ELSEVIER

Theoretical Computer Science 280 (2002) 35–68

Theoretical
Computer Science

www.elsevier.com/locate/tcs

A coalgebraic equational approach to specifying observational structures

Corina Cîrstea

Oxford University Computing Laboratory, Wolfson Building, Parks Road, Oxford OX1 3QD, UK

Abstract

A coalgebraic, equational approach to the specification of observational structures allowing for a choice in the result type of observations is presented. Observers whose result type is structured as a coproduct of basic types are considered, and notions of covariable, coterm and coequation, dual to the algebraic notions of variable, term and equation are used to specify the associated structures. A sound and complete deduction calculus for reasoning about observational structures is then formulated. Finally, the approach is extended in order to account for the availability of a fixed data universe in the specification of such structures. © 2002 Elsevier Science B.V. All rights reserved.

1. Introduction

Recent developments in the theory of coalgebras have demonstrated the suitability of coalgebraic techniques for the specification of state-based, dynamical systems [9, 11]. Such techniques have proved particularly fruitful for specifying observational properties of objects, with final coalgebras providing appropriate denotations for object specifications [5, 6]. Various approaches to reasoning about state observation have also been proposed: in [8, 10], ideas from modal logic have been applied to coalgebras, yielding logics whose sentences constrain single state observations, while in [3] equational sentences have been used to relate different observations of the same state. At the expense of using infinitary sentences, approaches stemming from modal logic are able to provide characterisability results for coalgebras [8]. However, the formulation of completeness results in such approaches requires a restriction to finitary sentences, as well as the satisfaction of some rather restrictive finiteness conditions by the endofunctors in question [10]. While not sufficiently expressive to yield similar characterisability results, equational approaches do not require any additional assumptions in order to

E-mail address: corina.cirstea@comlab.ox.ac.uk (C. Cîrstea).

0304-3975/02/$ - see front matter © 2002 Elsevier Science B.V. All rights reserved.
PII: S0304-3975(01)00020-2

derive completeness results [3]. Furthermore, equational sentences appear to be better suited for specifying in a concise manner observational properties quantified over state spaces. Since our aim is to reason about properties of collections of states (as opposed to single states), we shall restrict our attention to equational approaches.

In [3], suitably restricted algebraic terms are used to formalise state observations, and equations are used to constrain the results yielded by them. A sound and complete deduction calculus for reasoning about state observations is also formulated. However, the use in [3] of an algebraic syntax prevents observers with structured result type to be accommodated by the approach. Such observers turn out to be essential for capturing termination (of possibly infinite structures such as lists), as well as more general structural properties of state-based systems, including various dependencies between their components, or the presence/absence of certain components in some of the system states.

The present paper extends the approach in [3] in order to account for the possibility of a choice in what can be observed of a system in a particular state. State observations are formalised by the notion of *coterm*, which captures the successive evaluation of observers by providing alternatives for proceeding with an evaluation depending on the type of the result yielded by the most recently evaluated observer. Equational sentences are used to constrain observations, and a sound and complete deduction calculus for reasoning about the associated behaviours is formulated. Moreover, the resulting specification logic is shown to be an institution. The approach is then extended to allow for the interpretations of certain sorts to be fixed when specifying observational properties of systems. The resulting formalism is shown to be as expressive as many-sorted algebra with regard to the kinds of structures specifiable at the level of signatures (but less expressive as far as characterising classes of coalgebras is concerned). Moreover, moving from one- to many-sorted coalgebras is shown to be necessary in order to attain this expressiveness.

By moving from an essentially algebraic framework to a coalgebraic one, algebraic features such as the use of data values as constant observations, or the use of data arguments to state observers are discarded. Our approach could be adapted to include such features; however, we believe that their integration should take place at a different level, where it should be possible to specify arbitrary algebraic structures over coalgebraically specified state spaces.

Some familiarity with basic notions of category theory as well as with the use of algebra and coalgebra in specification is assumed in the following. The paper is structured as follows. Section 2 recalls some defining features of specification logics and, at the same time, establishes some notation for subsequent sections. Section 3 introduces a coalgebraic formalism for the specification of observational structures allowing for a choice in the result types of observations, and presents a sound and complete deduction calculus for reasoning about such structures. Section 4 extends the approach in order to account for the availability of a fixed data universe when specifying observational properties of systems. Section 5 investigates the expressiveness of the approach, while Section 6 discusses its relation to other approaches to the specification of observational structures. Finally, Section 7 summarises the results presented and outlines future work.

2. Specification logics

Formal specification and verification techniques employ a large variety of logics, whose common features include notions of *sentence*, *inference* of sentences from sets of sentences, *model*, and *satisfaction* of sentences by models. The semantical and, respectively, syntactical aspects of a specification logic are formally captured by the notions of *institution* [4] and *entailment system* [7].

Definition 1 (Goguen and Burstall [4]). An *institution* is a tuple $(\mathsf{Sign}, \mathsf{Mod}, \mathsf{Sen}, \models)$, where:

(1) Sign is a category whose objects are called *signatures*.

(2) $\mathsf{Sen} : \mathsf{Sign} \to \mathsf{Set}$ is a functor giving, for each signature, a set of *sentences* over that signature.

(3) $\mathsf{Mod} : \mathsf{Sign} \to \mathsf{Cat}^{\mathsf{op}}$ is a functor giving, for each signature Σ, a category $\mathsf{Mod}(\Sigma)$ whose objects are called *Σ-models* and whose arrows are called *Σ-homomorphisms*.

(4) $\models$ is a signature-indexed family of relations $(\models_\Sigma)_{\Sigma \in |\mathsf{Sign}|}$ with, for $\Sigma \in |\mathsf{Sign}|$, $\models_\Sigma \subseteq |\mathsf{Mod}(\Sigma)| \times \mathsf{Sen}(\Sigma)$ being called *Σ-satisfaction*

additionally satisfying: $M' \models_{\Sigma'} \mathsf{Sen}(\phi)(e)$ if and only if $\mathsf{Mod}(\phi)(M') \models_\Sigma e$, for any $(\phi : \Sigma \to \Sigma') \in \|\mathsf{Sign}\|$, any $M' \in |\mathsf{Mod}(\Sigma')|$ and any $e \in \mathsf{Sen}(\Sigma)$.

Signatures provide a syntax for constructing sentences, while signature morphisms define translations between syntaxes. The defining condition of institutions, known as the *satisfaction condition*, formalises the statement that *truth is invariant under changes of notation* [4].

One writes U_ϕ for $\mathsf{Mod}(\phi)$ and $\phi(e)$ for $\mathsf{Sen}(\phi)(e)$, with $(\phi : \Sigma \to \Sigma') \in \|\mathsf{Sign}\|$ and $e \in \mathsf{Sen}(\Sigma)$. The functors U_ϕ are called *reduct functors*.

Definition 2. Let $\mathscr{I} = (\mathsf{Sign}, \mathsf{Mod}, \mathsf{Sen}, \models)$ denote an institution.

(1) An *($\mathscr{I}$-)specification* is a pair (Σ, E) with $\Sigma \in |\mathsf{Sign}|$ and $E \subseteq \mathsf{Sen}(\Sigma)$.

(2) A *Σ-model M satisfies* a specification (Σ, E) (written $M \models_\Sigma E$) if and only if $M \models_\Sigma e$ for each $e \in E$.

(3) A *Σ-sentence e is semantically entailed* by a set E of Σ-sentences (written $E \models_\Sigma e$) if and only if $M \models_\Sigma E$ implies $M \models_\Sigma e$ for any $M \in |\mathsf{Mod}(\Sigma)|$.

(4) A *signature morphism* $\phi : \Sigma \to \Sigma'$ defines a *specification morphism* $\phi : (\Sigma, E) \to (\Sigma', E')$ if and only if $E' \models_{\Sigma'} \mathsf{Sen}(\phi)(e)$ for each $e \in E$.

One writes $\mathsf{Mod}(\Sigma, E)$ for the full subcategory of $\mathsf{Mod}(\Sigma)$ whose objects satisfy the specification (Σ, E). Then, specification morphisms $\phi : (\Sigma, E) \to (\Sigma', E')$ induce *reduct functors* $\mathsf{U}_\phi : \mathsf{Mod}(\Sigma', E') \to \mathsf{Mod}(\Sigma, E)$.

The notion of entailment employed by institutions is based on the satisfaction of sentences by models. A different notion of entailment, based on the inference of sentences according to specified rules is captured by *entailment systems*.

Definition 3 (Meseguer [7]). An *entailment system* is a triple $(\mathsf{Sign}, \mathsf{Sen}, \vdash)$, where:
(1) Sign is a category whose objects are called signatures.
(2) $\mathsf{Sen} : \mathsf{Sign} \to \mathsf{Set}$ is a functor giving, for each signature, a set of *sentences* over that signature.
(3) $\vdash$ is a signature-indexed family of relations $(\vdash_\Sigma)_{\Sigma \in |\mathsf{Sign}|}$ with, for $\Sigma \in |\mathsf{Sign}|$, $\vdash_\Sigma \subseteq \mathscr{P}(\mathsf{Sen}(\Sigma)) \times \mathsf{Sen}(\Sigma)$ being called *Σ-entailment*
such that the following hold:
(1) $\{e\} \vdash_\Sigma e$, for $e \in \mathsf{Sen}(\Sigma)$ (reflexivity),
(2) $E \vdash_\Sigma e$ and $E \subseteq E'$ imply $E' \vdash_\Sigma e$ (monotonicity),
(3) $E \vdash_\Sigma e_i$ for $i \in I$ and $\{e_i \mid i \in I\} \vdash_\Sigma e$ imply $E \vdash_\Sigma e$ (transitivity),
(4) $E \vdash_\Sigma e$ implies $\mathsf{Sen}(\phi)(E) \vdash_{\Sigma'} \mathsf{Sen}(\phi)(e)$, for $\phi : \Sigma \to \Sigma'$ ($\vdash$-translation).

A desirable property of any specification logic which involves both an institution and an entailment system is the existence of a certain compatibility between its two notions of entailment, in a sense made precise below.

Definition 4. Let Sign, Mod, Sen, $\models$ and $\vdash$ be such that $(\mathsf{Sign}, \mathsf{Mod}, \mathsf{Sen}, \models)$ is an institution and $(\mathsf{Sign}, \mathsf{Sen}, \vdash)$ is an entailment system. Then, $\vdash$ is *sound* (respectively, *complete*) for $\models$ if and only if $E \vdash_\Sigma e$ implies $E \models_\Sigma e$ ($E \models_\Sigma e$ implies $E \vdash_\Sigma e$) for any $\Sigma \in |\mathsf{Sign}|$, any $E \subseteq \mathsf{Sen}(\Sigma)$ and any $e \in \mathsf{Sen}(\Sigma)$.

3. Many-sorted coalgebra

This section presents a formalism for the specification of observational structures allowing for a choice in the result type of observers. The resulting formalism is, to a large extent, a syntactic dual of the many-sorted algebraic formalism for the specification of data types.

3.1. Cosignatures, covariables, coterms and substitution

Definition 5. A (*many-sorted*) *cosignature* is a pair (S, Δ) with S a set of *sorts* and Δ an $S \times S^+$-sorted set of *operation symbols* (where S^+ denotes the set of finite, non-empty sequences of sorts). One writes $\delta : s \to s_1 \ldots s_n$ for $\delta \in \Delta_{s,s_1 \ldots s_n}$.

In the following it is only assumed that the set of operation symbols of a many-sorted cosignature is enumerable. In practice however, this set is usually finite. Cosignatures (S, Δ) are abbreviated Δ whenever the context allows it. The set $\{\delta \in \Delta_{s,s_1 \ldots s_n} \mid s_1, \ldots, s_n \in S\}$, with $s \in S$ is denoted Δ_s.

The operation symbols of a many-sorted cosignature specify basic ways of observing the states of a given system. Arbitrary state observations are formalised by the notion of *coterm*, which provides alternatives for proceeding with an observation, depending on the result type of the most recently evaluated observer. *Covariables* are used in coterms as place-holders for their potential outputs, in a manner similar to the use of variables as place-holders for the inputs of algebraic terms.

Definition 6. Let Δ denote a many-sorted cosignature with sort set S, and let $\mathscr{C}$ denote an S-sorted set (of *covariables*). The (S-sorted) set $T_\Delta[\mathscr{C}]$ of *Δ-coterms with covariables from $\mathscr{C}$* is the least S-sorted set satisfying:
(1) $Z \in T_\Delta[\mathscr{C}]_s$ for $Z \in \mathscr{C}_s$,
(2) $[t_1,\ldots,t_n]\delta \in T_\Delta[\mathscr{C}]_s$ for $\delta \in \Delta_{s,s_1\ldots s_n}$ and $t_i \in T_\Delta[\mathscr{C}]_{s_i}$, $i=1,\ldots,n$.

Coterms of sort $s \in S$ (elements of $T_\Delta[\mathscr{C}]_s$) specify ways of observing states of type s. Their result type is determined by the sorts of the covariables appearing in them. There are no coterms over an empty set of covariables.

One writes $Z : s$ for $Z \in \mathscr{C}_s$. The S-sorted set of covariables actually appearing in a coterm $t \in T_\Delta[\mathscr{C}]$ (a subset of $\mathscr{C}$) is denoted $cov(t)$. (It then follows by Definition 6 that $cov(t)$ is finite for any $t \in T_\Delta[\mathscr{C}]$ and any set $\mathscr{C}$ of covariables.)

Definition 7. Let Δ denote a many-sorted cosignature. A coterm $t \in T_\Delta[\mathscr{C}]$ is said to be *non-identifying* if it contains at most one occurrence of each covariable in $\mathscr{C}$. The S-sorted set of non-identifying Δ-coterms with covariables in $\mathscr{C}$ is denoted $T_\Delta^1[\mathscr{C}]$.

Let $\mathscr{C}_0$ denote an S-sorted set of covariables, with $\mathscr{C}_{0,s}$ infinite but enumerable for each $s \in S$. Also, for a many-sorted cosignature Δ, let T_Δ^1 denote the set of non-identifying Δ-coterms with covariables in $\mathscr{C}_0$.[1] Then, since both $\mathscr{C}_{0,s}$ with $s \in S$ and the set of operation symbols of Δ are enumerable, so is $T_{\Delta,s}^1$ for any $s \in S$. The set T_Δ^1 will play an important rôle in characterising the elements of final and cofree coalgebras, as well as in the proof of a completeness result.

Substitution of coterms for covariables is now defined as follows.

Definition 8. If $t \in T_\Delta[\{Z_1,\ldots,Z_n\}]_s$ with $Z_i : s_i$ for $i=1,\ldots,n$, and if $t_i \in T_\Delta[\mathscr{C}]_{s_i}$ for $i=1,\ldots,n$, then the coterm obtained by *substituting $t_1,\ldots,t_n$ for $Z_1,\ldots,Z_n$ in t*, denoted $[t_1/Z_1,\ldots,t_n/Z_n]t$ ($[\bar{t}/\bar{Z}]t$ for short) is defined inductively on the structure of t as follows:
(1) $[\bar{t}/\bar{Z}]Z_i = t_i$, for $i=1,\ldots,n$,
(2) $[\bar{t}/\bar{Z}]([t'_1,\ldots,t'_m]\delta) = [[\bar{t}/\bar{Z}]t'_1,\ldots,[\bar{t}/\bar{Z}]t'_m]\delta$, for $\delta \in \Delta_{s,s'_1\ldots s'_m}$ and $t'_j \in T_\Delta[\{Z_1,\ldots,Z_n\}]_{s'_j}$, $j=1,\ldots,m$.

