Behavioral Reasoning for Conditional Equations [†]

MANUEL ANTÓNIO MARTINS[1] and DON PIGOZZI[2]

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

Received 3 March 2004

The behavioral equivalence of hidden terms in an equational specification logic is not itself specifiable in general (Buss and Roşu 2000). But much recent work has been done on its partial specification, in particular using coinduction. In this paper we consider the more general notion of conditional behavioral equivalence introduced by Reichel in 1984. We investigate the behavioral proof theory of a general class of equational specification logics, the *hidden equational logics*. Among other things we characterize the behaviorally valid conditional equations of a hidden equational logic as those conditional equations which, in a natural sense, do not increase the deductive power of the logic when they are added as new rules of inference. For a special kind of hidden equational logic (the *equivalential logics*) we obtain methods for proving behavioral validity that work well in practice. Those hidden equational logics whose behavioral is specifiable by a (non-hidden) equational logic are characterized in terms of a special class of equivalential logics—equivalently as those hidden equational logics that have a cobasis (Roşu and Goguen 2001) of a special form.

Contents

[†] Research partially supported under project PRODEP III 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 programs however present a special challenge for equational methods. A more appropriate model for the abstract machine in the case of 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 of 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 is partitioned into *visible* and *hidden* parts, with the latter representing the objects in the object-oriented paradigm. Programs are assumed to output only visible data. Hidden data can be only indirectly compared by comparing the outputs of the programs that take hidden data as input. Two hidden data elements are *behaviorally equivalent* if every program 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 as axioms and rules of inference; this is so because only visible data is used in the definition of behavioral equivalence. Consequently there is no primitive symbol in the language for equality between hidden terms. Such logics are referred to as *hidden equational logics*, or *HEL*'s. Here we follow Goguen and Malcolm (Goguen and Malcolm 2000) in the choice of the descriptive term "hidden", but note that they do not explicitly exclude hidden equations and conditional equations as possible axioms and rules of inference.

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 (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 that the methods of coalgebra, in particular coinduction, might be useful in verifying behavioral validity. And in fact a considerable amount of research has been done on developing various forms of coinduction, usually in combination with the methods of standard equational logic, for verifying behavioral validity for wide classes of hidden equational logics (Bouhoula and Rusinowitch 2002; Goguen and Malcolm 1999; Goguen and Malcolm 2000; Leavens and Pigozzi 2002; Roşu 2000; Roşu and Goguen 2000; Roşu and Goguen 2001). More abstract studies of the behavioral equivalence and validity relations can be found (Bidoit and Hennicker 1996; Hennicker 1997; Martins 2001; Pigozzi 1999).

Most of the previous work in this area has concentrated on *HEL*'s defined by equations and on the development of methods for verifying the behavioral validity of equations. Our approach is more general. We focus on *HEL*'s defined by conditional equations, and we describe various methods, including new forms of coinduction, for verifying the behavioral validity of conditional equations. Some of the methods can be taken as the bases of deterministic algorithms in the proof theory of conditional behavioral validity.

Apart from the emphasis on conditional equations, our approach differs substantially from that taken in most of the work referenced above in being greatly influenced by *abstract algebraic logic* (see (Pigozzi 2001) where other references can be found). It turns out that the behavioral validity of equations over a given *HEL* $\mathcal{L}$, when viewed as a binary relation on the set of terms, is a congruence relation on the term algebra, in fact the largest congruence that includes all of the theorems of $\mathcal{L}$, i.e., all the equations deducible from the axioms and rules of inference. This congruence plays a key role in the hidden equational logic of Goguen and his associates. (This can be seen most clearly in (Roşu and Goguen 2000) where it is explicitly used to import a form of coinduction into the equational logic of hidden data structures, and in Roşu and Goguen's work (Roşu and Goguen 2001) where the notion of a cobasis is used for a similar purpose.) In abstract algebraic logic the scope of the *Leibniz congruence* of the minimal theory of theorems (as the behavioral validity relation is called) is greatly expanded to apply to arbitrary theories of the most general kind of logical systems, and it plays an important role in almost all investigations. This is the approach we take here. In particular, the theory of models of a *HEL*, which plays such an important role in the standard development of hidden equational logic, is in large part supplanted by the combinatorial theory of the Leibniz congruences; this gives our work a distinctive proof theoretic flavor that, in our view, adds much by the way of clarity to the theory.

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 2.1.

Hidden k-logics are useful mainly because they 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). It also comprehends all sentential logics, the purview of abstract algebraic logic. The Leibniz congruence is introduced in this general context and its most basic properties are developed. In Section 2.2 we specialize to the hidden equational logics (*HEL*'s) and develop the connection between the Leibniz congruence and the models of *HEL* that play the most significant role in their metatheory. (These are the the so-called *equality models*; they form a proper subclass of models in the sense of hidden k-logics.) The section ends with two representative examples of *HEL*'s (Section 2.3).

The relations of behavioral equivalence and validity are defined in the standard way in Section 3, that is in terms of the equality models of the *HEL*. In the main lemma of the paper (Lemma 3.5) we characterize behavioral validity for a conditional equation in terms of combinatorial properties of Leibniz congruences on the term algebra; this characterization can be viewed as a form of coinduction for conditional equations.

In Section 3.1 we prove that all members of a set of conditional equations E are behaviorally valid 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 a 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 3.12) 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 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 turn to the problem of characterizing *HEL*'s whose behaviorally valid conditional equations can be derived, in standard equational logic (without coinduction), from some set of possibly hidden equations and conditional equations (the set need not be finite or even recursively enumerable). Such *HEL*'s are said to be *behaviorally specifiable* (see Definition 3.13 and the following theorem).

A sorted system of sorted systems of visible equations $E(x, y)$ in two variables is said to be an *equivalence system* (Definition 3.16) for a *HEL* $\mathcal{L}$ if certain special visible equations and visible conditional equations, with possibly infinitely many conditions, are derivable in $\mathcal{L}$ that collectively guarantee that $E(x, y)$ defines the Leibniz congruences in a natural way (Theorem 3.17). $\mathcal{L}$ is (*finitely*) *equivalential* if it has an equivalence system $E(x, y)$ (such that each of the special visible conditional equations mentioned have only a finite number of conditions). By Theorem 3.19 a *HEL* is behaviorally specifiable if and only if it is finitely equivalential. (This theorem is a special case of a more general result in (Pigozzi 1999).) Moreover, it is also shown that there that a *HEL* is behaviorally specifiable if and only if it has a cobasis (in the sense of (Roşu and Goguen 2001)) of a special kind.

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 3.20). This result can be useful in practice since many *HEL*'s have equivalence systems and even finite equivalence systems. In the last section of the paper we return in this regard to the examples of Section 2.3.

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

$$\Sigma = \langle SORT, VIS, \langle OP_\tau : \tau \in Type \rangle \rangle,$$

where $SORT$ is a countable non-empty set of sorts, VIS is a subset of $SORT$, which we call the set of *visible sorts*, and OP_τ is a countable set of operation symbols of type τ. We call the sorts in $SORT \setminus VIS$ *hidden sorts*.

Σ is said to be *standard* if there is a ground term of every sort.

Let B be a sorted set. We say that B is *locally countable* (*finite*), if for every sort S, B_S is a countable (finite) set. An algebra A is *locally countable* (*finite*) if its carrier set is locally countable (finite).

Let $X = \langle X_S : S \in SORT \rangle$ be a fixed locally countable sorted set of variables. We define the sorted set $\mathrm{Te}_\Sigma(X)$ of terms (or formulas) in the signature Σ as usual. We define in the natural way the operations in $\mathrm{Te}_\Sigma(X)$ to get the *term algebra* over the signature Σ.

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 $h^* : \mathrm{Te}_\Sigma(X) \to A$. In the sequel we will not distinguish these two maps. In particular 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 $\mathrm{Te}_\Sigma(X)$; similarly, we may write simply Te when Σ is clear from context.

To provide a context that allows us to deal simultaneously with specification logics that are assertional (for example ones with a Boolean sort) and equational, we introduce the notion of a k-term for any nonzero natural number k; a *k-term* of sort S over Σ is just a sequence of k Σ-terms all of the same sort S. k-terms are indicated by overlining, so $\bar{\varphi}{:}S = \langle \varphi_0{:}S, ..., \varphi_{k-1}{:}S \rangle$. When we do not want to make the common sort of each term of $\bar{\varphi}$ explicit, we simply write it as $\bar{\varphi}$. Te_Σ^k is the sorted set of all k-terms over

Σ. Thus $\mathrm{Te}^k_\Sigma = \langle \mathrm{Te}^k_S : S \in \mathit{SORT} \rangle$. The set of all visible k-terms $(\mathrm{Te}^k_\Sigma)_{VIS}$ is the set $\langle (\mathrm{Te}^k_\Sigma)_V : V \in VIS \rangle$.

A *k-data structure* (or a *k-abstract machine*) over Σ is a pair $\mathcal{A} = \langle A, F \rangle$, where A is a Σ-algebra and $F \subseteq A^k_{VIS}$. An example of a 2-data structure is any model of the free hidden equational logic over Σ (HEL_Σ) considered below (Definition 2.7). The standard model of HEL_Σ is of the form $\langle A, id_{A_{VIS}} \rangle$, where A is a Σ-algebra and $id_{A_{VIS}}$ 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 $id_{A_{VIS}}$. We can also consider the free Boolean logic over Σ if it has a Boolean sort. Here the standard models are the 1-data structures $\langle A, \{\mathit{true}\} \rangle$, 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 $\{\mathit{true}\}$ is replaced by an arbitrary filter on A_{VIS}.

Let $\langle A, F \rangle$ be a k-data structure. A congruence relation Θ on A is *compatible* with F if the following conditions holds for all $\bar{a}, \bar{a}' \in A^k_S$. If $a_i \equiv a'_i(\Theta))$ for all $i \leq k$, then $\bar{a} \in F$ iff (i.e., if and only if) $\bar{a}' \in F$.

Definition 2.1. Let $\langle A, F \rangle$ be a k-data structure. Then the *Leibniz congruence* of F on A is the largest congruence relation on A compatible with F. We denote it by $\Omega_A(F)$.

It is not difficult to see that such a largest congruence relation on A always exists.

One of the main properties of the Leibniz congruence is its preservation under inverse images of surjective homomorphisms. This is given in the following lemma. Let $h : B \to A$ be a mapping between sets. If $\bar{b} = \langle b_1, \cdots, b_k \rangle \in B^k$, then $h(\bar{b}) = \langle h(b_1), \cdots, h(b_k) \rangle \in A^k$, and if $\bar{a} = \langle a_1, \cdots, a_k \rangle \in A^k$, then $h^{-1}(\bar{a}) = \{\, \bar{b} \in B^k : h(\bar{b}) = \bar{a} \,\}$.

