalential HEL with equivalence system E. Then the following are equivalent.

(i) The conditional equation

$$t_0{:}S_0 \approx t'_0{:}S_0, \ldots, t_{n-1}{:}S_{n-1} \approx t'_{n-1}{:}S_{n-1} \to t_n{:}S_n \approx t'_n{:}S_n$$

is behaviorally valid over $\mathcal{L}$;

(ii) $\bigcup\{\, E_{S_i}(t_i{:}S_i, t'_i{:}S_i) : i < n \,\} \vdash_{\mathcal{L}} E_{S_n}(t_n{:}S_n, t'_n{:}S_n)$.

Furthermore, if $\mathcal{L}$ is finitely equivalential, i.e., if E_H is globally finite for each $H \in \mathrm{HID}$, then both conditions are equivalent to the following:

(iii) For every $s \approx s'$ in $E_{S_n}(t_n{:}S_n, t'_n{:}S_n)$, the visible conditional equation

$$\bigcup\{\, E_{S_i}(t_i{:}S_i, t'_i{:}S_i) : i < n \,\} \to s \approx s'$$

is a derivable rule of $\mathcal{L}$.

Proof. (i) ⇒ (ii) Define $G = \mathrm{Cn}_{\mathcal{L}}\big(\bigcup\{E_{S_i}(t_i{:}S_i, t'_i{:}S_i) : i < n\}\big)$. For each $i < n$, $t_i \equiv t'_i\,(\Omega(G))$ by Theorem 3.19. Then, from Theorem 3.4 and (i) we get $t_n \equiv t'_n\,(\Omega(G))$. So, applying Theorem 3.19 again, we get $E_{S_n}(t_n, t'_n) \subseteq G$, i.e., (ii) holds.

(ii) ⇒ (i) Let $T \in \mathrm{Th}(\mathcal{L})$. Suppose that $t_i \equiv t'_i\,(\Omega(T))$ for each $i < n$. Then, by

Theorem 3.19, $\bigcup\{ E_{S_i}(t_i{:}S_i, t'_i{:}S_i) \} \subseteq T$. Hence, by (ii),
$E_{S_n}(t_n{:}S_n, t'_n{:}S_n) \subseteq T$, and thus $t_n \equiv t'_n\,(\Omega(T))$.

The equivalence of (ii) and (iii) is immediate if E is globally finite. □

It follows easily from this theorem that, if a HEL $\mathcal{L}$ is equivalential and some equivalence system for it is RE, in particular if $\mathcal{L}$ is finitely equivalential, then the set of conditional equations that are behaviorally valid over $\mathcal{L}$ is RE. Moreover, in view of the remarks following Theorem 3.10, the set is recursive if the set of derivable (visible) conditional equations of $\mathcal{L}$ is recursive.

Many HEL's encountered in practice are equivalential, and in these cases Theorem 3.22 seems to be a useful way of verifying that a conditional equation is behaviorally valid. The following two examples illustrate this phenomenon.

Example 3.23. (**Flags**) We will use Theorem 3.22 to prove that $rev(G) \approx F \rightarrow rev(F) \approx G$ is behaviorally valid in $\mathcal{L}_{eflag}$. Using the equivalence system given in Example 3.18, together with condition (ii) of Theorem 3.22, it is enough to prove that

$$up?(rev(G)) \approx up?(F) \vdash_{\mathcal{L}_{eflag}} up?(rev(F)) \approx up?(G). \tag{29}$$

We have the following deduction in $\mathcal{L}_{eflag}$:

$up?(rev(G)) \approx up?(F)$	
$\neg(up?(G)) \approx up?(F)$	(axiom and IR_2)
$\neg(\neg(up?(G))) \approx \neg(up?(F))$	(IR_3)
$up?(G) \approx \neg(up?(F))$;	($\neg\neg x \approx x$ and IR_2)
$up?(G)) \approx up?(rev(F))$	(axiom and IR_2)

So, (29) is proved. Hence, $rev(G) \approx F \models^{\mathrm{beh}}_{\mathcal{L}_{eflag}} rev(F) \approx G$. ♢

Example 3.24. (**Stacks**) Using the equivalence system given in Example 3.18, in order to shown

$$S \approx push(n, S') \models^{\mathrm{beh}}_{\mathcal{L}_{Stacks}} pop(pop(S)) \approx pop(S'),$$

it is enough to prove that

$$\{top(pop^n(S)) \approx top(pop^n(push(n, S'))) : n \geq 0\} \vdash_{\mathcal{L}_{Stacks}}$$
$$\{top(pop^n(pop(pop(S)))) \approx top(pop^n(pop(S'))) : n \geq 0\}$$

This is a straightforward consequence of the axioms and rules for $\mathcal{L}_{stacks}$ given in Example 2.9.