If $t \in T_\Delta[\{Z_1,\ldots,Z_n\}]$, we write $\underline{t}$ for a coterm with the following properties:
(1) $\underline{t} \in T_\Delta^1[\{X_1,\ldots,X_m\}]$,
(2) $t = [Z_{i_1}/X_1,\ldots,Z_{i_m}/X_m]\underline{t}$, with $Z_{i_1},\ldots,Z_{i_m} \in \{Z_1,\ldots,Z_n\}$.

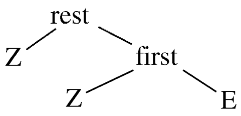
[1] Note that, since the sets of operation symbols of many-sorted cosignatures are enumerable, and since coterms only contain a finite number of covariables, restricting attention to coterms over $\mathscr{C}_0$ does not reduce the expressiveness of the formalism.

That is, t is obtained from $\underline{t}$ by renaming and possibly identifying some covariables. (Note that $\underline{t}$ is only defined up to a bijective renaming of its covariables.)

Example 9. Lists (finite or infinite) are specified using sorts `1` (denoting a one-element set), `Elt` and `List`, and operation symbols `first` : `List` → `1 Elt` and `rest` : `List` → `1 List`. The following are coterms of sort `List` : `[Z,E]first` (used to observe the first element of a list), `[Z,[Z,E]first]rest` (used to observe the second element), and so on. Their result type is `1` + `Elt`. (In the second case, this is because the covariable `Z` occurs twice in the coterm.)

Remark 10. Coterms can be represented as trees with the leaves labelled by covariables and with the internal nodes labelled by operation symbols:
(1) covariables Z are represented as trees having one node, labelled by Z,
(2) coterms of form $[t_1,\ldots,t_n]\delta$ are represented as trees having the root labelled by δ and its subtrees given by the trees associated to $t_1,\ldots,t_n$.
A path from the root of the tree associated to a coterm to one of its leaves is called an *evaluation path* for that coterm.

Given the cosignature in Example 9, the tree associated to `[Z,[Z,E]first]rest` is



with the evaluation paths corresponding to an empty list, a list with only one element, and respectively a list with at least two elements.

3.2. Coalgebras, finality and bisimilarity

The models of a many-sorted cosignature provide interpretations for its sorts and operation symbols.

Definition 11. Let Δ denote a many-sorted cosignature with sort set S. A (*many-sorted*) *Δ-coalgebra* is given by an S-sorted set A together with, for each $\delta : s \to s_1 \ldots s_n$ in Δ, a function $\delta_A : A_s \to A_{s_1} + \cdots + A_{s_n}$. Given Δ-coalgebras A and B, a *Δ-homomorphism* $f : A \to B$ is given by an S-sorted function $(f_s)_{s\in S}$ with $f_s : A_s \to B_s$ for $s \in S$, additionally satisfying: $[\iota_1 \circ f_{s_1},\ldots,\iota_n \circ f_{s_n}](\delta_A(a)) = \delta_B(f_s(a))$ for each $\delta : s \to s_1 \ldots s_n$ in Δ and each $a \in A_s$, with $s, s_1,\ldots,s_n \in S$ (where $\iota_j : B_{s_j} \to B_{s_1} + \cdots + B_{s_n}$ for $j = 1,\ldots,n$ are the coproduct injections). The category of Δ-coalgebras and Δ-homomorphisms is denoted $\mathsf{Coalg}(\Delta)$.

The use of the word *coalgebra* to refer to the models of a many-sorted cosignature is justified in the following.

Definition 12. Let $\mathsf{G}:\mathsf{C}\to\mathsf{C}$ denote an arbitrary endofunctor. A G-*coalgebra* is a pair $\langle A,\alpha\rangle$ with A a C-object and $\alpha : A\to \mathsf{G}A$ a C-arrow. A G-*coalgebra homomorphism* between G-coalgebras $\langle A,\alpha\rangle$ and $\langle B,\beta\rangle$ is a C-arrow $f:A\to B$ additionally satisfying: $\beta\circ f=\mathsf{G}f\circ\alpha$. The category of G-coalgebras and G-coalgebra homomorphisms is denoted $\mathsf{Coalg}(\mathsf{G})$.

Proposition 13. *Let Δ denote a many-sorted cosignature with sort set S, and let $\mathsf{G}_\Delta:\mathsf{Set}^S\to\mathsf{Set}^S$ be given by*: $(\mathsf{G}_\Delta X)_s=\prod_{\delta\in\Delta_{s,s_1\ldots s_n}}(X_{s_1}+\cdots+X_{s_n})$ *for $X\in|\mathsf{Set}^S|$ and $s\in S$. Then*, $\mathsf{Coalg}(\Delta)$ *and* $\mathsf{Coalg}(\mathsf{G}_\Delta)$ *are isomorphic.*

Proof. Δ-coalgebras A uniquely determine Set^S-arrows $\alpha:A\to\mathsf{G}_\Delta A$ (with α_s mapping $a\in A_s$ to $(\delta_A(a))_{\delta\in\Delta_{s,s_1\ldots s_n}}$, for $s\in S$) and conversely, any such Set^S-arrow uniquely defines a Δ-coalgebra structure on its domain. □

Example 14. Given the cosignature in Example 9, the coalgebra A defined by

$$\mathtt{A}_{1}=\{*\},\ \mathtt{A}_{\mathtt{Elt}}=\mathbb{N},\ \mathtt{A}_{\mathtt{List}}=\mathbb{N}^*$$

$$\mathtt{first}_A(l)=\begin{cases}\iota_1(*) & \mathtt{if}\ l=\varepsilon\\ \iota_2(e) & \mathtt{if}\ l=e:l',\end{cases}\qquad \mathtt{rest}_A(l)=\begin{cases}\iota_1(*) & \mathtt{if}\ l=\varepsilon,\\ \iota_2(l') & \mathtt{if}\ l=e:l'\end{cases}$$

(with $\mathbb{N}^*$ denoting the set of sequences of natural numbers and ε denoting the empty sequence of natural numbers) provides an implementation of finite lists.

We note that further constraints must, in general, be imposed to `first` and `rest` in order to ensure that their interpretations in coalgebras of the list cosignature are consistent with each other (i.e. that either both of them yield a result of type `1`, or none of them does). Such constrains will be considered in Section 3.3. We also note that, at this point, it is not possible to syntactically constrain the interpretation of the sort `1` in coalgebras of the list specification to a one-element set. This issue will be dealt within Section 4.

Given a Δ-coalgebra A, a set $\{Z_1,\ldots,Z_n\}$ of covariables with $Z_i:s_i$ for $i=1,\ldots,n$ and a covariable $Z\in\{Z_1,\ldots,Z_n\}$ with $Z:s$, one writes $\iota_Z:A_s\to A_{s_1}+\cdots+A_{s_n}$ for the corresponding coproduct injection.

The interpretation of Δ-operation symbols by Δ-coalgebras extends to an interpretation of Δ-coterms by Δ-coalgebras.

Definition 15. Let Δ denote a many-sorted cosignature. The *interpretation* of a Δ-coterm $t\in T_\Delta[\mathscr{C}]_s$, with $s\in S$, in a Δ-coalgebra A is a function $t_A:A_s\to\coprod_{Z\in\mathscr{C},Z:s'}A_{s'}$ defined as follows:
(1) $Z_A=\iota_Z$ for $Z\in\mathscr{C}_s$,
(2) $([t_1,\ldots,t_n]\delta)_A=[(t_1)_A,\ldots,(t_n)_A]\circ\delta_A$ for $\delta\in\Delta_{s,s_1\ldots s_n}$ and $t_i\in T_\Delta[\mathscr{C}]_{s_i}$, $i=1,\ldots,n$ with $[(t_1)_A,\ldots,(t_n)_A]:A_{s_1}+\cdots+A_{s_n}\to\coprod_{Z\in\mathscr{C},Z:s'}A_{s'}$ denoting the unique Set-arrow induced by $(t_i)_A:A_{s_i}\to\coprod_{Z\in\mathscr{C},Z:s'}A_{s'}$ with $i=1,\ldots,n$.

A characterisation of the behaviours observable using the operations specified by a cosignature is provided by (the elements of) a final coalgebra of that cosignature. Existence of final coalgebras of many-sorted cosignatures is an immediate consequence of Proposition 13 and of a general result regarding the existence of final coalgebras of ω^{op}-continuous endofunctors (see e.g. [11]). An alternative proof of the existence of such coalgebras which, in addition, provides a concrete description of their elements is given in the following.

Proposition 16. *Any many-sorted cosignature Δ admits a final coalgebra.*

Proof. Let F denote the Δ-coalgebra given by

$$F_s = \Big\{ \varphi : T^1_{\Delta,s} \to \bigcup \{cov(t) \mid t \in T^1_{\Delta,s}\} \mid t \in T^1_{\Delta,s} \Rightarrow \varphi(t) \in cov(t),$$

$$t, t' \in T^1_{\Delta,s},\ t' = [t_1/Z_1, \ldots, t_n/Z_n]t,\ \varphi(t) = Z_k \Rightarrow \varphi(t') \in cov(t_k) \Big\}$$

for $s \in S$, and

$$\delta_F(\varphi) = \varphi' \in F_{s'},\ \varphi'(t') = \varphi([Z_1, \ldots, t', \ldots, Z_n]\delta) \text{ for } t' \in T^1_{\Delta,s'}$$

$$\text{if } \varphi([Z_1, \ldots, Z_n]\delta) = Z_i : s'$$

for $\varphi \in F_s$ and $\delta \in \Delta_{s,s_1 \ldots s_n}$. That is, the elements of F are suitably restricted mappings from non-identifying coterms to covariables appearing in them (with, for each such coterm, the choice of covariable determining an evaluation path for that coterm). Then, F is a final Δ-coalgebra. For, given an arbitrary Δ-coalgebra A, the S-sorted function $f : A \to F$ defined by: $f(a)(t) = Z$ if $t_A(a) \in \iota_Z(A)$, for $t \in T^1_{\Delta,s}$, $a \in A_s$ and $s \in S$ defines a Δ-homomorphism from A to F. Moreover, any Δ-homomorphism from A to F is necessarily defined in this way. □

Remark 17. For $C \in |\mathsf{Set}^S|$, a cofree Δ-coalgebra A over C is given by

$$A_s = \Big\{ \varphi : T^1_{\Delta,s} \to \bigcup \{ cov(t) \times C \mid t \in T^1_{\Delta,s} \} \mid t \in T^1_{\Delta,s} \Rightarrow \pi_1(\varphi(t)) \in cov(t),$$

$$t, t' \in T^1_{\Delta,s},\ t' = [t_1/Z_1, \ldots, t_n/Z_n]t,\ \pi_1(\varphi(t)) = Z_k \Rightarrow \pi_1(\varphi(t')) \in cov(t_k),$$

$$\text{and moreover, if } t_k \text{ is a covariable then } \pi_2(\varphi(t')) = \pi_2(\varphi(t)) \Big\}$$

for $s \in S$ (where the product $cov(t) \times C$ is taken in Set^S), and:

$$\delta_A(\varphi) = \varphi' \in A_{s'},\ \varphi'(t') = \varphi([Z_1, \ldots, t', \ldots, Z_n]\delta) \text{ for } t' \in T^1_{\Delta,s'}$$

$$\text{if } \varphi([Z_1, \ldots, Z_n]\delta) = \langle Z_i, c_i \rangle \text{ with } Z_i : s'$$

for $\varphi \in A_s$ and $\delta \in \Delta_{s,s_1 \ldots s_n}$. This can be shown similarly to Proposition 16.

A characterisation of the notion of *bisimilarity* on (the G_Δ-coalgebras induced by) many-sorted Δ-coalgebras is given in the following.

Definition 18. Let $\mathsf{G}:\mathsf{C}\to\mathsf{C}$ be an arbitrary endofunctor. A G-*bisimulation* on a G-coalgebra $\langle A,\alpha\rangle$ is a G-coalgebra $\langle R,\rho\rangle$, with $\langle R,\pi_1,\pi_2\rangle$ a relation[2] on A in C, such that $\pi_1:R\to A$ and $\pi_2:R\to A$ define G-coalgebra homomorphisms from $\langle R,\rho\rangle$ to $\langle A,\alpha\rangle$. The largest bisimulation[3] on $\langle A,\alpha\rangle$, if it exists, is called *bisimilarity*. A G-coalgebra $\langle A,\alpha\rangle$ is *extensional* if and only if bisimilarity on $\langle A,\alpha\rangle$ is given by the equality relation on A.

Proposition 19. *Let Δ denote a many-sorted cosignature with sort set S, and let A denote a Δ-coalgebra. Then, given $s\in S$, two states $a,a'\in A_s$ are bisimilar if and only if for any $t\in T^1_{\Delta,s}$, there exists $Z\in cov(t)_{s'}$ with $s'\in S$ such that $t_A(a),t_A(a')\in \iota_Z(A_{s'})$.*

Proof. The conclusion follows from the observation that, if $f:A\to F$ denotes the unique Δ-homomorphism from A to the final Δ-coalgebra, then $a,a'\in A_s$ are bisimilar if and only if $f_s(a)=f_s(a')$.[4] □

That is, two states of a given coalgebra are bisimilar if and only if, when observed using any non-identifying coterm, the results yielded correspond to the same evaluation path for that coterm.

Example 20. The notion of bisimilarity associated to the cosignature in Example 9 relates two states of a coalgebra if and only if they denote lists with the same number of elements.[5] A finer notion of bisimilarity, which discriminates between lists with different elements will be obtained in Section 4 (see Example 52) by fixing the interpretation of the sort `Elt`.

The characterisation of bisimilarity given by Proposition 19 together with the extensionality of final coalgebras yield a coinductive technique for proving the equality of observations on the elements of final coalgebras.

Corollary 21. *Let Δ denote a many-sorted cosignature with sort set S, let F denote a final Δ-coalgebra, and let $l,r\in T_\Delta[\{Z_1,\ldots,Z_n\}]_s$ with $Z_1:s_1,\ldots,Z_n:s_n$. Then, given $\varphi\in F_s$, $l_F(\varphi)=r_F(\varphi)$ holds if and only if $([t_1/Z_1,\ldots,t_n/Z_n]l)_F(\varphi)$ and $([t_1/Z_1,\ldots,t_n/Z_n]r)_F(\varphi)$ are both in $\iota_Z(F_{s'})$ for some $Z:s'$, for any $t_i\in T^1_{\Delta,s_i}$ with $i=1,\ldots,n$.*

[2] See e.g. [1, p. 101] for a categorical definition of relations.

[3] The category of relations on A is a preorder.

[4] See e.g. [11]. (The fact that G_Δ preserves pullbacks is used here.)

[5] Here it is assumed that the constraints mentioned earlier regarding the consistency of `first` and `rest` are satisfied by the coalgebra in question.

Proof. The *only if* direction is straightforward. For the *if* direction, it suffices to show that $l_F(\varphi) \sim_F r_F(\varphi)$, with $\sim_F$ denoting Δ-bisimilarity on F.[6] Taking $t_i = Z_i$ for $i = 1,\ldots,n$ gives $l_F(\varphi), r_F(\varphi) \in \iota_{Z_i}(F_{s_i})$ for some $i \in \{1,\ldots,n\}$. Then, for any $t \in T^1_{\Delta,s_i}$, taking $t_j = Z_j$ for $j \in \{1,\ldots,i-1,i+1,\ldots,n\}$ and $t_i = t$ in the hypothesis gives $t_F(l_F(\varphi)) = t_F(r_F(\varphi))$. Hence, $l_F(\varphi) \sim_{F,s_i} r_F(\varphi)$. □

3.3. Coalgebraic equational specification

In algebraic specification, many-sorted equations are used to constrain the interpretation of terms by algebras. A similar approach proves suitable for constraining state observations, provided that one's interest is in relating different observations of the same state. This section presents such an approach, illustrating the kinds of constraints specifiable within it.