Lemma 2.2. 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. Then

$$h^{-1}(\Omega(F)) = \Omega(h^{-1}(F))). \tag{1}$$

Proof. $h^{-1}(\Omega(F))$ is a congruence on B, and it is compatible with $h^{-1}(F)$ since $\Omega(F)$ is compatible with F. So $h^{-1}(\Omega(F)) \subseteq \Omega(h^{-1}(F))$, by definition of the Leibniz congruence.

To prove the reciprocal inclusion we first note that,

$$\Omega(h^{-1}(F)) \subseteq h^{-1}(\Omega(F)) \quad \text{iff} \quad h(\Omega(h^{-1}(F))) \subseteq \Omega(F).$$

To see this it suffices to observe that the two inclusions $hh^{-1}((\Omega(F)) \subseteq \Omega(F)$ and $\Omega(h^{-1}(F)) \subseteq h^{-1}h(\Omega(h^{-1}(F)))$ hold (without the assumption that h is surjective).

Let Θ be the congruence generated by $h(\Omega(h^{-1}(F)))$. Since h is surjective, Θ is the transitive closure of $h(\Omega(h^{-1}(F)))$. Hence it is enough to prove that $h(\Omega(h^{-1}(F)))$ is compatible with F.

Let $\bar{a}, \bar{a}' \in A^k_S$ such that $\bar{a} \in F_S$ and $\bar{a} \equiv \bar{a}' \left(h(\Omega(h^{-1}(F)))^k_S\right)$ (i.e., for all $i \leq k$, $a_i \equiv a'_i \left(h(\Omega(h^{-1}(F)))_S\right)$ where $\bar{a} = (a_1, \ldots, a_k)$ and $\bar{a}' = (a'_1, \ldots, a'_k)$). Let $\bar{b}, \bar{b}' \in B^k_S$ such that $\bar{b} \equiv \bar{b}' \left(\Omega(h^{-1}(F))_S\right)$ 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 $\Omega(h^{-1}(F))$ is compatible with $h^{-1}(F)$. So $\bar{a}' \in F_S$. □

If $\mathcal{A} = \langle A, F \rangle$ is a k-data structure over Σ, we can form the quotient structure

$\mathcal{A}/\Omega(F) = \langle A, F\rangle/\Omega(F) = \langle A/\Omega(F),\, F/\Omega(F)\rangle$, where $A/\Omega(F)$ is the quotient of A and $F/\Omega(F) = \{\,(a_1/\Omega(F), \dots, a_k/\Omega(F)) : (a_1, \dots, a_k) \in F\,\}$. $\mathcal{A}$ is said to be *reduced* if $\Omega(F)$ is the identity congruence on A.

Corollary 2.3. The quotient of any k-data structure by the Leibniz congruence is reduced.

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

A systematic study of the Leibniz congruence in hidden k-logics can be found in (Pigozzi 1999); in particular a proof of the following characterization of the Leibniz congruence can be found there.[†]

If A is a Σ-algebra and $\bar\varphi(x_1{:}T_1, \dots, x_n{:}T_n)$ is a k-term and $(a_1, \dots, a_n) \in A_{T_1} \times \cdots \times A_{T_n}$, then we denote by $\bar\varphi^A(a_1, \dots, a_n)$ the value $\bar\varphi$ takes in A when the variables $x_1, \dots, x_n$ are interpreted respectively by $a_1, \dots, a_n$. More algebraically, $\bar\varphi^A(a_1, \dots, a_n) = h(\varphi)$, where $h : X \to A$ is any assignment such that $h(x_i) = a_i$ for all $i \le n$.

Theorem 2.4 ((Pigozzi 1999)). Let Σ be a hidden signature and let $\mathcal{A} = \langle A, F\rangle$ be a k-data structure over Σ. Then, for every $S \in \mathit{SORT}$ and for all $a, a' \in A_S$, $a \equiv a'$ $(\Omega(F)_S)$ iff for every visible k-term $\bar\varphi(z{:}S,\, u_1{:}Q_1, ..., u_m{:}Q_m){:}V$ and for all $\langle b_1, \dots, b_m\rangle \in A_{Q_1} \times \cdots \times A_{Q_m}$,

$$\bar\varphi^A(a, b_1, \dots, b_m) \in F_V \quad \text{iff} \quad \bar\varphi^A(a', b_1, ..., b_m) \in F_V. \tag{2}$$

Proof. Let Θ be the SORT-sorted binary relation on A where Θ_S is the set of pairs $\langle a, a'\rangle \in A_S^2$ such that for every visible k-term $\bar\varphi(z{:}S,\, \bar u{:}\bar Q){:}V$ the condition (2) holds for all $\bar b := \langle b_1, \dots, b_m\rangle \in A_{\bar Q} := A_{Q_1} \times \cdots \times A_{Q_m}$. It is easy to see that Θ is a equivalence relation on A. To see it is a congruence relation, let O be an operation of type $T_1, \dots, T_n \to S$ and suppose $\langle \bar a, \bar a'\rangle \in \Theta_{\bar T}$. We must show that, for any visible k-term $\bar\varphi(z{:}S, \bar u{:}\bar Q){:}V$, with the designated variable $z{:}S$, and for all parameters $\bar b \in A_{\bar Q}$, we have

$$\bar\varphi^A\big(O^A(\bar a, \bar b)\big) \in F_V \quad \text{iff} \quad \bar\varphi^A\big(O^A(\bar a', \bar b)\big) \in F_V. \tag{3}$$

Consider any $i \le n$. Using the assumption $\langle a_i, a_i'\rangle \in \Theta_{T_i}$ and taking x_i as the designated variable, $x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_n, u_1, \dots, u_n$ as parametric variables, and $a_1, \dots, a_{i-1}, a_{i+1}', \dots, a_n', b_1, \dots, b_n$ as parameters we have

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

Since this equivalence holds for all $i \le n$, (3) holds, and hence Θ is a congruence.

To see that Θ is compatible with F, consider $\bar a, \bar a' \in A_T^k$ such that $\bar a \equiv \bar a'$ (Θ_T^k). Let

[†] 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).

$\bar{\varphi}(\bar{x})$ be the k-sequence of pairwise distinct variables $\bar{x} = \langle x_1 : T, \ldots, x_n : T\rangle$ (called a *k-variable*). Using the assumption $a_i \equiv a'_i\ (\Theta_T)$ and taking x_i as the designated variable and $a_0, \ldots, a_{i-1}, a'_{i+1}, \ldots, a'_n$ as parameters we have, for each $i < n$,

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

So $\bar{a} \in F_V$ iff $\bar{a}' \in F_V$. Thus Θ is compatible with F.

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

For the purposes of this work it is convenient to define a hidden k-logic as an abstract closure relation on the set of k-terms, independently of any specific choice of axioms and rules of inference. By an *closure relation* on Te^k_Σ we mean a binary relation $\vdash\ \subseteq \mathcal{P}(\mathrm{Te}^k_\Sigma) \times \mathrm{Te}^k_\Sigma$ between subsets of k-terms and individual k-terms satisfying the following conditions. (1) $\Gamma \vdash \bar{\gamma}$ for each $\bar{\gamma} \in \Gamma$; (2) $\Gamma \vdash \bar{\varphi}$ and $\Delta \vdash \bar{\gamma}$ for each $\bar{\gamma} \in \Gamma$ implies $\Delta \vdash \bar{\varphi}$. The closure relation is *finitary* if $\Gamma \vdash \bar{\varphi}$ implies $\Delta \vdash \bar{\varphi}$ for some globally finite subset Δ of Γ. It is *substitution-invariant* if $\Gamma \vdash \bar{\varphi}$ implies $\sigma(\Gamma) \vdash \sigma(\bar{\varphi})$ for every substitution $\sigma : X \to \mathrm{Te}_\Sigma$. Every closure relation $\vdash$ on Te^k_Σ has a natural extension to a relation, also denoted by $\vdash$, between subsets of Te^k_Σ. It is defined by $\Gamma \vdash \Delta$ if $\Gamma \vdash \varphi$ for each $\varphi \in \Delta$. Moreover, if $\Gamma = \langle\, \Gamma_S : S \in \mathit{SORT}\,\rangle$ and $\Delta = \langle\, \Delta_S : S \in \mathit{SORT}\,\rangle$ are sorted systems of sets of k-terms, then by $\Gamma \vdash \Delta$ we will mean $\bigcup_{S \in \mathit{SORT}} \Gamma_S \vdash \bigcup_{S \in \mathit{SORT}} \Delta_S$.

Definition 2.5. An *hidden k-logic* over a hidden signature Σ is a pair $\mathcal{L} = \langle \Sigma, \vdash_{\mathcal{L}}\rangle$, where Σ is a hidden signature and $\vdash_{\mathcal{L}}$ is a substitution-invariant closure relation on the set $(\mathrm{Te}^k_\Sigma)_{\mathit{VIS}}$ of visible k-terms.

A hidden k-logic is *specifiable* if $\vdash_{\mathcal{L}}$ is finitary.

A hidden k-logic with $\mathit{VIS} = \mathit{SORT}$ will be called a *visible k-logic*, or simply a k-logic. By a *sentential logic* we mean a homogeneous (one-sorted) specifiable visible 1-logic.

Normally a specifiable hidden k-logic is presented by a set of axioms (visible terms) and inference rules of the general form

$$\frac{\bar{\varphi}_0 : V_0, \ldots, \bar{\varphi}_{n-1} : V_{n-1}}{\bar{\varphi}_n : V_n}, \tag{4}$$

where $\bar{\varphi}_0, \ldots, \bar{\varphi}_n$ are all visible k-terms. A visible k-term $\bar{\psi}$ is *directly derivable* from a set Γ of visible k-terms by a rule such as (4) 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-terms terminating in $\bar{\psi}$ such that each k-term in the sequence is either a substitution instance of an axiom or directly derivable from Γ by one of the rules of inference.

It is well known, and straightforward to show, that a hidden k-logic $\mathcal{L}$ is specifiable iff there exists a (possibly) infinite set of axioms and rules of inference such that, for any visible k-terms $\bar{\psi}$ and any set Γ of visible k-terms, $\Gamma \vdash_{\mathcal{L}} \bar{\psi}$ 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-term $\bar{\varphi}$ such that $\vdash_{\mathcal{L}} \bar{\varphi}$, i.e., $\emptyset \vdash_{\mathcal{L}} \bar{\varphi}$. The set of all theorems is denoted by $Thm(\mathcal{L})$. A rule such as (4) is said to be a *derivable rule* of $\mathcal{L}$ if $\{\bar{\varphi}_0, \dots, \bar{\varphi}_{n-1}\} \vdash_{\mathcal{L}} \bar{\varphi}_n$. A set of visible k-terms 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 $Th(\mathcal{L})$; if forms a complete lattice under set-theoretic inclusion. Given any set of visible k-terms Γ, the set of all consequences of Γ, in symbols $Con_{\mathcal{L}}(\Gamma)$, is the smallest theory that contains Γ. Clearly, $Con_{\mathcal{L}}(\Gamma) = \{\, \bar{\varphi} \in (\mathrm{Te}^{k}_{\Sigma})_{VIS} : \Gamma \vdash_{\mathcal{L}} \bar{\varphi}\}$.

