Title	Theorem Proving and Institutions
Author(s)	Gaina, Daniel
Citation	
Issue Date	2009-09
Type	Thesis or Dissertation
Text version	author
URL	http://hdl.handle.net/10119/8365
Rights	
Description	Supervisor:Professor Kokichi Futatsugi, 情報科学研究科, 博士

Theorem Proving and Institutions

by

Daniel GAINA

submitted to
Japan Advanced Institute of Science and Technology
in partial fulfillment of the requirements
for the degree of
Doctor of Philosophy

Supervisor: Professor Kokichi FUTATSUGI

School of Information Science
Japan Advanced Institute of Science and Technology

September 24, 2009

To my parents, Mircea and Viorica

Abstract

We investigate proof rules in various logics used in the area of computer science and prove their soundness and completeness in the abstract framework of institutions. The soundness and completeness results have great significance for logics because they establish a correspondence between the semantic truth and (syntactic) provability. We also specify and verify the correctness of software systems showing how theoretical results may be used in concrete specification examples.

During the process of software specification, we often use different logical systems to capture particular aspects of software systems. Each part of a software system may be described by a distinct logical system that best fit considered problems. It is important to present a (abstract) formal concept of a logical system which covers the population explosion of logics used in computer science. Institution theory of Goguen and Burstall arouse out of this necessity, with the ambition of doing as much as possible at a level of abstraction, independent of any particular logic. We try to provide general ideas and results that can be easily applied to a multitude of logical systems and may be reused in different contexts.

This research is largely focused on foundational aspects but it also takes seriously the task of providing support for the specification and verification of software and hardware systems. We specify a mutual exclusion protocol and prove that it satisfies the desired requirements with the help of the tools provided by our general framework. Even though we use CafeOBJ for mechanical assistance for proofs, our goal is not to present CafeOBJ in detail, but rather its underlying logics.

We develop an abstract proof calculus for logics whose sentences are universal Horn sentences of the form $(\forall X)(\wedge H \Rightarrow C)$ and prove an institution generalization of Birkhoff completeness theorem. This result is applied to Horn clause logic, the "Horn fragment" of preorder algebra, order-sorted algebra and partial algebra and their infinitary variants.

The completeness of the infinitary logic $L_{\omega_1,\omega}$ was proved by Carol Karp in 1964. We express and prove the completeness of infinitary first-order logics in the institution-independent setting by using forcing, a powerful method for constructing models. As a consequence of this abstraction, our results become available for the infinitary versions of many first-order logical systems. Although we emphasize the results for the infinitary logics our framework covers also the finitary cases.

Many computer science applications concern properties which are true of a restricted class of models, in most of the cases reachable models with constructor-generated elements. We introduce the concept of reachable model in the institution model theory. We present a couple of constructor-based institutions defined on top of the Horn and first-order institutions, basically by restricting the class of models to the reachable models. We define the proof rules for these logics, and lift the completeness results previously obtained to the constructor-based logics using institution-independent techniques.

Contents

Chapter 1

Introduction

This thesis is about providing practical framework(s) for the development of software systems; we define the semantics and proof rules for the algebraic specification languages. A suitable framework in which to carry out this study is the theory of institutions. More precisely, a logic is described in a very abstract manner, without concrete signatures, sentences, models and so on; two distinguished components are identified in it: an institution and an entailment system, corresponding to the semantic and the syntactic parts of a logic, respectively.

The concept of institution is a category-based model-oriented formalization of the model theory, including syntax, semantics and satisfaction between them. It provides an abstract approach towards model theory, this perspective having the advantage of clarifying model theoretic phenomena and causality relationships between them, allowing thus new fundamental insights and results even in traditional areas of model theory. A general axiomatic theory of logics should cover all the key ingredients of a logic, an institution plus a notion of entailment (also called provability) of a sentence from a set of axioms. The syntax, i.e. signatures and sentences, plus the entailment relation form an entailment system. This general approach is important especially in the context of the recent proliferation of logics in computer science, mostly in the area of formal specification, where it is now a tradition to have an institution underlying each language.

In a work like this, notation itself sometime becomes a problem. We try to use the standard concepts and notations which appear in the literature. The turnstile $\vdash$ is used for the syntactic provability relation, also called the entailment relation, and the double turnstile $\models$ is used for the semantic consequence relation, also called the satisfaction relation. This text justifies proof measures for a logical systems in the presence of model theory, with respect to the notions of model and satisfaction for that system. The concepts used here allow a natural generalization of the soundness and completeness properties. Soundness says that only sentences which are true of a class of models of some set of axioms Ax, are provable from Ax, mathematically, the syntactic relation is embedded into the semantic one ($\vdash \subseteq \models$). Completeness is the converse property to soundness, and it says that a sentence can be formally proved from a set of axioms Ax when that sentence holds in every model of Ax, more formally $\models \subseteq \vdash$.

Users are concerned whether certain properties, formalized as sentences, are true of certain models, which may be realized in a (software or hardware) system. Since the syntactic approach is the only effective way to infer properties from a given set of axioms, the completeness results ensures that the provability relation is reach enough to demonstrate the truth. Nevertheless, many logical systems enjoy only the soundness property, which is fundamental because it prevents the deduction of “invalid” properties.

1.1 Horn logics

Notice that in most of the standard cases, a logic comes with a notion of atomic sentence, with the help of with the formulas of the logic are built. Horn logics have the sentences of the form $(\forall X)(\wedge H) \Rightarrow C$, where H is a (finite) set of atoms in the given logic, C is an atom, $\wedge H$ is the conjunction of the sentences in H, and $(\wedge H) \Rightarrow C$ is the implication of C by $\wedge H$. We assume that the conjunction binds tighter then the implication, and we will write $\wedge H \Rightarrow C$ rather than $(\wedge H) \Rightarrow C$. One important property which holds in Horn logics presented here is the existence of initial model(s) for a given set of sentences. Moreover these logics can be implemented efficiently by term rewriting, which can serve as a theorem prover.

In 1935 Birkhoff first prove a completeness theorem for conditional equational logic, in the unsorted case. Goguen and Meseguer, giving a sound and complete system of proof rules for finitary many-sorted equational deduction, generalized the completeness theorem of Birkhoff to the completeness of finitary many-sorted equational logic and provided simultaneously a full algebraization of finitary many-sorted equational deduction. The unsorted rules can be unsound for many-sorted algebras that may have empty carriers, suggesting the idea that generalizations to other variants of equational logics may imply some difficulties. We generalize the Birkhoff completeness result to arbitrary institutions obtaining uniformly sound and complete systems of proof rules for Horn clause logic, the "Horn fragment" of preorder algebra, order-sorted algebra and partial algebra.

1.2 First-order logics

First-order logics have sentences constructed over the atoms by means of Boolean connectives and quantification. It is well known that not all sets of sentences in these logics have initial model or are not even consistent (there is no model for a given set of axioms). At this moment we can not give a characterization for the sets of first-order sentences which admit initial model. As we will see later on, in concrete specifications, we use first-order sentences (more precisely universal sentences of the form $(\forall X)\rho$ where ρ is a formula formed without quantifications) on top of the Horn sentences, to restrict the class of models of the Horn sentences, or to recursively define some operation symbols. We will argue that initial semantics is important only at the level of specifications, but for the formal verification we need only loose semantics in constructor-based framework which should include all Boolean connectives.

One important contribution of our study is the formalization of forcing in abstract model theory, thus providing an efficient tool for obtaining new results and showing the significance of the top-down approach towards model theory. We use forcing to prove the completeness of the first-order entailment systems in the abstract setting. The forcing technique was invented by Paul Cohen, for proving consistency and independence results in set theory, and later it was introduced by Robinson in model theory, and by Gaina and Petria in institution model theory.

1.3 Constructor-based logics

Applications concern properties which are true of a restricted class of models. In most of the cases the models of interest include the initial model(s) of a set of axioms. Some approaches consider the initial semantics and reason about properties which are true of initial model. Our work takes into account the generation aspects of software systems by considering

the constructor-based institutions. For example in Horn clause logic for each signature we distinguish a set of operation symbols called *constructors*. The result sorts of the constructors are called *constrained* and a sort which is not constrained it is *loose*. The constructors determine the class of *reachable* models which are of interest from the user point of view. Intuitively the carrier sets of such models consist of constructor-generated elements. The sentences and the satisfaction condition are preserved from the base institution. In order to obtain a constructor-based institution the signature morphisms of the base institution are restricted such that the *reducts* of the reachable models along the signature morphisms are also reachable. In the examples presented here it is simply required that constructors are preserved by signature morphisms, and no "new" constructors are introduced for "old" constrained sorts (for sorts being in the image of some constrained sorts of the source signature).

At the level of institutions we give a categorical definition of reachable model parameterized by two classes of signature morphisms. In Horn clause logic, by choosing appropriate parameters, we prove that the abstract definition lead to the same classical concept of reachability. Then we apply this institution-independent notion to order-sorted algebra, preorder algebra, and partial algebra and we obtain the constructor-based variants of these institutions.

We provide probability relations for the constructor-based institutions by adding proof rules which integrate the reachability concept to the proof rules for the base institutions (which may be Horn or first-order), and we prove a completeness result using institution-independent techniques. However the completeness is relative to a family of sufficient complete basic specifications (Σ, Γ) with signature Σ and set Γ of sentences. Intuitively (Σ, Γ) is sufficient complete when any term formed with operation symbols with the constrained result sort and variables of sort loose can be *reduced* to a term formed with constructors and variables of sort loose using the equations from Γ.

1.4 Structure of the thesis

This thesis consists of four parts.

The first part, chapters 2 and 3, introduce the main ingredients of institution proof theory, the concepts of institution and entailment system. We present several examples of basic institutions together with their constructor-based restrictions. We develop an "internal logic" which includes an interpretation of Boolean connectives and quantifiers at the level of an arbitrary institution. The chapter on entailment systems defines the soundness and completeness and explores the compactness property for the entailment relations generated by proof rules which deal with Boolean connectives and universal and existential quantifiers. Compactness is a key property for making the proofs finitary (written as finite sequences of sentences obtained by applying the proof rules to the previous ones).

The second part, chapters 4, 5 and 6, is devoted to the "logic for applications" and may be read independently. Conditional equational logic is the basic logic underlying the algebraic specification languages. We separate the specific proof rules of this logic from the general ones and we show how the abstract completeness results are reflecting in a concrete example of logic. We also give an example of unsound deduction showing that the rules for equational deduction in the unsorted case are unsound for the many-sorted case. The chapter on constructor-based equational logic defines the *Case splitting* rules and demonstrates that the rules for equational deduction plus *Case splitting* generate an entailment relation equal to the semantic consequence relation. However the rules of *Case splitting* have infinitary premises and the resulting entail-

ment system is not compact. Therefore, we define a basic induction scheme to deal with the infinite conditions of the rules and argue that we can not obtain a complete and compact entailment system for the constructor-based equational logic. This part contains also a discussion on the error handling with order-sorted algebra.

The third part, Chapter 7, demonstrates the applicability of our theoretical results, and may be seen as a motivation of our study. The example used here is a mutual exclusion protocol, an algorithm which ensure that no more then one process have access to a common shared source at a given time. The rigorous logical framework reflects to the level of proofs; the verification of the mutual exclusion property is significantly more simpler here comparing to the previous approaches.

The last part, chapters 8, 9, and 10 is the core of the original developments. We present several basic notions in the institution theory, reachability being the key concept for defining the constructor-based logics. We define the rules of *Case splitting* which integrate the reachability and we prove a quasi-completeness result for the constructor-based logics in the institution-independent setting. Our general layered approach allows to instantiate this result to Horn and first-order institutions, respectively. The forcing technique constitutes one of the most important contribution of the present research and it is used for proving completeness of first-order logics.

Chapter 2

Institutions

Institutions were introduced in [33] with the original goal of providing an abstract framework for algebraic specifications of computer science systems. By isolating the essence of a logical system in the abstract *satisfaction relation*, which states that *truth is invariant to change of notation*, and leaving open the details of signatures, sentences and models, these structure achieves an appropriate level of generality for the development of abstract model theory - i.e. independent of the specific nature of the underlying logic. Many logical notions and results can be developed in an institution-independent way, to mention just a few: ultraproducts [20], Craig interpolation [22], elementary chains [30], Robinson consistency [31], Beth definability [58]. A textbook dedicated to this topic is [24].

2.1 Categories

We assume that the reader is familiar with basic categorical notions like functor, natural transformation, co-limit, comma category, etc. A standard textbook on the topic is [46]. We are going to use the terminology from there, with a few exceptions that we point out below. We use both the terms "morphism" and "arrow" to refer morphisms of a category. Composition of morphisms and functors is denoted using the symbol ";" and is considered in diagrammatic order.

Let $\mathcal{C}$ and $\mathcal{C}'$ be two categories. Given an object $A \in |\mathcal{C}|$, the *comma category of objects in* $\mathcal{C}$ *under* A is denoted $A/\mathcal{C}$. Recall that the objects of this category are pairs (h,B), where $B \in |\mathcal{C}|$ and $A \xrightarrow{h} B$ is a morphism in $\mathcal{C}$. Throughout the paper, we might let either $(A \xrightarrow{h} B)$ or (h,B) indicate objects in $A/\mathcal{C}$. A morphism in $A/\mathcal{C}$ between two objects (h,B) and (g,D) is just a morphism $B \xrightarrow{f} D$ in $\mathcal{C}$ such that $h;f = g$ in $\mathcal{C}$. There exists a canonical forgetful functor between $A/\mathcal{C}$ and $\mathcal{C}$, mapping each (h,B) to B and each $f : (h,B) \to (g,D)$ to $f : B \to D$. Also, if $F : \mathcal{C}' \to \mathcal{C}$ is a functor, $A \in |\mathcal{C}|$, $A' \in |\mathcal{C}'|$, and $A \xrightarrow{u} F(A')$ is in $\mathcal{C}$, then there exists a canonical functor $u/F : A'/\mathcal{C}' \to A/\mathcal{C}$ mapping each $(A' \xrightarrow{h} B, B)$ to $(u;F(h),F(B))$ and each $f : (h,B) \to (g,D)$ to $F(f) : (u;F(h),F(B)) \to (u;F(g),F(D))$. If $\mathcal{C} = \mathcal{C}'$ and F is the identity functor $1_{\mathcal{C}}$, we write $u/\mathcal{C}$ instead of u/F; and if $F(A') = A$ and $u = 1_A$, we write A'/F instead of u/F.

Let $\mathcal{C}$ and $\mathcal{S}$ be two categories such that $\mathcal{S}$ is small. A functor $D : \mathcal{S} \to \mathcal{C}$ is also called a *diagram*. We usually identify a diagram $D : \mathcal{S} \to \mathcal{C}$ with its image in $\mathcal{C}$, $D(\mathcal{S})$. A *co-cone* of D is a natural transformation $\mu : D \Rightarrow V$ between the functor D and [the constant functor mapping all objects to V and all morphisms to 1_V]; V is an object in $\mathcal{C}$, the *vertex* of the co-limit, and

the components of μ are the *structural morphisms* of the co-limit. Any partially ordered set $(I,\leq)$ can be regarded as a category in the obvious way, with the arrows being pairs $i \leq j$. A non-empty partially ordered set $(I,\leq)$ is said to be *directed* if for all $i,j \in I$, there exists $k \in I$ such that $i \leq k$ and $j \leq k$, and is called a *chain* if the order $\leq$ is total. A diagram defined on a directed set (on a chain) shall be called *directed diagram (chain diagram)*, and a co-limit of such a diagram *directed co-limit (chain co-limit)*.

Let C' be a subcategory of C. C' is called a *broad subcategory* if it contains all the objects of C. C' is said to be *closed under directed co-limits (chain co-limits)* if for any directed diagram (chain diagram) $D:(I,\leq) \to C$ such that [for each $i \leq j$ in I, $D(i \leq j)$ is in C'], any co-limit $\{Di \xrightarrow{\mu_i} B\}_{i\in I}$ of D has all the structural morphisms μ_i in C'. C' is said to be *closed under pushouts* if for each pushout $(A_2 \xleftarrow{h_2} A \xrightarrow{h_1} A_1, A_2 \xrightarrow{h'_1} A' \xleftarrow{h'_2} A_1)$ in C, h'_1 is in C' whenever h_1 is in C'.

An object A in a category C is called *finitely presented* ([1]) if

- for each directed diagram $D:(J,\leq) \to C$ with co-limit $\{Di \xrightarrow{\mu_i} B\}_{i\in J}$, and for each morphism $A \xrightarrow{g} B$, there exists $i \in J$ and $A \xrightarrow{g_i} Di$ such that $g_i;\mu_j = g$,
- for any two arrows g_i and g_j as above, there exists $i \leq k, j \leq k \in J$ such that $g_i;D(i \leq k) = g_j;D(j \leq k) = g$.

2.2 Definition and Examples

Definition 2.2.1. *An institution consists of*

1. *a category* $\mathbb{S}ig$*, whose objects are called* signatures.
2. *a functor* $\mathbb{S}en : \mathbb{S}ig \to \mathbb{S}et$*, providing for each signature a set whose elements are called* (Σ-)sentences.
3. *a functor* $\mathbb{M}od : \mathbb{S}ig^{op} \to Cat$*, providing for every signature* Σ *a category whose objects are called* (Σ-)models *and whose arrows are called* (Σ-)morphisms.
4. *a relation* $\models_\Sigma \subseteq |\mathbb{M}od(\Sigma)| \times \mathbb{S}en(\Sigma)$ *for each* $\Sigma \in |\mathbb{S}ig|$*, called* ($\Sigma$-)satisfaction*, such that for each morphism* $\varphi : \Sigma \to \Sigma'$ *in* $\mathbb{S}ig$*, the following* satisfaction condition *holds:*

$$M' \models_{\Sigma'} \mathbb{S}en(\varphi)(e) \text{ iff } \mathbb{M}od(\varphi)(M') \models_\Sigma e$$

for all models $M' \in |\mathbb{M}od(\Sigma')|$ *and sentences* $e \in \mathbb{S}en(\Sigma)$.

Following the usual notational conventions, we sometimes let $\_\restriction_\phi$ denote the reduct functor $\mathbb{M}od(\varphi)$ and let φ denote the sentence translation $\mathbb{S}en(\varphi)$. When $M = M' \restriction_\varphi$ we say that M' is a φ-*expansion* of M, and that M is the φ-*reduct* of M'; and similarly for model morphisms. When E and E' are sets of sentences of the same signature Σ, we let $E \models_\Sigma E'$ denote the fact that $M \models E$ implies $M \models E'$ for all Σ-models M. The relation $\models_\Sigma$ between sets of sentences is called (Σ-)*semantic consequence relation* (notice that it is written just like the satisfaction relation).

Example 1 (First order logic (**FOL**) [33])**.** The signatures are triplets (S,F,P), where S is the set of sorts, $F = \{F_{w\to s}\}_{w\in S^*, s\in S}$ is the ($S^* \times S$ -indexed) set of operation symbols, and $P = \{P_w\}_{w\in S^*}$ is the (S^*-indexed) set of relation symbols. If $w = \lambda$, an element of $F_{w\to s}$ is

called a *constant symbol*, or a *constant*. By a slight notational abuse, we let F and P also denote $\bigcup_{(w,s)\in S^*\times S} F_{w\to s}$ and $\bigcup_{w\in S^*} P_w$ respectively. A signature morphism between (S,F,P) and (S',F',P') is a triplet $\varphi = (\varphi^{sort}, \varphi^{op}, \varphi^{rel})$, where $\varphi^{sort} : S \to S'$, $\varphi^{op} : F \to F'$, $\varphi^{rel} : P \to P'$ such that $\varphi^{op}(F_{w\to s}) \subseteq F'_{\varphi^{sort}(w)\to\varphi^{sort}(s)}$ and $\varphi^{rel}(P_w) \subseteq P'_{\varphi^{sort}(w)}$ for all $(w,s) \in S^* \times S$. When there is no danger of confusion, we may let φ denote each of φ^{sort}, φ^{rel} and φ^{op}.

Given a signature $\Sigma = (S,F,P)$, a Σ-model M is a triplet

$$M = (\{M_s\}_{s\in S}, \{M_\sigma^{w,s}\}_{(w,s)\in S^*\times S, \sigma\in F_{w,s}} \{M_\pi^w\}_{w\in S^*, \pi\in P_w})$$

interpreting

1. each sort s as a set M_s,
2. each operation symbol $\sigma \in F_{w\to s}$ as a function $M_\sigma^{w,s} : M_w \to M_s$ (where M_w stands for $M_{s_1} \times \ldots \times M_{s_n}$ if $w = s_1 \ldots s_n$), and
3. each relation symbol $\pi \in P_w$ as a relation $M_\pi^w \subseteq M_w$.

When there is no danger of confusion we may let M_σ and M_π denote $M_\sigma^{w,s}$ and M_π^w respectively. Morphisms between models are the usual Σ-morphisms, i.e., S-sorted functions that preserve the structure.

The Σ-sentences are the usual closed first-order logic formulae (formulae without free variables) built over atomic formulae given either as

1. equality atoms $t_1 = t_2$, where $t_1, t_2 \in (T_F)_s$ [1] or
2. relational atoms $\pi(t_1, \ldots, t_n)$, where $\pi \in P_{s_1 \ldots s_n}$ and $t_i \in (T_F)_{s_i}$ for each $i \in \{1, \ldots, n\}$),

and is closed under:

1. negation, disjunction and false;
2. universal or existential quantification over finite sets of constants (variables).

Satisfaction is the usual first-order satisfaction and is defined using the natural interpretations of ground terms t as elements M_t in models M. The definitions of functors $\mathbb{S}en$ and $\mathbb{M}od$ on morphisms are the natural ones: for any signature morphism $\varphi : \Sigma \to \Sigma'$, $\mathbb{S}en(\varphi) : \mathbb{S}en(\Sigma) \to \mathbb{S}en(\Sigma')$ translates sentences symbol-wise, and $\mathbb{M}od(\varphi) : \mathbb{M}od(\Sigma') \to \mathbb{M}od(\Sigma)$ is the forgetful functor.

The institution **FOEQL** of first-order equational logic is obtain from **FOL** by discarding both the relation symbols and their interpretations in models.

Example 2 (Universal first-order logic(**UFOL**))**.** A *universal sentence* for a **FOL** signature (S,F,P) is a sentence of the form $(\forall X)\rho$, where ρ is a sentence formed without quantifiers. **UFOL** has the same signatures and models as **FOL** but only universal sentences.

Example 3 (Horn Clause logic (**HCL**))**.** *A universal Horn sentence* for a **FOL** signature (S,F,P) is a (universal) sentence of the form $(\forall X)(\wedge H) \Rightarrow C$, where H is a finite set of (relational or equational) atoms, and C is a (relational or equational) atom. In the tradition of logic programming universal Horn sentences are known as *Horn Clauses*. Thus **HCL** has the same signatures and models as **FOL** but only universal Horn sentences as sentences.

By considering the case of empty sets of relational symbols, we obtain the conditional equational logic, **CEQL** [6].

[1] T_F is the ground term algebra over F.

Example 4 (Constructor-based first-order logic (**CFOL**)). The signatures of constructor-based first-order logic (S,F,F^c,P) consist of

1. a first-order signature (S,F,P), and
2. a distinguished set of *constructors* $F^c \subseteq F$.

The constructors determine the set of

1. *constrained* sorts $S^c \subseteq S$: $s \in S^c$ iff there exists a constructor $\sigma \in F^c_{w \to s}$ with the result sort s.
2. *loose* sorts $S^l = S - S^c$.

The (S,F,F^c,P)-sentences are the *universal constrained first-order sentences* of the form $(\forall X)\rho$ where

- X is a finite set of constrained variables [2], and
- ρ is a first-order formula formed over the atoms by applying Boolean connectives and quantifications over loose variables [3].

The (S,F,F^c,P)-models are the usual first-order structures M with the carrier sets for the constrained sorts consisting of interpretations of terms formed with constructors and elements of loose sorts, i.e. there exists

1. a set $Y = (Y_s)_{s \in S}$ of variables of loose sorts, and
2. a function $f : Y \to M$

such that for every constrained sort $s \in S^c$ the function $\overline{f}_s : (T_{F^c}(Y))_s \to M_s$ is a surjection, where $\overline{f}$ is the unique extension of f to a (S,F^c,P)-morphism.

A constructor-based first-order signature morphisms $\varphi : (S,F,F^c,P) \to (S_1,F_1,F_1^c,P_1)$ is a first-order signature morphism $\varphi : (S,F,P) \to (S_1,F_1,P_1)$ such that

1. the constructors are preserved along signature morphisms: if $\sigma \in F^c$ then $\varphi(\sigma) \in F_1^c$, and
2. no "new" constructors are introduced for "old" constrained sorts: if $\sigma_1 \in (F_1^c)_{w_1 \to s_1}$ and $s_1 \in \varphi(S^c)$ then there exists $\sigma \in F^c$ such that $\varphi(\sigma) = \sigma_1$.

Example 5 (Constructor-based universal first-order logic **CUFOL**). This institution is obtained from **CFOL** by restricting the sentences to *universal sentences* of the form $(\forall X)(\forall Y)\rho$, where X is a finite set of variables of constrained sorts, Y is a finite set of variables of loose sorts, and ρ is a sentence formed without quantifiers.

Example 6 (Constructor-based Horn clause logic (**CHCL**)). This institution is obtained from **CFOL** by restricting the sentences to *universal Horn sentences* of the form $(\forall X)(\forall Y) \wedge H \Rightarrow C$, where X is a finite set of variables of constrained sorts, Y is a finite set of variables of loose sorts, H is a finite set of (relational or equational) atoms, and C is an atom.

The institution of constructor-based conditional equational logic **CCEQL** is obtained from **CHCL** by forgetting the relation symbols.

[2] $X = (X_s)_{s \in S}$ is a set of constrained variables if $X_s = \emptyset$ for all $s \in S^l$

[3] $Y = (Y_s)_{s \in S}$ is a set of loose variables if $Y_s = \emptyset$ for all $s \in S^c$.

Example 7 (Infinitary first-order logic $\mathbf{FOL}_{\omega_1,\omega}$)**.** This is the infinitary version of first-order logic allowing disjunctions of countable sets of sentences.

Example 8 (Infinitary Horn clause logic ($\mathbf{HCL}_\infty$))**.** This is the infinitary extension of **HCL** obtained by allowing the set X of variables of a Horn clause $(\forall X)\bigwedge H \Rightarrow C$ to be infinite, and the hypothesis part $\bigwedge H$ to consist of infinitary conjunctions of atoms. Similarly one may extend **CHCL** to $\mathbf{CHCL}_\infty$.

Example 9 (Infinitary universal first-order logic ($\mathbf{UFOL}_\infty$))**.** This is the infinitary extension of **UFOL** obtained by allowing the set X of variables of a universal sentence $(\forall X)\rho$ to be infinite, and the quantifier-free part ρ to be constructed by applying disjunctions to infinite sets of sentences. Similarly one may extend **CUFOL** to $\mathbf{CUFOL}_\infty$.

Example 10 (Order-sorted algebra (**OSA**) [36])**.** An order-sorted signature $(S,\leq,F)$ consists of an algebraic signature (S,F), with a partial ordering $(S,\leq)$ such that the following *monotonicity condition* is satisfied

$$\sigma \in F_{w_1\to s_1} \cap F_{w_2\to s_2} \text{ and } w_1 \leq w_2 \text{ imply } s_1 \leq s_2$$

A morphism of **OSA** signatures $\varphi : (S,\leq,F) \to (S',\leq',F')$ is just a morphism of algebraic signatures $(S,F) \to (S',F')$ such that the ordering is preserved, i.e. $\varphi(s_1) \leq' \varphi(s_2)$ whenever $s_1 \leq s_2$.

Given an order-sorted signature $(S,\leq,F)$, an order-sorted $(S,\leq,F)$-algebra is a (S,F)-algebra M such that

- $s_1 \leq s_2$ implies $M_{s_1} \subseteq M_{s_2}$, and
- $\sigma \in F_{w_1\to s_1} \cup F_{w_2\to s_2}$ and $w_1 \leq w_2$ imply $M_\sigma^{w_1,s_1} = M_\sigma^{w_2,s_2}$ on M_{w_1}.

Given order-sorted $(S,\leq,F)$-algebras M and N, an order-sorted $(S,\leq,F)$-morphism $h : M \to N$ is a (S,F)-morphism such that $s_1 \leq s_2$ implies $h_{s_1} = h_{s_2}$ on M_{s_1}.

An order-sorted signature $(S,\leq,F)$ is *regular* iff for each $\sigma \in F_{w_1\to s_1}$ and each $w_0 \leq w_1$ there is a unique least element in the set $\{(w,s) \mid \sigma \in F_{w\to s} \text{ and } w_0 \leq w\}$.

Remark 2.2.2. *For regular signatures $(S,\leq,F)$, any F-term t has a least sort $LS(t)$ and the initial $(S,\leq,F)$-algebra can be defined as a term algebra, cf. [36].*

Proof. We proceed by induction on the structure of the term t. If $t \in F_{\to s_1}$ then by regularity with $w_0 = w_1 = \lambda$ there is a least $s \in S$ such that $t \in F_{\to s}$; this is the least sort of t. If $t = \sigma(t_1,\ldots,t_n) \in (T_F)_s$ then by induction hypothesis each t_i has a least sort, say s_i; let $w_0 = s_1 \ldots s_n$. Then $\sigma \in F_{w'\to s'}$ for some pair $(w',s') \in S^* \times S$ with $s' \leq s$ and $w_0 \leq w'$. By regularity, there exists least pair $(w'',s'') \in S^* \times S$ such that $\sigma \in F_{w''\to s''}$; this s'' is the desired least sort of t. (Q.E.D.)

Let $(S,\leq,F)$ be an order-sorted signature. We say that the sorts s_1 and s_2 are in the same *connected component* of S iff $s_1 \equiv s_2$, where $\equiv$ is the least equivalence on S that contains $\leq$. A partial ordering $(S,\leq)$ is *filtered* iff for all $s_1,s_2 \in S$, there is some $s \in S$ such that $s_1 \leq s$ and $s_2 \leq s$. A partial ordering is *locally filtered* iff every connected component of it is filtered. An order-sorted signature $(S,\leq,F)$ is *locally filtered* iff $(S,\leq)$ is locally filtered, and it is *coherent* iff it is both locally filtered and regular. Hereafter we assume that all **OSA** signatures are coherent.

The atoms of the signature $(S, \leq, F)$ are equations of the form $t_1 = t_2$ such that the least sort of the terms t_1 and t_2 are in the same connected component. The sentences are closed formulas built by application of Boolean connectives and quantification to the equational atoms. Order-sorted algebras were extensively studied in [34, 36, 61].

Universal order-sorted algebra (**UOSA**) and Horn order-sorted algebra (**HOSA**) are obtained by restricting the sentences of **OSA** to universal sentences and universal Horn sentences, respectively. Their infinitary variants $\mathbf{UOSA}_\infty$ and $\mathbf{HOSA}_\infty$ are obtained as in the first-order case by allowing the infinitary universal sentences and infinitary universal Horn sentences, respectively. $\mathbf{OSA}_{\omega_1,\omega}$ is extending **OSA** by allowing disjunctions of countable sets of sentences.

Example 11 (Constructor-based order-sorted logic (**COSA**))**.** This institution is defined on top of **OSA** similarly as **CFOL** is defined on top of **FOL**. The constructor-based order-sorted signatures $(S, \leq, F, F^c)$ consists of

1. an order-sorted signature $(S, \leq, F)$, and
2. a distinguished set of operational symbols $F^c \subseteq F$, called *constructors*, such that $(S, \leq, F^c)$ is an order-sorted signature (the monotonicity and coherence conditions are satisfied).

As in the first-order case the constructors determine the set of

1. *constrained* sorts $S^c \subseteq S$: $s \in S^c$ iff there exists a constructor $\sigma \in F^c_{w \to s}$ with the result sort s.
2. *loose* sorts $S^l = S - S^c$.

The $(S, \leq, F, F^c)$-sentences are the *universal constrained order-sorted sentences* of the form $(\forall X)\rho$, where

- X is finite set of variables of constrained sorts, and
- ρ is a formula with quantifications over variables of loose sorts only.

The $(S, \leq, F, F^c)$-models are the usual $(S, \leq, F)$-models with the carrier sets for the constrained sorts consisting of interpretation of terms formed with constructors and elements of loose sorts, i.e. there exists

1. a set of variables Y of loose sorts, and
2. a function $f : Y \to M$

such that for every constrained sort $s \in S^c$ the function $\overline{f}_s : (T_{F^c}(Y))_s \to M_s$ is a surjection, where $\overline{f}$ is the unique extension of f to a $(S, \leq, F^c)$-morphism.

A signature morphism $\varphi : (S, \leq, F, F^c) \to (S_1, \leq_1, F_1, F^c_1)$ is an order-sorted signature morphism such that

1. constructors are preserved along the signature morphisms: if $\sigma \in F^c$ then $\varphi(\sigma) \in F^c_1$,
2. no "new" constructors are introduced for "old" constrained sorts: if $\sigma_1 \in (F^c_1)_{w_1 \to s_1}$ and $s_1 \in \varphi(S)$ then there exists $\sigma \in F^c$ such that $\varphi(\sigma) = \sigma_1$, and

3. if $s'_1 \leq_1 s''_1$ and there exists $s'' \in S^c$ such that $s''_1 = \varphi(s'')$ then there exists $s' \in S^c$ such that $s'_1 = \varphi(s')$.

Constructor-based universal order-sorted algebra (**CUOSA**) and constructor-based Horn order-sorted algebra (**CHOSA**) are obtained by restricting the sentences of **COSA** to universal sentences and universal Horn sentences, respectively. Their infinitary variants $\mathbf{CUOSA}_\infty$ and $\mathbf{CHOSA}_\infty$ are obtained as in the first-order case.

Example 12 (Preorder algebra (**POA**) [26])**.** The **POA** signatures are just the ordinary algebraic signatures. The **POA** models are *preordered algebras* which are interpretations of the signatures into the category of preorders $\mathbb{P}re$ rather than the category of sets $\mathbb{S}et$. This means that each sort gets interpreted as a preorder, and each operation as a preorder functor, which means a preorder-preserving (i.e. monotonic) function. A *preordered algebra morphism* is just a family of preorder functors (preorder-preserving functions) which is also an algebra morphism.

The sentences have two kinds of atoms: equations and *preorder atoms*. A preorder atom $t \leq t'$ is satisfied by a preorder algebra M when the interpretations of the terms are in the preorder relation of the carrier, i.e. $M_t \leq M_{t'}$. Full sentences are constructed from equational and preorder atoms by using Boolean connectives and first-order quantification.

As in case of **FOL** we define universal preorder algebra (**UPOA**) and Horn preorder algebra (**HPOA**) by restricting the sentences to universal sentences and universal Horn sentences, respectively. The institution of constructor-based preorder algebra (**CPOA**) is obtained similarly as in first-order case. Their infinitary variants are obtained by allowing infinitary sentences.

POA constitutes an unlabeled form of Meseguer's rewriting logic [49], but later is not an institution.

Example 13 (Partial algebra (**PA**) [59, 12])**.** A *partial algebraic signature* (S,F) consists of a set S of sorts and a set F of *partial* operations. We assume that there is a distinguished constant on each sort $\bot_s : s$. Signature morphisms map the sorts and operations in a compatible way, preserving $\bot_s$; we also allow that constants can be mapped to terms.

A partial algebra is just like an ordinary algebra but interpreting the operations of F as partial rather than total functions; $\bot_s$ is always interpreted as undefined. A *partial algebra homomorphism* $h : A \to B$ is a family of (total) functions $\{h_s : A_s \to B_s\}_{s \in S}$ indexed by the set of sorts S of the signature such that $h_s(A_\sigma(a)) = B_\sigma(h_w(a))$ for each operation $\sigma : w \to s$ and each string of arguments $a \in A_w$ for which $A_\sigma(a)$ is defined.

Remark 2.2.3. *For every inclusion $\Sigma \hookrightarrow \Sigma(Z)$ in $\mathbb{D}$, where $\Sigma = (S, S^c, F)$ and $\Sigma(Z) = (S, S^c, F \cup Z)$, the $\Sigma(Z)$-models can be represented as pairs (A, a) where A is a Σ-model and $a : Z' \to A$ is a function such that $Z' \subseteq Z$ is the set of variables which are defined.*

We consider one kind of "base" sentences: *existence equality* $t \stackrel{e}{=} t'$. The existence equality $t \stackrel{e}{=} t'$ holds when both terms are defined and are equal. The definedness predicate and strong equality can be introduced as notations: $def(t)$ stands for $t \stackrel{e}{=} t$ and $t \stackrel{s}{=} t'$ stands for $(t \stackrel{e}{=} t') \vee (\neg def(t) \wedge \neg def(t'))$.

We consider the atomic sentences in $\mathbb{S}en(S,F)$ to be the atomic existential equalities that do not contain $\bot_s$. The sentences are formed from these "base" sentences by logical connectives and quantification over variables.

The definition of **PA** given here is slightly different from the one in [51] since it does not consider total operation symbols.

By restricting the sentences to universal sentences and universal Horn sentences formed over the existential equalities, we obtain **UPA** and **HPA**, respectively. Their infinitary versions are obtained by allowing infinitary sentences above.

Example 14 (Constructor-based partial algebra (**CPA**)). The signatures of constructor-based partial algebra (S,F,F^c) consist of a signature (S,F) in the base institution, and a distinguished set of *constructors* $F^c \subseteq F$.

The constructors determine the set of *constrained* sorts $S^c \subseteq S$: $s \in S^c$ iff there exists a constructor $\sigma \in F^c_{w\to s}$ with the result sort s, and the set of *loose* sorts $S^l = S - S^c$.

The (S,F,F^c)-sentences are the *universal constrained first-order sentences* of the form $(\forall X)\rho$ where X is a finite set of variables of constrained sorts, and ρ is a formula with quantifications over variables of loose sorts only.

The (S,F,F^c)-models are the usual partial algebras M with the carrier sets for the constrained sorts consisting of interpretations of terms formed with constructors and elements of loose sorts, i.e. there exists

1. a set $Y = (Y_s)_{s\in S}$ of variables of loose sorts, and
2. a function $f : Y \to M$

such that for every constrained sort $s \in S^c$ the function $f^\#_s : (T_{(M,f)})_s \to M_s$ is a surjection, where

1. $T_{(M,f)} \subseteq T_{F^c\cup Y}$ is the maximal partial $(S,F^c \cup Y)$-algebra of terms such that $(M,f) \models def(t)$ for all $t \in T_{(M,f)}$, and
2. $f^\# : T_{(M,f)} \to (M,f)$ is the unique $(S,F^c \cup Y)$-morphism.

A constructor-based first-order signature morphisms $\varphi : (S,F,F^c) \to (S_1,F_1,F^c_1)$ is a **PA**-signature morphism $\varphi : (S,F) \to (S_1,F_1)$ such that

1. constructors are preserved along signature morphisms: if $\sigma \in F^c$ then $\varphi(\sigma) \in F^c_1$, and
2. no "new" constructors are introduced for "old" constrained sorts: if $\sigma_1 \in (F^c_1)_{w_1\to s_1}$ and $s_1 \in \varphi(S^c)$ then there exists $\sigma \in F^c$ such that $\varphi(\sigma) = \sigma_1$.

The variants of **CPA** are defined similarly as in the previous cases.

Example 15 (Institution of presentations). A *presentation* is a pair (Σ,E) consisting of a signature Σ and a set E of Σ-sentences. A *presentation morphism* $\varphi : (\Sigma,E) \to (\Sigma',E')$ is a signature morphism $\varphi : \Sigma \to \Sigma'$ which maps the axioms of the source presentation to logical consequences of the target presentation: $E' \models \varphi(E)$. Presentation morphisms form a category, denoted $\mathbb{P}res^I$. The model functor $\mathbb{M}od$ of an institution can be extended from the category of its signatures $\mathbb{S}ig$ to a model functor from the category of its presentations $\mathbb{P}res$, by mapping a presentation (Σ,E) to the full subcategory $\mathbb{M}od^{pres}(\Sigma,E)$ of $\mathbb{M}od(\Sigma)$ consisting of all Σ-models satisfying E. The correctness of the definition of $\mathbb{M}od^{pres}$ is guaranteed by the satisfaction condition of the base institution; this is easy to check. This leads to the *institution of presentations* $I^{pres} = (\mathbb{S}ig^{pres}, \mathbb{S}en^{pres}, \mathbb{M}od^{pres}, \models^{pres})$ over the base institution I where

- $\mathbb{S}ig^{pres}$ is the category $\mathbb{P}res^I$
- $\mathbb{S}en^{pres}(\Sigma,E) = \mathbb{S}en(\Sigma)$, and
- for each (Σ,E)-model M and any Σ-sentence e, $M \models^{pres} e$ iff $M \models e$.

2.3 Internal Logic

The logical connectives and quantification can be defined generically in any institution.

Definition 2.3.1. *[63] In any institution*

1. *a sentence $\rho \in \mathbb{S}en(\Sigma)$ is called a semantic negation of a sentence $\rho_0 \in \mathbb{S}en(\Sigma)$ if for every Σ-model M we have $M \models \rho$ iff $M \not\models \rho_0$.*

2. *a sentence $\rho \in \mathbb{S}en(\Sigma)$ is called a semantic disjunction of two sentences $\rho_0, \rho_1 \in \mathbb{S}en(\Sigma)$ if for every Σ-model M we have $M \models \rho$ iff $M \models \rho_0$ or $M \models \rho_1$. The extension to the infinitary case is straightforward. A sentence $\rho \in \mathbb{S}en(\Sigma)$ is called a semantic disjunction of the set E if for every Σ-model M we have $M \models \rho$ iff $M \models e$ for some $e \in E$.*

3. *a sentence $\rho \in \mathbb{S}en(\Sigma)$ is called a semantic existential quantification of a sentence $\rho' \in \mathbb{S}en(\Sigma')$ over the signature morphism $\chi : \Sigma \to \Sigma'$ if for every Σ-model M we have $M \models \rho$ iff there exists a χ-expansion M' of M, i.e. $M' \restriction_\chi = M$, that satisfies ρ'.*

   A similar definition can be given for universal quantification.

Distinguished negation $\neg$, disjunction $\vee$, and existential quantification $(\exists\_)$ are called *first-order constructors* for sentences and they have the semantical meaning defined above.

Throughout this paper we assume the following commutativity of first-order constructors with the signature morphisms, i.e. for every signature morphism $\varphi : \Sigma \to \Sigma_1$ and each Σ-sentence

1. $\neg e$, $\varphi(\neg e) = \neg\varphi(e)$,

2. $\vee E$, $\varphi(\vee E) = \vee\varphi(E)$, and

3. $(\exists\chi)e'$, there exists a pushout

$$\begin{tikzcd} \Sigma' \arrow[r, dotted, "\varphi'"] & \Sigma'_1 \\ \Sigma \arrow[u, dotted, "\chi"] \arrow[r, "\varphi"'] & \Sigma_1 \arrow[u, "\chi'"'] \end{tikzcd}$$

   such that $\varphi((\exists\chi)e') = (\exists\chi_1)\varphi'(e')$.

Very often quantification is considered only for a restricted class of signature morphisms. For example, quantification in **FOL** considers only the finitary signature extensions with constants. Based on these connectives we can also define the other first-order constructers like $\wedge$, *false*, $(\forall\_)$ using the classical definitions.

Chapter 3

Entailment Systems

It is difficult (impossible in many cases) to establish the truth using the semantic consequence relation provided by the notion of institution. We introduce syntactic approach to the truth by defining consequence relations based on syntactic entities only (in the context of entailment systems). This is the most efficient way to demonstrate the truth. We justify the correctness of our proof measures by semantic grounds, i.e. we define soundness and completeness in the presence of model theory.

The entailment systems have been formalized in [48] in the institutional theory. A more general approach to demonstrate the truth is by using proof systems which have been introduced in [52] and developed in [23]. All the results in this chapter are particular cases or variations of the ones in [23]. Our notion of proof rule is more general than the one in [23] allowing to obtain some results uniformly.

3.1 Definition and Compactness

A *sentence system* $(\mathbb{S}ig, \mathbb{S}en)$ consists of a category of signatures $\mathbb{S}ig$ and a sentence functor $\mathbb{S}en : \mathbb{S}ig \to \mathbb{S}et$.

Definition 3.1.1. *An entailment system* $(\mathbb{S}ig, \mathbb{S}en, \vdash)$ *consists of a sentence system* $(\mathbb{S}ig, \mathbb{S}en)$ *and a family of entailment relations* $\vdash = \{\vdash_\Sigma\}_{\Sigma \in |\mathbb{S}ig|}$ *between sets of sentences with the following properties:*

$(Anti\text{-}monotonicity)$ $E_1 \vdash_\Sigma E_2$ *if* $E_2 \subseteq E_1$,
$(Transitivity)$ $E_1 \vdash_\Sigma E_3$ *if* $E_1 \vdash_\Sigma E_2$ *and* $E_2 \vdash_\Sigma E_3$, *and*
$(Unions)$ $E_1 \vdash_\Sigma E_2 \cup E_3$ *if* $E_1 \vdash_\Sigma E_2$ *and* $E_1 \vdash_\Sigma E_3$.
$(Translation)$ $E \vdash_\Sigma E'$ *implies* $\varphi(E) \vdash_{\Sigma'} \varphi(E')$ *for all* $\varphi : \Sigma \to \Sigma'$

We say that the entailment system is *weak* when it satisfies the first three properties, i.e. $Translation$ is omitted from the above definition. When we allow infinite $Unions$, i.e. $E \vdash_\Sigma \bigcup_{i \in J} E_i$ if $E \vdash_\Sigma E_i$ for all $i \in J$, we call the entailment system *infinitary*. In any institution $I = (\mathbb{S}ig, \mathbb{S}en, \mathbb{M}od, \models)$, the semantic consequence relation $\models$ between sets of sentences gives an example of an infinitary entailment system $(\mathbb{S}ig, \mathbb{S}en, \models)$, which is called the *semantic entailment system* of the institution I. When there is no danger of confusion we may omit the subscript Σ from $\vdash_\Sigma$ and for every signature morphism $\varphi \in \mathbb{S}ig$, we sometimes let φ denote the sentence translation $\mathbb{S}en(\varphi)$. For the sake of simplicity of notations we will write $\Gamma \vdash_\Sigma \rho$ instead of $\Gamma \vdash_\Sigma \{\rho\}$, where Γ is any set of Σ-sentences and ρ a Σ-sentence.

Definition 3.1.2. *An entailment system $E = (\mathbb{S}ig, \mathbb{S}en, \vdash)$ is compact whenever $\Gamma \vdash E_f$ for a finite set of sentences $E_f \subseteq \mathbb{S}en(\Sigma)$, there exists $\Gamma_f \subset \Gamma$ finite such that $\Gamma_f \vdash E_f$.*

For each entailment system $E = (\mathbb{S}ig, \mathbb{S}en, \vdash)$ one can easily construct the *compact entailment subsystem* $E^c = (\mathbb{S}ig, \mathbb{S}en, \vdash^c)$ by defining the entailment relation $\vdash^c$ as follows: $\Gamma \vdash^c E$ iff for each $E_f \subseteq E$ finite there exists $\Gamma_f \subseteq \Gamma$ finite such that $\Gamma_f \vdash E_f$.