The equivalence system can also be used to show that the two hidden equations (21), at end of section 3.1, are behaviorally valid. Substituting the two terms of the first equation $pop(push(x, S)) \approx S$ into the equations of the equivalence system we get, for every $n \geq 0$,

$$top\big(pop^n\big(pop(push(x, S))\big)\big) \approx top\big(pop^n(S)\big).$$

But this is just an instance of the axiom $top(pop^{n+1}(push(x, y))) \approx top(pop^n(y))$. The second equation of (21), $pop(empty) \approx empty$, is verified similarly using the axiom $top(pop^n(empty)) \approx zero$. ♢

It is shown in (Martins 2004) that $\mathcal{L}_{stacks}$ is not finitely equivalential, hence it is not behaviorally specifiable. However, the above equivalence system is clearly RE (indeed recursive), since the set of derivable rules of $\mathcal{L}_{stacks}$ is recursive (this is easily seen), we have that the set of behaviorally valid conditional equations of $\mathcal{L}_{stacks}$ is recursive.

4. Conclusion

In this paper a generalization of the theory of behavioral equivalence in abstract algebraic logic was presented that encompasses multi-sorted signatures and the "visible-hidden" dichotomy. It establishes a new bridge between AAL and the specification and verification theory of programs that provides an efficient way of applying the powerful machinery of abstract algebraic logic to the behavioral specification domain. We specialized to the study of HEL's. Our method is novel in that it relies almost exclusively on combinatorial properties of the theories over an arbitrary HEL and their Leibniz congruences.

We investigated the behavioral validity of conditional equations in hidden equational logics, HEL's; these are multi-sorted equational logics that contain a formal representation of equality only between visible data. We obtained characterizations of behavioral validity of conditional equations, some of which can be viewed as alternative methods of coinduction, and we showed how a HEL remains sound for behavioral validity when any number of behaviorally valid conditional equations are adjoined as new inference rules. This can be an effective way of verifying the behavioral validity of equations and conditional equations in many practical situations.

On a more theoretical note, we presented a pair of syntactical conditions that individually are both necessary and sufficient for the behaviorally valid conditional equations of a given HEL to be specifiable by some (non-hidden) equational logic. The conditions are simple enough to be useful in deciding in many cases whether or not the behavior of a HEL is specifiable. We also applied this generalized theory of AAL to the theory of cobases (see Section 3.2). We explained how they are closely related to the well known notion of equivalence systems in the AAL field. In Theorem 3.20 we characterized the HEL's that have a complete finite cobasis.

Generalizations of the notion of behavioral equivalence have been considered in the literature. Some authors require that each context contains only one occurrence of the distinguished variable z; however, they generate exactly the same behavioral equivalence relation. Another generalization is due to Goguen et al. who consider Γ-*behavioral equivalence*, with Γ a subset of the set of all operation symbols in the signature. A Γ-congruence is a relation compatible with all interpretations of the operation symbols in Γ. The Γ-behavioral equivalence is defined analogously to ordinary behavioral equivalence; it is also the largest Γ-congruence with the identity as the visible part. Our approach can be easily extended to accommodate Γ-behavioral equivalence. In fact, one needs only to change the definition of hidden equational logic by considering; precisely in the inference rule (IR_3) of Definition 2.6, the term t ranging among the ones generated using the operations symbols in Γ. Clearly, the notions of Leibniz congruence $\Omega(F)$ and the equivalence system have to be redefined to develop a parallel theory to ours. Some interesting questions arise in this context, such as the study of the compatibility of some operation

symbols outside of Γ with respect to Γ-behavioral equivalence. This problem has been studied in (Diaconescu and Futatsugi 2000) and (Bidoit and Hennicker 1999).

References

N. Berreged, A. Bouhoula, and M. Rusinowitch. Observational proofs with critical contexts. In *Fundamental Approaches to Software Engineering, volume 1382 of LNCS, Springer*, pages 38–53. 1998.

M. Bidoit and R. Hennicker. Proving behavioural theorems with standard first-order logic. In *Levi, Giorgio et al. (ed.), Algebraic and logic programming. 4th international conference, ALP '94, Madrid, Spain, September 14-16, 1994. Proceedings. Berlin: Springer. Lect. Notes Comput. Sci. 850*, pages 41–58. 1994.

M. Bidoit and R. Hennicker, *Behavioural theories and the proof of behavioural properties*, Theor. Comput. Sci. **165** (1996), no. 1, 3–55.

M. Bidoit and R. Hennicker. Observer complete definitions are behaviourally coherent. In *Proc. OBJ/CafeOBJ/Maude Workshop at Formal Methods'99, Toulouse, France, Sep.*, pages 83–94. 1999.

M. Bidoit, R. Hennicker, and M. Wirsing. *Behavioural and abstractor specifications.* Sci. Comput. Program., 25(2-3):149–186, 1995.