2.1. *Semantics*

Let $\mathcal{A} = \langle A, F\rangle$ be a k-data structure. A visible k-term $\bar{\varphi}{:}V$ is said to be a *semantic consequence* of a set of visible k-terms Γ in $\mathcal{A}$, in symbols $\Gamma \models_{\mathcal{A}} \bar{\varphi}$, if, for every assignment $h : X \to A$, $h(\bar{\varphi}) \in F_V$ whenever $h(\bar{\psi}) \in F_W$ for every $\bar{\psi}{:}W \in \Gamma$. A visible k-term $\bar{\varphi}$ is a *validity* of $\mathcal{A}$, and conversely $\mathcal{A}$ is a *model* (or a correct abstract machine) of $\bar{\varphi}$, if $\models_{\mathcal{A}} \bar{\varphi}$. A rule such as (4) is a *validity*, or a *valid rule*, of $\mathcal{L}$, and conversely $\mathcal{A}$ is a *model* of the rule, if $\{\bar{\varphi}_0, \dots, \bar{\varphi}_{n-1}\} \models_{\mathcal{A}} \bar{\varphi}_n$.

$\bar{\varphi}$ is a *semantic consequence* of Γ for an arbitrary class K of k-data structures over Σ, in symbols $\Gamma \models_K \bar{\varphi}$, if $\Gamma \models_{\mathcal{A}} \bar{\varphi}$ for each $\mathcal{A} \in K$. Similarly, A k-term or rule is a validity of K if it is a *validity* of each member of K.

$\mathcal{A}$ is a *model* of a hidden k-logic $\mathcal{L}$ if every consequence of $\mathcal{L}$ 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 $Mod(\mathcal{L})$. If $\mathcal{L}$ is a specifiable hidden k-logic, then $\mathcal{A}$ is a model of $\mathcal{L}$ iff every axiom and rule of inference is a validity of $\mathcal{A}$. The class of all reduced models of $\mathcal{L}$, i.e., all models $\langle A, F\rangle$ such that $\Omega(F) = id_A$, is denoted by $Mod^*(\mathcal{L})$.

The proof of the following theorem is straightforward and can be found in (Pigozzi 1999). For sentential logics the result is well known; see for example (Wójcicki 1988).

Theorem 2.6 (completeness theorem for k-logics[‡]).
For any hidden k-logic $\mathcal{L}$,

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

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

2.2. *Hidden equational logic*

In the remainder of this paper we deal almost exclusively with specifiable 2-logics, in particular two versions of equational logic in which a 2-term $\langle t, s\rangle$ is intended to represent an equation, which we denote by $t \approx s$, and a rule $\dfrac{\langle t_0, s_0\rangle, \dots, \langle t_{n-1}, s_{n-1}\rangle}{\langle t_n, s_n\rangle}$ represents a conditional equation, denoted by $t_n \approx s_n$ `if` $t_0 \approx s_0, \dots, t_{n-1} \approx s_{n-1}$.

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

As a consequence of the restriction to visible k-terms in our formalization of hidden k-logics, the non-visible part of our hidden equational logic is truly hidden; indeed no representation of the equality predicate between elements of the hidden domains even exists in the object language. In reasoning about hidden data in the object language, only visible properties expressible in the form of conditional equations are allowed. The rationale behind this restriction was explained in the introduction. Equality predicates over the hidden sorts are however present in our second version of equational logic (technically, this is accomplished by simply modifying the signature by making all sorts visible). But this is done solely for the purpose of being able to express behavioral equivalence in the object language. The interplay between these two versions of equational logics is a characteristic feature of the abstract algebraic logic approach specification logic; the two logics are formalized in the following definitions.

Definition 2.7 (*Free hidden equational logic*[§]). Let Σ be a hidden signature and *VIS* its set of visible sorts. The *free hidden equational logic* over Σ, in symbols HEL_Σ, is the specifiable hidden 2-logic presented as follows.

Axioms:

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

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

$$(\mathrm{IR}_1) \qquad \frac{x{:}V \approx y{:}V}{y{:}V \approx x{:}V}\ ,$$

$$(\mathrm{IR}_2) \qquad \frac{x{:}V \approx y{:}V, y{:}V \approx z{:}V}{x{:}V \approx z{:}V}\ ,$$

$$(\mathrm{IR}_3) \qquad \frac{\varphi{:}V \approx \psi{:}V}{\vartheta(x/\varphi){:}W \approx \vartheta(x/\psi){:}W}, \text{ for every } \vartheta \in \mathrm{Te}_W \text{ and every } x \in X_V.$$

The (*unrestricted*) *free equational logic* over Σ, EQL_Σ, contains an equality predicate for each sort, visible and hidden. The axioms and inference rules of the free EQL_Σ are the same as those of the free HEL_Σ, except that now V and W are allowed to range over all sorts. Thus the free EQL_Σ can be viewed as the free $\mathit{HEL}_{\Sigma'}$, where Σ' differs from Σ only in that all sorts are assumed to be visible.

$\mathcal{A} = \langle A, F\rangle$ is a model of the free HEL_Σ iff F is a congruence on the visible part of A. In this case F is called a *hidden congruence*; the terminology is justified by viewing F as a congruence on the entire algebra with part of it hidden (its restriction to $A_{\mathit{SORT}\setminus\mathit{VIS}}$) and thus indeterminate. The theories of the free HEL_Σ are the hidden congruences on the term algebra.

In the free EQL_Σ the models are the 2-data structures $\langle A, F\rangle$ where F is a congruence with no part of it hidden, i.e., a congruence on the entire algebra A; the theories are the congruences on the term algebra.

For every congruence F of A, whether hidden or not, we write $a \equiv a\ (F_S)$ alternatively

[§] 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 2.11 below we must assume that all the sort domains of each model are non-empty.

for $\langle a, a' \rangle \in F_S$. If A is the term algebra and hence a, a' are terms, we might also write $a \approx a' \in F_S$.

If we add additional axioms and inference rules of visible (unrestricted) sort to a free HEL_Σ (a free EQL_Σ) we obtain an *applied hidden equational logic* (an *applied equational logic*). (The subscript Σ may be omitted if it is clear from context.) We refer to these new axioms and inference rules as *extra-logical*; in view of the completeness theorem (Theorem 2.11 below) they correspond respectively to identities and conditional identities, respectively, of the class of models of $\mathcal{L}$ (see the remarks at the beginning of this subsection). In particular, the visible (unrestricted) conditional equation

$$t_n(\bar{x}) \approx s_n(\bar{x}) \ \texttt{if} \ t_0(\bar{x}) \approx s_0(\bar{x}), \dots, t_{n-1}(\bar{x}) \approx s_{n-1}(\bar{x}) \tag{5}$$

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

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

A theory of $\mathcal{L}$ 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, $Con_{\mathcal{L}}(E)$, is the smallest $\mathcal{L}$-congruence that contains the pair $\langle t, t' \rangle$ for each equation $t \approx t'$ in E.

The conditional equation (5) is a *quasi-identity* of A if it is a valid rule of $\langle A, F \rangle$ where $F = id_{A_{VIS}}$ ($F = id_A$). Models of the free HEL_Σ (the free EQL_Σ) of the form $\langle A, id_{A_{VIS}} \rangle$ ($\langle A, id_A \rangle$) are called *equality models.* The class of all equality models of a EQL_Σ (an EQL_Σ) $\mathcal{L}$ is denoted by $Mod^{=}(\mathcal{L})$. 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 $Mod^{=}(\mathcal{L})$ with $\{ A : \langle A, id_{A_{VIS}} \rangle \in Mod^{=}(\mathcal{L}) \}$, and similarly for the equality models of a EQL_Σ.

When applied to hidden equational logics, Theorem 2.4 has an alternative formulation (Pigozzi 1999). It uses the notion of a context. An S-*context* $\varphi(z{:}S, u_1{:}Q_1, ..., u_m{:}Q_m)$ is a term with a distinguished variable z of sort S and parametric variables $u_1, ..., u_m$.

Theorem 2.8. 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 hidden congruence on A. Then, for every $S \in SORT$ and all $a, a' \in A_S$, $a \equiv a' \ \big(\Omega(F)_S\big)$ iff, for every visible S-context $\varphi(z{:}S, u_1{:}Q_1, ..., u_m{:}Q_m){:}V$ and for all $(b_1, ..., b_m) \in A_{Q_1} \times ... \times A_{Q_m}$,

$$\varphi^A(a, b_1, ..., b_m) \equiv \varphi^A(a', b_1, ..., b_m) \, (F_V). \tag{6}$$

Proof. By Theorem 2.4, $a \equiv a' \ (\Omega(F)_V)$ iff, for every pair $\langle \varphi(z{:}S, \ \bar{u}{:}\bar{Q}), \psi(z{:}S, \ \bar{u}{:}\bar{Q}) \rangle$ of S-contexts of sort V, and every $\bar{b} \in A_{\bar{Q}}$,

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

Suppose (6) holds for every S context $\varphi(z, \bar{u})$ and every $\bar{b} \in A_{\bar{Q}}$.
If $\varphi^A(a, \bar{b}) \equiv \psi^A(a, \bar{b}) \ (F_V)$, then

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

(the first and third equivalences hold because F is a hidden congruence). Thus (7) holds for every pair of S-contexts and every sequence of parameters $\bar{b}$, i.e., $a \equiv a' \ (\Omega(F)_V)$.

Conversely, assume $a \equiv a'\ (\Omega(F)_V)$. Let $\varphi(z{:}S,\ \bar{u}{:}\bar{Q}){:}V$ be an arbitrary visible S-context, where $\bar{u}{:}\bar{Q} = \langle u_1{:}Q_1, \dots, u_m{:}Q_m\rangle$. 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 $\bar{u}^+ := \langle u_1, \dots, u_n, u_{n+1}\rangle$. φ can also be viewed as an S-context with the same parametric variables. Let $\langle b_1, \dots, b_n\rangle$ be any system of parameters of sort $\bar{Q}$, and extend it to a system $\bar{b} := \langle b_1, \dots, b_{n+1}\rangle$, 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 (7), $\varphi^A(a', \bar{b}^+) \equiv u^A_{n+1}(a', \bar{b}^+)\ (F_V)$. But $u^A_{n+1}(a', \bar{b}^+)$ also equals b_{n+1}. So $\varphi^A(a, \bar{b}) \equiv \varphi^A(a', \bar{b})\ (F_V)$. Thus (6) holds for every S context $\varphi(z, \bar{u})$ and every $\bar{b} \in A_{\bar{Q}}$. □

For equality models ($F = id_{A_{VIS}}$) 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 2.9 ((Pigozzi 1999)). Let $\mathcal{A} = \langle A, F\rangle$ be a model of the free HEL_Σ. Then $\Omega(F)$ is the largest congruence in A whose visible part is F.