Lemma 3.1.3. *$E^c = (\mathbb{S}ig, \mathbb{S}en, \vdash^c)$ is an entailment system.*

Proof. We need to show that E^c satisfies

1. *Anti-monotonicity*: assuming $E_2 \subseteq E_1$ we prove $E_1 \vdash^c E_2$. For any finite set $E_2' \subseteq E_2$ there exists a finite set $E_1'(= E_2') \subseteq E_1$ such that $E_1' \vdash E_2'$ which implies $E_1 \vdash^c E_2$.

2. *Transitivity*: assuming that $E_1 \vdash^c E_2$ and $E_2 \vdash^c E_3$ we prove $E_1 \vdash^c E_3$. Let $E_3' \subseteq E_3$ finite, since $E_2 \vdash^c E_3$ there exists $E_2' \subseteq E_2$ finite such that $E_2' \vdash E_3'$. Because $E_1 \vdash E_2$ there is a finite set $E_1' \subseteq E_1$ such that $E_1' \vdash E_2'$. By the *Transitivity* of E we obtain $E_1' \vdash E_3'$ which implies $E_1 \vdash_c E_3$.

3. *Unions*: assuming that $E_1 \vdash^c E_2$ and $E_1 \vdash^c E_3$ we prove $E_1 \vdash^c E_2 \cup E_3$. Let $E \subseteq E_2 \cup E_3$ finite; there exists finite sets $E_2' \subseteq E_2$ and $E_3' \subseteq E_3$ such that $E_2' \cup E_3' = E$; because $E_1 \vdash^c E_2$ and $E_1 \vdash^c E_3$ there is finite sets $E', E'' \subseteq E_1$ such that $E' \vdash E_2'$ and $E'' \vdash E_3'$, respectively; by *Anti-monotonicity* and *Transitivity* property we have $E_1' = E' \cup E'' \vdash E_2'$ and $E_1' \vdash E_3'$ and by *Unions* we obtain $E_1' \vdash E_2' \cup E_3' = E$. Because E was arbitrary we get $E_1 \vdash^c E_2 \cup E_3$.

4. *Translation* : assuming that $E_1 \vdash^c_\Sigma E_2$ we prove $\varphi(E_1) \vdash^c_{\Sigma'} \varphi(E_2)$ for all signature morphisms $\varphi : \Sigma \to \Sigma'$. Let $E_2'' \subseteq \varphi(E_2)$ finite; there exists $E_2' \subseteq E_2$ finite such that $\varphi(E_2') = E''$ and since $E_1 \vdash^c E_2$ there is $E_1' \subseteq E_1$ finite such that $E_1' \vdash E_2'$; by *Transitivity* we have $\varphi(E_1') \vdash \varphi(E_2')$; note that $E_1'' = \varphi(E_1')$ is finite and $E_2'' = \varphi(E_2')$. Because E_2'' was arbitrary we get $\varphi(E_1) \vdash^c \varphi(E_2)$.

(Q.E.D.)

Definition 3.1.4. *The entailment system $E = (\mathbb{S}ig, \mathbb{S}en, \vdash)$ of an institution $I = (\mathbb{S}ig, \mathbb{S}en, \mathbb{M}od, \models)$ is sound (resp. complete) when $\Gamma \vdash_\Sigma \rho$ implies $\Gamma \models_\Sigma \rho$ (resp. $\Gamma \models_\Sigma \rho$ implies $\Gamma \vdash_\Sigma \rho$) for every set Γ of Σ-sentences and any Σ-sentence ρ.*

3.2 Free entailment systems

Given a sentence system $(\mathbb{S}ig, \mathbb{S}en)$, we let $|P(\mathbb{S}ig)|$ denote the class of sets of signatures of the form $W = \{\Sigma_i \in |\mathbb{S}ig| \mid i \in J\}$, where J is any set. For every signature $\Sigma \in |\mathbb{S}ig|$ we denote by $P\mathbb{S}en_\Sigma$ the set $P(\mathbb{S}en(\Sigma)) \times P(\mathbb{S}en(\Sigma))$. For each set of signatures $W = \{\Sigma_i \in |\mathbb{S}ig| \mid i \in J\}$ we denote by $P\mathbb{S}en_W$ the cartesian product $\bigotimes_{i \in J} P\mathbb{S}en_{\Sigma_i}$.

Definition 3.2.1. *A system of proof rules $(\mathbb{S}ig, \mathbb{S}en, Rl)$ consists of a sentence system $(\mathbb{S}ig, \mathbb{S}en)$ and a family of sets of rules $Rl = (Rl_{W \to \Sigma})_{W \in |P(\mathbb{S}ig)|, \Sigma \in |\mathbb{S}ig|}$ such that $Rl_{W \to \Sigma} \subseteq P\mathbb{S}en_W \times P\mathbb{S}en_\Sigma$. For any proof rule $r \in Rl_{W \to \Sigma}$ we say that W is the arity and Σ is the sort of r.*

A proof rule of arity $W = \{\Sigma_i \mid i \in J\}$ and sort Σ may be written as

$$\frac{\{\langle E_i, E'_i\rangle \mid i \in J\}}{\langle E, E'\rangle}$$

or even as

$$\frac{\{E_i \vdash_{\Sigma_i} E'_i \mid i \in J\}}{E \vdash_{\Sigma} E'}$$

or

$$E \vdash_{\Sigma} E' \text{ if } E_i \vdash_{\Sigma_i} E'_i \text{ for all } i \in J$$

Note that any entailment system may be seen as a system of rules with the empty arity. Given an entailment system $E = (\mathbb{S}ig, \mathbb{S}en, \vdash)$ and a system of rules $R = (\mathbb{S}ig, \mathbb{S}en, Rl)$ we say that the entailment system E *satisfies a rule* $\frac{\{\langle E_i, E'_i\rangle \mid i \in J\}}{\langle E, E'\rangle}$ in Rl if $E_i \vdash E'_i$, for all $i \in J$, implies $E \vdash E'$. E satisfies Rl when E satisfies every rule in Rl.

Definition 3.2.2. *Given an entailment system $E = (\mathbb{S}ig, \mathbb{S}en, \vdash)$ and a system of rules $R = (\mathbb{S}ig, \mathbb{S}en, Rl)$, E* satisfies a rule $\frac{\{\langle E_i, E'_i\rangle \mid i \in J\}}{\langle E, E'\rangle}$ *in Rl if $E_i \vdash E'_i$, for all $i \in J$, implies $E \vdash E'$. E satisfies Rl when E satisfies every rule in Rl.*

The system of rules $R = (\mathbb{S}ig, \mathbb{S}en, Rl)$ of an institution $I = (\mathbb{S}ig, \mathbb{S}en, \mathbb{M}od, \models)$ is sound if the semantic entailment system $(\mathbb{S}ig, \mathbb{S}en \models)$ satisfies Rl.

Remark 3.2.3. *A system of rules $(\mathbb{S}ig, \mathbb{S}en, Rl)$ generates freely an entailment system $(\mathbb{S}ig, \mathbb{S}en, \vdash)$, where $\vdash$ is the least entailment relation which satisfies Anti-monotonicity, Transitivity, Unions, Translations, and the rules in Rl. The free infinitary entailment system is obtain by replacing Unions with infinite Unions in the above statement.*

Remark 3.2.4. *Consider an entailment system $E = (\mathbb{S}ig, \mathbb{S}en, \vdash)$ freely generated by a system of rules $R = (\mathbb{S}ig, \mathbb{S}en, Rl)$. Then for any entailment system $E' = (\mathbb{S}ig, \mathbb{S}en, \vdash')$ satisfying the rules in R we have $\vdash \subseteq \vdash'$.*

Definition 3.2.5. *We say that a rule $\frac{\{E_i \vdash_{\Sigma_i} E'_i \mid i \in J\}}{E \vdash_{\Sigma} E'}$ is* finitely generated *when E is finite.*

The result bellow is a corollary of Lemma 3.1.3.

Proposition 3.2.6. *The entailment system freely generated by a system of finitely generated rules is compact.*

Proof. Consider a system of finitely generated rules $R = (\mathbb{S}ig, \mathbb{S}en, Rl)$ and let $E = (\mathbb{S}ig, Sen, \vdash)$ be the entailment system freely generated by R. Assume that $E^c = (\mathbb{S}ig, \mathbb{S}en, \vdash^c)$ is the compact entailment subsystem of E. It is easy to notice that E^c satisfies the rules in Rl. Indeed, for any rule $\frac{\{\langle E_i, E'_i\rangle \mid i \in J\}}{\langle E, E'\rangle}$ in Rl, if $E_i \vdash^c E'_i$, for all $i \in J$, then $E_i \vdash E'_i$, for all $i \in J$, and since E satisfies all the rules in Rl we have $E \vdash E'$; given $E'_f \subseteq E'$ finite by *Anti-monotonicity* we have $E' \vdash E'_f$ and by *Transitivity* $E \vdash E'_f$; since E is finite and E'_f was arbitrary we get $E \vdash^c E'_f$. Because $\vdash$ is the least entailment relation satisfying the rules in Rl by Remark 3.2.4 $\vdash \subseteq \vdash^c$ which implies $\vdash = \vdash^c$. (Q.E.D.)

The following lemma shows that the free construction of entailment systems from systems of rules preserve the soundness property and explains the practice of establishing soundness of the entailment systems which consists only of checking the soundness of the rules.

Proposition 3.2.7. *The (infinitary) entailment system of an institution is sound whenever it is freely generated by a sound system of rules.*

Proof. Assume an institution $I = (\mathbb{S}ig, \mathbb{S}en, \mathbb{M}od, \models)$ with a sound system of rules $R = (\mathbb{S}ig, \mathbb{S}en, Rl)$. Let $E = (\mathbb{S}ig, \mathbb{S}en, \vdash)$ be the (infinitary) entailment system freely generated by R. Since $(\mathbb{S}ig, \mathbb{S}en, \models)$ satisfies Rl by Remark 3.2.4 we have $\vdash \subseteq \models$ which implies E is sound for I. (Q.E.D.)

3.3 Proof internal logic

Entailment systems with disjunctions. We say that an entailment system has disjunctions $(\vee\_)$ if it satisfies the following rules:

$$(Disjunction\ introduction)\ \frac{}{e \vdash \vee E}$$

for all sentences $\vee E$ such that $e \in E$, where E is a finite set of sentences.

$$(Disjunction\ elimination)\ \frac{\{\Gamma \vdash \vee E\} \cup \{\Gamma \cup \{e\} \vdash \rho \mid e \in E\}}{\Gamma \vdash \rho}$$

for all sentences $\vee E$, where E is a finite set of sentences, Γ is any set of sentences, and ρ is a sentence.

Proposition 3.3.1. *The entailment system with disjunctions freely generated by a compact entailment system is compact.*

Proof. Assume a compact entailment system $E = (\mathbb{S}ig, \mathbb{S}en, \vdash)$ and let $E' = (\mathbb{S}ig, \mathbb{S}en, \vdash')$ be the entailment system with disjunctions freely generated by E. We show that the compact entailment subsystem $E^c = (\mathbb{S}ig, \mathbb{S}en, \vdash^c)$ of E' has disjunctions. Since the rules of *Disjunction introduction* are finitely generated, E^c satisfies *Disjunction introduction*. Now assume that $\Gamma \vdash^c \vee E$ and for every $e \in E$ we have $\Gamma \cup \{e\} \vdash^c \rho$. By the definition of $\vdash^c$ there are finite subsets $\Gamma' \subseteq \Gamma$ and $\Gamma_e \subseteq \Gamma$ such that $\Gamma' \vdash' \vee E$ and $\Gamma_e \cup \{e\} \vdash' \rho$, for all $e \in E$. Because E is finite the set $\Gamma_f = \Gamma' \cup (\bigcup_{e \in E} \Gamma_e)$ is finite. By *Anti-monotonicity* we have $\Gamma_f \vdash' \vee E$ and $\Gamma_f \cup \{e\} \vdash' \Gamma_e \cup \{e\}$, for all $e \in E$. By *Transitivity* $\Gamma_f \vdash' \vee E$ and $\Gamma_f \cup \{e\} \vdash' \rho$, for all $e \in E$. Since the entailment system E' satisfies *Disjunction elimination*, we have $\Gamma_f \vdash' \rho$ which implies $\Gamma \vdash^c \rho$. Hence E^c satisfies the rules of *Disjunction elimination*. Since $E^c = (\mathbb{S}ig, \mathbb{S}en \vdash^c)$ is an entailment system with disjunctions satisfying the rules $\frac{}{E \vdash E'}$ in E (regarded as a system of proof rules), by Remark 3.2.4 we have $\vdash \subseteq \vdash^c$ which implies $\vdash = \vdash^c$. (Q.E.D.)

The definition of entailment systems with disjunctions can be straightforwardly extended to the infinitary case by allowing the set E of sentences to be infinite in the definitions of *Disjunction introduction* and *Disjunction elimination*. Proposition 3.3.1 may not hold for the free entailment systems with infinitary disjunctions $(\bigvee\_)$.

One can easily notice that the semantic entailment system of an institution with disjunctions satisfies the rules of *Disjunction introduction* and *Disjunction elimination*. The following is a corollary of Proposition 3.2.7 and shows that free entailment systems with disjunctions preserves soundness property.

Corollary 3.3.2. *The (infinitary) entailment system with (infinitary) disjunctions is sound for an institution when is freely generated by a sound system of rules.*

Entailment systems with false. We say that an entailment system has false ($false$) if it satisfies the following rules:

$$(False)\ \frac{}{false \vdash \rho}$$

where ρ is any sentence.

Proposition 3.3.3. *The entailment system with false freely generated by a compact entailment system is compact too.*

Proof. Since the rules of *False* are finitely generated any entailment system with negations and freely generated by a compact entailment system is compact. (Q.E.D.)

The entailment system of an institution which admits false satisfies the rules of *False* and by Proposition 3.2.7 the free entailment systems with false preserves soundness.

Corollary 3.3.4. *The (infinitary) entailment system with false of an institution is sound when is freely generated by a sound system of rules.*

Entailment systems with negations. We say that an entailment system has negations ($\neg\_$) if it satisfies the following rules:

$$(Red_1)\ \frac{\Gamma \cup \{\rho\} \vdash false}{\Gamma \vdash \neg\rho}$$

where Γ is a set of sentences and ρ is a sentence, and

$$(Red_2)\ \frac{\Gamma \vdash \neg\rho}{\Gamma \cup \{\rho\} \vdash false}$$

where Γ is a set of sentences and ρ is a sentence.

Proposition 3.3.5. *The entailment system with negations freely generated by a compact compact entailment system is compact.*

Proof. Assume a compact entailment system $E = (\mathbb{S}ig, \mathbb{S}en, \vdash)$ and let $E' = (\mathbb{S}ig, \mathbb{S}en, \vdash')$ be the entailment system with negations freely generated by E. We show that the compact entailment subsystem $E^c = (\mathbb{S}ig, \mathbb{S}en, \vdash^c)$ of E' has negations, i.e. E^c satisfies

1. Red_1: assuming that $\Gamma \cup \{\rho\} \vdash^c false$ we prove $\Gamma \vdash^c \neg\rho$. By the definition of $\vdash^c$ there is $\Gamma' \subseteq \Gamma$ finite such that $\Gamma' \cup \{\rho\} \vdash' false$. Since E' has negations we have $\Gamma' \vdash' \neg\rho$ which implies $\Gamma \vdash^c \neg\rho$.

2. Red_2: assuming that $\Gamma \vdash^c \neg\rho$ we prove $\Gamma \cup \{\rho\} \vdash^c false$. By the definition of $\vdash^c$ there is $\Gamma' \subseteq \Gamma$ finite such that $\Gamma' \vdash' \neg\rho$. Since E' has negations we have $\Gamma' \cup \{\rho\} \vdash' false$ which implies $\Gamma \cup \{\rho\} \vdash^c false$.

Since $E' = (\mathbb{S}ig, \mathbb{S}en, \vdash')$ is the free entailment system with negations over $E = (\mathbb{S}ig, \mathbb{S}en, \vdash)$ and $E^c = (\mathbb{S}ig, \mathbb{S}en, \vdash^c)$ has negations and satisfies the rules $\frac{}{E \vdash E'}$ in E, by Remark 3.2.4 we have $\vdash' \subseteq \vdash^c$ which implies $\vdash' = \vdash^c$. (Q.E.D.)

The following is a corollary of Proposition 3.2.7 and shows that free entailment systems with negations preserves soundness property.

Remark 3.3.6. *The conjunction ($\bigwedge\_$) is introduced using the disjunction and the negation:* $\bigwedge E = \neg(\bigvee_{e\in E} \neg e)$ *for any set E of sentences.*

Corollary 3.3.7. *The (infinitary) entailment system with negations is sound for an institution when it is freely generated by a sound system of rules.*

Entailment systems with implications. We say that an entailment system has implications ($\_ \Rightarrow \_$) if it satisfies the following rules:

$$(Implications_1)\ \frac{\Gamma \cup H \vdash C}{\Gamma \vdash (\wedge H) \Rightarrow C}$$

for every sentence $(\wedge H) \Rightarrow C$ and set Γ of sentences, where H is a finite set of sentences, C is a sentence, $\wedge H$ is the conjunction of H and $(\wedge H) \Rightarrow C$ is the implication of C by $\wedge H$, and

$$(Implications_2)\ \frac{\Gamma \vdash (\wedge H) \Rightarrow C}{\Gamma \cup H \vdash C}$$

for every sentence $(\wedge H) \Rightarrow C$ and set Γ of sentences, where H is a finite set of sentences and C is a sentence.

We assume that the conjunction ($\wedge\_$) binds tighter then the implication ($\_ \Rightarrow \_$) and we write $\wedge H \Rightarrow C$.

Proposition 3.3.8. *The entailment system with implications freely generated by a compact entailment system is compact.*

Proof. Consider a compact entailment system $E = (\mathbb{S}ig, \mathbb{S}en, \vdash)$ and let $E' = (\mathbb{S}ig, \mathbb{S}en, \vdash')$ be the entailment system with implications freely generated by E. We show that the compact entailment subsystem $E^c = (\mathbb{S}ig, \mathbb{S}en, \vdash^c)$ of E' has implications, i.e. E^c satisfies

1. $Implications_1$: assuming that $\Gamma \cup H \vdash^c C$ we prove that $\Gamma \vdash^c \wedge H \Rightarrow C$. By the definition of $\vdash^c$ there is $\Gamma' \subseteq \Gamma$ finite such that $\Gamma' \cup H \vdash' C$. Since E' has implications we have $\Gamma' \vdash' \wedge H \Rightarrow C$ which implies $\Gamma \vdash^c \wedge H \Rightarrow C$.

2. $Implications_2$: assuming that $\Gamma \vdash^c \wedge H \Rightarrow C$ we prove that $\Gamma \cup H \vdash^c C$. By the definition of $\vdash^c$ there is $\Gamma' \subseteq \Gamma$ finite such that $\Gamma' \vdash' H \Rightarrow C$. Since E' has implications we have $\Gamma' \cup H \vdash' C$. Because $\Gamma' \cup H$ is finite we get $\Gamma \vdash^c \wedge H \Rightarrow C$.

Since $E' = (\mathbb{S}ig, \mathbb{S}en, \vdash')$ is the free entailment system with implications over $E = (\mathbb{S}ig, \mathbb{S}en, \vdash)$ and the entailment system $E^c = (\mathbb{S}ig, \mathbb{S}en, \vdash^c)$ has implications and satisfies every rule $\frac{}{E \vdash E'}$ in E, by Remark 3.2.4 we have $\vdash' \subseteq \vdash^c$ which implies $\vdash' = \vdash^c$. (Q.E.D.)

One can easily extend the definition of entailment systems with implications to the infinitary case by considering the set H of sentences infinite in the definition of $Implications_1$ and $Implications_2$. The compactness result of Proposition 3.3.8 may not hold for the free entailment systems with infinitary implications.

The following is a corollary of Proposition 3.2.7 and shows that free entailment systems with implications preserves soundness property.

Corollary 3.3.9. *The (infinitary) entailment system with (infinitary) implications is sound for an institution when is freely generated by a sound system of rules.*

Entailment systems with universal quantifiers. We say that an entailment system $(\mathbb{S}ig, \mathbb{S}en, \vdash)$ has universal quantifications $(\forall\_)$ if it satisfies the following rules:

$$(Generalization_1)\ \frac{\Gamma \vdash_\Sigma (\forall\chi)\rho'}{\chi(\Gamma) \vdash_{\Sigma'} \rho'}$$

for every set of sentences Γ, each sentence $(\forall\chi)\rho'$, where $\Sigma \xrightarrow{\chi} \Sigma' \in D$, and

$$(Generalization_2)\ \frac{\chi(\Gamma) \vdash_{\Sigma'} \rho'}{\Gamma \vdash_\Sigma (\forall\chi)\rho'}$$

for every set of sentences Γ, and each sentence $(\forall\chi)\rho'$, where $\Sigma \xrightarrow{\chi} \Sigma' \in D$.

Proposition 3.3.10. *The entailment system with universal quantifications freely generated by a compact entailment system is compact.*

Proof. Assume a compact entailment system $E = (\mathbb{S}ig, \mathbb{S}en, \vdash)$ and let $E' = (\mathbb{S}ig, \mathbb{S}en, \vdash')$ be the entailment systems with universal quantifications freely generated by E. We show that the compact entailment subsystem $E^c = (\mathbb{S}ig, \mathbb{S}en, \vdash^c)$ of E' satisfies

1. $Generalization_1$: assuming that $\Gamma \vdash^c_\Sigma (\forall\chi)\rho'$ we prove $\chi(\Gamma) \vdash^c_{\Sigma'} \rho'$, where $\chi : \Sigma \to \Sigma'$. By the definition of $\vdash^c$ there is $\Gamma' \subseteq \Gamma$ finite such that $\Gamma \vdash'_\Sigma (\forall\chi)\rho'$. Since E' has universal quantifications we have $\chi(\Gamma') \vdash'_{\Sigma'} \rho'$ and because $\chi(\Gamma')$ is finite we get $\chi(\Gamma) \vdash^c_{\Sigma'} \rho'$.

2. $Generalization_2$: assuming that $\chi(\Gamma) \vdash^c_{\Sigma'} \rho'$ we prove $\Gamma \vdash^c_\Sigma (\forall\chi)\rho'$, where $\chi : \Sigma \to \Sigma'$. By the definition of $\vdash^c$ there is $\Gamma' \subseteq \chi(\Gamma)$ finite such that $\Gamma' \vdash'_{\Sigma'}$. There exists $\Gamma_f \subseteq \Gamma$ finite such that $\chi(\Gamma_f) = \Gamma'$. Since E' has universal quantifications we have $\Gamma_f \vdash'_\Sigma (\forall\chi)\rho'$ which implies $\Gamma \vdash^c_\Sigma (\forall\chi)\rho'$.

Since $E' = (\mathbb{S}ig, \mathbb{S}en, \vdash')$ is the free entailment system with universal quantifications over $E = (\mathbb{S}ig, \mathbb{S}en, \vdash)$ and $E^c = (\mathbb{S}ig, \mathbb{S}en, \vdash^c)$ has universal quantifications and satisfies the rules $\frac{}{E \vdash E'}$ in E, by Remark 3.2.4 we have $\vdash' \subseteq \vdash^c$ which implies $\vdash' = \vdash^c$. (Q.E.D.)

The following is a corollary of Proposition 3.2.7 and shows that free entailment systems with universal quantifiers preserves soundness property.

Corollary 3.3.11. *The (infinitary) entailment system with universal quantifiers is sound for an institution when is freely generated by a sound system of rules.*

Entailment systems with existential quantifiers. We say that an entailment system $(\mathbb{S}ig, \mathbb{S}en, \vdash)$ has existential quantifications $(\exists\_)$ if it satisfies the following rules:

$$(Generalization'_1)\ \frac{(\exists\chi)\rho' \vdash_\Sigma e}{\rho' \vdash_{\Sigma'} \chi(e)}$$

for every sentence e, each sentence $(\exists\chi)\rho'$, where $\Sigma \xrightarrow{\chi} \Sigma' \in D$, and

$$(Generalization'_2)\ \frac{\rho' \vdash_{\Sigma'} \chi(e)}{(\exists\chi)\rho' \vdash_\Sigma e}$$

for every sentence e, each sentence $(\exists\chi)\rho'$, where $\Sigma \xrightarrow{\chi} \Sigma' \in D$.

Proposition 3.3.12. *The entailment system with existential quantifications freely generated by a compact entailment system is compact.*

Proof. By noticing that the rules of $Generalizaation'_1$ and $Generalization'_2$ are finitely generated. (Q.E.D.)

The following is a corollary of Proposition 3.2.7 and shows that free entailment systems with existential quantifiers preserves soundness property.

Corollary 3.3.13. *The (infinitary) entailment system with existential quantifiers is sound for an institution when is freely generated by a sound system of rules.*

Consider a system of rules $R = (\mathbb{S}ig, \mathbb{S}en, Rl)$. We say that a rule $r \in R_{W \to \Sigma}$ is *infinitary* when its arity W is an infinite set. If R contains infintary rules, like infinitary versions of $Disjunction\ elimination$ or $Implications$, the entailment system freely generated by R is not compact, in general.

All the results in this section hold not only for the entailment systems but also for the weak entailment systems but for the sake of simplicity we do not mention it above. One can omit the $Translation$ property from the definition of entailment systems and all the results in this section will hold. We define the rules of $Generalization$ as the union of the rules of $Generalization_1$ and $Generalization_2$. Similarly we define $Generalization'$, $Implications$ and Red.

Entailment systems have been introduced in [48] in order to formalize the notion of syntactic consequence in the institutional model theory. Abstract systems of proof rules have been introduced in [23] which also developed the free proof systems defined in [52]. The results concerning the compactness and soundness of free entailment systems are due to [23] and they are developed in the more general setting of proof systems. Entailment systems are just proof systems such that the category of proofs for a given signature is a preorder. Our notion of proof rule is more general than in [23] since it admits arity, and it allows to obtain uniformly some of the results.

Chapter 4

Equational Deduction

Equational deduction is reasoning with properties of equality and constitutes the basis of formal verification in algebraic specifications. We give a system of rules for conditional equational logic that is sound and such that the entailment system freely generated by the given rules is complete. The proof of completeness is organized on three layers reflecting the structure of the sentences, and allowing the generalization to the institution level. In fact, the completeness result here is due to [16] and it is significantly different from the one in [35] where the proof rules specific to the **CEQL** (like *Reflexivity*, *Symmetry*, *Transitivity* and *Congruence*) are mixed with the rules of *Generalization*, and the rules of *Substitutivity* are combined somehow with the rules of *Implications* making the result a little bit weaker. More precisely in [35] it is proved that

$$\Gamma \models (\forall X)t = t' \text{ implies } \Gamma \vdash (\forall X)t = t'$$

for every set Γ of conditional equations and each equation $(\forall X)t = t'$, while here

$$\Gamma \models (\forall X) \wedge H \Rightarrow (t = t') \text{ implies } \Gamma \vdash (\forall X) \wedge H \Rightarrow (t = t')$$

for every set Γ of conditional equations and each conditional equation $(\forall X) \wedge H \Rightarrow (t = t')$.

We specify different systems by conditional equations and we infer properties from the formal specifications. The specifications will be written using the CafeOBJ notations. CafeOBJ is an algebraic specification language, the modern successor of OBJ. Its definition is given in [25] and a presentation of the logical foundations can be found in [26].

4.1 Preliminaries and Definition

It is convenient (but not always necessary) for each variable symbol to have just one sort; therefore we assume that any S-indexed set $X = (X_s)_{s \in S}$ used to provide variables for a signature (S,F) is such that X_{s_1} and X_{s_2} are disjoint whenever $s_1 \neq s_2$, and such that all symbols in X are distinct from those in F.

Definition 4.1.1 (Ground reachable algebras)**.** *A (S,F)-algebra M is ground reachable if its carrier sets consists only of interpretations of terms, i.e. the unique morphism $T_F \to M$ is surjective.*

Notations. Recall that a (S,F)-algebra M provides an interpretation for each operation symbol in F, and in particular, for each constant symbol in F. If X is a set of new constant symbols (a set of variables), then an interpretation for X is just a (many-sorted) function f :

$X \to M$. Thus a (S,F)-algebra M and a function $f : X \to M$ give an interpretation in M of $(S,F \cup X)$, allowing the pair (M, f) to be seen as a $(S,F \cup X)$-algebra. In such situation we call $f : X \to M$ an *interpretation* or an *assignment* of the variable symbols in X.

Definition 4.1.2 (Algebraic substitutions)**.** *Let (S,F) be an algebraic signature. A (S,F)-substitution of F-terms with variables in Y for variables in X is an arrow $\theta : X \to T_F(Y)$. The unique extension of θ to*

1. *F-terms with variables in X is $\overline{\theta} : T_F(X) \to T_F(Y)$ which replaces the variables $x \in X$ with $\theta(x)$ in each $(F \cup X)$-term t.*

2. *sentences in $\mathbb{S}en(S,F \cup X)$ is $\mathbb{S}en(\theta) : \mathbb{S}en(S,F \cup X) \to \mathbb{S}en(S,F \cup Y)$ which replaces all symbols from X with the corresponding $(F \cup Y)$-terms according to θ. This can be formally defined as follows:*

   - *$\mathbb{S}en(\theta)(t = t')$ is defined as $\overline{\theta}(t) = \overline{\theta}(t')$ for each $(S,F \cup X)$-equation $t = t'$.*
   - *$\mathbb{S}en(\theta)(\wedge H \Rightarrow C)$ is defined as $\wedge \mathbb{S}en(\theta)(H) \Rightarrow \mathbb{S}en(\theta)(C)$ for each quantifier-free $(S,F \cup X)$-sentence $\wedge H \Rightarrow C$.*
   - *$\mathbb{S}en(\theta)((\forall Z) \wedge H \Rightarrow C) = (\forall Z)\mathbb{S}en(\theta_Z)(\wedge H \Rightarrow C)$ for each $(S,F \cup X)$-sentence $(\forall Z) \wedge H \Rightarrow C$, where θ_Z is the trivial extension of θ to a $(S,F \cup Z)$-substitution [1].*

   As in case of signature morphisms when there is no danger of confusion we let θ to denote the sentence translation $\mathbb{S}en(\theta)$.

For any $(S,F \cup Y)$-model (M, f) we define the $(S,F \cup X)$-model $(M, f) \restriction_\theta$ as $(M, \theta; \overline{f})$, where $\overline{f} : T_F(Y) \to M$ is the unique extension of f to a (S,F)-morphism.

Notation. Given $t \in T_F(X)$ and $\theta : X \to T_F(Y)$ such that $X = \{x_1, \ldots, x_n\}$ and $\theta(x_i) = t_i$ for $i \in \{1, \ldots, n\}$, then we may write $\overline{\theta}(t)$ in the form $t(x_1 \leftarrow t_1, \ldots, x_n \leftarrow t_n)$.

Lemma 4.1.3 (Satisfaction condition for substitutions)**.** *Given a (S,F)- substitution $\theta : X \to T_F(Y)$, for every sentence $\rho \in \mathbb{S}en(S,F \cup X)$ and each $(S,F \cup Y)$-algebra M we have $M \models \mathbb{S}en(\theta)(\rho)$ iff $M \restriction_\theta \models \rho$.*

Proof. By noticing that $\mathbb{M}od(\theta)(M)_t = M_{\overline{\theta}(t)}$ for each $(F \cup X)$-term t, and by a straightforward induction on the structure of the sentences. (Q.E.D.)

Definition 4.1.4 (Equational deduction)**.** *The equational entailment system is the least entailment system with implications and universal quantifications and which satisfies the followings rules*

$(Reflexivity)$	$\frac{}{\emptyset \vdash_{(S,F)} t = t}$ *for each term $t \in T_F$*
$(Symmetry)$	$\frac{}{t = t' \vdash_{(S,F)} t' = t}$ *for any terms $t, t' \in T_F$*
$(Transitivity)$	$\frac{}{\{t = t', t' = t''\} \vdash_{(S,F)} t = t''}$ *for any terms $t, t', t'' \in T_F$*
$(Congruence)$	$\frac{}{\{t_i = t'_i \mid 1 \le i \le n\} \vdash_{(S,F)} \sigma(t_1, \ldots, t_n) = \sigma(t'_1, \ldots, t'_n)}$ *for any function symbol $\sigma \in F$ and terms $t_i \in T_F$, where $i \in \{1, \ldots, n\}$*
$(Substitutivity)$	$\frac{}{(\forall Y)\rho \vdash_{(S,F)} (\forall X)\theta(\rho)}$ *for any conditional equation $(\forall Y)\rho$ and substitution $\theta : Y \to T_F(X)$*

[1] Without loss of generality we assume that $Z_s \cap Y_s = \emptyset$, for all $s \in S$.

Proposition 4.1.5 (Soundness of **CEQL**). *The equational entailment system is sound.*

Proof. By Proposition 3.2.7, and Corollaries 3.3.9 and 3.3.11 we have only to show the soundness of the generating rules. Let M be a (S,F)-algebra.

1. *(Reflexivity)* For any term $t \in T_F$, we have $M_t = M_t$, hence $M \models t = t$.

2. *(Symmetry)* For any terms $t, t' \in T_F$ of the same sort, if $M \models t = t'$ then $M_t = M_{t'}$. By the symmetry of the equality we have $M_{t'} = M_t$, hence $M \models t' = t$.

3. *(Transitivity)* For any terms $t, t', t'' \in T_F$ of the same sort, if $M \models t = t'$ and $M \models t' = t''$ then $M_t = M_{t'}$ and $M_{t'} = M_{t''}$. By the transitivity of the equality we have $M_t = M_{t''}$, hence $M \models t = t''$.

4. *(Congruence)* For any terms $\sigma(t_1, \ldots, t_n), \sigma(t'_1, \ldots, t'_n) \in T_F$, where $\sigma \in F$ is an operation symbol and $t_i, t'_i \in T_F$ are terms for all $i \in \{1, \ldots, n\}$, if $M_{t_i} = M_{t'_i}$ for all $i \in \{1, \ldots, n\}$, then $M_\sigma(M_{t_1}, \ldots, M_{t_n}) = M_\sigma(M_{t'_1}, \ldots, M_{t'_n})$ which means $M_{\sigma(t_1,\ldots,t_n)} = M_{\sigma(t'_1,\ldots,t'_n)}$. Hence $M \models \sigma(t_1, \ldots, t_n) = \sigma(t'_1, \ldots, t'_n)$.

5. *(Substitutivity)* Consider a conditional (S,F)-equation $(\forall Y)\rho$, and a substitution $\theta : Y \to T_F(X)$ such that $M \models (\forall Y)\rho$. For any $(S, F \cup X)$-expansion M' of M, since $M' \restriction_\theta$ is a $(S, F \cup Y)$-expansion of M we have $M \restriction_\theta \models \rho$, and by the satisfaction condition for substitutions $M' \models \theta(\rho)$.

(Q.E.D.)

4.2 Completeness

We present a layered completeness result for conditional equational logic. Informally, the completeness of the system of rules for the restriction of conditional equational logic to the atomic sentences is lifted to the completeness of conditional equational logic by firstly adding the rules which deal with logical implication, and then with universal quantification.

Let **AEQL** (*the atomic equational logic*) be the restriction of **CEQL** to the atomic sentences. The entailment system of **AEQL** is freely generated by the rules of *Reflexivity*, *Symmetry*, *Transitivity* and *Congruence*. These rules are sound for **CEQL**, hence for **AEQL** too.

Proposition 4.2.1 (Completeness of **AEQL**). *The followings hold*

1. *The entailment system of* **AEQL** *is compact and complete, and*

2. *for every set of equational atoms Γ and any equation $t = t'$ we have: $\Gamma \models t = t'$ iff $M \models \bigwedge \Gamma \Rightarrow (t = t')$, for all ground reachable algebras M.*

Proof. We let $\vdash$ to denote the entailment relation of **AEQL**.

1. For the compactness part note that all the rules of **AEQL** are finitely generated and by Proposition 3.2.6 the entailment system of **AEQL** is compact. Now we focus on completeness.

   For any set Γ of equational (S,F)-atoms we define $\equiv_\Gamma = \{(t,t') | \Gamma \vdash t = t'\}$. The system of rules for **AEQL** insure that $\equiv_\Gamma$ is a F-congruence. Now note that $\Gamma \vdash t = t'$ iff $t \equiv_\Gamma t'$ iff $t/_{\equiv_\Gamma} = t'/_{\equiv_\Gamma}$ iff $(T_F)_{\equiv_\Gamma} \models t = t'$, where $(T_F)_{\equiv_\Gamma}$ is quotient of the term algebra T_F by the congruence $\equiv_\Gamma$. Now if $\Gamma \models t = t'$ then $(T_F)_{\equiv_\Gamma} \models t = t'$ which means $\Gamma \vdash t = t'$.

2. The implication from left to right is straightforward. Assume that $M \models \bigwedge \Gamma \Rightarrow (t = t')$, for all reachable algebras M. Since $(T_F)_{\equiv_\Gamma}$ is reachable and $(T_F)_{\equiv_\Gamma} \models \Gamma$, we obtain $(T_F)_{\equiv_\Gamma} \models t = t'$ which implies $\Gamma \vdash t = t'$. By the completeness result above we get $\Gamma \models t = t'$.

(Q.E.D.)

Let **QfEQL** (*the quantifier-free equational logic*) be the restriction of **CEQL** to the quantifier-free sentences.The entailment system of **QfEQL** is freely generated by the rules of *Reflexivity*, *Symmetry*, *Transitivity*, *Congruence* and *Implications*.

Proposition 4.2.2 (Completeness of **QfEQL**). *The followings hold*

1. *The entailment system of* **QfEQL** *is compact and complete, and*

2. *for every set of quantifier-free sentences* Γ *and any conditional equation* $\wedge H \Rightarrow C$ *we have:* $\Gamma \models \wedge H \Rightarrow C$ *iff* $M \models \bigwedge \Gamma \Rightarrow (\wedge H \Rightarrow C)$, *for all ground reachable algebras* M.

Proof. We let $\vdash$ denote the entailment relation of **QfEQL**.

1. The compactness of **AEQL** is lifted to the compactness of **QfEQL** by Proposition 3.3.8.

   As for completeness, because the entailment system of **QfEQL** has implications it suffices to prove $\Gamma \models_{(S,F)} t = t'$ implies $\Gamma \vdash_{(S,F)} t = t'$ for every set of sentences Γ and each equation $t = t'$ in **QfEQL**. We define the set of sentences $\Gamma_0 = \{t_1 = t_2 \mid \Gamma \vdash t_1 = t_2\}$ and the congruence $\equiv_\Gamma = \{(t_1, t_2) \mid (t_1 = t_2) \in \Gamma_0\}$. We have

   (a) $(T_F)_{\equiv_\Gamma} \models t_1 = t_2$ iff $t_1/_{\equiv_\Gamma} = t_2/_{\equiv_\Gamma}$ iff $t_1 \equiv_\Gamma t_2$ iff $\Gamma \vdash t_1 = t_2$, for all equations $t_1 = t_2$.

   (b) $(T_F)_{\equiv_\Gamma} \models \Gamma$. For every sentence $H \Rightarrow (t_1 = t_2) \in \Gamma$ if $(T_F)_{\equiv_\Gamma} \models H$ then by 1a and *Unions* $\Gamma \vdash H$. By *Implications* $\Gamma \vdash t_1 = t_2$ and by 1a $(T_F)_{\equiv_\Gamma} \models t_1 = t_2$.

   By 1b $(T_F)_{\equiv_\Gamma} \models \Gamma$ which implies $\Gamma \vdash t = t'$. By 1a $(T_F)_{\equiv_\Gamma} \models t = t'$ and $\Gamma \vdash t = t'$.

2. The implication from left to right is straightforward. Now assume $M \models \bigwedge \Gamma \Rightarrow (\wedge H \Rightarrow C)$, for all reachable algebras M. By completeness it suffices to prove $\Gamma \vdash \wedge H \Rightarrow C$. We define $(\Gamma \cup H)_0 = \{t_1 = t_2 \mid (\Gamma \cup H) \vdash t_1 = t_2\}$ and $\equiv_{\Gamma \cup H} = \{(t_1, t_2) \mid t_1 = t_2 \in (\Gamma \cup H)_0\}$. By 1b we have $(T_F)/_{\equiv_{\Gamma \cup H}} \models \Gamma \cup H$ which implies $(T_F)/_{\equiv_{\Gamma \cup H}} \models C$. By 1a $\Gamma \cup H \vdash C$, and by *Implications* $\Gamma \vdash \wedge H \Rightarrow C$.

(Q.E.D.)

Theorem 4.2.3 (Completeness of **CEQL**). *The followings hold*

1. *the entailment system of* **CEQL** *is compact and complete, and*

2. *for any set of sentences* Γ *and any sentence* $(\forall X)\rho$ *in* **CEQL** *we have:* $\Gamma \models_{(S,F)} (\forall X)\rho$ *iff* $M \models_{(S,F \cup X)} \bigwedge \Gamma \Rightarrow \rho$ *for all ground reachable* $(S, F \cup X)$*-algebras* M.

Proof. Let $\vdash$ be the entailment relation of **CEQL**.

1. The compactness of **QfEQL** is lifted to the compactness of **CEQL** by Proposition 3.3.10.

   For the completeness part, assume that $\Gamma \models_{(S,F)} (\forall X)\rho$ and suppose towards a contradiction $\Gamma \nvdash (\forall X)\rho$. We define the set of $(S, F \cup X)$-sentences $\Gamma_1^X = \{\wedge H \Rightarrow C \mid \Gamma \vdash_{(S,F\cup X)} \wedge H \Rightarrow C\}$.

   Assuming that $\Gamma_1^X \vdash_{(S,F\cup X)} \rho$ we have: by the compactness of the entailment system of **CEQL** there is a finite set $\Gamma' \subseteq \Gamma_1^X$ such that $\Gamma' \vdash_{(S,F\cup X)} \rho$, by *Unions* $\Gamma \vdash_{(S,F\cup X)} \Gamma'$, by *Transitivity* $\Gamma \vdash_{(S,F\cup X)} \rho$, and by *Generalization* $\Gamma \vdash_{(S,F)} (\forall X)\rho$ which is a contradiction with our assumption. Thus $\Gamma_1^X \nvdash \rho$. By Proposition 4.2.2 there exists a reachable $(S, F \cup X)$-algebra M' such that $M' \models \Gamma_1^X$ and $M' \not\models \rho$. If we prove $M' \restriction_{(S,F)} \models \Gamma$ we obtain a contradiction with $\Gamma \models_{(S,F)} (\forall X)\rho$.

   Recall that for any set of variables Z, a $(S, F \cup Z)$-algebra consists of a (S,F)-algebra A plus an interpretation $h : Z \to A$ of the variable symbols in Z. Thus $M' = (M, f)$, where M is an (S,F)-algebra and $f : X \to M$ a function. Note that $M' \restriction_{(S,F)} = M$, and since M' is reachable, $\overline{f} : T_F(X) \to M$ is surjective. Let $(\forall Y)e' \in \Gamma$ and (M, g) be a expansion of M to the signature $(S, F \cup Y)$. Because $\overline{f} : T_F(X) \to M$ is surjective there exists a function/substitution $\theta : Y \to T_F(X)$ such that $\theta; f = g$.

$$\begin{tikzcd} T_F(X) \arrow[r, "\overline{f}"] & M \\ Y \arrow[u, dotted, "\theta"] \arrow[ur, "g"'] & \end{tikzcd}$$

   By *Substitutivity* $\Gamma \vdash_{(S,F)} (\forall X)\theta(e')$ and by *Generalization* $\Gamma \vdash_{(S,F\cup X)} \theta(e')$ which means $\theta(e') \in \Gamma_1^X$ and $(M, f) \models \theta(e')$. Note that $(M, f) \restriction_\theta = (M, \theta; \overline{f}) = (M, g)$ and by satisfaction condition for substitutions $(M, f) \restriction_\theta = (M, g) \models e'$.

2. We prove the implication from right to left. Assume that $\Gamma \not\models_{(S,F)} (\forall X)\rho$ by soundness $\Gamma \nvdash_{(S,F)} (\forall X)\rho'$ and following the above reasoning there exists a reachable algebra M' such that $M' \models_{(S,F\cup X)} \Gamma$ and $M' \not\models_{(S,F\cup X)} \rho$.

(Q.E.D.)

4.3 Applications

In applications we use a specialized rule of *Congruence* which is equivalent to the one previously defined.

(*Congruence*) $\frac{}{\{t_1 = t_2\} \vdash_{(S,F)} t_0(z \leftarrow t_1) = t_0(z \leftarrow t_2)}$, for every terms $t_1, t_2 \in T_F$ of sort s, and each term $t_0 \in T_F(\{z\})$ with one occurrence of variable z of sort s.

Example 16. Consider the following specification of groups theory

```
mod GROUP {
[Group]
op 0 :  -> Group
op _+_ :  Group Group -> Group
op —_ :  Group -> Group
vars X Y Z : Group
```

```
eq [lid] :  0 + X = X .
eq [linv] :  (- X) + X = 0 .
eq [assoc] :  X + (Y + Z) = (X + Y) + Z . }
```

Note that we can give names to the equations in CafeOBJ. Let $F = \{0, +, -\}$, $\Gamma = \{$`lid, linv, assoc`$\}$, and $S = \{$`Group`$\}$. This specification describes the class of all groups but this fact is not obvious because the standard specification of group theory contains two more equations

```
eq [rid] X + 0 = X .
eq [rinv] X + (- X) = 0 .
```

The second equation `rinv` can be deduced from the axioms Γ.

Firstly, note that by *Generalization* we have $\Gamma \vdash_{(S,F)}$ (∀`X`) `X+(-X)=0` iff $\Gamma \vdash_{(S,F\cup\{a\})}$ `a+(-a)=0`, where `a` is a any constant of sort `Group`. Secondly, we prove $\Gamma \vdash_{(S,F\cup\{a\})}$ `a+(-a) = 0` by the following inference chain.

1. `-(-a)+(-a)=0` by `linv` for X substituted by `-a`.
2. `0+(-a)=-a` by `lid` for `X` substituted by `-a`.
3. `-(-a)+(0+(-a))=-(-a)+(-a)` by *Congruence* with t_0=`-(- a)+z`.
4. `-(-a)+(0+(-a))=0` by *Transitivity* applied to 3 and 1.
5. `-(-a)+(0+(-a))=(-(-a)+0)+(-a)` by assoc for `X=-(-a), Y=0` and `Z=-a`.
6. `(-(-a)+0)+(-a)=-(-a)+(0+(-a))` by *Symmetry*.
7. `(-(-a)+0)+(-a)=0` by *Transitivity* applied to 6 and 4.
8. `(-a)+a=0` by linv for `X` substituted by `a`.
9. `(-(-a)+((-a)+a))+(-a)=(-(-a)+0)+(-a)` by *Congruence* with t_0=`(-(-a)+z)+(-a)`.
10. `(-(-a)+((-a)+a))+(-a)=0` by *Transitivity* applied to 9 and 7.
11. `-(-a)+((-a)+a)=(-(-a)+(-a))+a` by `assoc` for `X=-(-a)`, `Y=(-a)` and `Z=a`.
12. `(-(-a)+(-a))+a=-(-a)+((-a)+a)` by *Symmetry*.
13. `((-(-a)+(-a))+a)+(-a)=(-(-a)+((-a)+a))+(-a)` by *Congruence* with t_0=`z+(-a)`.
14. `((-(-a)+(-a))+a)+(-a)=0` by *Transitivity* applied to 13 and 10.
15. `((-(-a)+(-a))+a)+(-a)=(0+a)+(-a)` by *Congruence* with t_0 = `(z+a)+(-a)` applied to 1.
16. `(0+a)+(-a)=((-(-a)+(-a))+a)+(-a)` by *Symmetry*.
17. `(0+a)+(-a)=0` by *Transitivity* applied to 16 and 14.
18. `0+a=a` by lid for `X=a`.

