Math. Struct. in Comp. Science (2007), *vol.* 17, *pp.* 1075–1113.
doi:10.1017/S0960129507006305 Printed in the United Kingdom

Behavioural reasoning for conditional equations†

MANUEL A. MARTINS‡ and DON PIGOZZI§

‡*Department of Mathematics, University of Aveiro, 3810-193 Aveiro, Portugal*
Email: martins@mat.ua.pt

§*Department of Mathematics, Iowa State University, Ames, IA 50011, U.S.A.*
Email: dpigozzi@iastate.edu

Received 23 April 2003; revised 12 April 2007; first published online 4 October 2007

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

1. Introduction

Equational logic serves as the underlying logic in many formal approaches to program specification. The algebraic data types specified in this formal way can be viewed as abstract machines on which the programs are to be run. This is one way of giving a precise algebraic semantics for programs, against which the correctness of a program can be tested. Object-oriented (OO) programs, however, present a special challenge for equational methods. A more appropriate model for the abstract machine in the case of an

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

OO program is, arguably, a state transition system: like a state of such a system, a state of an OO program can be viewed as encapsulating all pertinent information about the abstract machine when it reaches the state during execution of the program. As a way of meeting this challenge, the standard equality predicate can be augmented by *behavioural equivalence*; in this way many of the characteristic properties of state transition systems can be grafted onto equational logic.

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

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

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

Research in the area has generally focused on computationally effective coinductive and specialised rewriting techniques that can serve as the basis of special languages that support automated behavioural reasoning. Bouhoula and Rusinowitch (2002) proposed an automatic method for proving behavioural validity of conditional equations in conditional specifications based on the fact that there are specifications for which a small set of contexts, called *critical contexts*, is sufficient to determine behavioural validity. This is the genesis of the SPIKE language (Berreged *et al.* 1998), which uses context induction (see `http://www.loria.fr/bouhoula/spike.html`). The language

CafeOBJ was developed by Diaconescu and Futatsugi (Diaconescu and Futatsugi 1998) (see `http://www.ldl.jaist.ac.jp/Research /CafeOBJ/`). It implements behavioural rewriting to make behaviourally sound reductions of terms, and is based on a behavioural version of the well-known efficient method of rewriting for automated theorem proving.

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

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

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

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

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

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

1.1. *Outline of the paper*

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

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

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

Section 3 forms the core of the paper. We give precise definitions of behaviourally valid equations and conditional equations over a hidden k-logic and, as a special case, a HEL. In the main lemma of the paper (Theorem 3.4), behavioural validity is characterised in terms of combinatorial properties of Leibniz congruences on the term algebra; this characterisation can be viewed as the most abstract form of coinduction for conditional equations, and all subsequent results of the paper derive from it.

In Section 3.1 we prove that all members of a set of conditional equations E are behaviourally valid over a HEL if and only if every conditional equation with visible consequent that is derivable using E as a set of additional inference rules is already derivable without the aid of E (Theorem 3.10). This gives an alternative form of coinduction

https://doi.org/10.1017/S0960129507006305 Published online by Cambridge University Press

for conditional equations that uses only standard equational logic. It generalises in a natural way a similar result in Leavens and Pigozzi (2002, Theorem 3.18) for equations. As a consequence (Corollary 3.13), we get that the set of conditional equations that are behaviourally valid over a HEL is closed under equational consequence in the sense that any conditional equation that is derivable using any set of behaviourally valid conditional equations as additional rules is itself behaviourally valid. Thus coinduction (in either of the alternative forms mentioned above) remains sound as well as complete with respect to behavioural validity when augmented by the standard deductive apparatus of equational logic. This turns out to be especially useful in the case of behaviourally specifiable HELs (see following paragraph) for which there are just a few behaviourally valid equations and conditional equations that, once their behavioural validity is verified in some way, for example by coinduction, can be used to derive all other behavioural validities by means of standard equational logic. An example of the use of this technique for establishing the behavioural validity of equations can be found in Leavens and Pigozzi (2002).

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

If $\mathscr{L}$ 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 behaviourally valid if and only if each of its transforms is derivable in $\mathscr{L}$; in the case of a finite equivalence system, the set of transforms is finite and each is a standard conditional equation (Theorem 3.22). This result can be useful in practice since many HELs have equivalence systems and even finite equivalence systems.

2. Hidden logics

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

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

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

https://doi.org/10.1017/S0960129507006305 Published online by Cambridge University Press

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

We get from each hidden signature Σ the associated *un-hidden* signature Σ^{UH} by making all the sorts of Σ visible:

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

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

A Σ-*algebra* is a pair

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

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

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

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

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

We define, in the usual way, operations over $\mathrm{Te}_\Sigma(X)$ to obtain the *term algebra* over the signature Σ (also denoted by $\mathrm{Te}_\Sigma(X)$). It is well known that $\mathrm{Te}_\Sigma(X)$ has the *universal mapping property* over X in the sense that, for every Σ-algebra A and every sorted map $h : X \to A$, called an *assignment*, there is a unique sorted homomorphism $h^* : \mathrm{Te}_\Sigma(X) \to A$, which extends h. From now on we will not distinguish between these two maps. If φ is the term (1), and $a_i \in A_{T_i}$, we write $\varphi^A(a_1, \ldots, a_n)$ for the image $h(\varphi)$ under any homomorphism h such that $h(x_i) = a_i$ for all i.

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

To provide a context that allows us to deal simultaneously with specification logics that are assertional (for example, ones with a Boolean sort but no equality) and equational,

https://doi.org/10.1017/S0960129507006305 Published online by Cambridge University Press

we introduce the notion of a k-formula for any non-zero natural number k. A *k-formula* of sort S over Σ is a sequence of k Σ-terms all of the same sort S. We indicate k-formulas by overlining, for example, $\bar{\varphi}:S = \langle \varphi_0 :S, \ldots, \varphi_{k-1}:S\rangle$. When we do not need to make the common sort S of each term of $\bar{\varphi}:S$ explicit, we simply write it as $\bar{\varphi}$. Te_Σ^k is the sorted set of all k-formulas over Σ. Hence, $\mathrm{Te}_\Sigma^k = \langle (\mathrm{Te}_\Sigma)_S^k : S \in \mathrm{SORT}\rangle$. The set of all visible k-formulas $(\mathrm{Te}_\Sigma^k)_{\mathrm{VIS}}$ is the VIS-sorted set $\langle (\mathrm{Te}_\Sigma)_V^k : V \in \mathrm{VIS}\rangle$. More generally, for any subset $\mathscr{S}$ of sorts and any sorted set A, the $\mathscr{S}$-sorted set $\langle A_s : S \in \mathscr{S}\rangle$ is denoted by $A_{\mathscr{S}}$.