Proof. Suppose $a \equiv a'\ (\Omega(F)_V)$ with $V \in \mathit{VIS}$. Let z be a variable of sort V. Then z is a visible V-context and hence $a = z^A(a) \equiv z^A(a') = a'\ (F_V)$. Thus $\Omega(F)_{\mathit{VIS}} \subseteq F$. Conversely, assume $a \equiv a'\ (F_V)$. Then for every V-context $\varphi(z, \bar{u})$ and every choice of parameters $\bar{b} \in A_{\bar{Q}}$, we have $\varphi^A(a, \bar{b}) \equiv \varphi^A(a', \bar{b})\ (F_V)$. Thus $a \equiv a'\ (\Omega(F)_V)$ and hence $\Omega(F)_{\mathit{VIS}} = F$. If Θ is any other congruence on A such that $\Theta_{\mathit{VIS}} = G$, then Θ is compatible with F and hence $\Theta \subseteq \Omega(F)$. □

Definition 2.10.

(i) Let $\mathcal{L}$ be a *HEL* (a *EQL*). For any given set of equations and conditional equations E of visible (unrestricted) sort we define $\mathcal{L}[E]$ to be the *HEL* (the *EQL*) obtained from $\mathcal{L}$ by adjoining the equations and conditional equations in E as new axioms and new inference rules, respectively.

(ii) For every *HEL* $\mathcal{L}$ we take $\mathcal{L}^+$ to be the *EQL* over the same signature whose extra-logical axioms and inference rules are those of $\mathcal{L}$; $\mathcal{L}^+$ is called the *EQL-expansion* of $\mathcal{L}$.

For each theory T of a HEL_Σ $\mathcal{L}$ we have $\Omega(T) \cap \big(\mathrm{Te}_\Sigma)^2_{\mathit{VIS}}\big) = T$ by Corollary 2.9. Thus $\Omega(T) \in \mathit{Th}(\mathcal{L}^+)$. It also follows easily from Corollary 2.9 that if $\langle A, F\rangle \in \mathit{Mod}(\mathcal{L})$, then $\langle A, \Omega(F)\rangle \in \mathit{Mod}(\mathcal{L}^+)$. In particular, if $T \in \mathit{Th}(\mathcal{L})$, then $\Omega(T) \in \mathit{Th}(\mathcal{L}^+)$.

The following completeness theorem for hidden and unrestricted equational logic is special case of Theorem 2.6.

Theorem 2.11 (completeness theorem for equational logic[¶]). Let $\mathcal{L}$ be a HEL_Σ

[¶] As in the case of Theorem 2.6, this theorem is valid in general only under the assumption that all sort domains of models are non-empty. 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).

or a EQL_Σ. Then the following are equivalent for every visible conditional equation ξ in the *HEL* case and every unrestricted conditional equation ξ in the *EQL* case, the following are equivalent.

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

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

Proof. The equivalence of items (i), (ii), and (iv) follows immediately from Theorem 2.6. The equivalence of these with (iii) is an immediate consequence of the fact that $Mod^{*}(\mathcal{L}) \subseteq Mod^{=}(\mathcal{L})$ which follows from Corollary 2.9. □

2.3. *Examples*

Example 2.12. (**Flags**) This example was given by Goguen and Malcolm in (Goguen and Malcolm 1999). Consider the hidden signature Σ_{Flag}:

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

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

and the operation symbols for the Boolean part: $\neg, \wedge, \vee, True, False$.

The specification logic of Flags, $\mathcal{L}_{Flag}$, This is a specification of semaphores, which are commonly used in scheduling resources. With each resource is associated a flag. When a resource is being used by some process its flag is put "up" to indicate access is forbidden After being used its flag is put "down", which means that the resource is available to be used by another process. The operation *up*? is used to test the state of the semaphore. is the $HEL_{\Sigma_{Flag}}$ logic with the following Extra-logical axioms:

$$up?(up(F)) \approx True,$$
$$up?(dn(F)) \approx False,$$
$$up?(rev(F)) \approx \neg(up?(F)),$$

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

Example 2.13. (**Stacks**) This specification of stacks of natural numbers is unusual in the following two respects. First, the extra-logical axioms and inference rules are visible (they must be visible because there is no primitive notion of equality for hidden data elements). Consequently, we get an infinite number of axioms. Second, 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 (Goguen and Malcolm 2000).

Consider the hidden signature Σ_{Stacks}:

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

$empty : \quad \to Stack$	$Top : Stack \to Nat$
$zero : \quad \to Nat$	$Pop : Stack \to Stack$
$Push : Nat, Stack \to Stack$	$s : Nat \to Nat$

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:

$s(x) \approx s(y)$ `if` $x \approx y$.

3. Behavioral Reasoning

Two hidden data elements of the same type are *behaviorally equivalent* if any procedure whose parameter is of this type returns the same visible result 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 (called *methods*) that return hidden, as opposed to visible, elements induce transitions between states.

Behavioral equivalence has proved to be an useful device for importing the techniques and intuitions of transition systems into the algebraic paradigm. The concept of *behaviorally valid consequence* (Definition 3.3 below) was introduced in order to reason effectively about behavioral equivalence; it can be reified as a 2-logic that is not in general specifiable. 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 investigators: 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; Pigozzi 1999). The focus of the proof-theoretic investigation in all this work is on equations. 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 form of coinduction as a method of verifying the behavioral validity of a conditional equation is given in Theorem 3.5. The use of coinduction and standard equational logic in combination 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 standard equational deduction (Corollary 3.12). In the last part of the section we look at the case when behavioral validity is actually specifiable. The notion of a *HEL* that is behaviorally specifiable is defined in Definition 3.13. In Theorem 3.17 those *HEL*'s that are behaviorally specifiable are characterized in terms of the consequence of the *HEL* (this specializes a more general result for hidden k-logics in (Pigozzi 1999)). As a consequence, in Theorem 3.20 we obtain for behaviorally specifiable *HEL*'s a characterization of behaviorally valid conditional equations that does not make use of coinduction.

Definition 3.1. Let A be a Σ-algebra and let S be an unrestricted 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 $\varphi(z{:}S,\ u_1{:}T_1, ..., u_m{:}T_m)$ and for all $(b_1, ..., b_m) \in A_{S_1} \times ... \times A_{S_m}$, $\varphi^A(a, b_1, ..., b_m) = \varphi^A(a', b_1, ..., b_m)$.

The following corollary is an immediate consequence of Theorem 2.8.

Corollary 3.2. Let A be a Σ-algebra and S any sort. Then, for all $a, a' \in A_S$,

$$a \equiv_A^{\text{beh}} a' \quad \text{iff} \quad a \equiv a' \,\big(\Omega(id_{A_{VIS}})\big).$$

Since $\Omega(id_{A_{VIS}})$ coincides with $id_{A_{VIS}}$ on the visible part of A, we have that two visible elements are behaviorally equivalent iff they are equal.

Definition 3.3. Let A be a Σ-algebra.

(i) An equation $t \approx t'$ of unrestricted sort is said to be a *behaviorally valid consequence* of a set E of equations (of unrestricted sorts) in A, in symbols $E \models_A^{\text{beh}} t \approx t'$, if, for every assignment $h : X \to A$, $h(t) \equiv_A^{\text{beh}} h(t')$ whenever $h(s) \equiv_A^{\text{beh}} h(s')$ for every equation $s \approx s'$ in E.

(ii) An equation $t \approx t'$ is *behaviorally valid* in A if $\models_A t \approx t'$, and a conditional equation $t_n \approx t'_n$ `if` $t_0 \approx t'_0, \dots, t_{n-1} \approx t'_{n-1}$ is *behaviorally valid* in A if $t_0 \approx t'_0, \dots, t_{n-1} \approx t'_{n-1} \models_A^{\text{beh}} t_n \approx t'_n$.

Let $\mathcal{L}$ be an *HEL*.

(iii) An equation $t \approx t'$ of unrestricted sort is said to be *behavioral consequence over* $\mathcal{L}$ of a set E of equations (of unrestricted sorts), in symbols $E \models_{\mathcal{L}}^{\text{beh}} t \approx t'$, if $E \models_A^{\text{beh}} t \approx t'$ for every $A \in Mod^{=}(\mathcal{L})$.

(iv) An equation or conditional equation is *behaviorally valid over* $\mathcal{L}$ if it is behaviorally valid in every $A \in Mod^{=}(\mathcal{L})$.

One of the central problems of hidden equational logic is specifying the behavioral validities of a given *HEL*.

The following technical lemma will prove useful in the sequel.

Lemma 3.4. Let A be an arbitrary Σ-algebra.

(i) Let $a, a' \in A_S$ be elements of A of the same unrestricted sort S. Let $h : B \to A$ be a surjective homomorphism onto A from some other Σ-algebra B. Then, for any $b, b' \in B_S$ such that $h(b) = a$ and $h(b') = a'$,

$$a \equiv^{\mathrm{beh}}_{A} a' \quad \text{iff} \quad b \equiv b' \left(h^{-1}(\Omega(id_{A_{VIS}}))\right).$$

(ii) Let $t \approx t'$ be any equation and E any set of of equations (all of unrestricted sort). If $E \models^{\mathrm{beh}}_{B} t \approx t'$ for every locally countable subalgebra B of A, then $E \models^{\mathrm{beh}}_{A} t \approx t'$.
In particular, if a conditional equation is behaviorally valid in every locally countable subalgebra of A, then it is behaviorally valid in A.

Proof. (i) is an immediate consequence of Lemma 2.2 and Corollary 3.2.

(ii). We prove the contrapositive. Assume $E \not\models^{\mathrm{beh}}_{A} t \approx t'$. Then there is an assignment $g : X \to A$ such that $g(s) \equiv^{\mathrm{beh}}_{A} g(s')$ for all $s \approx s'$ in E, but $g(t) \not\equiv^{\mathrm{beh}}_{A} g(t')$. Let S be the common sort of t and t'. Then by the definition of behavioral equivalence there is a visible S-context $\varphi(z{:}S, \bar{u}{:}\bar{T})$, with $\bar{u}{:}\bar{T} = u_1{:}T_1, \dots, u_m{:}T_m$ and $\bar{b} \in A_{T_1} \times ... \times A_{T_m}$ such that $\varphi^A(g(t), \bar{b}) \neq \varphi^A(g(t'), \bar{b})$. Let B be the subalgebra of A generated by $g(X) \cup \bar{b}$; 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 $\varphi^B(g(t), \bar{b}) = \varphi^A(g(t), \bar{b}) \neq \varphi^A(g(t'), \bar{b}) = \varphi^B(g(t'), \bar{b})$. So $g(t) \not\equiv^{\mathrm{beh}}_{B} g(t')$.

