

# Institutional 2-cells and Grothendieck institutions

Till Mossakowski

DFKI Lab Bremen and Dept. of Computer Science, University of Bremen, Germany

**Abstract.** We propose to use Grothendieck institutions based on 2-categorical diagrams as a basis for heterogeneous specification. We prove a number of results about colimits and (some weak variants of) exactness. This framework can also be used for obtaining proof systems for heterogeneous theories involving institution semi-morphisms.

## 1 Introduction

“There is a population explosion among the logical systems used in computer science. Examples include first order logic, equational logic, Horn clause logic, higher order logic, infinitary logic, dynamic logic, intuitionistic logic, order-sorted logic, and temporal logic; moreover, there is a tendency for each theorem prover to have its own idiosyncratic logical system. We introduce the concept of *institution* to formalize the informal notion of ‘logical system’.” [10]

This famous quote from Joseph Goguen’s and Rod Burstall’s seminal paper introducing institutions lead, in its consequences, also to the introduction of Grothendieck institutions by Răzvan Diaconescu [5], which provide the semantic basis for heterogeneous specifications, i.e. the involvement of a multitude of logical systems within a single specification.

While the properties of Grothendieck institutions and their interaction with colimits, exactness, liberality, Craig interpolation etc. is well-studied now (cf. the forthcoming book [4]), the present theory of Grothendieck institutions still does not answer certain practical problems. During the development of the heterogeneous tool set (HETS) [15, 17], a parsing, static analysis and proof management tool for heterogeneous specifications, we have encountered the following problems:

- often there is a plethora of possible translations between two given institutions, making choice difficult for the user;
- often premises for theorems about Grothendieck institutions do not hold for some of the institution involved — however, failure of a premise just for one institution usually destroys applicability of a theorem;
- also, the premises needed for institution (co)morphisms do not hold in all cases;

- finally, this means that the applicability of theorem proving for structured specifications [2] is limited for Grothendieck institutions, and hence for heterogeneous specifications.

We introduce two ideas that may help solving these problems: the use of institutional 2-cells, and the weakening of exactness properties to quasi-exactness. We prove a number of properties of these and discuss examples. Proofs can be found in the appendix.

## 2 Institutions

Let  $\mathcal{CAT}$  be the category of categories and functors.<sup>1</sup>

**Definition 1.** An *institution*  $I = (\mathbf{Sign}, \mathbf{Sen}, \mathbf{Mod}, \models)$  consists of

- a category **Sign** of *signatures*,
- a functor **Sen**: **Sign**  $\longrightarrow$  **Set** giving, for each signature  $\Sigma$ , the set of *sentences*  $\mathbf{Sen}(\Sigma)$ , and for each signature morphism  $\sigma: \Sigma \longrightarrow \Sigma'$ , the *sentence translation map*  $\mathbf{Sen}(\sigma): \mathbf{Sen}(\Sigma) \longrightarrow \mathbf{Sen}(\Sigma')$ , where often  $\mathbf{Sen}(\sigma)(\varphi)$  is written as  $\sigma(\varphi)$ ,
- a functor **Mod**: **(Sign)<sup>op</sup>**  $\longrightarrow$   $\mathcal{CAT}$  giving, for each signature  $\Sigma$ , the category of *models*  $\mathbf{Mod}(\Sigma)$ , and for each signature morphism  $\sigma: \Sigma \longrightarrow \Sigma'$ , the *reduct functor*  $\mathbf{Mod}(\sigma): \mathbf{Mod}(\Sigma') \longrightarrow \mathbf{Mod}(\Sigma)$ , where often  $\mathbf{Mod}(\sigma)(M')$  is written as  $M'|_\sigma$ ,
- a satisfaction relation  $\models_\Sigma \subseteq |\mathbf{Mod}(\Sigma)| \times \mathbf{Sen}(\Sigma)$  for each  $\Sigma \in |\mathbf{Sign}|$ ,

such that for each  $\sigma: \Sigma \longrightarrow \Sigma'$  in **Sign** the following *satisfaction condition* holds:

$$M' \models_{\Sigma'} \sigma(\varphi) \Leftrightarrow M'|_\sigma \models_\Sigma \varphi$$

for each  $M' \in |\mathbf{Mod}(\Sigma')|$  and  $\varphi \in \mathbf{Sen}(\Sigma)$ . □

Institutions can alternatively, and more succinctly, be characterized as functors into a certain category of “twisted relations” [10], called “rooms” in [9]:

An *institution room*  $(S, \mathcal{M}, \models)$  consists of

- a set of  $S$  of *sentences*,
- a category  $\mathcal{M}$  of *models*, and
- a satisfaction relation  $\models \subseteq |\mathcal{M}| \times S$ .

Rooms are connected via corridors (which model change of notation within one logic, as well as translations between logics).

An *institution corridor*  $(\alpha, \beta): (S_1, \mathcal{M}_1, \models_1) \longrightarrow (S_2, \mathcal{M}_2, \models_2)$  consists of

- a sentence translation function  $\alpha: S_1 \longrightarrow S_2$ , and
- a model reduction functor  $\beta: \mathcal{M}_2 \longrightarrow \mathcal{M}_1$ , such that

<sup>1</sup> Strictly speaking,  $\mathcal{CAT}$  is not a category but only a so-called quasicategory, which is a category that lives in a higher set-theoretic universe [11].

$$M_2 \models_2 \alpha(\varphi_1) \Leftrightarrow \beta(M_2) \models_1 \varphi_1$$

holds for each  $M_2 \in |\mathcal{M}_2|$  and each  $\varphi_1 \in S_1$  (*satisfaction condition*).

Now, an institution can equivalently be defined to be just a functor  $I: \mathbf{Sign} \rightarrow \mathbf{InsRoom}$  (where  $\mathbf{Sign}$  is the category of signatures).

**Example 2.** The institution  $FOL^=$  of many-sorted first-order logic with equality. Signatures are many-sorted first-order signatures, i.e. many-sorted algebraic signatures enriched with predicate symbols with arities. Signature morphisms map signature symbols in a coherent way. Models are many-sorted first-order structures, and model morphisms are standard algebra homomorphisms that preserve the holding of predicates. Model (morphism) reduction is done by renaming model (morphism) components. Sentences are first-order formulas, and sentence translation means replacement of the translated symbols. Satisfaction is the usual satisfaction of a first-order sentence in a first-order structure.  $\square$

**Example 3.** The institution  $Eq^=$  of equational logic is the restriction of  $FOL^=$  to signatures without predicates, and (universally quantified) equations as the only sentences.  $\square$

**Example 4.** The institution  $PFOL^=$  of partial first-order logic with equality. Signatures are many-sorted first-order signatures enriched by partial function symbols. Models are many-sorted partial first-order structures. Sentences are first-order formulas containing existential equations, strong equations, definedness statements and predicate applications as atomic formulas. Satisfaction is defined using total valuations of variables, while valuation of terms is partial due to the existence of partial functions. An existential equation holds if both sides are defined and equal, whereas a strong equation also holds if both sides are undefined. A definedness statement holds if the term is defined. A predicate application holds if the terms contained in it are defined, and the corresponding tuple of values is in the interpretation of the predicate. This is extended to first-order formulas as usual. Moreover, signature morphisms, model reductions and sentence translations are defined like in  $FOL^=$ .  $\square$

**Example 5.** The CASL institution extends  $PFOL^=$  with subsorting and induction (for datatypes), see [14, 3] for details. CASL has, among others, a modal logic extension MODALCASL [15] and a coalgebraic extension CoCASL [18].  $\square$

**Example 6.** There is an institution  $PLNG$  of a programming language [21]. It is built over an algebra of built-in data types and operations of a programming language. Signatures are given as function (functional procedure) headings; sentences are function bodies; and models are maps that for each function symbol, assign a computation (either diverging, or yielding a result) to any sequence of actual parameters. A model satisfies a sentence iff it assigns to each sequence of parameters the computation of the function body as given by the sentence. Hence, sentences determine particular functions in the model uniquely. Finally, signature morphisms, model reductions and sentence translations are defined similarly to those in  $FOL^=$ .  $\square$

*Institution morphisms* [10, 7] relate two given institutions. A typical situation is that an institution morphism expresses the fact that a “larger” institution is *built upon* a “smaller” institution by *projecting* the “larger” institution onto the “smaller” one. Dually, institution comorphisms [7] typically express that an institution is included, or *encoded* into another one.