A first approximation of the notion of coequation is given by a pair of coterms of the same sort. Satisfaction of a coequation by a coalgebra then corresponds to the coalgebra providing identical interpretations for the two coterms. For instance, a coequation of form: $\mathtt{[Z,[Z,E]first]rest} = \mathtt{[Z',E]first}$ constrains the interpretation of the sort $\mathtt{List}$ in coalgebras A satisfying the coequation to constant, infinite lists (as it requires $[\iota_{\mathtt{Z}}, \iota_{\mathtt{E}}] \circ (\mathtt{[Z,[Z,E]first]rest})_A$, $[\iota_{\mathtt{Z'}}, \iota_{\mathtt{E}}] \circ (\mathtt{[Z',E]first})_A : A_{\mathtt{List}} \to A_1 + A_{\mathtt{Elt}} + A_1$ to yield similar results on any list). However, due to the presence of choice in the result types of observers, one expects reasoning with coequations to involve some form of case analysis on the possible evaluation paths of coterms. For instance, in order to derive the coequation: $\mathtt{[Z,L]rest} = \mathtt{[Z',L]rest}$ (constraining $\mathtt{rest}_A$ to always yield a result of type $\mathtt{List}$, by requiring that the observations $[\iota_{\mathtt{Z}}, \iota_{\mathtt{L}}] \circ (\mathtt{[Z,L]rest})_A$, $[\iota_{\mathtt{Z'}}, \iota_{\mathtt{L}}] \circ (\mathtt{[Z',L]rest})_A : A_{\mathtt{List}} \to A_1 + A_{\mathtt{List}} + A_1$ yield similar results) from the previous coequation, a case analysis on the possible evaluation paths of $\mathtt{[Z,L]}$ $\mathtt{rest}$ should be carried out. Specifically, the satisfaction of this coequation would follow by showing that the assumption that the evaluation path corresponds to the covariable $\mathtt{Z}$ together with the satisfaction of the initial coequation yield a contradiction. It turns out that in order to obtain a complete deduction calculus for coequations, this form of case analysis should be incorporated in the notion of coequation. This justifies the following definition.

Definition 22. Let Δ denote a many-sorted cosignature. A *Δ-coequation* is a tuple (l, r, C), with $l, r \in T_\Delta[\mathscr{C}]_s$ and $C = \{(t_1, \mathscr{C}'_1), \ldots, (t_n, \mathscr{C}'_n)\}$ for some $s \in S$ and $t_i \in T_\Delta[\mathscr{C}_i]_s$, $\mathscr{C}'_i \subseteq \mathscr{C}_i$ for $i = 1,\ldots,n$. A Δ-coalgebra A *satisfies* a Δ-coequation e of the above form (written $A \models_\Delta e$) if and only if $l_A(a) = r_A(a)$ holds whenever $a \in A_s$ is such that $(t_i)_A(a) \in \iota_{Z_i}(A_{s_i})$ for some $Z_i \in (\mathscr{C}'_i)_{s_i}$, for $i = 1,\ldots,n$ (case in which a is said to *satisfy* the conditions C).

The coequation (l, r, C) is alternatively denoted $l = r$ if $(t_1, \mathscr{C}'_1), \ldots, (t_n, \mathscr{C}'_n)$. Also, if $\mathscr{C}'_i = \{Z_i\}$, one writes (t_i, Z_i) as a shorthand for $(t_i, \mathscr{C}'_i)$. Finally, given a set E of

[6] As final coalgebras are extensional, see e.g. [11].

Δ-coequations together with $s \in S$, one writes E_s for the subset of E consisting of coequations of sort s.

Example 23. A state invariant for lists is specified using the coequations:

$$\texttt{[Z,L]rest} = \texttt{[Z,L}'\texttt{]rest if ([Z,E]first,Z)},$$

$$\texttt{[Z,E]first} = \texttt{[Z,E}'\texttt{]first if ([Z,L]rest,Z)},$$

stating that a list is either empty, in which case it has neither a head nor a tail, or non-empty, in which case it has both a head and a tail. The coequation:

$$\texttt{[Z,[Z,[Z,E]first]rest]rest} = \texttt{[Z,E]first if ([Z,[Z,L]rest]rest,L)},$$

further constrains the interpretation of the sort `List` to alternating lists. It is also worth noting that the absence of any algebraic structure limits the expressiveness of coequational specification. For instance, the property of lists stating that each two adjacent elements of a list are different from each other cannot be formalised using coequations, as no means to compare two elements of a list are available.

Given $\delta \in \Delta_{s,s_1\ldots s_n}$ together with $i \in \{1,\ldots,n\}$ and conditions C of form $(t_1,\mathscr{C}_1'),\ldots,(t_m,\mathscr{C}_m')$ for the sort s_i, one writes $[Z_1,\ldots,C,\ldots,Z_n]\delta$ as a shorthand for $([Z_1,\ldots,t_j,\ldots,Z_n]\delta, \mathscr{C}_j' \cup \{Z_1,\ldots,Z_{i-1},Z_{i+1},\ldots,Z_n\})_{j=1,\ldots,m}$, with $\{Z_1,\ldots,Z_n\} \cap cov(t_j) = \emptyset$ for $j = 1,\ldots,m$. The conditions $[Z_1,\ldots,C,\ldots,Z_n]\delta$ require the result yielded by δ to satisfy the conditions C whenever the evaluation path for $[Z_1,\ldots,Z_n]\delta$ corresponds to the covariable $Z_i : s_i$. Also, given $t \in T_\Delta[\{Z_1,\ldots,Z_n\}]_s$ with $Z_i : s_i$, $i = 1,\ldots,n$, and i, C as before, one writes $[Z_1/Z_1,\ldots,C/Z_i,\ldots,Z_n/Z_n]t$ for $([Z_1/Z_1,\ldots,t_j/Z_i,\ldots,Z_n/Z_n]t, \mathscr{C}_j' \cup \{Z_1,\ldots,Z_{i-1},Z_{i+1},\ldots,Z_n\})_{j=1,\ldots,m}$. This notation will be used when formulating a deduction calculus for coequations.

While, in many-sorted algebra, equations of form $X = X'$ are only satisfied by algebras whose corresponding carrier is a one-element set, here coequations of form $Z = Z'$ are only satisfied by coalgebras whose corresponding carrier is empty. More generally, coequations of form $l = r$ with $cov(l) \neq cov(r)$ constrain the result type of l and r to the type of a covariable appearing in both l and r. Among such coequations, of particular interest are those with l and r being the same up to a renaming of their covariables.

Definition 24. Let Δ denote a many-sorted cosignature, let $t \in T_\Delta[\mathscr{C}]_s$ for some set $\mathscr{C}$ of covariables and some $s \in S$, and let $\mathscr{C}' \subseteq \mathscr{C}$. The coequation: $\underline{t} = [y_1/X_1,\ldots,y_m/X_m]\underline{t}$, where $t = [Z_{i_1}/X_1,\ldots,Z_{i_m}/X_m]\underline{t}$ with $\underline{t} \in T_\Delta^1[\{X_1,\ldots,X_m\}]$, and

$$y_j = \begin{cases} X_j & \text{if } Z_{i_j} \in \mathscr{C}' \\ Y_j & \text{if } Z_{i_j} \notin \mathscr{C}' \end{cases} \quad \text{for } j = 1,\ldots,m$$

is called a *type constraint* for t and is denoted $c(t,\mathscr{C}')$.

$c(t,\mathscr{C}')$ constrains the result type of t to the type of a covariable in $\mathscr{C}'$: given a Δ-coalgebra A, $c(t,\mathscr{C}')$ holds in a state $a \in A_s$ if and only if $t_A(a) \in \iota_Z(A_{s'})$ for some $Z \in \mathscr{C}'_{s'}$. If $\mathscr{C}' = \{Z\}$, $c(t,\mathscr{C}')$ is alternatively denoted $c(t,Z)$.

Remark 25. If $t \in T^1_\Delta[\{Z_1,\dots,Z_n\}]$ and $i \in \{1,\dots,n\}$, then $c(t,Z_i)$ has the form: $t = [Y_1/Z_1,\dots,Z_i/Z_i,\dots,Y_n/Z_n]t$.

Since $\underline{t}$ is only defined up to a bijective renaming of its covariables, so are the type constraints for t. Consequently, the covariables X_i, Y_i can be arbitrarily chosen, provided that they are all distinct. This observation will be used when proving a completeness result for the satisfaction of coequations by coalgebras.

Some immediate properties of the notion of satisfaction of coequations are stated below.

Proposition 26. *Let A and B denote Δ-coalgebras, let $f : A \to B$ denote a Δ-homomorphism, and let e denote a Δ-coequation. Then*:

(1) $A \models_\Delta e$ *implies* $\mathsf{Im}(f) \models_\Delta e$.

(2) *If all the components of f corresponding to sorts of covariables appearing in e are injective, then $B \models_\Delta e$ implies $A \models_\Delta e$.*

Proof. The fact that $t_{\mathsf{Im}(f)}(f_s(a)) = [\iota_1 \circ f_{s_1},\dots,\iota_n \circ f_{s_n}](t_A(a))$ for each $s \in S$, $t \in T_\Delta[\{Z_1,\dots,Z_n\}]_s$ with $Z_1 : s_1,\dots,Z_n : s_n$ and $a \in A_s$ is used. (This is a consequence of the definition of Δ-homomorphisms.) □

As a result, the class of coalgebras satisfying a set of coequations is a *covariety*.

Definition 27. Let $\mathsf{G} : \mathsf{C} \to \mathsf{C}$ denote an arbitrary endofunctor, and let $\langle A, \alpha \rangle$ denote a G-coalgebra. A G-*subcoalgebra* of $\langle A, \alpha \rangle$ is a G-coalgebra $\langle B, \beta \rangle$ for which there exists a G-coalgebra homomorphism $b : \langle B, \beta \rangle \to \langle A, \alpha \rangle$ with $b : B \to A$ a C-monomorphism. Also, a *homomorphic image* of $\langle A, \alpha \rangle$ is a G-coalgebra $\langle C, \gamma \rangle$ for which there exists a G-coalgebra homomorphism $c : \langle A, \alpha \rangle \to \langle C, \gamma \rangle$ with $c : A \to C$ a C-epimorphism. A class of G-coalgebras is a *covariety* if and only if it is closed under subcoalgebras, homomorphic images and coproducts.

Corollary 28. *Let Δ denote a many-sorted cosignature and let E denote a set of Δ-coequations. The class of Δ-coalgebras satisfying E is a covariety.*

The fact that coequations induce predicates on the carriers of coalgebras results in the existence of largest subcoalgebras satisfying given sets of coequations. The next result provides a concrete description of such subcoalgebras.

Proposition 29. *Let Δ denote a many-sorted cosignature, let E denote a set of Δ-coequations, and let A denote an arbitrary Δ-coalgebra. The largest Δ-subcoalgebra*

A_E of A satisfying the coequations in E has its carrier given by

$$A_{E,s} = \{a \in A_s \mid l_A(t_A(a)) = r_A(t_A(a)) \textit{ whenever}$$
$$t \in T^1_\Delta[\{Z_1,\ldots,Z_n\}]_s,\ i \in \{1,\ldots,n\} \textit{ and } (l = r \textit{ if } C) \in E_{s_i}$$
$$\textit{are such that } t_A(a) \in \iota_{Z_i}(A_{s_i}) \textit{ and } C \textit{ holds in } t_A(a)\}, \quad s \in S.$$

Proof. To show that the S-sorted set $(A_{E,s})_{s\in S}$ defines a Δ-subcoalgebra of A, let $a \in A_{E,s}$ and $\delta \in \Delta_{s,s_1\ldots s_m}$. Say $\delta_A(a) \in \iota_j(A_{s_j})$ with $j \in \{1,\ldots,m\}$. Then, given $t' \in T^1_\Delta[\{Z_1,\ldots,Z_n\}]_{s_j}$ and $(l = r$ if $C) \in E$ such that C holds in $t'_A(\delta_A(a))$, taking $t = [X_1,\ldots, X_{j-1}, t', X_{j+1},\ldots,X_m]\delta$ in the definition of A_E gives $l_A(t'_A(\delta_A(a))) = r_A(t'_A(\delta_A(a)))$. That is, $\delta_A(a) \in \iota_j(A_{E,s_j})$. Also, given an arbitrary (Δ,E)-subcoalgebra A' of A, the inclusion $\iota_{A'}$ of A' into A factors through the inclusion ι_{A_E} of A_E into A. (Proposition 26 gives $\mathsf{Im}(\iota_{A'}) \models_\Delta E$, which, together with the definition of A_E, gives $\mathsf{Im}(\iota_{A'}) \subseteq A_E$.) □

3.4. An institution of many-sorted coalgebras

Definition 30. Let Δ and Δ' denote many-sorted cosignatures with sort sets S and, respectively, S'. A (*many-sorted*) *cosignature morphism* from Δ to Δ' consists of a function $\phi : S \to S'$, together with an $S \times S^+$-sorted function $(\phi_{s,w})_{s\in S, w\in S^+}$, with $\phi_{s,w} : \Delta_{s,w} \to \Delta'_{\phi(s),\phi^+(w)}$ (with ϕ^+ denoting the pointwise extension of $\phi : S \to S'$ to a function from S^+ to S'^+). The category of many-sorted cosignatures and cosignature morphisms is denoted Cosign.

Cosignature morphisms $\phi : \Delta \to \Delta'$ induce reduct functors $\mathsf{U}_\phi : \mathsf{Coalg}(\Delta') \to \mathsf{Coalg}(\Delta)$, taking Δ'-coalgebras A' to the Δ-coalgebras having carriers $A = (A'_{\phi(s)})_{s\in S}$, and operations $\delta_A(a) = \phi(\delta)_{A'}(a)$ for $s \in S$, $a \in A_s$ and $\delta \in \Delta_s$.

Proposition 31. *Let $\phi : \Delta \to \Delta'$ denote a cosignature morphism. Then, for any Δ-coalgebra C, there exists a cofree Δ'-coalgebra over C w.r.t. U_ϕ.*

Proof. The conclusion follows by instantiating a result in [2] regarding the existence of right adjoints to functors between categories of coalgebras. □

The mapping from many-sorted cosignatures to their categories of coalgebras extends to a functor $\mathsf{Coalg} : \mathsf{Cosign} \to \mathsf{Cat}^{\mathsf{op}}$. Also, the translations of sorts and operation symbols along cosignature morphisms extend to translations of coterms and hence of coequations, yielding a functor $\mathsf{Coeqn} : \mathsf{Cosign} \to \mathsf{Set}$.

Theorem 32. $(\mathsf{Cosign}, \mathsf{Coalg}, \mathsf{Coeqn}, \models)$ *is an institution.*

Proof. For a many-sorted cosignature morphism $\phi : \Delta \to \Delta'$, a Δ'-coalgebra A' and a Δ-coequation e, the fact that $\mathsf{U}_\phi A' \models_\Delta e$ is equivalent to $A' \models_{\Delta'} \phi(e)$ follows from the observation that $t_{\mathsf{U}_\phi A'} = \phi(t)_{A'}$ for any Δ-coterm t (with $\phi(t)$ denoting the translation of t along ϕ). This observation also yields $t_{\mathsf{U}_\phi A'} \in \iota_Z((\mathsf{U}_\phi A')_s)$ if and only if $\phi(t)_{A'} \in \iota_Z(A_{s'})$, for any $Z \in cov(t)$. □

This institution will be called *many-sorted coalgebra.*[7] Its specifications and specification morphisms will be referred to as *coalgebraic specifications* and, respectively, *coalgebraic specification morphisms.*

A consequence of Propositions 31 and 29 is the existence of cofree coalgebras w.r.t. the reduct functors induced by coalgebraic specification morphisms.