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

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

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

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

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

In the rest of the paper, we will normally omit the term 'visible' and simply say a k-data structure. An example of a 2-data structure is any model of the free hidden equational logic over Σ. The standard model of the free HEL_Σ is of the form $\langle A, \mathrm{id}_{A_{\mathrm{VIS}}}\rangle$, where A is a Σ-algebra and $\mathrm{id}_{A_{\mathrm{VIS}}}$ is the identity relation on the visible part of A, but one gets more general 2-data structures as models by taking any congruence relation on the visible part of A in place of $\mathrm{id}_{A_{\mathrm{VIS}}}$. By a *congruence relation on the visible part of* A, or simply a VIS-*congruence*, we mean a VIS-sorted set $\langle F_V : V \in \mathrm{VIS}\rangle$ such that, for every $V \in \mathrm{VIS}$, F_V is an equivalence relation on A_V, and for every term $\varphi(x_1 : V_1, \ldots, x_n : V_n) : V$, with $V_1, \ldots, V_n, V \in \mathrm{VIS}$, if $\langle a_i, b_i\rangle \in F_{V_i}$ for all $i \leqslant n$, then $\langle \varphi^A(a_1, \ldots, a_n), \varphi^A(b_1, \ldots, b_n)\rangle \in F_V$.

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

We can also consider the free Boolean logic over Σ, provided Σ has a Boolean sort. Here the standard models are the 1-data structures $\langle A, \{\mathit{true}\}\rangle$, 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 Boolean filter on A_{VIS}.

2.1. *Consequence*

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

(a) $\Gamma \vdash \bar{\gamma}$ for each $\bar{\gamma} \in \Gamma$;

(b) $\Gamma \vdash \bar{\varphi}$, and $\Delta \vdash \bar{\gamma}$ for each $\bar{\gamma} \in \Gamma$, imply $\Delta \vdash \bar{\varphi}$.

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

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

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

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

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

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

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

where $\bar{\varphi}_0, \ldots, \bar{\varphi}_n$ are all visible k-formulas. A visible k-formula $\bar{\psi}$ is *directly derivable* from a set Γ of visible k-formulas by a rule such as (2) if there is a substitution $h : X \to \mathrm{Te}_\Sigma$ such that $h(\bar{\varphi}_n) = \bar{\psi}$ and $h(\bar{\varphi}_0), \ldots, h(\bar{\varphi}_{n-1}) \in \Gamma$. $\bar{\psi}$ is *derivable* from Γ by a given set of axioms and rules of inference if there is a finite sequence of k-formulas $\bar{\psi}_0, \ldots, \bar{\psi}_{n-1}$ such

https://doi.org/10.1017/S0960129507006305 Published online by Cambridge University Press

that $\bar{\psi}_{n-1} = \bar{\psi}$, and for each $i < n$ either:

(a) $\bar{\psi}_i \in \Gamma$, or (b) $\bar{\psi}_i$ is a substitution instance of an axiom; or
(c) $\bar{\psi}_i$ is directly derivable from $\{\bar{\psi}_j : j < i\}$ by one of the rules of inference.

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

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

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

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

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

2.2. *Semantics*

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

(i) A visible k-formula $\bar{\varphi} : V$ is said to be a *valid consequence* of a set of visible k-formulas Γ in K, in symbols $\Gamma \vDash_K \bar{\varphi}$, if
$$(\forall\ \langle A, F \rangle \in K)(\forall\ h : X \to A)\big[\big((\forall\ \bar{\psi} : W \in \Gamma)\,(h(\bar{\psi}) \in F_W)\big) \Rightarrow h(\bar{\varphi}) \in F_V\big].$$
(ii) A visible k-formula $\bar{\varphi}$ is *valid* in K if $h(\bar{\varphi}) \in F_V$ for every $\langle A, F \rangle \in K$ and every assignment $h : X \to A$, that is, if it is a valid consequence, in K, of the empty set of k-formulas, in symbols $\vDash_K \bar{\varphi}$.
(iii) A rule like (2) is a *valid rule* of K, if $\{\bar{\varphi}_0, \dots, \bar{\varphi}_{n-1}\} \vDash_K \bar{\varphi}_n$.

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

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

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

https://doi.org/10.1017/S0960129507006305 Published online by Cambridge University Press

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

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

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

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

that is, for every set of k-formulas Γ and any k-formula $\bar{\varphi}$, $\Gamma \vdash_{\mathscr{L}} \bar{\varphi}$ if and only if $\Gamma \models_{\mathrm{Mod}(\mathscr{L})} \bar{\varphi}$.

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

2.3. *Hidden equational logic*

In the present context, hidden equational logic is a special class of 2-logics in which a 2-formula $\langle t, s\rangle$ is intended to represent an equation, which we denote by $t \approx s$, and a rule

$$\frac{\langle t_0, s_0\rangle, \ldots, \langle t_{n-1}, s_{n-1}\rangle}{\langle t_n, s_n\rangle}$$

represents a conditional equation, denoted by

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

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

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

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

Axioms:

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

Inference rules:

For each $V, W \in \mathrm{VIS}$:

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

https://doi.org/10.1017/S0960129507006305 Published online by Cambridge University Press

(IR$_2$) $x:V \approx y:V, y:V \approx z:V \to x:V \approx z:V$,

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

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

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

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

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

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

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

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

is a valid rule of a model $\mathscr{A} = \langle A, F \rangle$ of the free HEL$_\Sigma$ (free UHEL$_\Sigma$) if, for every assignment $\bar{a}$ of the elements of A to $\bar{x}$ (of the appropriate sorts),

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

The applied unhidden equational logics we deal with are, on the contrary, normally unspecifiable since they come from the behavioural equivalence of hidden equational logics and more general hidden k-logics.