Using the notation of institutions as functors, given institutions  $I_1: \mathbf{Sign}_1 \rightarrow \mathbf{InsRoom}$  and  $I_2: \mathbf{Sign}_2 \rightarrow \mathbf{InsRoom}$ , an *institution morphism*  $(\Psi, \mu): I_1 \rightarrow I_2$  consists of a functor  $\Psi: \mathbf{Sign}_1 \rightarrow \mathbf{Sign}_2$  and a natural transformation  $\mu: I_2 \circ \Psi \rightarrow I_1$ . (Alternatively, we split  $\mu$  into two natural transformations, denoted by  $\alpha$  and  $\beta$ ). By contrast, an *institution comorphism*  $(\Phi, \rho): I_1 \rightarrow I_2$  consists of a functor  $\Phi: \mathbf{Sign}_1 \rightarrow \mathbf{Sign}_2$  and a natural transformation  $\rho: I_1 \rightarrow I_2 \circ \Phi$ .

Together with obvious identities and composition, this gives us the category **Ins** (**CoIns**) of institutions and institution (co)morphisms. An institution *semi-(co)morphism* is like an institution (co)morphism, but without the sentence translation component (and hence also without the satisfaction condition).

Example 7. There is an institution morphism going from first-order logic with equality to equational logic. A first-order signature is translated to an algebraic signature by just forgetting the set of predicate symbols; similarly, a first-order model is turned into an algebra by forgetting the predicates. Sentence translation is just inclusion of equations into first-order sentences.  $\square$

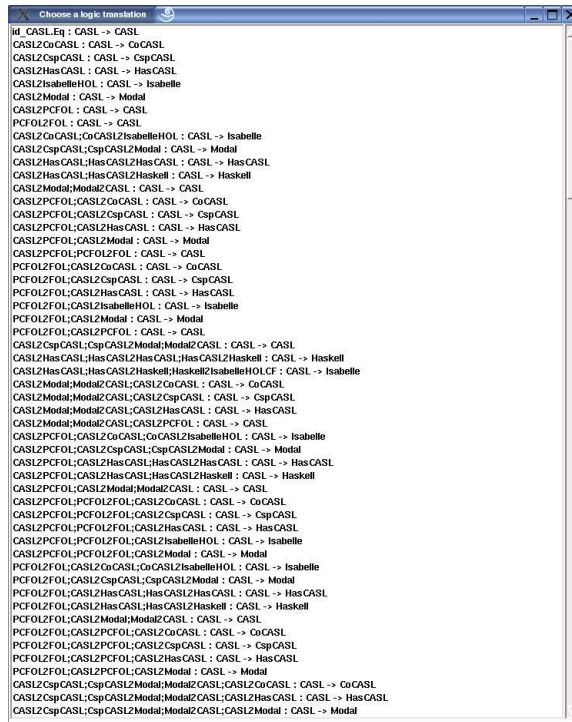
Example 8. There is an institution semi-morphism *toCASL* from PLNG to CASL [21]. It extracts an algebraic signature with partial operations out of a PLNG-signature by adding the signature of built-in data types and operations of the programming language. For any function declared, any PLNG-model determines its computations on given arguments, from which we can extract a partial function that maps any sequence of arguments to the result of the computation (if any). These are used to expand the built-in algebra of data types and operations of the programming language with an interpretation for the extra function names in the signature obtained.  $\square$

Example 9. There is an institution comorphism going from equational logic to first-order logic with equality. An algebraic signature is translated to a first-order signature by just taking the set of predicate symbols to be empty. Sentence translation is just inclusion of equations into first-order sentences. A first-order model with empty set of predicates is translated by just considering it as an algebra.  $\square$

Example 10. Similarly, there are obvious inclusion comorphisms from CASL to MODALCASL and CoCASL, see [15].  $\square$

Example 11. Define an institution comorphism going from partial first-order logic with equality to first-order logic with equality as follows: A partial first-order signature is translated to a total one by encoding each partial function symbol as a total one, plus a (new) unary predicate  $D$  (“definedness”) and a (new) function symbol  $\perp$  (“undefined”) for each sort (this means that  $\perp$  and

$D$  are heavily overloaded). Furthermore, we add axioms<sup>2</sup> stating that  $D$  does not hold on  $\perp$ , and that (encoded) total functions preserve (“totality”) and reflect (“strictness”)  $D$ , while partial functions only reflect  $D$  (and the holding of predicates implies  $D$  to hold on the arguments). Sentence translation is done by replacing all partial function symbols by the total functions symbols encoding them, replacing strong equations  $t = u$  by  $(D(t) \vee D(u)) \Rightarrow t = u$ , existence equations by conjunctions of the equation and the definedness (using  $D$ ) of one of the sides of the equation, replacing definedness with  $D$ , and leaving predicate symbols as they are. For a given total model of the translated signature, we just take as carriers of the partial model the interpretations of the definedness predicates in the total model, while the total functions are restricted to these new carriers, yielding partial functions.  $\square$



**Fig. 1.** Dozens of translation possibilities for a CASL theory in HETS (from a logic graph without comorphism modifications; using modifications, the number of possible translations can be greatly reduced).

<sup>2</sup> Hence, strictly speaking, this comorphism is a so-called simple theoroidal one, see [19] for details.

### 3 Institution (Co)Morphism Modifications

A typical experience with using the heterogeneous tool set [15, 17] is the following: for some specification, you want to prove a theorem, and hence want to see a list of its possible translations (along (co)comorphisms) into tool-supported institutions. Now even with a small diagram of institutions, the list can become quite large, because also composites should be shown (see Fig. 1 for a menu of such translations). Now such lists generally bear a lot of redundancy, since two different translation paths, though differing as (co)morphisms, lead to essentially same results, as the following example shows:

Example 12. There are two ways to go from equational logic to first-order logic: one is the obvious substitution comorphism  $\rho_1$  from Example 9, the other one is the composition  $\rho_2$  of the obvious substitution comorphism from equational logic to partial first-order logic composed with the encoding of partial first-order logic into first-order logic from Example 11.<sup>3</sup> These comorphisms are different:  $\rho_2$  adds some (superfluous) coding of partiality. Yet, for e.g. the purpose of re-using proof tools,  $\rho_1$  and  $\rho_2$  are essentially the same.

In this context, the notion of *modification* helps.