Proposition 33. *Let $\phi : (\Delta, E) \to (\Delta', E')$ denote a coalgebraic specification morphism. Then, for any $A \in |\mathsf{Coalg}(\Delta, E)|$, there exists $A' \in |\mathsf{Coalg}(\Delta', E')|$ cofree over A w.r.t. U_ϕ.*

Taking $(\Delta, E) = ((S, \emptyset), \emptyset)$ then yields cofree coalgebras over given S-sorted sets.

Corollary 34. *Let (Δ, E) denote a coalgebraic specification. Then, for any $C \in |\mathsf{Set}^S|$, there exists $A \in |\mathsf{Coalg}(\Delta, E)|$ cofree over C.*

Also, taking C to be final in Set^S yields a final (Δ, E)-coalgebra.

Corollary 35. *Any coalgebraic specification (Δ, E) admits a final coalgebra.*

3.5. Coalgebraic equational deduction

We are now in the position to formulate a sound and complete deduction calculus for coequations. We consider the following deduction rules:

$$[base] \qquad \frac{}{E \vdash e} \quad e \in E,$$

$$[cond] \qquad \frac{}{E \vdash c(t, \mathscr{C}) \text{ if } (t, \mathscr{C})},$$

$$[weakening] \qquad \frac{E \vdash t = t' \text{ if } C}{E \vdash t = t' \text{ if } C, C'},$$

$$[reflexivity] \qquad \frac{}{E \vdash t = t},$$

$$[symmetry] \qquad \frac{E \vdash t = t' \text{ if } C}{E \vdash t' = t \text{ if } C},$$

$$[transitivity] \qquad \frac{E \vdash t = t' \text{ if } C, \; E \vdash t' = t'' \text{ if } C}{E \vdash t = t'' \text{ if } C},$$

[7] The use of this terminology is justified by the syntactic duality w.r.t. many-sorted algebra.

$$[\mathit{closure}] \qquad \frac{E \vdash t_1 = t_1' \text{ if } C_1, \ldots, E \vdash t_n = t_n' \text{ if } C_n}{E \vdash [t_1, \ldots, t_n]\delta = [t_1', \ldots, t_n']\delta \text{ if } [C_1, \ldots, Z_n]\delta, \ldots, [Z_1, \ldots, C_n]\delta},$$

$$[\mathit{substitution}] \qquad \frac{E \vdash t = t' \text{ if } C}{E \vdash [t_1/Z_1, \ldots, t_n/Z_n]t = [t_1/Z_1, \ldots, t_n/Z_n]t' \text{ if } C},$$

$$[\mathit{contradiction}] \qquad \frac{E \vdash t = t' \text{ if } C}{E \vdash l = r \text{ if } C},$$

for $t, t' \in T_\Delta[\mathscr{C}]_s,\ cov(t) \cap cov(t') = \emptyset,\ l, r \in T_\Delta[\mathscr{C}']_s$,

$$[\mathit{case}] \qquad \frac{E \vdash t = t' \text{ if } C, (t_0, \mathscr{C}_1), \ldots, E \vdash t = t' \text{ if } C, (t_0, \mathscr{C}_n)}{E \vdash t = t' \text{ if } C},$$

for $t, t' \in T_\Delta[\mathscr{C}']_s,\ t_0 \in T_\Delta[\mathscr{C}]_s,\ \mathscr{C} = \mathscr{C}_1 \cup \cdots \cup \mathscr{C}_n$.

Proposition 36. $(\mathsf{Cosign}, \mathsf{Coeqn}, \vdash)$ *is an entailment system.*

Theorem 37 (Soundness). *Let (Δ, E) denote a coalgebraic specification and let e denote a Δ-coequation. Then, $E \vdash e$ implies $E \models_\Delta e$.*

Proof. We use induction on the structure of the proof of $E \vdash e$ to show that $E \models_\Delta e$. If the last rule applied is *base*, then $E \models_\Delta e$ follows from the definition of $A \models_\Delta E$ for a Δ-coalgebra A. If the last rule applied is *weakening*, then $E \models_\Delta t = t'$ if C, C' follows from the fact that if C, C' holds in a state $a \in A_s$ of some Δ-coalgebra A, then C holds in a. If the last rule applied is *cond* or *reflexivity*, then $E \models_\Delta e$ follows by any Δ-coalgebra (and hence any (Δ, E)-coalgebra) satisfying any coequation of form $c(t, \mathscr{C})$ if $(t, \mathscr{C})$, respectively, $t = t$. If the last rule applied is one of *symmetry*, *transitivity* or *substitution*, then $E \models_\Delta e$ follows from the induction hypothesis by using standard properties of equality. If the last rule applied is *closure*, then for any (Δ, E)-coalgebra A and any $a \in A_s$ satisfying $[C_1, \ldots, Z_n]\delta, \ldots, [Z_1, \ldots, C_n]\delta$, say $\delta_A(a) \in \iota_{Z_i}(A_{s_i})$ with $i \in \{1, \ldots, n\}$, the satisfaction of $[Z_1, \ldots, C_i, \ldots, Z_n]\delta$ by a implies the satisfaction of C_i by $\delta_A(a)$, which yields $(t_i)_A(\delta_A(a)) = (t_i')_A(\delta_A(a))$ (by the induction hypothesis); that is, $([t_1, \ldots, t_n]\delta)_A(a) = ([t_1', \ldots, t_n']\delta)_A(a)$. If the last rule applied is *contradiction*, then $E \models_\Delta l = r$ if C follows from the fact that for a (Δ, E)-coalgebra A, there are no states $a \in A_s$ satisfying C (as they would then have to satisfy $t_A(a) = t_A'(a)$). Finally, if the last rule applied is *case*, $E \models_\Delta t = t'$ if C follows from one of the conditions $(t_0, \mathscr{C}_1), \ldots, (t_0, \mathscr{C}_n)$ holding in any state $a \in A_s$ satisfying C, for any (Δ, E)-coalgebra A. □

The completeness proof requires some preliminary results.

Lemma 38. *Let Δ denote a many-sorted cosignature and let E denote a set of Δ-coequations. If $E \vdash l = r$ if $C, (t, \mathscr{C})$ and $E \vdash c(t, \mathscr{C})$ if C, C', then $E \vdash l = r$ if C, C'.*

Proof. If $\mathscr{C}' = cov(t)\backslash\mathscr{C}$, then the soundness of the *weakening* and *contradiction* rules gives $E \vdash l = r$ if $C, C', (t, \mathscr{C})$ and $E \vdash l = r$ if $C, C', (t, \mathscr{C}')$. The conclusion then follows by the soundness of the *case* rule. □

The next two lemmas will prove crucial to the completeness proof. The former states that whenever a set of coequations is inconsistent w.r.t. a given sort and a set of conditions for that sort, a contradiction for the given conditions can be syntactically derived from the coequations, while the latter states that if two coterms constrained to the same covariable cannot be proved equal under certain conditions, then the two coterms are distinguished by a state satisfying the given conditions, in a coalgebra satisfying the specification.

Lemma 39. *Let (Δ, E) denote a coalgebraic specification and let F_E denote a final (Δ, E)-coalgebra. Also, let $s \in S$ and let C denote some conditions for sort s. If $E \not\vdash l = r$ if C for any $l, r \in T_\Delta[\mathscr{C}]_s$ with $cov(l) \cap cov(r) = \emptyset$, then $F^C_{E,s} = \{\varphi \in F_{E,s} \mid C$ holds in $\varphi\} \neq \emptyset$.*

Proof. We define an ω^{op}-chain in Set whose limit object L has the following properties:
(a) $L \neq \emptyset$ implies $F^C_{E,s} \neq \emptyset$,
(b) if $L = \emptyset$ then $E \vdash l = r$ if C with $l, r \in T_\Delta[\mathscr{C}]_s$, $cov(l) \cap cov(r) = \emptyset$.
Then, $F^C_{E,s} = \emptyset$ gives $L = \emptyset$, which, in turn, gives $E \vdash l = r$ if C for some $l, r \in T_\Delta[\mathscr{C}]_s$ with $cov(l) \cap cov(r) = \emptyset$, yielding a contradiction. Hence, $F^C_{E,s} \neq \emptyset$.

We begin by recalling that the set $T^1_{\Delta,s}$ is enumerable; say $T^1_{\Delta,s} = \{t_1, t_2, \ldots\}$. We then consider the following ω^{op}-chain:

$$C_1 \xleftarrow{p_1} C_2 \xleftarrow{p_2} C_3 \xleftarrow{p_3} \cdots$$

where

$$\begin{aligned} C_n = \{(Z_{t_1}, \ldots, Z_{t_n}) \mid\ & Z_{t_i} \in cov(t_i) \text{ for } i \in \{1, \ldots, n\} \\ & E \not\vdash l = r \text{ if } C, (t_1, Z_{t_1}), \ldots, (t_n, Z_{t_n}) \\ & \text{for any } l, r \in T_\Delta[\mathscr{C}]_s \text{ with } cov(l) \cap cov(r) = \emptyset\} \end{aligned}$$

and $p_n(Z_{t_1}, \ldots, Z_{t_{n+1}}) = (Z_{t_1}, \ldots, Z_{t_n})$ for $n = 1, 2, \ldots$. A limit object L for this ω^{op}-chain is given by:

$$\begin{aligned} L = \{(Z_{t_i})_{i \in \{1,2,\ldots\}} \mid\ & E \not\vdash l = r \text{ if } C, (t_1, Z_{t_1}), \ldots, (t_n, Z_{t_n}) \\ & \text{for any } l, r \in T_\Delta[\mathscr{C}]_s \text{ with } cov(l) \cap cov(r) = \emptyset \text{ and any } n\}. \end{aligned}$$

To show (a), let $(Z_{t_i})_{i \in \{1,2,\ldots\}} \in L$, and let $\varphi : T^1_{\Delta,s} \to \bigcup\{cov(t) \mid t \in T^1_{\Delta,s}\}$ be given by $\varphi(t_i) = Z_{t_i}$ for $i = 1, 2, \ldots$.

To show that $\varphi \in F_s$, let $t_i, t_j \in T^1_{\Delta,s}$ be such that $t_j = [t'_1/Z_1, \ldots, t'_n/Z_n]t_i$. If $Z_{t_i} = Z_k$, we must show that $Z_{t_j} \in cov(t'_k)$. Suppose $Z_{t_j} \notin cov(t'_k)$. Then

$$E \vdash t_j = [t'_1/Z_1, \ldots, t'_n/Z_n]t_i$$

(following by *reflexivity*) together with

$$E \vdash t_i = [U_1/Z_1, \ldots, Z_k/Z_k, \ldots, U_n/Z_n]t_i \text{ if } C, (t_1, Z_{t_1}), \ldots, (t_i, Z_{t_i})$$

and

$$E \vdash t_j = [V_1/Z'_1, \ldots, Z_{t_j}/Z_{t_j}, \ldots, V_m/Z'_m]t_j \text{ if } C, (t_1, Z_{t_1}), \ldots, (t_j, Z_{t_j})$$

(both following by *cond* and *weakening*) yield (by *substitution* followed by *weakening* and then by *transitivity*):

$$E \vdash [V_1/Z'_1, \ldots, Z_{t_j}/Z_{t_j}, \ldots, V_m/Z'_m]t_j = [U_1/Z_1, \ldots, t'_k/Z_k, \ldots, U_n/Z_n]t_i$$
$$\text{if } C, (t_1, Z_{t_1}), \ldots, (t_N, Z_{t_N})$$

with $N = max(i, j)$. But this contradicts the definition of L, as the lhs and rhs of the last coequation have no covariable in common. Hence, $Z_{t_j} \in cov(t'_k)$.

To show that $\varphi \in F_{E,s}$, let $t \in T^1_\Delta[\{Z_1, \ldots, Z_n\}]_s$, $i \in \{1, \ldots, n\}$ and $(t_i = t'_i \text{ if } C_i) \in E$ be such that $t_F(\varphi) \in \iota_{Z_i}(F_{s_i})$, $t_i, t'_i \in T_\Delta[\mathscr{C}_i]_{s_i}$ and C_i holds in $t_F(\varphi)$. According to Proposition 29, we must show that $(t_i)_F(t_F(\varphi)) = (t'_i)_F(t_F(\varphi))$. However, by Corollary 21, it suffices to show that, for any coterms $u_1, \ldots, u_q$ of suitable sort, $l_F(\varphi)$ and $r_F(\varphi)$ are both in $\iota_Z(F_{s'})$ for some $Z : s'$, where:

$$l = [u_1/U_1, \ldots, u_q/U_q][Z_1/Z_1, \ldots, t_i/Z_i, \ldots, Z_n/Z_n]t,$$

$$r = [u_1/U_1, \ldots, u_q/U_q][Z_1/Z_1, \ldots, t'_i/Z_i, \ldots, Z_n/Z_n]t$$

with $\{U_1, \ldots, U_q\} = \mathscr{C}_i \cup \{Z_1, \ldots, Z_{i-1}, Z_{i+1}, \ldots, Z_n\}$.

Now let $l = [V_{i_1}/X_1, \ldots, V_{i_m}/X_m]\underline{l}$ with $\underline{l} \in T^1_\Delta[\{X_1, \ldots, X_m\}]_s$, and $r = [V_{j_1}/Y_1, \ldots, V_{j_p}/Y_p]\underline{r}$ with $\underline{r} \in T^1_\Delta[\{Y_1, \ldots, Y_p\}]_s$. From

$$E \vdash t_i = t'_i \text{ if } C_i$$

(following by *base*) we can infer, by successive applications of the *closure* rule, followed by *substitution*:

$$E \vdash l = r \text{ if } [Z_1/Z_1, \ldots, C_i/Z_i, \ldots, Z_n/Z_n]t.$$

We claim that if $Z_{\underline{l}} = X_k$ and $Z_{\underline{r}} = Y_l$, then $V_{i_k} = V_{j_l}$. For, if this was not the case, *cond* together with *substitution* would yield:

$$E \vdash [S_1/V_1, \ldots, V_{i_k}/V_{i_k}, \ldots, S_o/V_o]l = [T_1/V_1, \ldots, V_{j_l}/V_{j_l}, \ldots, T_o/V_o]r$$
$$\text{if } [Z_1/Z_1, \ldots, C_i/Z_i, \ldots, Z_n/Z_n]t, (\underline{l}, X_k), (\underline{r}, Y_l)$$

with $V_{i_k} \neq V_{j_l}$, which would then yield:

$$E \vdash [S_1/V_1, \ldots, V_{i_k}/V_{i_k}, \ldots, S_o/V_o]l = [T_1/V_1, \ldots, V_{j_l}/V_{j_l}, \ldots, T_o/V_o]r$$
$$\text{if } (t_1, Z_{t_1}), \ldots, (t_N, Z_{t_N})$$

for N sufficiently large (the fact that $[Z_1/Z_1, \ldots, C_i/Z_i, \ldots, Z_n/Z_n]t$ holds in φ together with Lemma 38 are used here). But this would contradict the definition of L. Hence, $V_{i_k} = V_{j_l} = Z : s'$ and $l_F(\varphi), r_F(\varphi) \in \iota_Z(F_{s'})$. This gives $\varphi \in F_{E,s}$.

In addition, $\varphi \in F^C_{E,s}$. For, if this was not the case, the conditions in C would contradict $(t_1, Z_{t_1}), \ldots, (t_N, Z_{t_N})$ for N sufficiently large (by Lemma 38), yielding $E \vdash l = r$ if $C, (t_1, Z_{t_1}), \ldots, (t_N, Z_{t_N})$ with $cov(l) \cap cov(r) = \emptyset$. This concludes the proof of (a).