We give several examples of specifiable hidden logics. We have deliberately chosen simple, well-known ones that allow us to illustrate the basic ideas without burdening the reader with irrelevant detail. The first two illustrate how the logic of a particular data structure can be alternatively formalised as a Boolean 1-logic or as an equational 2-logic,

https://doi.org/10.1017/S0960129507006305 Published online by Cambridge University Press

a HEL. The flag logics provide two different ways of specifying semaphores, which are commonly used in scheduling resources (Goguen and Malcolm 1999).

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

SORT $= \{flag, bool\}$, with *bool* the unique visible sort and the 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 $\neg, \wedge, \vee, true, false$ for the Boolean part.

The Boolean biconditonal $\varphi \leftrightarrow \psi$ is an abbreviation for the compound operation $(\neg\varphi \vee \psi) \wedge (\neg\psi \vee \varphi)$.

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

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

together with the usual logical axioms for the classical propositional logic. There are no extra-logical rules of inference.

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

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

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

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

As expected, $\mathscr{L}_{bflag}$ and $\mathscr{L}_{eflag}$ are equivalent. To be precise,

$$\frac{\varphi_1 \leftrightarrow \varphi_1', \ldots, \varphi_n \leftrightarrow \varphi_n'}{\psi \leftrightarrow \psi'}$$

is a derivable rule of $\mathscr{L}_{bflag}$ if and only if

$$\frac{\varphi_1 \approx \varphi_1', \ldots, \varphi_n \approx \varphi_n'}{\psi \approx \psi'}$$

is a derivable rule of $\mathscr{L}_{eflag}$.

Example 2.9 (Stacks of Natural Numbers as a HEL). As in the standard specification of the logic of stacks, only the natural numbers are visible. Consequently, the axioms and rules of inference can only reference the 'numerical behaviour' of stacks rather than the stacks themselves. In particular, there can be no axiom or rule involving equality between stacks. Because of this, we get an infinite number of axioms, where in the standard formalisations, where assertions about the equality of stacks are allowed, the axiomatisation is finite and, on the face of it, conceptually simpler. We will have more to say about this later.

https://doi.org/10.1017/S0960129507006305 Published online by Cambridge University Press

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

Consider the hidden signature Σ_{stacks}:

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

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

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

Extra-logical axioms:

$$\begin{array}{l} top(pop^n(empty)) \approx zero, \text{ for all } n \\ top(push(x,y)) \approx x \\ top(pop^{n+1}(push(x,y))) \approx top(pop^n(y)), \text{ for all } n\,. \end{array}$$

Extra-logical inference rule:

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

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

Consider the hidden signature Σ_{sets}:

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

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

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

The extra-logical axioms are the axioms of the Boolean algebra together with

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

and the extra-logical inference rule is

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

https://doi.org/10.1017/S0960129507006305 Published online by Cambridge University Press

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

The operations are

$$\begin{aligned} &lub, glb : num, num \to num \\ &ub, lb : set \to num \\ &elt\text{-}of : set \to num \\ &\cup, \& : set, set \to set\,. \end{aligned}$$

The axioms are

$$\begin{aligned} &\langle x, x, x\rangle \\ &\langle glb(x, y),\ x,\ lub(x, y)\rangle \\ &\langle glb(x, y),\ y,\ lub(x, y)\rangle \\ &\langle lb(s),\ elt\text{-}of(s),\ ub(s)\rangle \\ &\langle glb(lb(s),\ lb(t)),\ elt\text{-}of(\cup(s, t)),\ lub(up(s),\ ub(t)\rangle \\ &\langle lub(lb(s),\ lb(t)),\ elt\text{-}of(\&(s, t)),\ glb(up(s),\ ub(t)\rangle\,. \end{aligned}$$

The rules of inference are

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

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

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

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

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

2.4. *Behavioural equivalence*

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

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

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

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

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

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

Variants of this notion of behavioural equivalence can be found in the literature. For example, Goguen and Malcolm (Goguen and Malcolm 2000) restrict the set of contexts to those built from a predefined set of observational operational symbols – see the Conclusion section (Section 4) for more details.

To generalise the notion of behavioural equivalence so that it applies to hidden k-logics, we first generalise the notion of context. A (k, S)-*context* over a hidden signature Σ is a k-term

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

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

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

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

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

2.5. *Leibniz congruence*

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

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

$$\text{if } a_i \equiv a_i'(\Theta_V) \text{ for all } i \leqslant k \text{ then, } \bar{a} \in F_V \text{ if and only if } \bar{a}' \in F_V\,.$$

That is, each F_V is the union of a cartesian product of Θ_V-classes, that is,

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

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

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

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

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

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

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

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

Theorem 2.16. Let Σ be a hidden signature and $\mathscr{A} = \langle A, F\rangle$ be a k-data structure over Σ. Then, $\equiv^{\text{beh}}_{\mathscr{A}} = \Omega_A(F)$, that is, for every $S \in \text{SORT}$ and for all $a, a' \in A_S$, $a \equiv^{\text{beh}}_{\mathscr{A}} a'$ if and only if $a \equiv a' \,(\Omega_A(F)_S)$.

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

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

Consider any $i \leqslant n$. Using the assumption $a_i \equiv^{\text{beh}}_{\mathscr{A}} a'_i$, and taking x_i as the designated variable, $x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n, u_1, \ldots, u_n$ as parametric variables, and $a_1, \ldots, a_{i-1}$, $a'_{i+1}, \ldots, a'_n, b_1, \ldots, b_m$ as parameters, we have

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

Since this equivalence holds for all $i \leqslant n$, (7) holds, so $\equiv^{\text{beh}}_{\mathscr{A}}$ is a congruence on A.

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

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

So $\bar{a} \in F_V$ if and only if $\bar{a}' \in F_V$. Thus $\equiv^{\text{beh}}_{\mathscr{A}}$ is compatible with F.