In order to ensure that the difference between two translations really is inessential, a crucial property of modifications is that they do not lead to identifications of different sentence or model translation maps. Hence, we strengthen the original notion from [5] to *discrete* modifications:

**Definition 13.** Given institution morphisms  $(\Psi, \mu): I_1 \rightarrow I_2$  and  $(\Psi', \mu'): I_1 \rightarrow I_2$ , a *discrete institution morphism modification*  $\theta: (\Psi, \mu) \rightarrow (\Psi', \mu')$  is just a natural transformation  $\theta: \Psi \rightarrow \Psi'$  such that  $\mu = \mu' \circ (I_2 \cdot \theta)$ . Similarly, given institution comorphisms  $(\Phi, \rho): I_1 \rightarrow I_2$  and  $(\Phi', \rho'): I_1 \rightarrow I_2$ , a *discrete institution comorphism modification*  $\theta: (\Phi, \rho) \rightarrow (\Phi', \rho')$  is a natural transformation  $\theta: \Phi \rightarrow \Phi'$  such that  $(I_2 \cdot \theta) \circ \rho = \rho'$ .

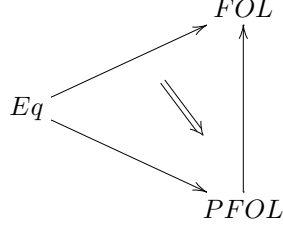
Together with obvious identities and compositions, modifications can serve as 2-cells, leading to 2-categories **Ins** and **CoIns**.  $\square$

In [5, 4], a weaker notion of institution morphism modification has been introduced, involving an additional natural transformation on the side of the models. We have not found this extra generality of practical use and hence work with the above stronger notion of discrete modification. However, since we will not use any non-discrete modification, we will omit the qualification of being discrete henceforth.

---

<sup>3</sup> Actually, since the latter is a simple theoroidal comorphism, we should take both to end in  $FOL^{th}$ , the institution of  $FOL$ -theories.

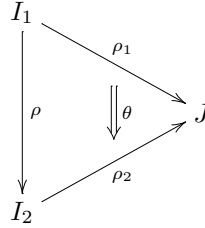
Example 14. Consider the comorphisms from Example 12.



The comorphism modification  $\theta: \rho_1 \longrightarrow \rho_2$  is just the pointwise inclusion of an algebraic signature viewed as first-order signature into the theory coding a partial variant of that signature.  $\square$

Modifications also interplay with amalgamation:

**Definition 15.** Let  $\rho = (\Phi, \alpha, \beta): I_1 \longrightarrow I_2$ ,  $\rho_1 = (\Phi_1, \alpha_1, \beta_1): I_1 \longrightarrow J$  and  $\rho_2 = (\Phi_2, \alpha_2, \beta_2): I_2 \longrightarrow J$  be three comorphisms. A lax triangle



of institution comorphisms and modifications is called *(weakly) amalgamable*, if

$$\begin{array}{ccc}
 \mathbf{Mod}^{I_1}(\Sigma) & \xleftarrow{(\beta_1)_\Sigma} & \mathbf{Mod}^J(\Phi_1(\Sigma)) \\
 \uparrow \beta_\Sigma & & \uparrow \mathbf{Mod}^J(\theta_\Sigma) \\
 \mathbf{Mod}^{I_2}(\Sigma) & \xleftarrow{(\beta_2)_\Sigma} & \mathbf{Mod}^J(\Phi_2(\Sigma))
 \end{array}$$

is a (weak) pullback for each signature  $\Sigma \in |\mathbf{Sign}^I|$ .  $\square$

## 4 Colimits in Hom-Categories

As a first result about the 2-categorical structure of  $\mathbf{CoIns}$ , we examine colimits in the Hom-categories, which play a rôle for some results about the Grothendieck construction (see Prop. 22 below):

**Proposition 16.** Given two institutions  $I$  and  $J$ , if  $J$  has pushouts of signatures, then the Hom-category  $\mathbf{CoIns}(I, J)$  has pushouts as well. This generalizes to arbitrary non-empty colimits of connected diagrams.  $\square$

Note that initial objects in Hom-categories  $\mathbf{CoIns}(I, J)$  generally do not exist: an initial comorphism from  $I$  to  $J$  would have to translate  $I$ -sentences to  $J$ -sentences over the initial signature, thereby losing any specific reference to the signature, which generally destroys the satisfaction condition.

The dual situation is better for initial objects:

**Proposition 17.** Given two institutions  $I$  and  $J$ , if  $J$  has an initial signature with empty set of sentences and terminal model category, then the Hom-category  $\mathbf{Ins}(I, J)$  has an initial object.  $\square$

However, pushouts in  $\mathbf{Ins}(I, J)$  seem to exist only under rather strong additional assumptions.

We hence prefer to work with comorphisms in the sequel.

## 5 Comorphism-Based Grothendieck Institutions

Grothendieck institutions have been introduced by Diaconescu [5] as a foundation for heterogeneous specification. The basic data for comorphism-based heterogeneous specification is a graph of institutions, comorphisms and modifications. Remember from Sect. 2 that the modifications are needed because we want to express that certain compositions of comorphisms are the same. This means that we need to specify both compositions and modifications. We hence arrive at the following:

**Definition 18.** Given an index 2-category  $Ind$ , a *2-indexed coinstitution* is a 2-functor  $\mathcal{I}: Ind^* \rightarrow \mathbf{CoIns}$ <sup>4</sup> into the 2-category of institutions, institution comorphisms and institution comorphism modifications.  $\square$

A 2-indexed coinstitution can be flattened, using the so-called *Grothendieck construction*. The basic idea here is that all signatures of all institutions are put side by side, and a signature morphism in this large realm of signatures consists of an intra-logic signature morphism plus an inter-logic translation (along some logic comorphism). The other components (sentences, models, satisfaction) are then defined in a straightforward way.

The Grothendieck construction for indexed institutions has been described in [5]; we develop its dual here [13]. In an indexed coinstitution  $\mathcal{I}$ , we use the notation  $\mathcal{I}^i = (\mathbf{Sign}^i, \mathbf{Sen}^i, \mathbf{Mod}^i, \models^i)$  for  $\mathcal{I}(i)$ ,  $(\Phi^d, \rho^d)$  for the comorphism  $\mathcal{I}(d)$ , and  $\mathcal{I}^u$  for the modification  $\mathcal{I}(u)$ .