19. `a=0+a` by *Symmetry*.

20. `a+(-a)=(0+a)+(-a)` by *Congruence* with t_0=`z+(-a)`.

21. `a+(-a)=0` by *Transitivity* applied to 20 and 17.

The first equation `rid` can be deduced from the second one `rinv`. Note that by *Generalization* $\Gamma \vdash_{(S,F)}$ (∀X)`X+0=X` iff $\Gamma \vdash_{(S,F\cup\{a\})}$`a+0=a`, where `a` is a any constant of sort `Group`. We prove $\Gamma \vdash_{(S,F\cup\{a\})}$`a+0=a` as follows.

1. `a+(-a)=0` by `rinv` for `X` substituted by `a`.

2. `(a+(-a))+a=0+a` by *Congruence* with t_0=`z+a`.

3. `0+a=a` by `lid` for `X` substituted by `a`.

4. `(a+(-a))+a=a` by *Transitivity* applied to 2 and 3.

5. `a+(-a+a)=(a+(-a))+a` by assoc for `X=a`, `Y=-a` and `Z=a`.

6. `a+(-a+a)=a` by *Transitivity* applied to 5 and 4.

7. `-a+a=0` by `linv` for `X=a`.

8. `0=-a+a` by *Symmetry*.

9. `a+0=a+(-a+a)` by *Congruence* with t_0=`a+z`.

10. `a+0=a` by *Transitivity* applied to 9 and 6.

Example 17. The formulation of equational deduction in the unsorted case do not involve explicit universal quantifiers for variables. The unsorted rules of deduction are exactly the same as the many-sorted rules except that all quantifiers are omitted, the terms in the rules may contain variables, and the rules of *Generalization* are not considered. We will show that explicit quantifiers are necessary for an adequate treatment of satisfaction. Consider the following specification:

```
mod MAP {
[A B < Elt]
ops T F : -> B
ops (_∨_) (_∧_) :  B B -> B
op ¬_ :  B -> B
op map :  A -> B
var X : B .
var Y : A .
eq [M1] :  X ∨ ¬ X = T .
eq [M2] :  X ∧ ¬ X = F .
eq [M3] :  X ∨ X = X .
eq [M4] :  X ∧ X = X .
eq [M5] :  ¬ F = T .
eq [M6] :  ¬ T = F .
eq [M7]:  ¬ map(Y) = map(Y) . }
```

We will show that unsorted equational deduction can prove an equation that does not hold in some models of the specification MAP above.

1. `map(Y)=¬map(Y)` by *Symmetry* applied to `M7`.
2. `map(Y)∨¬map(Y)=T` by `M1` for `X=map(Y)`.
3. `map(Y)∨map(Y)=map(Y)∨¬map(Y)` from `M7` by *Congruence* with t_0`=map(Y)∨z`.
4. `map(Y)∨map(Y)=T` by *Transitivity* applied to 3 and 2.
5. `map(Y)∨map(Y)=map(Y)` by `M3` with `X=map(Y)`.
6. `map(Y)=map(Y)∨map(Y)` by *Symmetry*.
7. `map(Y)=T` by *Transitivity* applied to 6 and 4.

8. `map(Y)∧map(Y)=map(Y)` by `M4` with `X=map(Y)`.
9. `map(Y)=map(Y)∧map(Y)` by *Symmetry*.
10. `map(Y)∧map(Y)=map(Y)∨¬map(Y)` from `M7` by *Congruence* with t_0`=map(Y)∧z`.
11. `map(Y)=map(Y)∧¬map(Y)` by *Transitivity* applied to 9 and 10.
12. `map(Y)∧¬map(Y)=F` by `M2` for `X=map(Y)`.
13. `map(Y)=F` by *Transitivity* applied to 11 and 12.
14. `F=map(Y)` by *Symmetry*.

15. `F=T` by *Transitivity* applied to 14 and 7.

Thus we proved that `F=T`. Now consider the algebra M interpreting the sort A as the empty set and the sort B as the set {`T`, `F`}, where `T` and `F` are distinct, and where ∨, ∧, ¬ are interpreted as expected for the Booleans, and where `map` is the empty function. It is easy to check that $M \models (\forall Y)$`F=T`, where Y is of sort A, and M does not satisfies the equation `F=T`. We conclude that these rules are not sound for the many sorted algebras but we note that the unsorted rules of deduction are sound and complete for the classical case (studied by Birkhoff and others) where only unsorted algebras are used as models. For detailed discussion on this issue see [35].

A specialized rule of inference using subterm replacement is the basis for term rewriting, a powerful technique for mechanical inference implemented in CafeOBJ.

$$(\textit{Subterm replacement})\frac{\Gamma \vdash_{(S,F)} (\forall Y) \wedge \theta(H)}{\Gamma \vdash_{(S,F)} (\forall Y) t_0(z \leftarrow \theta(t_1)) = t_0(z \leftarrow \theta(t_2))}$$

for every set of sentences Γ with $(\forall X) \wedge H \Rightarrow (t_1 = t_2) \in \Gamma$, each substitution $\theta : X \rightarrow T_F(Y)$ and any term $t_0 \in T_F(Y \cup \{z\})$ such that $z \notin Y$.
CafeOBJ not only supports writing theories, such as that of groups, but also deducing new equations from theories by applying subterm replacement. The proof of the second equation `rinv` of using CafeOBJ is as follows.

```
open GROUP
op a :  -> S .
start a + (- a) = 0 .
apply -.lid with X = a + (- a) at (1) .
**> result 0 + (a + (- a)) = 0 :  Bool
apply -.linv with X = - a at (1 1) .
**> result (- (- a) + (- a)) + (a + (- a)) = 0 :  Bool
apply assoc at (1) .
**> ((- (- a) + (- a)) + a) + (- a) = 0 :  Bool
apply -.assoc at (1 1) .
**> result (- (- a) + (- a + a)) + (- a) = 0 :  Bool
apply -.assoc at (1) .
**> result - (- a) + ((- a + a) + (- a)) = 0 :  Bool
apply red at term .
**> result true :  Bool
close
```

The proof of the first equation `rid` in CafeOBJ is as follows.

```
open GROUP
op a :  -> Group .
eq [rinv] :  X + (- X) = 0 .
start a + 0 = a .
apply -.linv with X = a at (1 2) .
**> result a + (- a + a) = a :  Bool
apply assoc at (1) .
**> result (a + (- a)) + a = a :  Bool
apply red at term .
**> result true :  Bool
close
```

Birkhoff calculus and its completeness have been developed for the unsorted version of **CEQL** in [10]; this result has been extended to many-sorted case in [35], and to arbitrary institutions in [16]. The completeness result presented here is due to [16], and a layered approach to institution-independent completeness may be found also in [11] within the framework of specification theory. Concerning related work, another abstract calculus for equational logics is developed in [62], in a categorial framework, based on satisfaction by injectivity. Example 17 showing that the unsorted rules can be unsound for many-sorted algebras that may have empty carriers, is from [35]. Rewriting is the basis of the CafeOBJ operational semantics and constitutes the operational semantics for the equational specification by regarding the equational specifications as term rewriting systems. A comprehensive presentation of rewriting can be found in [32].

Chapter 5

Constructor-based Equational Deduction

Conditional equational logic **CEQL** is a "sub-institution" of constructor-based equational logic **CCEQL** in the sense that any (ordinary) algebraic signature (S,F) can be regarded as a constructor-based algebraic signature $(S,F,\emptyset)$, and any conditional equation $(\forall Y)\wedge H \Rightarrow C$ in **CEQL** can be viewed as a conditional equation in **CCEQL** with the empty set of constrained variables. Actually an embedding of institutions, formalized as a co-morphism (see [37, 48]), can be defined with source **CEQL** and target **CCEQL**. We define the infinitary rules of *Case splitting* and show that the constructor-based equational entailment system of **CCEQL** generated by the rules of equational deduction and *Case splitting* is sound, complete. We define the rules of *Structural induction* to deal with infinitary premises of *Case Splitting* but the infinitary rules can not be replaced with the finitary ones in order to obtain a complete and compact entailment system because the class of sentences true of a class of models for a given constructor-based specification is not in general recursively enumerable. Gödel's famous incompleteness theorem show that this holds even for the specification of natural numbers. The completeness of **CCEQL** is due to [28] and appears to be new in the literature since it infers the completeness of the calculus for the initial models of the specifications in the context of Gödel's incompleteness theorem.

5.1 Preliminaries and Definition

The sentences in **CCEQL** are of the form $(\forall X)(\forall Y)\wedge H \Rightarrow C$, where X is a set of constrained variables, Y is a set of loose variables, H is a finite set of equational atoms, and C is an equational atom. For the sake of simplicity we will write $(\forall X)\rho$, where $\rho = (\forall Y)\wedge H \Rightarrow C$. One can choose different representations for the sentences in **CCEQL**. For example $(\forall X \cup Y)\wedge H \Rightarrow C$ denote the sentence $(\forall X)(\forall Y)\wedge H \Rightarrow C$ but we choose to emphases the set of constrained variables.

Recall that for every signature (S,F^c,F) we denote by

- S^c the set of constrained sorts $S^c = \{s \in S \mid \text{ there exists } \sigma \in F^c_{w\to s}\}$, and
- S^l the set of loose sorts $S - S^c$.

Definition 5.1.1 (Reachable algebras)**.** *An (S,F)-algebra M is S'-reachable, where $S' \subseteq S$, iff there exists a set Y of variables with the sorts in $S - S'$ and a function $f : Y \to M$ such that for every $s \in S'$ the function $\overline{f}_s : (T_F(Y))_s \to M_s$ is surjective, where $\overline{f} : T_F(Y) \to M$ is the unique extension of f to a (S,F)-morphism.*

Remark 5.1.2. *A (S,F)-algebra is S'-reachable, where $S' \subseteq S$, iff there exists a set Y of variables with sorts in $S - S'$ and a function $f : Y \to M$ such that for every $s \in S'$ the function*

$f^{\#}_s : (T_{F^{S'}}(Y))_s \to M_s$ is surjective, where $F^{S'}$ is the set of operations in F with the resulting sorts in S' ($F^{S'}_{w\to s} = F_{w\to s}$ when $s \in S'$ and $F^{S'}_{w\to s} = \emptyset$ otherwise) and $f^{\#} : T_{F^{S'}}(Y) \to M$ is the unique extension of f to a $(S, F^{S'})$-morphism.

Proof. The implication from right to left is straightforward. For the converse implication assume a function $f : Y \to M$, where Y is a set of variables with the sorts in $S - S'$, such that for every $s \in S'$ the function $\overline{f}_s : (T_F(Y))_s \to M_s$ is surjective. Let Z be a new set of variables such that

- $Z_s = \emptyset$ when $s \in S'$, and
- Z_s is renaming of M_s for all $s \in (S - S')$.

For all $s \in (S - S')$ there exists a bijection $g_s : Z_s \to M_s$. Let $g^{\#} : T_{F^{S'}}(Z) \to M$ be the unique extension of g to a $(S, F^{S'})$-morphism. It suffices to show that for each term $t \in T_F(Y)$ there exists a term $t' \in T_{F^{S'}}(Z)$ such that $\overline{f}(t) = g^{\#}(t')$. We proceed by induction on the structure of the term t.

1. For $t \in F_{\to s}$. If $s \in S'$ then take $t' = t$. If $s \in (S - S')$ then take $t' = g^{-1}(M_t)$.
2. For $t = \sigma(t_1, \ldots, t_n)$. Assume that $t \in (T_F(Y))_s$. If $s \in S'$ then $\sigma \in F^{S'}$; by induction hypothesis there exists $t'_i \in T_{F^{S'}}(Z)$ such that $\overline{f}(t_i) = g^{\#}(t'_i)$ for all $i \in \{1, \ldots, n\}$; we have $\overline{f}(t) = \overline{f}(\sigma(t_1, \ldots, t_n)) = M_\sigma(\overline{f}(t_1), \ldots, \overline{f}(t_n)) = M_\sigma(g^{\#}(t'_1), \ldots, g^{\#}(t'_n)) = g^{\#}(\sigma(t'_1, \ldots, t'_n))$ and $t' = \sigma(t'_1, \ldots, t'_n) \in T_{F^{S'}}(Z)$. If $s \in (S - S')$ then take $t' = g^{-1}(M_t)$.

(Q.E.D.)

Remark 5.1.3. *Given a constructor-based* **CCEQL**-*signature (S, F, F^c) the (S, F, F^c)-models are S^c-reachable (S, F^c)-algebras.*

Proposition 5.1.4. *Assume a signature (S, F, F^c) and an (S, F)-algebra M. If $M \in \mathbb{M}od(S, F, F^c)$ then for every finite set X of constrained variables and each $(S, F \cup X)$-expansion M' of M there exists a finite set of loose variables Y, an $(S, F \cup Y)$-expansion M'' of M, and a substitution $\theta : X \to T_{F^c}(Y)$ such that $M'' \restriction_\theta = M'$.*

Proof. Let Y be a set of loose variables and $f : Y \to M$ an interpretation of variables in Y such that $\overline{f}_s : (T_{F^c}(Y))_s \to M_s$ is surjective for all $s \in S^c$. Let (M, g) be an expansion of M to the signature $(S, F \cup X)$. Since $\overline{f}$ is surjective on the constrained sorts, there exists a function $\theta : X \to T_{F^c}(Y)$ such that $\theta; \overline{f} = g$. Because X is finite there exists $Y' \subseteq Y$ finite such that $\theta(Y') = X$.

$$\begin{tikzcd}
T_{F^c}(Y') \arrow[dr, hook] & & X \arrow[ll, dotted, "\theta'"'] \arrow[dl, "\theta"'] \arrow[dd, "g"] \\
& T_{F^c}(Y) \arrow[dr, "\overline{f}"] & \\
Y' \arrow[uu, hook] \arrow[ur, hook] \arrow[rr, dotted, "f'"'] & & M
\end{tikzcd}$$

We define $\theta' : X \to T_{F^c}(Y')$ as the co-restriction of θ (for all $x \in X$, $\theta'(x) = \theta(x)$) and $f' : Y' \to M$ as the restriction of f (for all $y \in Y'$, $f'(y) = f(y)$). Now note that $(M, f') \restriction_{\theta'} = (M, \theta'; \overline{f'}) = (M, \theta; \overline{f}) = (M, g)$.

(Q.E.D.)

We define the rules of constructor-based equational deduction as follows.

Definition 5.1.5 (Constructor-based equational deduction)**.** *Constructor-based equational entailment system is the least entailment system with implications, universal quantifications freely generated by the rules of equational deduction plus the following (infinitary) rules*

$$(\textit{Case splitting})\frac{\{\Gamma \vdash_{(S,F,F^c)} (\forall Y)\theta(\rho) \mid Y - \textit{loose variables},\ \theta : X \to T_{F^c}(Y)\}}{\Gamma \vdash_{(S,F,F^c)} (\forall X)\rho}$$

for every set of sentences Γ*, and any sentence* $(\forall X)\rho$*, where* X *is a set of constrained variables.*

Remark 5.1.6. *For any constructor-based algebraic signature* (S,F,F^c) *we have* $\Gamma \vdash_{(S,F,F^c)} e$ *whenever* $\Gamma \vdash_{(S,F)} e$*.*

In order to explain the rules of *Case splitting* we consider the particular case when $X = \{x\}$. If for any term t formed with constructors and loose variables $\Gamma \vdash_{(S,F,F^c)} (\forall Y)\rho(x \leftarrow t)$ holds, where Y are all (loose) variables which occur in t, then we have proved $\Gamma \vdash_{(S,F,F^c)} (\forall x)\rho$. In most of the cases the set of terms t formed with constructors and loose variables [1] is infinite which implies that the rules of *Case splitting* are infinitary and thus, the corresponding entailment system is not compact. Not all proofs can be written as finite sequences of sentences which means that the semantic consequences of the theories are not in general recursively enumerable.

Example 18. Consider the following example of queue with arbitrary elements.

```
mod SIMPLE-QUEUE {
[Elt]
[Queue]
-- constructors
op empty :  -> Queue {constr}
op _,_ :  Queue Elt -> Queue {constr}
-- operators
op none :  -> Elt
op _@_ :  Queue Queue -> Queue
vars Q Q' : Queue
vars X Y : Elt
eq [Q1] :  Q @ empty = Q .
eq [Q2] :  Q @ (Q',X) = (Q @ Q'),X .
}
```

Note that there is one constrained sort `Queue` and one loose sort `Elt`. Suppose we want to prove the associativity of the concatenation `_@_`, `(∀Q1)(∀Q2)(∀Q3)(Q1@Q2)@Q3 = Q1@(Q2@Q3)`, we deal with each constrained variable separately; by *Case splitting* we need to prove

1. `(∀Q1)(∀Q2)(Q1@Q2)@ empty = Q1 @(Q2 @ empty)`
2. `(∀Q1)(∀Q2)(∀X)(Q1 @ Q2)@(empty,X) = Q1 @ (Q2 @(empty,X))`
3. `(∀Q1)(∀Q2)(∀X1)(∀X2)(Q1 @ Q2)@(empty,X1,X2) = Q1@(Q2@(empty, X1,X2))`

[1] We consider terms modulo renaming variables.

$\vdots$

Remark 5.1.7. *The splitting is made without considering the (loose) constant none.*

Special care is needed when we apply the rules of *Generalization*. In this case we have
(*Generalization*) $\Gamma \vdash_{(S,F,F^c)} (\forall Y)\rho$ iff $\Gamma \vdash_{(S,F\cup Y,F^c)} \rho$ for every set of (S,F,F^c)-sentences Γ and any (S,F,F^c)-sentence $(\forall Y)\rho$ such that Y is a set of loose variables.

This rules are sound because the inclusions $(S,F,F^c) \hookrightarrow (S,F\cup X,F^c)$ are **CCEQL** signature morphisms. Note that if Y contains any constrained variable then these rules are not sound in general.

Remark 5.1.8. *If* $\Gamma \vdash_{(S,F\cup\{y\},F^c)} \rho$, *where* y *is a constant of constrained sort, then we have proved* $\Gamma \vdash_{(S,F,F^c)} (\forall y)\rho$

Proof. Follows easily in three steps:

1. $\Gamma \vdash_{(S,F\cup Z,F^c)} \rho(x \leftarrow t)$ by substituting t for y, for all terms t formed with constructors and loose variables (where Z is the set of all loose variables in t),

2. $\Gamma \vdash_{(S,F,F^c)} (\forall Z)\rho(x \leftarrow t)$ by *Generalization*, for all terms t formed with constructors and loose variables (where Z is the set of all variables in t), and

3. $\Gamma \vdash_{(S,F,F^c)} (\forall y)\rho$ by *Case splitting*.

(Q.E.D.)

Proposition 5.1.9 (Soundness of **CCEQL**). *The entailment system of* **CCEQL** *is sound.*

Proof. By Proposition 3.2.7, and Corollaries 3.3.9 and 3.3.11 we have only to show the soundness of the generating rules. By Proposition 4.1.5 the rules of equational deduction are sound for **CEQL**, hence they are sound for **CCEQL** too. We need to check only the soundness of *Case splitting*.

Let Γ be a set of (S,F,F^c)-sentences and $(\forall X)\rho$ a (S,F,F^c)-sentence such that $\Gamma \models (\forall Z)\theta(\rho)$ for all sentences $(\forall Z)\theta(\rho)$, where Z is a set of loose variables and $\theta : X \to T_{F^c}(Z)$ is a substitution. We assume $M \models \Gamma$, where $M \in |\mathbb{M}od(S,F,F^c)|$ and we prove $M \models (\forall X)\rho$. Let M' be an expansion of M to the signature $(S,F\cup X,F^c)$. By Proposition 5.1.4 there exists a finite set Y of loose variables, a substitution $\theta : X \to T_{F^c}(Y)$, and an expansion M'' of M to the signature $(S,F\cup Y,F^c)$ such that $M'' \restriction_\theta = M'$. By satisfaction condition $M \models_{(S,F,F^c)} \Gamma$ implies $M'' \models_{(S,F\cup Y,F^c)} \Gamma$ and since $\Gamma \models_{(S,F,F^c)} (\forall Y)\theta(\rho)$, we have $\Gamma \models_{(S,F\cup Y,F^c)} \theta(\rho)$ and $M'' \models \theta(\rho)$. By the satisfaction condition for substitutions $M'' \restriction_\theta = M' \models_{(S,F\cup X,F^c)} \rho$. Since M' was arbitrary we get $M \models (\forall X)\rho$. (Q.E.D.)

5.2 Completeness

The result in this section lifts the completeness of **CEQL** to the completeness of **CCEQL** by adding the rules of *Case splitting* which deals with universal quantifications over variables of constrained sorts. However, the completeness result is relative to a class of *sufficient-complete* sets of sentences.

Definition 5.2.1. *A basic specification $((S,F,F^c),\Gamma)$-sentences, where (S,F,F^c) is a signature and Γ is a set of sentences, is sufficient-complete if for every term t formed with operation symbols in F^{S^c} (where $F^{S^c}_{w\to s} = F_{w\to s}$ when $s \in S^c$ and $F^{S^c}_{w\to s} = \emptyset$ when $s \in S^l$) and loose variables in Y there exists a term t' formed with operation symbols in F^c and loose variables in Y such that $\Gamma \vdash_{(S,F)} (\forall Y)t = t'$.*

Theorem 5.2.2 (Completeness of **CCEQL**). $\Gamma \models_{(S,F,F^c)} \rho$ *implies* $\Gamma \vdash_{(S,F,F^c)} \rho$ *whenever the specification* $((S,F,F^c),\Gamma)$ *is sufficient-complete.*

Proof. Let Γ be a sufficient-complete set of sentences such that $\Gamma \models_{(S,F,F^c)} (\forall X)\rho$. Suppose towards a contradiction that $\Gamma \not\vdash_{(S,F,F^c)} (\forall X)\rho$. Then there exists a set Y of loose variables and a substitution $\theta : X \to T_{F^c}(Y)$ such that $\Gamma \not\vdash_{(S,F,F^c)} (\forall Y)\theta(\rho)$ (if $\Gamma \vdash_{(S,F,F^c)} (\forall Y)\theta(\rho)$, for all sentences $(\forall Y)\theta(\rho)$, where Y is a set of loose variables and $\theta : X \to T_{F^c}(Y)$ is a substitution, then by *Case splitting* $\Gamma \vdash_{(S,F,F^c)} (\forall X)\rho$).

We define the following set of sentences $\Gamma_2 = \{(\forall Z) \wedge H \Rightarrow C \mid Z - \textit{loose variables}, \Gamma \vdash_{(S,F,F^c)} (\forall Z) \wedge H \Rightarrow C\}$.

We show that $(\forall Y)\theta(\rho)$ can not be deduced from Γ_2 in **CEQL**, i.e. $\Gamma_2 \not\vdash_{(S,F)} (\forall Y)\theta(\rho)$. If $\Gamma_2 \vdash_{(S,F)} (\forall Y)\theta(\rho)$ then by compactness of equational deduction there exists a finite set $\Gamma' \subseteq \Gamma_2$ such that $\Gamma' \vdash_{(S,F)} (\forall Y)\theta(\rho)$. By Remark 5.1.6 $\Gamma' \vdash_{(S,F,F^c)} (\forall Y)\theta(\rho)$, and since $\Gamma \vdash_{(S,F,F^c)} e$ for all $e \in \Gamma'$, we obtain $\Gamma \vdash_{(S,F,F^c)} \Gamma'$ which implies $\Gamma \vdash_{(S,F,F^c)} (\forall Y)\theta(\rho)$, a contradiction with our assumption.

By Theorem 4.2.3 there exists a ground reachable $(S, F \cup Y)$-algebra (M, f) such that

$$(M, f) \models_{(S,F\cup Y)} \Gamma_2 \text{ and } (M, f) \not\models_{(S,F\cup Y)} \theta(\rho)$$

1. Firstly we prove that $M \models_{(S,F)} \Gamma$. Let $(\forall X')\rho' \in \Gamma$, and $g : X' \to M$ an assignment of the variables in X'.

$$\begin{tikzcd} T_F(Y) \arrow[r, "\overline{f}"] & M \\ X' \arrow[u, dotted, "\theta'"] \arrow[ur, "g"'] & \end{tikzcd}$$

   Since $\overline{f} : T_F(Y) \to M$ is surjective on the constrained sorts there exists a substitution $\theta' : X' \to T_F(Y)$ such that $\theta'; \overline{f} = g$. By *Substitutivity* we have $\Gamma \vdash_{(S,F,F^c)} (\forall Y)\theta'(\rho')$ which means $(\forall Y)\theta'(\rho') \in \Gamma_2$. $M \models_{(S,F)} \Gamma_2$ implies $M \models_{(S,F)} (\forall Y)\theta'(\rho')$ and $(M, f) \models_{(S,F\cup Y)} \theta'(\rho')$. Since $(M, f) \restriction_{\theta'} = (M, \theta'; \overline{f}) = (M, g)$ by the satisfaction condition for substitutions $(M, g) \models_{(S,F\cup X')} \rho'$.

2. Secondly we prove that $M \in \mathbb{M}od(S,F,F^c)$. By Remark 5.1.2 there exists a function $h : Z \to M$, where Z is a set of loose variables, such that for every sort $s \in S^c$ the function $\overline{h}_s : T_{F^{S^c}}(Z) \to M_s$ is surjective, where $\overline{h} : T_{F^{S^c}}(Z) \to M$ is the unique extension of h to a (S, F^{S^c})-morphism. We prove that for every $s \in S^c$ the function $h^{\#}_s : (T_{F^c}(Z))_s \to M_s$ is surjective, where $h^{\#} : T_{F^c}(Z) \to M$ is the unique extension of h to a (S, F^c)-morphism. Let $s \in S^c$ and $m \in M_s$. Because $\overline{h}_s : (T_{F^{S^c}}(Z)) \to M_s$ is surjective there exists a term $t \in (T_{F^{S^c}}(Z))_s$ such that $\overline{h}_s(t) = m$. Since $((S,F,F^c),\Gamma)$ is sufficient-complete there exists a term $t' \in (T_{F^c}(Z'))_s$, where $Z' \subseteq Z$ is the set of all (loose) variables occurring in t, such that $\Gamma \vdash_{(S,F)} (\forall Z')t = t'$. We have $\Gamma \models_{(S,F)} (\forall Z')t = t'$ and $M \models_{(S,F)} (\forall Z')t = t'$ which implies $m = \overline{h}_s(t) = \overline{h}_s(t') = h^{\#}_s(t')$.

$M \models_{(S,F)} \Gamma$ implies $M \models_{(S,F,F^c)} \Gamma$. $(M, f) \not\models_{(S,F\cup Y)} \theta(\rho)$ implies $M \not\models_{(S,F)} (\forall X)\rho$ and $M \not\models_{(S,F,F^c)} (\forall X)\rho$ which is a contradiction with $\Gamma \models_{(S,F,F^c)} (\forall X)\rho$. Our assumption $\Gamma \not\vdash_{(S,F,F^c)} (\forall X)\rho$ does not hold and we get $\Gamma \vdash_{(S,F,F^c)} (\forall X)\rho$. (Q.E.D.)

Example 19. The following example shows that the sufficient-completeness assumption in Theorem 5.2.2 is crucial.

```
mod ISPEC {
[S]
-- constructors
op a :  -> S {constr}
-- operators
op b :  -> S
}
```

Note that $\emptyset \models$ `a = b` but there is no way to prove $\emptyset \vdash$ `a = b` because `ISPEC` is not sufficient complete.

Example 20. The following is a specification of natural numbers with addition. We will prove that the following specification is sufficient-complete.

```
mod SIMPLE-NAT {
[Nat]
-- constructors
op 0 :  -> Nat {constr}
op s_ :  Nat -> Nat {constr}
-- operators
op _+_ :  Nat Nat -> Nat
-- variables
vars M N : Nat
-- equations
eq [lid] :  0 + N = N .
eq [ladd] :  s M + N = s (M + N) . }
```

The signature of the above specification consists of a constrained sort `Nat`, two constructors `0` and `s`, and one ordinary operation $+$. Let $F_{Nat} = \{0, s, +\}$, $F^c_{Nat} = \{0, s\}$ and $\Gamma_{Nat} = \{$`lid`, `ladd`$\}$. For the sufficient-completeness of Γ_{Nat} it suffices to show that for any terms $t_1, t_2 \in T_{F^c_{Nat}}$ there exists a term $t \in T_{F^c_{Nat}}$ such that $\Gamma_{Nat} \vdash t_1 + t_2 = t$. By induction on the structure of t_1.

For $t_1 = 0$. Take $t_2 = t$ and we have

1. $0 + t_2 = t_2$ by `lid` for $N = t_2$.
2. $0 + t_2 = t$ by *Transitivity*.

For $t_1 = s\, t'_1$. By induction hypothesis there exists a term $t' \in T_{F^c_{Nat}}$ such that $\Gamma_{Nat} \vdash t'_1 + t_2 = t'$. We have that

1. $s\, t'_1 + t_2 = s(t'_1 + t_2)$ by `ladd` for $M = t'_1$ and $N = t_2$.
2. $s(t'_1 + t_2) = s\, t'$ by *Congruence* applied to the induction hypothesis.
3. $s\, t'_1 + t_2 = s\, t'$.

5.3 Structural induction

Assume we want $\Gamma \vdash_{(S,F,F^c)} (\forall x)\rho$, where x is a variable of constrained sort s, then we use *Case splitting*. In order to prove the premises of *Case splitting*, in many cases, we use induction on the structure of terms. For any t formed with constructors in F^c and loose variables we define (*Structural induction*) $\Gamma \vdash_{(S,F,F^c)} (\forall V)\rho(x \leftarrow t)$ if

1. (*Induction base*) for all $cons \in F^c_{\to s}$, $\Gamma \vdash_{(S,F,F^c)} \rho(x \leftarrow cons)$,
2. (*Induction step*) for all $\sigma \in F^c_{s_1 \ldots s_n \to s}$, $\Gamma \cup \{\rho(x \leftarrow x') \mid x' \in X\} \vdash_{(S,F\cup C,F^c)} \rho(x \leftarrow \sigma(c_1, \ldots, c_n))$, where
   - $C = \{c_1, \ldots, c_n\}$ is a set of new variables such that c_i has the sort s_i, for all $i \in \{1, \ldots, n\}$, and
   - $X \subseteq C$ is the set of variables with the sort s.

where V are all (loose) variables in t.

A more familiar way to define the rules of *Structural induction* is when the conclusion is $(\forall x)\rho$, however we prefer this formulation.

Proposition 5.3.1. *The entailment system of* **CCEQL** *satisfies the rules of Structural induction.*

Proof. Let Z be a set of loose variables such that for each $s' \in S^l$ the set Z_s is infinite. We define the S-sorted set of terms T by

- $T_s = \{t \in T_{F^c}(Z) \mid \Gamma \vdash_{(S,F\cup Z',F^c)} \rho(x \leftarrow t),\ Z' \subseteq Z$ is the least set such that $t \in T_{F^c}(Z')\}$, and
- $T_{s'} = (T_{F^c}(Z))_{s'}$ for all sorts $s' \neq s$.

We prove that T is a (S,F^c)-algebra, where $T_\sigma(t_1, \ldots, t_n) = \sigma(t_1, \ldots, t_n)$, for all operation symbols $\sigma \in F^c_{s_1 \ldots s_n \to s}$ and terms $t_1, \ldots, t_n$.

By *Induction base* all the constants $cons \in F^c_{\to s}$ are in T_s.

Now let $\sigma \in F^c_{s_1 \ldots s_n \to s}$ and assume that $t_i \in T_{s_i}$ for all $i \in \{1, \ldots, n\}$. We show that $\sigma(t_1, \ldots, t_n) \in T_s$. We denote by Z^i the set of variables in t_i, where $i \in \{1, \ldots, n\}$. We define $J' \subseteq \{1, \ldots, n\}$ such that $s_i = s$ for every $i \in J'$. We have $\Gamma \vdash_{(S,F\cup Z^i,F^c)} \rho(x \leftarrow t_i)$ for all $i \in J'$, which implies $\Gamma \vdash_{(S,F\cup Z',F^c)} \{\rho(x \leftarrow t_i) \mid i \in J'\}$, where $Z' = \bigcup_{i\in J'} Z^i$. We obtain $\Gamma \vdash_{(S,F\cup Z'',F^c)} \{\rho(x \leftarrow t_i) \mid i \in J'\}$, where $Z'' = \bigcup_{i=1}^{i\leq n} Z^i$. By *Induction step* $\Gamma \cup \{\rho(x \leftarrow t_i) \mid i \in J'\} \vdash_{(S,F\cup Z'',F^c)} \rho(x \leftarrow \sigma(t_1, \ldots, t_n))$ which implies $\Gamma \vdash_{(S,F\cup Z'',F^c)} \rho(x \leftarrow \sigma(t_1, \ldots, t_n))$ meaning that $\sigma(t_1 \ldots, t_n) \in T_s$.

Since $T_{F^c}(Z)$ does not have any proper subalgebra we get $T = T_{F^c}(Z)$. Therefore $\Gamma \vdash_{(S,F,F^c)} (\forall V)\rho(x \leftarrow t)$ for all terms $t \in T_{F^c}(Z)$, where $V \subseteq Z$ is the set of all (loose) variables in t.

Assume that *Induction base* and *Induction step* holds and let t be a term of sort s formed with constructors and loose variables; we want $\Gamma \vdash_{(S,F,F^c)} (\forall V)\rho(x \leftarrow t)$, where V is the set of all loose variables which occur in t. Without loss of generality we assume that $V \subseteq Z$. We have $t \in T_s$ which implies $\Gamma_{(S,F\cup V,F^c)}\rho(x \leftarrow t)$ and by *Generalization* we obtain $\Gamma_{(S,F,F^c)}(\forall V)\rho(x \leftarrow t)$. (Q.E.D.)

5.4 Applications

One example of structural induction is Peano induction. We use it to prove the commutativity of addition of natural numbers (see Example 20) in three steps:

```
1. eq [rid] :  M + 0 = M

2. eq [radd] :  M + s N = s(M + N)

3. eq [comm] :  M + N = N + M
```

1. We prove first equation `rid` by induction on the structure of M.

```
IB open SIMPLE-NAT
   red 0 + 0 = 0 .
   **> result true :  Bool
   close
IS open SIMPLE-NAT
   op a :  -> Nat .
   eq a + 0 = a .
   red s a + 0 = s a .
   **> result true :  Bool
   close
```

2. We prove the equation `radd` by induction on the structure of M.

```
IB open SIMPLE-NAT
   red 0 + s N = s(0 + N) .
   **> result true :  Bool
   close
IS open SIMPLE-NAT
   op a :  -> Nat .
   eq a + s N = s(a + N) .
   red s a + s N = s(a + s N) .
   **> result true :  Bool
   close
```

3. Finally, we prove the commutativity of addition by induction on the structure of M. We add the equations `rid` and `radd` as premises for our proof.

```
IB open SIMPLE-NAT
   eq [rid] :  N + 0 = N .
   eq [radd] :  M + s N = s(M + N) .
   red 0 + N = N + 0 .
   **> result true :  Bool
   close
```

```
IS open SIMPLE-NAT
   op a :  -> Nat .
   eq a + N = N + a .
   red s a + N = N + s a .
   **> result true :  Bool
   close
```

Consider Example 18 and prove `(∀Q1)(∀Q2)(∀Q3)(Q1@Q2)@Q3 = Q1@(Q2@Q3)` by induction on the structure of `Q3`. We need to prove the following:

`IB (∀Q1)(∀Q2)(Q1@Q2)@ empty = Q1@(Q2@ empty), and`

`IS` $\Gamma \cup \{$ `(∀Q1)(∀Q2)(Q1 @ Q2)@ q = Q1 @(Q2 @ q)`$\}\vdash_{(S,F\cup\{q,a\},F^c)}$ `(∀Q1)(∀Q2)(Q1 @ Q2)@ (q,a) = Q1 @(Q2 @(q,a)).`

where $S = \{$`Queue,Elt`$\}$, $F = \{$`none,empty,(_,_),_@_`$\}$, $F^c = \{$`empty,(_,_)`$\}$, and $\Gamma = \{$`Q1,Q2`$\}$. The proof in CafeOBJ is as follows:

```
IB open SIMPLE-QUEUE
   vars Q1 Q2 :  Queue .
   red (Q1 @ Q2) @ empty = Q1 @ (Q2 @ empty) .
   **> result true :  Bool
   close

IS open SIMPLE-QUEUE
   vars Q1 Q2 :  Queue .
   op q :  -> Queue .
   op x :  -> Elt .
   eq (Q1 @ Q2) @ q = Q1 @ (Q2 @ q) .
   red (Q1 @ Q2) @ (q,x) = Q1 @ (Q2 @ (q,x)) .
   **> result true :  Bool
   close
```

The constructor-based logics have been studied in [8] and [7]. The calculus given here is complete for the initial models of the specifications. The completeness of **CCEQL** is due to [28], where the result is proved in the framework of institutions. The *Structural induction* generalizes the Peano induction. We may define the rules of *Structural induction* with the conclusion $(\forall X)\rho$ and restrict the institution **CCEQL** to the signatures with finite number of constructors; then the entailment system generated by the rules of equational deduction and *Structural induction* are compact, but not complete.

Chapter 6

Error Handling with Order-Sorted Algebra

Order-sorted algebra provide sub-sorts declarations which allow a more precise definition of the operations, declarations of partial functions, and error handling. As the title suggests this chapter is largely focused on error handling and its correctness. A different approach toward error handling may be found in [36] where the errors are captured by retract functions. The method presented here seems to be more efficient than the one in [36].

6.1 Order-sorted Equational Deduction

The rules of order-sorted equational deduction are the same as for equational deduction, and the same results as for equational deduction generally carry over. We prove only the completeness of the restriction of **OSA** to the equational atoms. The completeness of **HOSA** and the completeness of **CHOSA** are given in Chapter 8, in the framework of institutions.

Definition 6.1.1 (Order-sorted congruence)**.** *A congruence relation $\equiv$ on a $(S,\leq,F)$-model M is a (S,F)-congruence relation $\equiv = (\equiv_s)_{s\in S}$ such that if $s \leq s'$ in $(S,\leq)$ and $a,a' \in M_s$ then $a \equiv_s a'$ if and only if $a \equiv_{s'} a'$.*

We denote by **AOSA** the restriction of **OSA** to the atomic sentences.

Proposition 6.1.2 (Completeness of **AOSA**)**.** *The entailment system of* **AOSA** *generated by the rules of $Reflexivity$, $Symmetry$, $Transitivity$, and $Congruence$ is complete and compact.*

Proof. For any set Γ of equations for a signature $(S,\leq,F)$ we define $\equiv_\Gamma = \{(t,t')|\Gamma \vdash t = t'\}$. Since the signature $(S,\leq,F)$ is regular the term algebra T_F is the initial $(S,\leq,F)$-algebra in $\mathbb{M}od(S,\leq,F)$. By $Reflexivity$, $Symmetry$, $Transitivity$ and $Congruence$ the relation $\equiv_\Gamma$ is a (S,F)-congruence on T_F. $\equiv_\Gamma$ is also an order-sorted congruence on T_F, because the definition of $\equiv_\Gamma$ does not depend upon a sort. Since the signature $(S,\leq,F)$ is locally filtered we may define a model M_Γ as the quotient of the initial algebra (term algebra) T_F by order-sorted congruence $\equiv_\Gamma$. Notice that for each $(S,\leq,F)$-equation $t = t'$, $\Gamma \vdash t = t'$ iff $M_\Gamma \models t = t'$. Now if $\Gamma \models t = t'$ then $M_\Gamma \models t = t'$ which means $\Gamma \vdash t = t'$.

For the second assertion, note that all the rules are finitely generated and by Proposition 3.2.6 we obtain the compactness of **AOSA**. (Q.E.D.)

As in the case of conditional equational logic, it is convenient for each variable symbol to have only one sort; therefore we assume that any S-indexed set $X = \{X_s \mid s \in S\}$ used to provide variables for a signature $(S, \leq, F)$ is such that X_{s_1} and X_{s_2} are disjoint whenever $s_1 \neq s_2$, and such that all symbols are in X are distinct from those in F. Note that if $(S, \leq, F)$ is coherent then $(S, \leq', F \cup X)$ is also coherent, where $\leq' = \leq \cup \{(x,x) \mid x \in X\}$. By an abuse of notation we let $\leq$ to denote $\leq'$.

Definition 6.1.3 (Order-sorted substitutions)**.** *Let $(S, \leq, F)$ be an order-sorted signature. A $(S, \leq, F)$-substitution of F-terms with variables in Y for variables in X is an arrow $\theta : X \to T_F(X)$. The unique extension of θ to*

1. *F-terms with variables in X is $\overline{\theta} : T_F(X) \to T_F(Y)$.*
2. *sentences in $\mathbb{S}en(S, \leq, F \cup X)$ is $\mathbb{S}en(\theta) : \mathbb{S}en(S, \leq, F \cup X) \to \mathbb{S}en(S, \leq, F \cup Y)$. As in case of signature morphisms when is no danger of confusion we let θ to denote the sentence translation $\mathbb{S}en(\theta)$.*

For any $(S, F \cup Y)$-model (M, f) we define the $(S, \leq, F \cup X)$-model $(M, f) \restriction_\theta$ as $(M, \theta; \overline{f})$, where $\overline{f} : T_F(Y) \to M$ is the unique extension of f to $(S, \leq, F)$-morphism.

Recall that given an order-sorted signature $(S, \leq, F)$ for any F-term t there exists a least sort denoted by $LS(t)$.

Lemma 6.1.4. *Order-sorted substitutions are sort decreasing, in that $LS(\theta(x)) \leq s$ for any $x \in X_s$ and more generally, $LS(\theta(t)) \leq LS(t)$ for any $(F \cup X)$-term.*

Proof. The first assertion follows because $\theta(x) \in (T_F(Y))_s$ and $LS(t) \leq s$ for any $x \in X_s$. The second assertion can be proved by induction on the structure of the term t. (Q.E.D.)

6.2 Error Sorts

The rules of order-sorted equational deduction are the same as for the equational deduction, but special care is needed when applying the rules of *Substitutivity*, according to Lemma 6.1.4.

Example 21. Consider the following specification

```
mod NON-DED{
[A<B]
op a :  -> A
op b :  -> B
ops f g :  A -> A
var X : A
eq f(X) = g(X) .
eq a = b .  }
```

The first equation can deduce `g(a)` from `f(a)`, and then the second equation can apparently deduce `g(b)` from `f(a)`; but `g(b)` is not a well-formed term. The problem is we can not substitute `b` for `X` because the sort `B` of `b` is (strictly) greater then the sort `A` of `X`, and by Lemma 6.1.4 the substitutions are sort decreasing.

Example 22. The models of the following specification are what one would expect, lists with elements 1, 2, 3.

```
mod LIST {
[Elt]
[NeList < List]
-- constructors
op empty :  -> List {constr}
op _,_ :  List Elt -> NeList {constr}
-- operators
ops :  1 2 3 -> Elt
op put :  Elt List -> NeList
op get :  NeList -> List
op top :  NeList -> Elt
-- variables
var Q : List
vars X Y : Elt
-- equations
eq [L1] :  put(X,empty) = empty,X .
eq [L2] :  put(X,(Q,Y)) = put(X,Q),Y .
eq [L3] :  get((Q,X)) = Q .
eq [L4] :  top((Q,X)) = X . }
```

Note that the terms like `top(get(put(1,put(2,put(3,empty)))))` are not well-formed because that the sub-term beginning with get has sort `List` while `top` requires sort `NeList`. However it is desirable to give such expressions the "benefit of the doubt" because they could evaluate (for the term above the correct answer is 2). Error sorts provide this capability by capturing terms which are not well-formed.

Example 23. We define the list with errors by extending the signature of `LIST` with error sorts.

```
mod ELIST {
[Elt < ErrElt]
[NeList < ErrNeList]
[List < ErrList]
[ErrNeList < ErrList]
-- constructors
op empty :  -> List {constr}
op _,_ :  List Elt -> NeList {constr}
-- operators
op _,_ :ErrList ErrElt -> ErrNeList
ops :  1 2 3 -> Elt
op put :  Elt List -> NeList
op put :  ErrElt ErrList -> ErrNeList
op get :  NeList -> List
op get :  ErrList -> ErrList
op top :  NeList -> Elt
op top :  ErrList -> ErrElt
-- variables
vars X Y : Elt
```

```
var Q : List
-- equations
eq [L1] :  put(X,empty) = empty,X .
eq [L2] :  put(X,(Q,Y)) = put(X,Q),Y .
eq [L3] :  get(Q,X) = Q .
eq [L4] :  top(Q,X) = X . }
```

Terms like `top(get(put(1,put(2,put(3,empty)))))` dot not parse in the context of `List` theory of Example 22, but they are accepted when super-sorts are added, as in Example 23; using CafeOBJ we get the following:

```
1. parse top(get(put(1,put(2,put(3,empty))))) .
   result top(get(put(1,put(2,put(3,empty))))):ErrElt

2. reduce top(get(put(1,put(2,put(3,empty))))) .
   result 2:Elt
```

meaning that the term `top(get(put(1,put(2,put(3,empty)))))` has the least sort `ErrElt` and it is equivalent modulo equations {`L1,...,L4`} to the term `2` which has the sort `Elt`. Note that the signature of `ELIST` is coherent.

Example 24. The following example shows that the above strategy needs some improvements.

```
mod NON-MON {
[S1 < S]
[S2 < S]
[S3]
[S4]
op f :  S1 -> S3
op f :  S2 -> S4
op a :  -> S
}
```

The signature of `NON-MON` is monotone and coherent. If we extend the above signature with error sorts then the monotonicity condition is not satisfied. We would have

```
op f :  ErrS -> ErrS3
op f :  ErrS -> ErrS4
```

If we use retracts functions (see [36]) then the resulting signature is monotone but in order to parse the term `f(a)` we do not know which retract should insert

```
op r:(S>S1) :  S -> S1, or
op r:(S>S2) :  S -> S2
```

to obtain `f(r:(S>S1)(a))` or `f(r:(S>S2)(a))`. Bellow we give the condition for a signature to be extendible with error sorts.

Definition 6.2.1. *A signature $(S,\leq,F)$ with finite number of symbols is extendible (with error sorts) if for every $\sigma \in F_{w_1\to s_1} \cap F_{w_2\to s_2}$ we have $w_1 \equiv w_2$ implies $s_1 \equiv s_2$, where $\equiv$ is the least equivalence relation over $\leq$.*

There are two ways to make the specification of Example 24 extendible: by adding a sort S' greater then $S1$ and $S2$, or by changing the name of the operation symbol `op f : S2 -> S4 .`

Assume an extendible signature $(S, \leq, F)$ and let $\equiv$ be the least congruence relation over $\leq$. For any operation symbol $\sigma \in F_{w \to s}$ we define

- $A^w_\sigma = \{w' \in S^* \mid w' \equiv w\}$ the connected component of w,
- $S^w_\sigma = \{s' \in S \mid \sigma \in F_{w' \to s'}, w' \equiv w\}$ the set of all sorts of σ with the arity in the same connected component as w,
- $(S')^w_\sigma = \{s' \in S \mid (\forall s'' \in S^w_\sigma) s'' \leq s'\}$ the set of all sorts greater then the ones in S^w_σ, and
- $(S'')^w_\sigma = \{s' \in (S')^w_\sigma \mid (\forall s'' \in (S')^w_\sigma) s' \leq s'' \vee s'' \leq s'\}$ the possible candidates for the error sort of σ.