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

So $\equiv^{\text{beh}}_{\mathscr{A}}$ is a congruence relation on the whole algebra A, and hence for any k-data structure $\mathscr{A}$ over the hidden signature Σ, the associated 2-data structure $\langle A, \equiv^{\text{beh}}_{\mathscr{A}}\rangle$ is a model of the free UHEL_Σ.

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

Definition 2.17.

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

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

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

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

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

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

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

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

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

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

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

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

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

https://doi.org/10.1017/S0960129507006305 Published online by Cambridge University Press

Proof. Let $\langle A, F\rangle$ be a k-data structure and $h : A \to A/\Omega_A(F)$ be the natural homomorphism, and note that $\Omega_A(F)$ is the kernel of h. By Lemma 2.18,

$$h^{-1}\big(\Omega_{A/\Omega_A(F)}(F/\Omega_A(F))\big) = \Omega_A\big(h^{-1}(F/\Omega_A(F))\big) = \Omega_A(F).$$

So $\Omega\big(F/\Omega_A(F)\big)$ is the identity congruence on $A/\Omega_A(F)$. □

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

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

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

Theorem 2.21. Let $\mathscr{A} = \langle A, F\rangle$ and $\mathscr{B} = \langle B, G\rangle$ be two k-data structures. If $\mathscr{A} \succcurlyeq \mathscr{B}$, then $\vDash_{\mathscr{A}} = \vDash_{\mathscr{B}}$, that is, for any set $\Gamma \cup \{\bar\varphi\}$ of visible k-formulas, we have $\Gamma \vDash_{\mathscr{A}} \bar\varphi$ if and only if $\Gamma \vDash_{\mathscr{B}} \bar\varphi$.

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

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

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

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

As h is surjective, $h(\bar a)$ ranges over all $\bar b \in B_{\bar S}$ as $\bar a$ ranges over all of $A_{\bar S}$. Thus $\Gamma \vDash_{\mathscr{A}} \bar\varphi$ if and only if $\Gamma \vDash_{\mathscr{B}} \bar\varphi$. □

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

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

$$\vdash_{\mathscr{L}} \;=\; \vDash_{\mathrm{Mod}^*(\mathscr{L})}.$$

That is, for every set of k-formulas Γ and any k-formula $\bar\varphi$, $\Gamma \vdash_{\mathscr{L}} \bar\varphi$ if and only if $\Gamma \vDash_{\mathrm{Mod}^*(\mathscr{L})} \bar\varphi$.

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

Let $h : A \to A^*$ be the natural homomorphism. We must show $h^{-1}(F^*) = F$, so suppose $\bar a \in A$ and $h(\bar a) \in F^* = F/\Omega_A(F)$. This means that $\bar a \equiv \bar a'\ (\Omega_A(F)^k)$ for some $\bar a' \in F$. Thus, since $\Omega_A(F)$ is compatible with F, we have $\bar a \in F$. □

https://doi.org/10.1017/S0960129507006305 Published online by Cambridge University Press

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

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

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

Proof. By Theorem 2.16, $a \equiv_{\Omega(F)_S} a'$ if and only if, for every (2,S)-context

$$\langle \varphi(z\!:\!S,\, \bar{u}\!:\!\bar{Q}), \psi(z\!:\!S, \bar{u}\!:\!\bar{Q})\rangle$$

of sort V and every $\bar{b} \in A_{\bar{Q}}$, we have

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

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

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

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

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

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

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

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

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

https://doi.org/10.1017/S0960129507006305 Published online by Cambridge University Press

Θ is any other congruence on A such that $\Theta_{\mathrm{VIS}} = F$, then Θ is compatible with F, and thus $\Theta \subseteq \Omega_A(F)$. □

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

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

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

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

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

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

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

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

3. Behavioural reasoning

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

The behavioural validity for equations and conditional equations was introduced by Reichel in 1984 (Reichel 1985). These notions and their proof theory have been studied by a number of researchers: Goguen, Malcolm and Roşu (Goguen and Malcolm 1999; Goguen and Malcolm 2000; Roşu and Goguen 2000; Roşu 2000; Roşu and Goguen 2001);

https://doi.org/10.1017/S0960129507006305 Published online by Cambridge University Press

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

Our particular characterisation of behavioural validity of a conditional equation is given in Theorem 3.4. The use of unhidden equational logic in verifying behavioural validity of conditional equations is addressed in Theorem 3.10. As a corollary, we get that the set of all behaviourally valid conditional equations is closed under unhidden equational deduction (Corollary 3.13).

In the final part of the section we consider the important problem of determining when a HEL $\mathscr{L}$ has specifiable behaviour, that is, when there exists a set of axioms and rules in the form of equations and conditional equations, respectively, such that an equation $t \approx s$ (of arbitrary sort) is a behaviourally valid consequence of a set E of equations if and only if $t \approx s$ is derivable from E in standard equational using the given axioms and rules. Several characterisations of this property are obtained. Possibly the most interesting deals with the notion of a *cobasis*. This concept, which was introduced in Roşu and Goguen (2001), has served as the principal method of partially verifying the behavioural validity of hidden equations in a large class of HELs. We show that the behaviour of a HEL is specifiable only when it has a cobasis of a very special kind (Theorem 3.20).

The definition of a behaviourally specifiable HEL is given in Definition 3.14. In Theorem 3.19 those HELs that are behaviourally specifiable are characterised in terms of the consequence of the HEL. As a consequence, in Theorem 3.22 we obtain for behaviourally specifiable HELs a characterisation of behaviourally valid conditional equations.

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

(i) An equation $t \approx t'$ of arbitrary sort is said to be a *behaviourally valid consequence* of a set E of equations (of arbitrary sorts) over K, in symbols $E \vDash_K^{\mathrm{beh}} t \approx t'$, if, for every $\mathscr{A} \in K$ and every assignment $h : X \to A$, we have $h(t) \equiv_{\mathscr{A}}^{\mathrm{beh}} h(t')$ whenever $h(s) \equiv_{\mathscr{A}}^{\mathrm{beh}} h(s')$ for every equation $s \approx s'$ in E.