**Definition 19.** Given a 2-indexed coinstitution  $\mathcal{I}: Ind^* \rightarrow \mathbf{CoIns}$ , define the *Grothendieck institution*  $\mathcal{I}^\#$  as follows:

- signatures in  $\mathcal{I}^\#$  are pairs  $(i, \Sigma)$ , where  $i \in |Ind|$  and  $\Sigma$  a signature in  $\mathcal{I}^i$ ,
- signature morphisms  $(d, \sigma): (i, \Sigma_1) \rightarrow (j, \Sigma_2)$  consist of a morphism  $d: j \rightarrow i \in Ind$  and a signature morphism  $\sigma: \Phi^d(\Sigma_1) \rightarrow \Sigma_2$  in  $\mathcal{I}^j$ ,
- composition is given by  $(d_2, \sigma_2) \circ (d_1, \sigma_1) = (d_1 \circ d_2, \sigma_2 \circ \Phi^{d_2}(\sigma_1))$ ,

<sup>4</sup>  $Ind^*$  is the 2-categorical dual of  $Ind$ , where both 1-cells and 2-cells are reversed.

$$- \mathcal{I}^\#(i, \Sigma) = \mathcal{I}^i(\Sigma), \text{ and } \mathcal{I}^\#(d, \sigma) = \mathcal{I}^i(\Sigma_1) \xrightarrow{\rho^d} \mathcal{I}^j(\Phi^d(\Sigma_1)) \xrightarrow{\mathcal{I}^j(\sigma)} \mathcal{I}^j(\Sigma_2). \quad \square$$

That is, the room  $\mathcal{I}^\#(i, \Sigma)$  (consisting of sentences, models and satisfaction) for a Grothendieck signature  $(i, \Sigma)$  is defined component-wise, while the corridor for a Grothendieck signature morphism is obtained by composing the corridor given by the inter-institution comorphism with that given by the intra-institution signature morphism. We also denote the Grothendieck institution by  $(\mathbf{Sign}^\#, \mathbf{Sen}^\#, \mathbf{Mod}^\#, \models^\#)$ .

While the comorphism based Grothendieck construction nearly satisfies all of our needs, one problem remains. Sometimes, the Grothendieck construction makes too many distinctions between signature morphisms (cf. Fig. 1). Therefore, we use the institution comorphism modifications to obtain a congruence on Grothendieck signature morphisms: the congruence is generated by

$$(d', \mathcal{I}_\Sigma^u: \Phi^{d'}(\Sigma) \longrightarrow \Phi^d(\Sigma)) \equiv (d, id: \Phi^d(\Sigma) \longrightarrow \Phi^d(\Sigma)) \quad (1)$$

relating morphisms from  $(i, \Sigma)$  to  $(j, \Phi^d(\Sigma))$ , for  $\Sigma \in |\mathbf{Sign}^i|$ ,  $d, d': j \longrightarrow i \in \mathbf{Ind}$ , and  $u: d \Rightarrow d' \in \mathbf{Ind}$ . We will later examine what is really added by the congruence closure. But first, let us state the following crucial property:

**Proposition 20.**  $\equiv$  is contained in the kernel of  $\mathcal{I}^\#$  (considered as a functor).  $\square$

Let  $q^\mathcal{I}: \mathbf{Sign}^\# \longrightarrow \mathbf{Sign}^\# / \equiv$  be the quotient functor induced by  $\equiv$  (see [12] for the definition of quotient category). Note that it is the identity on objects. We easily obtain that the functor  $\mathcal{I}^\#$  factors through the quotient category  $\mathbf{Sign}^\# / \equiv$ :

**Corollary 21.**  $\mathcal{I}^\#: \mathbf{Sign}^\# \longrightarrow \mathbf{InsRoom}$  leads to a quotient Grothendieck institution  $\mathcal{I}^\# / \equiv: \mathbf{Sign}^\# / \equiv \longrightarrow \mathbf{InsRoom}$ .  $\square$

By abuse of notation, we denote  $\mathcal{I}^\# / \equiv$  by  $(\mathbf{Sign}^\# / \equiv, \mathbf{Sen}^\#, \mathbf{Mod}^\#, \models^\#)$ .

When considering e.g. the comorphism going from partial first-order logic  $PFO L^\#$  to first-order logic  $FOL^\#$ , and the composite comorphism going from  $PFO L^\#$  to CASL and then to  $FOL^\#$ , we end up in different comorphisms, which are however related by a comorphism modification. The above identification process in the Grothendieck institution now tells us that it does not matter which way we choose.

In some cases, the congruence  $\equiv$  can be described succinctly:

**Proposition 22.** Assume that  $\mathbf{Ind}^*$  has cocones for diagrams of 2-cells of shape  $\bullet \Longrightarrow \bullet \longleftarrow \bullet$  that are mapped to pushouts of 2-cells in  $\mathbf{CoIns}$ . Then the congruence  $\equiv$  defined above is explicitly given by

$$(d_1, \sigma \circ \mathcal{I}_\Sigma^{u_1}) \equiv (d_2, \sigma \circ \mathcal{I}_\Sigma^{u_2})$$

for  $\Sigma \in |\mathbf{Sign}^i|$ ,  $d, d_1, d_2: j \longrightarrow i \in \mathbf{Ind}$ ,  $\sigma: \Phi^d(\Sigma) \longrightarrow \Sigma' \in \mathbf{Sign}^j$  and  $u_1: d \Rightarrow d_1, u_2: d \Rightarrow d_2 \in \mathbf{Ind}$ .  $\square$

Note that according to Prop. 16, under relatively mild assumptions, pushouts of 2-cells in **CoIns** exist. Hence, the assumption of Prop. 22 that  $Ind^*$  has cocones for diagrams of 2-cells of shape  $\bullet \rightrightarrows \bullet \leftleftarrows \bullet$  that are mapped to pushouts of 2-cells in **CoIns** is quite realistic. In particular, it is possible to add suitable cocones to Hom-categories in  $Ind^*$  and interpret these as pushouts in **CoIns**.

## 6 Amalgamation and Exactness

The amalgamation property (called ‘exactness’ in [6]) is a major technical assumption in the study of specification semantics [20] and is important in many respects. It allows the computation of normal forms for specifications [1, 2], and it is a prerequisite for good behaviour w.r.t. parameterization, conservative extensions [6] and proof systems [16].

**Definition 23.** A cocone for a diagram in **Sign** is called *(weakly) amalgamable* if it is mapped to a (weak) limit under **Mod**.  $I$  (or **Mod**) admits *(finite) (weak) amalgamation* if (finite) colimit cocones are (weakly) amalgamable, i.e. if **Mod** maps (finite) colimits to (weak) limits. This property is also called (weak) exactness, while (weak) semi-exactness is its restriction to pushout diagrams.  $\square$

More generally, given a diagram  $D: J \rightarrow \mathbf{Sign}^I$ , a family of models  $(M_j)_{j \in |J|}$  is called *D-consistent* if  $M_k|_{D(\delta)} = M_j$  for each  $\delta: j \rightarrow k \in J$ . A cocone  $(\Sigma, (\mu_j)_{j \in |J|})$  over the diagram in  $D: J \rightarrow \mathbf{Sign}^I$  is called *weakly amalgamable* if for each  $D$ -consistent family of models  $(M_j)_{j \in |J|}$ , there is a  $\Sigma$ -model  $M$  with  $M|_{\mu_j} = M_j$  ( $j \in |J|$ ). If this model is unique, the cocone is called *amalgamable*.

**Proposition 24.** An institution admits (weak) amalgamation iff each colimiting cocone in the category of signatures is (weakly) amalgamable.  $\square$

A further weakening just requires the existence of weakly amalgamable cocones:

**Definition 25.** Call an institution  $I$  *quasi-exact* if for each diagram  $D: J \rightarrow \mathbf{Sign}^I$ , there is some weakly amalgamable cocone over  $D$ . *Quasi-semi-exactness* is the restriction of this notion to diagrams of shape  $\bullet \leftarrow \bullet \rightarrow \bullet$ .

The importance of this definition lies in the fact that it

1. interacts quite nicely with heterogeneous specification (the property holds for Grothendieck institutions under very mild and practically feasible assumptions), and it
2. is a prerequisite for the (soundness and completeness of the) proof calculus of development graphs [15, 16].