All sorts in $(S')^w_\sigma$ are in the same connected component as s. Since the number of sorts is finite and the signature $(S, \leq, F)$ is coherent, there exists the greatest element of each connected component which implies that $(S')^w_\sigma$ is non-empty. The greatest element of the connected component of s is also in the set $(S'')^w_\sigma$ and $((S'')^w_\sigma, \leq)$ is a total ordering.

We extend the signature $(S, \leq, F)$ to the signature $(S_e, \leq_e, F^e)$ having

- the set of sorts $S_e = S \cup \{s_e \mid s \in S\}$,
- the ordering relation $\leq_e$ being the reflexive and transitive closure of $\leq \cup \{(s, s_e) \mid s \in S\} \cup \{(s_e, s'_e) \mid s \leq s'\}$, and
- the operations in F^e obtained by overloading the operations in F: for every $\sigma \in F_{w_1 \to s_1}$ we define $\sigma \in F^e_{w'_e \to s'_e}$ where w' is the greatest element of A^w_σ and s' is the least element of $(S'')^w_\sigma$.

Proposition 6.2.2. $(S_e, \leq_e, F^e)$ *is a coherent order-sorted signature.*

Proof. We prove that monotonicity condition is satisfied. Let $\sigma \in F^e_{w_1 \to s_1} \cap F^e_{w_2 \to s_2}$ such that $w_1 \leq_e w_2$.

1. *Case* $w_2 \in S^*$. Easy.
2. *Case* $w_2 = w''_e$, *where* $w'' \in S^*$.[1] There exists $s'' \in S$ such that $s_2 = s''_e$.
   (a) *Case* $w_1 \in S^*$. We have $s_1 \in S$ and by the definition of $\sigma \in F_{w'' \to s''}$ we have that s'' is the least element of $(S'')^{w_1}_\sigma$ and all the sorts in $(S'')^{w_1}_\sigma$ are greater then s_1 which implies $s_1 \leq s''$ and we get $s_1 \leq_e s''_e$.
   (b) *Case* $w_1 = w'_e$, *where* $w' \in S^*$. There exists $s' \in S$ such that $s_2 = s'_e$. Since $\sigma \in F_{w'_e \to s'_e} \cap F_{w''_e \to s''_e}$ and $w'_e \leq_e w''_e$, we have $w'_e = w''_e$ and $s'_e = s''_e$.

It is straightforward to prove that $(S_e, \leq_e, F^e)$ is locally filtered. We prove that $(S_e, \leq_e, F^e)$ is regular. Given $\sigma \in F^e_{w_1 \to s_1}$ and $w_0 \leq_e$ we show that the set $\{(w, s) \mid \sigma \in F^e_{w \to s}$ and $w_0 \leq_e w\}$ has an unique least element.

[1] $(s_1 \ldots s_2)_e = (s_1)_e \ldots (s_n)_e$

1. *Case* $w_1 \in S^*$. Easy.

2. *Case* $w_1 = w'_e$, *where* $w' \in S^*$. There exists $s' \in S$ such that $s_1 = s'_e$.

   (a) Assume there exists $\sigma \in F_{w_2 \to s_2}$ such that $w_0 \leq w_2$. Since $(S, \leq, F)$ is regular, the set $\{(w,s) \mid \sigma \in F_{w \to s} \text{ and } w_0 \leq w\}$ has an unique least element which is the unique least element of the set $\{(w,s) \mid \sigma \in F^e_{w \to s} \text{ and } w_0 \leq_e w\}$.

   (b) Assuming the contrary we get that (w'_e, s'_e) is the unique least element of the set $\{(w,s) \mid \sigma \in F^e_{w \to s} \text{ and } w_0 \leq_e w\}$.

(Q.E.D.)

Given an order-sorted signature $\Sigma = (S, \leq, F)$, extend it to the signature $\Sigma_e = (S_e, \leq_e, F^e)$ by adding error sorts and overloading the operations. Our requirement is that the signature inclusion $\Sigma \hookrightarrow \Sigma_e$ should be *conservative* in the sense that for every set of sentences $\Gamma \subseteq \mathbb{S}en(S, \leq, F)$ and each sentence $\rho \in \mathbb{S}en(S, \leq, F)$ we have $\Gamma \models_{(S,\leq,F)} \rho$ iff $\Gamma \models_{(S_e,\leq_e,F^e)} \rho$. Note that the implication from left to right holds by the satisfaction condition.

Proposition 6.2.3. *Any inclusion* $\iota : (S, \leq, F) \hookrightarrow (S_e, \leq_e, F^e)$ *is conservative.*

Proof. It suffices to prove that any order-sorted $(S, \leq, F)$-algebra M admits an ι-expansion M'. Indeed if $\Gamma \models_{(S_e,\leq_e,F^e)} \rho$ then assuming that $M \models_{(S,\leq,F)} \Gamma$ (for an arbitrary chosen $(S, \leq, F)$-model M) there exists an ι-expansion M' of M; by the satisfaction condition $M' \models_{(S_e,\leq_e,F^e)} \Gamma$ and we have $M' \models_{(S_e,\leq_e,F^e)} \rho$ and using again the satisfaction condition we obtain $M \models_{(S,\leq,F)} \rho$; since M was arbitrary we get $\Gamma \models_{(S,\leq,F)} \rho$.

Given an order-sorted $(S, \leq, F)$-algebra we define the S_e-indexed set M^e recursively by the following:

1. $M_s \subseteq M^e_s$, for $s \in S$,

2. $s \leq_e s'$ implies $M^e_s \subseteq M^e_{s'}$,

3. $\sigma \in F^e_{w \to s}$ with $(w,s) \in (S^e)^+ \times (S^e)$, $m \in M^e_w$, and $m \notin M_{w_0}$ for all $w_0 \leq_e w$ such that $\sigma \in F_{w_0 \to s_0}$, imply $\sigma(m) \in M^e_s$.

Now we define the functions on M^e:

1. for every $\sigma \in F_{w \to s}$, since $M^e_w = M_w$, we define $M^e_\sigma = M_\sigma$,

2. for every $\sigma \in F^e_{w \to s}$ we define $M^e_\sigma : M^e_w \to M^e_s$ as follows: for every $m \in M^e_w$

   - $M^e_\sigma(m) = M_\sigma(m)$ when there exists $\sigma \in F_{w_0 \to s_0}$ such that $w \leq_e w$ and $m \in M_{w_0}$
   - $M^e_\sigma(m) = \sigma(m)$, otherwise.

Because $M_s = M^e_s$ for all sorts $s \in S$ and $M_\sigma = M^e_\sigma$ for all operation symbols $\sigma \in F$, the order-sorted model M^e is an ι-expansion of M. (Q.E.D.)

Example 25. Now extend the signature of `MAP` (see Example 17) with error sorts.

```
mod EMAP {
[A B < Elt]
[A < ErrA]
[B < ErrB]
```

```
[Elt < ErrElt]
[ErrA ErrB < ErrElt]
ops T F : -> B
ops (_∨_) (_∧_) :  B B -> B
ops (_∨_) (_∧_) :  ErrElt ErrElt -> ErrB .
op ¬_ :  B -> B op
¬_ :  ErrElt -> ErrB
op map :  A -> B
op map :  ErrElt -> ErrB
var X : B .
var Y : A .
eq [M1] :  X ∨ ¬ X = T .
eq [M2] :  X ∧ ¬ X = F .
eq [M3] :  X ∨ X = X .
eq [M4] :  X ∧ X = X .
eq [M5] :  ¬ F = T .
eq [M6] :  ¬ T = F .
eq [M7] :  ¬ map(Y) = map(Y) . }
```

Note that the extension of the signature of `MAP` with error sorts is conservative but the extension of signature of `MAP` with retracts is not conservative. Indeed, since `MAP` $\models$ `(∀Y) T = F` and the extension of `MAP` with retracts `RMAP` contains the terms `r:(A<Elt)(0)` and `r:(A<Elt)(1)`, we have `RMAP` $\models$ `T = F`, but `MAP` $\not\models$ `T = F` (for details see [36, 32]).

Given an arbitrary order-sorted signature $(S, \leq, F)$ which is not extendible with error sorts, then by adding a distinguished "super-sort" sp greater then all the sorts in S, the new signature becomes extendible. If we denote by $(S', \leq', F')$ the new signature then the signature inclusion $(S, \leq, F) \hookrightarrow (S', \leq', F')$ is conservative and also $(S, \leq, F) \hookrightarrow (S'_e, \leq'_e, (F')^e)$.

Chapter 7

A Case Study

We specify a transitional system using constructor-based universal order-sorted algebra with predicates (abrev. **CUOSAP**) and point out some methodologies for modeling and proof plans. The institution **CUOSAP** is an extension of **CUOSA** with

- signatures $(S, \leq, F, F^c, P)$ consisting of a constructor-based order-sorted signature $(S, \leq, F, F^c)$ and a set P of predicate symbols,
- universal sentences $(\forall X)(\forall Y)\rho$ formed over equational and relational atoms, where X is a finite set of constrained variables, Y a finite set of loose variables and ρ a quantifier-free sentence,
- models consisting of an order-sorted algebra M plus an interpretation for each predicate symbol $\pi \in P_w$ as a relation $M_\pi \subseteq M_w$.

Remark 7.0.4. *Recall that an universal sentence* $(\forall X)(\forall Y)\rho$ *may be written as* $(\forall X \cup Y)\rho$.

Not all sets of sentences in **CUOSAP** admit initial model, or are even consistent. Since our work is closely related to algebraic specification languages, one important issue is the consistency of the specifications (the class of models of the given specification is not empty). For example if we consider only sentences of the form $(\forall X)H \Rightarrow C$, where X is any set of variables, H is any quantifier-free sentence, and C is an equational atom, then any basic specification is consistent (has models).

The example used to present the applicability of our theoretical results is a mutual exclusion protocol, due to [27] which also describes the *OTS/CafeOBJ method*. The OTS/CafeOBJ method is a modeling, specification and verification method for systems, and it has been developed and refined through some case studies [27, 54, 53, 56, 55]. Our theoretical framework is slightly different since we do not use hidden logic and initial semantics for the specifications and the verification of the mutual exclusion property significantly more simpler than in [27].

7.1 Preliminaries

Definition 7.1.1. *The entailment system of* **CUOSAP** *is the entailment system with disjunctions, false, negations, and universal quantifications freely generated by the rules of*

$$(Reflexivity)\frac{}{\emptyset \vdash_{(S,\leq,F,F^c,P)} t = t}$$

for each term $t \in T_F$.

$$(Symmetry)\frac{}{t = t' \vdash_{(S,\leq,F,F^c,P)} t' = t}$$

for any terms $t, t' \in T_F$.

$$(Transitivity)\frac{}{\{t = t', t' = t''\} \vdash_{(S,\leq,F,F^c,P)} t = t''}$$

for any terms $t, t', t'' \in T_F$.

$$(Congruence)\frac{}{\{t_i = t_i' | 1 \leq i \leq n\} \vdash_{(S,\leq,F,F^c,P)} \sigma(t_1, ..., t_n) = \sigma(t_1', ..., t_n')}$$

for any function symbol $\sigma \in F$ *and terms* $t_i \in T_F$, *where* $i \in \{1, \ldots, n\}$.

$$(PCongruence)\frac{}{\{t_i = t_i' | 1 \leq i \leq n\} \cup \{\pi(t_1, ..., t_n)\} \vdash_{(S,\leq,F,F^c,P)} \pi(t_1', ..., t_n')}$$

for any predicate symbol $\pi \in P$ *and terms* $t_i \in T_F$, *where* $i \in \{1, \ldots, n\}$.

$$(Substitutivity)\frac{}{(\forall Y)\rho \vdash_{(S,\leq,F,F^c,P)} (\forall X)\theta(\rho)}$$

for any universal sentence $(\forall Y)\rho$ *and substitution* $\theta : Y \to T_F(X)$, *where* X *and* Y *are any sets of loose variables, and* ρ *a quantifier-free sentence.*

$$(Case\ splitting)\frac{\{\Gamma \vdash_{(S,\leq,F,F^c,P)} (\forall Y)\theta(\rho) \mid Y - loose\ variables,\ \theta : X \to T_{F^c}(Y)\}}{\Gamma \vdash_{(S,\leq,F,F^c,P)} (\forall X)\rho}$$

for every set of sentences Γ, *and any universal sentence* $(\forall X)\rho$, *where* X *is a set of constrained variables.*

Theorem 7.1.2 (Completeness of **CUOSAP**). *The entailment system of* **CUOSAP** *is sound and complete.*

The proof of the above theorem will be given in Chapter 8 in the framework of institutions. Note that semantic entailment of **CUOSAP** satisfies the rules of *Implications* and by Theorem 7.1.2 we obtain that the entailment system of **CUOSAP** satisfies the rules of *Implications*. One direct consequence is that the entailment system of **CUOSAP** satisfies the rules of *Modus Ponens*.

$$(Modus\ ponens)\frac{\{\rho_1 \Rightarrow \rho_2, \rho_1\}}{\rho_2}$$

Since $\{\neg\rho\} \vdash \neg\rho$, by *Red* we have

$$(Contr)\{\neg\rho, \rho\} \vdash false$$

In CafeOBJ each module imports the data type of the Boolean by default [25]. This has multiple consequences, for example, it supports a more general form of conditional equations, where conditions are Boolean-sorted terms rather than just finite conjunctions of identities. By protecting the Boolean-values `true` and `false` the Boolean-sorted terms may be interpreted as predicates. The other operations on `Bool` (such as `and, or`) may be regarded as first-order constructors for sentences in the sense of Definition 2.3.1.

7.2 Specifying a mutual exclusion protocol

The example used here is a mutual exclusion protocol, an algorithm which ensure that no more than one process have access to a common shared source at a given time. Initially, each process `i` is in the *reminder section*. After process `i` puts its name at the bottom of a waiting queue, `i` is in the *waiting section*. Process `i` will be in the *critical section* and have access to the information when it will be the first in the queue. When it leaves the source process `i` will be removed from the queue entering again in the remainder section.

We use a "super-sort" `Univ`, greater than the rest of the sorts such that the meta equality and the object-level equality, provided by the predicate `pred _=_ : Univ Univ`, are the same according to the equations `[m=>o]` and `[o=>m]` bellow. The module `UNIV` will be imported by all other modules and it will provide an equality predicate for all the sorts. The sort `Univ` works like a parameter.

```
mod UNIV{
[Univ]
pred _=_ :  Univ Univ
vars X Y : Univ
eq [m=>o] :  (X = X) = true .
ceq [o=>m] :  X = Y if (X = Y) .
}
```

`Label` is the sort for the set of labels of each section.

```
mod LABEL (ONE ::  UNIV){
[Label < Univ]
-- constructors
ops rm wt cs :  -> Label {constr}
-- equations
eq [L1] :  (rm = wt) = false .
eq [L2] :  (rm = cs) = false .
eq [L3] :  (wt = cs) = false .
}
```

We could declare the specification `LABEL` with initial semantics and ignore the equations `L1,L2,L3`. The classes of models of the specifications `LABEL` and `I-LABEL` (see bellow) are equal, but we need to specify that the constants `rm, wt, cs` are distinct in order to prove the desired properties.

```
mod!  I-LABEL (ONE ::  UNIV){
using(UNIV)
[Label < Univ]
-- constructors
ops rm wt cs :  -> Label {constr}
}
```

`Pid` is the sort for the set of process names. We use an error sort `ErrPid` to declare a constant `nonepid` different of all process names.

```
mod PID (TWO ::  UNIV){
[Pid < ErrPid < Univ]
-- operations
op nonepid :  -> ErrPid
-- variables
```

```
var I : Pid
-- equations
eq (nonepid = I) = false .
}
```

`Queue` is the sort for the queues of process IDs. The constant `empty` denotes the empty queue and the operator `op _,_ : Queue Pid -> Queue` is the data constructor of non-empty queues. The operators `put, get, top` are the usual functions of queues, which are defined with equations.

```
mod QUEUE {
using(PID)
[Queue < Univ]
-- constructors
op empty : -> Queue {constr}
op _,_ : Queue Pid -> Queue {constr}
-- operators
op put : Pid Queue -> Queue
op get : Queue -> Queue
op top : Queue -> ErrPid
-- variables vars X Y : Pid
var Q : Queue
-- equations
eq put(X,empty) = empty,X .
eq put(X,(Q,Y)) = put(X,Q),Y .
eq get(empty) = empty .
eq get(Q,X) = Q .
eq top(empty) = nonepid .
eq top(Q,X) = X .
}
```

The pseudo-code executed by each process `i` can be written as follows:

rm: `put(i,queue)`

wt: **repeat until** `top(queue) = i`

`Critical section`

cs: `get(queue)`

where `queue` is the queue of process IDs shared by all processes; `put(i,queue)` puts a process ID `i` at the end of `queue`, `get(queue)` deletes the top element from `queue`, and `top(queue)` returns the top element of `queue`. Initially, each process `i` is at the label `rm` and the `queue` is empty. The transition system is specified as follows:

```
mod QLOCK {
using(LABEL(UNIV))
using(QUEUE(UNIV))
[Sys < Univ]
-- constructors
op init : -> Sys {constr}
ops want try exit : Sys Pid -> Sys {constr}
```

```
-- operators
op pc :  Sys Pid -> Label
op queue :  Sys -> Queue
-- variables
var S : Sys
vars I J : Pid
-- equations
-- for init
eq queue(init) = empty .
eq pc(init,I) = rm .
-- for want
op c-want :  Sys Pid -> Bool {strat:  (0 1 2)}
eq c-want(S,I) = (pc(S,I) = rm) .
ceq pc(want(S,I),J) =
(if (I = J) then wt else pc(S,J) fi) if c-want(S,I) .
ceq queue(want(S,I)) = put(I,queue(S)) if c-want(S,I) .
ceq want(S,I) = S if not c-want(S,I) .
-- for try
op c-try :  Sys Pid -> Bool {strat:  (0 1 2)}
eq c-try(S,I) = (pc(S,I) = wt) and (top(queue(S)) = I) .
ceq pc(try(S,I),J) =
(if (I = J) then cs else pc(S,J) fi) if c-try(S,I) .
eq queue(try(S,I)) = queue(S) .
ceq try(S,I) = S if not c-try(S,I) .
-- for exit
op c-exit :  Sys Pid -> Bool {strat:  (0 1 2)}
eq c-exit(S,I) = (pc(S,I) = cs) .
ceq pc(exit(S,I),J) =
(if (I = J) then rm else pc(S,J) fi) if c-exit(S,I) .
ceq queue(exit(S,I)) = get(queue(S)) if c-exit(S,I) .
ceq exit(S,I) = S if not c-exit(S,I) .
}
```

There are three constructors for the sort `Queue`: `want`, `try` and `exit`. The operators `pc` and `queue` are inductively defined on the structure of the terms of sort `Sys`. The predicates `c-want`, `c-try` and `c-exit` may be regarded as derived operators, and depending whether they are `true` or `false`, the state will change or remains the same.

7.3 Verifying the mutual exclusion property

The property to be shown is that at most one process is in the critical section (or at the label `cs`) at any moment, that is `(∀S)(∀I)(∀J)pc(S,I)=cs∧pc(S,J)=cs⇒(I=J)` holds. Firstly we prove `(∀S)(∀I)pc(S,I)=cs⇒top(queue(S))=I`. By *Structural induction* we need to deduce

IB `(∀ I)pc(init,I) = cs ⇒ top(queue(init)) = I`, and

IS `(∀J)pc(s,J) = cs ⇒ top(queue(s)) = J` implies

1. (∀J)pc(want(s,i),J) = cs ⇒ top(queue(want(s,i))) = J
2. (∀J)pc(try(s,i),J) = cs ⇒ top(queue(try(s,i))) = J
3. (∀J)pc(exit(s,i),J) = cs ⇒ top(queue(exit(s,i))) = J

where s is a constant of sort Sys and i is a constant of sort Pid.

We declare a predicate inv which represents the formula to be proved and we add new constant symbols op s : -> Sys, ops i j : -> Pid. Since the induction hypothesis ceq [IH] : top(queue(s)) = J if pc(s,J) = cs is not executable by rewriting we add also the equations IH-i and IH-j obtained from IH by substituting i and j for J.

```
mod INV{
using(QLOCK)
pred inv :  Sys Pid
var S : Sys
var J : Pid
eq inv(S,J) = (pc(S,J) = cs implies top(queue(S)) = J) .
op s :  -> Sys
ops i j :  -> Pid
ceq [IH] : top(queue(s)) = J if pc(s,J) = cs .
ceq [IH-i] :  top(queue(s)) = i if pc(s,i) = cs .
ceq [IH-j] :  top(queue(s)) = j if pc(s,j) = cs .
}
```

For the induction base, we write a proof passage, which is as follows:

```
open INV
red inv(init,j) .
close
```

The first thing to do for the induction step is to split each case into two sub-cases depending whether the condition to change the state holds or not. Take for example the constructor want: because INV⊢c-want(s,i)∨¬c-want(s,i) if INV ∪ {c-want(s,i)}⊢inv(want(s,i),j) and INV ∪ {¬c-want(s,i)}⊢ inv(want(s,i),j) then by *Disjunction elimination* INV ⊢ inv(want(s,i),j).

Because the state does not change when the condition for changing the state does not hold, we will focus on the (sub-)cases when the conditions hold.

1. Since ∅⊢(i=j)∨¬(i=j), where _ = _ is the equality predicate, if INV ∪ {i=j} ⊢ inv(want(s,i),j) and INV ∪ {¬ i = j } ⊢ inv(want(s,i),j) then by *Disjunction elimination* we have INV⊢inv(want(s,i),j). So we split this (sub)-case into two sub-cases as follows:

   (a)
   ```
   -- c-want(s,i) j = i
   open INV
   eq j = i .
   eq c-want(s,i) = true .  eq pc(s,i) = rm .
   red inv(want(s,i),j) .
   close
   ```

Because `c-want(s,i) = (pc(s,i) = rm)` and the object-level equality is equivalent to the meta equality, we have introduced `eq pc(s,i) = rm` in the proof passage above.

(b)
```
-- c-want(s,i) j=/=i
open INV
var X : Pid
var Q : Queue
eq (i = j) = false .
eq c-want(s,i) = true .
eq pc(want(s,i),j) = cs .  eq pc(s,j) = cs .
ceq top(put(X,Q)) = top(Q) if (top(Q) :is Pid) .
red inv(want(s,i),j) .
close
```

In this case `pc(want(s,i),j)=pc(s,j)` and since `pc(want(s,i),j)=cs`, we introduced `pc(s,j) = cs`. We proved `pc(want(s,i),j)=cs implies (top(queue(want(s,i)))=j)` assuming `pc(want(s,i),j) = cs`. By *Modus ponens* we obtain `(top(queue(want(s,i)))=j)` assuming `pc(want(s,i),j)=cs` which is the goal here.

2. Using *Disjunction elimination* as above, we split this (sub-)case into two sub-cases depending on whether `i = j` is `true` or not.

(a)
```
-- c-try(s,i) j = i
open INV
eq j = i .
eq c-try(s,i) = true .
eq pc(s,i) = wt .  eq top(queue(s)) = i .
red inv(try(s,i),j) .
close
```

Since `c-try(s,i) = (pc(s,i) = wt and top(queue(s)) = i)` and `c-try(s,i)=true`, we added the equations `pc(s,i)=cs` and `top(queue(s))=i`.

(b)
```
-- c-try(s,i) j=/=i
open INV
eq (i = j) = false .
eq c-try(s,i) = true .
eq pc(try(s,i),j) = cs .  eq pc(s,j) = cs .
red inv(try(s,i),j) .
close
```

Here we proved `pc(try(s,i),j) = cs implies (top(queue(try(s,i))) = j)` assuming `pc(try(s,i),j) = cs`. By *Modus ponens* we obtain `top(queue(try(s,i)))=j` assuming `pc(try(s,i),j) = cs` which is the goal of this case.

3. As above, we split this (sub)-case into two sub-cases, depending on whether `(i=j)` is `true` or not.

   (a)
   ```
   -- c-exit(s,i) j = i
   open INV
   eq j = i .
   eq c-exit(s,i) = true .  eq pc(s,i) = cs .
   red inv(exit(s,i),j) .
   close
   ```

   (b)
   ```
   -- c-exit(s,i) j=/=i
   open INV
   eq (i = j) = false .
   eq c-exit(s,i) = true .
   eq pc(s,i) = cs .
   eq pc(exit(s,i),j) = cs .  eq pc(s,j) = cs .
   start i = j .
   apply -.IH-j at (2) .
   apply red at term .
   apply red at term .
   -- since (i=j) = false, we have reached a contradiction.
   close
   ```

   In this case we have `(i=j) = false` and by adding the equation `eq pc(exit(s,i),j) = cs` we deduce `i = j` which is a contradiction. By *False* we obtain `top(queue(exit(s,i))) = j`.

Finally, the proof of mutual exclusion property `(∀ S)(∀ I)(∀ J)pc(S,I) = cs ∧ pc(S,J) = cs ⇒ (I = J)`, is as follows:

```
open QLOCK
op s :  -> Sys .
ops i j :  -> Pid .
ceq [inv] :  top(queue(S:Sys)) = I:Pid if pc(S,I) = cs .
eq pc(s,i) = cs .  eq pc(s,j) = cs .
start i = j .
apply -.inv with I = i, S = s at (1) .
apply red at term .
apply -.inv with I = j, S = s at (2) .
apply red at term .
apply red at term .
close
```

Breaking the goals into smaller subgoals by applying *Structural induction* or *Disjunction elimination*, are conducted by hand here but future developments of CafeOBJ aim for mechanizing the proofs. The initial semantics for specifications plays an important role only at level of specifications. For proving properties of systems we make use of all Boolean connectors. Intuitively, we use the "non-Horn" sentences to define recursively some operations, like `pc` or `queue` above, or to reduce the class of models of the specifications, possible to the initial model (see the specifications `I-LABEL` and `LABEL`).

The theoretical framework and results (more precisely the layered approach to completeness) reflect to the level of proofs. When we want to infer a property from a set of axioms, firstly, we establish an induction scheme; this has the effect of breaking the initial goal into "smaller" subgoals, sentences formed without quantifications over constrained variables. The semantic consequences of the theories of constructor-based logics are not in general recursively enumerable which implies that there is no general algorithm to find an induction scheme, even the formulas to be proved are the true of all models of the given specification.

The new goals are sentences of the form $(\forall Y)\rho$, where Y is a set of loose variables and ρ is a quantifier-free sentence, which are "computable" whenever they are the semantic consequences of the given axioms. In order to prove the new properties formalized as sentences, we use the rules of *Generalization*; we add the loose variables to the initial signature and prove the quantifier-free part of the sentences in the new signature.

The example with the mutual exclusion protocol is due to [27] which describes also the OTS/CafeOBJ method. The proof of mutual exclusion property is more simpler than in [27] because of the intermediate property/invariant `(∀S)(∀I)pc(S,I)=cs⇒top(queue(S))=I` that we deduce first. This shows that intuition plays an important role in simplifying the proofs. Also note that we do not use here simultaneous induction.

Chapter 8

Universal Institutions

We present an institution-independent completeness result applicable to constructor-based Horn institutions such as **CHCL**, **CHOSA**, **CHPOA**, **CHPA** and also their infinitary versions. Our study isolates the particular aspects of the logics from general ones in order to obtain an abstract completeness which covers many examples such as the ones mentioned above and also the variations of them: for example constructor-based Horn order-sorted algebra with transitions or/and predicates. The applicability of the main theorems are also investigated in the next chapter.

The present work has a great significance to computer science. Modern algebraic specification languages (such as CafeOBJ [26], CASL [2], or Maude [15]) are rigorously based on logic, in the sense that each feature and construct in a language can be expressed within a certain logic underlying it. In the context of proliferation of a multitude of specification languages, these abstract results provide complete systems of proof rules for the logical systems underlying the algebraic specification languages.

In this chapter we present the abstract concept of universal institution [16] and reachable universal weak entailment system [28] which is proved sound and complete with respect to a class of reachable models, under conditions which are also investigated. The weak entailment system developed here is then borrowed by constructor-based institutions through institution morphisms. Soundness is preserved, and completeness is relative to a family of sets of sentences.

8.1 Definition and Examples

Let $I = (\mathbb{S}ig, \mathbb{S}en, \mathbb{M}od, \models)$ be an institution, $D \subseteq \mathbb{S}ig$ be a broad subcategory of signature morphisms, and $\mathbb{S}en^\bullet$ be a sub-functor of $\mathbb{S}en$ (i.e. $\mathbb{S}en^\bullet : \mathbb{S}ig \to \mathbb{S}et$ such that $\mathbb{S}en^\bullet(\Sigma) \subseteq \mathbb{S}en(\Sigma)$ and $\varphi(\mathbb{S}en^\bullet(\Sigma)) \subseteq \mathbb{S}en^\bullet(\Sigma')$, for each signature morphism $\varphi : \Sigma \to \Sigma'$). We denote by $I^\bullet$ the institution $(\mathbb{S}ig, \mathbb{S}en^\bullet, \mathbb{M}od, \models)$. We say that I is a *D-universal institution over $I^\bullet$* when

- I admits all sentences of the form $(\forall\chi)\rho$, where $\chi : \Sigma \to \Sigma'$ is a signature morphism in D and ρ is a sentence in $\mathbb{S}en^\bullet(\Sigma')$, and
- any sentence of I is of the form $(\forall\chi)\rho$ as above.

The followings are a couple of examples of universal institutions.

Example 26 (Generalized first-order logic (**GFOL**))**.** Its signatures (S, S^c, F, P) consist of a first-order signature (S, F, P) and a distinguished set of sorts $S^c \subseteq S$. We call the set of sorts

S^c *constrained* and $S^l = S - S^c$ *loose*. A *generalized first-order signature morphism* between (S, S^c, F, P) and (S_1, S_1^c, F_1, P_1) is a simple signature morphism between (S, F, P) and $(S_1, F_1 + T_{F_1}, P_1)$, i.e. constants can be mapped to terms. The sentences are the *universal constrained first-order sentences* of the form $(\forall X)e$, where X is a finite set of variables of constrained sorts and e is a formula formed over atoms by applying Boolean connectives and quantifications over variables of loose sorts. Models are the usual first-order structures and satisfaction is the usual first-order satisfaction. Note that **GFOL** is a D^c-universal institution over its restriction to first-order sentences built over the atoms by applying Boolean connectives and quantifications over variables of loose sorts, where D^c is the class of signature extensions with finite number of constants of constrained sorts.

GFOL$_{\omega_1,\omega}$ is the infinitary extension of **GFOL** obtained by allowing for a sentence $(\forall X)e$ countable disjunctions for the construction of the first-order part e. In case of **GFOL**$_{\omega_1,\omega}$ we do not allow quantifications over infinite sets of variables. **GFOL**$_{\omega_1,\omega}$ is a D^c-universal institution over its restriction to infinitary first-order sentences built over the atoms by applying Boolean connectives and quantifications over finite sets of variables of loose sorts, where D^c is the subcategory of signature morphisms which consists of signature extensions with finite number of constants of constrained sorts.

Example 27 (Generalized universal first-order logic (**GUFOL**)). This is the restriction of **GFOL** to *universal sentences* of the form $(\forall X)(\forall Y)\rho$, where X is a finite set of constrained variables, Y is a finite set of loose variables, and ρ is a quantifier-free sentence. **GUFOL** is a D^c-universal institution over the restriction of **GFOL** to universal sentences $(\forall Y)\rho$ with Y a finite set of loose variables, and ρ a quantifier-free sentence, where D^c is the same as in the case of **GFOL**.

GUFOL$_\infty$ is the infinitary extension of **GUFOL** obtained by allowing:

- the sets X and Y of variables of a sentence $(\forall X)(\forall Y)\rho$ to be infinite, and
- infinitary disjunctions for the construction of the quantifier-free part ρ.

Note that **GUFOL**$_\infty$ is also a D^c-universal institution over its restriction to infinitary universal sentences $(\forall Y)\rho$ with Y a set of loose variables (possible infinite) and ρ a quantifier-free sentence, where D^c consists of signature extensions with constants (possible infinite) of constrained sorts.

Example 28 (Generalized Horn clause logic (**GHCL**)). This is the sub-institution of **GFOL** obtained by restricting the sentences to *universal Horn sentences* of the form $(\forall X)(\forall Y) \wedge H \Rightarrow C$, where X is a finite set of variables of constrained sorts, Y is a finite set of variables of loose sorts, H is a finite set of (relational or equational) atoms, C is a (relational or equational) atom, $\wedge H$ is the conjunction of the set of sentences in H, and $\wedge H \Rightarrow C$ is the implication of C by $\wedge H$. **GHCL** is a D^c-universal institution over the restriction of **GFOL** to the quantifier-free sentences, where D^c consists of signature extensions with finite number of constants of constrained sorts.

GHCL$_\infty$ is the infinitary extension of **GHCL** obtained by allowing *infinitary universal Horn sentences* $(\forall X)(\forall Y) \wedge H \Rightarrow C$ where the sets X, Y and H may be infinite. **GHCL**$_\infty$ is also a D^c-universal institution, but this time D^c consists of signature extensions with constants (possible infinite) of constrained sorts.

By considering the case of empty sets of relational symbols, we obtain the generalized conditional equational logic, **GCEQL**, and its infinitary version **GCEQL**$_\infty$.

By allowing constants to be mapped into terms, and distinguishing a subset of constrained sorts for each signature, we obtain the generalizations of

1. order-sorted algebra: **GOSA**, **GUOSA**, **GHOSA**, and also their infinitary versions such as $\mathbf{GOSA}_{\omega_1,\omega}$, $\mathbf{GUOSA}_{\infty}$, $\mathbf{GHOSA}_{\infty}$

2. preorder algebra: **GPOA**, **GUPOA**, **GHPOA**, and also their infinitary versions such as $\mathbf{GPOA}_{\omega_1,\omega}$, $\mathbf{GUPOA}_{\infty}$, $\mathbf{GHPOA}_{\infty}$

3. partial algebra: **GPA**, **GUPA**, **GHPA**, and also their infinitary versions $\mathbf{GPA}_{\omega_1,\omega}$, $\mathbf{GUPA}_{\infty}$, $\mathbf{GHPA}_{\infty}$

8.2 Institution Independent Notions

Reasoning at the institutional level is an attempt to reason generically about the properties of the logics. In order to obtain non-trivial results about classes of logics we define abstractly the properties of these logics together with the explanations in concrete examples.

8.2.1 Soundness and Completeness - revisited

Recall that a weak entailment system (abbreviated *WES*) is defined as an entailment system without the *Translation* property.

Definition 8.2.1. *Assume an institution $I = (\mathbb{S}ig, \mathbb{S}en, \mathbb{M}od, \models)$ and a family of classes of models $M = \{M_\Sigma\}_{\Sigma \in |Sig|}$. A WES $E = (\mathbb{S}ig, \mathbb{S}en, \vdash)$ of the institution I is* sound *(resp.* complete*) with respect to M when $E \vdash e$ implies $M \models (\bigwedge E \Rightarrow e)$ (resp. $M \models (\bigwedge E \Rightarrow e)$ implies $E \vdash e$)* [1] *for all sets of sentences $E \subseteq \mathbb{S}en(\Sigma)$, sentences $e \in \mathbb{S}en(\Sigma)$ and models $M \in M_\Sigma$.*

Remark 8.2.2. *Note that the entailment system E is* sound *(resp.* complete*) when $M_\Sigma = |\mathbb{M}od(\Sigma)|$ for all signatures Σ.*

Let $I = (\mathbb{S}ig, \mathbb{S}en, \mathbb{M}od, \models)$ be an institution, and $M = \{M_\Sigma\}_{\Sigma \in |Sig|}$ a family of classes of models. We say that a rule

$$\frac{\{E_i \vdash_{\Sigma_i} E'_i \mid i \in J\}}{E \vdash_\Sigma E'}$$

of a system of rules $R = (\mathbb{S}ig, \mathbb{S}en, Rl)$ is sound with respect to M whenever $M \models (\bigwedge E_i \Rightarrow \bigwedge E'_i)$, for all models $M \in M$ and indexes $i \in J$ implies $M \models (\bigwedge E \Rightarrow \bigwedge E')$ for all models $M \in M$. We say that R is sound with respect to M whenever each rule in Rl is sound with respect to M.

Proposition 8.2.3. *An entailment system $E = (\mathbb{S}ig, \mathbb{S}en, \vdash)$ of an institution $I = (\mathbb{S}ig, \mathbb{S}en, \mathbb{M}od, \models)$ is sound with respect to a family M of classes of models whenever is generated by a system of rules sound with respect to M.*

Proof. The proof is straightforward by induction in the definition of $\vdash$. (Q.E.D.)

[1] $M \models (\bigwedge E \Rightarrow e)$ iff $M \models E$ implies $M \models e$

8.2.2 Basic sentences

A set of sentences $E \subseteq Sen(\Sigma)$ is called *basic* [20] if there exists a Σ-model M_E such that, for all Σ-models M, $M \models E$ iff there exists a morphism $M_E \to M$.

Lemma 8.2.4. *Any set of atomic sentences in* **FOL**, **OSA**, **POA**, *and* **PA** *is basic.*

Proof. In **FOL** the basic model M_E for a set E of atomic (S,F,P)-sentences is constructed as follows: on the quotient $(T_F)/_{\equiv_E}$ of the term model T_F by the congruence generated by the equational atoms of E, we interpret each relation symbol $\pi \in P$ by $(M_E)_\pi = \{(t_1/_{\equiv_E}, \ldots, t_n/_{\equiv_E}) \mid \pi(t_1,\ldots,t_n) \in E\}$. A similar argument as the preceding holds for **POA** and **OSA**.

In **PA** for a set of atomic sentences E we define S_E to be the set of sub-terms appearing in E. Note that S_E is a partial algebra. The basic model M_E will be the quotient of this algebra by the partial congruence induced by the equalities from E. (Q.E.D.)

Basic sentences were introduced in [64] under the name of "ground positive elementary sentences". We prefered to use the terminology from [20].

8.2.3 Reachable models

As implied by the definition of signature morphisms of the generalized institutions defined in this chapter, we are going to treat the substitutions as signature morphisms.

Definition 8.2.5. *Consider two signature morphisms $\chi_1 : \Sigma \to \Sigma_1$ and $\chi_2 : \Sigma \to \Sigma_2$ of an institution. A signature morphisms $\theta : \Sigma_1 \to \Sigma_2$ such that $\chi_1;\theta = \chi_2$ is called a* substitution *between χ_1 and χ_2.*

A more general treatment of substitutions can be found in Chapter 10.

Definition 8.2.6. *Let $\mathcal{D}$ be a broad subcategory of signature morphisms of an institution. We say that a Σ-model M is $\mathcal{D}$-reachable if for each span of signature morphisms $\Sigma_1 \xleftarrow{\chi_1} \Sigma_0 \xrightarrow{\chi} \Sigma$ in $\mathcal{D}$, each χ_1-expansion M_1 of $M\restriction_\chi$ determines a substitution $\theta : \chi_1 \to \chi$ such that $M\restriction_\theta = M_1$.*

Proposition 8.2.7. *In* **GFOL**, **GOSA**, **GPOA** *and* **GPA**, *assume that $\mathcal{D}$ is the class of signature extensions with (possibly infinite number of) constants. A model M is $\mathcal{D}$-reachable iff its elements are exactly the interpretations of terms.*

Proof. We treat each case separately.

GFOL : For every inclusion $\Sigma \hookrightarrow \Sigma(Z)$ in $\mathcal{D}$, where $\Sigma = (S,S^c,F,P)$ and $\Sigma(Z) = (S,S^c,F \cup Z,P)$, the $\Sigma(Z)$-models can be represented as pairs (A,a), where A is a Σ-model and $a : Z \to A$ is a function.

Let $\Sigma = (S,S^c,F,P)$ be a signature and assume a Σ-model M which is $\mathcal{D}$-reachable. We prove that $T_F \to M$ is surjective, i.e. for every $m \in M$ there exists $t \in T_F$ such that $M_t = m$. Let $m \in M_s$ be an arbitrary element of M. Consider a variable x of sort s and let N be an expansion of M along $\Sigma \hookrightarrow \Sigma(x)$ (where $\Sigma(x) = (S,S^c,F \cup \{x\},P)$) which interprets the constant symbol x as m. Since M is $\mathcal{D}$-reachable there exists a substitution $\theta : \{x\} \to T_F$ such that $M\restriction_\theta = N$. Take $t = \theta(x)$ and we have $M_t = M_{\theta(x)} = (M\restriction_\theta)_x = N_x = m$.

For the converse implication let $\Sigma = (S,S^c,F,P)$ be a signature, X and Y two disjoint sets of constants with elements which are different from the symbols in Σ, and (M,h) a

$\Sigma(Y)$-model with elements which are interpretation of terms, i.e. the unique extension $\overline{h} : T_F(Y) \to M$ of h to a Σ-morphism is surjective. Then for every $\Sigma(X)$-model (M,g) there exists a function $\theta : X \to T_F(Y)$ such that $\theta;\overline{h} = g$.

$$\begin{tikzcd} T_F(Y) \arrow[rr, "\overline{h}"] & & M \\ & X \arrow[ul, dotted, "\theta"] \arrow[ur, "g"'] & \end{tikzcd}$$

We straightforwardly extend θ to a signature morphism $\theta' : (S,S^c,F \cup X,P) \to (S,S^c,F \cup Y,P)$ such that θ' is

- equal to θ on X, and
- the identity on (S,S^c,F,P).

Note that for any $x \in X$ we have $((M,h) \restriction_{\theta'})_x = \overline{h}(\theta(x)) = g(x) = (M,g)_x$. Hence, $(M,h) \restriction_{\theta'} = (M,g)$. The cases of **GOSA** and **GPOA** can be treated similarly as **GFOL**.

GPA : For every inclusion $\Sigma \hookrightarrow \Sigma(Z)$ in D, where $\Sigma = (S,S^c,F)$ and $\Sigma(Z) = (S,S^c,F \cup Z)$, the $\Sigma(Z)$-models can be represented as pairs (A,a) where A is a Σ-model and $a : Z' \to A$ is a function such that $Z' \subseteq Z$ is the set of variables which are defined.

Consider a (S,S^c,F)-model M which is D-reachable. Let $T_M \subseteq T_F$ be the maximal subset of terms such that $M \models def(t)$ for all $t \in T_M$. Note that T_M is a partial algebra interpreting each partial operation symbol $\sigma \in F_{s_1 \ldots s_n \to s}$ as follows:

- $(T_M)_\sigma(t_1,\ldots,t_n) = \sigma(t_1,\ldots,t_n)$ if $\sigma(t_1,\ldots,t_n) \in T_M$, and
- $(T_M)_\sigma(t_1,\ldots,t_n)$ is undefined, otherwise,

where $t_i \in (T_M)_{s_i}$ for all $i \in \{1,\ldots,n\}$. We prove that the unique morphism $T_M \to M$ is surjective. Let $m \in M_s$ be an arbitrary element of M. Consider a variable x of sort s and let N be an expansion of M along $\Sigma \hookrightarrow \Sigma(\{x\})$ which interprets the constant symbol x as m. Since M is D-reachable there exists a substitution $\theta : \{x\} \to T_F$ such that $M \restriction_\theta = N$. Take $t = \theta(x)$ and we have $M_t = M_{\theta(x)} = (M \restriction_\theta)_x = N_x = m$.

For the converse implication let $\Sigma = (S,S^c,F)$ be a signature, X and Y two disjoint sets of constants with elements which are different from the symbols in Σ, and M'' a $\Sigma(Y)$-model, with elements which are interpretation of terms, i.e. the unique $\Sigma(Y)$-morphism $h : T_{M''} \to M$ is surjective, where $T_{M''} \subseteq T_{F \cup Y}$ is the maximal algebra of terms such that $M'' \models def(t)$ for all $t \in T_{M''}$. For every $\Sigma(X)$-expansion M' of $M'' \restriction_\Sigma$, where $M' = (M'' \restriction_\Sigma, g)$, $g : X' \to M''$ and $X' \subseteq X$, since h is surjective, there exists a function $\theta : X' \to T_{M''}$ such that $\theta;h = g$.

$$\begin{tikzcd} T_{M''} \arrow[rr, "h"] & & M'' \\ & X' \arrow[ul, dotted, "\theta"] \arrow[ur, "g"'] & \end{tikzcd}$$

We straightforwardly extend θ to a signature morphism $\theta' : (S,S^c,F \cup X) \to (S,S^c,F \cup Y)$ such that

- θ' is the identity on (S,S^c,F),

– it is equal to θ on X', and
– $\theta(x) = \perp$ for all $x \in (X - X')$.

Note that for every

– $x \in X'$ we have: $(M'' \restriction_{\theta'})_x = M''_{\theta'(x)} = M''_{\theta(x)} = h(\theta(x)) = g(x) = M'_x$, and
– $x \in (X - X')$ we have: $(M'' \restriction_{\theta'})_x = M''_{\theta'(x)} = M''_{\perp} = M'_{\perp} = M'_x$.

Hence $M'' \restriction_{\theta} = M'$.

(Q.E.D.)

Remark 8.2.8. *For each set E of atomic sentences in* **GFOL**, **GOSA**, **GPOA**, *and* **GPA**, *the model M_E defining E as basic set of sentences is reachable.*

Definition 8.2.9. *Given an institution $(\mathbb{S}ig, \mathbb{S}en, \mathbb{M}od, \models)$, we say that a signature morphism $\Sigma \xrightarrow{\varphi} \Sigma' \in \mathbb{S}ig$ is finitary if it is finitely presented in the category $\Sigma/\mathbb{S}ig$.*

In concrete institutions, such as **GFOL**, **GPOA**, **GOSA**, and **GPA**, the extension of signatures with finitely numbers of symbols are finitary.

Definition 8.2.10. *Let D^c and D^l be two broad subcategories of signature morphisms. We say that that a Σ-model M is (D^c, D^l)-reachable if for every signature morphism $\chi : \Sigma \to \Sigma'$ in D^c and each χ-expansion M' of M there exists a signature morphism $\varphi : \Sigma \to \Sigma''$ in D^l, a substitution $\theta : \chi \to \varphi$ and a Σ''-model M'' such that $M'' \restriction_{\theta} = M'$.*

The two notions of reachability, apparently different, are closely related.