On the other hand, for each $s{:}S \approx s'{:}S$ in E, $g(s), g(s') \in B$ and hence, for every visible$S$-context $\psi(z{:}S, \bar{y}{:}\bar{U})$ and all $\bar{c} \in B_{\bar{U}}$, we have $\psi^B(g(s), \bar{c}) = \psi^A(g(s), \bar{c}) = \psi^A(g(s'), \bar{c}) = \psi^B(g(s'), \bar{c})$. So $g(s) \equiv^{\mathrm{beh}}_{B} g(s')$ for each $s \approx s'$ in E. Thus $E \not\models^{\mathrm{beh}}_{B} t \approx t'$ □

The following result is the main lemma of the paper; it shows how coinduction (in our form) is used to verify the behavioral validity of conditional equations. More precisely, 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 *HEL*. It should be compared with the coinduction rule in (Roşu and Goguen 2000) for verifying the behavioral validity of equations.

Lemma 3.5. Let $\mathcal{L}$ be a *HEL*.

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

$$\forall T \in \mathit{Th}(\mathcal{L}) \left(\forall (s \approx s') \in E \ (s \equiv s' \ (\Omega(T)) \ \Rightarrow t \equiv t' \ (\Omega(T))\right). \tag{8}$$

(ii) A conditional equation

$$t_n \approx t'_n \ \texttt{if} \ t_0 \approx t'_0, \dots, t_{n-1} \approx t'_{n-1} \tag{9}$$

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

$$\forall T \in \mathit{Th}(\mathcal{L}) \left(\forall i < n (t_i \equiv t'_i \ (\Omega(T)) \ \Rightarrow t_n \equiv t'_n \ (\Omega(T)\right).$$

Proof. (i): Assume $E \models^{\mathrm{beh}}_{\mathcal{L}} t \approx t'$. Let $T \in \mathit{Th}(\mathcal{L})$ such that $s \equiv s' \big(\Omega(T)\big)$ for all $s \approx s'$ in E. Let $\mathcal{A} = \langle \mathrm{Te}_\Sigma/\Omega(T), T/\Omega(T)\rangle$ be the quotient of $\langle \mathrm{Te}_\Sigma, T\rangle$ by $\Omega(T)$. By Corollary 2.3, $\mathcal{A}$ is a reduced model of $\mathcal{L}$; in particular, it is an equality model. Let $A = \mathrm{Te}_\Sigma/\Omega(T)$. Then $\mathcal{A} = \langle A, id_{A_{VIS}}\rangle$ and $\Omega(id_{A_{VIS}}) = id_A$ since $\mathcal{A}$ is reduced. Let

$h : \mathrm{Te}_\Sigma \to A$ be the natural homomorphism. Then $\Omega(T) = h^{-1}(id_A) = h^{-1}\big(\Omega(id_{A_{VIS}})\big)$. By assumption $h(s) = h(s')$, i.e., $h(s) \equiv h(s')\ \big(\Omega(id_{A_{VIS}})\big)$, for every $s \approx s'$ in E. Since $E \models^{\mathrm{beh}}_{\mathcal{L}} t \approx t'$ by hypothesis, $h(t) \equiv h(t')\big(\Omega(id_{A_{VIS}})\big)$. Then $t \equiv t'\ \big(\Omega(T)\big)$. So the condition (8) holds.

Conversely, assume (8) holds. By Lemma 3.4(ii) it suffices to show that $E \models^{\mathrm{beh}}_{A} t \approx t'$ for every locally countable identity 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 $\bar{t} \approx \bar{t}'$ and $\widehat{E} = \{\, \bar{s} \approx \bar{s}' : (s \approx s') \in E \,\}$ with this property and such that $\widehat{E} \models^{\mathrm{beh}}_{\mathcal{L}} \bar{s} \approx \bar{s}'$ iff $E \models^{\mathrm{beh}}_{\mathcal{L}} s \approx s'$.

Let $A \in \mathit{Mod}^{=}(\mathcal{L})$ be locally countable, and let $h : X \to A$ be an arbitrary assignment such that $h(s)$ and $h(s')$ are behaviorally equivalent in A 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, and thus by Lemma 3.4(i), $s \equiv s'\ \big(\Omega(h^{-1}(id_{A_{VIS}}))\big)$ for each $s \approx s'$ in E. Then by hypothesis, $t \equiv t'\big(\Omega(h^{-1}(id_{A_{VIS}}))\big)$. Hence, $h(t)$ and $h(t')$ are behaviorally equivalent in A, again by Lemma 3.4(i).

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

This result can be reformulated in the following convenient way.

Corollary 3.6. Let $\mathcal{L}$ be a *HEL*, and let E be a set of unrestricted conditional equations. Then every conditional equation in E is behaviorally valid over $\mathcal{L}$ iff $\Omega\big(\mathit{Th}(\mathcal{L})\big) \subseteq \mathit{Th}\big(\mathcal{L}^{+}[E]\big)$.

Proof. Assume each conditional equation of E is behaviorally valid over $\mathcal{L}$. Let $T \in \mathit{Th}(\mathcal{L})$. Then as we have previously observed $\Omega(T) \in \mathit{Th}(\mathcal{L}^{+})$. Thus to show $\Omega(T) \in \mathit{Th}\big(\mathcal{L}^{+}[E]\big)$ it suffices to show that $\langle \mathrm{Te}_\Sigma, \Omega(T)\rangle$ is a model of each rule in E. Let $\xi \in E$ be of the form

$$t_n \approx t'_n \ \texttt{if} \ t_0 \approx t'_0, \ldots, t_{n-1} \approx t'_{n-1}. \tag{10}$$

Let $\sigma : X \to \mathrm{Te}_\Sigma$ 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 2.2. Thus, since $\sigma^{-1}(T) \in \mathit{Th}(\mathcal{L})$ and ξ is behaviorally valid over $\mathcal{L}$ by assumption, we have by Lemma 3.5 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 $\tau : X \to \mathrm{Te}_\Sigma$ 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 $\langle \mathrm{Te}_\Sigma, \Omega(T)\rangle$ is a model of ξ for each $\xi \in E$, and hence $\Omega(T) \in \mathit{Th}\big(\mathcal{L}^{+}[E]\big)$.

For the implication in the other direction, assume $\Omega\big(\mathit{Th}(\mathcal{L})\big) \subseteq \mathit{Th}\big(\mathcal{L}^{+}[E]\big)$ Let $T \in \mathit{Th}(\mathcal{L})$. Let ξ be a rule of E of the form (10) and 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 $\Omega(T) \in \mathit{Th}\big(\mathcal{L}^{+}[E]\big)$ by assumption. So ξ is behaviorally valid over $\mathcal{L}$ by Lemma 3.5. □

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

In the following corollaries we give two simpler characterizations for conditional equations of a special kind to be behaviorally valid in $\mathcal{L}$; 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 (9) are all visible then condition ((ii)) can be simplified in the last theorem since, in this case, $t_i \equiv t'_i \ \big(\Omega(T)\big)$ iff $t_i \equiv t'_i \ (T)$ by Corollary 2.9. Thus we get the following result.

Corollary 3.7. Let $\mathcal{L}$ be a *HEL*. A conditional equation (9) with visible antecedents is behaviorally valid over $\mathcal{L}$ iff $t_n \equiv t'_n \ \big(\Omega(\mathit{Con}_{\mathcal{L}}\{\, t_i \approx t'_i : i < n \,\}\big)$.

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

$$t \equiv t' \ \big(\Omega(\mathit{Thm}(\mathcal{L}[\{\, t_i \approx t'_i : i < n \,\}])\big). \tag{11}$$

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

If the consequent $t_n \approx t'_n$ of the conditional equation (9) is visible, then the characterization of behavioral validity given in Lemma 3.5 can be simplified in the following way.

Corollary 3.8. Let $\mathcal{L}$ be a *HEL*. A conditional equation (9) with a visible consequent is behaviorally valid over $\mathcal{L}$ iff

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

Proof. Let

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

Assume (9) is not behaviorally valid over $\mathcal{L}$. Then by Lemma 3.5 there is a theory T of $\mathcal{L}$ such that

$$t_i \equiv t'_i \ (\Omega(T)), \text{ for all } i < n, \quad \text{and} \quad t_n \not\equiv t'_n \ (\Omega(T)). \tag{12}$$

From the first condition we conclude by Theorem 2.8 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 (12) we conclude that $t_n \not\equiv t'_n \ (T)$. So $t_n \not\equiv t'_n \ (G)$.

Assume now that (9) is behaviorally valid over $\mathcal{L}$. $G \in \mathit{Th}(\mathcal{L})$ and, by definition of G, $t_i \equiv t'_i \ (\Omega(G))$. Hence, by Lemma 3.5, we get that $t_n \equiv t'_n \ (\Omega(G))$. Thus $t_n \equiv t'_n \ (G)$ since t_n, t'_n are visible. □

According to the next corollary, another straightforward consequence of Lemma 3.5, the theorems of the *EQL*-expansion $\mathcal{L}^+$ of $\mathcal{L}$ are all behaviorally valid over $\mathcal{L}$, and, what is more interesting, the same is true for any extension of $\mathcal{L}^+$ obtained by adjoining a behaviorally valid conditional equation as a new inference rule.

Corollary 3.9. Let $\mathcal{L}$ be a HEL_Σ, and assume $\xi = (t_n \approx t'_n \ \texttt{if} \ t_1 \approx t'_1, \dots, t_{n-1} \approx t'_{n-1})$ is behaviorally valid in $\mathcal{L}$. Then for every Σ-equation $s \approx s'$ (of unrestricted sort), $\vdash_{\mathcal{L}^+[\xi]} s \approx s'$ implies that $s \approx s'$ is behaviorally valid over $\mathcal{L}$.