The theory of amalgamation and exactness in Grothendieck institutions for indexed institutions has been developed by Diaconescu [5]. Actually, the corresponding theory for indexed institutions turns out to be much simpler [13].

**Theorem 26.** Let  $\mathcal{I}: Ind^{op} \rightarrow \mathbf{CoIns}$  be an indexed coinstitution and  $K$  be some small category such that

1.  $Ind$  is  $K$ -complete,
2.  $\Phi^d$  is  $K$ -cocontinuous for each  $d: i \rightarrow j \in Ind$ , and
3. the indexed category of signatures of  $\mathcal{I}$  is locally  $K$ -cocomplete (the latter meaning that  $\mathbf{Sign}^i$  is  $K$ -cocomplete for each  $i \in |Ind|$ ).

Then the signature category  $\mathbf{Sign}^\#$  of the Grothendieck institution has  $K$ -colimits.  $\square$

We cannot expect that this result directly carries over to the quotient Grothendieck institution, since quotients of categories generally do not interact well with colimits. However, we can say something provided that we work with a quotient of the index category  $Ind$ :

**Proposition and Definition 27** Given a 2-category  $Ind$ , the relation of being in the same connected component of a Hom-category defines a congruence  $\equiv$  on the objects of the Hom-categories, i.e. the morphisms of  $Ind$ .  $Ind/\equiv$  is the corresponding quotient 1-category.  $\square$

**Lemma 28.** Given a 2-indexed coinstitution  $\mathcal{I}: Ind^* \rightarrow \mathbf{CoIns}$ , if  $(d_2, \sigma_1) \equiv (d_1, \sigma_2)$  in  $\mathbf{Sign}^\#$ , then  $d_1 \equiv d_2$ .  $\square$

**Proposition 29.** Assume that  $Ind^*$  has cocones for diagrams of 2-cells of shape  $\bullet \rightrightarrows \bullet \leftleftarrows \bullet$  that are mapped to pushouts of 2-cells in  $\mathbf{CoIns}$ . Then the congruence  $\equiv$  in  $Ind$  defined above is explicitly given by  $d_1: i \rightarrow j \equiv d_2: i \rightarrow j$  iff there exist  $d: i \rightarrow j \in Ind$  and  $u_1: d \rightarrow d_1, u_2: d \rightarrow d_2 \in Ind$ .  $\square$

**Theorem 30.** Let  $\mathcal{I}: Ind^* \rightarrow \mathbf{CoIns}$  be a 2-indexed coinstitution such that

1.  $Ind/\equiv$  is  $K$ -complete for some small category  $K$ ,
2. each connected component (considered as a subcategory) of a Hom-category  $Ind(i, j)$  has a distinguished canonical weakly terminal object, such that these canonical objects are stable under composition,
3.  $(d, \sigma_1) \equiv (d, \sigma_2)$  in  $\mathbf{Sign}^\#$  implies  $\sigma_1 = \sigma_2$ ,
4.  $\Phi^d$  is  $K$ -cocontinuous for each  $d: i \rightarrow j \in Ind$ , and
5. the indexed category of signatures of  $\mathcal{I}$  is locally  $K$ -cocomplete.

Then the signature category  $\mathbf{Sign}^\#/\equiv$  of the quotient Grothendieck institution has  $K$ -colimits. (Note that assumptions 2 and 3 are vacuous in case of discrete Hom-categories; we then get Theorem 26 as a special case.)  $\square$

By contravariance of  $\mathcal{I}$ , assumption 2 of the above proposition means that if institution comorphisms are linked by modifications, there is always a “smallest” comorphism that can be embedded into the other ones. This is quite realistic in practice. However, it is not so realistic to assume that these smallest comorphisms are stable under composition. For example, the composition of the smallest embedding of  $FOL^=$  into CASL with the smallest embedding of CASL

into second-order logic will give not given the smallest embedding of  $FOL^=$  into second-order logic, but rather a more complex one.

Assumption 3 basically means that the congruence does not identify signature morphisms within one institution, i.e. that each signature category  $\mathbf{Sign}^i$  is faithfully embedded into  $\mathbf{Sign}^\#/\equiv$ . This assumption is a reasonable and desirable property in practice. We record this explicitly:

**Proposition 31.**  $emb^i: \mathbf{Sign}^i \longrightarrow \mathbf{Sign}^\#/\equiv$  is an embedding preserving colimits under the assumptions of Theorem 30.  $\square$

Let us now come to exactness. We extend the notion of semi-exactness to comorphisms and to the indexed case. An institution comorphism  $(\Phi, \alpha, \beta)$  is called (weakly) exact, if the naturality squares for  $\beta$  are (weak) pullbacks. An 2-indexed coinstitution  $\mathcal{I}: Ind^* \longrightarrow \mathbf{CoIns}$  is called (weakly) locally semi-exact, if each institution  $I^i$  is (weakly) semi-exact ( $i \in |Ind|$ ). Assuming that equivalence classes of 2-cells have canonical weakly terminal objects,  $\mathcal{I}$  is called (weakly) semi-exact if for each pullback in  $Ind/\equiv$

$$\begin{array}{ccc} i & \xleftarrow{[d_1]} & j1 \\ [d_2] \uparrow & & [e_1] \uparrow \\ j2 & \xleftarrow{[e_2]} & k \end{array}$$

the square

$$\begin{array}{ccc} \mathbf{Mod}^i(\Sigma) & \xleftarrow{\beta_\Sigma^{d_1}} & \mathbf{Mod}^{j1}(\Phi^{d_1}(\Sigma)) \\ \beta_\Sigma^{d_2} \uparrow & & \beta_\Sigma^{e_1} \uparrow \\ \mathbf{Mod}^{j2}(\Phi^{d_2}(\Sigma)) & \xleftarrow{\beta_\Sigma^{e_2}} & \mathbf{Mod}^k(\Phi^{e_1}(\Phi^{d_1}(\Sigma))) = \mathbf{Mod}^k(\Phi^{e_2}(\Phi^{d_2}(\Sigma))) \end{array}$$

is a (weak) pullback for each signature  $\Sigma$  in  $\mathbf{Sign}^i$ , where canonical weakly terminal representatives are used.<sup>5</sup>

**Theorem 32.** Assume that the 2-indexed coinstitution  $\mathcal{I}: Ind^* \longrightarrow \mathbf{CoIns}$  fulfills the assumptions of Theorem 30. Then the quotient Grothendieck institution  $\mathcal{I}^\#/\equiv$  is (weakly) semi-exact if and only if

1.  $\mathcal{I}$  is (weakly) locally semi-exact,
2.  $\mathcal{I}$  is (weakly) semi-exact, and
3. for all canonical weakly terminal  $d: i \longrightarrow j \in Ind$ , in  $\mathcal{I}^d$  is (weakly) exact.  $\square$

<sup>5</sup> It might be useful to weaken these notions in the way such that model morphisms are ignored.