(ii) An equation $t \approx t'$ is *behaviourally valid* over K if $\vDash_K^{\mathrm{beh}} t \approx t'$, and a conditional equation $t_0 \approx t_0', \dots, t_{n-1} \approx t_{n-1}' \to t_n \approx t_n'$ is *behaviourally valid* over K if $\{t_0 \approx t_0', \dots, t_{n-1} \approx t_{n-1}'\} \vDash_K^{\mathrm{beh}} t_n \approx t_n'$.

We write $\vDash_{\mathscr{A}}^{\mathrm{beh}}$ for $\vDash_{\{\mathscr{A}\}}^{\mathrm{beh}}$.

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

https://doi.org/10.1017/S0960129507006305 Published online by Cambridge University Press

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

(i) An equation $t \approx t'$ is said to be a *behaviourally valid consequence* of a set E of equations over $\mathscr{L}$, in symbols $E \models^{\mathrm{beh}}_{\mathscr{L}} t \approx t'$, if $E \models^{\mathrm{beh}}_{\mathrm{Mod}(\mathscr{L})} t \approx t'$.

(ii) An equation or conditional equation is *behaviourally valid over* $\mathscr{L}$ if it is behaviourally valid over $\mathrm{Mod}(\mathscr{L})$.

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

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

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

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

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

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

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

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

https://doi.org/10.1017/S0960129507006305 Published online by Cambridge University Press

The following theorem may be viewed of as a form of coinduction for conditional equations. It gives a characterisation, in terms of combinatorial properties of Leibniz congruences on the term algebra, for a conditional equation to be behaviourally valid in a given hidden k-logic. It should be compared with the coinduction rule in Roşu and Goguen (2000) for verifying the behavioural validity of equations in HELs.

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

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

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

(ii) A conditional equation

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

is behaviourally valid over $\mathscr{L}$ if and only if

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

Proof.

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

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

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

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

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

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

This result takes a simpler form when it is applied to hidden equational logic, but this requires the notion of an extension of a k-logic by additional axioms and rules of inference.

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

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

— $\Theta \cap (\mathrm{Te}_\Sigma^2)_{\mathrm{VIS}} \in \mathrm{Th}(\mathscr{L})$.
— Θ is closed under the equations and conditional equations of E in the following sense. For every equation $t \approx t' \in E$ and substitution $\sigma : X \to \mathrm{Te}_\Sigma$, $\sigma(t) \approx \sigma(t') \in \Theta$, and for every conditional equation $t_0 \approx t'_0, \dots, t_{n-1} \approx t'_{n-1} \to t_n \approx t'_n$ in E and every $\sigma : X \to \mathrm{Te}_\Sigma$, if $h(t_i) \approx \sigma(t'_i) \in \Theta$ for all $i < n$, then $\sigma(t_n) \approx \sigma(t'_n) \in \Theta$.

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

For each theory T of $\mathscr{L}$ we have $\Omega(T) \cap (\mathrm{Te}_\Sigma^2)_{\mathrm{VIS}} = T$ by Corollary 2.24. Thus $\Omega(T) \in \mathrm{Th}(\mathscr{L}^{\mathrm{UH}})$. More generally, it follows easily from Corollary 2.24 that, if $\langle A, F \rangle \in \mathrm{Mod}(\mathscr{L})$, then $\langle A, \Omega(F) \rangle \in \mathrm{Mod}(\mathscr{L}^{\mathrm{UH}})$.

Corollary 3.6. Let $\mathscr{L}$ be a HEL and E be a set of equations and conditional equations of arbitrary type. Then every equation and conditional equation in E is behaviourally valid over $\mathscr{L}$ if and only if for every $T \in \mathrm{Th}(\mathscr{L})$, $\Omega(T) \in \mathrm{Th}(\mathscr{L}^{\mathrm{UH}}[E])$.

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

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 $\Omega(T)$ is closed under ξ for every $\xi \in E$, and hence $\Omega(T) \in \mathrm{Th}(\mathscr{L}^{\mathrm{UH}}[E])$.

For the implication in the other direction, assume $\Omega(T) \in \mathrm{Th}(\mathscr{L}^{\mathrm{UH}}[E])$ for each $T \in \mathrm{Th}(\mathscr{L})$. Let $T \in \mathrm{Th}(\mathscr{L})$ and ξ be a conditional equation in E of the form (12). Suppose that for all $i < n$, we have $t_i \equiv t_i' \left(\Omega(T)\right)$. Then $t_n \equiv t_n' \left(\Omega(T)\right)$ since $\Omega(T) \in \mathrm{Th}\left(\mathscr{L}^{\mathrm{UH}}[E]\right)$ by assumption. So ξ is behaviourally valid over $\mathscr{L}$ by Theorem 3.4. □

As a special case of this result, we have that an equation $t \approx t'$ is behaviourally valid over $\mathscr{L}$ if and only if $t \equiv t' \left(\Omega(\mathrm{Thm}(\mathscr{L})\right)$.

In the following corollaries we give two simpler characterisations for conditional equations of a special kind to be behaviourally valid in a HEL $\mathscr{L}$; in the first case the antecedents are all visible and in the second it is the consequent that is visible.

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

Corollary 3.7. Let $\mathscr{L}$ be a HEL. A conditional equation (12) with visible antecedents is behaviourally valid over $\mathscr{L}$ if and only if $t_n \equiv t_n' \left(\Omega(\mathrm{Cn}_{\mathscr{L}}\{\, t_i \approx t_i' : i < n\,\})\right)$.

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

$$t_n \equiv t_n' \left(\Omega(\mathrm{Thm}(\mathscr{L}[\{\, t_i \approx t_i' : i < n\,\}]))\right). \tag{13}$$

For this it is enough to note that $\mathrm{Cn}_{\mathscr{L}}\{\, t_i \approx t_i' : i \leqslant n\}$ is the set of all theorems of the HEL $\mathscr{L}[\{\, t_i \approx t_i' : i < n\,\}]$. This result can be found in Roşu (2000), where it is called the *Deduction Theorem.*

If the consequent $t_n \approx t_n'$ of the conditional equation (12) is visible, then the characterisation of behavioural validity given in Theorem 3.4 can be simplified as follows.