To show (b), assume $L = \emptyset$. Then, for any $Z \in C_1$, there exists $n_Z \in \{2, \ldots\}$ such that $Z \notin \mathsf{Im}(p_1 \circ \cdots \circ p_{n_Z})$. For, if $Z \in C_1$ was such that $Z \in \mathsf{Im}(p_1 \circ \cdots \circ p_n)$ for any $n \in \{2, \ldots\}$, then also $Z \in \mathsf{Im}(l_1)$ (with $l_1 : L \to C_1$ denoting the corresponding arrow of the limiting cone), which would contradict the assumption that $L = \emptyset$. Now let $n' = max\{n_Z \mid Z \in C_1\}$. It then follows by *weakening* and *contradiction* that $E \vdash l = r$ if $C, (t_1, Z_1), \ldots, (t_{n'}, Z_{n'})$ for any choice of $Z_1 \in cov(t_1), \ldots, Z_{n'} \in cov(t_{n'})$, with $l, r \in T_\Delta[\mathscr{C}]_s$ being such that $cov(l) \cap cov(r) = \emptyset$. Then, successive applications of the *case* rule yield $E \vdash l = r$ if C with $l, r \in T_\Delta[\mathscr{C}]_s$ and with $cov(l) \cap cov(r) = \emptyset$, thus contradicting the hypothesis. This concludes the proof of (b). □

Lemma 40. *Let (Δ, E) denote a coalgebraic specification, let $l, r \in T_\Delta[\mathscr{C}]_s$ for some set $\mathscr{C}$ of covariables and some $s \in S$, and let $Z \in \mathscr{C}$. Also, let A_E denote a cofree (Δ, E)-coalgebra over the S-sorted set $(\{*, *'\})_{s \in S}$. If $E \not\vdash l = r$ if $C, (l, Z), (r, Z)$, then there exists $\varphi \in A^{C,(l,Z),(r,Z)}_{E,s}$ such that $l_{A_E}(\varphi) \neq r_{A_E}(\varphi)$.*

Proof. We begin by recalling that the cofree (Δ, E)-coalgebra A_E over the S-sorted set $(\{*, *'\})_{s \in S}$ has elements given by functions $\varphi : T^1_{\Delta,s} \to \bigcup\{\, cov(t) \times (\{*, *'\})_{s \in S} \mid t \in T^1_{\Delta,s}\}$, additionally satisfying:

(1) $t \in T^1_{\Delta,s}$ implies $\pi_1(\varphi(t)) \in cov(t)$;

(2) $t, t' \in T^1_{\Delta,s}$, $t' = [t_1/Z_1, \ldots, t_n/Z_n]t$ and $\pi_1(\varphi(t)) = Z_k$ imply $\pi_1(\varphi(t')) \in cov(t_k)$ and moreover, if t_k is a covariable, then $\pi_2(\varphi(t')) = \pi_2(\varphi(t))$;

(3) $(t_i)_A(t_A(\varphi)) = (t'_i)_A(t_A(\varphi))$ holds whenever $\varphi \in A_s$, $t \in T^1_\Delta[\{Z_1, \ldots, Z_n\}]_s$, $i \in \{1, \ldots, n\}$ and $(t_i = t'_i$ if $C_i) \in E$ are such that $t_A(\varphi) \in \iota_{Z_i}(A_{s_i})$, $t_i, t'_i \in T_\Delta[\mathscr{C}_i]_{s_i}$ and C_i holds in $t_A(\varphi)$, with A denoting the cofree Δ-coalgebra over $(\{*, *'\})_{s \in S}$.

(This is a consequence of Remark 17 together with Corollary 34, see also Proposition 29.)

The proof is similar to that of Lemma 39. We define an ω^{op}-chain in **Set** whose limit object is a non-empty set provided that $E \not\vdash l = r$ if $C, (l, Z), (r, Z)$, and then use an element of the limit object to construct $\varphi \in A^{C,(l,Z),(r,Z)}_{E,s}$ with $l_{A_E}(\varphi) \neq r_{A_E}(\varphi)$.

Consider the following ω^{op}-chain:

$$S_1 \xleftarrow{p_1} S_2 \xleftarrow{p_2} S_3 \xleftarrow{p_3} \cdots$$

where

$$S_n = \{(Z_{t_1},\dots,Z_{t_n}) \mid Z_{t_i} \in cov(t_i) \text{ for } i \in \{1,\dots,n\},$$
$$E \not\vdash l = r \text{ if } C,(l,Z),(r,Z),(t_1,Z_{t_1}),\dots,(t_n,Z_{t_n})\}$$

and $p_n(Z_{t_1},\dots,Z_{t_{n+1}}) = (Z_{t_1},\dots,Z_{t_n})$ for $n = 1,2,\dots$. A limit object L for this ω^{op}-chain is given by

$$L = \{(Z_{t_i})_{i\in\{1,2,\dots\}} \mid Z_{t_i} \in cov(t_i) \text{ for } i \in \{1,2,\dots\},$$
$$E \not\vdash l = r \text{ if } C,(l,Z),(r,Z),(t_1,Z_{t_1}),\dots,(t_n,Z_{t_n}) \text{ for any } n\}.$$

We claim that:
(a) $S_n \neq \emptyset$ for any $n \in \{1,2,\dots\}$,
(b) $L \neq \emptyset$.
To show (a), assume $S_n = \emptyset$ for some $n \in \{1,2,\dots\}$. That is

$$E \vdash l = r \text{ if } C,(l,Z),(r,Z),(t_1,Z_{t_1}),\dots,(t_n,Z_{t_n})$$

for any $Z_{t_i} \in cov(t_i)$ with $i = 1,\dots,n$. It then follows by *case* that:

$$E \vdash l = r \text{ if } C,(l,Z),(r,Z).$$

But this contradicts the hypothesis. Therefore $S_n \neq \emptyset$ for any $n \in \{1,2,\dots\}$.

To show (b), assume $L = \emptyset$. Hence, for any $Z \in S_1$, there exists $n_Z \in \{2,\dots\}$ such that $Z \notin \mathsf{Im}(p_1 \circ \cdots \circ p_n)$. If $n' = max\{n_Z \mid Z \in S_1\}$, it follows by *weakening* that:

$$E \vdash l = r \text{ if } C,(l,Z),(r,Z),(t_1,Z_{t_1}),\dots,(t_{n'},Z_{t_{n'}})$$

for any choice of $Z_{t_1} \in cov(t_1),\dots,Z_{t_{n'}} \in cov(t_{n'})$. Hence, by *case*

$$E \vdash l = r \text{ if } C,(l,Z),(r,Z).$$

Again, this contradicts the hypothesis. Hence, $L \neq \emptyset$.

We now fix $(Z_{t_i})_{i=1,2,\dots} \in L$ and use it to define $\varphi \in A_{E,s}^{C,(l,Z),(r,Z)}$ such that $l_{A_E}(\varphi) \neq r_{A_E}(\varphi)$. Say $\mathscr{C} = \{Z_1,\dots,Z_n\}$. Let $l = [Z_{i_1}/X_1,\dots,Z_{i_m}/X_m]\underline{l}$ for some $\underline{l} \in T_\Delta^1[\{X_1,\dots,X_m\}]_s$, and $r = [Z_{j_1}/Y_1,\dots,Z_{j_p}/Y_p]\underline{r}$ for some $\underline{r} \in T_\Delta^1[\{Y_1,\dots,Y_p\}]_s$. Also, let $k \in \{1,\dots,m\}$ be such that $X_k = Z_{\underline{l}}$, and $l \in \{1,\dots,p\}$ be such that $Y_l = Z_{\underline{r}}$. One can immediately infer that $Z_{i_k} = Z$ and $Z_{j_l} = Z$; for if, say, $Z_{i_k} \neq Z$, then the conditions (l, Z) and $(\underline{l}, X_k)$ would contradict each other, yielding:

$$E \vdash l' = r' \text{ if } C,(l,Z),(r,Z),(t_1,Z_{t_1}),\dots,(t_N,Z_{t_N})$$

with $cov(l') \cap cov(r') = \emptyset$ for N sufficiently large. Finally, for $n \in \{1,2,\dots\}$, let C_n stand for $(t_1,Z_{t_1}),\dots,(t_n,Z_{t_n})$.

Now define

$$T = \{t \in T_{\Delta,s}^1 \mid \text{there exists } n \in \{1,2,\dots\} \text{ such that}$$
$$E \vdash t = [Y_1/Y_1,\dots,Z_t/Y_l,\dots,Y_p/Y_p]\underline{r} \text{ if } C,(l,Z),(r,Z),C_n\},$$

where $\{Y_1,\ldots,Y_p\}\cap cov(t)=\emptyset$ for any $t\in T^1_{\Delta,s}$. That is, T consists of Δ-coterms whose interpretation must agree with that of $\underline{r}$ on any state in $A^{C,(l,Z),(r,Z)}_{E,s}$ which, in addition, satisfies the conditions (t_i,Z_i), with $i=1,2,\ldots$. Then let $\varphi\in A^{C,(l,Z),(r,Z)}_{E,s}$ be given by $\varphi(t)=\langle Z_t,c_t\rangle$ for $t\in T^1_{\Delta,s}$, where

$$c_t=\begin{cases} * & \text{if } t\notin T\\ *' & \text{if } t\in T\end{cases}.$$

Note that if, say, $Z:s'$, then $t\in T$ gives $Z_t:s'$ (as $Z_{\underline{r}}=Y_l:s'$).

We now claim that:
(c) $\varphi\in A^{C,(l,Z),(r,Z)}_{E,s}$,
(d) $r_{A_E}(\varphi)\neq l_{A_E}(\varphi)$.
Proving (c) reduces to proving that $\varphi\in A_{E,s}$ and that each of $C,(l,Z),(r,Z)$ holds in φ.

The proof of $\varphi\in A_s$, with A denoting the cofree Δ-coalgebra over $(\{*,*'\}_s)_{s\in S}$ is similar to the proof of $\varphi\in F_s$ in Lemma 39. In addition, here we must show that if $t_i,t_j\in T^1_{\Delta,s}$ are such that $t_j=[t'_1/Z'_1,\ldots,t'_n/Z'_n]t_i$, $Z_{t_i}=Z'_k$ and $t'_k=Z_{t_j}$, then either t_i and t_j are both in T, or none of them is in T. One can distinguish two cases:
(1) $t_i\in T$. That is:

$$E\vdash t_i=[Y_1/Y_1,\ldots,Z'_k/Y_l,\ldots,Y_m/Y_m]\underline{r}\ \text{if}\ C,(l,Z),(r,Z),C_{n_0}$$

for some $n_0\in\{1,2,\ldots\}$. Then, *substitution* yields

$$E\vdash t_j=[t'_1/Z'_1,\ldots,t'_n/Z'_n][Y_1/Y_1,\ldots,Z'_k/Y_l,\ldots,Y_m/Y_m]\underline{r}$$
$$\text{if}\ C,(l,Z),(r,Z),C_{n_0}.$$

This, together with

$$\{Z'_1,\ldots,Z'_{k-1},Z'_{k+1},\ldots,Z'_n\}\cap\{Y_1,\ldots,Y_{l-1},Y_{l+1},\ldots,Y_m\}=\emptyset$$

and $t'_k=Z_{t_j}$ yields

$$E\vdash t_j=[Y_1/Y_1,\ldots,Z_{t_j}/Y_l,\ldots,Y_m/Y_m]\underline{r}\ \text{if}\ C,(l,Z),(r,Z),C_{n_0}.$$

That is, $t_j\in T$.
(2) $t_j\in T$. That is

$$E\vdash t_j=[Y_1/Y_1,\ldots,Z_{t_j}/Y_l,\ldots,Y_m/Y_m]\underline{r}\ \text{if}\ C,(l,Z),(r,Z),C_{n_0}$$

for some $n_0\in\{1,2,\ldots\}$. Then, $t_j=[t'_1/Z'_1,\ldots,t'_n/Z'_n]t_i$ gives

$$E\vdash[t'_1/Z'_1,\ldots,t'_n/Z'_n]t_i=[Y_1/Y_1,\ldots,Z_{t_j}/Y_l,\ldots,Y_m/Y_m]\underline{r}$$
$$\text{if}\ C,(l,Z),(r,Z),C_{n_0}.$$

But $Z_{t_i} = Z'_k$ together with *substitution* and *cond* yield

$$E \vdash [t'_1/Z'_1, \ldots, t'_n/Z'_n]t_i = [Z'_1/Z'_1, \ldots, t'_k/Z'_k, \ldots, Z'_n/Z'_n]t_i \\ \text{if } C, (l, Z), (r, Z), C_N$$

for N sufficiently large. Also, $t'_k = Z_{t_j}$. Hence, by *transitivity*:

$$E \vdash [Z'_1/Z'_1, \ldots, Z_{t_j}/Z'_k, \ldots, Z'_n/Z'_n]t_i \\ = [Y_1/Y_1, \ldots, Z_{t_j}/Y_l, \ldots, Y_m/Y_m]\underline{r} \text{ if } C, (l, Z), (r, Z), C_N.$$

Finally, substituting Z_{t_i} for Z_{t_j} yields

$$E \vdash t_i = [Y_1/Y_1, \ldots, Z_{t_i}/Y_l, \ldots, Y_m/Y_m]\underline{r} \text{ if } C, (l, Z), (r, Z), C_N.$$

That is, $t_i \in T$.

Hence, either both t_i and t_j belong to T, or neither of them does, and therefore $c_{t_i} = c_{t_j}$. This concludes the proof of $\varphi \in A_s$.

The proof of $\varphi \in A_{E,s}$ is, again, similar to the proof of $\varphi \in F_{E,s}$ in Lemma 39. In addition, here we must show that given $t \in T^1_\Delta[\{Z'_1, \ldots, Z'_n\}]_s$, $i \in \{1, \ldots, n\}$ and $(t_i = t'_i \text{ if } C_i) \in E$ such that $t_A(\varphi) \in \iota_{Z'_i}(A_{s_i})$, $t_i, t'_i \in T_\Delta[\mathscr{C}_i]_{s_i}$ and C_i holds in $t_A(\varphi)$, then either both $\underline{l}'$ and $\underline{r}'$ are in T, or none of them is (where l' and r' are defined similarly to l and r from Lemma 39).

Suppose $\underline{l}' \in T$. On the one hand,

$$E \vdash l' = r' \text{ if } [Z'_1/Z'_1, \ldots, C_i/Z'_i, \ldots, Z'_n/Z'_n]t$$

(following by successive applications of the *closure* rule) together with the fact that $[Z'_1/Z'_1, \ldots, C_i/Z'_i, \ldots, Z'_n/Z'_n]t$ holds in φ yield

$$E \vdash l' = r' \text{ if } C_N$$

for N sufficiently large (Lemma 38 is used here). That is

$$E \vdash [W_{i_1}/U_1, \ldots, W_{i_q}/U_q]\underline{l}' = [W_{j_1}/V_1, \ldots, W_{j_r}/V_r]\underline{r}' \text{ if } C_N.$$

One can immediately infer that if $q_0 \in \{1, \ldots, q\}$ and $r_0 \in \{1, \ldots, r\}$ are defined by $Z_{\underline{l}'} = U_{q_0}$ and respectively $Z_{\underline{r}'} = V_{r_0}$, then $W_{i_{q_0}} = W_{j_{r_0}}$.