Theorems 26, 30 and 32 already provide a good theoretical basis for heterogeneous specification. However, in some cases, these theorems are not general enough: Given a diagram  $J \rightarrow \text{Ind}$ , its limit must be the index of some institution that can serve to encode (via comorphisms) all the institutions indexed by the diagram. While the existence of such an institution may not be a problem (e.g. higher-order logic often serves as such a “universal” logic for coding other logics), the uniqueness condition imposed by the limit property is more problematic. This means that any two such “universal” institutions must have isomorphic indices and hence be isomorphic themselves. This might work well in some circumstances, but may not be desirable in others: after all, a number of non-isomorphic logics, such as classical higher-order logic, the calculus of constructions and rewriting logic have been proposed as such a “universal” logic.<sup>6</sup>

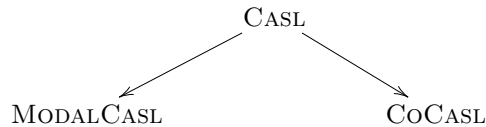
A related problem<sup>7</sup> is that the assumptions of Theorem 32 are too strong to be met for all practical examples. E.g. the CASL institution is not weakly semi-exact, and its encoding into  $HOL^\equiv$  [14] is neither exact, nor does it have a cocontinuous signature translation.

We hence now generalize the previous results by replacing weak exactness with quasi-exactness, i.e. amalgamable colimits with weakly amalgamable cocones, and thereby dropping the uniqueness requirement. Hence, several non-isomorphic “universal” institutions may coexist peacefully with our approach, and also non-exact institutions and comorphisms may be included in the indexed coinstitution serving as basis for heterogeneous specification.

We first extend Def. 25 to indexed coinstitution:

**Definition 33.** An indexed coinstitution  $\mathcal{I}: \text{Ind}^{op} \rightarrow \mathbf{CoIns}$  is called *locally quasi-exact*, if each institution  $\mathcal{I}^i$  is quasi-exact ( $i \in |\text{Ind}|$ ). It is called *quasi-exact*, if for each diagram  $D: J \rightarrow \text{Ind}$ , there is some cone  $(l, (d_j)_{j \in |J|})$  over  $D$  whose image under  $\mathcal{I}$  is weakly amalgamable. *Quasi-semi-exactness* is the restriction of these notions to diagrams of shape  $\bullet \longleftarrow \bullet \longrightarrow \bullet$ .  $\square$

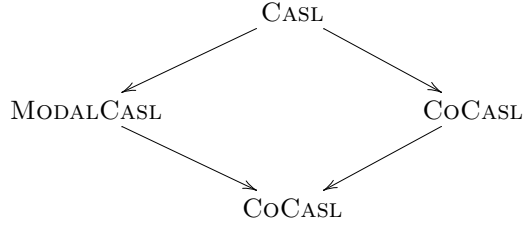
However, for the index level, even quasi-exactness may be too strong. Consider the diagram



How do we obtain a weakly amalgamable cocone? A simple way is to use the embedding of MODALCASL into CASL and compose it with the inclusion of CASL into CoCASL:

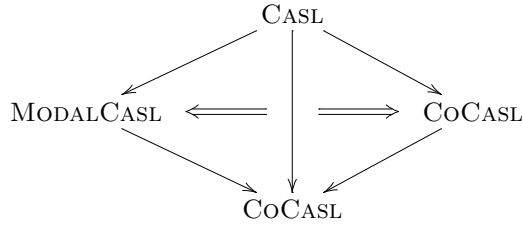
<sup>6</sup> This problem can possibly be circumvented by formally adjoining limits to the index category, which are then interpreted using Grothendieck institutions over subdiagrams. However, this would add considerable complexity to the construction.

<sup>7</sup> This problem already has been noted by Diaconescu [5] for his more special version of Theorem 32; see [13] why we consider it to be more special.



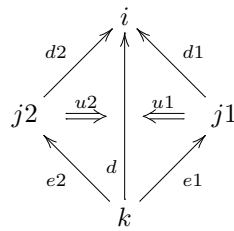
but the resulting square does not even commute.<sup>8</sup> The reason is that on the way from CASL to CoCASL via MODALCASL, MODALCASL adds an implicit set of worlds, which is made explicit by the embedding of MODALCASL into CASL.<sup>9</sup> To obtain a commuting square, we would need to have a comorphism from CoCASL to itself which adds an explicit set of worlds. However, this solution is rather inelegant, since it means that any (present or future) extension of CASL without possible world semantics (e.g. for HASCASL), we need a similar comorphism.

We hence prefer to split the square into two lax triangles:



and indeed, the square is weakly amalgamable in the following sense:

**Definition 34.** Given a 2-indexed coinstitution  $\mathcal{I}: \text{Ind}^* \rightarrow \mathbf{CoIns}$ , a square consisting of two lax triangles of index morphisms



<sup>8</sup> Of course, we could also embed everything into *HOL*, which would not cause any relevant change to the subsequent discussion.

<sup>9</sup> See [15] for the reason why the set of worlds cannot be omitted even for models of signatures without modalities.

is called (weakly) amalgamable, if the following diagram is a (weak) pullback

$$\begin{array}{ccccc}
\mathbf{Mod}^i(\Sigma) & \xleftarrow{\beta_{\Sigma}^{d1}} & & & \mathbf{Mod}^{j1}(\Phi^{d1}(\Sigma)) \\
\uparrow \beta_{\Sigma}^{d2} & & \swarrow \beta_{\Sigma}^d & & \uparrow \beta_{\Sigma}^{e1} \\
& & \mathbf{Mod}^k(\Phi^d(\Sigma)) & \xleftarrow{\mathbf{Mod}^k(\mathcal{I}_{\Sigma}^{u1})} & \mathbf{Mod}^k(\Phi^{e1}(\Phi^{d1}(\Sigma))) \\
& & \uparrow \mathbf{Mod}^k(\mathcal{I}_{\Sigma}^{u2}) & & \uparrow \text{dotted} \\
\mathbf{Mod}^{j2}(\Phi^{d2}(\Sigma)) & \xleftarrow{\beta_{\Sigma}^{e2}} & \mathbf{Mod}^k(\Phi^{e2}(\Phi^{d2}(\Sigma))) & \xleftarrow{\text{dotted}} & \bullet
\end{array}$$

where the lower right square is a pullback. That is, each pair consisting of a  $\Phi^{d2}(\Sigma)$ - and a  $\Phi^{d1}(\Sigma)$ -model with the same  $\Sigma$ -reduct is (weakly) amalgamable to a pair consisting of a  $\Phi^{e2}(\Phi^{d2}(\Sigma))$ - and a  $\Phi^{e1}(\Phi^{d1}(\Sigma))$ -model having the same  $\Phi^d(\Sigma)$ -reduct.

$\mathcal{I}$  is called *lax-quasi-exact*, if each for pair of arrows  $j1 \xrightarrow{d1} i \xleftarrow{d2} j2$  in  $Ind$ , there is some square

$$\begin{array}{ccc}
& & i \\
& \nearrow & \uparrow \\
j1 & \Rightarrow & j2 \\
& \searrow & \downarrow \\
& & k
\end{array}$$

consisting of a weakly amalgamable square of lax triangles, such that additionally  $\mathcal{I}^k$  is quasi-semi-exact.  $\square$

Note that this property is different from (and indeed, incomparable to) amalgamability of the individual lax triangles:

**Definition 35.** Given a 2-indexed coinstitution  $\mathcal{I}: Ind^* \rightarrow \mathbf{CoIns}$ , a lax triangle of index morphisms

$$\begin{array}{ccc}
i & & \\
\downarrow & \searrow & \\
& & j \\
& \swarrow & \\
k & & 
\end{array}
\quad \Leftarrow$$

is called (weakly) amalgamable, if  $\mathcal{I}$  maps it to a (weakly) amalgamable lax triangle in the sense of Definition 15.  $\square$

**Theorem 36.** For a 2-indexed coinstitution  $\mathcal{I}: Ind^* \rightarrow \mathbf{CoIns}$ , assume that

- $\mathcal{I}$  is lax-quasi-exact, and
- all institution comorphisms in  $\mathcal{I}$  are weakly exact.