Corollary 3.8. Let $\mathscr{L}$ be a HEL. A conditional equation (12) with a visible consequent is behaviourally valid over $\mathscr{L}$ if and only if

$$t_n \equiv t_n' \left(\mathrm{Cn}_{\mathscr{L}}(\textstyle\bigcup_{i<n}\{\, \varphi(t_i, \bar{x}) \approx \varphi(t_i', \bar{x}) : \varphi \text{ an appropriate context for } t_i, t_i' \,\})\right).$$

Proof. Let

$$G = \mathrm{Cn}_{\mathscr{L}}(\textstyle\bigcup_{i<n}\{\, \varphi(t_i, \bar{x}) \approx \varphi(t_i', \bar{x}) : \varphi \text{ an appropriate context for } t_i, t_i' \,\}).$$

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

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

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

Assume now that (12) is behaviourally valid over $\mathscr{L}$. $G \in \mathrm{Th}(\mathscr{L})$ and, by definition of G, $t_i \equiv t_i' (\Omega(G))$. Hence, by Theorem 3.4, we get that $t_n \equiv t_n' (\Omega(G))$. Thus $t_n \equiv t_n' (G)$ since t_n, t_n' are visible. □

https://doi.org/10.1017/S0960129507006305 Published online by Cambridge University Press

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

Corollary 3.9. Let $\mathscr{L}$ be a HEL$_\Sigma$ and ξ be a conditional equation (of arbitrary sort) that is behaviourally valid over $\mathscr{L}$. Then for every Σ-equation $s \approx s'$ (of arbitrary sort), $\vdash_{\mathscr{L}^{\text{UH}}[\xi]} s \approx s'$ implies that $s \approx s'$ is behaviourally valid over $\mathscr{L}$.

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

3.1. *Closure of behavioural validity under equational consequence*

Intuitively, since the terms of a behaviourally 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 has been shown (Leavens and Pigozzi 2002, Theorem 3.18) that, not only is this indeed the case, but the property serves to actually characterise behaviourally valid equations. In the next theorem this result is generalised in a natural way to conditional equations. This gives another characterisation of the conditional equations that are behaviourally 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 $\mathscr{L}$ be a HEL, and let E be a set of (unrestricted) conditional equations. Then every rule in E is behaviourally valid over $\mathscr{L}$ if and only if every conditional equation with visible consequent that is a derivable rule of $\mathscr{L}^{\text{UH}}[E]$ is already a derivable rule of $\mathscr{L}^{\text{UH}}$, that is, for every conditional equation $s_0 \approx s'_0, \dots, s_{m-1} \approx s'_{m-1} \to s_m \approx s'_m$ with a visible consequent,

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

Proof. Assume that each rule in E is behaviourally valid over $\mathscr{L}$. Assume also that

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

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

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

$$\Omega\left(\text{Th}(\mathscr{L})\right) \subseteq \text{Th}(\mathscr{L}^{\text{UH}}[E]). \tag{17}$$

https://doi.org/10.1017/S0960129507006305 Published online by Cambridge University Press

Suppose $T \in \mathrm{Th}(\mathscr{L})$ and let $G = \mathrm{Cn}_{\mathscr{L}^{\mathrm{UH}}[E]}\big(\Omega(T)\big)$, the $\mathscr{L}^{\mathrm{UH}}[E]$-theory generated by $\Omega(T)$. We claim that $G_{\mathrm{VIS}} = T$. To see the inclusion from left to right, assume s, s' are visible terms such that $s \equiv s'\,(G)$. Since G is generated as a $\mathscr{L}^{\mathrm{UH}}[E]$-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 $\{s_0 \approx s_0', \dots, s_{m-1} \approx s_{m-1}'\} \vdash_{\mathscr{L}^{\mathrm{UH}}[E]} s \approx s'$. Thus, by assumption, $\{s_0 \approx s_0', \dots, s_{m-1} \approx s_{m-1}'\} \vdash_{\mathscr{L}^{\mathrm{UH}}} s \approx s'$. Hence $s \equiv s'\,\big(\Omega(T)\big)$, since $\Omega(T)$ is an $\mathscr{L}^{\mathrm{UH}}$-theory, as previously observed. But $s \approx s'$ is visible, so $s \equiv s'\,(T)$. Thus $G_{\mathrm{VIS}} \subseteq T$. Since the opposite inclusion is obvious, we have verified the claim. Then $\Omega(T) = \Omega(G_{\mathrm{VIS}}) \supseteq G$; but obviously $\Omega(T) \subseteq G$. So $\Omega(T) = G \in \mathrm{Th}\big(\mathscr{L}^{\mathrm{UH}}[E]\big)$. Hence (17) holds and thus every rule in E is behaviourally valid over $\mathscr{L}$ by Corollary 3.6. □

Considering the analogous characterisation of behavioural validity of equations (see Leavens and Pigozzi (2002)), one might expect to be able to characterise the behavioural equivalence of the set E of conditional equations by the condition that any completely visible conditional equation that is a derivable rule of $\mathscr{L}^{\mathrm{UH}}[E]$ is already a derivable rule of $\mathscr{L}^{\mathrm{UH}}$, that is, by the weaker version of (15) 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 condition (15) in its full strength is necessary.

Consider the Flags example and the conditional equation

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

3.2. *The specification of behavioural validity*

Recall that a k-logic is behaviourally specifiable if its behavioural consequence relation can be axiomatised in standard equational logic by a possibly infinite set of equations and conditional equations. We present several characterisations of the behavioural specifiability of HELs in this subsection, one of which (the existence of a *finite equivalence system*) can be useful in practice. The behavioural specification problem for arbitrary k-logics is more complicated and will not be treated here; see Martins (2004).