Proof. We want to show that $s \equiv s' \big(\mathit{Thm}(\mathcal{L}^+[\xi])\big)$ implies $s \equiv s' \big(\Omega(\mathit{Thm}(\mathcal{L})\big)$. But $\mathit{Thm}(\mathcal{L}^+[\xi]) \subseteq \Omega(\mathit{Thm}(\mathcal{L}))$ because $\Omega(\mathit{Thm}(\mathcal{L}))$ is a theory of $\mathcal{L}^+$, and hence also a theory of $\mathcal{L}^+[\xi]$ since, by Lemma 3.5, 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 $\mathcal{L}^+[E]$ is already a derivable rule of $\mathcal{L}^+$, i.e., for every conditional equation $s_m \approx s'_m \ \texttt{if} \ s_0 \approx s'_0, \dots, s_{m-1} \approx s'_{m-1}$ with a visible consequent,

$$\begin{aligned}\{s_0 \approx s'_0, \dots, s_{m-1} \approx s'_{m-1}\} &\vdash_{\mathcal{L}^+[E]} s_m \approx s'_m \\ &\text{implies} \quad \{s_0 \approx s'_0, \dots, s_{m-1} \approx s'_{m-1}\} \vdash_{\mathcal{L}^+} s_m \approx s'_m. \qquad (13)\end{aligned}$$

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

$$\{s_0 \approx s'_0, \dots, s_{m-1} \approx s'_{m-1}\} \vdash_{\mathcal{L}^+[E]} s_m \approx s'_m \qquad (14)$$

with $s_m \approx s'_m$ visible. Let G be any theory of $\mathcal{L}^+$ such that $s_i \equiv s'_i\,(G)$ for all $i < m$. G_{VIS} is a theory of $\mathcal{L}$ and $\Omega(G_{\mathit{VIS}})$ is a theory of $\mathcal{L}^+[E]$ by Corollary 3.6, and since $G \subseteq \Omega(G_{\mathit{VIS}})$, we have that $s_i \equiv s'_i\,(\Omega(G_{\mathit{VIS}}))$ for each $i < m$. So by the assumption (14), $s_m \equiv s'_m\,(\Omega(G_{\mathit{VIS}}))$. But then $s_m \equiv s'_m\,(G_{\mathit{VIS}})$ since $s_m \approx s'_m$ is visible. Thus $\{s_0 \approx s'_0, \dots, s_{m-1} \approx s'_{m-1}\} \vdash_{\mathcal{L}^+} s_m \approx s'_m$. This verifies (13).

Assume now that (13) holds for every conditional equation $s_m \approx s'_m \ \texttt{if} \ s_0 \approx s'_0, \dots, s_{m-1} \approx s'_{m-1}$ with visible antecedent. By Corollary 3.6 it suffices to show that

$$\Omega\big(\mathit{Th}(\mathcal{L})\big) \subseteq \mathit{Th}(\mathcal{L}^+[E]). \qquad (15)$$

Suppose $T \in \mathit{Th}(\mathcal{L})$, and let $G = \mathit{Con}_{\mathcal{L}^+[E]}\big(\Omega(T)\big)$, the $\mathcal{L}^+[E]$-theory generated by $\Omega(T)$. We claim that $G_{\mathit{VIS}} = T$. 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 $\mathcal{L}^+[E]$-theory by $\Omega(T)$, there are equations $s_0 \approx s'_0, \dots, s_{m-1} \approx s_{m-1}$ such that $s_i \equiv s'_i\,\big(\Omega(T)\big)$, for $i < m$, and $\{s_0 \approx s'_0, \dots, s_{m-1} \approx s'_{m-1}\} \vdash_{\mathcal{L}^+[E]} s \approx s'$. Thus, by assumption, $\{s_0 \approx s'_0, \dots, s_{m-1} \approx s'_{m-1}\} \vdash_{\mathcal{L}^+} s \approx s'$. Hence $s \equiv s'\,\big(\Omega(T)\big)$, since $\Omega(T)$ is a $\mathcal{L}^+$-theory as previously observed. But $s \approx s'$ is visible, so $s \equiv s'\,(T)$. Thus $G_{\mathit{VIS}} \subseteq T$. Since the opposite inclusion is obvious, we have verified the claim. Then $\Omega(T) = \Omega(G_{\mathit{VIS}}) \supseteq G$; but obviously $\Omega(T) \subseteq G$. So $\Omega(T) = G \in \mathit{Th}\big(\mathcal{L}^+[E]\big)$. Hence (15) 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 $\mathcal{L}^+[E]$ is already a derivable rule of $\mathcal{L}^+$, i.e., by the weaker version of (13) where the antecedents $s_0 \approx s'_0, \dots, s_{m-1} \approx s'_{m-1}$ are all required to be visible. However, the following counterexample shows that the condition (13) in its full strength is necessary.

Consider the Flags example and the conditional equation

$$\mathit{dn}(F) \approx F \ \ \texttt{if} \ \ \mathit{rev}(\mathit{rev}(F)) \approx F. \tag{16}$$

On one hand, since $\mathit{rev}(\mathit{rev}(F)) \approx F$ is behaviorally valid while $\mathit{dn}(F) \approx F$ is not, this is not a behaviorally valid conditional equation. One the other hand, the weaker version of (13), where the conditional equations are restricted to be visible, holds. This follows from the easily verified fact that no substitution instance of $\mathit{rev}(\mathit{rev}(F)) \approx F$ 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 (16) can never be applied.

It follows easily from Theorem 3.10 that, if the set of derivable rules of $\mathcal{L}$ is recursively enumerable (RE), in particular, if $\mathcal{L}$ has a presentation with a finite number of axioms and rules of inference, then the set of behaviorally valid conditional equations over $\mathcal{L}$ is at level $\prod^0_2$ 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 $\prod^0_2$-complete. But note also 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.

Corollary 3.11. Let $\mathcal{L}$ be a *HEL* and let ξ be a behaviorally valid conditional equation over $\mathcal{L}$. Then, for every $s, s' \in \mathrm{Te}_{\mathit{VIS}}$,

$$\vdash_{\mathcal{L}^+[\xi]} s \approx s' \quad \text{iff} \quad \vdash_{\mathcal{L}} s \approx s'. \tag{17}$$

This corollary shows that the converse of Corollary 3.9 holds for visible equations.

In the final result of this subsection we show that the set E of 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 $\mathcal{L}^+[E]$ is already a member of E.

Corollary 3.12. 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 $\mathcal{L}^+[E]$ 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 $\mathcal{L}^+[E]$. Clearly then

$$\vdash_{\mathcal{L}^+[\xi]} \subseteq \vdash_{\mathcal{L}^+[E]} . \tag{18}$$

Then, applying Theorem 3.10, we get that ξ is behaviorally valid. In fact, let $s_m \approx s'_m$ `if` $s_0 \approx s'_0, \dots, s_{m-1} \approx s'_{m-1}$ be any conditional equation with visible consequent, and suppose that $\{s_0 \approx s'_0, \dots, s_{m-1} \approx s'_{m-1}\} \vdash_{\mathcal{L}^+[\xi]} s_m \approx s'_m$. Then, by (18), $\{s_0 \approx s'_0, \dots, s_{m-1} \approx s_{m-1}\} \vdash_{\mathcal{L}^+[E]} s_m \approx s'_m$. Hence, applying Theorem 3.10 we get $\{s_0 \approx s'_0, \dots, s_{m-1} \approx s_{m-1}\} \vdash_{\mathcal{L}} s_m \approx s'_m$. 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 $\mathcal{L}$. □

3.2. *The specification of behavioral validity*

In this subsection we provide a syntactic characterization of those *HEL*'s whose behavioral validity is specifiable.

Definition 3.13 ((Pigozzi 1999)). Let $\mathcal{L}$ be a *HEL*. We say that a *HEL* is *behaviorally specifiable* if there is an *EQL* $\mathcal{L}'$, in the same language, such that $\Omega\big(\mathit{Th}(\mathcal{L})\big) = \mathit{Th}(\mathcal{L}')$, where $\Omega\big(\mathit{Th}(\mathcal{L})\big) = \{\, \Omega(T) : T \in \mathit{Th}(\mathcal{L}) \,\}$. We call $\mathcal{L}'$ a *behavioral specification* of $\mathcal{L}$.

As an immediate consequence of Lemma 3.5 we have the following result.

Theorem 3.14. Let $\mathcal{L}$ be a *HEL*. An *EQL* $\mathcal{L}'$ over the same signature is a behavioral specification of $\mathcal{L}$ iff $\models^{\text{beh}}_{\mathcal{L}} = \vdash_{\mathcal{L}'}$ i.e., for every set of equations $E \cup \{t \approx t'\}$ (of unrestricted sort) we have $E \models^{\text{beh}}_{\mathcal{L}} t \approx t'$ iff $E \vdash_{\mathcal{L}'} t \approx t'$.

By definition the behavior of a *HEL* $\mathcal{L}$ is specified by the *EQL* $\mathcal{L}'$ iff Ω is surjective as a mapping from $\mathit{Th}(\mathcal{L})$ to $\mathit{Th}(\mathcal{L}')$. This mapping is always injective, because if $\Omega(T) = \Omega(G)$, then $T = \Omega(T)_{\mathit{VIS}} = \Omega(G)_{\mathit{VIS}} = G$. It is also always monotonic: For suppose $T \subseteq G$. Then $\Omega(T)$ is compatible with G, because $\Omega(T)_{\mathit{VIS}} \subseteq G$, and hence $\Omega(T) \subseteq \Omega(G)$. Consequently, if $\mathcal{L}'$ behaviorally specifies $\mathcal{L}$, then Ω is a isomorphism between the algebraic lattices $\mathit{Th}(\mathcal{L})$ and $\mathit{Th}(\mathcal{L}')$. Thus Ω gives a one-one correspondence between the sets of compact elements of the two lattices $\mathit{Th}(\mathcal{L})$ and $\mathit{Th}(\mathcal{L}')$. But $T \in \mathit{Th}(\mathcal{L})$ is compact the lattice of theories iff it is finitely generated, and similarly for theories of $\mathcal{L}'$. This gives the following lemma.

Lemma 3.15. Let $\mathcal{L}$ be a behaviorally specifiable *HEL* and $\mathcal{L}'$ its behavioral specification. If $G \in \mathit{Th}(\mathcal{L}')$ is finitely generated then G_{VIS} is also finitely generated as a $\mathcal{L}$-theory.

If a *HEL* is behaviorally specifiable, then its associated *EQL* of behavioral valid consequence has a presentation by some set of axioms and rules of inference. Many *HEL*'s that arise in practice are behaviorally specifiable, $\mathcal{L}_{\mathit{Flags}}$ for example (see Section 4).

However, many are not; for example, $\mathcal{L}_{Stacks}$ is not behaviorally specifiable (see (Martins 2001)). And in many of these cases, there are just a few equations and conditional equations that when adjoined to the axioms and rules of inference of the *HEL*, give a complete presentation of is associated *EQL*. Once these are identified and proved behaviorally valid using Theorem 3.5 or some other version of coinduction, the all behaviorally valid equations and conditional equations can be obtained by standard equational logic. There still remains however the problem of determining when a given set of behaviorally valid equations and conditional equations is complete in this sense. For this problem the following characterization of behavioral specifiable *HEL*'s may be useful.