Then  $\mathcal{I}^\#/\equiv$  is quasi-semi-exact.  $\square$

Call a diagram *acyclic (connected)* if the graph underlying its index category is acyclic (connected) when the identity arrows are deleted.

**Corollary 37.** Let  $\mathcal{I}$  satisfy the assumptions of Theorem 36. Then  $\mathcal{I}^\#/\equiv$  admits weak amalgamation of finite acyclic connected diagrams.  $\square$

As stated above, the importance of these results lies in the fact that quasi-(semi-)exactness is a prerequisite for the (soundness and completeness of the) proof calculus of development graphs [15, 16]. Due to lack of space, we cannot go into the details here. Instead, we provide a simple application of a typical situation of a view (or a refinement) involving hiding, illustrating a simple application of the rule *Theorem-Hide-Shift* from the calculus of [15, 16].

**Proposition 38.** In an institution, let a span of theories

$$\begin{array}{ccc} & \Sigma & \\ \sigma_2 \swarrow & & \searrow \sigma_1 \\ (\Sigma_1, \Psi_1) & & (\Sigma_2, \Psi_2) \end{array}$$

be given. Then the refinement statement

$$\mathbf{Mod}(\sigma_1)^{-1}(\mathbf{Mod}(\sigma_2)(|\mathbf{Mod}(\Sigma_2, \Psi_2)|)) \subseteq |\mathbf{Mod}(\Sigma_1, \Psi_1)|$$

follows from (and, hence can be reduced to) the statement

$$\mathbf{Mod}(\Sigma_3, \theta_2(\Psi_2)) \subseteq \mathbf{Mod}(\Sigma_3, \theta_1(\Psi_1))$$

provided that

$$\begin{array}{ccc} & \Sigma & \\ \sigma_2 \swarrow & & \searrow \sigma_1 \\ \Sigma_1 & & \Sigma_2 \\ \theta_1 \searrow & & \swarrow \theta_2 \\ & \Sigma_3 & \end{array}$$

is a weakly amalgamable square.  $\square$

## 7 From Specifications to Programs

Consider a specification  $SortSpec$  of sorting written in CASL (let it have signature  $\Sigma_S$ ), and a sorting program  $SortProg$  written in PLNG (let it have signature  $\Sigma_P$ ). We can use the institution semi-morphism  $toCASL: PLNG \rightarrow CASL$  from example 8 to express that  $SortProg$  is an implementation of  $SortSpec$ . Let  $(\Phi, \beta)$  be  $toCASL$  decomposed in its signature and model translation component. Then the property that we need to express is

$$\beta_{\Sigma_P}(\mathbf{Mod}^{PLNG}(SortProg)) \subseteq \mathbf{Mod}^{CASL}(SortSpec)$$

assuming that  $\Phi(\Sigma_P) = \Sigma_S$  (if needed, we can ensure this property by massaging the CASL specification appropriately).

Now the question arises how to prove this property. It would be easy if  $toCASL$  could be extended to an institution morphism; however, there is no hope to translate CASL formulas into programs. However, we can split the semi-morphism  $toCASL = (\Phi, \beta)$  into a span of comorphisms

$$PLNG \xleftarrow{toCASL^-} CASL \circ \Phi \xrightarrow{toCASL^+} CASL$$

as follows:

$$\begin{array}{ccccc} \mathbf{Sign}^{PLNG} & \xleftarrow{id} & \mathbf{Sign}^{PLNG} & \xrightarrow{\Phi} & \mathbf{Sign}^{CASL} \\ \mathbf{Sen}^{PLNG} & \xleftarrow{incl} & \emptyset & \xrightarrow{incl} & \mathbf{Sen}^{CASL \circ \Phi} \\ \mathbf{Mod}^{PLNG} & \xrightarrow{\beta} & \mathbf{Mod}^{CASL \circ \Phi^{op}} & \xleftarrow{id} & \mathbf{Mod}^{CASL \circ \Phi^{op}} \end{array}$$

Here, the “middle” institution  $CASL \circ \Phi$  is the institution with signature category inherited from PLNG, no sentences, and models inherited from CASL via  $\Phi$ .

Our refinement statement can now be reformulated in terms of comorphisms:

$$(\beta_{\Sigma_P}^{toCASL^+})^{-1}(\beta_{\Sigma_P}^{toCASL^-}(\mathbf{Mod}^{PLNG}(SortProg))) \subseteq \mathbf{Mod}^{CASL}(SortSpec)$$

We can regard this in a suitable Grothendieck institution; then it has exactly the form of the statement in Prop. 38. We hence can reformulate the statement, provided that we have quasi-semi-exactness. By Theorem 36, we need lax-quasi-exactness of the indexed coinstitution. The essential ingredient to find a square of two weakly amalgamable lax triangles for the span

$PLNG \xleftarrow{toCASL^-} CASL \circ \Phi \xrightarrow{toCASL^+} CASL$ . But this can e.g. be given by coding of both CASL and PLNG into a common logic such as higher order logic (indexing institutions and comorphisms by themselves):

$$\begin{array}{ccccc} & & HOL & & \\ & PLNG2HOL \nearrow & \uparrow & \nwarrow CASL2HOL & \\ PLNG & \xrightarrow{id} & & \xleftarrow{\theta} & CASL \\ & toCASL^- \searrow & \downarrow & \nearrow toCASL^+ & \\ & & CASL \circ \Phi & & \end{array}$$

By Theorem 36, this lead to a weakly amalgamable square in the Grothendieck institution:

$$\begin{array}{ccc}
 & (\text{CASL} \circ \Phi, \Sigma_P) & \\
 \begin{array}{c} \swarrow \\ (toCASL^-, id) \end{array} & & \begin{array}{c} \searrow \\ (toCASL^+, id) \end{array} \\
 (\text{PLNG}, \Sigma_P) & & (\text{CASL}, \Sigma_S) \\
 \begin{array}{c} \searrow \\ (PLNG2HOL, id) \end{array} & & \begin{array}{c} \swarrow \\ (CASL2HOL, \theta_{\Sigma_S}) \end{array} \\
 & (\text{HOL}, \text{PLNG2HOL}(\Sigma_P)) &
 \end{array}$$

By Prop. 38, our refinement statement can now be reformulated as follows:

$$\mathbf{Mod}^{\text{HOL}}(\text{PLNG2HOL}(\text{SortProg})) \subseteq \mathbf{Mod}^{\text{HOL}}(\theta(\text{CASL2HOL}(\text{SortSpec})))$$

which is amount to proving, in HOL,

$$\text{PLNG2HOL}(\text{SortProg}) \vdash \theta(\text{CASL2HOL}(\text{SortSpec})).$$

An implementation of this machinery for the case PLNG=Haskell is under way, to become part of the Heterogeneous Tool Set HETS [15, 17].

**Acknowledgments** There are a number of colleagues who have introduced me into the field and who always are open for interesting discussions and collaborations; here I shall name only Joseph Goguen, Răzvan Diaconescu and Andrzej Tarlecki. Andrzej Tarlecki made very valuable comments on a draft.