Proposition 8.2.11. *Let D^c, D^l and D be three broad subcategories of signature morphisms such that $D^c, D^l \subseteq D$. A Σ-model M is (D^c, D^l)-reachable if there exists a signature morphism $\Sigma \xrightarrow{\varphi} \Sigma' \in D$ and a φ-expansion M' of M such that*

1. *M' is D-reachable, and*
2. *either*
   (a) *$\varphi \in D^l$, or*
   (b) *every signature morphism in D^c is finitary and φ is the vertex of a directed co-limit $(\varphi_i \xrightarrow{u_i} \varphi)_{i \in J}$ of a directed diagram $(\varphi_i \xrightarrow{u_{i,j}} \varphi_j)_{(i \leq j) \in (J, \leq)}$ in $\Sigma/\mathbb{S}ig$, and $\varphi_i \in D^l$ for all $i \in J$.*

Proof. The case when $\varphi \in D^l$ is straightforward. We focus on the second condition. Assume a signature morphism $(\chi : \Sigma \to \Sigma_1) \in D^c$ and a χ-expansion N of M. Since M' is D-reachable, there exists a substitution $\theta : \chi \to \varphi$ such that $M' \restriction_{\theta} = N$. Because χ is finitely presented in the category $\Sigma/\mathbb{S}ig$, there exists $i \in J$ and $\theta_i : \chi \to \varphi_i$ such that $\theta_i; u_i = \theta$. Note that $M_i = M' \restriction_{u_i}$ is a φ_i-expansion of M such that $M_i \restriction_{\theta_i} = N$. (Q.E.D.)

The above proposition comes in two variants: infinitary and finitary. The infinitary variant corresponds to the first condition ($\varphi \in D^l$) and is applicable to infinitary institutions, such as **GUFOL**$_\infty$ or **GHCL**$_\infty$ while the finitary variant is applicable to **GFOL**. Throughout this paper we implicitly assume that D represents the broad subcategory of signature morphisms which consists of signature extensions with constants; D^c represents the broad subcategory of signature morphisms which consists of signature extensions with constants of constrained sorts; D^l represents the subcategory of signature morphisms which consists of signature extensions with constants of loose sorts. In the finitary cases, such as **GFOL**, we assume that the signature morphisms in D^c and D^l are finitary.

The following is a corollary of Proposition 8.2.11.

Corollary 8.2.12. *In* **GFOL**, *a Σ-model M, where $\Sigma = (S, S^c, F, P)$, is (D^c, D^l)-reachable iff there exists a set of loose variables Y and a function $f : Y \to M$ such that for every constrained sort $s \in S^c$ the function $\overline{f}_s : (T_F(Y))_s \to M_s$ is surjective, where $\overline{f}$ is the unique extension of f to a (S, F, P)-morphism.*

Proof. The implication from right to left is a direct consequence of Proposition 8.2.11. Let $\Sigma \overset{\varphi}{\hookrightarrow} \Sigma(Y)$ (where $\Sigma = (S, S^c, F, P)$ and $\Sigma = (S, S^c, F \cup Y, P)$) be the vertex of the directed colimit $((\Sigma \overset{\varphi_i}{\hookrightarrow} \Sigma(Y_i)) \overset{u_i}{\hookrightarrow} (\Sigma \overset{\varphi}{\hookrightarrow} \Sigma(Y)))_{Y_i \subseteq Y\, finite}$ of the directed diagram $((\Sigma \overset{\varphi_i}{\hookrightarrow} \Sigma(Y_i)) \overset{u_{i,j}}{\hookrightarrow} (\Sigma \overset{\varphi_j}{\hookrightarrow} \Sigma(Y_j)))_{Y_i \subseteq Y_j \subseteq Y\, finite}$. By Proposition 8.2.11 M is reachable.

For the converse implication we define the set of (loose) variables Y as follows: $Y_s = \emptyset$ for all $s \in S^c$ and Y_s is a renaming of the elements M_s for all $s \in S^l$ such that $Y_s \cap Y_{s'}$ whenever $s \neq s'$. So, there exists a surjective function $f : Y \to M$. We prove that for every constraint sort $s' \in S^c$ and element $m \in M_{s'}$ there exists a term $t \in T_F(Y)$ such that $\overline{f}(t) = m$, where $\overline{f}$ is the unique extension of f to a Σ-morphism. Let $m \in M_{s'}$ with $s' \in S^c$. Let x be a variable and (M, g) be a $\Sigma(\{x\})$-algebra such that $g(x) = m$. By hypothesis there exists a finite set Z of loose variables, a $\Sigma(Z)$-algebra (M, h) and a substitution $\theta : \{x\} \to T_F(Z)$ such that $\theta; \overline{h} = g$, where $\overline{h}$ is the unique extension of h to a Σ-morphism.

$$\begin{tikzcd}
T_F(Z) \arrow[dr, "\overline{h}"] \arrow[dd, hook, "\iota_Z"'] & & \{x\} \arrow[ll, "\theta"'] \arrow[dl, "g"] \\
& M & \\
Z \arrow[ur, "h"] & & T_F(Y) \arrow[ul, "\overline{f}"']
\end{tikzcd}$$

Let $t' = \theta(x)$ and $t = t'(z_1 \leftarrow y_1, \ldots, z_n \leftarrow y_n)$, where $t'(z_1 \leftarrow y_1, \ldots, z_n \leftarrow y_n)$ is the term obtained by substituting the variables y_i for z_i, and $y_i \in f^{-1}(h(z_i))$, for all $i \in \{1, \ldots, n\}$. Note that $\overline{f}(t) = M_{t'}(f(y_1), \ldots, f(y_n)) = M_{t'}(h(z_1), \ldots, h(z_n)) = \overline{h}(t') = \overline{h}(\theta(x)) = g(x) = m$. [2] (Q.E.D.)

Since **GFOL**$_{\omega_1,\omega}$ allows quantification over finite number of variables, we let the subcategories of signature morphisms D, D^c and D^l to be the same as in the case of **GFOL**. Because D, D^c and D are fixed in concrete institutions, we will refer to D-reachable model(s) as ground reachable model(s), and to (D^c, D^l)-reachable model(s) as reachable model(s) [7].

[2] For every term $t \in (T_F(\{z_1 : s_1, \ldots, z_m : s_n\}))_s$ we denote by $M_t : M_{s_1} \times, \ldots, \times M_{s_m} \to M_s$ the derived operation defined by $M_t(m_1, \ldots, m_n) = a^\#(t)$, where $a : \{z_1 : s_1, \ldots, z_m : s_n\} \to M$, $a(z_i) = m_i$ for all $i \in \{1, \ldots, n\}$, and $a^\#$ is the unique extension of a to a morphism.

8.3 Universal Completeness

We provide proof rules for the constructor-based institutions and we prove a completeness result using institution-independent techniques. The results below come both in a finite and an infinite variant, the finite one being obtained by adding (to the hypotheses of the infinite one) all the finiteness hypotheses marked in the brackets.

The *reachable universal weak entailment system* (*RUWES*) developed in this section consists of four layers: the "atomic" layer which in abstract settings is assumed but is developed in concrete examples, the layer of the *weak entailment system with implications* (*IWES*), the layer of the *generic universal weak entailment system* (*GUWES*) and the upmost layer of the RUWES of I. The soundness and the completeness at each layer is obtained relatively to the soundness and completeness of the layer immediately below.

Reachable universal weak entailment systems (RUWES). Let us assume a D^c-universal institution $I = (\mathbb{S}ig, \mathbb{S}en, \mathbb{M}od, \models)$ over $I_2 = (\mathbb{S}ig, \mathbb{S}en_2, \mathbb{M}od, \models)$ such that I_2 has D^l-quantifications for a subcategory $D^l \subseteq \mathbb{S}ig$ of signature morphisms.

We define the following proof rules, for the WES of I.

(*Substitutivity*) $\dfrac{}{(\forall\chi)\rho \vdash_\Sigma (\forall\varphi)\theta(\rho)}$ for all Σ-sentences $(\forall\chi)\rho$ and any substitution $\theta : \chi \to \varphi$.

(*Case splitting*) $\dfrac{\{\Gamma \vdash_\Sigma (\forall\varphi)\theta(\rho) \mid \varphi \in D^l,\ \theta : \chi \to \varphi\}}{\Gamma \vdash_\Sigma (\forall\chi)\rho}$ where Γ is any set of Σ-sentences and $(\forall\chi)\rho$ is a Σ-sentence with $\Sigma \xrightarrow{\chi} \Sigma' \in D^c$ and $\rho \in \mathbb{S}en_2(\Sigma')$.

In **GHCL**, assume a set Γ of Σ-sentences and a Σ-sentence $(\forall x)\rho$ such that x is a constrained variable. In this case, *Case splitting* says that if for any term t formed with loose variables and operation symbols from Σ, we have $\Gamma \vdash (\forall Y)\rho(x \leftarrow t)$, where Y are all (loose) variables which occur in t, then we have proved $\Gamma \vdash (\forall x)\rho$. In most of the cases the set of terms t formed with loose variables and operation symbols from a given signature [3] is infinite which implies that the premises of *Case splitting* are infinite, and thus, the corresponding entailment system is not compact.

Given a compact WES $E_2 = (\mathbb{S}ig, \mathbb{S}en_2, \vdash^2)$ for I_2, the RUWES of I consists of the least WES over E_2 closed under *Substitutivity* and *Case splitting*. This is the finitary version of the RUWES, and is applicable to **GFOL**, $\mathbf{GFOL}_{\omega_1,\omega}$ **GUFOL** and **GHCL**. Note that the resulting entailment system is not compact (even if E_2 is compact) since *Case splitting* is an infinitary rule. The infinitary variant is obtained by dropping the compactness condition, and by considering the infinitary WES for I, and is applicable to $\mathbf{GUFOL}_\infty$ and $\mathbf{GHCL}_\infty$.

Proposition 8.3.1. *The RUWES of I is sound with respect to all (D^c, D^l)-reachable models if the WES of I_2 is sound with respect to all (D^c, D^l)-reachable models.*

Proof. By Proposition 8.2.3 it suffices to prove the soundness of the rules of *Case splitting* and *Substitutivity*.

We prove that *Case splitting* is sound with respect to all (D^c, D^l)-reachable models. Let Γ be a set of Σ-sentences and $(\forall\chi)\rho$ a Σ-sentence, where $\Sigma \xrightarrow{\chi} \Sigma' \in D^c$, and assume that for every (D^c, D^l)-reachable model M we have $M \models (\bigwedge\Gamma \Rightarrow (\forall\varphi)\theta(\rho))$, for all substitutions $\theta : \chi \to \varphi$ with $\varphi \in D^l$. Let M be a (D^c, D^l)-reachable Σ-model such that $M \models \Gamma$ and let M' be an χ-expansion of M. Since M is (D^c, D^l)-reachable there exists a signature morphism $\Sigma \xrightarrow{\varphi} \Sigma'' \in D^l$, a substitution $\theta : \chi \to \varphi$, and an φ-expansion M'' of M such that $M'' \restriction_\theta = M'$. We have $M'' \models \theta(\rho)$ and by the satisfaction condition $M' \models \rho$.

[3] We consider terms modulo renaming variables.

We prove that *Substitutivity* is sound with respect to all models. Let M be a Σ-model such that $M \models (\forall\chi)\rho$. Assume a substitution $\theta : \chi \to \varphi$ such that $(\forall\varphi)\rho \in \mathbb{S}en(\Sigma)$, and let M_2 be any φ-expansion of M. Because $M_2 \restriction_\theta$ is a χ-expansion of M (since $(M_2 \restriction_\theta) \restriction_\chi = M_2 \restriction_\varphi$) which by hypothesis satisfies $(\forall\chi)\rho$, we have that $M_2 \restriction_\theta \models \rho$. By the satisfaction condition, we obtain that $M_2 \models \theta(\rho)$. Since M_2 was an arbitrary expansion of M, we have thus proved $M \models (\forall\varphi)\theta(\rho)$. (Q.E.D.)

Theorem 8.3.2 (Reachable universal completeness)**.** *The RUWES of I is complete with respect to all (D^c, D^l)-reachable models if*

1. *the WES of I_2 is complete with respect to all (D^c, D^l)-reachable models (and compact), and*

2. *for each set of sentences $E \subseteq \mathbb{S}en_2(\Sigma)$ and each sentence $e \in \mathbb{S}en_2(\Sigma)$, we have $E \models e$ iff $M \models (\bigwedge E \Rightarrow e)$ for all (D^c, D^l)-reachable models M.*

Proof. Assume that for all (D^c, D^l)-reachable models M we have $M \models (\bigwedge \Gamma \Rightarrow (\forall\chi)e')$, where $\Sigma \xrightarrow{\chi} \Sigma' \in D^c$. We want $\Gamma \vdash (\forall\chi)e'$. Suppose towards a contradiction that $\Gamma \nvdash (\forall\chi)e'$. Then there exists a signature morphism $\Sigma \xrightarrow{\varphi} \Sigma''$ in D^l and a substitution $\theta : \chi \to \varphi$ such that $\Gamma \nvdash (\forall\varphi)\theta(e')$.

We define the set of Σ-sentences $\Gamma_2 = \{\rho \in \mathbb{S}en_2(\Sigma) \mid \Gamma \vdash \rho\}$.

We show that $\Gamma_2 \nvdash^2 (\forall\varphi)\theta(e')$. Assume that $\Gamma_2 \vdash^2 (\forall\varphi)\theta(e')$. For the infinitary case take $\Gamma' = \Gamma_2$. For the finitary case, since the WES of I_2 is compact, there exists a finite $\Gamma' \subseteq \Gamma_2$ such that $\Gamma' \vdash^2 (\forall\varphi)\theta(e')$ which implies $\Gamma' \vdash (\forall\varphi)\theta(e')$. Since $\Gamma \vdash \rho$ for all $\rho \in \Gamma'$ we have $\Gamma \vdash \Gamma'$. Hence, $\Gamma \vdash (\forall\varphi)\theta(e')$ which is a contradiction with our assumption.

We have $\Gamma_2 \nvdash^2 (\forall\varphi)\theta(e')$, and by completeness of I_2 we obtain $\Gamma_2 \not\models (\forall\varphi)\theta(e')$. There exists a (D^c, D^l)-reachable model such that $M \models \Gamma_2$ and $M \not\models (\forall\varphi)\theta(e')$. Note that $M \not\models (\forall\varphi)\theta(e')$ implies $M \not\models (\forall\chi)e'$. If we have proved that $M \models \Gamma$ we have reached a contradiction with $A \models (\bigwedge \Gamma \Rightarrow (\forall\chi)e')$ for all (D^c, D^l)-reachable models A.

Let $(\forall\chi_1)e_1 \in \Gamma$, where $\Sigma \xrightarrow{\chi_1} \Sigma_1 \in D^c$, and let N be any χ_1-expansion of M. Since M is (D^c, D^l)-reachable there exists a signature morphism $\Sigma \xrightarrow{\varphi_1} \Sigma_1'$ in D^l, a substitution $\psi : \chi_1 \to \varphi_1$, and a φ_1-expansion N' of M such that $N' \restriction_\theta = N$. By *Substitutivity* $(\forall\varphi_1)\psi(e_1) \in \Gamma_2$ which implies $M \models (\forall\varphi_1)\psi(e_1)$. Since N' is φ_1-expansion of M we have $N' \models \psi(e_1)$ and by satisfaction condition $N' \restriction_\psi = N \models e_1$. (Q.E.D.)

Generic universal weak entailment systems (GUWES). Let us assume a D^l-universal institution $I = (\mathbb{S}ig, \mathbb{S}en, \mathbb{M}od, \models)$ over I_1 with $\mathbb{S}en_1$ the sub-functor of $\mathbb{S}en$.

Given a compact WES $E_1 = (\mathbb{S}ig, \mathbb{S}en_1, \vdash^1)$ for I_1, the GUWES of I consists of the least WES with universal quantifications over E_1, closed under *Substitutivity*. This is the finitary version of the GUWES, and is applicable to the restriction of **GHCL** to the sentences quantified over finite sets of variables of loose sorts. Its infinitary variant is obtained by dropping the compactness condition, and by considering the infinitary WES of I; it is applicable to the restriction of $\mathbf{GHCL}_\infty$ to the sentences quantified over sets (possible infinite) of variables of loose sorts.

Proposition 8.3.3. *The GUWES of I is sound (and compact) whenever the WES of I_1 is sound (and compact).*

Proof. By Proposition 8.2.3 and Corollary 3.3.11 it is suffices to prove the soundness of *Substitutivity* which may be found in the proof of Proposition 8.3.1.

For the compactness of the GUWES of I consider the compact sub-WES $E^c = (\mathbb{S}ig, Sen, \vdash^c)$ of $E = (\mathbb{S}ig, \mathbb{S}en, \vdash)$. It contains E_1 because E_1 is compact. Note that E^c satisfies *Substitutivity* because the rules of *Substitutivity* are finitely generated. If we prove that E^c satisfies *Generalization* then because E is the least WES over E_1 satisfying the rules of *Substitutivity* and *Generalization* we obtain $E^c = E$.

If $\Gamma \vdash^c (\forall\varphi)e'$ then there exists $\Gamma' \subseteq \Gamma$ finite such that $\Gamma' \vdash (\forall\varphi)e'$. By *Generalization* $\varphi(\Gamma') \vdash e'$ which means $\varphi(\Gamma) \vdash^c e'$. Now if $\varphi(\Gamma) \vdash^c e'$ then there is $\Gamma' \subseteq \Gamma$ finite such that $\varphi(\Gamma') \vdash e'$. Using the *Generalization* again we get $\Gamma' \vdash (\forall\varphi)e'$ which means $\Gamma \vdash^c (\forall\varphi)e'$. (Q.E.D.)

Theorem 8.3.4 (Generic universal completeness)**.** *Let D be a broad subcategory of signature morphisms such that $D^l \subseteq D$. Assume that*

1. *the WES of I_1 is complete, and*
2. *for each set of sentences $E \subseteq \mathbb{S}en_1(\Sigma)$ and each sentence $e \in \mathbb{S}en_1(\Sigma)$, we have $E \models_\Sigma e$ iff $M \models_\Sigma (\bigwedge E \Rightarrow e)$ for all D-reachable models M.*

Then we have

1. *the GUWES of I is complete (and compact), and*
2. *$\Gamma \models_\Sigma (\forall\varphi)e'$, where $\Sigma \xrightarrow{\varphi} \Sigma' \in D^l$, iff $M \models_{\Sigma'} (\bigwedge \varphi(\Gamma) \Rightarrow e')$ for all D-reachable models M.*

Proof. 1. Assume that $\Gamma \models_\Sigma (\forall\varphi)e'$ where $\Sigma \xrightarrow{\varphi} \Sigma' \in D$. We want $\Gamma \vdash_\Sigma (\forall\varphi)e'$. Suppose towards a contradiction that $\Gamma \not\vdash_\Sigma (\forall\varphi)e'$.

We define the set of Σ'-sentences $\Gamma_1^\varphi = \{\rho' \in \mathbb{S}en_1(\Sigma') | \Gamma \vdash_\Sigma (\forall\varphi)\rho'\}$.

Suppose $\Gamma_1^\varphi \vdash^1_{\Sigma'} e'$. For the infinitary case we take $\Gamma' = \Gamma_1^\varphi$. For the finitary case, since the WES of I_1 is compact, there exists a finite $\Gamma' \subseteq \Gamma_1^\varphi$ such that $\Gamma' \vdash^1 e'$. By *Generalization* $\varphi(\Gamma) \vdash_{\Sigma'} \rho'$ for all $\rho' \in \Gamma'$, which implies $\varphi(\Gamma) \vdash_{\Sigma'} \Gamma'$. Since $\Gamma_1^\varphi \vdash^1_{\Sigma'} e'$ implies $\Gamma_1^\varphi \vdash_{\Sigma'} e'$, we obtain $\varphi(\Gamma) \vdash_{\Sigma'} e'$ and again by *Generalization* $\Gamma \vdash_\Sigma (\forall\varphi)e'$, which contradicts our assumption. Hence, $\Gamma_1^\varphi \not\vdash^1_{\Sigma'} e'$.

By completeness of I_1 $\Gamma_1^\varphi \not\models e'$. There exists a D-reachable model M such that $M \models \Gamma_1^\varphi$ but $M \not\models e'$. This implies $M \restriction_\varphi \not\models (\forall\varphi)e'$. If we proved that $M \restriction_\varphi \models \Gamma$ we reached a contradiction with $\Gamma \models (\forall\varphi)e'$. We will therefore focus on proving that $M \restriction_\varphi \models \Gamma$.

Let $(\forall\varphi_1)e_1 \in \Gamma$, where $\Sigma \xrightarrow{\varphi_1} \Sigma_1 \in D$, and let N be any φ_1-expansion of $M \restriction_\varphi$. We show that $N \models e_1$. Since M is D-reachable there exists a substitution $\theta : \varphi_1 \to \varphi$ such that $M \restriction_\theta = N$. By *Substitutivity* we obtain $\Gamma \vdash (\forall\varphi)\theta(e_1)$ which implies $\theta(e_1) \in \Gamma_1^\varphi$. Since $M \models \Gamma_1^\varphi$ we have $M \models \theta(\rho)$ and by the satisfaction condition $M \restriction_\theta = N \models e_1$.

2. The non-trivial implication is from right to left. Assume that $\Gamma \not\models_\Sigma (\forall\varphi)e'$, where $\Sigma \xrightarrow{\varphi} \Sigma' \in D^l$, then by soundness of the WES of I we have $\Gamma \nvdash (\forall\varphi)e'$. Using the first part of the proof we get a D-reachable Σ'-model M such that $M \models \varphi(\Gamma)$ and $M \not\models e'$. Therefore there exists a D-reachable model M such that $M \not\models (\bigwedge \varphi(\Gamma) \Rightarrow e')$.

(Q.E.D.)

The following remark addresses the second condition of Theorem 8.3.2.

Remark 8.3.5. *Under the assumption of Theorem 8.3.4, for any subcategory $D^c \subseteq D$ of signature morphisms, we have $\Gamma \models_\Sigma (\forall\varphi)e'$ iff $M \models_\Sigma (\bigwedge\Gamma \Rightarrow (\forall\varphi)e')$ for all (D^c, D^I)-reachable models M.*

Weak entailment systems with implications (IWES). Assume an institution $I = (\mathbb{S}ig, \mathbb{S}en, \mathbb{M}od, \models)$, a sub-functor $\mathbb{S}en_0 : \mathbb{S}ig \to \mathbb{S}et$ of $\mathbb{S}en$ such that

- $(\bigwedge H \Rightarrow C) \in \mathbb{S}en(\Sigma)$, for all (finite) sets of sentences $H \subseteq \mathbb{S}en_0(\Sigma)$ and any sentence $C \in \mathbb{S}en_0(\Sigma)$, and
- any sentence in I is of the form $(\bigwedge H \Rightarrow C)$ as above.

We denote the institution $(\mathbb{S}ig, \mathbb{S}en_0, \mathbb{M}od, \models)$ by I_0.

Given a compact WES $E_0 = (\mathbb{S}ig, \mathbb{S}en_0, \vdash^0)$ for I_0, the IWES of I consists of the least WES over E_0, closed under the rules of *Implications*. This is the finitary version of the IWES for I, and is applicable to the restriction of **GHCL** to the quantifier-free sentences. Its infinitary variant is obtained by dropping the compactness condition and by considering the infinitary WES for I; it is applicable to the restriction of $\mathbf{GHCL}_\infty$ to the quantifier-free sentences.

Proposition 8.3.6. *The WES of I is sound (and compact) whenever the WES of I_0 is sound (and compact).*

Proof. The soundness of the WES of I_0 is lifted to the soundness of I using Corollary 3.3.9.

In the finitary case the WES of I_0 is compact. By Proposition 3.3.8 the IWES of I is compact. (Q.E.D.)

Theorem 8.3.7. *Let us assume that*

1. *the WES of I_0 is complete,*
2. *every set of sentences in I_0 is basic, and*
3. *there exits a broad subcategory $D \subseteq \mathbb{S}ig$ such that for each set $B \subseteq \mathbb{S}en_0(\Sigma)$ there is a D-reachable model M_B defining B as basic set of sentences.*

Then we have

1. *the IWES of I is sound, complete (and compact), and*
2. *$\Gamma \models \rho$ iff $M \models (\bigwedge\Gamma \Rightarrow \rho)$ for all D-reachable models M.*

Proof. 1. Because the entailment system of I has *Implications* it is enough to prove that

$$\Gamma \models \rho \text{ implies } \Gamma \vdash \rho$$

for each $\Gamma \subseteq \mathbb{S}en_1(\Sigma)$ and each $\rho \in \mathbb{S}en_0(\Sigma)$. Let M_{Γ_0} be the model defining the set of sentences $\Gamma_0 = \{e \in \mathbb{S}en_0(\Gamma) | \Gamma \vdash e\}$ as basic. We use the following couple of lemmas.

Lemma 8.3.8. *$M_{\Gamma_0} \models e$ iff $\Gamma \vdash e$ for all sentences $e \in \mathbb{S}en_0(\Sigma)$.*

Lemma 8.3.9. *$M_{\Gamma_0} \models \Gamma$.*

If $\Gamma \models \rho$ then by Lemma 8.3.9 we have that $M_{\Gamma_0} \models \rho$. Now by Lemma 8.3.8 we obtain $\Gamma \vdash \rho$. By Proposition 3.3.8 the WES of I is compact.

Lemma 8.3.8. The implication from right to left holds by the definition of Γ_0. For the other implication let us consider a sentence e such that $M_{\Gamma_0} \models e$. For any model M such that $M \models \Gamma_0$, because Γ_0 is basic there exists a model homomorphism $M_{\Gamma_0} \to M$. Since $M_{\Gamma_0} \models e$ and e is basic, there exists another model homomorphism $M_e \to M_{\Gamma_0}$. These give a model homomorphism $M_e \to M$ which means $M \models e$. We have thus shown that $\Gamma_0 \models e$.

By the completeness of I_0 we obtain that $\Gamma_0 \vdash e$. For the infinitary case let us take $\Gamma'_0 = \Gamma_0$. For the finitary case, since the WES of I_0 is compact, there exists $\Gamma'_0 \subseteq \Gamma_0$ finite such that $\Gamma'_0 \vdash e$. By the definition of Γ_0 we obtain that $\Gamma \vdash \Gamma'_0$ hence $\Gamma \vdash e$. (Q.E.D.)

Lemma 8.3.9. Let us consider that we have a I-sentence $\bigwedge H \Rightarrow C \in \Gamma$ and let us assume that $M_{\Gamma_0} \models H$. By Lemma 8.3.8 we have that $\Gamma \models H$ and because $\bigwedge H \Rightarrow C \in \Gamma$ and the WES of I has *Implications* we obtain that $\Gamma \vdash C$. By Lemma 8.3.8 again we deduce $M_{\Gamma_0} \models C$. (Q.E.D.)

2. Let $\rho = (\bigwedge H \Rightarrow C)$ with $H \subseteq \mathbb{S}en_0(\Sigma)$ and $C \in \mathbb{S}en_0(\Sigma)$. Consider the model $M_{(\Gamma \cup H)_0}$ defining $(\Gamma \cup H)_0 = \{e \in \mathbb{S}en_0(\Sigma) | \Gamma \cup H \models e\}$ as basic set of sentences. By Lemma 8.3.9 we have that $M_{(\Gamma \cup H)_0} \models \Gamma \cup H$. By the hypothesis this implies $M_{(\Gamma \cup H)_0} \models \bigwedge H \Rightarrow C$. Because $M_{(\Gamma \cup H)_0} \models H$ too, it follows that $M_{(\Gamma \cup H)_0} \models C$. Since C is basic there exists a homomorphism $M_C \to M_{(E \cup H)_0}$.

   Now let M be any model such that $M \models \Gamma \cup H$. By Lemma 8.3.8 we obtain that $M \models (\Gamma \cup H)_0$. Because $(\Gamma \cup H)_0$ is basic, there exists a homomorphism $M_{(\Gamma \cup H)_0} \to M$. We obtain thus a homomorphism $M_C \to M$, which means $M \models C$.

   (Q.E.D.)

The following is a consequence of Theorems 8.3.2, 8.3.4 and 8.3.7.

Theorem 8.3.10. *Consider an institution $I = (\mathbb{S}ig, \mathbb{S}en, \mathbb{M}od, \models)$ with three broad subcategories D, D^c and D^l of signatures morphisms, where $D^c \subseteq D$ and $D^l \subseteq D$, and a sub-functor $\mathbb{S}en_0$ of $\mathbb{S}en$ ($I_0 = (\mathbb{S}ig, \mathbb{S}en_0, \mathbb{M}od, \models)$) such that*

- *$(\forall\chi)(\forall\varphi)(\bigwedge H \Rightarrow C) \in \mathbb{S}en(\Sigma)$ for all signature morphisms $\Sigma \xrightarrow{\chi} \Sigma' \in D^c$, $\Sigma' \xrightarrow{\varphi} \Sigma'' \in D^l$, all (finite) sets $H \subseteq \mathbb{S}en_0(\Sigma'')$ and any sentence $C \in \mathbb{S}en_0(\Sigma'')$, and*
- *all sentences are of the form $(\forall\chi)(\forall\varphi) \bigwedge H \Rightarrow C$ as in the item above.*

If $E_0 = (\mathbb{S}ig, \mathbb{S}en_0, \vdash^0)$ is a WES for I_0 then the free WES of I over E_0 with Implications *and universal quantifications, and satisfying* Case splitting *and* Substitutivity *is sound and complete with respect to all (D^c, D^l)-reachable models whenever*

1. *the WES of I_0 is sound, complete (and compact),*
2. *every set of sentences in I_0 is basic, and*
3. *for each set $B \subseteq \mathbb{S}en_0(\Sigma)$ there is a D-reachable model M_B defining B as basic set of sentences.*

Atomic weak entailment systems (AWES). In order to develop concrete sound and complete universal WES we need to define sound and complete WES for the "atomic" layer of the institutions.

GFOL :

Proposition 8.3.11. *Let* **GHCL**$_0$ *be the restriction of* **GHCL** *to the atomic sentences. The WES of* **GHCL**$_0$ *generated by the rules bellow is sound, complete and compact.*
$(Reflexivity)$ $\emptyset \vdash t = t$, *where* t *is a term.*
$(Symmetry)$ $t = t' \vdash t' = t$, *where* t, t' *are terms.*
$(Transitivity)$ $\{t = t', t' = t''\} \vdash t = t''$, *where* t, t', t'' *are terms.*
$(Congruence)$ $\{t_i = t'_i | 1 \leq i \leq n\} \vdash \sigma(t_1, ..., t_n) = \sigma(t'_1, ..., t'_n)$, *where* $t_i, t'_i \in T_F$ *are terms and* σ *is an operation symbol.*
$(PCongruence)$ $\{t_i = t'_i | 1 \leq i \leq n\} \cup \{\pi(t_1, ..., t_n)\} \vdash \pi(t'_1, ..., t'_n)$, *where* t_i, t'_i *are terms and* π *is a predicate symbol.*

Proof. Soundness follows by simple routine check and compactness by applying Proposition 3.2.6 after noting that all the rules are finitely generated. For proving the completeness, for any set E of atoms for a signature (S, F, P) we define

$$\equiv_E = \{(t, t') | E \vdash t = t'\}$$

By *Reflexivity*, *Symmetry*, *Transitivity* and *Congruence* this is a congruence on T_F. Then we define a model M_E as follows:

- the (S, F)-algebra part of M_E is defined as the quotient of the initial algebra (term algebra) T_F by $\equiv_E$, and
- for each relation symbol $\pi \in P$, we define $(M_E)_\pi = \{x/_{\equiv_E} | E \vdash \pi(x)\}$

The definition of $(M_E)_\pi$ is correct because of the rule *PCongruence*. Now we note that for each (S, F, P)-atom ρ we have $E \vdash \rho$ iff $M_E \models \rho$. Now if $E \models \rho$ then $M_E \models \rho$ which means $E \vdash \rho$. (Q.E.D.)

GOSA:

Definition 8.3.12. *A congruence relation* $\equiv$ *on a* $(S, \leq, F)$*-model* M *is a* (S, F)*-congruence relation* $\equiv = (\equiv_s)_{s \in S}$ *such that if* $s \leq s'$ *in* $(S, \leq)$ *and* $a, a' \in M_s$ *then* $a \equiv_s a'$ *iff* $a \equiv_{s'} a'$.

Proposition 8.3.13. *Let* **GOSA**$_0$ *be the restriction of* **GOSA** *to the atomic sentences. The WES of* **GOSA**$_0$ *generated by the rules bellow is sound, complete and compact.*
$(Reflexivity)$ $\emptyset \vdash t = t$, *where* t *is a term.*
$(Symmetry)$ $t = t' \vdash t' = t$, *where* t, t' *are terms.*
$(Transitivity)$ $\{t = t', t' = t''\} \vdash t = t''$, *where* t, t', t'' *are terms.*
$(Congruence)$ $\{t_i = t'_i | 1 \leq i \leq n\} \vdash \sigma(t_1, ..., t_n) = \sigma(t'_1, ..., t'_n)$, *where* $t_i, t'_i \in T_F$ *are terms and* σ *is an operation symbol.*

Proof. Soundness follows by simple routine check and compactness by applying Proposition 3.2.6 after noting that all the rules are finitely generated. For proving the completeness, for any set E of equations for a signature $(S, \leq, F)$ we define

$$\equiv_E = \{(t, t') | E \vdash t = t'\}$$

Since the signature $(S,\leq,F)$ is regular the term algebra T_F is the initial $(S,\leq,F)$-algebra in $\mathbb{M}od(S,\leq,F)$. By (*Reflexivity*), (*Symmetry*), (*Transitivity*) and (*Congruence*) this is an F-congruence on T_F. $\equiv_E$ is also an order-sorted congruence on T_F, because the definition of $\equiv_E$ does not depend upon a sort. Since the signature $(S,\leq,F)$ is locally filtered we may define a model M_E as the quotient of the initial algebra (term algebra) T_F by order-sorted congruence $\equiv_E$.

Notice that for each $(S,\leq,F)$-equation $t=t'$, $E\vdash t=t'$ iff $M_E\models t=t'$. Now if $E\models t=t'$ then $M_E\models t=t'$ which means $E\vdash t=t'$. (Q.E.D.)

GPOA:

Definition 8.3.14. *A (preorder) congruence relation on a (S,F)-preorder algebra M is a pair $(\equiv,\sqsubseteq)$ where $\equiv$ is a (S,F)-congruence relation and $\sqsubseteq$ is a preorder on M which*

- *preserve the preorder structure of M, i.e. $m\leq m'$ implies $m\sqsubseteq m'$ for all elements $m,m'\in M$,*
- *is compatible with operations in F, i.e. $m\leq m'$ implies $M_\sigma(m)\leq M_\sigma(m')$ for all operations $\sigma\in F_{w,s}$ and all elements $m,m'\in M_w$, and*
- *is compatible with the congruence $\equiv$, i.e. $m_1\equiv m_2$, $m_2\sqsubseteq m_3$ and $m_3\equiv m_4$ implies $m_1\sqsubseteq m_4$ for all elements $m_1,m_2,m_3,m_4\in M$.*

Proposition 8.3.15. *Let* **GPOA**$_0$ *be the restriction of* **GPOA** *to the atomic sentences. The WES of* **GPOA**$_0$ *generated by the rules bellow is sound, complete and compact.*
$(Reflexivity)$ $\emptyset\vdash t=t$ *for each term* t
$(Symmetry)$ $t=t'\vdash t'=t$ *for any terms* t,t'
$(Transitivity)$ $\{t=t',t'=t''\}\vdash t=t''$ *for any terms* t,t',t''
$(Congruence)$ $\{t_i=t_i'|1\leq i\leq n\}\vdash\sigma(t_1,...,t_n)=\sigma(t_1',...,t_n')$ *for any* $\sigma\in F$
$(Reflexivity')\emptyset\vdash t\leq t$ *for each term* t
$(Transitivity')\{t\leq t',t'\leq t''\}\vdash t\leq t''$ *for any terms* t,t',t''
$(Congruence')\{t_i\leq t_i'|1\leq i\leq n\}\vdash\sigma(t_1,...,t_n)\leq\sigma(t_1',...,t_n')$ *for any* $\sigma\in F$
(ET) $\{t_1=t_2,\ t_2\leq t_3,\ t_3=t_4\}\vdash t_1\leq t_4$ *for any terms* t_1,t_2,t_3,t_4

Proof. Soundness follows by simple routine check and compactness by applying Proposition 3.2.6 after noting that all the rules are finitely generated. For proving the completeness, for any set E of atoms for a signature (S,P) we define the congruence $(\equiv_E,\sqsubseteq_E)$

- $\equiv_E=\{(t,t')\mid E\vdash t=t'\}$
- $\sqsubseteq_E=\{(t,t')\mid E\vdash t\leq t'\}$

By the above rules of **GPOA**$_0$ the pair $(\equiv_E,\sqsubseteq_E)$ is a preorder congruence on the term algebra T_F. Then we define the preorder algebra M_E as the quotient of the term algebra by $(\equiv_E,\sqsubseteq_E)$. We note that for each equational or transitional (S,F)-atom ρ

$$E\vdash\rho \text{ if and only if } M_E\models\rho$$

Now if $E\models\rho$ then $M_E\models\rho$ which means $E\vdash\rho$. (Q.E.D.)

GPA:

Definition 8.3.16. *A congruence relation $\equiv$ on a (S,F)-model M is a S-sorted equivalence relation $\equiv = (\equiv_s)_{s\in S}$ such that for every operation symbol $\sigma \in F$ and elements m, $m' \in M$ with $m \equiv m'$ if both $M_\sigma(m)$ and $M_\sigma(m')$ are defined then $M_\sigma(m) \equiv M_\sigma(m')$.*

Proposition 8.3.17. *Let* $\mathbf{GPA}_0$ *be the restriction of* **GPA** *to the atomic sentences. The WES of* $\mathbf{GPA}_0$ *generated by the rules bellow is sound, complete and compact.*
(Symmetry) $t \stackrel{e}{=} t' \vdash t' \stackrel{e}{=} t$ *for any terms* t, t'
(Transitivity) $\{t \stackrel{e}{=} t',\ t' \stackrel{e}{=} t''\} \vdash t \stackrel{e}{=} t''$ *for any terms* t, t', t''
(Congruence) $\{t_i \stackrel{e}{=} t'_i,\ def(\sigma(t_1,\ldots,t_n)),\ def(\sigma(t'_1,\ldots,t'_n))\} \vdash$
$\sigma(t_1,\ldots,t_n) \stackrel{e}{=} \sigma(t'_1,\ldots,t'_n)$ *for any* $\sigma \in F$
(Subterm) $def(\sigma(t_1,\ldots,t_n)) \vdash \{def(t_i) \mid i \in \overline{1,n}\}$ *for any* $\sigma \in F$

Proof. Soundness follows by simple routine check and compactness by applying Proposition 3.2.6 after noting that all the rules are finitely generated. For proving the completeness, for any set E of atoms for a signature (S, TF, PF) we define

$$\equiv_E = \{(t,t') | E \vdash t \stackrel{e}{=} t'\}$$

Note that For every set of existence equations $E \subseteq \mathbb{S}en(S,F)$ we have that $E \vdash def(t)$ if and only if $t \in T_E$, where T_E is the partial algebra having the carrier the set of all sub-terms appearing in E.

Firstly we prove that $\equiv_E$ is a congruence relation on T_E. The reflexivity of $\equiv_E$ is given by the above remark. The first two rules ensure the symmetry and the transitivity of $\equiv_E$. By the rule (C) we have that $\equiv_E$ is a congruence relation on T_E.

For each existence equation $t \stackrel{e}{=} t'$ we have $E \vdash t \stackrel{e}{=} t' \iff t \equiv_E t' \iff T_E/_{\equiv_E} \models t \stackrel{e}{=} t'$. If $E \models t \stackrel{e}{=} t'$ then $T_E/_{\equiv_E} \models t \stackrel{e}{=} t'$ which implies $E \vdash t \stackrel{e}{=} t'$. (Q.E.D.)

The following is a corollary of Theorem 8.3.10.

Corollary 8.3.18. *[Completeness of the* **GHCL***] The RUWES of* **GHCL** *generated by the rules of* Case splitting, Substitutivity, Generalization, Implications, Reflexivity, Symmetry, Transitivity, Congruence *and* PCongruence *is sound and complete with respect to all reachable models.*

Similar completeness results hold for **GHOSA**, **GHPOA**, **GHPA** and also their infinitary variants $\mathbf{GHCL}_\infty$, $\mathbf{GHOSA}_\infty$, $\mathbf{GHPOA}_\infty$, $\mathbf{GHPA}_\infty$.

8.4 Borrowing Completeness

Let $I' = (\mathbb{S}ig', \mathbb{S}en', \mathbb{M}od', \models')$ and $I = (\mathbb{S}ig, \mathbb{S}en, \mathbb{M}od, \models)$ be two institutions. An *institution morphism* $(\phi, \alpha, \beta) : I' \to I$ consists of

- a functor $\phi : \mathbb{S}ig' \to \mathbb{S}ig$, and
- two natural transformations $\alpha : \phi;\mathbb{S}en \Rightarrow \mathbb{S}en'$ and $\beta : \mathbb{M}od' \Rightarrow \phi^{op};\mathbb{M}od$ such that the following satisfaction condition for institution morphisms holds:

$$M' \models'_{\Sigma'} \alpha_{\Sigma'}(e) \text{ iff } \beta_{\Sigma'}(M') \models_{\phi(\Sigma')} e$$

for every signature $\Sigma' \in \mathbb{S}ig'$, each Σ'-model M', and any $\phi(\Sigma')$-sentence e.

Definition 8.4.1. *We say that a WES $E = (\mathbb{S}ig, \mathbb{S}en, \vdash)$ of an institution $I = (\mathbb{S}ig, Sen, \mathbb{M}od, \models)$ is Ω-complete, where $\Omega = (\Omega_\Sigma)_{\Sigma \in |\mathbb{S}ig|}$ is a family of sets of sentences ($\Omega_\Sigma \subseteq P(\mathbb{S}en(\Sigma))$ for all signatures Σ) iff $\Gamma \models_\Sigma e$ implies $\Gamma \vdash_\Sigma e$ for all $\Gamma \in \Omega_\Sigma$ and $e \in \mathbb{S}en(\Sigma)$.*

Remark 8.4.2. *Let $(\phi, \alpha, \beta) : I' \to I$ be an institution morphism, where $I = (\mathbb{S}ig, \mathbb{S}en, \mathbb{M}od, \models)$ and $I' = (\mathbb{S}ig', \mathbb{S}en', \mathbb{M}od', \models')$. Every WES $E = (\mathbb{S}ig, \mathbb{S}en, \vdash)$ for I generates freely a WES $E' = (\mathbb{S}ig', \mathbb{S}en', \vdash')$ for I', where E' is the least WES closed under the rules $\dfrac{}{\alpha_{\Sigma'}(\Gamma) \vdash'_{\Sigma'} \alpha_{\Sigma'}(E)}$, where $\Gamma \vdash_{\phi(\Sigma')} E$ is a deduction in E.*

Theorem 8.4.3. *Consider*

1. *an institution morphism $(\phi, \alpha, \beta) : I' \to I$ (where $I' = (\mathbb{S}ig', \mathbb{S}en', \mathbb{M}od', \models')$ and $I = (\mathbb{S}ig, \mathbb{S}en, \mathbb{M}od, \models)$) such that $\alpha_{\Sigma'}$ is surjective for all $\Sigma' \in |\mathbb{S}ig'|$,*
2. *a class of models $M = (M_\Sigma)_{\Sigma \in |\mathbb{S}ig|}$ (in I) such that $\beta_{\Sigma'}(|\mathbb{M}od'(\Sigma')|) \subseteq M_{\phi(\Sigma')}$ for all signatures $\Sigma' \in |\mathbb{S}ig|$, and*
3. *a WES $E = (\mathbb{S}ig, \mathbb{S}en, \vdash)$ for I which is sound and complete with respect to M.*

Then the entailment system $E' = (\mathbb{S}ig', \mathbb{S}en', \vdash')$ of I' determined by E is

1. *sound, and*
2. *Ω-complete*

where for every signature $\Sigma' \in |\mathbb{S}ig'|$ we have $\Gamma' \in \Omega_{\Sigma'}$ iff $\Gamma = \alpha^{-1}_{\Sigma'}(\Gamma')$ has the following property: $M \models_{\phi(\Sigma')} \Gamma$ implies $M \in \beta_{\Sigma'}(|\mathbb{M}od'(\Sigma')|)$, for any $M \in M_{\phi(\Sigma')}$.

Proof. Since $\alpha_{\Sigma'}$ is surjective, for all signatures $\Sigma' \in |\mathbb{S}ig'|$, $E' = (\mathbb{S}ig', \mathbb{S}en', \vdash')$ with $\vdash'_{\Sigma'} = \alpha_{\Sigma'}(\vdash_{\phi(\Sigma')})$, for all signatures $\Sigma' \in |\mathbb{S}ig'|$, is the WES of I' determined by the institution morphism (ϕ, α, β).

1. Suppose that $\Gamma' \vdash'_{\Sigma'} E'$ and let M' be a Σ'-model such that $M' \models' \Gamma'$. By the definition of E' there exists $\Gamma \vdash_{\phi(\Sigma')} E$ such that $\alpha_{\Sigma'}(\Gamma) = \Gamma'$ and $\alpha_{\Sigma'}(E) = E'$. By the satisfaction condition for the institution morphisms we have $\beta_{\Sigma'}(M') \models_{\phi(\Sigma')} \Gamma$. Since E is sound with respect to M we have $M \models_{\phi(\Sigma')} (\Gamma \Rightarrow E)$ for all models $M \in M_{\phi(\Sigma')}$. Because $\beta_{\Sigma'}(M') \in M_{\phi(\Sigma')}$ we have that $\beta_{\Sigma'}(M') \models_{\phi(\Sigma')} (\Gamma \Rightarrow E)$ which implies $\beta_{\Sigma'}(M') \models_{\phi(\Sigma')} E$. By the satisfaction condition for institution morphisms we get $M' \models'_{\Sigma'} \alpha_{\Sigma'}(E)$. Hence $M' \models'_{\Sigma'} E'$.

2. Assume $\Gamma' \models_{\Sigma'} E'$, where $\Gamma' \in \Omega$, and let $\Gamma = \alpha^{-1}_{\Sigma'}(\Gamma')$ and $E = \alpha^{-1}_{\Sigma'}(E')$. Note that $M \models (\Gamma \Rightarrow E)$ for all $M \in M_\Sigma$. Indeed for any $M \in M_\Sigma$ we have: $M \models_{\phi(\Sigma')} \Gamma$ implies $M \in \beta_{\Sigma'}(|\mathbb{M}od'(\Sigma')|)$; so, there exists a Σ'-model M' such that $\beta_{\Sigma'}(M') = M$ and by satisfaction condition for institution morphisms $M' \models' \Gamma'$ which implies $M' \models' E'$; applying again satisfaction condition we obtain $M \models E$. Since I is complete with respect to M we have $\Gamma \vdash E$ which implies $\Gamma' \vdash' E'$. (Q.E.D.)