By a *pre-equivalence system* over Σ we mean a *HID*-sorted set $E = \langle E_H(x{:}H, y{:}H) : H \in \mathit{HID}\rangle$, where, for each H, $E_H(x{:}H, y{:}H)$ is itself a *VIS*-sorted set $\big\langle E_{H,V}(x{:}H, y{:}H) : V \in \mathit{VIS}\big\rangle$ such that $E_{H,V}(x{:}H, y{:}H)$ is a set of equations (2-terms) of sort V in the same two variables x and y of sort H, i.e., $E_{H,V}(x{:}H, y{:}H) \subseteq \big(\mathrm{Te}^2(\{x, y\})\big)_V$.

The following definition of equivalence system for hidden equational logics in a special case of a more general notion of arbitrary k-deductive systems given in (Pigozzi 1999).

Definition 3.16. Let $\mathcal{L}$ be a *HEL*. A pre-equivalence system $E = \langle E_H : H \in \mathit{HID}\rangle$ is called an *equivalence system* for $\mathcal{L}$ if the following conditions hold for every $H \in \mathit{HID}$.

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

(a) If $S_n \notin \mathit{VIS}$ then
$$\{\, E_{S_i}(x_i{:}S_i, y_i{:}S_i) : S_i \in \mathit{HID}\,\} \cup \{x_i \approx y_i : S_i \in \mathit{VIS}\} \vdash_{\mathcal{L}} E_{S_n}(O(x_0, \dots, x_{n-1}){:}S_n, O(y_0, \dots, y_{n-1}){:}S_n);$$

(b) If $S_n \in \mathit{VIS}$ then
$$\{\, E_{S_i}(x_i{:}S_i, y_i{:}S_i) : S_i \in \mathit{HID}\,\} \cup \{x_i \approx y_i : S_i \in \mathit{VIS}\} \vdash_{\mathcal{L}} O(x_0, \dots, x_{n-1}) \approx O(y_0, \dots, y_{n-1}).$$

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 Δ_H is globally finite (i.e. $\bigcup E_{H,V}(x{:}H, y{:}H)$ is finite) for each $H \in \mathit{HID}$, then $\mathcal{L}$ is called *finitely equivalential*.

The following theorem shows that a pre-equivalence systems is an equivalence system if and only if it defines the Leibniz congruence in a natural way.

Theorem 3.17. Let $\mathcal{L}$ be a *HEL* and E a pre-equivalence system for $\mathcal{L}$. Then, E is an equivalence system for $\mathcal{L}$ iff for every $T \in \mathit{Th}(\mathcal{L})$ and every sort $H \in \mathit{HID}$,
$$(\Omega(T))_H = \{\langle t, t'\rangle : E_H(t, t') \subseteq T\}. \tag{19}$$

Proof. Suppose E is and equivalence system. Let Θ be defined as the set
$$\Theta_H = \big\{(t, t') : E_H(t, t') \subseteq T\big\}, \text{ for } H \in \mathit{HID} \text{ and } \Theta_{VIS} = T.$$

From the definition of equivalence system it is easily seen that Θ is a congruence with visible part T. To see that Θ is the largest such congruence, let Φ be any congruence whose visible part is T. Assume that $t \equiv t'$ (Φ_H). Then for every equation $\delta_0(x, y) \approx \delta_1(x, y)$ in $E_{H,V}$,

$$\delta_0(t,t) \equiv \delta_0(t,t')\ (\Phi_V) \quad \text{and} \quad \delta_1(t,t) \equiv \delta_1(t,t')\ (\Phi_V).$$

Thus, since $\Phi_V = T_V$.

$$\langle \delta_0(t,t),\ \delta_0(t,t') \rangle, \langle \delta_1(t,t),\ \delta_1(t,t') \rangle \in T_V.$$

But $\langle \delta_0(t,t),\ \delta_1(t,t) \rangle \in T_V)$, so by transitivity we have $\langle \delta_0(t,t'),\ \delta_1(t,t') \rangle \in T_V$ for every $\delta_0(x,y) \approx \delta_1(x,y)$ in $E_{H,V}$. Hence, $t \equiv t'$ (Θ_H). Therefore, Θ is the largest congruence whose visible part is T, which shows that $\Theta = \Omega(T)$.

Suppose now that (19) holds. The properties of $\Omega(T)$ as a congruence relation whose visible part is T translate directly into the properties that define E has an equivalence system. For example condition 3.16(iii) canbe proved in the following way. Let $T \in \mathit{Th}(\mathcal{L})$ and suppose that $E_H(t,t'), E_H(t',t'') \subseteq T$ then $t \equiv t'$ $(\Omega(T))$ and $t' \equiv t''$ $(\Omega(T))$. Hence, by transitivity of $\Omega(T)$, $t \equiv t''$ $(\Omega(T))$, i.e., $E_H(t,t'') \subseteq T$. Since this is true for every theory T, 3.16(iii) holds. □

Roşu and Goguen in (Roşu and Goguen 2001) introduced the concept of cobasis that is intimately related to our notion of equivalence system. Theorem 3.19 below shows such relationship.

By a *pre-cobasis* over a hidden signature Σ we mean a *HID*-sorted set

$$\Delta = \langle \Delta_H(z{:}H,\ \bar{u}{:}\bar{Q}) : H \in \mathit{HID} \rangle,$$

where, for each H, $\Delta_H(z{:}H,\ \bar{u}{:}\bar{Q})$ is itself a *SORT*-sorted set

$$\big\langle \Delta_{H,S}(z{:}H,\ \bar{u}{:}\bar{Q}) : S \in \mathit{SORT} \big\rangle$$

such that $\Delta_{H,S}(z{:}H, \bar{u}{:}\bar{Q})$ is a set of H-contexts of sort S, each with distinguished variable z and parameters $u_0, u_1, \ldots, u_{n_\delta - 1}$, which for convenience we assume is an initial segment of a (possibly infinite) sequence of variables $\bar{u}{:}\bar{Q} = \langle u_0{:}Q_0, u_1{:}Q_1, u_2{:}Q_2, \ldots \rangle$ that excludes an infinite set of variables of each sort. We take $Te_{\bar{Q}}(X)$ as shorthand for $\mathrm{Te}_{Q_0} \times \mathrm{Te}_{Q_1} \times \ldots$.

In order to simplify matters we sometimes abuse notation by identifying the *SORT*-sorted set Δ_H with its union $\bigcup_{S \in \mathit{SORT}} \Delta_{H,S}$.

Definition 3.18. Let $\mathcal{L}$ be a *HEL*. A pre-cobasis $\Delta = \langle \Delta_H(z{:}H,\ \bar{u}{:}\bar{Q}) : H \in \mathit{HID} \rangle$ is called a *cobasis* for $\mathcal{L}$ if, for each $T \in \mathit{Th}(\mathcal{L})$, each sort $H \in \mathit{HID}$ and all $t,\ t' \in \mathrm{Te}_H$,

$$\big(\forall\, \delta \in \Delta_H,\ \forall\, \bar{\vartheta} \in \mathrm{Te}_{\bar{Q}}(X),\ \delta(t, \bar{\vartheta}) \equiv \delta(t', \bar{\vartheta})\ (\Omega(T))\big) \implies t \equiv t'\ (\Omega(T)).$$

If, for each $H \in \mathit{HID}$, $\Delta_{H,S} = \emptyset$ for every non-visible S, Δ is said to be *visible.* If Δ_H is globally finite for each $H \in \mathit{HID}$, Δ is said to be *locally globally finite.*

It follows from Theorem 2.8 that the set of all visible contexts is an example of a visible cobasis.

Recall that a signature Σ is *standard* if there is a ground term of every sort.

Theorem 3.19. Let $\mathcal{L}$ be a specifiable *HEL* over a standard signature Σ. Then the following conditions are equivalent.

(i) $\mathcal{L}$ is behaviorally specifiable.

(ii) $\mathcal{L}$ is finitely equivalential.

(iii) There is a visible cobasis Δ for $\mathcal{L}$ such that the set of parameters is empty and Δ_H is globally finite for each hidden sort H.

Proof. (iii) $\Longrightarrow$ (ii). Let Δ be a globally finite visible cobasis for $\mathcal{L}$ with and empty set of parameters and such that Δ_H is globally finite for each $H \in \mathit{HID}$. Define, for each hidden sort H and each visible sort V,

$$E_{H,V}(x{:}H, y{:}H) = \{\, \delta(x{:}H) \approx \delta(y{:}H) : \delta(z{:}H) \in \Delta_{H,V}(z{:}H) \,\}.$$

Suppose $E_H(t,t') \subseteq T$. Then $\delta(t) \equiv \delta(t')$ $(\Omega(T))$ for each $\delta \in \Delta_H$ since $T \subseteq \Omega(T)$. Hence $t \equiv t'$ $(\Omega(T))$ by definition of cobasis. Conversely, if $t \equiv t'$ $(\Omega(T))$, then $\delta(t) \equiv \delta(t')$ $(\Omega(T))$ since $\Omega(T)$ is a congruence. Thus $E_H(t,t') \subseteq T$ since each equation in $E_H(t,t')$ is visible and $\Omega(T)_{\mathit{VIS}} = T$. Applying Theorem 3.17 we have that $E(x,y)$ is a equivalence system for $\mathcal{L}$ such that E_H is globally finite for each $H \in \mathit{HID}$.

(ii) $\Longrightarrow$ (i). Let $E(x,y)$ be an equivalence system for $\mathcal{L}$ such that $E(x,y)_H$ is globally finite for each $H \in \mathit{VIS}$. Define $\mathcal{L}'$ as the *EQL* obtained from $\mathcal{L}^+$ by adding, for each hidden sort H, the new inference rule

$$x \approx y \ \texttt{if} \ \varphi_1(x,y) \approx \psi_1(x,y), \dots, \varphi_n(x,y) \approx \psi_n(x,y), \tag{20}$$

where $E_H(x{:}H, y{:}H) = \{\varphi_1(x,y) \approx \psi_1(x,y), \dots, \varphi_n(x,y) \approx \psi_n(x,y)\}$. We will show that $\{\, \Omega(T) : T \in \mathit{Th}(\mathcal{L}) \,\} = \mathit{Th}(\mathcal{L}')$.