On the other hand, $\underline{l}' \in T$ gives

$$E \vdash \underline{l}' = [Y_1/Y_1, \ldots, Z_{l'}/Y_l, \ldots, Y_m/Y_m]\underline{r} \text{ if } C, (l, Z), (r, Z), C_{n_0}$$

for some $n_0 \in \{1, 2, \ldots\}$.

The last two statements, together with

$$E \vdash \underline{l}' = [W_{i_1}/U_1, \ldots, U_{q_0}/U_{q_0}, \ldots, W_{i_q}/U_q]\underline{l}' \text{ if } C_N$$

and

$$E \vdash \underline{r}' = [W_{j_1}/V_1, \ldots, V_{r_0}/V_{r_0}, \ldots, W_{j_r}/V_r]\underline{r}' \text{ if } C_N$$

(both following by *cond* for N sufficiently large) can then be used to infer

$$E \vdash \underline{r'} = [Y_1/Y_1, \ldots, Z_{r'}/Y_l, \ldots, Y_m/Y_m]\underline{r} \text{ if } C, (l, Z), (r, Z), C_N.$$

That is, $\underline{r'} \in T$. This concludes the proof of $\varphi \in A_{E,s}$.

It remains to prove that each of $C, (l, Z), (r, Z)$ holds in φ. If this was not the case, the condition $C, (l, Z), (r, Z), C_N$ would be contradictory for N sufficiently large, yielding $E \vdash l = r$ if $C, (l, Z), (r, Z), C_N$. This, in turn, contradicts the definition of L. We have therefore proved (c).

To prove (d), it suffices to show that $\underline{l} \notin T$. Then, since $\underline{r} \in T$, the claim follows from $* \neq *'$. We show that $\underline{l} \in T$ yields a contradiction. If $\underline{l} \in T$, then

$$E \vdash \underline{l} = [Y_1/Y_1, \ldots, X_k/Y_l, \ldots, Y_m/Y_m]\underline{r} \text{ if } C, (l, Z), (r, Z), C_{n_0}$$

for some $n_0 \in \{1, 2, \ldots\}$. This, together with

$$E \vdash l = [X_1/X_1, \ldots, Z/X_k, \ldots, X_m/X_m]\underline{l} \text{ if } C_N$$

and

$$E \vdash r = [Y_1/Y_1, \ldots, Z/Y_l, \ldots, Y_p/Y_p]\underline{r} \text{ if } C_N$$

for N sufficiently large (both following by *transitivity* and *cond*) can then be used to infer

$$E \vdash l = r \text{ if } C, (l, Z), (r, Z), C_N$$

for N sufficiently large. But this contradicts the fact that $(Z_{t_i})_{i=1,2,\ldots} \in L$. Hence, $\underline{l} \notin T$. This concludes the proof of (d).

We have therefore constructed $\varphi \in A_{E,s}$ such that $C, (l, Z), (r, Z)$ holds in φ, but $r_{A_E}(\varphi) \neq l_{A_E}(\varphi)$. This concludes the proof. □

Theorem 41 (Completeness). *Let (Δ, E) denote a coalgebraic specification and let e denote a Δ-coequation. Then, $E \models_\Delta e$ implies $E \vdash e$.*

Proof. Let e be of form $l = r$ if C with $l, r \in T_\Delta[\mathscr{C}]_s$, let F_E denote a final (Δ, E)-coalgebra, and let A_E denote a cofree (Δ, E)-coalgebra over the S-sorted set $(\{*, *'\})_{s \in S}$. We distinguish the following cases.

(1) $F^C_{E,s} = \emptyset$. Then, $E \vdash e$ follows immediately by Lemma 39.

(2) $F^C_{E,s} \neq \emptyset$. We assume that $E \not\vdash e$ and show that this yields a contradiction. From $E \not\vdash e$ one can immediately infer that there exist $Z \in \mathscr{C}_{s'}$ and $Z' \in \mathscr{C}_{s''}$ with $s', s'' \in S$ such that $E \not\vdash l = r$ if $C, (l, Z), (r, Z')$ (otherwise $E \vdash l = r$ if C would follow by *case*). We now distinguish two sub-cases.

   (a) $Z \neq Z'$. We have: $E \not\vdash l' = r'$ if $C, (l, Z), (r, Z')$ for any $l', r' \in T_\Delta[\mathscr{C}']_s$ with $cov(l') \cap cov(r') = \emptyset$ (otherwise *contradiction* could be applied to infer $E \vdash l = r$ if $C, (l, Z), (r, Z')$). Lemma 39 then gives $\varphi \in F_{E,s}$ such that $C, (l, Z), (r, Z')$ holds in φ. That is, φ satisfies the conditions C but $l_{F_E}(\varphi) \neq r_{F_E}(\varphi)$

(as $l_{F_E}(\varphi) \in \iota_Z(F_{E,s'})$ and $r_{F_E}(\varphi) \in \iota_{Z'}(F_{E,s''})$, with $Z \neq Z'$). Hence, $F_E \not\models_\Delta l = r$ if C.

(b) $Z = Z'$. Since $E \nvdash l = r$ if $C, (l, Z), (r, Z)$, it follows by Lemma 40 that there exists $\varphi \in A_{E,s}$ such that $C, (l, Z), (r, Z)$ holds in φ but $l_{A_E}(\varphi) \neq r_{A_E}(\varphi)$. Hence, $A_E \not\models_\Delta l = r$ if C.

In both of the above sub-cases one can infer that $E \not\models_\Delta e$, which contradicts the hypothesis. Hence, $E \vdash e$.

This concludes the proof of completeness. □

Example 42. Given the cosignature in Example 9, the fact that:

$$E \vdash \texttt{[Z,L]rest} = \texttt{[Z}'\texttt{,L]rest}$$

with

$$E = \{\texttt{[Z,[Z,E]first]rest} = \texttt{[Z}'\texttt{,E]first}\},$$

follows by *case-analysis* from

$$E \vdash \texttt{[Z,L]rest} = \texttt{[Z}'\texttt{,L]rest if ([Z,L]rest,L)},$$

following directly by *cond*, together with

$$E \vdash \texttt{[Z,L]rest} = \texttt{[Z}'\texttt{,L]rest if ([Z,L]rest,Z)},$$

following by *contradiction* from

$$E \vdash \texttt{[Z,[Z,E]first]rest} = \texttt{[Z}'\texttt{,E}'\texttt{]first if ([Z,L]rest,Z)}.$$

The last statement follows by *transitivity* from

$$E \vdash \texttt{[Z,[Z,E]first]rest} = \texttt{[Z,[Z,E}'\texttt{]first]rest if ([Z,L]rest,Z)},$$

following by *cond* and *substitution*, together with

$$E \vdash \texttt{[Z,[Z,E}'\texttt{]first]rest} = \texttt{[Z}'\texttt{,E}'\texttt{]first if ([Z,L]rest,Z)},$$

following by *base* and *weakening*.

4. Coalgebraic specification over a data universe

This section extends the approach in the previous section in order to account for the availability of a fixed data universe when specifying observational properties of systems. A sound and complete deduction calculus for reasoning about such properties is obtained by extending the deduction calculus of many-sorted coalgebra (see Section 3.5) with a rule that accounts for the data universe being fixed. Throughout this section, V denotes a set of *visible sorts*, while D denotes a V-sorted set (of data values). Furthermore, it is assumed that $D_v \neq \emptyset$ for each $v \in V$.

4.1. Destructor cosignatures

Definition 43. A *destructor cosignature over* V is a pair (H, Δ) with H a set of *hidden sorts* and Δ a $V \cup H$-sorted cosignature such that $\Delta_v = \emptyset$ for $v \in V$. A *cosignature morphism* between destructor cosignatures (H, Δ) and (H', Δ') over V is a many-sorted cosignature morphism $\phi : (V \cup H, \Delta) \to (V \cup H', \Delta')$ such that $\phi \restriction_V = 1_V$ and such that $\phi(H) \subseteq H'$. The category of destructor cosignatures over V and cosignature morphisms is denoted Cosign_V.

Whenever possible, destructor cosignatures (H, Δ) over V are abbreviated Δ, while the set $V \cup H$ is denoted S.

Example 44. The many-sorted cosignature in Example 9 can be regarded as a destructor cosignature over `1` and `Elt`.

4.2. Coalgebras, finality and bisimilarity

Definition 45. Let Δ denote a destructor cosignature over V. A *Δ_D-coalgebra* is a many-sorted Δ-coalgebra A such that $A_v = D_v$ for each $v \in V$. Also, a *Δ_D-homomorphism* between Δ_D-coalgebras A and B is a many-sorted Δ-homomorphism $f : A \to B$ such that $f_v = 1_{D_v}$ for each $v \in V$. The category of Δ_D-coalgebras and Δ_D-homomorphisms is denoted $\mathsf{Coalg}_D(\Delta)$.

Destructor cosignature morphisms $\phi : \Delta \to \Delta'$ induce reduct functors $\mathsf{U}_\phi : \mathsf{Coalg}_D(\Delta') \to \mathsf{Coalg}_D(\Delta)$ in the usual way.

Example 46. Given the destructor cosignature in Example 44, fixing the interpretation of `1` and `Elt` to $\{*\}$ and, respectively, $\mathbb{N}$ results in the coalgebras of this cosignature implementing finite and infinite lists of natural numbers.

The next result relates coalgebras of destructor cosignatures with coalgebras of endofunctors induced by such cosignatures.

Proposition 47. *Let Δ denote a destructor cosignature, let Set_D^S denote the category of S-sorted sets whose V-sorted components are given by D and S-sorted functions whose V-sorted components are given by 1_D, and let $\mathsf{G}_\Delta : \mathsf{Set}_D^S \to \mathsf{Set}_D^S$ be given by*

$$(\mathsf{G}_\Delta X)_s = \begin{cases} D_s & \text{if } s \in V, \\ \prod_{\delta \in \Delta_{s, s_1 \ldots s_n}} (X_{s_1} + \cdots + X_{s_n}) & \text{if } s \in H \end{cases}$$

for $X \in |\mathsf{Set}_D^S|$ and $s \in S$. Then, $\mathsf{Coalg}_D(\Delta)$ and $\mathsf{Coalg}(\mathsf{G}_\Delta)$ are isomorphic.

Proof. Δ_D-coalgebras A induce Set_D^S-arrows $\alpha : A \to \mathsf{G}_\Delta A$ (whose h-component maps $a \in A_h$ to $(\delta_A(a))_{\delta \in \Delta_{h, s_1 \ldots s_n}}$ for each $h \in H$) and conversely, any such Set_D^S-arrow defines a Δ_D-coalgebra structure on its domain. □

Proposition 47 results in the existence of final and cofree coalgebras. Such coalgebras can alternatively be obtained as cofree many-sorted coalgebras over suitably chosen sorted sets.

Proposition 48. *Let Δ denote a destructor cosignature over V, let $C \in |\mathsf{Set}_D^S|$, and let A denote the cofree many-sorted Δ-coalgebra over C. Then, A defines a cofree Δ_D-coalgebra over C.*

Proof. The fact that $\Delta_v = \emptyset$ for $v \in V$ ensures that A defines a Δ_D-coalgebra. Cofreeness of A in $\mathsf{Coalg}_D(\Delta)$ follows from its cofreeness w.r.t. the functor taking many-sorted Δ-coalgebras to their carrier. □

Taking C to be final in Set_D^S yields a final Δ_D-coalgebra.

Corollary 49. *Let Δ denote a destructor cosignature over V, and let $C \in |\mathsf{Set}_D^S|$ be given by $C_v = D_v$ for $v \in V$, and $C_h = \{*\}$ for $h \in H$. The carrier of the final Δ_D-coalgebra is given by*

$$\begin{aligned}F_h = \Big\{ \varphi : T^1_{\Delta,h} \to \bigcup \{ cov(t) \times C \mid t \in T^1_{\Delta,h} \} \mid\ & t \in T^1_{\Delta,h} \Rightarrow \pi_1(\varphi(t)) \in cov(t),\\ & t, t' \in T^1_{\Delta,h},\ t' = [t_1/Z_1, \ldots, t_n/Z_n]t,\ \pi_1(\varphi(t)) = Z_k \Rightarrow \pi_1(\varphi(t')) \in cov(t_k)\\ & \text{and moreover, if } t_k \text{ is a covariable then } \pi_2(\varphi(t')) = \pi_2(\varphi(t)) \Big\}, \quad h \in H\end{aligned}$$

$$F_v = D_v, \quad v \in V.$$

The notion of bisimilarity induced by destructor cosignatures is finer than the one induced by their underlying many-sorted cosignatures – the visible components of bisimilarity relations are equality relations, as opposed to universal relations. As far as the hidden components of bisimilarity relations are concerned, a characterisation similar to the one in Proposition 19 can be given.

Proposition 50. *Let Δ denote a destructor cosignature over V and let A denote a Δ_D-coalgebra. Then, given $h \in H$, two states $a, a' \in A_h$ are bisimilar if and only if for any $t \in T^1_{\Delta,h}$, there exists $Z \in cov(t)_s$ with $s \in S$ such that $t_A(a), t_A(a') \in \iota_Z(A_s)$ and moreover, $t_A(a) = t_A(a')$ if $s \in V$.*

Corollary 51. *Let Δ denote a destructor cosignature over V, let F denote a final Δ_D-coalgebra and let $l, r \in T_\Delta[\{Z_1, \ldots, Z_n\}]_h$ with $Z_1 : s_1, \ldots, Z_n : s_n$ and $h \in H$. Then, for $\varphi \in F_h$, $l_F(\varphi) = r_F(\varphi)$ if and only if for any $t_i \in T^1_{\Delta,s_i}$ for $i = 1, \ldots, n$, $([t_1/Z_1, \ldots, t_n/Z_n]l)_F(\varphi)$ and $([t_1/Z_1, \ldots, t_n/Z_n]r)_F(\varphi)$ are both in $\iota_Z(F_s)$ for some $Z : s$ and $s \in S$ and moreover, $([t_1/Z_1, \ldots, t_n/Z_n]l)_F(\varphi) = ([t_1/Z_1, \ldots, t_n/Z_n]r)_F(\varphi)$ if $s \in V$.*

Example 52. The notion of bisimilarity induced by the destructor cosignature in Example 44 relates two elements of sort `List` if and only if they denote lists with the same number of elements as well as with the same elements.

4.3. An institution of D-coalgebras

The fact that destructor cosignatures and their morphisms are suitably restricted many-sorted cosignatures and, respectively, cosignature morphisms, and that the coalgebras of destructor cosignatures are suitably restricted coalgebras of the underlying many-sorted cosignatures automatically yields an institution w.r.t. the satisfaction of many-sorted coequations of hidden sort.

Theorem 53. *Let* $\mathsf{Coalg}_D : \mathsf{Cosign}_V \to \mathsf{Cat}^{\mathsf{op}}$ *denote the functor taking destructor cosignatures to their categories of coalgebras, and* $\mathsf{HCoeqn} : \mathsf{Cosign}_V \to \mathsf{Set}$ *denote the functor taking destructor cosignatures to their sets of hidden coequations. Then,* $\mathscr{C}oalg_D = (\mathsf{Cosign}_V, \mathsf{Coalg}_D, \mathsf{HCoeqn}, \models)$ *is an institution.*

The specifications and specification morphisms of this institution will be referred to as *destructor specifications* and *destructor specification morphisms*.

Given a destructor specification (Δ, E) together with a Δ_D-coalgebra A, the largest many-sorted Δ-subcoalgebra of A satisfying E defines a Δ_D-coalgebra. This results in the existence of final coalgebras of destructor specifications, as well as of cofree coalgebras along destructor specification morphisms.

The final coalgebra of a destructor specification has the property that it satisfies precisely those coequations in visible-sorted covariables which are semantic consequences of the coequations in the specification.