W. J. Blok and D. Pigozzi, *Algebraizable logics*, Mem. Am. Math. Soc. **396** (1989).

A. Bouhoula and M. Rusinowitch, *Observational proofs by rewriting*, Theor. Comput. Sci. **275** (2002), no. 1-2, 675–698.

S. Buss and G. Roşu, *Incompleteness of behavioral logics*, Reichel, Horst (ed.), CMCS 2000. Coalgebraic methods in computer science, Berlin, Germany, March 25-26, 2000. Amsterdam: Elsevier, Electronic Notes in Theoretical Computer Science. 33, 19 p., electronic only, 2000.

R. Diaconescu and K. Futatsugi. CafeOBJ report: The language, proof techniques, and methodologies for object-oriented algebraic specification. In AMAST series in Computing, editor, *World Scientific*, volume 6, 1998.

R. Diaconescu and K. Futatsugi. Behavioural coherence in object-oriented algebraic specification. *Journal of Universal Computer Science* , 6(1):74–96, 2000.

H. Ehrig and B. Mahr, *Fundamentals of algebraic specification 1: Equations and initial semantics*, EATCS Monographs on Theoretical Computer Science, Springer-Verlag, New York, N.Y., 1985.

J. Fiadeiro and A. Sernadas. Structuring theories on consequence. In *Recent trends in data type specification. Specification of abstract data types, Sel. Pap. 5th Workshop, Gullane/UK 1987, Lect. Notes Comput. Sci. 332*, pages 44–72. 1988.

J. Font, R. Jansana and D. Pigozzi *A survey of abstract algebraic logic*, Studia Logica, **74** (2003), 13–97.

J. Goguen and G. Malcolm, *Hidden coinduction: Behavioural correctness proofs for objects*, Math. Struct. Comput. Sci. **9** (1999), no. 3, 287–319.

J. Goguen and G. Malcolm, *A hidden agenda*, Theor. Comput. Sci. **245** (2000), no. 1, 55–101.

J. Goguen, K. Lin, and G. Roşu. Conditional circular coinductive rewriting with case analysis. In *16th International Workshop, WADT 2002*, volume 2755 of *Lecture Notes in Computer Science*, pages 216–232, Frauenchiemsee, Germany, September 2002.

V. Gorbunov, *Algebraic theory of quasivarieties. Transl. from the Russian*, Siberian School of Algebra and Logic. New York, NY: Consultants Bureau. xii, 1998.

R. Hennicker and M. Bidoit. Observational logic. In *Proc. AMAST '98, 7th International Conference on Algebraic Methodology and Software Technology. Lecture Notes in Computer Science, Berlin: Springer*, pages 263–277. 1999.

R. Hennicker, *Structural specifications with behavioural operators: semantics, proof methods and applications*, Habilitationsschrift, Institut für Informatik, Ludwig-Maximilians-Universität München 1997.

M. Hofmann and D. Sannella. On behavioural abstraction and behavioural satisfaction in higher-order logic. *Theor. Comput. Sci.*, 167(1-2):3–45, 1996.

G. Leavens and D. Pigozzi, , *Equational reasoning with subtypes*, Iowa State University, Technical Report TR #02-07, July 2002. ftp://ftp.cs.iastate.edu/pub/techreports/TR02-07/TR.pdf

K. Lin, J. Goguen and G. Roşu. Circular coinductive rewriting. In *Proceedings, Automated Software Engineering '00* (*Grenoble France*), *IEEE Press*, pages 123–131. September 2000.

J. Meseguer. General logics. In *Logic colloq. '87, Proc. Colloq., Granada/Spain 1987, Stud. Logic Found. Math. 129*, pages 275–329. 1989.

M. Martins, *Behavioral reasoning in generalized hidden logics*, Ph.D. thesis, University of Lisbon, Lisbon, September 2004.

D. Pigozzi, *Abstract algebraic logic*, Encyclopedia of Mathematics, Supplement III (M. Hazewinkel, ed.), Kluwer Academic Publishers, Dordrecht, December 2001, pp. 2–13.

H. Reichel, *Behavioural validity of conditional equations in abstract data types*, Contributions to general algebra 3, Proc. Conf., Vienna 1984, 301-324 , 1985.

G. Roşu, *Hidden logic*, Ph.D. thesis, University of California, San Diego, 2000.

G. Roşu and J. Goguen, *Hidden congruence deduction*, Automated Deduction in Classical and Non-Classical Logics (R. Caferra and G. Alzer, eds.), Lecture Notes in Artificial Intelligence, vol. 1761, Springer-Verlag, 2000, pp. 252–267.

G. Roşu and J. Goguen, *Circular coinduction*, In: Proceedings of International Joint Conference on Automated Reasoning (IJCAR'01), Siena, 2001.

R. Wójcicki, *Theory of logical calculi. basic theory of consequence operations*, Synthese Library, no. 199, Reidel, Dordrecht, 1988.