Definition 3.14. Let $\mathscr{L}$ be a k-logic. We say that $\mathscr{L}$ is *behaviourally specifiable* if there is a specifiable UHEL $\mathscr{L}'$, over the same signature, such that $\vDash_{\mathscr{L}}^{\text{beh}} = \vdash_{\mathscr{L}'}$, that is, for

https://doi.org/10.1017/S0960129507006305 Published online by Cambridge University Press

every set of equations $E \cup \{t \approx t'\}$ (of arbitrary sort) we have $E \vDash^{\text{beh}}_{\mathscr{L}} t \approx t'$ if and only if $E \vdash_{\mathscr{L}'} t \approx t'$. We call $\mathscr{L}'$ a *behavioural specification* of $\mathscr{L}$.

The theory of behavioural specifiability is much simpler when it is restricted to hidden equational logic, and that is what we shall do in this subsection, with only an occasional reference to general k-logics.

If a HEL $\mathscr{L}$ is behaviourally specifiable, it must be specifiable in the standard sense, that is, its consequence relation $\vdash_{\mathscr{L}}$ is finitary in the sense that $E \vdash_{\mathscr{L}} t \approx s$ implies $E' \vdash_{\mathscr{L}} t \approx s$ for some finite subset E' of E. To see this, let $\mathscr{L}$ be a behavioural specification of $\mathscr{L}$. Then, since the equations are all visible, $E \vdash_{\mathscr{L}} t \approx s$ if and only if $E \vDash^{\text{beh}}_{\mathscr{L}} t \approx s$ if and only if $E \vdash_{\mathscr{L}'} t \approx s$ if and only if for a finite $E' \subseteq E$ such that $E \vdash_{\mathscr{L}'} t \approx s$ if and only if $E' \vdash_{\mathscr{L}} t \approx s$.

Theorem 3.15. Let $\mathscr{L}$ be a HEL. A UHEL $\mathscr{L}'$ over the same signature is a behavioural specification of $\mathscr{L}$ if and only if $\Omega\big(\text{Th}(\mathscr{L})\big) = \text{Th}(\mathscr{L}')$.

In order to prove this theorem, it is useful to first establish some properties of Ω as an abstract mapping from the set of theories of $\mathscr{L}$ into the set of congruences of the term algebra Te_Σ.

— Ω *is monotonic*, that is, if $T, G \in \text{Th}(\mathscr{L})$ and $T \subseteq G$, then $\Omega(T) \subseteq \Omega(G)$.

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

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

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

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

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

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

https://doi.org/10.1017/S0960129507006305 Published online by Cambridge University Press

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

1 If $S_n \notin \mathrm{VIS}$, then

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

2 If $S_n \in \mathrm{VIS}$, then

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

For technical reasons it is sometimes convenient 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 $\mathscr{L}$ has an equivalence system, it is said to be *equivalential*. Moreover, if E is locally globally finite (that is, $\bigcup_{V\in\mathrm{VIS}} E_{V,H}$ is finite for each $H \in \mathrm{HID}$), then $\mathscr{L}$ is said to be *finitely equivalential*.

Not every HEL is equivalential, a counter-example can be found in Martins (2004); this reference also has details of the following two examples.

Example 3.18.

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

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

II - Stacks. The specification of stacks $\mathscr{L}_{stacks}$ is equivalential with equivalence system

$$E = \langle E_{nat}, E_{stack}\rangle$$

where

$$E_{nat}(x{:}nat, y{:}nat) = \{x \approx y\}$$

and

$$E_{stack}(x{:}stack, y{:}stack) = \{top(pop^n(x)) \approx top(pop^n(y)) : n \geqslant 0\}\,.$$

However, $\mathscr{L}_{stacks}$ is not finitely equivalential.

Note that neither of these equivalence systems contains a parametric variable. This is not an uncommon situation. If a HEL is (finitely) equivalential, then it has a (finite)

https://doi.org/10.1017/S0960129507006305 Published online by Cambridge University Press

equivalence system without parametric parameters, provided its signature has the property that every sort contains a ground term. This is because any (finite) equivalence system with parameters can be converted into one without parameters by replacing each parametric variable by an arbitrary ground term of the same sort.

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

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

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

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

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

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

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

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

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

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

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

Note that in the course of the proof it has been shown that, as a consequence of Theorem 3.4, the theorem can also be expressed as follows:

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

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

We are now finally ready to give the promised characterisation of behaviourally specifiable HELs.

https://doi.org/10.1017/S0960129507006305 Published online by Cambridge University Press

Theorem 3.20. A specifiable HEL $\mathscr{L}$ is behaviourally specifiable if and only if it is finitely equivalential.

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

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

where $E_H(x:H, y:H, \bar{u}:\bar{Q}) = \{\varphi_1(x,\bar{u}) \approx \varphi_1(y,\bar{u}), \dots, \varphi_n(x,\bar{u}) \approx \varphi_n(y,\bar{u})\}$, and x, y are variables of sort H distinct from all the variables in $\bar{u}$. To see that $\mathscr{L}$ is a behavioural specification of $\mathscr{L}$, it suffices by Theorem 3.15 to show that

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

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

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

Therefore, $\mathscr{L}'$ is the behavioural specification of $\mathscr{L}$.

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

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

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

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

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

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

https://doi.org/10.1017/S0960129507006305 Published online by Cambridge University Press

Then

$$\{\varphi_i(x:H,\,\bar{u}:\bar{Q}) \approx \varphi_i(y:H,\,\bar{u}:\bar{Q}) : i \leqslant m\}$$
$$\vdash_{\mathscr{L}} \psi(x:H,\bar{\vartheta}:\bar{R}) \approx \psi(y:H,\bar{\vartheta}:\bar{R}) \quad \text{for every } \psi \in C_H \text{ and } \bar{\vartheta} \in (\mathrm{Te}_\Sigma)_{\bar{R}}. \quad (27)$$

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

$$\{\varphi_i(t:H,\,\bar{u}:\bar{Q}) \approx \varphi_i(t':H,\,\bar{u}:\bar{Q}) : i \leqslant m\}$$
$$\vdash_{\mathscr{L}} \psi(t:H,\bar{\vartheta}:\bar{R}) \approx \psi(t':H,\bar{\vartheta}:\bar{R}) \quad \text{for every } \psi \in C_H \text{ and } \bar{\vartheta} \in (\mathrm{Te}_\Sigma)_{\bar{R}}. \quad (28)$$

Let

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

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

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

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

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

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

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

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

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

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

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

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

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

(i) The conditional equation

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

is behaviourally valid over $\mathscr{L}$.

https://doi.org/10.1017/S0960129507006305 Published online by Cambridge University Press

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

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

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

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

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

Proof.