Proposition 54. *Let* (Δ, E) *denote a destructor specification, let* F_E *denote a final* (Δ_D, E)*-coalgebra, and let* e *denote a* Δ*-coequation in visible-sorted covariables. Then,* $E \models_\Delta e$ *if and only if* $F_E \models_\Delta e$.

Proof. The *if* direction follows from 2 of Proposition 26 (the visible-sorted components of any Δ_D-homomorphism, and hence also of the unique Δ_D-homomorphisms into the final (Δ_D, E)-coalgebra, are injective), while the *only if* direction follows from $E \models_\Delta e$ together with $F_E \models_\Delta E$. □

4.4. Deduction

The deduction rules of many-sorted coalgebra are sound for the satisfaction of hidden coequations by coalgebras of destructor specifications. However, in order to derive a completeness result, additional deduction rules are required. It turns out that adding the following rule:

$$[unity] \quad \frac{}{E \vdash t = t' \text{ if } (t, Z), (t', Z)} \quad Z : v,\ |D_v| = 1$$

(inspired by a rule in [3]) to the deduction calculus in Section 3.5 yields a calculus which is both sound and complete for the satisfaction of coequations by coalgebras of destructor specifications.

Theorem 55 (Soundness). *The deduction calculus obtained by adding the* unity *rule to the deduction calculus of many-sorted coalgebra is sound for the satisfaction of Δ-coequations by (Δ_D, E)-coalgebras.*

Proof. Soundness of the deduction rules of many-sorted coalgebra follows from Theorem 37 together with the fact that any (Δ_D, E)-coalgebra is a (many-sorted) (Δ, E)-coalgebra. Also, soundness of the *unity* rule follows from the fact that if $Z : v$ and $|D_v| = 1$, then $t_A(a) = t'_A(a)$ holds whenever $t_A(a), t'_A(a) \in \iota_Z(D_v)$, for any Δ_D-coalgebra A and any $a \in A_s$. □

The completeness proof follows the same line as in the many-sorted case.

Lemma 56. *Let (Δ, E) denote a destructor specification and let F_E denote a final (Δ_D, E)-coalgebra. Also, let $h \in H$ and let C denote some conditions for sort h. If $E \not\vdash l = r$ if C for any $l, r \in T_\Delta[\mathscr{C}]_h$ with $cov(l) \cap cov(r) = \emptyset$, then $F^C_{E,h} \neq \emptyset$.*

Proof. We begin by noting that F_E is isomorphic to the many-sorted, cofree (Δ, E)-coalgebra over the S-sorted set C given by: $C_v = D_v$ for $v \in V$, and $C_h = \{*\}$ for $h \in H$.

The proof is now similar to the proof of Lemma 39. We show that $F^C_{E,h}$ has a surjective mapping into the limit object L of the ω^{op}-chain defined in Lemma 39. Specifically, we show that $\varphi \in F^C_{E,h} \mapsto (\pi_1(\varphi(t_i)))_{i \in \{1,2,\ldots\}} \in L$ defines a surjective mapping from $F^C_{E,h}$ to L. Then, $F^C_{E,h} = \emptyset$ gives $L = \emptyset$, which, by the proof of Lemma 39, gives $E \vdash l = r$ if C for some $l, r \in T_\Delta[\mathscr{C}]$ with $cov(l) \cap cov(r) = \emptyset$, thus contradicting the hypothesis.

For the above mapping to be correctly defined, $(\pi_1(\varphi(t_i)))_{i \in \{1,2,\ldots\}} \in L$ must hold for each $\varphi \in F^C_{E,h}$. If this was not the case for some $\varphi \in F^C_{E,h}$, then $E \vdash l = r$ if $C, (t_1, Z_{t_1}), \ldots, (t_n, Z_{t_n})$ for some $l, r \in T_\Delta[\mathscr{C}]_h$ with $cov(l) \cap cov(r) = \emptyset$ and some $n \in \{1, 2, \ldots\}$ would contradict the soundness of $\vdash$ (as both C and each (t_i, Z_{t_i}) with $i = 1, \ldots, n$ hold in $\varphi \in F^C_{E,h}$, whereas $l = r$ does not). Hence, $(\pi_1(\varphi(t_i)))_{i \in \{1,2,\ldots\}} \in L$ for each $\varphi \in F^C_{E,h}$.

To show that the mapping $\varphi \mapsto (Z_{t_i})_{i \in \{1,2,\ldots\}}$ is surjective, we fix $c_s \in C_s$ for each $s \in S$. Then, given $(Z_{t_i})_{i \in \{1,2,\ldots\}} \in L$, we let $\varphi \in F^C_{E,h}$ be given by $\varphi(t_i) = \langle Z_{t_i}, c_{t_i} \rangle$ for $i = 1, 2, \ldots$, with $c_{t_i} = c_{s_i}$ if $Z_{t_i} : s_i$, for $i = 1, 2, \ldots$.

The proof of $\varphi \in F^C_{E,h}$ is based on the proof of $\varphi \in F^C_{E,s}$ in Lemma 39. First, given $t_i, t_j \in T^1_{\Delta,h}$ with $t_j = [t'_1/Z_1, \ldots, t'_n/Z_n]t_i$ and with $Z_{t_i} = Z_k$, the proof of Lemma 39 gives $Z_{t_j} \in cov(t'_k)$. Moreover, if $t'_k = Z_{t_j}$ then $s_i = s_j$, and hence $c_{t_i} = c_{t_j}$. Next, given $t \in T^1_\Delta[\{Z_1, \ldots, Z_n\}]_h$, $i \in \{1, \ldots, n\}$ and $(t_i = t'_i$ if $C_i) \in E$ such that $t_F(\varphi) \in \iota_{Z_i}(F_{s_i})$, $t_i, t'_i \in T_\Delta[\mathscr{C}_i]_{s_i}$ and C_i holds in $t_F(\varphi)$, and given coterms $u_1, \ldots, u_q$ of suitable sort, the proof of Lemma 39 gives $l_F(\varphi), r_F(\varphi) \in \iota_Z(F_s)$ for some $Z : s$. Moreover, $l_F(\varphi) = r_F(\varphi)$, as both are equal to c_s. Hence, $\varphi \in F_{E,h}$. The proof of Lemma 39 also gives $\varphi \in F^C_{E,h}$.

Hence, $F^C_{E,h}$ has a surjective mapping into L. This concludes the proof. □

Lemma 57. *Let (Δ, E) denote a destructor specification, let $l, r \in T_\Delta[\mathscr{C}]_h$ for some set $\mathscr{C}$ of covariables and some $h \in H$, and let $Z \in \mathscr{C}$. Also, let A_E denote a cofree (Δ_D, E)-coalgebra over the S-sorted set $C \in |\mathsf{Set}_D^S|$ given by*: $C_v = D_v$ *for* $v \in V$, *and* $C_h = \{*, *'\}$ *for* $h \in H$. *If* $E \not\vdash l = r$ *if* $C, (l, Z), (r, Z)$, *then there exists* $\varphi \in A_{E,h}^{C,(l,Z),(r,Z)}$ *such that* $l_{A_E}(\varphi) \neq r_{A_E}(\varphi)$.

Proof. Again, we use the fact that A_E is isomorphic to the (many-sorted) cofree (Δ, E)-coalgebra over C.

Say $Z : s$ with $s \in S$. One can immediately infer that $s \in V$ implies $|D_s| > 1$ (otherwise *unity* together with *weakening* would yield $E \vdash l = r$ if $C, (l, Z), (r, Z)$). Let $c_s, c_s' \in C_s$ be such that $c_s \neq c_s'$.

The proof is now similar to the proof of Lemma 40. An element of the limit object L of the ω^{op}-chain defined in Lemma 40 is used to construct $\varphi \in A_{E,h}^{C,(l,Z),(r,Z)}$ with $l_{A_E}(\varphi) \neq r_{A_E}(\varphi)$, under the assumption that $E \not\vdash l = r$ if $C, (l, Z), (r, Z)$. Specifically, given $(Z_{t_i})_{i=1,2,\ldots} \in L$, $\varphi \in A_{E,h}^{C,(l,Z),(r,Z)}$ is given by $\varphi(t) = \langle Z_t, c_t \rangle$ for $t \in T_{\Delta,h}^1$, where

$$c_t = \begin{cases} c_s & \text{if } t \notin T,\ Z_t : s, \\ c_s' & \text{if } t \in T,\ Z_t : s \end{cases}$$

and where T is defined as in Lemma 40.

The proof of $\varphi \in A_{E,h}^{C,(l,Z),(r,Z)}$ is similar to the proof of $\varphi \in A_{E,s}^{C,(l,Z),(r,Z)}$ in Lemma 40. Lemma 40 also gives $l_{A_E}(\varphi) \neq r_{A_E}(\varphi)$. This concludes the proof. □

Theorem 58 (Completeness). *The deduction calculus obtained by adding the* unity *rule to the deduction calculus of many-sorted coalgebra is complete for the satisfaction of coequations by coalgebras of destructor specifications.*

Proof. Let (Δ, E) denote a destructor specification, and let e denote a Δ-coequation such that $E \models_\Delta e$. Also, let F_E denote a final (Δ_D, E)-coalgebra, and let A_E denote a cofree (Δ_D, E)-coalgebra over the S-sorted set C defined in Lemma 57. The proof of $E \vdash e$ is similar to the corresponding proof in Theorem 41. If $F_{E,h}^C = \emptyset$, then $E \vdash e$ follows by Lemma 56. Also, if $F_{E,h}^C \neq \emptyset$, Lemma 56 and, respectively, Lemma 57 are used to show that the assumption that $E \not\vdash e$ yields a contradiction. □

Example 59. Consider the specification of lists given in Example 44 (regarded as a destructor specification with visible sorts `1` and `Elt`), and let E consist of the two coequations defining the list invariant. Provided that the sort `1` is interpreted by D as a one-element set, one can show that the following holds:

$$E \vdash \texttt{[Z,E]first} = \texttt{[Z,L]rest if ([Z,E]first,Z)}.$$

This follows by *case-analysis* from

$$E \vdash \texttt{[Z,E]first} = \texttt{[Z,L]rest if ([Z,E]first,Z),([Z,L]rest,Z)},$$

$$E \vdash \texttt{[Z,E]first} = \texttt{[Z,L]rest if ([Z,E]first,Z),([Z,L]rest,L)}$$

with the first statement following by *unity* (as $\mathtt{Z} : \mathtt{1}$), and with the second statement following by *contradiction* from

$$E \vdash \mathtt{[Z,L]rest} = \mathtt{[Z',L']rest\ if\ ([Z,E]first,Z),([Z,L]rest,L)}.$$

The last statement follows by *transitivity* from:

$$E \vdash \mathtt{[Z,L]rest} = \mathtt{[Z,L']rest\ if\ ([Z,E]first,Z),([Z,L]rest,L)}$$

(following by *base* and *weakening*), and:

$$E \vdash \mathtt{[Z,L]rest} = \mathtt{[Z',L]rest\ if\ ([Z,E]first,Z),([Z,L]rest,L)}$$

(following by *cond* and *weakening*).

4.5. Abstracting away bisimilar states

The standard notion of satisfaction of coequations (see Section 3.3) may prove restrictive in cases where one's interest is to only specify system properties up to indistinguishability by observations yielding visible results. In such cases, a notion of satisfaction of coequations up to bisimulation appears to be more appropriate.

Definition 60. Let Δ denote a destructor cosignature over V, and let e denote a Δ-coequation of form $l = r$ if $(t_1, \mathscr{C}'_1), \ldots, (t_n, \mathscr{C}'_n)$. A Δ_D-coalgebra A is said to *satisfy e up to bisimulation* (written $A \models^{\mathsf{b}}_{\Delta} e$) if and only if, whenever $a \in A_h$ is such that $(t_i)_A(a) \in \iota_{Z_i}(A_{s_i})$ for some $Z_i \in (\mathscr{C}'_i)_{s_i}$, for $i = 1, \ldots, n$, it follows that $l_A(a), r_A(a) \in \iota_Z(A_{s'})$ for some $Z \in cov(l) \cap cov(r)$, $Z : s'$ and moreover, $l_A(a) \sim_A r_A(a)$ (with $\sim_A$ denoting Δ_D-bisimilarity on A).

Example 61. The coequation

$$\mathtt{[Z,[Z,L]rest]rest} = \mathtt{L\ if\ ([Z,[Z,L]rest]rest,L)}$$

holds, up to bisimulation, in all coalgebras satisfying the specification of alternating lists in Example 23.

Versions of the results in Section 3.3 can also be formulated for the notion of satisfaction of coequations up to bisimulation. In particular, Proposition 26, and consequently Corollary 28 hold. Moreover, no restriction on the homomorphism f is required by 2 of Proposition 26.

For coalgebras that are extensional, the notion of satisfaction of coequations up to bisimulation coincides with the standard notion of satisfaction. This results in the final coalgebra of a destructor specification (Δ, E) also defining a final object for the full subcategory of $\mathsf{Coalg}_D(\Delta)$ whose objects satisfy E up to bisimulation. Furthermore, a more general version of Proposition 54 holds for the satisfaction of coequations up to bisimulation.

Proposition 62. *Let (Δ, E) denote a destructor specification, let F_E denote a final (Δ_D, E)-coalgebra, and let e denote a Δ-coequation. Then, $E \models^{\mathsf{b}}_{\Delta} e$ if and only if $F_E \models_{\Delta} e$.*

Proof. The *if* direction follows from the fact that coalgebra homomorphisms (in particular, homomorphisms into the final (Δ_D, E)-coalgebra) reflect bisimulations, while the *only if* direction follows from $F_E \models^{\mathsf{b}}_{\Delta} E$. □

The deduction calculus in Section 4.4 is sound for the satisfaction up to bisimulation of arbitrary coequations, and complete for the satisfaction up to bisimulation of coequations with no hidden-sorted covariables.

Theorem 63. *Let (Δ, E) denote a destructor specification and let e denote a Δ-coequation. Then, the following hold:*
(1) *$E \vdash e$ implies $E \models^{\mathsf{b}}_{\Delta} e$.*
(2) *$E \models^{\mathsf{b}}_{\Delta} e$ implies $E \vdash e$ if e contains no hidden-sorted covariables.*

Proof. Soundness of $\vdash$ for $\models^{\mathsf{b}}$ follows from the soundness of $\vdash$ for $\models$, after observing that $A \models^{\mathsf{b}}_{\Delta} e$ is equivalent to $A/_{\sim_A} \models_{\Delta} e$ for any Δ_D-coalgebra A. Completeness of $\vdash$ for the satisfaction of coequations with no hidden-sorted covariables follows from the completeness of $\vdash$ for $\models$, together with $E \models^{\mathsf{b}}_{\Delta} e$ being equivalent to $E \models_{\Delta} e$ in the case when all the covariables appearing in e are visible-sorted. □

5. Expressiveness of the approach

The fact that the components of arbitrary polynomial endofunctors on Set^S (i.e. endofunctors whose components are constructed from constant and projection functors using finite products and coproducts) can be written as coproducts of finite products of projection functors[8] results in the class of algebraic structures specifiable with many-sorted signatures being isomorphic to the class of algebras of polynomial endofunctors. Characterising the class of coalgebraic structures specifiable with many-sorted cosignatures (or, equivalently, with polynomial endofunctors whose components have the form of products of finite coproducts of projection functors) is not as straightforward as in the case of many-sorted signatures, as, on the one hand, coproducts do not distribute over products in Set, and on the other hand, constant functors can not be written as products of finite coproducts of projection functors. In this case, a change in the underlying category is required to transform an arbitrary polynomial endofunctor into the an endofunctor having the form of a product of finite coproducts of constant/projection functors, in such a way that the categories of coalgebras of the two endofunctors are isomorphic. Furthermore, this also holds for *shape extended* polynomial endofunctors

[8] This is a consequence of the distributivity of products over coproducts in Set, on the one hand, and of the existence of a Set-theoretic isomorphism $C \simeq \coprod_{c \in C} 1$ with C an arbitrary set and 1 a one-element set, on the other.