In order to develop sound and complete WES for the constructor-based institutions we need to set the parameters of Theorem 8.4.3. We define the institution morphism $\Delta_{\mathbf{HCL}} = (\phi, \alpha, \beta) : \mathbf{CHCL} \to \mathbf{GHCL}$ such that

1. the functor ϕ maps

   - every **CHCL** signature (S, F, F^c, P) to a **GHCL** signature (S, S^c, F, P), where S^c is the set of constrained sorts determined by F^c, and

   - every **CHCL** signature morphism $(\varphi^{sort}, \varphi^{op}, \varphi^{pred})$ to the **GHCL** signature morphism $(\varphi^{sort}, \varphi^{op}, \varphi^{pred})$;

2. α is the identity natural transformation (recall that $\mathbb{S}en(S,F,F^c,P) = \mathbb{S}en(S,S^c,F,P)$, where S^c is a the set of constrained sorts determined by the constructors in F^c), for every **CHCL** signature (S,F,F^c,P) we have $\alpha_{(S,F,F^c,P)} = 1_{\mathbb{S}en(S,F,F^c,P)}$;

3. β is the inclusion natural transformation (note that every (S,F,F^c,P)-model M is also a (S,S^c,F,P)-model; indeed if there exists a set of loose variables Y and a function $f : Y \to M$ such that for every constrained sort $s \in S^c$ the function $f^\#_s : (T_{F^c}(Y))_s \to M_s$ is a surjection, where $f^\#$ is the unique extension of f to a (S,F^c,P)-morphism, then for every constrained sort $s \in S^c$ the function $\overline{f}_s : (T_F(Y))_s \to M_s$ is a surjection too, where $\overline{f}$ is the unique extension of f to a (S,F,P)-morphism), for every **CHCL** signature (S,F,F^c,P) the functor $\beta_{(S,F,F^c,P)} : \mathbb{M}od(S,F,F^c,P) \to \mathbb{M}od(S,S^c,F,P)$ is defined by $\beta_{(S,F,F^c,P)}(M) = M$ for all models $M \in |\mathbb{M}od(S,F,F^c,P)|$ and $\beta_{(S,F,F^c,P)}(h) = h$ for all morphism $h \in \mathbb{M}od(S,F,F^c,P)$.

Notation. Recall that for every **GHCL** signature (S,S^c,F,P) we let F^{S^c} to denote the set of operations with constrained resulting sorts $\{\sigma \in F_{w\to s} \mid s \in S^c\}$.

Remark 8.4.4. *A (S,S^c,F,P)-model M in* **GHCL** *is reachable iff there exists a set of loose variables Y and a function $f : Y \to M$ such that for every constrained sort $s \in S^c$ the function $\overline{f}_s : (T_{F^{S^c}}(Y))_s \to M_s$ is surjective, where $\overline{f}$ is the unique extension of f to a (S,F^{S^c},P)-morphism.*

Proof. Almost identic with the proof of Remark 5.1.2. (Q.E.D.)

Definition 8.4.5. *A basic specification (Σ,Γ) in* **CHCL** *is sufficient-complete, where the signature Σ is (S,F,F^c,P), if for every term t formed with symbols from F^{S^c} and loose variables from Y there exists a term t' formed with constructors and loose variables from Y such that $\Gamma \models_{(S,F,P)} (\forall Y)t = t'$.*

The following is a corollary of Theorem 8.4.3.

Corollary 8.4.6. *The WES of* **CHCL** *generated by the proof rules for* **GHCL** *is sound and Ω-complete, where $\Gamma \in \Omega_{(S,F,F^c,P)}$ iff $((S,F,F^c,P),\Gamma)$ is a sufficient-complete specification.*

Proof. We set the parameters of Theorem 8.4.3. The institution I' is **CHCL** and the institution I is **GHCL**. The institution morphism is $\Delta_{\mathbf{HCL}}$ and the entailment system E of **GHCL** is the least entailment system closed under the rules enumerated in Corollary 8.3.18. M is the class of all reachable models. We need to prove that for every sufficient-complete specification $((S,F,F^c,P),\Gamma)$ and any reachable (S,S^c,F,P)-model M (where S^c is the set constrained sorts determined by F^c) we have: $M \models \Gamma$ implies $M \in |\mathbb{M}od(S,F,F^c,P)|$. Because M is reachable by Remark 8.4.4 there exists a function $f : Y \to M$, where Y is a set of loose variables, such that for every constrained sort $s \in S^c$ the function $f^\#_s : (T_{F^{S^c}}(Y))_s \to M_s$ is a surjection, where $f^\#$ is the unique extension of f to an (S,F^{S^c},P)-morphism. Because $((S,S^c,F,P),\Gamma)$ is sufficient-complete, for every constrained sort $s \in S^c$ the function $\overline{f}_s : (T_{F^c}(Y))_s \to M_s$ is a surjection too, where $\overline{f}$ is the unique extension of f to a (S,F^c,P)-morphism. (Q.E.D.)

Similar results as Corollary 10.4.14 can be formulated for **GHCL**$_\infty$.

In general, the proof rules given here for the constructor-based institutions are not complete. Recall Example 19: the signature (S,F,F^c,P) in **CHCL**, where $S = \{s\}$, $F_{\to s} = \{a,b\}$, $F^c = \{a\}$ and $P = \emptyset$. It is easy to notice that $\models a = b$ but there is no way to prove $\emptyset \vdash a = b$.

Structural Induction. In the constructor-based institutions presented here the elements of models consist of interpretations of terms formed with constructors and elements of loose sort. Thus, *Case Splitting* can be rephrased as follows:

Case splitting $\dfrac{\{\Gamma \vdash_{(S,F,F^c,P)} (\forall Y)\rho(x \leftarrow t) \mid Y - \textit{loose variables},\ t \in T_{F^c}(Y)\}}{\Gamma \vdash_{(S,F,F^c,P)} (\forall x)\rho}$ where Γ is a set of sentences, and $(\forall x)\rho$ a sentence such that x is a variable of constrained sort.

In order to prove the premises of *Case splitting*, in many cases, we use induction on the structure of terms. For any t formed with constructors in F^c and loose variables we have *(Structural induction)* $\Gamma \vdash_{(S,F,F^c,P)} (\forall V)\rho(x \leftarrow t)$ if

1. *Induction base* for all $cons \in F^c_{\to s}$, $\Gamma \vdash_{(S,F,F^c,P)} \rho(x \leftarrow cons)$,
2. *Induction step* for all $\sigma \in F^c_{s_1 \ldots s_n \to s}$, $\Gamma \cup \{\rho(x \leftarrow x') \mid x' \in X\} \vdash_{(S,F \cup C,F^c,P)} \rho(x \leftarrow \sigma(c_1, \ldots, c_n))$, where
   (a) $C = \{c_1, \ldots, c_n\}$ is a set of new variables such that c_i has the sort s_i, for all $i \in \{1, \ldots, n\}$, and
   (b) $X \subseteq C$ is the set of variables with the sort s.

where V are all (loose) variables in t.

Proposition 8.4.7. *The entailment system of* **CHCL** *satisfies the rules of* Structural induction.

Proof. Almost identical with the proof of Proposition 5.3.1. (Q.E.D.)

We define the infinitary rules of *Case splitting* and show that the WES of **CHCL** is sound and complete. As in case of **CCEQL** we have defined the rules of *Structural induction* to deal with infinitary premises of *Case spliting* but the infinitary rules can not be replaced with the finitary ones in order to obtain a complete and compact WES because the class of sentences true of a class of models for a given constructor-based specification is not in general recursively enumerable (it would be a contradiction with Gödel's famous incompleteness theorem).

Similar completeness results hold also for **CHOSA**, **CHPOA**, **CHPA** and their infinitary variants $\mathbf{CHCL}_\infty$, $\mathbf{CHOSA}_\infty$, $\mathbf{CHPOA}_\infty$, $\mathbf{CHPA}_\infty$ or variations of these institutions. The results here are due to [28]. If D^c is the broad subcategory consisting of identity morphisms then all models are reachable and we may obtain the result in [16] concerning Horn institutions. In the next chapter we investigate the applicability of Theorem 8.3.2 to **GFOL** by adapting the completeness of first-order institutions developed in [29]. Then it is straightforward to construct an institution morphism **CFOL** $\to$ **GFOL** and obtain an entailment system sound and complete (relatively to a family of sufficient-complete sets of sentences) for **CFOL**.

Chapter 9

Forcing and First-order Institutions

In this chapter we introduce the forcing technique in institutional model theory, apply it to prove a first-order completeness result, and points out some particular cases. The formalization of forcing in abstract model theory constitutes one of the most important contribution of our research, and it provides an efficient tool for obtaining new results showing also the significance of the top-down approach towards model theory. Forcing is a technique invented by Paul Cohen, for proving consistency and independence results in set theory [17, 18]. A. Robinson [60] developed an analogous theory of forcing in model theory, and Barwise [4] extended Robinson's theory to infinitary logic and used it to give a new proof of Omitting Types Theorem. A general treatment of the Omitting Types Theorem may be found in [44]. The forcing technique in classical model theory is presented also in [41].

We emphasize the results obtained for the infinitary logics, but we will also obtain completeness for the finitary logics. However the results for the finitary case is weaker than the known completeness results for the (finitary) first-order logic [39] as it requires a countable number of symbols in a signature. A paper with similar objectives dedicated to finitary logics that captures the case of uncountable signatures is [57].

9.1 Institution-independent Notions

Definition 9.1.1. *A signature morphism $\chi : \Sigma \to \Sigma'$ is non-void if there exists a substitution $\theta : \chi \to 1_\Sigma$.*

In **FOL** the non-void quantification translates into accepting extensions of signatures with constants of non-empty sorts. If we accept only signatures with non-empty sorts (for each sort there exists at least one term), signatures which are sensible [42], then all the extensions of signatures with constants are non-void.

Definition 9.1.2. *In any institution a Σ-sentence ρ is* finitary *iff it can be written as $\varphi(\rho_f)$ where $\varphi : \Sigma_f \to \Sigma$ is a signature morphism such that Σ_f is a finitely presented signature and ρ_f is a Σ_f sentence. An institution* has finitary sentences *when all its sentences are finitary.*

In concrete institutions this condition usually means that the sentences contain only a finite number of symbols. This is the case of **FOL**, **POA**, **OSA**, **PA**, and also their generalized versions.

9.2 Forcing and Generic Models

Forcing is a method of construction models satisfying some properties. In this paper we introduce the notion of forcing in institution model theory and we study completeness of various "first-order" logics. For this we assume an institution $I = (\mathbb{S}ig, \mathbb{S}en, \mathbb{M}od, \models)$ with a broad subcategory $D^l \subseteq \mathbb{S}ig$ of signature morphisms and a sub-functor $\mathbb{S}en_0 \subseteq \mathbb{S}en$.

Definition 9.2.1 (First order fragments)**.** *By a D^l-first-order Σ-fragment we mean an extension L of $\mathbb{S}en_0(\Sigma)$ ($\mathbb{S}en_0(\Sigma) \subseteq L$) such that*

1. *every sentence of L is constructed from the sentences of $\mathbb{S}en_0(\Sigma)$ by means of negations, (infinitary) disjunctions and existential quantifications over the signature morphisms in D^l, and*

2. *L has the following properties:*

   (a) *L is closed to negations, i.e. if $e \in L$ then $\neg e \in L$.*

   (b) *L is closed to the "sub-sentence" relation, i.e.*
   - *if $\neg e \in L$ then $e \in L$,*
   - *if $\bigvee E \in L$ then $e \in L$ for all $e \in E$, and*
   - *if $(\exists\chi)e' \in L$, where $\chi \in D^l$, and $\theta : \chi \to 1_\Sigma$ then $\theta(e') \in L$.*

Note that the closure of L to "sub-sentence" relation enable us to apply induction on the structure of the sentences. Our definition of fragments is slightly different from the one in [44]. We do not assume the closure of L to

- disjunctions, i.e. $e_1,\ e_2 \in L$ implies $e_1 \vee_2 \in L$, or

- existential quantifications, i.e. $\theta(e') \in L$ implies $(\exists\chi)e' \in L$ in case there exists a substitution $\theta : \chi \to 1_\Sigma$.

Definition 9.2.2. *A forcing property for a signature Σ is a tuple $\mathbb{P} = \langle P, \leq, f\rangle$ such that:*

1. *$\langle P, \leq\rangle$ is a partially ordered set with a least element 0.*

2. *f is a function which associates with each $p \in P$ a set $f(p)$ of sentences in $\mathbb{S}en_0(\Sigma)$.*

3. *Whenever $p \leq q$, $f(p) \subseteq f(q)$.*

4. *For each set of sentences $E \subseteq \mathbb{S}en_0(\Sigma)$ and any sentence $e \in \mathbb{S}en_0(\Sigma)$ if $E \subseteq f(p)$ and $E \models e$ then there is $q \geq p$ such that $e \in f(q)$.*

The elements of P are called *conditions* of $\mathbb{P}$. We will define the forcing relation $\Vdash \subseteq P \times L$ associated to a forcing property $\mathbb{P} = (P, f, \leq)$.

Definition 9.2.3. *Let $\mathbb{P} = \langle P, f, \leq\rangle$ be a forcing property for a signature Σ and L a Σ-fragment. The relation $p \Vdash e$ in $\mathbb{P}$, read p forces e, is defined by induction on e, for $p \in P$ and $e \in L$, as follows:*

- For $e \in \mathbb{S}en_0(\Sigma)$. *$p \Vdash e$ if $e \in f(p)$.*

- For $\neg e \in L$. *$p \Vdash \neg e$ if there is no $q \geq p$ such that $q \Vdash e$.*

- For $\bigvee E \in L$. $p \Vdash \bigvee E$ *if* $p \Vdash e$ *for some* $e \in E$.
- For $(\exists\chi)e \in L$. $p \Vdash (\exists\chi)e$ *if* $p \Vdash \theta(e)$ *for some substitution* $\theta : \chi \to 1_\Sigma$.

We say that p *weakly forces* e, in symbols $p \Vdash^w e$, iff $p \Vdash \neg\neg e$. The above definition is a generalization of the forcing studied in [60], [4] and [44].

Lemma 9.2.4. *Let* $\mathbb{P} = (P, f, \leq)$ *be a forcing property for a signature* Σ, L *a* Σ*-fragment and* e *a sentence in* L.

1. $p \Vdash^w e$ *iff for each* $q \geq p$ *there is a condition* $r \geq q$ *such that* $r \Vdash e$.
2. *If* $p \leq q$ *and* $p \Vdash e$ *then* $q \Vdash e$.
3. *If* $p \Vdash e$ *then* $p \Vdash^w e$.
4. *We can not have both* $p \Vdash e$ *and* $p \Vdash \neg e$.

Proof.

1. $p \Vdash^w e$ iff $p \Vdash \neg\neg e$ iff for each $q \geq p$, $q \nVdash \neg e$ iff for each $q \geq p$, there exists $r \geq q$ such that $r \Vdash e$.
2. By induction on e.

   For $e \in \mathbb{S}en_0(\Sigma)$. The conclusion follows from $f(p) \subseteq f(q)$.

   For $\neg e \in L$. We have $p \Vdash \neg e$. Suppose towards a contradiction $q \nVdash \neg e$, then by definition of forcing there is $q' \geq q$ such that $q' \Vdash e$. Therefore there is $q' \geq p$ such that $q' \Vdash e$, thus $p \nVdash \neg e$, which is a contradiction.

   For $\bigvee E \in L$. $p \Vdash e$ for some $e \in E$. By induction $q \Vdash e$ which implies $q \Vdash \bigvee E$.

   For $(\exists\chi)e \in L$. Since $p \Vdash (\exists\chi)e$ then $p \Vdash \theta(e)$ for some substitution $\theta : \chi \to 1_\Sigma$. By induction $q \Vdash \theta(e)$, and by the definition of forcing relation $q \Vdash (\exists\chi)e$.
3. It follows easily from 1 and 2.
4. Obvious.

(Q.E.D.)

By Lemma 9.2.4 (4), we may introduce $p \nVdash false$, for all conditions $p \in P$, in the Definition 9.2.3 and nothing will be changed in the future developments.

Definition 9.2.5. *Let* $\mathbb{P} = (P, f, \leq)$ *be a forcing property for a signature* Σ, *and* L *a* Σ*-fragment. A subset* $G \subseteq P$ *is said to be a generic (relatively to the fragment* L*) iff*

1. $p \in G$ *and* $q \leq p$ *implies* $q \in G$.
2. $p, q \in G$ *implies that there exists* $r \in G$ *with* $p \leq r$ *and* $q \leq r$.
3. *for each sentence* $e \in L$ *there exists a condition* $p \in G$ *such that either* $p \Vdash e$ *or* $p \Vdash \neg e$.

Lemma 9.2.6. *If* L *is countable then every* p *belongs to a generic set.*

Proof. The proof of this lemma is similar to the one in [44]. Since L is countable let $\{e_n \mid n < \omega\}$ be an enumeration of L. We form a chain of conditions $p_0 \leq p_1 \leq \ldots$ in P as follows. Let $p_0 = p$. If $p_n \Vdash \neg e_n$, let $p_{n+1} = p_n$, otherwise choose $p_{n+1} \geq p_n$ such that $p_{n+1} \Vdash e_n$. The set $G = \{q \in P \mid q \leq p_n \text{ for some } n < \omega\}$ is generic and contains p. (Q.E.D.)

Definition 9.2.7. *Let $\mathbb{P} = \langle P, \leq, f \rangle$ be a forcing property for a signature Σ and L a Σ-fragment.*

1. *M is a model for $G \subseteq P$ if for every sentence $e \in L$*

$$M \models e \text{ iff } G \Vdash e$$

2. *M is a generic model for $p \in P$ if there is a generic set $G \subseteq P$ such that $p \in G$ and M is a model for G.*

Proposition 9.2.8. *Assume that*

1. *every set of sentences in $\mathbb{S}en_0(\Sigma)$ is basic,*
2. *there exists a subcategory D of signature morphisms such that*
   (a) *$D^l \subseteq D$, and*
   (b) *for each $E \subseteq \mathbb{S}en_0(\Sigma)$ there exists a basic model M_E that is D-reachable,*
3. *the semantic entailment system $(\mathbb{S}ig, \mathbb{S}en_0, \models)$ of I_0 is compact.*

Then there is a D-reachable model for every generic set G.

Proof. Let T be the set of all sentences of L which are forced by G. Let $B = \mathbb{S}en_0(\Sigma) \cap T$. We prove that for each $e \in L$ $M_B \models e$ iff $e \in T$ by induction on e.

For $e \in \mathbb{S}en_0(\Sigma)$. Suppose $M_B \models e$ then we have $B \models e$ and by the hypothesis there is $B' \subseteq B$ finite such that $B' \models e$. Since G is generic there exists $p \in G$ such that $B' \subseteq f(p)$. Suppose towards a contradiction that $e \notin T$ which because G is generic leads to $\neg e \in T$. Then there is $q \in G$ such that $q \Vdash \neg e$. Since G is generic there is $r \in G$ such that $r \geq p$ and $r \geq q$. We have $B' \subseteq f(r)$ and using Lemma 9.2.4(2) we obtain $r \Vdash \neg e$. By the definition of forcing property $r' \Vdash e$ for some $r' \geq r$ and and by Lemma 9.2.4(2) $r' \Vdash \neg e$ which is a contradiction. If $e \in T$ then $e \in B$ and $M_B \models e$.

For $\neg e \in L$. Exactly one of e, $\neg e$ is in T. Since G is generic there is $p \in G$ such that either $p \Vdash e$ or $p \Vdash \neg e$. Therefore $e \in T$ or $\neg e \in T$. Suppose towards a contradiction that e ,$\neg e \in T$, then there exists $p, q \in G$ such that $p \Vdash e$ and $q \Vdash \neg e$. By the definition of generic sets there is $r \in G$ such that $r \geq p$ and $r \geq q$. By Lemma 1(2) $r \Vdash e$ and $r \Vdash \neg e$ which is a contradiction.

Let $\neg e \in T$. Suppose that $M_B \models e$, then by induction we have $e \in T$, which is a contradiction. Therefore $M_B \models \neg e$. Now if $M_B \models \neg e$, then e is not in T, therefore $\neg e \in T$.

For $\bigvee E \in L$. If $M_B \models \bigvee E$ then $M_B \models e$ for some $e \in E$. By induction $e \in T$. We have $p \Vdash e$ for some $p \in G$ and we obtain $p \Vdash \bigvee E$. Thus, $\bigvee E \in T$. Now if $\bigvee E \in T$ then $e \in T$, for some $e \in E$. Therefore, by induction, $M_B \models e$ and thus $M_B \models \bigvee E$.

For $(\exists\chi)e \in L$. Assume that $M_B \models (\exists\chi)e$ where $\chi : \Sigma \to \Sigma'$. There exists a χ-expansion N of M_B such that $N \models e$. Because M_B is D-reachable there exists a substitution $\theta : \chi \to 1_\Sigma$ such that $M_B \restriction_\theta = N$. By the satisfaction condition $M_B = N \restriction_\chi \models \theta(e)$. By induction $\theta(e) \in T$ which implies $(\exists\chi)e \in T$. For the converse implication assume that $p \Vdash (\exists\chi)e$ for some $p \in G$. We have that $p \Vdash \theta(e)$ for some substitution $\theta : \chi \to 1_\Sigma$. By induction $M_B \models \theta(e)$ which implies $M_B \restriction_\theta \models e$. Since $(M_B \restriction_\theta) \restriction_\chi = M_B$ we obtain $M_B \models (\exists\chi)e$. (Q.E.D.)

Theorem 9.2.9. *(Generic model theorem) Under the conditions of Proposition 9.2.8, if L is countable then there is a generic D-reachable model for each condition $p \in P$.*

Proof. By Lemma 9.2.6 there is a set generic set $G \subseteq P$ such that $p \in G$ and by Proposition 9.2.8 there is a D-reachable model M for G. (Q.E.D.)

The following is a corollary of the generic model theorem.

Corollary 9.2.10. *Under the condition Theorem 9.2.9 for every condition $p \in P$ and any sentence $e \in L$ we have that $p \Vdash^w e$ iff $M \models e$ for each generic D-reachable model M for p.*

Proof. Suppose $p \Vdash^w e$ and M is a generic D-reachable model for p. We have $p \Vdash \neg\neg e$ which implies $M \models \neg\neg e$ and $M \models e$. Now for the converse implication suppose that $p \nVdash^w e$. There is $q \Vdash \neg e$ for some $q \geq p$. By Proposition 9.2.8 there is a generic D-reachable model M for q which implies $M \models \neg e$. But M is also a generic model for p. (Q.E.D.)

9.3 First-order Institutions and Entailment Systems

As in case of universal institutions the results concerning the first-order entailment systems come both in a finite and an infinite variant, the finite one being obtained by adding (to the hypotheses of the infinite one) all the finiteness hypotheses marked in the brackets.

Let $I = (\mathbb{S}ig, \mathbb{S}en, \mathbb{M}od, \models)$ be an institution and

- let $\mathbb{S}en_0$ be a sub-functor of $\mathbb{S}en$ (i.e. $\mathbb{S}en_0 : \mathbb{S}ig \to \mathbb{S}et$ such that $\mathbb{S}en_0(\Sigma) \subseteq \mathbb{S}en(\Sigma)$ and $\varphi(\mathbb{S}en_0(\Sigma)) \subseteq \mathbb{S}en_0(\Sigma')$ for each signature morphism $\varphi : \Sigma \to \Sigma'$), and
- $D^l \subseteq \mathbb{S}ig$ is a broad subcategory of signature morphisms.

We say that I is a D^l*-first-order institution* over I_0, where $I_0 = (\mathbb{S}ig, \mathbb{S}en, \mathbb{M}od, \models)$, when for every signature Σ the set $\mathbb{S}en(\Sigma)$ is a D^l-first-order fragment.

Let **AFOL** be the restriction of **FOL** to the atomic sentences. **FOL** is a first-order institution over **AFOL**, where the quantification class D^l of signature morphisms is the class of all signature extensions with a finite number of constants. Similarly, the infinitary version $\mathbf{FOL}_{\omega_1,\omega}$ is an example of first-order institution.

Let us assume a D^l-first-order institution $I = (\mathbb{S}ig, \mathbb{S}en, \mathbb{M}od, \models)$ over I_0 with $\mathbb{S}en_0$ the sub-functor of $\mathbb{S}en$. We define the following proof rules for the entailment system of I:

(*Substitutivity'*) $(\exists\varphi)\theta(\rho) \vdash (\exists\chi)\rho$ for all Σ-sentences $(\exists\chi)\rho$ and $(\exists\varphi)\theta(\rho)$, where $\theta : \chi \to \varphi$ is a substitution.

In this chapter we consider the following version of *Generalization*:

(*Generalization*) $\Gamma \vdash_\Sigma \neg(\exists\chi)\rho'$ iff $\chi(\Gamma) \vdash_{\Sigma'} \neg\rho'$ for all sets of Σ-sentences Γ and all Σ-sentences $\neg(\exists\chi)\rho'$, where $\chi : \Sigma \to \Sigma'$.

Given a compact entailment system $E_0 = (\mathbb{S}ig, \mathbb{S}en, \vdash^0)$ for I_0, the first-order entailment of I (abbreviated *FOES*) consists of the least entailment system over E_0 with disjunctions, false, negations, existential quantifications, and closed under *Substitutivity'*.

Note that these rules are given for both finitary and infinitary case. In the finitary case the disjunction $\bigvee E$ occurring in the *Disjunction introduction* and *Disjunction elimination* property is finitary, i.e. E is a finite set of sentences. Generally speaking, if one of the first-order constructor for sentences is missing then the corresponding properties are disregarded. For example in case of **QfFOL**, the restriction of **FOL** to quantifier-free sentences, *Substitutivity* and *Generalization* are omitted. However, if *false* is missing then the definitions of *Red* and *False* may be rephrased using $\{\rho, \neg\rho\}$ instead of *false*, where ρ is any sentence.

We call a set E of sentences *inconsistent* when $E \vdash false$, or alternatively $E \vdash \rho$ and $E \vdash \neg\rho$ for some sentence ρ.

Proposition 9.3.1. *The FOES of I is sound (and compact) whenever the entailment system of I_0 is sound (and compact).*

Proof. The soundness of *Substitutivity'* is similar to the one for *Substitutivity*. By Corollaries 3.3.2 and 3.3.7 we obtain the soundness for the FOES of I.

For the the compactness of the entailment system of I consider the compact entailment subsystem $E^c = (\mathbb{S}ig, \mathbb{S}en, \vdash^c)$ of the FOES $E = (\mathbb{S}ig, \mathbb{S}en, \vdash)$ of I. Since the entailment system $E_0 = (\mathbb{S}ig, \mathbb{S}en_0, \vdash^0)$ of I_0 is compact, E^c satisfies all the rules in E_0. Using an argument similar as in the proof of Propositions 3.3.1, 3.3.5 and 3.3.3 the entailment E^c has disjunctions, negations and false. Since the rules of *Substitutivity'* are finitely generated E^c satisfies the rules of *Substitutivity'*. By Proposition 3.3.10 E^c satisfies *Generalization* and because E is the least FOES over E_0 with disjunctions,negations and false, and satisfying the rules of *Substitutivity'* and *Generalization* we obtain $E^c = E$. (Q.E.D.)

We also assume another mild condition, namely that the sentences of I_0 are not obtained by applying the first-order constructors. An immediate consequence of this definition is the following.

Remark 9.3.2. *Let $\varphi : \Sigma \to \Sigma'$ be a signature morphism, $e \in \mathbb{S}en(\Sigma)$ and $e' \in \mathbb{S}en(\Sigma')$ two sentences such that $\varphi(e) = e'$. Then*

- *$e \in \mathbb{S}en_0(\Sigma)$ iff $e' \in \mathbb{S}en_0(\Sigma')$,*
- *e is obtained by applying Boolean connectives iff e' is obtained by applying Boolean connectives, and*
- *e is an existential quantified sentence iff e' is a existential quantified sentence.*

9.3.1 First-order Completeness

Completeness of the first-order entailment systems is significantly more difficult than soundness and therefore requires more conceptual infrastructure. The first-order completeness result below is applicable to institutions with "countable" signatures, i.e. signatures Σ with $card(\mathbb{S}en_0(\Sigma)) \leq \omega$.

Definition 9.3.3. *Let $D \subseteq \mathbb{S}ig$ be a subcategory of signature morphisms such that $D^l \subseteq D$. We say that $\Sigma \xrightarrow{\chi} \Sigma' \in D$ is a (D, D^l)-extension of Σ if*

1. *χ is non-void, and*
2. *it is the vertex of a directed co-limit $(\chi_i \xrightarrow{\varphi_i} \chi)_{i \in J}$ of a directed diagram $(\chi_i \xrightarrow{\varphi_{i,j}} \chi_j)_{(i \leq j) \in (J, \leq)}$ in Σ/D^l ($\Sigma \xrightarrow{\chi_i} \Sigma_i \in D^l$ for all $i \in J$ and $\Sigma_i \xrightarrow{\varphi_{i,j}} \Sigma_j \in D^l$ for all $(i, j) \in (J, \leq)$) such that for all signature morphisms $\Sigma_i \xrightarrow{\psi_i} \Sigma'_i \in D^l$ there exists a substitution $\psi_i \xrightarrow{\psi_{i,j}} \varphi_{i,j} \in (\Sigma_i/\mathbb{S}ig)$ which is non-void.*

Throughout this section we assume that the institution I has the following properties

1. every signature morphism in D^l is non-void and finitary,
2. there exists a subcategory $D \subseteq \mathbb{S}ig$ of signature morphisms such that every signature Σ has a (D, D^l)-extension, and

3. every sentence of I_0 is finitary.

The (D,D^l)-extension property is easily fulfilled in concrete examples. Take for example **GFOL** and assume that D is the class of all signature extensions with arbitrary number of constants of any sort, and D^l is the class of signature extensions with finite number of constants of non-void loose sorts ($s \in S^l$ with $(T_F) \neq \emptyset$). For every signature Σ consider a set C of new constant symbols (C does not contain any symbol from Σ) such that

- C_s is an infinite set for all non-void sorts $s \in S^l$, and
- $C_s \cap C_{s'}$ for all loose sorts $s, s' \in S^l$.

The inclusion $\Sigma \overset{\chi}{\hookrightarrow} \Sigma(C) \in D$ is non-void, and it is the vertex of the directed co-limit $((\Sigma \overset{\chi_i}{\hookrightarrow} \Sigma(C_i)) \overset{\varphi_i}{\hookrightarrow} (\Sigma \overset{\chi}{\hookrightarrow} \Sigma(C)))_{C_i \subseteq C finite}$ of the directed diagram $(\chi_i \overset{\varphi_{i,j}}{\hookrightarrow} \chi_j)_{C_i \subseteq C_j \subseteq Y finite}$ in $D^l/\mathbb{S}ig$. Since C is infinite, for every signature extension $\psi_i : \Sigma(C_i) \hookrightarrow \Sigma_i(C_i \cup Y)$, where Y is a finite set of new constants of non-void loose sorts, there exists an injective mapping $\psi_{i,j} : C_i \cup Y \to C_j$ such that the restriction $\psi_{i,j}|_{C_i} : C_i \to C_j$ is the inclusion.

In case of first-order institutions with sentences formed without quantifiers we may consider D the broad subcategory of $\mathbb{S}ig$ with $D(\Sigma,\Sigma) = 1_\Sigma$ and $D(\Sigma,\Sigma') = \emptyset$ for all signatures $\Sigma \neq \Sigma'$. Note that in this case, we may take $D^l = D$ and any signature Σ has a (D,D^l)-extension $\chi = 1_\Sigma$.

Canonical Forcing Properties. Let $\chi : \Sigma \to \Sigma'$ be a (D,D^l)-extension of Σ as in Definition 9.3.3. We have the following consequence of the finiteness of the "atomic" sentences.

Lemma 9.3.4. $Sen_0(\Sigma') = \bigcup_{i \in J} \varphi_i(\mathbb{S}en_0(\Sigma_i))$

Proof. We show $\mathbb{S}en_0(\Sigma') \subseteq \bigcup_{i \in J} \varphi_i(\mathbb{S}en_0(\Sigma_i))$. Let $e \in \mathbb{S}en_0(\Sigma')$. Since e is finitary it can be written as $v(e_f)$ where $v : \Sigma_f \to \Sigma'$ is a signature morphism such that Σ_f is finitely presented in the category $\mathbb{S}ig$. By finiteness of Σ_f there exists a signature morphism $v_i : \Sigma_f \to \Sigma_i$ such that $v_i;\varphi_i = v$. We have that $e = \varphi_i(v_i(e_f))$. Therefore $\mathbb{S}en_0(\Sigma') = \bigcup_{i \in J} \varphi_i(\mathbb{S}en_0(\Sigma_i))$. (Q.E.D.)

We denote by $L_{\Sigma'}$ the set of sentences $\bigcup_{i \in J} \varphi_i(\mathbb{S}en(\Sigma_i))$ and we have the following consequence of Remark 9.3.2 and the finiteness of signature morphisms in D^l.

Lemma 9.3.5. *$L_{\Sigma'}$ is a first-order fragment.*

Proof. By Lemma 9.3.4 we have that $\mathbb{S}en_0(\Sigma) \subseteq L_{\Sigma'}$.

The closure properties of $L_{\Sigma'}$ are consequences of Remark 9.3.2 and the finiteness of signature morphisms in D. The most interesting case is the closure of $L_{\Sigma'}$ to substitutions. The remaining cases are straightforward. Let $(\exists\psi)e \in L_{\Sigma'}$ (where $\psi : \Sigma' \to \Sigma'_1$) and a substitution $\theta : \psi \to 1_{\Sigma'}$. By the definition of $L_{\Sigma'}$ and Remark 9.3.2 we have $(\exists\psi)\varphi'_k(e_k) = \varphi_k((\exists\psi_k)e_k)$ for some $(\exists\psi_k)e_k \in \mathbb{S}en(\Sigma_k)$, where

$$\begin{tikzcd}
 & \Sigma'_k \arrow[r, dotted, "\varphi'_k"] & \Sigma'_1 \\
\Sigma_k \arrow[ur, dotted, "\psi_k"] \arrow[r, "\varphi_k"'] & \Sigma' \arrow[ur, "\psi"'] &
\end{tikzcd}$$

is a pushout of signature morphisms with $\psi_k \in D^l$. Since ψ_k is finitary and $(\varphi_{k,i} \xrightarrow{\varphi_i} \varphi_k)_{(k \leq i) \in (J,\leq)}$ is a directed co-limit in the category $\Sigma_k/\mathbb{S}ig$, there exists $\theta_k : \psi_k \to \varphi_{k,k'}$, where $k \leq k'$ such that $\theta_k;\varphi_{k'} = \varphi'_k;\theta$.

$$\begin{tikzcd}
 & \Sigma'_k \arrow[r, dotted, "\varphi'_k"] \arrow[d, dotted, "\theta_k"] & \Sigma' \arrow[d, "\theta"] \\
\Sigma_k \arrow[ur, dotted, "\psi_k"] \arrow[r, "\varphi_{k,k'}"'] & \Sigma_{k'} \arrow[r, "\varphi_{k'}"'] & \Sigma \arrow[u, "\psi"] \arrow[r, "1_\Sigma"'] & \Sigma
\end{tikzcd}$$

Therefore $\theta(e) = \theta(\varphi'_k(e_k)) = \varphi_{k'}(\theta_k(e_k)) \in L_{\Sigma'}$. (Q.E.D.)

Now, let L be an arbitrary Σ'-fragment. We define the *canonical forcing property* $\mathbb{P} = (P, f, \leq)$ (relatively to the fragment L).

- $P = \{\varphi_i(p_i) \mid \ p_i \subseteq \mathbb{S}en(\Sigma_i),\ \varphi_i(p_i) \subseteq L$ and $\varphi_i(p_i)$ is consistent$\}$,
- $f(p) = p \cap \mathbb{S}en_0(\Sigma)$ for all $p \in P$, and
- $\leq$ is the inclusion relation $\subseteq$.

Proposition 9.3.6. *$\mathbb{P} = (P, \leq, f)$ is a forcing property.*

Proof. All the conditions of the forcing property, except the last one, obviously hold for $\mathbb{P}$. Assume a condition $p \in P$ and a set of sentences $E \subseteq f(p)$ such that $E \models e$ where $e \in \mathbb{S}en_0(\Sigma)$. We prove that $p \cup \{e\} \in P$.

By the completeness of the proof rules for I_0 we get $E \vdash e$ and moreover $p \vdash e$ which implies $p \cup \{e\}$ consistent. By the definition of $\mathbb{P}$ the condition $p \in P$ may be written as $p = \varphi_i(p_i)$ for some $i \in J$ and $p_i \in \mathbb{S}en(\Sigma_i)$. Since e is a sentence in $\mathbb{S}en_0(\Sigma')$ it may be written as $e = \varphi_j(e_j)$ for some $j \in J$ and $e_j \in \mathbb{S}en_0(\Sigma_j)$. Let $(i \leq k) \in (J, \leq)$ and $(j \leq k) \in (J, \leq)$. We have that $p \cup \{e\} = \varphi_k(\varphi_{i,k}(p_i) \cup \{\varphi_{j,k}(e_j)\})$ is consistent. Therefore $p \cup \{e\} \in P$. (Q.E.D.)

Lemma 9.3.7. *$\mathbb{P}$ has the following properties.*

1. *if $p \in P$ and $\bigvee E \in p$ then $p \cup \{e\} \in P$ for some $e \in E$.*
2. *if $p \in P$ and $(\exists \psi)e \in p$ (where $\psi : \Sigma' \to \Sigma'_1$) there exists a substitution $\theta : \psi \to 1_\Sigma$ such that $p \cup \{\theta(e)\} \in P$.*

Proof. 1. Suppose towards a contradiction that $p \cup \{e\} \notin P$ for all $e \in E$.

If $e \in E$ then $p \cup \{e\} \in L$. By Remark 9.3.2 there exists $\bigvee E_i \in p_i$ such that $\varphi_i(E_i) = E$. Since $p \cup \{e\} = \varphi_i(p_i \cup \{e_i\})$ for some $e_i \in E_i$, $p \cup \{e\} \subseteq L$ and $p \cup \{e\} \notin P$ we get $p \cup \{e\}$ not consistent.

Because $p \vdash \bigvee E$ and for every $e \in E$ we have $p \cup \{e\}$ inconsistent by Disjunction elimination property we get p inconsistent which is a contradiction.

2. There exists $p_i \subseteq \mathbb{S}en(\Sigma_i)$ such that $\varphi_i(p_i) = p$. By Remark 9.3.2 there is a sentence $(\exists \psi_i)e_i \in p_i$ and a pushout

$$\begin{tikzcd}
\Sigma'_i \arrow[r, dotted, "\varphi'_i"] & \Sigma'_1 \\
\Sigma_i \arrow[u, dotted, "\psi_i"] \arrow[r, "\varphi_i"'] & \Sigma' \arrow[u, "\psi"']
\end{tikzcd}$$

such that $\varphi_i((\exists\psi_i)e_i) = (\exists\psi)\varphi'_i(e_i)$ and $e = \varphi'_i(e_i)$. By Definition 9.3.3 there exists $(i \leq j) \in (J, \leq)$ and a substitution $\psi_{i,j} : \psi_i \to \varphi_{i,j}$ with $\psi_{i,j}$ non-void as a signature morphism.

$$\begin{tikzcd}
 & \Sigma'_i \arrow[rr, dotted, "\varphi'_i"] \arrow[d, dotted, "\psi_{i,j}"] & & \Sigma'_1 \\
\Sigma_i \arrow[ur, dotted, "\psi_i"] \arrow[r, "\varphi_{i,j}"'] & \Sigma_j \arrow[r, "\varphi_j"'] & \Sigma' \arrow[ur, "\psi"] &
\end{tikzcd}$$

Because $\{\Sigma'_i \xleftarrow{\psi_i} \Sigma_i \xrightarrow{\varphi_i} \Sigma',\ \Sigma' \xrightarrow{\psi} \Sigma'_1 \xleftarrow{\varphi'_i} \Sigma'_i\}$ is a pushout and $\psi_i;(\psi_{i,j};\varphi_j) = \varphi_i;1_{\Sigma'}$ there exists $\theta : \Sigma'_1 \to \Sigma'$ such that $\varphi'_i;\theta = (\psi_{i,j};\varphi_j)$ and $\psi;\theta = 1_{\Sigma'}$.

$$\begin{tikzcd}
 & \Sigma'_i \arrow[rr, dotted, "\varphi'_i"] \arrow[d, dotted, "\psi_{i,j}"] & & \Sigma'_1 \arrow[d, dotted, "\theta"] \\
\Sigma_i \arrow[ur, dotted, "\psi_i"] \arrow[r, "\varphi_{i,j}"'] & \Sigma_j \arrow[r, "\varphi_j"'] & \Sigma' \arrow[ur, "\psi"] \arrow[r, "1'_\Sigma"'] & \Sigma'
\end{tikzcd}$$

We show that $\psi_i(p_i) \cup \{e_i\}$ is consistent. Suppose towards a contradiction that $\psi_i(p_i) \cup \{e_i\}$ is inconsistent. We have that $\psi_i(p_i) \vdash \neg e_i$ and by *Generalization* we get $p_i \vdash \neg(\exists\psi_i)e_i$ which is a contradiction with the consistency of p_i.

Since $\psi_{i,j}$ is non-void and $\psi_i(p_i) \cup \{e_i\}$ is consistent we have that $\psi_{i,j}(\psi_i(p_i) \cup \{e_i\})$ is consistent. Since φ_j is non-void, we obtain that $\varphi_j(\psi_{i,j}(\psi_i(p_i) \cup \{e_i\})) = p \cup \theta(e)$ is consistent. Therefore $p \cup \{\theta(e)\} \in P$.

(Q.E.D.)

Proposition 9.3.8. *If $L \subseteq L_{\Sigma'}$ then for each sentence $e \in L$ and each condition $p \in P$*

$$\textit{there exists } q \geq p \textit{ such that } q \Vdash e \textit{ iff } p \cup \{e\} \in P$$

Proof. For $e \in \mathbb{S}en_0(\Sigma')$. If there is $q \geq p$ such that $q \Vdash e$ then $e \in q$ which implies $p \cup \{e\} \subseteq q$. q is consistent and any subset of q is consistent too which implies $p \cup \{e\}$ is consistent. Therefore $p \cup \{e\} \in P$. For the converse implication take $q = p \cup \{e\}$.

For $\neg e$. By the induction hypothesis, applied to e, for each $q \in P$ we have

$$\text{for each } r \geq q, r \nVdash e \iff q \cup \{e\} \notin P$$

which implies that for each $q \in P$ we have

$$q \Vdash \neg e \iff q \cup \{e\} \notin P$$

We need to prove

$$\text{there exists } q \geq p \text{ such that } q \cup \{e\} \notin P \iff p \cup \{\neg e\} \in P$$

Assume that there is $q \geq p$ such that $q \cup \{e\} \notin P$. Then $q \cup \{e\}$ inconsistent which implies $q \vdash \neg e$. We obtain $q \cup \{\neg e\}$ consistent (suppose $q \cup \{\neg e\}$ is inconsistent we obtain $q \vdash \neg\neg e$, a contradiction with the consistency of q). Since $p \cup \{\neg e\} \subseteq q \cup \{\neg e\}$, we have $p \cup \{\neg e\}$ consistent. Therefore $p \cup \{\neg e\} \in P$. For the converse implication, take $q = p \cup \{\neg e\}$.

For $\bigvee E$. If there is $q \geq p$ such that $q \Vdash \bigvee E$, then there is $e \in E$ such that $q \Vdash e$. By the induction hypothesis, $p \cup \{e\} \in P$. If $p \cup \{e\}$ consistent implies $p \cup \{\bigvee E\}$ consistent then $p \cup \{\bigvee E\} \in P$. Suppose towards a contradiction that $p \cup \{\bigvee E\}$ is not consistent, then $p \cup \{e, \bigvee E\}$ is not consistent. Because $p \cup \{e\} \vdash \bigvee E$ (by *Disjunction introduction*) we obtain $p \cup \{e\}$ inconsistent which is a contradiction.

For the converse implication assume that $p \cup \{\bigvee E\} \in P$. By Lemma 9.3.7 (1) there is $e \in E$ such that $p \cup \{\bigvee E, e\} \in P$. By induction hypothesis applied to e we have $q \Vdash e$ for some $q \geq p \cup \{\bigvee E\}$. Hence there exists $q \geq p$ such that $q \Vdash \bigvee E$.

For $(\exists\psi)e$. Assume that there is $q \geq p$ such that $q \Vdash (\exists\psi)e$. By the definition of forcing relation there exists a substitution $\theta : \psi \to 1_\Sigma$ such that $q \Vdash \theta(e)$. By induction $p \cup \{\theta(e)\} \in P$. By *Substitutivity'* $p \cup \{\theta(e)\} \vdash (\exists\psi)e$ which implies $p \cup \{\theta(e), (\exists\psi)e\}$ consistent. Because $p \cup \{(\exists\psi)e\} \subseteq p \cup \{\theta(e), (\exists\psi)e\}$ we get $p \cup \{(\exists\psi)e\}$ consistent. Therefore $p \cup \{(\exists\psi)e\} \in P$.

For the converse implication assume that $p \cup \{(\exists\psi)e\} \in P$ where $\psi : \Sigma' \to \Sigma'_1$. By Lemma 9.3.7 (2) there exists a substitution $\theta : \psi \to 1_{\Sigma'}$ such that $p \cup \{(\exists\psi)e,\ \theta(e)\} \in P$. Applying the induction hypothesis to $\theta(e)$ we obtain $q \geq p \cup \{(\exists\psi)e\}$ such that $q \Vdash \theta(e)$. Therefore, by the definition of forcing relation $q \Vdash (\exists\psi)e$. (Q.E.D.)

We have the following consequence of the above proposition.

Corollary 9.3.9. *If* $L \subseteq L_{\Sigma'}$ *then for each condition* $p \in P$*, any generic model* M *for* p *satisfies* p*.*

Proof. Let $G \subseteq P$ be the generic set such that $p \in G$ and M is a model for G. We prove that $M \models e$ for all $e \in p$.

Let e be an arbitrary sentence in p. Since $G \subseteq P$ is a generic set there exists $q \in G$ such that either $q \Vdash e$ or $q \Vdash \neg e$. Suppose that $q \Vdash \neg e$ then there is $r \in G$ such that $r \geq p$ and $r \geq q$. By Lemma 9.2.4 (2) $r \Vdash \neg e$. By Proposition 9.3.8 since $e \in r$ there exists $r' \geq r$ such that $r' \Vdash e$. Using Lemma 9.2.4 (2) again we get $r' \Vdash \neg e$ which is a contradiction. Therefore $q \Vdash e$ and since M is a model for G we have that $M \models e$. (Q.E.D.)

Existence of generic sets. Corollary 9.3.9 does not state that for each condition there is a generic set which includes it. Therefore we need to prove that generic sets actually exists. For this we will consider only signatures that have a countable set of symbols.

Definition 9.3.10. *We say that a signature* Σ *is* countable *if it has a countable set of "atomic" sentences, i.e.* $card(\mathbb{S}en_0(\Sigma)) \leq \omega$*.*

Lemma 9.3.11. *Assume that all the signatures of* I *are countable and let*

- $\chi : \Sigma \to \Sigma'$ *be a an extension of* Σ *as in Definition 9.3.3, and*
- Γ *be a countable set of* Σ*-sentences.*

If L *is the least first-order fragment which contains* $\chi(\Gamma)$ *then every condition* $p \in P$ *belongs to a generic set.*

Proof. Since the signature Σ is countable we have that L is countable. By Lemma 9.2.6 every condition p belongs to a generic set. (Q.E.D.)

In case the sentences of I are formed without quantifiers, the countable condition is not needed.