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

(ii) $\Rightarrow$ (i) Let $T \in \mathrm{Th}(\mathscr{L})$. Suppose that $t_i \equiv t'_i(\Omega(T))$ for each $i < n$. Then, by Theorem 3.19, $\bigcup\{ E_{S_i}(t_i : S_i, t'_i : S_i \} \subseteq T$. Hence, by (ii), $E_{S_n}(t_n : S_n, t'_n : S_n) \subseteq T$, and thus $t_n \equiv t'_n(\Omega(T))$.

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

It follows easily from this theorem that if a HEL $\mathscr{L}$ is equivalential and some equivalence system for it is RE, in particular, if $\mathscr{L}$ is finitely equivalential, then the set of conditional equations that are behaviourally valid over $\mathscr{L}$ 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 $\mathscr{L}$ is recursive.

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

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

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

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

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

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

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

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

https://doi.org/10.1017/S0960129507006305 Published online by Cambridge University Press

it is enough to prove that

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

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

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

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

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

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

4. Conclusion

In this paper we have presented a generalisation of the theory of behavioural equivalence in abstract algebraic logic that encompasses multi-sorted signatures and the 'visible–hidden' dichotomy. This establishes a new bridge between AAL and the specification and verification theory of programs that provides an efficient way of applying the powerful machinery of abstract algebraic logic to the behavioural specification domain. In particular, we have specialised to the study of HELs. Our method is novel in that it relies almost exclusively on combinatorial properties of the theories over an arbitrary HEL and their Leibniz congruences.

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

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

Generalisations of the notion of behavioural equivalence have been considered in the literature. Some authors require that each context contains only one occurrence of the distinguished variable z; however, they generate exactly the same behavioural equivalence relation. Another generalisation is due to Goguen *et al.*, who consider Γ-*behavioural equivalence*, with Γ a subset of the set of all operation symbols in the signature. A Γ-congruence is a relation compatible with all interpretations of the operation symbols in Γ. The Γ-behavioural equivalence is defined analogously to ordinary behavioural equivalence; it is also the largest Γ-congruence with the identity as the visible part. It is easy to extend our approach to accommodate Γ-behavioural equivalence. In fact, one needs only to change the definition of hidden equational logic by considering; precisely in the inference rule (IR_3) of Definition 2.6, the term t ranging among the ones generated using the operations symbols in Γ. Clearly, the notions of Leibniz congruence $\Omega(F)$ and the equivalence system have to be redefined to develop a parallel theory to ours. Some interesting questions arise in this context, such as the study of the compatibility of some operation symbols outside of Γ with respect to Γ-behavioural equivalence. This problem has been studied in Diaconescu and Futatsugi (2000) and Bidoit and Hennicker (1999).

References

Berreged, N., Bouhoula, A. and Rusinowitch, M. (1998) Observational proofs with critical contexts. In: Fundamental Approaches to Software Engineering. *Springer-Verlag Lecture Notes in Computer Science* **1382** 38–53.

Bidoit, M. and Hennicker, R. (1994) Proving behavioural theorems with standard first-order logic. In: Levi, G. *et al.* (eds.) Proceedings: Algebraic and logic programming. 4th international conference, ALP '94. *Springer-Verlag Lecture Notes in Computer Science* **850** 41–58.

Bidoit, M. and Hennicker, R. (1996) Behavioural theories and the proof of behavioural properties. *Theoretical Computer Science* **165** (1) 3–55.

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

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

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

Bouhoula, A. and Rusinowitch, M. (2002) Observational proofs by rewriting. *Theoretical Computer Science* **275** 675–698.

Buss, S. and Roşu, G. (2000) Incompleteness of behavioral logics. In: Reichel, H. (ed.) Coalgebraic Methods in Computer Science: CMCS 2000. *Electronic Notes in Theoretical Computer Science* **33**.

Diaconescu, R. and Futatsugi, K. (1998) *Cafe*OBJ *report: The language, proof techniques, and methodologies for object-oriented algebraic specification*, AMAST series in Computing **6**, World Scientific.

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

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

Fiadeiro, J. and Sernadas, A. (1988) Structuring theories on consequence. In: Recent trends in data type specification. Specification of abstract data types. Selected Papers, 5th Workshop, Gullane/UK 1987. *Springer-Verlag Lecture Notes in Computer Science* **332** 44–72.

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

Goguen, J. and Malcolm, G. (1999) Hidden coinduction: Behavioural correctness proofs for objects. *Mathematical Structures in Computer Science* **9** (3) 287–319.

Goguen, J. and Malcolm, G. (2000) A hidden agenda. *Theoretical Computer Science* **245** (1) 55–101.

Goguen, J., Lin, K. and Roşu, G. (2002) Conditional circular coinductive rewriting with case analysis. In: 16th International Workshop, WADT 2002, Frauenchiemsee, Germany. *Springer-Verlag Lecture Notes in Computer Science* **2755** 216–232.

Gorbunov, V. (1998) *Algebraic theory of quasivarieties*, (Siberian School of Algebra and Logic), Consultants Bureau, Plenum Publishing Corporation (translated from the Russian).

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

Hennicker, R. and Bidoit, M. (1999) Observational logic. In: Proc. AMAST '98, 7th International Conference on Algebraic Methodology and Software Technology. *Springer-Verlag Lecture Notes in Computer Science* **1548** 263–277.

Hofmann, M. and Sannella, D. (1996) On behavioural abstraction and behavioural satisfaction in higher-order logic. *Theoretical Computer Science* **167** (1-2) 3–45.

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

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

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

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

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

Reichel, H. (1985) Behavioural validity of conditional equations in abstract data types. In: *Contributions to general algebra 3*, (Conference Proceedings, Vienna 1984), 301–324.

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

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

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

Wójcicki, R. (1988) *Theory of logical calculi. Basic theory of consequence operations*, Synthese Library **199**, Reidel.