(i.e. endofunctors whose components are constructed from constant and projection functors using finite products and coproducts, and exponentials with constant exponent).

Theorem 64. *Let* $\mathsf{T} : \mathsf{Set}^S \to \mathsf{Set}^S$ *denote an extended polynomial endofunctor, such that all the sets appearing as exponents in* T *are enumerable.*[9] *Then,* $\mathsf{Coalg}(\mathsf{T}) \simeq \mathsf{Coalg}(\mathsf{G_T})$ *for some endofunctor* $\mathsf{G_T} : \mathsf{Set}^{S_\mathsf{T}} \to \mathsf{Set}^{S_\mathsf{T}}$ *whose components are products of finite coproducts of constant/projection functors.*

Proof. We define $S_\mathsf{T} \in |\mathsf{Set}|$ and $\mathsf{G_T} : \mathsf{Set}^{S_\mathsf{T}} \to \mathsf{Set}^{S_\mathsf{T}}$ by structural induction on the components of T.

For $\mathsf{F} : \mathsf{Set}^S \to \mathsf{Set}$ an extended polynomial functor, we let $S_\mathsf{F} \in |\mathsf{Set}|$, $\mathsf{G_F} : \mathsf{Set}^{S+S_\mathsf{F}} \to \mathsf{Set}$ and $(\mathsf{F}_{s'})_{s' \in S_\mathsf{F}}$ with $\mathsf{F}_{s'} : \mathsf{Set}^{S+S_\mathsf{F}} \to \mathsf{Set}$ for $s' \in S_\mathsf{F}$ be defined as follows:

(1) if $\mathsf{F} = \Pi_s$ for some $s \in S$ or if $\mathsf{F} = A$, then:

(a) $S_\mathsf{F} = \emptyset$,

(b) $\mathsf{G_F} = \mathsf{F}$

(F is already of the required form.)

(2) if $\mathsf{F} = \mathsf{F}_1 \times \mathsf{F}_2$, then:

(a) $S_\mathsf{F} = S_{\mathsf{F}_1} + S_{\mathsf{F}_2}$,

(b) $\mathsf{G_F} = (\mathsf{G}_{\mathsf{F}_1}\Pi_1)(\mathsf{G}_{\mathsf{F}_2}\Pi_2)$,

(c) $\mathsf{F}_{s'} = \begin{cases} (\mathsf{F}_1)_{s_1}\Pi_1 & \text{if } s' = \iota_1(s_1) \text{ for some } s_1 \in S_{\mathsf{F}_1}, \\ (\mathsf{F}_2)_{s_2}\Pi_2 & \text{if } s' = \iota_2(s_2) \text{ for some } s_2 \in S_{\mathsf{F}_2}, \end{cases}$

where for $i \in \{1,2\}$, $\Pi_i : \mathsf{Set}^{S+S_\mathsf{F}} \to \mathsf{Set}^{S+S_{\mathsf{F}_i}}$ denotes the projection functor induced by the injection $S + S_{\mathsf{F}_i} \rightarrowtail S + S_\mathsf{F}$. (Again, F is already of the required form provided that F_1 and F_2 are.)

(3) if $\mathsf{F} = \mathsf{F}_1 + \mathsf{F}_2$, then

(a) $S_\mathsf{F} = S_{\mathsf{F}_1} + S_{\mathsf{F}_2} + \{s_1'\} + \{s_2'\}$,

(b) $\mathsf{G_F} = \Pi_1' + \Pi_2'$,

(c) $\mathsf{F}_{s'} = \begin{cases} (\mathsf{F}_1)_{s_1}\Pi_1 & \text{if } s' = \iota_1(s_1) \text{ for some } s_1 \in S_{\mathsf{F}_1}, \\ (\mathsf{F}_2)_{s_2}\Pi_2 & \text{if } s' = \iota_2(s_2) \text{ for some } s_2 \in S_{\mathsf{F}_2}, \\ \mathsf{G}_{\mathsf{F}_1}\Pi_1 & \text{if } s' = \iota_3(s_1'), \\ \mathsf{G}_{\mathsf{F}_2}\Pi_2 & \text{if } s' = \iota_4(s_2'), \end{cases}$

where, for $i \in \{1,2\}$, $\Pi_i : \mathsf{Set}^{S+S_\mathsf{F}} \to \mathsf{Set}^{S+S_{\mathsf{F}_i}}$ denotes the projection functor induced by the injection $S + S_{\mathsf{F}_i} \rightarrowtail S + S_\mathsf{F}$, while $\Pi_i' : \mathsf{Set}^{S+S_\mathsf{F}} \to \mathsf{Set}$ denotes the projection functor induced by the injection $\{s_i'\} \rightarrowtail S + S_{\mathsf{F}_1} + S_{\mathsf{F}_2} + \{s_1'\} + \{s_2'\}$. ($\mathsf{F}$ is transformed into a functor of the required form by transferring the structures specified by F_1 and F_2 to two new sorts s_1' and s_2', and then capturing the structure specified by F by means of an operation symbol with result type $s_1' + s_2'$.)

[9] This condition guarantees that the set of operation symbols of the resulting destructor cosignature is enumerable. Theorem 64 also holds for polynomial endofunctors which do not satisfy this condition, but the resulting endofunctors do not give rise to destructor cosignatures (unless the requirement regarding the enumerability of the set of operation symbols of a many-sorted cosignature is left out).

(4) if $\mathsf{F} = (\mathsf{F}_1)^A$ (with A enumerable), then:

(a) $S_{\mathsf{F}} = S_{\mathsf{F}_1}$,

(b) $\mathsf{G}_{\mathsf{F}} = \prod_{a \in A} \mathsf{G}_{\mathsf{F}_1}$,

(c) $\mathsf{F}_{s'} = (\mathsf{F}_1)_{s'}$ for each $s' \in S_{\mathsf{F}_1}$

(The existence of a **Set**-isomorphism between B^A and $\prod_{a \in A} B$, with $A, B \in |\mathsf{Set}|$ is used here to transform F into a functor of the required form.)

It then follows by structural induction on F that both G_{F} and each of the $\mathsf{F}_{s'}$ with $s' \in S_{\mathsf{F}}$ are in the form of products of finite coproducts of constant/projection functors.

Now given $\mathsf{T} : \mathsf{Set}^S \to \mathsf{Set}^S$, $\mathsf{T} = (\mathsf{T}_s)_{s \in S}$, let $S_{\mathsf{T}} = S + \coprod_{s \in S} S_{\mathsf{T}_s}$ and $\mathsf{G}_{\mathsf{T}} : \mathsf{Set}^{S_{\mathsf{T}}} \to \mathsf{Set}^{S_{\mathsf{T}}}$ be given by

$$(\mathsf{G}_{\mathsf{T}})_{s'} = \begin{cases} \mathsf{G}_{\mathsf{T}_s} \Pi_s & \text{if } s' = \iota_1(s) \text{ for some } s \in S, \\ (\mathsf{T}_s)_{s''} \Pi_s & \text{if } s' = \iota_2(s'') \text{ for some } s'' \in S_{\mathsf{T}_s} \text{ and some } s \in S, \end{cases}$$

where, for $s \in S$, $\Pi_s : \mathsf{Set}^{S_{\mathsf{T}}} \to \mathsf{Set}^{S + S_{\mathsf{T}_s}}$ denotes the projection functor induced by the injection $S + S_{\mathsf{T}_s} \rightarrowtail S_{\mathsf{T}}$. The fact that $\mathsf{Coalg}(\mathsf{T}) \simeq \mathsf{Coalg}(\mathsf{G}_{\mathsf{T}})$ now follows by structural induction on (the components of) T. □

Thus, destructor cosignatures are at least as expressive for coalgebra as many-sorted signatures are for algebra. It is worth noting that, unlike in the algebraic case, moving from one- to many-sorted coalgebras, and from many-sorted cosignatures to destructor cosignatures is actually necessary in order to model via cosignatures arbitrary (extended) polynomial endofunctors.

We exemplify the construction of G_{T} by taking T to be the endofunctor typically used to specify binary trees, that is, $\mathsf{T} : \mathsf{Set}^{\{\mathtt{Tree}\}} \to \mathsf{Set}^{\{\mathtt{Tree}\}}$, $\mathsf{T} = 1 + (\mathsf{Id} \times \mathsf{Id})$. In this case, the construction gives

(1) $S_1 = \emptyset$, $\mathsf{G}_1 = 1$,

(2) $S_{\mathsf{Id}} = \emptyset$, $\mathsf{G}_{\mathsf{Id}} = \mathsf{Id}$,

(3) $S_{\mathsf{Id} \times \mathsf{Id}} = \emptyset$, $\mathsf{G}_{\mathsf{Id} \times \mathsf{Id}} = \mathsf{G}_{\mathsf{Id}} \times \mathsf{G}_{\mathsf{Id}} = \mathsf{Id} \times \mathsf{Id}$,

(4) $S_{1 + (\mathsf{Id} \times \mathsf{Id})} = \{\mathtt{Leaf}, \mathtt{Node}\}$,

$\mathsf{G}_{1 + (\mathsf{Id} \times \mathsf{Id})} : \mathsf{Set}^{\{\mathtt{Tree}, \mathtt{Leaf}, \mathtt{Node}\}} \to \mathsf{Set}$, $\mathsf{G}_{1 + (\mathsf{Id} \times \mathsf{Id})} = \Pi_{\mathtt{Leaf}} + \Pi_{\mathtt{Node}}$,

$(1 + (\mathsf{Id} \times \mathsf{Id}))_{\mathtt{Leaf}} = \mathsf{G}_1 \Pi_{\mathtt{Tree}} = 1$,

$(1 + (\mathsf{Id} \times \mathsf{Id}))_{\mathtt{Node}} = \mathsf{G}_{\mathsf{Id} \times \mathsf{Id}} \Pi_{\mathtt{Tree}} = \Pi_{\mathtt{Tree}} \times \Pi_{\mathtt{Tree}}$,

($\Pi_{\mathtt{Tree}}, \Pi_{\mathtt{Leaf}}, \Pi_{\mathtt{Node}} : \mathsf{Set}^{\{\mathtt{Tree}, \mathtt{Leaf}, \mathtt{Node}\}} \to \mathsf{Set}$ denote the corresponding projection functors.)

Hence, $\mathsf{G}_{\mathsf{T}} : \mathsf{Set}^{\{\mathtt{Tree}, \mathtt{Leaf}, \mathtt{Node}\}} \to \mathsf{Set}^{\{\mathtt{Tree}, \mathtt{Leaf}, \mathtt{Node}\}}$ is given by: $\mathsf{G}_{\mathsf{T}}(X, Y, Z) = (Y + Z, 1, X \times X)$ for $X, Y, Z \in |\mathsf{Set}|$.

6. Related work

This section discusses the relationship between the equational approach to system specification presented here and the ones in [3] and, respectively, [10].

To a certain extent, our approach can be regarded as a generalisation of [3], as it allows for observers whose result type is structured as a coproduct of basic types. However, what distinguishes the approach here from the one in [3] is the absence of any algebraic features in our approach, which results in the inability to constrain state observations to particular data values using coequations. In our opinion such constraints should only be imposed to observations of particular states (such as the ones yielded by state constructors), and therefore should not be considered when coalgebraically specifying state spaces. In addition to operation symbols of arity $\sigma : h \rightarrow h$ and $\alpha : h \rightarrow v$, operation symbols of arity $\sigma : hv \rightarrow h$ or $\alpha : hv \rightarrow v'$ were also considered in [3]. Our approach could be extended to accommodate such operation symbols, as well as more general ones of arity $\delta : hv \rightarrow s_1 \ldots s_n$. However, we believe that such operations should not be regarded as observers, especially if the types associated to their visible argument sorts are infinite. In particular, operation symbols denoting a change of state rather than a property of states should not be considered at this level.

As far as modal logic approaches to coalgebraic specification are concerned, the main difference w.r.t. equational approaches stands in the existence of characterisability results for (classes of) coalgebras [8]. However, such results are obtained at the expense of employing infinitary sentences, while the formulation of completeness results for particular formalisms requires a restriction to finitary sentences as well as the satisfaction of some rather restrictive finiteness conditions by the endofunctors in question [10]. Although equational sentences are not sufficiently expressive to yield similar characterisability results, such sentences appear to be better suited for specifying in a concise way observational properties quantified over state spaces. In addition, no further restrictions are required in equational approaches in order to derive completeness results (see Sections 3.5 and 4.4).

7. Conclusions and future work

A coalgebraic, equational approach to the specification of observational structures allowing for a choice in the result type of observations has been obtained by syntactically dualising the setting of many-sorted algebra. Next, a sound and complete deduction calculus for reasoning about observational properties specifiable with coequations has been formulated. Finally, the formalism has been extended to allow for fixed interpretations of certain (visible) sorts.

Coequations appear to be sufficiently expressive to capture constraints regarding the structure of system states (including the sharing of data or of subcomponents between the system components, or the presence, respectively, absence of certain components in some of the system states). However, the specification of state-based, dynamical systems also involves constraints regarding the relationship between the evolution of systems and the observation of their properties. An approach that integrates algebraic and coalgebraic techniques in order to allow the specification of this relationship is therefore needed to fully specify these systems. Such an approach should clearly distinguish between (algebraic) operations used to construct new states, and (coalgebraic) operations used to observe properties of existing states.

Acknowledgements

The author wishes to thank Andrea Corradini for a useful discussion on an earlier version of this paper, and the two anonymous referees for their valuable comments.

References

[1] F. Borceux, Handbook of Categorical Algebra, vol. II, Cambridge University Press, Cambridge, 1994.

[2] C. Cîrstea, Integrating observations and computations in the specification of state-based, dynamical systems, Ph.D. Thesis, University of Oxford, 2000.

[3] A. Corradini, A completeness result for coequational deduction in coalgebraic specification, in: F. Parisi-Presicce (Ed.), Recent Trends in Algebraic Development Techniques, Lecture Notes in Computer Science, Vol. 1376, Springer, Berlin, 1998, pp. 190–205.

[4] J. Goguen, R. Burstall, Institutions: abstract model theory for specification and programming, J. ACM 39(1) (1992) 95–146.

[5] B. Jacobs, Objects and classes, coalgebraically, in: B. Freitag, C.B. Jones, C. Lengauer, H.-J. Schek (Eds.), Object Orientation with Parallelism and Persistence, Kluwer Academic Publishers, Dordrecht, 1996, pp. 83–103.

[6] B. Jacobs, Invariants, bisimulations and the correctness of coalgebraic refinements, in: M. Johnson (Ed.), Algebraic Methodology and Software Technology, Lecture Notes in Computer Science, Vol. 1349, Springer, Berlin, 1997, pp. 276–291.

[7] J. Meseguer, in: H.-D. Ebbinghaus, et al. (Eds.), General logics, Logic Colloquium'87, North-Holland, Amsterdam, 1989, pp. 275–329.

[8] L.S. Moss, Coalgebraic logic, Ann. Pure Appl. Logic 96 (1999) 277–317.

[9] H. Reichel, An approach to object semantics based on terminal coalgebras, Math. Struct. Comput. Sci. 5 (1995) 129–152.

[10] M. Rößiger, From modal logic to terminal coalgebras, Tech. Report, Technical University Dresden, 1998.

[11] J. Rutten, Universal coalgebra: a theory of systems, Tech. Report CS-R9652, CWI, 1996.