Lemma 9.3.12. *If all the sentences of I are formed without quantifiers then for any condition p there exists a generic set G such that $p \in G$.*

Proof. Note that in this case the extension χ is the identity 1_Σ. Let $\{e_i \mid i < card(L)\}$ be an enumeration of L. We form a chain of conditions $p_0 \leq p_1 \leq \ldots$ in P as follows: let $p_0 = p$. If $p_i \Vdash \neg e_i$, let $p_{i+1} = p_i$, otherwise choose $p_{i+1} \geq p_i$ such that $p_{i+1} \Vdash e_i$; for any limit ordinal $\alpha < card(L)$ let $p_\alpha = \bigcup_{i<\alpha} p_i$. The set $G = \{q \in P \mid q \leq p_i$ for some $i < card(L)\}$ is generic and contains p. (Q.E.D.)

Theorem 9.3.13 (First-order completeness)**.** *Consider a D^l-first-order institution $I = (\mathbb{S}ig, \mathbb{S}en, \mathbb{M}od, \models)$ over $I_0 = (\mathbb{S}ig, \mathbb{S}en_0, \mathbb{M}od, \models)$ and a broad subcategory $D \subseteq \mathbb{S}ig$ of signature morphisms, where $D^l \subseteq D$ and such that*

1. *either*
   (a) *the sentences of I are formed without quantifiers (in this case we assume that D^l is the broad subcategory of signature morphisms which consists of identities only), or*
   (b) *all the signatures are countable and disjunctions are applied only to countable sets of sentences ,*
2. *every signature Σ has a (D, D^l)-extension,*
3. *every signature morphism in D^l is non-void and finitary,*
4. *the semantic entailment system $(\mathbb{S}ig, \mathbb{S}en_0, \models)$ of I_0 is compact,*
5. *every sentence of I_0 is finitary, and*
6. *for every $E \subseteq \mathbb{S}en_0(\Sigma)$ there exists a D-reachable model M_E defining E as basic set of sentences.*

If the entailment system of I_0 is complete then we have

1. *$\Gamma \models_\Sigma \rho$ implies $\Gamma \vdash_\Sigma \rho$, and moreover*
2. *$\Gamma \models_\Sigma \rho$ iff for every (D, D^l)-extension $(\Sigma \xrightarrow{\chi} \Sigma') \in D$ of Σ and each D-reachable Σ'-model M' we have $M' \restriction_\chi \models (\bigwedge \Gamma \Rightarrow \rho)$,*

where Γ is a countable set of Σ-sentences and ρ is any Σ-sentence.

Proof. We consider the case all the signatures of Σ are countable. The case when I admits sentences without quantifiers is similar.

1. Assume that $\Gamma \nvdash_\Sigma \rho$, where Γ is a countable set of sentences. Let $\Sigma \xrightarrow{\chi} \Sigma'$ be a (D, D^l)-extension of Σ as in Definition 9.3.3. We define L as the least Σ'-fragment which includes $\chi(\Gamma)$.

   Because χ is non-void we have $\chi(\Gamma) \nvdash_{\Sigma'} \chi(\rho)$. We have that $\chi(\Gamma \cup \{\neg\rho\})$ is consistent. If $\chi(\Gamma \cup \{\neg\rho\})$ is not consistent then $\Gamma \cup \{\neg\rho\}$ is not consistent which implies $\Gamma \vdash \neg\neg\rho$ and by *Double negation elimination* we obtain $\Gamma \vdash \rho$ which is a contradiction with our assumption. By the first hypothesis of the theorem and Lemma 9.3.11 (when the sentences of I are formed without quantifiers we apply Lemma 9.3.12) the condition $\chi(\Gamma \cup \{\neg\rho\})$

(of the canonical forcing property $\mathbb{P} = (P, \leq, f)$) belongs to a generic set. By Theorem 9.2.9 there exists a generic D-reachable Σ'-model M' for the condition $\chi(\Gamma \cup \{\neg\rho\})$. By Corollary 9.3.9 $M' \models \chi(\Gamma \cup \{\neg\rho\})$ and by satisfaction condition $M' \restriction_\chi \models \Gamma \cup \{\neg\rho\}$ which implies $\Gamma \not\models \rho$.

2. The implication from left to right is obvious. Therefore we will focus on the converse implication. Assume that $\Gamma \not\models_\Sigma \rho$. By completeness of FOES of I we have $\Gamma \not\vdash_\Sigma \rho$ and by the first part of the proof for any (D, D^l)-extension $\chi : \Sigma \to \Sigma'$ of Σ there exists a D-reachable model M' such that $M' \models \chi(\Gamma \cup \{\neg\rho\})$ which implies $M' \restriction_\chi \not\models (\Gamma \Rightarrow \rho)$.

(Q.E.D.)

9.3.2 Working Examples

Let $\mathbf{FOL}'$ be the institution which restricts **FOL** to

1. signatures with a countable number of symbols, and
2. sentences which allows quantifications over variables of non-void sorts.

Let $\mathbf{FOL}'_{\omega_1,\omega}$ be the infinitary extension of $\mathbf{FOL}'$ which allows disjunctions of countable sets of sentences. The followings are Corollaries of Theorem 9.3.13.

Corollary 9.3.14. *The FOES of* $\mathbf{FOL}'$ *is complete.*

Proof. In this case

- D^l is the class of all signature extensions with a finite number of constants of non-void sorts,
- D is the class of signature extensions with constants of any sort, and
- the atomic entailment system is the one defined in Proposition 8.3.11.

Since the set of sentences of any given signature is countable, by Theorem 9.3.13 the FOES of $\mathbf{FOL}'$ is complete. (Q.E.D.)

Corollary 9.3.15. *In* $\mathbf{FOL}'_{\omega_1,\omega}$ *we have*

$$\Gamma \models_\Sigma \rho \textit{ implies } \Gamma \vdash_\Sigma \rho$$

for all countable sets Γ *of sentences and any sentence* ρ.

Proof. As in the case of $\mathbf{FOL}'$

- D^l is the class of all signature extensions with a finite number of constants of non-void sorts,
- D is the class of signature extensions with constants of any sort, and
- the atomic entailment system is similar to the one defined in Proposition 8.3.11.

The result follows directly from Theorem 9.3.13 by considering the first subcase of the first hypothesis. (Q.E.D.)

The following is a corollary of Theorems 8.3.4 and 9.3.13.

Corollary 9.3.16. *The GUWES of* **UFOL** *is complete.*

Proof. By Theorem 9.3.13 we obtain the completeness of the FOES for the restriction of **UFOL** to the sentences formed without quantifiers. By Theorem 8.3.4 we lift it to the completeness of the GUWES of **UFOL**. (Q.E.D.)

Corollary 9.3.17. *The GUWES of* $\mathbf{UFOL}_\infty$ *is complete.*

Proof. Similarly to the proof of Corollary 9.3.16 (Q.E.D.)

Let $\mathbf{CFOL}'$ be the institution which restricts **CFOL** to

1. signatures with a countable number of symbols, and
2. sentences $(\forall X)\rho$, where X is a finite set of variables of constrained sorts, and ρ is formed over the atoms by applying Boolean connectives and quantifications over variables of loose sorts that are non-void.

The followings are consequences of Theorems 8.3.2, 9.3.13 and 8.4.3.

Corollary 9.3.18. *The WES with (universal and existential) quantifiers, disjunctions, negations and false generated by the rules of* Reflexivity, Transitivity, Congruence, PCongruence, Substitutivity *and* Case splitting *is* Ω*-complete for* $\mathbf{CFOL}'$*, where* $\Gamma \subseteq \Omega_\Sigma$ *iff* (Σ, Γ) *is a sufficient complete specification.*

Proof. Firstly, we define $\mathbf{GFOL}'$ as the restriction of **GFOL** to

1. signatures with a countable number of symbols, and
2. sentences $(\forall X)\rho$, where X is a set of variables of constrained sorts, and ρ is formed over the atoms by applying Boolean connectives and quantifications over variables of loose sorts that are non-void.

We prove that RUWES of $\mathbf{GFOL}'$ is Ω-complete. Assume that

- D^c is the class of all signature extensions with a finite number of constants of constrained sorts,
- D^l is the class of all signature extensions with a finite number of constants of loose sorts that are non-void,
- D is the class of signature extensions with constants of any sort, and
- the atomic entailment system is the one defined in Proposition 8.3.11.

By Theorem 9.3.13 we obtain that the FOES of the restriction of $\mathbf{GFOL}'$ to the "first-order" sentences formed without quantifications over variables of constrained sorts is complete. By Theorem 8.3.2 we lift the completeness of the FOES to the Ω-completeness of the RUWES of $\mathbf{GFOL}'$ which is relative to the class of all reachable models.

Secondly we define an institution morphism $\Delta_{FOL} : \mathbf{GFOL}' \to \mathbf{CFOL}'$, similarly as $\Delta_{\mathbf{HCL}} : \mathbf{GHCL} \to \mathbf{CHCL}$ defined in the previous chapter, and by Theorem 8.4.3 we obtain the Ω-completeness of $\mathbf{CFOL}'$. (Q.E.D.)

The following is a corollary of Theorems 8.3.2, 8.3.4, 9.3.13, and 8.4.3.

Corollary 9.3.19. *The WES of* **CUFOL** *is* Ω*-complete, where* $\Gamma \subseteq \Omega_\Sigma$ *iff* (Σ, Γ) *is a sufficient complete specification.*

Proof. Similar to the proof of Corollary 9.3.18. (Q.E.D.)

We have introduced the forcing technique in institution model theory; using this we have proved the completeness of the first-order entailment systems in the abstract institutional setting and then we applied the result to

- **FOL**$'$ and $\mathbf{FOL}'_{\omega_1,\omega}$, the restrictions of **FOL** and $\mathbf{FOL}_{\omega_1,\omega}$ to
  - signatures with a countable number of symbols, and
  - sentences formed with quantifications over variables of non-empty sorts;
- **UFOL** and $\mathbf{UFOL}_\infty$.

The presentation given in this chapter in slightly different from [29], and it allows us to link the first-order completeness results to the ones in [28] presented also in the previous chapter. Thus, the results for the institutions **CFOL**$'$ and **CUFOL** are developed for the first time here. We instantiate our results only to first-order logic but one may easily formulate similar corollaries for order-sorted, preorder, and partial algebras, and also to combinations of these logics; thus, we obtain that the proof rules for **CUOSAP** given in Chapter 7 are sound and complete.

Chapter 10

Partial First-order Logic

Note that all the examples of institutions given contain either total or partial operation symbols. In this chapter we extend the previous institutional framework and results regarding the universal institutions for the class of logics which have both partial and total operation symbols and quantifications over total constant/variable symbols such as partial first-order logic (**PFOL**). This institution underlies CASL language [2] which have been designed for the specification and development of modular software systems.

Example 29 (The institution of partial first-order logic (**PFOL**) [13, 51])**.** A signature in **PFOL** is a tuple (S, TF, PF) such that $(S, TF \cup PF)$ is an algebraic signature. TF is the set of total operations and PF is the set of partial operations. **PFOL** do not contain the distinguished (partial) constant $\perp$. A morphism of **PFOL** signatures $\varphi : (S, TF, PF) \to (S', TF', PF')$ is just a morphism of algebraic signatures $(S, TF \cup PF) \to (S', TF' \cup PF')$ such that $\varphi(TF) \subseteq TF'$ and $\varphi(PF) \subseteq PF'$.

A partial algebra M for a **PFOL** signature (S, TF, PF) is just like an ordinary algebra but interpreting the operations of PF as partial functions, which means that M_σ might be undefined for some arguments. A partial algebra homomorphism $h : M \to N$ is a family of (total) functions $\{h_s : M_s \to N_s\}_{s \in S}$ indexed by the set of sorts S of the signature such that $h_w(M_\sigma(a)) = N_\sigma(h_s(a))$ for each operation symbol $\sigma : w \to s$ and each string of arguments $a \in M_w$ for which $M_\sigma(a)$ is defined.

The sentences have three kinds of atoms: *definedness* $def(\_)$, *strong* equality $\overset{s}{=}$ and existence equality $\overset{e}{=}$. The *definedness* $def(t)$ of a term t holds in a partial algebra M when the interpretation M_t of t is defined. The strong equality $t_1 \overset{s}{=} t_2$ holds when both terms are undefined or both of them are defined and are equal. The existence equality $t_1 \overset{e}{=} t_2$ holds when both terms are defined and are equal. The sentences are formed from these atoms by means of Boolean connectives and quantification over total (first-order) variables. Notice that each definedness atom $def(t)$ is semantically equivalent with $t \overset{e}{=} t$ and any strong equality $t_1 \overset{s}{=} t_2$ is semantically equivalent with $(def(t_1) \vee def(t_2)) \Rightarrow t_1 \overset{e}{=} t_2$.

By restricting the sentences to universal sentences and universal Horn sentences formed over the existential equalities, we obtain **UPFOL** and **HPFOL**, respectively. Their infinitary versions are obtained by allowing infinitary universal sentences.

Notations. Let $\Sigma = (S, TF, PF)$ be a signature in **PFOL** and M a Σ-model.

1. We denote by T_M the Σ-model with the carrier sets $\{t \in T_{TF \cup PF} \mid M \models def(t)\}$ and interpreting each operation symbol $\sigma \in TF \cup PF$ as a (partial) function $(T_M)_\sigma : (T_M)_{s_1} \times \ldots \times$

$(T_M)_{s_n} \to (T_M)_s$ defined by $(T_M)_\sigma(t_1,\ldots,t_n) = \sigma(t_1,\ldots,t_n)$ when $M \models def(\sigma(t_1,\ldots,t_n))$, and undefined otherwise. If $\sigma \in TF_{s_1\ldots s_n \to s}$ and $t_i \in (T_M)_{s_i}$ for all $i \in \{1,\ldots,n\}$ then $(T_M)_\sigma$ is totaly defined. Note that there exists an unique morphism $T_M \to M$ given by the unique interpretations of terms in T_M into the model M.

2. If X is a set of new total constant symbols, then an interpretation for X is just a (many-sorted total) function $f : X \to M$. As in **FOL** a (S,TF,PF)-algebra M and a function $f : X \to M$ give an interpretation in M of $\Sigma(X)$, where $\Sigma(X) = (S, TF \cup X, PF)$, allowing the pair (M, f) to be seen as a $\Sigma(X)$-algebra.

Example 30 (Constructor-based partial first-order logic (**CPFOL**)). The signatures of constructor-based partial first-order logic (S,TF,TF^c,PF,PF^c) consist of a partial first-order signature (S,TF,PF), and a distinguished set of both *total constructors* $TF^c \subseteq TF$ and *partial constructors* $PF \subseteq PF^c$. The constructors determine the set of *constrained* sorts $S^c \subseteq S$: $s \in S^c$ iff there exists a constructor $\sigma \in TF^c_{w\to s}$ or $\sigma \in PF^c_{w\to s}$ with the result sort s, and the set of *loose* sorts $S^l = S - S^c$.

The (S,F,F^c)-sentences are the *universal constrained first-order sentences* of the form $(\forall X)\rho$ where X is a finite set of variables of constrained sorts, and ρ is a formula with quantifications over variables of loose sorts only.

The (S,TF,TF^c,PF,PF^c)-models are the usual partial (S,TF,PF)-algebras M with the carrier sets for the constrained sorts consisting of interpretations of terms formed with constructors and elements of loose sorts, i.e. there exists

1. a set $Y = (Y_s)_{s\in S}$ of total variables of loose sorts, and

2. a function $f : Y \to M$

such that for every constrained sort $s \in S^c$ the function $f^\#_s : (T_{(M,f)})_s \to M_s$ is a surjection, where

1. $T_{(M,f)} \subseteq T_{TF^c \cup PF^c}(Y)$ is the maximal partial $(S, TF^c \cup Y, PF^c)$-algebra of terms such that $(M, f) \models def(t)$ for all $t \in T_{(M,f)}$, and

2. $f^\# : T_{(M,f)} \to (M, f)$ is the unique $(S, TF^c \cup Y, PF^c)$-morphism.

A constructor-based first-order signature morphisms

$$\varphi : (S,TF,TF^c,PF,PF^c) \to (S_1,TF_1,TF^c_1,PF_1,PF^c_1)$$

is a **PFOL**-signature morphism $\varphi : (S,TF,PF) \to (S_1,TF_1,PF_1)$ such that

1. constructors are preserved along signature morphisms: if $\sigma \in TF^c \cup PF^c$ then $\varphi(\sigma) \in TF^c_1 \cup PF^c_1$, and

2. no "new" constructors are introduced for "old" constrained sorts: if $\sigma_1 \in (TF^c_1)_{w_1\to s_1} \cup (PF^c_1)_{w_1\to s_1}$ and $s_1 \in \varphi(S^c)$ then there exists $\sigma \in TF^c \cup PF^c$ such that $\varphi(\sigma) = \sigma_1$.

CPFOL$_{\omega_1,\omega}$ is the infinitary extension of **CPFOL** obtained by allowing countable disjunctions for construction of the first-order part of sentences, i.e. the **CPFOL**$_{\omega_1,\omega}$ sentences $(\forall X)\rho$ are **CPFOL** sentences such that the first-order part ρ which contains quantifications over (total) variables of loose sorts only, may be formed by applying disjunctions to countable sets of sentences. **CPFOL**$_{\omega_1,\omega}$ is a D^c-universal institution over its restriction to infinitary first-order

sentences built over the atoms by applying disjunctions to countable sets of sentences, negations, false, and quantifications over finite sets of (total) variables of loose sorts, where D^c is the subcategory of signature morphisms which consists of signature extensions with finite number of total constants of constrained sorts.

CUPFOL, **CHPFOL** are defined by restricting the sentences of **CPFOL** as in the previous cases. Their infinitary variants are obtained by allowing infinitary universal sentences.

Example 31 (Generalized partial first-order logic (**GPFOL**)). The signatures (S, S^c, TF, PF) consist of a first-order signature (S, TF, PF) and a distinguished set of sorts $S^c \subseteq S$. We call the set of sorts S^c *constrained* and $S^l = S - S^c$ *loose*. A *generalized partial first-order signature morphism* between (S, S^c, F, P) and (S_1, S_1^c, F_1, P_1) is a simple signature morphism (we do not allow mappings of constants into terms as in the previous cases). The sentences are the *universal constrained first-order sentences* of the form $(\forall X)e$, where X is a finite set of total variables of constrained sorts and e is a formula formed over atoms by applying Boolean connectives and quantifications over total variables of loose sorts. Models are the usual **PFOL**-models and the satisfaction is inherited from **PFOL**. Note that **GPFOL** is a D^c-universal institution over its restriction to first-order sentences built over the atoms by applying Boolean connectives and quantifications over total variables of loose sorts, where D^c is the class of signature extensions with finite number of total constants of constrained sorts.

The variants of **GPFOL** are defined similarly as in the previous cases.

10.1 PFOL-Substitutions

Given a **PFOL** signature (S, TF, PF) and two sets of new total constants X and Y, a *first-order* (S, TF, PF)*-substitution* from X to Y consists of a mapping $\theta : X \to T_{TF \cup PF}(Y)$ of the variables X with $(TF \cup PF)$-terms over Y. Let $def(\theta)$ to denote the set $\{def(\theta(x)) \mid x \in X\}$ of $(S, TF \cup Y, PF)$-sentences.

On the semantics side, each (S, TF, PF)-substitution $\theta : X \to T_{TF \cup PF}(Y)$ determines a functor $\mathbb{M}od(\theta) : \mathbb{M}od((S, TF \cup Y, PF), def(\theta)) \to \mathbb{M}od(S, F \cup X, P)$ defined by

- $\mathbb{M}od(\theta)(M)_x = M_x$ for each sort $x \in S$, or operation symbol $x \in TF \cup PF$, and
- $\mathbb{M}od(\theta)(M)_x = M_{\theta(x)}$, i.e. the evaluation of the term $\theta(x)$ in M, for each $x \in X$. Notice that since $M \models def(\theta)$ the term $\theta(x)$ which may contain partial operation symbols is evaluated in the model M.

On the syntax side, θ determines a sentence translation function $\mathbb{S}en(\theta) : \mathbb{S}en(S, TF \cup X, PF) \to \mathbb{S}en(S, TF \cup Y, PF)$ which in essence replaces all symbols from X with the corresponding $(TF \cup Y \cup PF)$-terms according to θ

- $\mathbb{S}en(\theta)(t_1 \stackrel{e}{=} t_2)$ is defined as $\overline{\theta}(t) \stackrel{e}{=} \overline{\theta}(t')$ for each $(S, TF \cup X, PF)$-existence equation $t_1 = t_2$, where $\overline{\theta} : T_{TF \cup PF}(X) \to T_{TF \cup PF}(Y)$ is the unique extension of θ to an $(TF \cup PF)$-homomorphism ($\overline{\theta}$ is replacing variables $x \in X$ with $\theta(x)$ in each $(TF \cup X \cup PF)$-term t).
- $\mathbb{S}en(\theta)(\rho_1 \vee \rho_2)$ is defined as $\mathbb{S}en(\theta)(\rho_1) \vee \mathbb{S}en(\theta)(\rho_2)$ for each disjunction $\rho_1 \vee \rho_2$ of $(S, TF \cup X, PF)$-sentences, and similarly for the case of any other Boolean connectives.

- $\mathbb{S}en(\theta)((\forall Z)\rho)$ is defined as $(\forall Z)\mathbb{S}en(\theta_Z)(\rho)$ for each $(S, TF \cup X \cup Z, PF)$-sentence ρ, where θ_Z is the trivial extension of θ to a $(S, TF \cup Z, PF)$-substitution [1].

The satisfaction condition is given by the proposition bellow.

Proposition 10.1.1 (Satisfaction condition for **PFOL**-substitutions)**.** *For each* **PFOL** *signature and each* (S, TF, PF)*-substitution*
$\theta : X \to T_{TF \cup PF}(Y)$

$$\mathbb{M}od(\theta)(M) \models \rho \textit{ iff } M \models \mathbb{S}en(\theta)(\rho)$$

for each $(S, TF \cup Y, PF)$*-model* M *which satisfies* $def(\theta)$ *and each* $(S, TF \cup X, PF)$*-sentence* ρ.

Proof. By induction on the structure of the sentence ρ and by noticing that $\mathbb{M}od(\theta)(M)_t = M_{\overline{\theta}(t)}$ for each $(TF \cup X \cup PF)$-term t. (Q.E.D.)

10.2 General Substitutions

The satisfaction condition property expressed above permits the definition of a general concept of substitution by abstracting

- **PFOL** signatures (S, TF, PF) to signatures Σ in arbitrary institutions, and
- sets of first order variables X for (S, TF, PF) to signature morphisms $\Sigma \to \Sigma_1$.

For any signature Σ of an institution, and each span $\{\Sigma_1 \xleftarrow{\chi_1} \Sigma \xrightarrow{\chi_2} \Sigma_2\}$ of signature morphisms, a Σ-*substitution* [21] $\theta : \chi_1 \to \chi_2$ consists of a pair $(\mathbb{S}en(\theta), \mathbb{M}od(\theta))$, where

1. $\mathbb{S}en(\theta) : \mathbb{S}en(\Sigma_1) \to \mathbb{S}en(\Sigma_2)$ is a function and
2. $\mathbb{M}od(\theta) : \mathbb{M}od(\Sigma_2) \to \mathbb{M}od(\Sigma_1)$ is a functor,

such that both of them preserve Σ, i.e. the following diagrams commute:

$$\begin{tikzcd}
\mathbb{S}en(\Sigma_1) \arrow[rr, "\mathbb{S}en(\theta)"] & & \mathbb{S}en(\Sigma_2) \\
& \mathbb{S}en(\Sigma) \arrow[ul, "\mathbb{S}en(\chi_1)"] \arrow[ur, "\mathbb{S}en(\chi_2)"'] &
\end{tikzcd}
\qquad
\begin{tikzcd}
\mathbb{M}od(\Sigma_1) \arrow[dr, "\mathbb{M}od(\chi_1)"'] & & \mathbb{M}od(\Sigma_2) \arrow[ll, "\mathbb{M}od(\theta)"'] \arrow[dl, "\mathbb{M}od(\chi_2)"] \\
& \mathbb{M}od(\Sigma) &
\end{tikzcd}$$

and such that the following Satisfaction Condition holds:

$$\mathbb{M}od(\theta)(M_2) \models \rho_1 \text{ if and only if } M_2 \models \mathbb{S}en(\rho_1)$$

for each Σ_2-model M_2 and each Σ_1-sentence ρ_1.

We sometimes let $\_\restriction_\theta$ denote the functor $\mathbb{M}od(\theta)$ and θ denote the sentence translation $\mathbb{S}en(\theta)$. In **PFOL**, given a (S, TF, PF)-substitution $\theta : X \to T_{TF \cup PF}(Y)$ we may consider

1. $\chi_1 : (S, TF, PF) \hookrightarrow (S, TF \cup X, PF)$ and $\chi_2 : (S, TF, PF) \hookrightarrow ((S, TF \cup Y, PF), def(\theta))$
2. $\mathbb{S}en(\theta) : \mathbb{S}en(S, TF \cup X, PF) \to \mathbb{S}en((S, TF \cup Y, PF), def(\theta))$, and

[1] Without loss of generality we may assume that variables in Z are distinct from variables in Y

3. $\mathbb{M}od(\theta) : \mathbb{M}od((S,TF,cupY,PF),def(\theta)) \to \mathbb{M}od(S,TF \cup X,PF)$

with the definition given in the previous section which is actually a substitution in the institution of presentations $\mathbf{PFOL}^{pres}$. In fact in **PFOL** the expansion of a model with the carrier sets consisting of interpretations of terms along a signature extension with (total) constants determines a substitution in $\mathbf{PFOL}^{pres}$ rather than **PFOL** which makes impossible to apply the framework developed in the Chapters 8 and 9 to partial first-order logic.

10.3 Reachability - revisited

We give the definition of reachable models parameterized by a class S of substitutions. Consider an institution $I = (\mathbb{S}ig, \mathbb{S}en, \mathbb{M}od, \models)$ with a broad subcategory of signature morphisms D, and a sub-functor $\mathbb{S}en_b \subseteq \mathbb{S}en$. We say that a substitution $\theta : (\Sigma \xrightarrow{\chi} \Sigma') \to (\Sigma \xrightarrow{\varphi} (\Sigma'', B))$ in I^{pres} is a $(D, \mathbb{S}en_b)$-substitution when $\chi, \varphi \in D$ and $B \subseteq \mathbb{S}en_b(\Sigma'')$.

Definition 10.3.1. *Let $I = (\mathbb{S}ig, \mathbb{S}en, \mathbb{M}od, \models)$ be an institution and S a class of $(D, \mathbb{S}en_b)$-substitutions for I. A Σ-model M is S-reachable if for each span $\Sigma_1 \xleftarrow{\chi} \Sigma_0 \xrightarrow{\varphi} \Sigma$ of signature morphisms in D, each χ-expansion N of $M \restriction_\varphi$ generates a substitution $\theta : (\Sigma_0 \xrightarrow{\chi} \Sigma_1) \to (\Sigma_0 \xrightarrow{\varphi} (\Sigma, B))$ in S such that $M \models B$ and $M \restriction_\theta = N$.*

In the previous definition of reachability the parameters $\mathbb{S}en_b$ and S were fixed. For each signature Σ we had $\mathbb{S}en_b(\Sigma) = \emptyset$ and S consisted of morphisms in comma category of signature morphisms. We fix the parameters for **PFOL**:

1. D to consists of signature extension with total constant symbols,
2. $\mathbb{S}en_b(S,TF,PF) = \{def(t) \mid t \in T_{TF \cup PF}\}$, and
3. S to consists of substitutions defined above $\theta : X \to T_{TF \cup PF}(Y)$, where (S,TF,PF) is a **PFOL** signature.

Proposition 10.3.2. *In* **PFOL** *a model M is S-reachable iff it consists of interpretations of terms.*

Proof. Let $\Sigma = (S,TF,PF)$ be a signature and assume a Σ-model M which is S-reachable. We prove that $T_M \to M$ is surjective, where $T_M = \{t \in T_{TF \cup PF} \mid M \models def(t)\}$. We show that for every $m \in M$ there exists $t \in T_{TF \cup PF}$ such that $M_t = m$. Consider a total constant x of sort s and let N be an expansion of M along $\Sigma \hookrightarrow \Sigma(\{x\})$ (where $\Sigma(\{x\}) = (S, TF \cup \{x\}, PF)$) which interprets the constant symbol x as m. Since M is S-reachable there exists a substitution $\theta : \{x\} \to T_{TF \cup PF}$ such that $M \restriction_\theta = N$. Take $t = \theta(x)$ and we have $M_t = M_{\theta(x)} = (M \restriction_\theta)_x = N_x = m$.

For the converse implication let $\Sigma = (S,TF,PF)$ be a signature, X and Y two disjoint sets of total constants with elements which are different from the symbols in Σ, and (M,h) a $\Sigma(Y)$-model with elements which are interpretation of terms, i.e. the unique morphism $h^\# : T_{(M,h)} \to (M,h)$ is a surjection. For each $\Sigma(X)$-model (M,g) there exists a function $\theta' : X \to T_{(M,h)}$ such that $\theta'; (h^\# \restriction_\Sigma) = g$.

$$\begin{tikzcd}
T_{(M,h)} \restriction_\Sigma \arrow[rr, "h^\# \restriction_\Sigma"] & & M \\
& X \arrow[ul, dotted, "\theta'"] \arrow[ur, "g"'] &
\end{tikzcd}$$

Note that $T_{(M,h)} \restriction_\Sigma \subseteq T_{TF\cup PF}(Y)$. We define the substitution $\theta : X \to T_{TF\cup PF}(Y)$ by $\theta(x) = \theta'(x)$ for all $x \in X$, and we have $(M,h) \restriction_\theta = (M, \theta'; h^\# \restriction_\Sigma) = (M,g)$. (Q.E.D.)

Definition 10.3.3. *Let $I = (\mathbb{S}ig, \mathbb{S}en, \mathbb{M}od, \models)$ be an institution and S a class of $(D, \mathbb{S}en_b)$-substitutions for I. Let $D^c, D^l \subseteq D$ be two broad subcategories of signature morphisms. We say that Σ-model M is (S, D^c, D^l)-reachable if for every signature morphism $\Sigma \xrightarrow{\chi} \Sigma'$ in D^c and each χ-expansion M' of M there exists a signature morphism $\Sigma \xrightarrow{\varphi} \Sigma''$ in D^l, a substitution $\theta : (\Sigma \xrightarrow{\chi} \Sigma') \to (\Sigma \xrightarrow{\varphi} (\Sigma'', B))$ in S and a (Σ'', B)-model M'' such that $M'' \restriction_\theta = M'$.*

Proposition 10.3.4. *In* **GPFOL**, *a Σ-model M is (S, D^c, D^l)-reachable, where the signature Σ is (S, S^c, TF, PF), iff there exists a set Y of total constants of loose sorts and a function $h : Y \to M$ such that for every constrained sort $s \in S^c$ the function $h^\#_s : (T_{(M,h)})_s \to (M,h)_s$ is surjective, where $h^\# : T_{(M,h)} \to (M,h)$ is the unique $\Sigma(Y)$-morphism.*

Proof. For the direct implication we define the set of (loose) variables Y as follows: $Y_s = \emptyset$ for all $s \in S^c$ and Y_s is a renaming of the elements M_s for all $s \in S^l$ such that $Y_s \cap Y_{s'}$ whenever $s \neq s'$. So, there exists a S-sorted function $h : Y \to M$ surjective on loose components, i.e. $h_s : Y_s \to M_s$ is surjective for all $s \in S^l$. We prove that for every constraint sort $s' \in S^c$ and element $m \in M_{s'}$ there exists a term $t \in T_{(M,h)}$ such that $h^\#(t) = m$, where $h^\# : T_{(M,h)} \to (M,h)$ is the unique $\Sigma(Y)$-morphism.

Let $m \in M_{s'}$ with $s' \in S^c$. Let x be a variable and (M,g) be a $\Sigma(\{x\})$-algebra such that $g(x) = m$. By hypothesis there exists a finite set Z of total constant symbols of loose sorts, a $\Sigma(Z)$-algebra (M, f) and a substitution $\theta : \{x\} \to T_{TF\cup PF}(Z)$ such that $(M, f) \restriction_\theta = (M,g)$.

Assume that $t = \theta(x)$ and let $\{z_1, \ldots, z_n\}$ all the variables in t. We define the $\Sigma(Y)$-term $t' = t(z_1 \leftarrow h^{-1}(f(z_1)), \ldots, z_1 \leftarrow h^{-1}(f(z_n)))$ and the substitution $\theta' : \{x\} \to T_{TF\cup PF}(Y)$ by $\theta'(x) = t'$.

$$\begin{tikzcd}
 & \Sigma(Y) \\
\Sigma(\{x\}) \arrow[ur, dotted, "\theta'"] \arrow[r, dotted, "\theta"] & \Sigma(Z) \\
 & \Sigma \arrow[ul, hook] \arrow[u, hook]
\end{tikzcd}$$

We have $m = (M,g)_x = ((M, f) \restriction_\theta)_x = (M, f)_{\theta(x)} = M_t(f(z_1) \ldots, f(z_n)) = M_{t'}(h(h^{-1} f(z_1)), \ldots, h(h^{-1} f(z_n))) = (M,h)_{t'}$ [2].

For the converse implication let Y be a set of total variables of loose sorts, and $h : Y \to M$ a function such that for every constrained sort $s \in S^c$ the function $h^\#_s : (T_{(M,h)})_s \to (M,h)_s$ is surjective, where $h^\# : T_{(M,h)} \to (M,h)$ is the unique $\Sigma(Y)$-morphisms. Assume a finite set X of total constant symbols and (M,g) a $\Sigma(X)$-expansion of M. Reasoning similarly as in Proposition 10.3.2 there exists a substitution $\theta : X \to T_{(TF\cup PF)}(Y)$ such that $(M,h) \restriction_\theta = (M,g)$. Now let $Y' \subseteq Y$ be the least subset such that $\theta(x) \in T_{TF\cup PF}(Y')$ for all $x \in X$. Since X is finite we have

[2] For every term $t \in (T_{TF\cup PF}(\{z_1 : s_1, \ldots, z_m : s_n\}))_s$ the derived partial operation $M_t : M_{s_1} \times, \ldots, \times M_{s_m} \to M_s$ is defined by $M_t(m_1, \ldots, m_n) = a^\#(t)$ when $t \in T_{(M,a)}$ and undefined otherwise, where $a : \{z_1 : s_1, \ldots, z_m : s_n\} \to M$, $a(z_i) = m_i$ for all $i \in \{1, \ldots, n\}$, and $a^\# : T_{(M,a)} \to (M,a)$ is the unique $\Sigma(\{z_1 : s_1, \ldots, z_m : s_n\})$-morphism.

that Y' is finite.

$$\begin{tikzcd}
 & \Sigma(Y) \\
\Sigma(X) \arrow[ur, dotted, "\theta"] \arrow[r, dotted, "\theta'"] & \Sigma(Y') \arrow[u, hook] \\
 & \Sigma \arrow[ul, hook] \arrow[ur, hook]
\end{tikzcd}$$

(Q.E.D.)

Let $h' : Y' \to M$ be the restriction of $h : Y \to M$ to Y'. Note also that $(M,h) \restriction_{\Sigma(Y')} = (M,h')$ and $(M,h') \restriction_{\theta'} = (M,h) \restriction_{\theta} = (M,g)$.

As in the previous cases of institutions since the parameters D, D^c, D^l, $\mathbb{S}en_b$ and S are fixed, we call

1. S-reachable models ground reachable, and
2. (S, D^c, D^l)-reachable models reachable models.

Lemma 10.3.5. *In* **PFOL**, *for each set E of existence equations is basic and moreover there exists a ground reachable model M_E defining E as basic set of sentences.*

Proof. In **PFOL**, for a set E of existence (S, TF, PF)-equations we let S_E to be the set of subterms of the terms which appear in the existence equations in E. We also define $T_{TF}(S_E)$ as the partial algebra generated by the set of terms S_E. The basic model M_E will be the quotient of this algebra by the partial congruence induced by the existence equations in E. By Proposition 10.3.2 the model M_E is ground reachable. (Q.E.D.)

10.4 Universal Completeness - revisited

The reachable universal weak entailment system developed in this section consists of four layers but the proof rules are adapted for institutions with both partial and total operation symbols and having quantifications over total constant symbols.

Reachable universal weak entailment system(RUWES). Assume

1. a D^c-universal institution $I = (\mathbb{S}ig, \mathbb{S}en, \mathbb{M}od, \models)$ over $I_2 = (\mathbb{S}ig, \mathbb{S}en_2, \mathbb{M}od, \models)$ such that I_2 has D^l-quantifications for a subcategory $D^l \subseteq \mathbb{S}ig$ of signature morphisms,
2. a sub-functor $\mathbb{S}en_b \subseteq \mathbb{S}en_2$, a subcategory $D \subseteq \mathbb{S}ig$ of signature morphisms such that $D^c \subseteq D$ and $D^l \subseteq D$, and a class S of $(D, \mathbb{S}en_b)$-substitutions.
3. for each (finite) set of sentences $B \subseteq \mathbb{S}en_b(\Sigma)$ and any sentence $\rho \in \mathbb{S}en(\Sigma)$ there exists a sentence in $\mathbb{S}en(\Sigma)$ semantically equivalent with $\bigwedge B \Rightarrow \rho$.

For the finitary case we assume that for every substitution $\theta : (\Sigma \xrightarrow{\chi} \Sigma_1) \to (\Sigma \xrightarrow{\varphi} (\Sigma_2, B))$ the set B of sentences is finite whenever $\chi \in D^c$ or $\chi \in D^l$. This assumption is connected to the last condition above: for any substitution $\theta : (\Sigma \xrightarrow{\chi} \Sigma_1) \to (\Sigma \xrightarrow{\varphi} (\Sigma_2, B))$ and any Σ_1-sentence ρ there exists a Σ_2-sentence semantically equivalent with $\bigwedge B \Rightarrow \theta(\rho)$.

Remark 10.4.1. *Assume a D-universal institution $I = (\mathbb{S}ig, \mathbb{S}en, \mathbb{M}od, \models)$ over the institution $I_1 = (\mathbb{S}ig, \mathbb{S}en_1, \mathbb{M}od, \models)$, and a sub-functor $\mathbb{S}en_b \subseteq \mathbb{S}en_1$. For every set B of Σ-sentences in $\mathbb{S}en_b(\Sigma)$ and any Σ-sentence $(\forall\varphi)\rho \in \mathbb{S}en(\Sigma)$ we have*

1. *$\bigwedge B \Rightarrow (\forall\varphi)\rho$ is semantically equivalent with $(\forall\varphi)\bigwedge\varphi(B) \Rightarrow \rho$ [3], and*
2. *if $\rho = \bigwedge H \Rightarrow C$ then $\bigwedge B \Rightarrow (\forall\varphi)\bigwedge H \Rightarrow C$ is semantically equivalent with $(\forall\varphi)\bigwedge(\varphi(B) \cup H) \Rightarrow \rho$.*

Proof. Straightforward by using the standard interpretations of logical symbols. (Q.E.D.)

We define the general variants of the proof rules presented in Chapter 8:
(*Substitutivity*) $(\forall\chi)\rho \vdash_\Sigma (\forall\varphi)\bigwedge B \Rightarrow \theta(\rho)$, where$(\forall\chi)\rho$ is any Σ-sentence and $\theta : (\Sigma \xrightarrow{\chi} \Sigma_1) \to (\Sigma \xrightarrow{\varphi} (\Sigma_2, B))$ is a substitution in S.
(*Case splitting*) $\Gamma \vdash_\Sigma (\forall\chi)\rho$ if $\Gamma \vdash_\Sigma (\forall\varphi)\bigwedge B \Rightarrow \theta(\rho)$ for all substitutions $\theta : (\Sigma \xrightarrow{\chi} \Sigma_1) \to (\Sigma \xrightarrow{\varphi} (\Sigma_2, B))$ in S such that $\varphi \in D^l$, where $\Gamma \subseteq \mathbb{S}en(\Sigma)$ and $(\forall\chi)\rho \in \mathbb{S}en(\Sigma)$ with $\Sigma \xrightarrow{\chi} \Sigma' \in D^c$ and $\rho \in \mathbb{S}en_2(\Sigma')$.

Given a compact WES $E_2 = (\mathbb{S}ig, \mathbb{S}en_2, \vdash^2)$ for I_2, the RUWES of I consists of the least WES over E_2, closed under *Substitutivity* and *Case splitting*. This is the finitary version of the RUWES and is applicable to **GHPFOL**. Its infinitary variant is obtained by dropping the compactness condition, and by considering the infinitary WES of I; it is applicable to **GHPFOL**$_\infty$.

Proposition 10.4.2. *The RUWES of I is sound with respect to all (D^c, D^l)-reachable models if the WES of I_2 is sound with respect to all (D^c, D^l)-reachable models.*

Proof. By Proposition 8.2.3 it suffices to prove the soundness of the rules of *Case splitting* and *Substitutivity*.

We prove that *Case splitting* is sound with respect to all (S, D^c, D^l)-reachable models. Let Γ be a set of Σ-sentences and $(\forall\chi)\rho$ a Σ-sentence, where $\Sigma \xrightarrow{\chi} \Sigma' \in D^c$, and assume that for every (S, D^c, D^l)-reachable model M we have $M \models \bigwedge\Gamma \Rightarrow (\forall\varphi)(\bigwedge B \Rightarrow \theta(\rho))$ for all substitutions $\theta : (\Sigma \xrightarrow{\chi} \Sigma_1) \to (\Sigma \xrightarrow{\varphi} (\Sigma_2, B))$ in S such that $\varphi \in D^l$. Let M be a (S, D^c, D^l)-reachable Σ-model such that $M \models \Gamma$, and let M' be an arbitrary χ-expansion of M. We want $M' \models \rho$. Since M is (S, D^c, D^l)-reachable there exists a substitution $\theta : (\Sigma \xrightarrow{\chi} \Sigma_1) \to (\Sigma \xrightarrow{\varphi} (\Sigma_2, B))$, and an φ-expansion M'' of M which satisfies B such that $M'' \restriction_\theta = M'$. $M \models \Gamma$ implies $M \models (\forall\varphi)\bigwedge B \Rightarrow \theta(\rho)$ and $M'' \models B$ implies $M'' \models \theta(\rho)$ and by the satisfaction condition for substitutions $M' \models \rho$.

We prove that *Substitutivity* is sound with respect to all models. Let M be a Σ-model such that $M \models (\forall\chi)\rho$. Consider a substitution $\theta : (\Sigma \xrightarrow{\chi} \Sigma_1) \to (\Sigma \xrightarrow{\varphi} (\Sigma_2, B))$ and let M_2 be any φ-expansion of M. We want $M_2 \models \bigwedge B \Rightarrow \theta(\rho)$. Assuming that $M_2 \models B$ we have that $M_2 \restriction_\theta = M_1$ is a χ-expansion of M (since $(M_2 \restriction_\theta) \restriction_\chi = M_2 \restriction_\varphi$) which by hypothesis satisfies $(\forall\chi)\rho$; we obtain $M_2 \restriction_\theta \models \rho$ and by the satisfaction condition for substitutions $M_2 \models \theta(\rho)$. (Q.E.D.)

Theorem 10.4.3 (Reachable universal completeness)**.** *The RUWES of I is complete with respect to all (S, D^c, D^l)-reachable models if*

1. *the WES of I_2 is complete with respect to all (S, D^c, D^l)-reachable models (and compact), and*

[3] $\bigwedge B \Rightarrow (\forall\varphi)\rho$ and $(\forall\varphi)\bigwedge\varphi(B) \Rightarrow \rho$ are sentences in the meta-language; in concrete institutions $\bigwedge\varphi(B) \Rightarrow \rho$ will be replaced by a semantically equivalent sentence which belongs to the underlying institution.

2. *for each set of sentences $E \subseteq \mathbb{S}en_2(\Sigma)$ and each sentence $e \in \mathbb{S}en_2(\Sigma)$, we have $E \models e$ iff $M \models (\bigwedge E \Rightarrow e)$ for all (S, D^c, D^l)-reachable models M.*

Proof. Assume that for all (S, D^c, D^l)-reachable models M we have $M \models \bigwedge \Gamma \Rightarrow (\forall\chi)e'$, where $\Sigma \xrightarrow{\chi} \Sigma' \in D^c$. We want $\Gamma \vdash (\forall\chi)e'$. Suppose towards a contradiction that $\Gamma \nvdash (\forall\chi)e'$. Then there exists a substitution $\theta : (\Sigma \xrightarrow{\chi} \Sigma') \to (\Sigma \xrightarrow{\varphi} (\Sigma'', B))$ in S with $\varphi \in D^l$ such that $\Gamma \nvdash (\forall\varphi) \bigwedge B \Rightarrow \theta(e')$.

We define the set of Σ-sentences $\Gamma_2 = \{\rho \in \mathbb{S}en_2(\Sigma) \mid \Gamma \vdash \rho\}$.

We show that $\Gamma_2 \nvdash^2 (\forall\varphi) \bigwedge B \Rightarrow \theta(e')$. Assume that $\Gamma_2 \vdash^2 (\forall\varphi) \bigwedge B \Rightarrow \theta(e')$. For the infinitary case take $\Gamma' = \Gamma_2$. For the finitary case, since the WES of I_2 is compact, there exists a finite $\Gamma' \subseteq \Gamma_2$ such that $\Gamma' \vdash^2 (\forall\varphi) \bigwedge B \Rightarrow \theta(e')$ which implies $\Gamma' \vdash (\forall\varphi) \bigwedge B \Rightarrow \theta(e')$. Since $\Gamma \vdash \rho$ for all $\rho \in \Gamma'$ we have $\Gamma \vdash \Gamma'$. Hence, $\Gamma \vdash (\forall\varphi) \bigwedge B \Rightarrow \theta(e')$ which is a contradiction with our assumption.

We have $\Gamma_2 \nvdash^2 (\forall\varphi) \bigwedge B \Rightarrow \theta(e')$, and by the hypothesis there exists a (S, D^c, D^l)-reachable model M such that $M \models \Gamma_2$ and $M \not\models (\forall\varphi) \bigwedge B \Rightarrow \theta(e')$. Note that $M \not\models (\forall\varphi)B \Rightarrow \theta(e')$ implies $M \not\models (\forall\chi)e'$. If we have proved that $M \models \Gamma$ we have reached a contradiction with $\Gamma \models (\forall\chi)e'$.

Let $(\forall\chi_1)e_1 \in \Gamma$, where $\Sigma \xrightarrow{\chi_1} \Sigma_1 \in D^c$, and let N be any χ_1-expansion of M. We show $N \models e_1$. Since M is (S, D^c, D^l)-reachable there exists a substitution $\psi : (\Sigma \xrightarrow{\chi_1} \Sigma_1) \to (\Sigma \xrightarrow{\varphi_1} (\Sigma_2, B''))$, and a φ_1-expansion N' of M which satisfies B'' such that $N' \restriction_\theta = N$. By *Substitutivity* $(\forall\varphi_1) \bigwedge B'' \Rightarrow \psi(e_1) \in \Gamma_2$ which implies $M \models (\forall\varphi_1) \bigwedge B'' \Rightarrow \psi(e_1)$. Since N' is a φ_1-expansion of M which satisfies B'' we have $N' \models \psi(e_1)$ and by satisfaction condition $N' \restriction_\psi = N \models e_1$. (Q.E.D.)