Let $T \in \mathit{Th}(\mathcal{L})$. We have already seen that $\Omega(T) \in \mathit{Th}(\mathcal{L}^+)$, so in order to get $\Omega(T) \in \mathit{Th}(\mathcal{L}')$, it is enough to show that $\Omega(T)$ is closed under the new inference rules (20). Let t, t' be H-terms such that $\varphi_i(t,t') \equiv \psi_i(t,t')$ $(\Omega(T))$ for $i \le n$. Since the $\varphi_i(t,t') \approx \psi_i(t,t')$ are visible equations, we have $E_H(t,t') \subseteq T$, and hence $t \approx t'$ $(\Omega(T))$ by Theorem 3.17. So $\{\, \Omega(T) : T \in \mathit{Th}(\mathcal{L}) \,\} \subseteq \mathit{Th}(\mathcal{L}')$.

To prove the other inclusion, let $G \in \mathit{Th}(\mathcal{L}')$. Since $G \in \mathit{Th}(\mathcal{L}^+)$, $G_{\mathit{VIS}} \in \mathit{Th}(\mathcal{L})$, and hence $G \subseteq \Omega(G_{\mathit{VIS}})$ because $\Omega(G_{\mathit{VIS}})$ is the largest congruence whose visible part is G_{VIS}. Suppose $t \equiv t'$ $\big(\Omega(G_{\mathit{VIS}})_H\big)$. Since E is an equivalence system, $E_H(t,t') \subseteq (G_{\mathit{VIS}})_H$. So $\varphi_i(t,t') \equiv \psi_i(t,t')$ $(\Omega(G))$ for all $i \le n$. Using the inference rule (20) we conclude that $\langle t, t' \rangle \in G$. Hence $\Omega(G_{\mathit{VIS}}) \subseteq G$, and thus $G = \Omega(G_{\mathit{VIS}})$.

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

(i) $\Longrightarrow$ (iii). Suppose that $\mathcal{L}$ is behaviorally specifiable and let $\mathcal{L}'$ be its behavioral specification. Let H be a fixed but arbitray 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., $G = \mathit{Con}_{\mathcal{L}'}(\{\langle x, y \rangle\})$. Then G_{VIS} is finitely generated because G is (see the remarks following Theorem 3.14). On the other hand, by Theorem 2.8 G_{VIS} is also generated by the set

$$\big\{\, \langle \varphi(x{:}H, \bar{\vartheta}{:}\bar{Q}),\ \varphi(y{:}S, \bar{\vartheta}{:}\bar{Q}) \rangle : \varphi \in C_H, \bar{\vartheta} \in \mathrm{Te}_{\bar{Q}}(X) \,\big\},$$

where C_H is the set of all visible H-contexts. In fact, let T be the $\mathcal{L}$-theory generated by this set of equations. Then $x \equiv y\ (\Omega(T))$, and hence, since $\Omega(T)$ is an $\mathcal{L}'$-theory by assumption, we have that $G \subseteq \Omega(T)$. It follows that $G_{VIS} \subseteq \Omega(T)_{VIS} = T$. On the other hand, it is obvious that $T \subseteq G_{VIS}$. So $G_{VIS} = T$.

Consequently, there is a finite subset

$$\Delta_H(z{:}H, v_1{:}R_1, \dots, v_n{:}R_n) := \{\, \delta_i(z{:}H, v_1{:}R_1, \dots, v_n{:}R_n) : i \leq m \,\}$$

of visible H-contexts such that the set of equations $\big\{\delta_i(x{:}H,\ \bar{v}{:}\bar{R}) \approx \delta_i(x{:}H,\ \bar{v}{:}\bar{R}) : i \leq m \,\big\}$ also generates G_{VIS}. In particular

$$\begin{aligned}&\big\{\delta_i(x{:}H,\ \bar{v}{:}\bar{R}) \approx \delta_i(x{:}H,\ \bar{v}{:}\bar{R}) : i \leq m \,\big\}\\ &\qquad\qquad \vdash_{\mathcal{L}} \varphi(x{:}H, \bar{u}{:}\bar{Q}) \approx \varphi(y{:}H, \bar{u}{:}\bar{Q}) \quad \text{for each } \varphi \in C_H, \end{aligned} \tag{21}$$

where we assume without loss of generality that $\bar{u}{:}\bar{Q}$ is a infinite sequence of variables each of which is distinct from $v_1, \dots, v_n$. Let $\bar{s}{:}\bar{R} = \langle s_1{:}R_1, \dots, s_n{:}R_n \rangle$ be a sequence of ground terms; such a sequence exists by the assumption Σ is standard. Consider any $t, t' \in \mathrm{Te}_H(X)$ and any $\bar{\vartheta} \in \mathrm{Te}_{\bar{Q}}$. From (21) we have by the substitution invariance of $\vdash_{\mathcal{L}}$ that

$$\begin{aligned}&\big\{\delta_i(x{:}H,\ \bar{s}{:}\bar{R}) \approx \delta_i(x{:}H,\ \bar{s}{:}\bar{R}) : i \leq m \,\big\}\\ &\qquad \vdash_{\mathcal{L}} \varphi(t{:}H, \bar{\vartheta}{:}\bar{Q}) \approx \varphi(t'{:}H, \bar{\vartheta}{:}\bar{Q}) \quad \text{for every } \varphi \in C_H \text{ and } \vartheta \in \mathrm{Te}_{\bar{Q}}(X). \end{aligned} \tag{22}$$

From this we will conclude that $\Delta' := \langle\, \Delta_H(x{:}H,\ y{:}H,\ \bar{s}{:}\bar{R}) : H \in \mathit{HID} \,\rangle$ is a locally globally visible cobasis for $\mathcal{L}$ with an empty set of parameters. Only the cobasis property is not obvious. For the purpose of verifying it, let $T \in \mathit{Th}(\mathcal{L})$, $H \in \mathit{HID}$ and $t, t' \in \mathrm{Te}_H(X)$, and suppose that $\delta(t, \bar{s}) \equiv \delta(t', \bar{s})\ (\Omega(T)_H)$ for each $\delta \in \Delta_H$. Then by (22), $\varphi(t\bar{\vartheta}) \equiv \varphi(t', \bar{\vartheta})$ for every $\varphi \in C_H$ and $\vartheta \in \mathrm{Te}_{\bar{Q}}(X)$. Thus by Theorem 2.8 $t \equiv t'\ (\Omega(T)_H)$. □

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

(i) The conditional equation

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

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 $H \in \mathit{HID}$, 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

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

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

Proof. (i) ⇒ (ii) Define $G = \mathit{Con}_{\mathcal{L}}\big(\bigcup\{E_{S_i}(t_i{:}S_i, t'_i{:}S_i) : i < n\}\big)$. For each $i < n$, $t_i \equiv t'_i\,(\Omega(G))$ by Theorem 3.17. Then, from Lemma 3.5 and (i) we get $t_n \equiv t'_n\,(\Omega(G))$. So, applying Theorem 3.17 again, we get $E_{S_n}(t_n, t'_n) \subseteq G$, i.e., (ii) holds.

(ii) ⇒ (i) Let $T \in \mathit{Th}(\mathcal{L})$. Suppose that $t_i \equiv t'_i\,(\Omega(T))$ for each $i < n$. Then, by Theorem 3.17, $\bigcup\{\, E_{S_i}(t_i{:}S_i, t'_i{:}S_i\,\} \subseteq T$. 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.

4. Applications

Many of the the *HEL*'s encountered in practice are equivalential, and in these cases Theorem 3.20 seems to be a useful way of verifying a conditional equation is behaviorally valid. The following two example illustrate this phenomenon.

Example 4.1. (**Flags**) We will use Theorem 3.20 to prove that $\mathit{rev}(F) \approx G$ if $\mathit{rev}(G) \approx F$ is behaviorally valid in $\mathcal{L}_{\mathit{Flag}}$.

It can be verified that $\mathcal{L}_{\mathit{Flag}}$ 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

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

(see (Martins 2001)). Using (ii) of Theorem 3.20, it is enough to prove that

$$\mathit{up?}(\mathit{rev}(G)) \approx \mathit{up?}(F) \vdash_{\mathcal{L}_{\mathit{Flag}}} \mathit{up?}(\mathit{rev}(F)) \approx \mathit{up?}(G). \tag{23}$$

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

$$\begin{array}{ll}
\mathit{up?}(\mathit{rev}(G)) \approx \mathit{up?}(F) & \\
\neg(\mathit{up?}(G)) \approx \mathit{up?}(F) & \text{(axiom and IR}_2\text{)}\\
\neg(\neg(\mathit{up?}(G))) \approx \neg(\mathit{up?}(F)) & \text{(inf. rule IR}_3\text{)}\\
\mathit{up?}(G) \approx \neg(\mathit{up?}(F)); & (\neg\neg x \approx x \text{ and IR}_2)\\
\mathit{up?}(G)) \approx \mathit{up?}(\mathit{rev}(F)) & \text{(axiom and IR}_2\text{)}
\end{array}$$

So, (23) is proved. Hence, $\mathit{rev}(G) \approx F \models^{\mathrm{beh}}_{\mathcal{L}_{\mathit{Flag}}} \mathit{rev}(F) \approx G$.

Example 4.2. (**Stacks**) It can be verified that $\mathcal{L}_{\mathit{Stacks}}$ is equivalential with equivalence system $E = \langle E_{\mathit{num}}, E_{\mathit{stak}}\rangle$ where $E_{\mathit{num}}(x{:}\mathit{num}, y{:}\mathit{num}) = \{x \approx y\}$ and
$E_{\mathit{stack}}(x{:}\mathit{stack}, y{:}\mathit{stack}) = \{\mathit{Top}(\mathit{Pop}^n(x)) \approx \mathit{Top}(\mathit{Pop}^n(y)) : n \geq 0\}$ (see (Martins 2001)).

It can be shown that, $S \approx \mathit{Push}(n, S') \models^{\mathrm{beh}}_{\mathcal{L}_{\mathit{Stacks}}} \mathit{Pop}(\mathit{Pop}(S)) \approx \mathit{Pop}(S')$.

For that, 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 2.12.

It is shown in (Martins 2001) that $\mathcal{L}_{Stacks}$ is not finitely equivalential, hence is not behaviorally specifiable. However, the above equivalence system is clearly RE (indeed recursive), equivalence 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.

References

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

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

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

Buss, Samuel and Roşu, Grigore, *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.

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

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

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

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

Hennicker, Rolf *Structural specifications with behavioural operators: semantics, proof methods and applications*, Ph.D. thesis, 1997.

Leavens, Gary and Pigozzi, Don, *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

Martins, Manuel António *Behavioral equivalence relation in hidden equational logics*, Manuscript, December 2001.

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

Pigozzi, Don, *Abstract algebraic logic and the specification of abstract data types*, Preprint, June 1999.

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

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

Roşu, Grigore and Goguen, Joseph, *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.

Roşu, Grigore and Goguen, Joseph, *Circular coinduction*, Circular Coinduction, International Joint Conference on Automated Reasoning (IJCAR'01), 2001.

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