Generic universal weak entailment systems (GUWES). Let us assume

1. a D^l-universal institution $I = (\mathbb{S}ig, \mathbb{S}en, \mathbb{M}od, \models)$ over I_1 with $\mathbb{S}en_1$ the sub-functor of $\mathbb{S}en$,

2. a sub-functor $\mathbb{S}en_b \subseteq \mathbb{S}en_1$, a subcategory $D \subseteq \mathbb{S}ig$ of signature morphisms such that $D^l \subseteq D$, and a class S of $(D, \mathbb{S}en_b)$-substitutions.

3. for each (finite) set of sentences $B \subseteq \mathbb{S}en_b(\Sigma)$ and any Σ-sentence ρ there exists a Σ-sentence semantically equivalent with $\bigwedge B \Rightarrow \rho$.

For the finitary case we assume that for every substitution $\theta : (\Sigma \xrightarrow{\chi} \Sigma_1) \to (\Sigma \xrightarrow{\varphi} (\Sigma_2, B))$ the set B of sentences is finite whenever $\chi \in D^l$.

Given a compact WES $E_1 = (\mathbb{S}ig, \mathbb{S}en_1, \vdash^1)$ for I_1, the GUWES of I consists of the least WES with universal quantifications over E_1, closed under *Substitutivity*. This is the finitary version of the GUWES, and is applicable to

1. **HPFOL**, and

2. the restriction of **GHPFOL** to the sentences quantified over finite sets of total variables of loose sorts.

Its infinitary variant is obtained by dropping the compactness condition, and by considering the infinitary WES for I; it is applicable to

1. **HPFOL**$_\infty$, and

2. the restriction of **GHPFOL**$_\infty$ to the sentences quantified over sets (possible infinite) of total variables of loose sorts.

Proposition 10.4.4. *The GUWES of I is sound (and compact) whenever the WES of I_1 is sound (and compact).*

Proof. By Proposition 8.2.3 and Corollary 3.3.11 it is suffices to prove the soundness of *Substitutivity* which may be found in the proof of Proposition 8.3.1.

For the compactness of the GUWES of I consider the compact sub-WES $E^c = (\mathbb{S}ig, Sen, \vdash^c)$ of $E = (\mathbb{S}ig, \mathbb{S}en, \vdash)$. It contains E_1 because E_1 is compact. Since the rules of *Substitutivity* are finitely generated we have that E^c satisfies *Substitutivity*. As in the proof of Proposition 8.3.3 we can prove E^c satisfies *Generalization* and then, because E is the least WES over E_1 satisfying the rules of *Substitutivity* and *Generalization*, we obtain $E^c = E$. (Q.E.D.)

Theorem 10.4.5 (Generic universal completeness)**.** *Assume that*

1. *the WES of I_1 is complete, and*
2. *for each set of sentences $E \subseteq \mathbb{S}en_1(\Sigma)$ and each sentence $e \in \mathbb{S}en_1(\Sigma)$, we have $E \models_\Sigma e$ iff $M \models_\Sigma (\bigwedge E \Rightarrow e)$ for all D-reachable models M.*

Then we have

1. *the GUWES of I is complete, and*
2. *$\Gamma \models_\Sigma (\forall\varphi)e'$, where $\Sigma \xrightarrow{\varphi} \Sigma' \in D^l$, iff $M \models_{\Sigma'} (\bigwedge \varphi(\Gamma) \Rightarrow e')$ for all D-reachable models M.*

Proof. 1. Assume that $\Gamma \models_\Sigma (\forall\varphi)e'$ where $\Sigma \xrightarrow{\varphi} \Sigma' \in D$. We want to show that $\Gamma \vdash_\Sigma (\forall\varphi)e'$. Suppose towards a contradiction that $\Gamma \not\vdash_\Sigma (\forall\varphi)e'$.

We define the set of Σ'-sentences $\Gamma_1^\varphi = \{\rho' \in \mathbb{S}en_1(\Sigma') | \Gamma \vdash_\Sigma (\forall\varphi)\rho'\}$.

Suppose $\Gamma_1^\varphi \vdash^1_{\Sigma'} e'$. For the infinitary case we take $\Gamma' = \Gamma_1^\varphi$. For the finitary case, since the WES of I_1 is compact, there exists a finite $\Gamma' \subseteq \Gamma_1^\varphi$ such that $\Gamma' \vdash^1 e'$. By *Generalization* $\varphi(\Gamma) \vdash_{\Sigma'} \rho'$ for all $\rho' \in \Gamma'$, which implies $\varphi(\Gamma) \vdash_{\Sigma'} \Gamma'$. $\Gamma_1^\varphi \vdash^1_{\Sigma'} e'$ implies $\Gamma_1^\varphi \vdash_{\Sigma'} e'$, and we obtain $\varphi(\Gamma) \vdash_{\Sigma'} e'$ and again by *Generalization* $\Gamma \vdash_\Sigma (\forall\varphi)e'$, which contradicts our assumption. Hence, $\Gamma_1^\varphi \not\vdash^1_{\Sigma'} e'$.

By completeness of I_1 $\Gamma_1^\varphi \not\models e'$. There exists a D-reachable model M such that $M \models \Gamma_1^\varphi$ but $M \not\models e'$. This implies $M \restriction_\varphi \not\models (\forall\varphi)e'$. If we proved that $M \restriction_\varphi \models \Gamma$ we reached a contradiction with $\Gamma \models (\forall\varphi)e'$. We will therefore focus on proving that $M \restriction_\varphi \models \Gamma$.

Let $(\forall\varphi_1)e_1 \in \Gamma$, where $\Sigma \xrightarrow{\varphi_1} \Sigma_1 \in D^l$, and let N be any φ_1-expansion of $M \restriction_\varphi$. We have to show that $N \models_{\Sigma_1} e_1$. Since M is S-reachable there exists a substitution $\theta : (\Sigma \xrightarrow{\varphi_1} \Sigma_1) \to (\Sigma \xrightarrow{\varphi} (\Sigma', B))$ in S such that $M \models_{\Sigma'} B$ and $M \restriction_\theta = N$. By *Substitutivity* we obtain $\Gamma \vdash_\Sigma (\forall\varphi) \bigwedge B \Rightarrow \theta(e_1)$ which implies $\bigwedge B \Rightarrow \theta(e_1) \in \Gamma_1^\varphi$. $M \models_{\Sigma'} \Gamma_1^\varphi$ implies $M \models_{\Sigma'} \bigwedge B \Rightarrow \theta(e_1)$ and since $M \models_{\Sigma'} B$ we obtain $M \models \theta(\rho)$; by the satisfaction condition $M \restriction_\theta = N \models e_1$.

2. The non-trivial implication is from right to left. Assume that $\Gamma \not\models_\Sigma (\forall\varphi)e'$, where $\Sigma \xrightarrow{\varphi} \Sigma' \in D^l$, then by soundness of the WES of I we have $\Gamma \nvdash (\forall\varphi)e'$. Using the first part of the proof we get a S-reachable Σ'-model M such that $M \models \varphi(\Gamma)$ and $M \not\models e'$. Therefore there exists a S-reachable model M such that $M \not\models \bigwedge \varphi(\Gamma) \Rightarrow e'$.

(Q.E.D.)

The following remark addresses the second condition of Theorem 10.4.3.

Remark 10.4.6. *Under the assumption of Theorem 10.4.5, for any subcategory $D^c \subseteq D$ of signature morphisms, we have $\Gamma \models_\Sigma (\forall\varphi)e'$ iff $M \models_\Sigma (\Gamma \Rightarrow (\forall\varphi)e')$ for all (S, D^c, D^l)-reachable models M.*

Proof. Almost identical with the proof of Remark 8.3.5. (Q.E.D.)

Weak entailment systems with implications (IWES). Assume

1. an institution $I = (\mathbb{S}ig, \mathbb{S}en, \mathbb{M}od, \models)$, a sub-functor $\mathbb{S}en_0 : \mathbb{S}ig \to \mathbb{S}et$ of $\mathbb{S}en$ such that
   - I admits all sentences of the form $(\bigwedge H \Rightarrow C)$, where H is a (finite) set of sentences in I_0 and C is a sentence in I_0, and
   - any sentence in I is of the form $(\bigwedge H \Rightarrow C)$ as above;

   we denote the institution $(\mathbb{S}ig, \mathbb{S}en_0, \mathbb{M}od, \models)$ by I_0;
2. a class S of $(D, \mathbb{S}en_b)$-substitutions such that $\mathbb{S}en_b \subseteq \mathbb{S}en_0$.

Given a compact WES $E_0 = (\mathbb{S}ig, \mathbb{S}en_0, \vdash^0)$ for I_0, the IWES of I consists of the least WES over E_0, closed under the rules of *Implications*. This is the finitary version of the IWES for I, and is applicable to the restrictions of **HPFOL** and **GHPFOL** to the quantifier-free sentences. Its infinitary variant is obtained by dropping the compactness condition and by considering the infinitary WES for I; it is applicable to the restrictions of **HPFOL**$_\infty$ and **GHPFOL**$_\infty$ to the quantifier-free sentences.

Proposition 10.4.7. *The WES of I is sound (and compact) whenever the WES of I_0 is sound (and compact).*

Proof. See the proof of Proposition 8.3.6. (Q.E.D.)

Theorem 10.4.8. *Let us assume that*

1. *the WES of I_0 is complete,*
2. *every set of sentences in I_0 is basic, and*
3. *for each set $B \subseteq \mathbb{S}en_0(\Sigma)$ there is a S-reachable model M_B defining B as basic set of sentences.*

Then we have

1. *the IWES of I is complete, and*
2. *$\Gamma \models \rho$ iff $M \models (\Gamma \Rightarrow \rho)$ for all S-reachable models M.*

Proof. Similar with the proof of Theorem 8.3.7. (Q.E.D.)

When we apply our results to **PFOL** and **GPFOL** we use Lemma 10.3.5 to adress to the second and third condition of Theorem 10.4.8 above.

Atomic weak entailment systems (AWES). In order to develop sound and complete universal WES for **PFOL**, **GPFOL** and their infinitary variants we need to define sound and complete WES for the 'atomic' layer of these institutions.

Proposition 10.4.9. *Let* **PFOL**$_0$ *be the restriction of* **PFOL** *to the atomic sentences. The WES of* **PFOL**$_0$ *generated by the rules bellow is sound, complete and compact.*

- (*Symmetry*) $t \stackrel{e}{=} t' \vdash t' \stackrel{e}{=} t$ *for any terms* t, t'
- (*Transitivity*) $\{t \stackrel{e}{=} t',\ t' \stackrel{e}{=} t''\} \vdash t \stackrel{e}{=} t''$ *for any terms* t, t', t''
- (*Congruence*) $\{t_i \stackrel{e}{=} t'_i,\ def(\sigma(t_1,\ldots,t_n)),\ def(\sigma(t'_1,\ldots,t'_n))\} \vdash \sigma(t_1,\ldots,t_n) \stackrel{e}{=} \sigma(t'_1,\ldots,t'_n)$ *for any* $\sigma \in TF \cup PF$
- (*Totality*) $\{def(t_i) \mid i = \overline{1,n}\} \vdash def(\sigma_t(t_1,\ldots,t_n))$ *for any* $\sigma_t \in TF$
- (*Subterm*) $def(\sigma(t_1,\ldots,t_n)) \vdash \{def(t_i) \mid i \in \overline{1,n}\}$ *for any* $\sigma \in TF \cup PF$

Proof. Soundness follows by simple routine check and compactness by applying Proposition 3.2.6 after noting that all the rules are finitely generated. For proving the completeness, for any set E of atoms for a signature (S, TF, PF) we define

$$\equiv_E = \{(t,t') | E \vdash t \stackrel{e}{=} t'\}$$

We use the following Lemma (which we prove later).

Lemma 10.4.10. *For every set of existence equations* $E \subseteq \mathbb{S}en(S, TF, PF)$ *we have that* $E \vdash def(t)$ *if and only if* $t \in M_{def(E)}$.

Firstly we prove that $\equiv_E$ is a congruence relation on $M_{def(E)}$. The reflexivity of $\equiv_E$ is given by the above Lemma. The first two rules ensure the symmetry and the transitivity of $\equiv_E$. By *Congruence* we have that $\equiv_E$ is a congruence relation on $M_{def(E)}$.

For each existence equation $t \stackrel{e}{=} t'$ we have $E \vdash t \stackrel{e}{=} t' \iff t \equiv_E t' \iff M_{def(E)}/_{\equiv_E} \models t \stackrel{e}{=} t'$. If $E \models t \stackrel{e}{=} t'$ then $M_{def(E)}/_{\equiv_E} \models t \stackrel{e}{=} t'$ which implies $E \vdash t \stackrel{e}{=} t'$.

of Lemma 10.4.10. "the only if part" one can easily prove by induction in the definition of $\vdash$ that $E \vdash t \stackrel{e}{=} t'$ implies $t, t' \in M_{def(E)}$.

"the if part" We prove this by induction on the structure of the term t. Let $\sigma(t_1,\ldots,t_n)$ be a term such that $t_i \in M_{def(E)}$, for all $i \in \{1,\ldots,n\}$. By the hypothesis induction we have $E \vdash def(t_i)$, for all $i \in \{1,\ldots,n\}$.

- if $\sigma \in TF$ then by *Totality* rule we obtain $E \vdash def(\sigma(t_1,\ldots,t_n))$

- if $\sigma \in PF$ then by the definition of $M_{def(E)}$ we have $\sigma(t_1,\ldots,t_n) \in S_E$. By the definition of S_E there exists an existence equation $t_1 \stackrel{e}{=} t_2 \in E$ such that $t \in S_{t_1 \stackrel{e}{=} t_2}$. Without loss of generality we assume that $t \in S_{def(t_1)}$. We have $E \vdash t_1 \stackrel{e}{=} t_2$ and $E \vdash t_2 \stackrel{e}{=} t_1$ which implies $E \vdash def(t_1)$. By *Subterm*, $def(t_1) \vdash def(t)$. So $E \vdash def(t)$. (Q.E.D.)

(Q.E.D.)

Similarly, we may define **GPFOL**$_0$ and prove that proof rules of **PFOL**$_0$ are sound and complete for **GPFOL**$_0$ too. The following is a corollary of Theorem 8.3.10.

Corollary 10.4.11. *[Completeness of* **GHPFOL***] The RUWES of* **GHPFOL** *generated by the rules* Case splitting, Substitutivity, Generalization, Implications, Reflexivity, Symmetry, Transitivity, Congruence *and* Totality *are sound and complete with respect to all reachable models.*

Constructor-based universal completeness.

As in the previous cases the completeness for **CPFOL** is obtained by borrowing the entailment system of **GPFOL** through an institution morphism, according to Theorem 8.4.3.

We define the institution morphism $\Delta_{\mathbf{HPFOL}} = (\phi, \alpha, \beta) : \mathbf{CHPFOL} \to \mathbf{GHPFOL}$ such that

1. the functor ϕ maps

   - every **CHPFOL** signature (S, TF, TF^c, PF, PF^c) to a **GHPFOL** signature (S, S^c, TF, PF), where S^c is the set of constrained sorts determined by $TF^c \cup PF^c$, and

   - every **CHPFOL** signature morphism φ to a **GHPFOL** signature morphism which works the same as φ on sorts and operation symbols;

2. α is the identity natural transformation, for every **CHPFOL** signature (S, TF, F^c, PF, PF^c) we have $\alpha_{(S,TF,TF^c,PF,PF^c)} = 1_{\mathbb{S}en(S,TF,TF^c,PF,PF^c)}$;

3. β is the inclusion natural transformation, for every **CHPFOL** signature (S, TF, TF^c, PF, PF^c) the functor $\beta_{(S,TF,TF^c,PF,PF^c)} : \mathbb{M}od(S, TF, TF^c, PF, PF^c) \to \mathbb{M}od(S, S^c, TF, PF)$ is defined by $\beta_{(S,TF,TF^c,PF,PF^c)}(M) = M$ for all models $M \in |\mathbb{M}od(S, TF, TF^c, PF, PF^c)|$ and $\beta_{(S,TF,TF^c,PF,PF^c)}(h) = h$ for all morphism $h \in \mathbb{M}od(S, TF, TF^c, PF, PF^c)$.

Notation. For every **GHPFOL**-signature (S, S^c, TF, PF) we let

1. TF^{S^c} to denote the set of total operations with constrained resulting sorts $\{\sigma \in TF_{w \to s} \mid s \in S^c\}$, and

2. PF^{S^c} to denote the set of total operations with constrained resulting sorts $\{\sigma \in PF_{w \to s} \mid s \in S^c\}$,

Remark 10.4.12. *A (S, S^c, TF, PF)-model M in* **GPFOL** *is reachable iff there exists a set of total variables Y of loose sorts and a function $f : Y \to N$, where $N = M \restriction_{(S,TF^{S^c},PF^{S^c})}$ such that for every constrained sort $s \in S^c$ the function $f^{\#}_s : (T_{(N,f)})_s \to (N, f)_s$ is surjective, where $f^{\#} : T_{(N,f)} \to (N, f)$ is the unique $(S, TF^{S^c} \cup Y, PF^{S^c})$-morphism.*

Definition 10.4.13. *A basic specification (Σ, Γ) in* **CHPFOL** *is sufficient complete, where $\Sigma = (S, TF, TF^c, PF, PF^c)$, if for every term t formed with symbols from $TF^{S^c} \cup PF^{S^c}$ and loose variables from Y there exists a term t' formed with constructors and loose variables from Y such that $\Gamma \models_{(S,TF,PF)} (\forall Y) def(t) \Rightarrow t \overset{e}{=} t'$.*

The following is a corollary of Theorem 8.4.3.

Corollary 10.4.14. *The WES of* **GHPFOL** *generated by the proof rules for* **CHPFOL** *is sound and Ω-complete, where $\Gamma \in \Omega_{(S,TF,TF^c,PF,PF^c)}$ iff the specification $((S, TF, TF^c, PF, PF^c), \Gamma)$ is sufficient complete.*

Proof. We set the parameters of Theorem 8.4.3. The institution I' is **CHPFOL** and the institution I is **GHPFOL**. The institution morphism is $\Delta_{\mathbf{HPFOL}}$ and the entailment system E of **GHPFOL** is the least entailment system closed under the rules enumerated in Corollary 10.4.11. M is the class of all reachable models. We need to prove that for every sufficient complete specification (Σ, Γ), where $\Sigma = (S, TF, TF^c, PF, PF^c)$ and any reachable (S, S^c, TF, PF)-model M (where S^c is the set constrained sorts determined by $TF^c \cup PF^c$) we have: $M \models \Gamma$ implies $M \in |\mathbb{M}od(\Sigma)|$. Because M is reachable by Remark 8.4.4 there exists a function $f : Y \to N$,

where $N = M \restriction_{(S,S^c,TF^{S^c},PF^{S^c})}$ and Y is a set of total variables of loose sorts, such that for every constrained sort $s \in S^c$ the function $f^{\#}_s : (T_{(N,f)})_s \to (N,f)_s$ is a surjection, where $f^{\#} : T_{(N,f)} \to (N,f)$ is the unique $(S, TF^{S^c} \cup Y, PF^{S^c})$-morphism. Let $N' = N \restriction_{(S,S^c,TF^c,PF^c)}$. Because (Σ,Γ) is sufficient complete, for every constrained sort $s \in S^c$ the function $\overline{f}_s : (T_{(N',f)})_s \to (N',f)_s$ is a surjection too, where $\overline{f} : T_{(N',f)} \to (N',f)$ is the unique $(S, TF^c \cup Y, PF^c)$-morphism. (Q.E.D.)

Structural induction. Assume we want $\Gamma \vdash_\Sigma (\forall x)\rho$ where $\Sigma = (S, TF, TF^c, PF, PF^c)$ and x is of sort s. By *Case Splitting* we need to prove $(\forall V)def(t) \Rightarrow \rho(x \leftarrow t)$ for all terms t formed with constructors and loose variables, where V are all the loose variables which occur in t. We define the following rules

(*Structural induction*) $\Gamma \vdash_\Sigma (\forall V)def(t) \Rightarrow \rho(x \leftarrow t)$ if

1. (*Induction base*) for all $cons \in (TF^c \cup PF^c)_{\to s}$, $\Gamma \cup \{def(cons)\} \vdash_\Sigma \rho(x \leftarrow cons)$,

2. (*Induction step*) for all $\sigma \in (TF^c \cup PF^c)_{s_1 \ldots s_n \to s}$ we have $\Gamma \cup \{\rho(x \leftarrow x') \mid x' \in X\} \cup \{def(\sigma(c_1,\ldots,c_n))\} \vdash_{\Sigma(C)} \rho(x \leftarrow \sigma(c_1,\ldots,c_n))$, where

   - $C = \{c_1,\ldots,c_n\}$ is a set of new total variables such that c_i has the sort s_i, for all $i \in \{1,\ldots,n\}$, and

   - $X \subseteq C$ is the set of variables with the sort s.

where t is any term formed with constructors and variables of loose sorts, and V are all (loose) variables which occur in t.

Proposition 10.4.15. *The entailment system of* **CHPFOL** *satisfies the rules of* Structural induction.

Proof. By induction on the depth of the term t.

1. Assume that t has the depth 0, i.e. is a constant. This case follows easily from *Induction base*.

2. Assume that $t = \sigma(t_1,\ldots,t_n)$. Let Z_i be the set of all variables in t_i for all $i \in \{1,\ldots,n\}$ and $J \subseteq \{1,\ldots,n\}$ such that t_i has the sort s. By induction hypothesis we have $\Gamma \cup \{def(t_j)\} \vdash_{\Sigma(Z_j)} \rho(x \leftarrow t_j)$ for all $j \in J$ which implies $\Gamma \cup \{def(t_j)\} \vdash_{\Sigma(Z)} \rho(x \leftarrow t_j)$ for all $j \in J$, where $Z = \bigcup_{i=1}^{i \le n} Z^i$. Since $def(\sigma(t_1,\ldots,t_n)) \vdash_{\Sigma(Z)} def(t_i)$ for all $i \in \{1,\ldots,n\}$ we obtain $\Gamma \cup \{def(\sigma(t_1,\ldots,t_n))\} \vdash_{\Sigma(Z)} \{\rho(x \leftarrow t_j) \mid j \in J\}$. By *Induction step* we have $\Gamma \cup \{\rho(x \leftarrow t_j) \mid j \in J\} \cup \{def(\sigma(t_1,\ldots,t_n))\} \vdash_{\Sigma(Z)} \rho(x \leftarrow \sigma(t_1,\ldots,t_n))$ and we get $\Gamma \cup \{def(\sigma(t_1,\ldots,t_n))\} \vdash_{\Sigma(Z)} \rho(x \leftarrow \sigma(t_1,\ldots,t_n))$. Finally $\Gamma \vdash_{\Sigma(Z)} def(\sigma(t_1,\ldots,t_n)) \Rightarrow \rho(x \leftarrow \sigma(t_1,\ldots,t_n))$ which implies $\Gamma \vdash_\Sigma (\forall Z)def(\sigma(t_1,\ldots,t_n)) \Rightarrow \rho(x \leftarrow \sigma(t_1,\ldots,t_n))$.

(Q.E.D.)

This Chapter generalizes the previous one on universal completeness and it is applicable to a wider class of logics with both partial and total operations symbols and with quantifications over total variables. We defined the rules of *Structural induction* which can be derived, according to Proposition 10.4.15, from the entailment system of **CHPFOL**. By using the results in Chapter 9 one can easily define an entailment system for **CUPFOL**.

Chapter 11

Conclusions

The pattern of institution-independent reasoning is to find categorical definitions of the conditions that are sufficient to prove the desired results. In this thesis we have studied layered entailment systems for reasoning about the logical consequences of the basic specifications in arbitrary institutions. The small and natural set of conditions that we identify for the underlying institution to ensure completeness helps in understanding at an abstract level "why" a logic is complete.

11.1 Summary

Our study distinguishes clearly the specific aspects of the logics from the general ones. Note that each institution comes with a class of atomic sentences which are the starting blocks for building sentences. We identify proof rules for the atomic sentences and prove their soundness for each logic. In the abstract setting for an institution $I = (\mathbb{S}ig, \mathbb{S}en, \mathbb{M}od, \models)$ we assume a sub-functor $\mathbb{S}en_0$ which associates to each signature a set of "atomic" sentences, and a system of sound proof rules for $I_0 = (\mathbb{S}ig, \mathbb{S}en_0, \mathbb{M}od, \models)$. By Proposition 3.2.7 the entailment system generated by the rules for the "atomic" sentences is sound.

Completeness is significantly more difficult then soundness, and it is closely related to the structure of the sentences. Take for example **CCEQL** with the sentences of the form $(\forall X)(\forall Y) \wedge H \Rightarrow C$, where X is a set of constrained variables, Y is a set of loose variables, H is a set of atoms, C is an atom. The completeness of the restriction of **CCEQL** to the atomic sentences is lifted to the completeness of **CCEQL** by firstly adding the rules which deal with the logical implications and then with the universal quantifications over loose and constrained sorts, respectively. Note that a sentence may have more than one representation. Take for example a Σ-sentence $(\forall X)(\forall Y) \wedge H \Rightarrow C$ in **CCEQL**. This sentence may be written as $(\forall X \cup Y) \wedge H \Rightarrow C$, or even as $(\forall \iota_X)(\iota_Y) \wedge H \Rightarrow C$, using the institution denotation, where $\iota_X : \Sigma \hookrightarrow \Sigma(X)$ and $\iota_Y : \Sigma \hookrightarrow \Sigma(Y)$ are extensions of Σ with constants from X and Y, respectively. This perspective lead to the abstraction: assume an institution $I = (\mathbb{S}ig, \mathbb{S}en, \mathbb{M}od, \models)$, a sub-functor $\mathbb{S}en_0 \subseteq \mathbb{S}en$, and two broad subcategories $D^c, D^l \subseteq \mathbb{S}ig$ of signature morphisms such that all the sentences are of the form $(\forall \chi)(\forall \varphi) \wedge H \Rightarrow C$ where χ is a signature morphism in D^c, φ is a signature morphism in D^l, H is a set of "atomic" sentences in $I_0 = (\mathbb{S}ig, \mathbb{S}en_0, \mathbb{M}od, \models)$, C is a sentence in I_0. The entailment system of I is constructed gradually as follows:

1. the "atomic" entailment system (AES) is specific to each logic. Therefore, in abstract settings is assumed, and it is developed in concrete examples;

$$\begin{array}{c} RUES(\forall_c) \\ | \\ GUES(\forall_l) \\ | \\ IES(\Rightarrow) \\ | \\ AES \end{array}$$

Figure 11.1: RUES

2. the entailment system for the restriction of I to the sentences formed without quantifiers, also called the entailment system with implications (IES), is obtained by adding the rules of *Implications*;

3. the entailment system for the restriction of I to the sentences formed without D^c-quantifications, also called the generic universal entailment system (GUES), is obtain by adding the rules of *Substitutivity* and *Generalization*;

4. the reachable universal entailment system for I (RUES), is obtain by adding the rules of *Case splitting*.

Remark 11.1.1. *Due some technical reasons, in Chapter 8 we used weak entailment systems, but since we have proved the soundness and completeness for those systems, the weak entailment systems are actually entailment systems.*

The completeness for each layer is obtained relatively to the completeness of the layer immediately below. When we instantiate GUES with IES, and IES with AES we obtain complete entailment systems for **HCL**, **HOSA**, **HPOA** and **HPA**. When we instantiate RUES with GUES, GUES with IES, and IES with AES we obtain entailment systems for **CHCL**, **CHOSA**, **CHPOA** and **CHPA** which are complete relatively to the class of sufficient complete basic specifications.

Recall that we have defined $\mathbf{FOL}'$ as the restriction of **FOL** to

- the signatures with a countable number of symbols, and
- sentences formed with quantifications over variables of sorts which are non-void [1].

Similarly we define $\mathbf{OSA}'$, $\mathbf{POA}'$, and $\mathbf{PA}'$. The sentences of these institutions are formed over the equational and relational atoms by applying Boolean connectives and quantifications. In the abstract setting we consider an institution $I = (\mathbb{S}ig, \mathbb{S}en, \mathbb{M}od, \models)$, a sub-functor $\mathbb{S}en_0 \subseteq \mathbb{S}en$ which gives the "atomic" sentences, and a broad sub-category of signature morphisms D^l used for quantifications, such that all that for each signature Σ the set $\mathbb{S}en(\Sigma)$ is a D^l-first-order Σ-fragment (see Definition 9.2.1). Note that this condition is more general than if we assumed that the sentences of I are formed over the "atomic" sentences in I_0 by means of Boolean connectives and D^l-quantifications.

[1] Given a first-order signature (S,F,P) a sort s is non-void iff $(T_F)_s \neq \emptyset$.

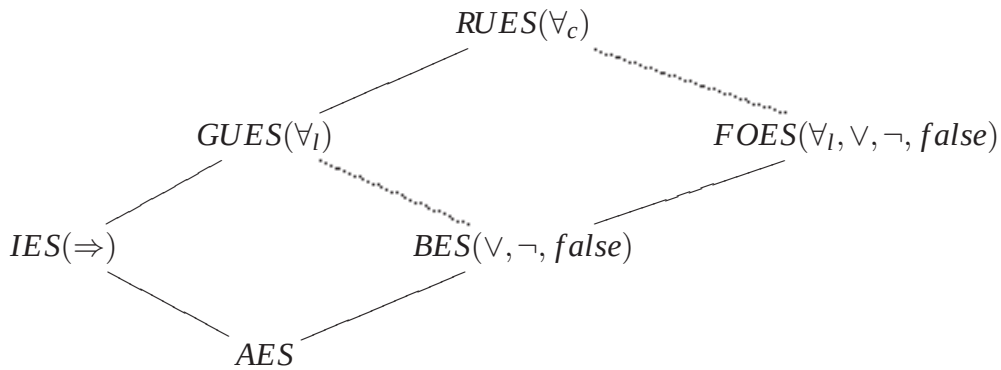

Figure 11.2: RUES-FOES

Assuming a system of proof rules for $I_0 = (\mathbb{S}ig, \mathbb{S}en_0, \mathbb{M}od, \models)$ which generates the "atomic" entailment system (AES) of I_0 , the first-order entailment (FOES) of I is the obtained by adding the rules which deals with the Boolean connectives and (existential) quantifications. One important particular case is when the sub-category D^l consists of identities only. We will call the corresponding entailment system (generated by the rules which deal with Boolean connectives) the Bool entailment system (BES).

As in the previous case the completeness of AES is lifted to the completeness of FOES. The FOES may be applied to **FOL**$'$, **OSA**$'$,**POA**$'$, and **PA**$'$. Again our general approach allows to instantiate the GUES with BES and RUES with FOES as in Fig. 11.2.

By instantiating GUES with BES, and BES with AES we obtain the completeness of **UFOL**, **UOSA**, **UPOA** and **UPA**. By instantiating RUES with GUES, GUES with BES, and BES with AES we obtain the completeness of **CUFOL**, **CUOSA**, **CUPOA** and **CUPA** relatively the class of sufficient complete basic specifications. By instantiating RUES with FOES, and FOES with AES we obtain the completeness of **CFOL**$'$, **COSA**$'$, **CPOA**$'$ and **CPA**$'$ wich is relative to the class of sufficient complete basic specifications. Recall that each of entailment system comes with an infinitary variant and following the figure 11.2, one can easily obtain the completeness of the infinitary logics defined in this paper. In chapter 10 we generalize the results concerning universal institutions to the class of logics with both partial and total operations and with quantifications over total variables.

11.2 Related Work

The fundamental assumption underlying the algebraic specifications is that programs are modeled as algebraic structures consisting of a collection of sets of data values together with functions over those sets. The theoretical foundations of algebraic specification are model-oriented, largely in terms of constructions on algebraic models. Theorem proving is syntactic manipulation used to demonstrate the truth. We justify our proof measure on sematic grounds. This approach is in contrast with Martin-Löf's intuitionistic type theory [47] and Coquand's Calculus of Constructions [19] where the emphasis is almost entirely on syntax and the system of rules, and semantics is absent or identified with the syntax. What we are calling soundness reappear in this context as consistency problems and is significantly more difficult to justify.

Institutions has been introduced by Goguen and Burstall in a seminal paper [33] with goal of providing uniform logical support for the algebraic specification languages. Meseguer extended

institutions with entailment systems [48], arriving at the notion of logic. These are the main ingredients for expressing and proving soundness and completeness in the abstract institutional framework. The completeness for single-sorted conditional equational logic was first proved in [10], which inaugurated the subject called "universal algebra". The first completeness result for many-sorted conditional was given by [5] in the categorical approach. The first satisfactory solution to many-sorted equational deduction is given in [35] where the proof rules deals explicitly with universal quantifications. Other categorical approaches to equational deduction may be found in [38], where the result is instantiated to partial algebras, and [62] based on satisfaction by injectivity. Here we present the first institutional approach to Birkhoff completeness organized on three layers, closely connected to the structure of the sentences.

The first institution-independent completeness result for finitary first-order institutions is due to [57] where the Henkin's method is generalized to arbitrary institutions. The completeness of infinitary logic $L_{\omega_1,\omega}$ was proved by Carol Karp [43]. Here we express and prove a completeness result for first-order institutions with signatures consisting of countable number of symbols which captures uniformly both finitary and infinitary cases. The technique used is forcing, a powerful method for constructing models introduced by Robinson in classical model theory [60] and studied by Keisler [44] and Barwise [4]. Paul Cohen invented the method of forcing to prove the independence of both the axiom of choice and the continuum hypothesis from Zermelo-Fraenkel set theory [17, 18]. This method has had profound effects on a number of branches of mathematical logic such as set theory and model theory as we mentioned above, recursion theory [45], and computational complexity [3].

Reachability concepts focus on the specification of generation principles usually presented by a set of constructors. Most algebraic specification languages incorporate features to express reachability like, for instance, CafeOBJ [25], CASL [2] and Maude [15]. Constructor-based logics has been studied in [7] and [8]. Institutions with both partial and total operation symbols have been studied in [13, 2], and detailed descriptions can be found in [9].

11.3 Future Work

One can easily define a constructor-based institution on top of some base institution $I = (\mathbb{S}ig, \mathbb{S}en, \mathbb{M}od, \models)$ in the abstract setting by defining the constructor-based signatures as signature morphisms in the base institution, and models for a constructor based-signature $\Sigma_0 \xrightarrow{\chi} \Sigma \in \mathbb{S}ig$ as models $M \in |\mathbb{M}od(\Sigma)|$ in the base institution such that $M\restriction_\chi$ is (D^c, D^l)-reachable. This construction may be useful when lifting the interpolation and amalgamation properties (necessary for modularization) from the base institution.

Consider the signature (S, F, F^c) in **CCEQL** such that $F = F^c$. We have $S^l = \emptyset$ which implies that the carrier sets of every (S, F, F^c)-algebra consist of interpretations of terms. Every set Γ of conditional (S, F, F^c)-equations admits an initial model O_Γ, i.e. for every (S, F, F^c)-algebra M which satisfies Γ there exists an unique morphism $O_\Gamma \to M$. Let $\Gamma \subseteq \mathbb{S}en(S, F, F^c)$ be an arbitrary set of conditional equations. Since all algebras consists of interpretations of terms we have that every (S, F, F^c)-morphism $O_\Gamma \to M$ is a surjection, and surjective morphism preserve the satisfaction, i.e. $O_\Gamma \models \rho$ implies $M \models \rho$ for all (S, F, F^c)-algebras M and conditional equations $\rho \in \mathbb{S}en(S, F, F^c)$. We obtain $\Gamma \models \rho$ iff $O_\Gamma \models \rho$ for all $\rho \in \mathbb{S}en(S, F, F^c)$. Since **CCEQL** is complete we obtain that the proof rules for the signature (S, F, F^c) are complete for the initial model O_Γ. We have defined the rules of *Structural induction* to deal with infinitary premises of *Case spliting* but the infinitary rules can not be replaced with the finitary ones

in order to obtain a complete and compact entailment system; we would obtain complete and compact entailment relations to reason with the logical consequences of the initial models of the specifications. Gödel incompleteness theorem shows that this is not possible even for the initial model of the specification of natural numbers.

We have introduced the forcing technique in institution-independent model theory and we have proved a completeness result for the first-order logics. We have linked the universal completeness results to the first-order completeness and demonstrate their applicability by specifying and verifying a mutual exclusion protocol. Future research aim for extending the area of applications in software engineering.

Forcing is a powerful method for constructing models which has been successfully applied in classical model theory. We believe that it may bring great benefit to the institution-independent model theory too. It is to investigate the applicability of our results to other institutions such as higher-order logic [14, 40], and membership algebra [50].

Bibliography

[1] J. Adámek and J. Rosický. *Locally Presentable and Accessible Categories*. Number 189 in London Mathematical Society Lecture Notes. Cambridge University Press, 1994.

[2] E. Astesiano, M. Bidoit, H. Kirchner, B. Krieg-Brückner, P. D. Mosses, D. Sannella, and A. Tarlecki. CASL: the Common Algebraic Specification Language. *Theor. Comput. Sci.*, 286(2):153–196, 2002.

[3] T. P. Baker, J. Gill, and R. Solovay. Relativizatons of the P =? NP Question. *SIAM J. Comput.*, 4(4):431–442, 1975.

[4] J. Barwise. Notes on forcing and countable fragments. 1970. Mimeographed.

[5] J. Benabou. On the structure of abstract algebras. *Cahiers de Topologie et Geometrie Differentiel*, 10:1–24, 1968.

[6] J. A. Bergstra and J. V. Tucker. A characterisation of computable data types by means of a finite equational specification method. In *ICALP*, pages 76–90, 1980.

[7] M. Bidoit and R. Hennicker. Constructor-based observational logic. *J. Log. Algebr. Program.*, 67(1-2):3–51, 2006.

[8] M. Bidoit, R. Hennicker, and A. Kurz. Observational logic, constructor-based logic, and their duality. *Theor. Comput. Sci.*, 3(298):471–510, 2003.

[9] M. Bidoit and P. D. Mosses. *Casl User Manual - Introduction to Using the Common Algebraic Specification Language*, volume 2900 of *Lecture Notes in Computer Science*. Springer, 2004.

[10] G. Birkhoff. On the structure of abstract algebras. *Proceedings of the Cambridge Philosophical Society*, 31:433–454, 1935.

[11] T. Borzyszkowski. Logical systems for structured specifications. *Theoretical Computer Science*, 286:2002, 1997.

[12] P. Burmeister. *A Model Theoretic Oriented Appraoch to Partial Algebras*. Akademie-Verlag Berlin, 1986.

[13] M. Cerioli, A. E. Haxthausen, B. Krieg-Brückner, and T. Mossakowski. Permissive Subsorted Partial Logic in CASL. In *AMAST*, pages 91–107, 1997.

[14] A. Church. A formulation of the simple theory of types. *J. Symb. Log.*, 5(2):56–68, 1940.

[15] M. Clavel, F. Durán, S. Eker, P. Lincoln, N. Martí-Oliet, J. Meseguer, and C. L. Talcott, editors. *All About Maude - A High-Performance Logical Framework, How to Specify, Program and Verify Systems in Rewriting Logic*, volume 4350 of *Lecture Notes in Computer Science*. Springer, 2007.

[16] M. Codescu and D. Gaina. Birkhoff Completeness in Institutions. *Logica Universalis*, 2(2):277–309, October 2008.

[17] P. J. Cohen. The Independence of the Continuum Hypothesis. *Proceedings of the National Academy of Sciences of the United States of America*, 50(6):1143–1148, December 1963.

[18] P. J. Cohen. The Independence of the Continuum Hypothesis. *Proceedings of the National Academy of Sciences of the United States of America*, 51(1):105–110, January 1964.

[19] T. Coquand and G. P. Huet. The Calculus of Constructions. *Inf. Comput.*, 76(2/3):95–120, 1988.

[20] R. Diaconescu. Institution-independent Ultraproducts. *Fundamenta Informaticæ*, 55(3-4):321–348, 2003.

[21] R. Diaconescu. Herbrand Theorems in arbitrary institutions. *Inf. Process. Lett.*, 90:29–37, 2004.

[22] R. Diaconescu. An Institution-independent proof of Craig Interpolation Theorem. *Studia Logica*, 77(1):59–79, 2004.

[23] R. Diaconescu. Proof Systems for Institutional Logic. *Journal of Logic and Computation*, 16(3):339–357, 2006.

[24] R. Diaconescu. *Institution-independent Model Theory*. Studies in Universal Logic. Birkhäuser, 2008.

[25] R. Diaconescu and K. Futatsugi. *CafeOBJ Report: The Language, Proof Techniques, and Methodologies for Object-Oriented Algebraic Specification*, volume 6 of *AMAST Series in Computing*. World Scientific, 1998.

[26] R. Diaconescu and K. Futatsugi. Logical Foundations of CafeOBJ. *Theoretical Computer Science*, 285:289–318, 2002.

[27] K. Futatsugi, J. A. Goguen, and K. Ogata. Verifying Design with Proof Scores. In *VSTTE*, pages 277–290, 2005.

[28] D. Gaina, K. Futatsugi, and K. Ogata. Constructor-based Institutions. In *CALCO*, volume 5728 of *Lecture Notes in Computer Science*. Springer, 2009.

[29] D. Gaina and M. Petria. Completeness by forcing. *Journal of Logic and Computation*. accepted.

[30] D. Gaina and A. Popescu. An Institution-independent Generalization of Tarski's Elementary Chain Theorem. *Journal of Logic and Computation*, 16(6):713–735, 2006.

[31] D. Gaina and A. Popescu. An Institution-Independent Proof of Robinson Consistency Theorem. *Studia Logica*, 85(1):41–73, 2007.

[32] J. Goguen. *Theorem Proving and Algebra*. MIT. to appear.

[33] J. Goguen and R. Burstall. Institutions: Abstract Model Theory for Specification and Programming. *Journal of the Association for Computing Machinery*, 39(1):95–146, January 1992.

[34] J. Goguen and R. Diaconescu. An Oxford Survey of Order Sorted Algebra. *Mathematical Structures in Computer Science*, 4(3):363–392, 1994.

[35] J. Goguen and J. Meseguer. Completeness of many-sorted equational logic. *Houston Journal of Mathematics*, 11(3):307–334, 1985.

[36] J. Goguen and J. Meseguer. Order-Sorted Algebra I: Equational Deduction for Multiple Inheritance, Overloading, Exceptions and Partial Operations. *Theoretical Computer Science*, 105(2):217–273, 1992.

[37] J. Goguen and G. Rosu. Institution Morphisms. *Formal Asp. Comput.*, 13(3-5):274–307, 2002.

[38] H.Andréka and I.Németi. Generalization of the concept of variety and quasivariety to partial algebras through category theory. *Dissertationes Mathematicae*, 204, 1983.

[39] L. Henkin. The Completeness of the First-order Functional Calculus. *Journal of Symbolic Logic*, 14(3):159–166, 1949.

[40] L. Henkin. Completeness in the Theory of Types. *J. Symb. Log.*, 15(2):81–91, 1950.

[41] J. Hirschfeld and W. Wheeler. *Forcing, arithmetic, division rings*. Springer, 1975.

[42] G. Huet and D. C. Oppen. Equations and rewrite rules: a survey. *Formal Language Theory: Perspectives and Open Problems*, pages 349–405, 1980.

[43] C. R. Karp. *Languages with Expressions of Infinite Length*. North-Holland, Amsterdam, 1964.

[44] J. Keisler. Forcing and the omitting types theorem. *Studies in Model Theory*, 8:96–133, 1973.

[45] M. Lerman. Degrees of Unsolvability: Local and Global Theory. *Perspectives in Mathematical Logic*, 11, 1983.

[46] S. Mac Lane. *Categories for the Working Mathematician*. Springer, 1971.

[47] P. Martin-Löf. *Intuitionistic Type Theory. Notes by Giovanni Sambin of a series of lectures given in Padua, June 1980*. Bibliopolis, Napoli, 1984.

[48] J. Meseguer. General logics. In *Logic Colloquium 87*, pages 275–329. North Holland, 1989.

[49] J. Meseguer. Conditional Rewriting Logic as a Unified Model of Concurrency. *Theoretical Computer Science*, pages 73–155, 1992.

[50] J. Meseguer. Membership algebra as a logical framework for equational specification. In *WADT*, pages 18–61, 1997.

[51] T. Mossakowski. Relating CASL with other specification languages: the institution level. *Theor. Comput. Sci.*, 286(2):367–475, 2002.

[52] T. Mossakowski, J. Goguen, R. Diaconescu, and A. Tarlecki. What is a logic? In J.-Y. Beziau, editor, *Logica Universalis*, pages 113–133. Birkhauser, 2005.

[53] K. Ogata and K. Futatsugi. Formally Modeling and Verifying Ricart&Agrawala distributed Mutual Exclusion Algorithm. In *APAQS*, pages 357–366, 2001.

[54] K. Ogata and K. Futatsugi. Formal Analysis of Suzuki & Kasami Distributed Mutual Exclusion Algorithm. In *FMOODS*, pages 181–195, 2002.

[55] K. Ogata and K. Futatsugi. Flaw and modification of the iKP electronic payment protocols. *Inf. Process. Lett.*, 86(2):57–62, 2003.

[56] K. Ogata and K. Futatsugi. Equational Approach to Formal Analysis of TLS. In *ICDCS*, pages 795–804, 2005.

[57] M. Petria. An Institutional Version of Gödel's Completeness Theorem. In T. Mossakowski, U. Montanari, and M. Haveraaen, editors, *CALCO*, volume 4624 of *Lecture Notes in Computer Science*, pages 409–424. Springer, 2007.

[58] M. Petria and R. Diaconescu. Abstract Beth definability in institutions. *Journal of Symbolic Logic*, 71(3):1002–1028, 2006.

[59] H. Reichel. *Structural Induction on Partial Algebras*. Akademie-Verlag Berlin, 1984.

[60] A. Robinson. Forcing in model theory. *Symposia Mathematica*, 50:69–82, 1971.

[61] G. Rosu. The Institution of Order-Sorted Equational Logic. *Bulletin of EATCS*, 53:250–255, 1994.

[62] G. Rosu. Complete categorical deduction for satisfaction as injectivity. In *Essays Dedicated to Joseph A. Goguen*, pages 157–172, 2006.

[63] A. Tarlecki. Bits and pieces of the theory of institutions. In D. Pitt, S. Abramsky, A. Poigné, and D. Rydeheard, editors, *Proceedings, Summer Workshop on Category Theory and Computer Programming, Lecture Notes in Computer Science*, volume 240, pages 334–360. Springer, 1986.

[64] A. Tarlecki. Quasi-varieties in abstract algebraic institutions. *J. Comput. Syst. Sci.*, 33(3):333–360, 1986.

Publications

[1] Daniel Gaina and Andrei Popescu: “An Institution-independent Generalization of Tarski’s Elementary Chain Theorem”, Journal of Logic and Computation, vol.16, no.6, pp.713-735 (Aug. 2006).

[2] Daniel Gaina and Andrei Popescu: “An Institution-Independent Proof of Robinson Consistency Theorem”, Studia Logica, vol.85, no.1, pp.41-73 (Feb. 2007).

[3] Mihai Codescu and Daniel Gaina: “Birkhoff Completeness in Institutions”, Logica Universalis, vol. 2, no. 2, pp.277-309 (Oct. 2008).

[4] Daniel Gaina, Kokichi Futatsugi and Kazuhiro Ogata: “Constructor-based Institutions”, LNCS 5728, pp 398-412, CALCO 2009.

[5] Daniel Gaina and Marius Petria: “Completeness by forcing”, accepted to Journal of Logic and Computation.