This work has been supported by the *Deutsche Forschungsgemeinschaft* under Grants KR 1191/5-1 and KR 1191/5-2.

## References

1. J. Bergstra, J. Heering, and P. Klint. Module Algebra. *J. ACM*, 37(2):335–372, 1990.
2. T. Borzyszkowski. Generalized interpolation in CASL. *Information Processing Letters*, 76/1-2:19–24, 2000.
3. CoFI (The Common Framework Initiative). *CASL Reference Manual*. LNCS Vol. 2960 (IFIP Series). Springer, 2004.
4. R. Diaconescu. *Institution-independent Model Theory*. To appear. Book draft. (Ask author for a current draft.).
5. R. Diaconescu. Grothendieck institutions. *Applied categorical structures*, 10:383–402, 2002.
6. R. Diaconescu, J. Goguen, and P. Stefanias. Logical support for modularisation. In G. Huet and G. Plotkin, editors, *Proceedings of a Workshop on Logical Frameworks*, 1991.
7. J. Goguen and G. Roşu. Institution morphisms. *Formal aspects of computing*, 13:274–307, 2002.

8. J. A. Goguen and R. M. Burstall. Introducing institutions. volume 164 of *Lecture Notes in Computer Science*, pages 221–256. Springer Verlag, 1984.
9. J. A. Goguen and R. M. Burstall. A study in the foundations of programming methodology: Specifications, institutions, charters and parchments. In D. P. et al., editor, *Category Theory and Computer Programming*, volume 240 of *Lecture Notes in Computer Science*, pages 313–333. Springer Verlag, 1985.
10. J. A. Goguen and R. M. Burstall. Institutions: Abstract model theory for specification and programming. *Journal of the Association for Computing Machinery*, 39:95–146, 1992. Predecessor in: LNCS 164, 221–256, 1984.
11. H. Herrlich and G. Strecker. *Category Theory*. Allyn and Bacon, Boston, 1973.
12. S. Mac Lane. *Categories for the Working Mathematician*. Springer, 1998. Second edition.
13. T. Mossakowski. Comorphism-based Grothendieck logics. In K. Diks and W. Rytter, editors, *Mathematical foundations of computer science*, volume 2420 of *LNCS*, pages 593–604. Springer, 2002.
14. T. Mossakowski. Relating CASL with other specification languages: the institution level. *Theoretical Computer Science*, 286:367–475, 2002.
15. T. Mossakowski. Heterogeneous specification and the heterogeneous tool set. Habilitation thesis, University of Bremen, 2005.
16. T. Mossakowski, S. Autexier, and D. Hutter. Development graphs – proof management for structured specifications. *Journal of Logic and Algebraic Programming*, 67(1-2):114–145, 2006.
17. T. Mossakowski, C. Maeder, K. Lüttich, and S. Wölfl. The heterogeneous tool set. Submitted for publication.
18. T. Mossakowski, L. Schröder, M. Roggenbach, and H. Reichel. Algebraic-co-algebraic specification in CoCASL. *Journal of Logic and Algebraic Programming*, 67(1-2):146–197, 2006.
19. G. Roşu and J. Goguen. Composing hidden information modules over inclusive institutions, 2004.
20. D. Sannella and A. Tarlecki. Specifications in an arbitrary institution. *Information and Computation*, 76:165–210, 1988.
21. A. Tarlecki. Moving between logical systems. In M. Haveranen, O. Owe, and O.-J. Dahl, editors, *Recent Trends in Data Type Specifications. 11th Workshop on Specification of Abstract Data Types*, volume 1130 of *Lecture Notes in Computer Science*, pages 478–502. Springer Verlag, 1996.
22. A. Tarlecki, R. M. Burstall, and J. A. Goguen. Some fundamentals algebraic tools for the semantics of computation. Part 3: Indexed categories. *Theoretical Computer Science*, 91:239–264, 1991.

## A Proofs of the Theorems

Proof of Prop. 16. Given comorphisms  $(\Phi_i, \rho_i): I \longrightarrow J$  ( $i = 1, 2, 3$ ) and a span of modifications

$$\begin{array}{ccc}
 & (\Phi_1, \rho_1) & \\
 \tau_1 \swarrow & & \searrow \tau_2 \\
 (\Phi_2, \rho_2) & & (\Phi_3, \rho_3)
 \end{array}$$

construct the signature component  $\Phi(\Sigma)$  of the resulting comorphism as the pushout

$$\begin{array}{ccc}
 & \Phi_1(\Sigma) & \\
 (\tau_1)_\Sigma \swarrow & & \searrow (\tau_2)_\Sigma \\
 \Phi_2(\Sigma) & & \Phi_3(\Sigma) \\
 \text{\scriptsize $\dots\dots$} \searrow & & \swarrow \text{\scriptsize $\dots\dots$} \\
 & \Phi(\Sigma) & \\
 (\theta_2)_\Sigma \searrow & & \swarrow (\theta_1)_\Sigma
 \end{array}$$

By the universal property of the pushout, this extends to a functor  $\Phi: \mathbf{Sign}^I \longrightarrow \mathbf{Sign}^J$  such that  $\theta_1: \Phi_3 \longrightarrow \Phi$  and  $\theta_2: \Phi_2 \longrightarrow \Phi$  become natural transformations.

$$\begin{array}{ccccc}
 & & I & & \\
 & \rho_2 \swarrow & \downarrow \rho_1 & \searrow \rho_3 & \\
 J \circ \Phi_2 & \xleftarrow{J \cdot \tau_1} & J \circ \Phi_1 & \xrightarrow{J \cdot \tau_2} & J \circ \Phi_3 \\
 & \searrow J \cdot \theta_2 & & \swarrow J \cdot \theta_1 & \\
 & & J \circ \Phi & & 
 \end{array}$$

We can then define room component of the pushout comorphism  $\rho: I \longrightarrow J \circ \Phi$  to be  $J \cdot \theta_2 \circ \rho_2 = J \cdot \theta_1 \circ \rho_3$ , and the cocone consisting of  $\theta_1: (\Phi_3, \rho_3) \Longrightarrow (\Phi, \rho)$  and  $\theta_2: (\Phi_2, \rho_2) \Longrightarrow (\Phi, \rho)$  is easily seen to satisfy the universal property of a pushout.

The proof for coproducts, coequalizers or arbitrary non-empty colimits of connected diagrams is very similar.  $\square$

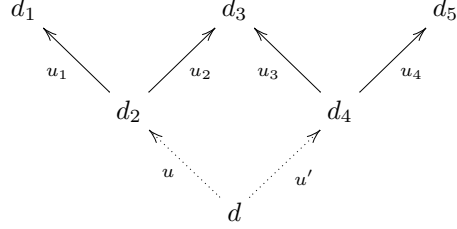
Proof of Prop. 17: The initial institution morphism  $(\Phi, \mu): I \longrightarrow J$  is defined by letting  $\Phi(\Sigma)$  be the initial signature, and  $\mu_\Sigma$  consist of the empty map of sentences and the unique functor into the terminal model category.  $\square$

Proof of Prop. 20: By the definition of comorphism modification,  $(\mathcal{I}^j \cdot \mathcal{I}^u) \circ \rho^{d'} = \rho^d$ . But this just means that equivalent signature morphisms induce the same corridors.  $\square$

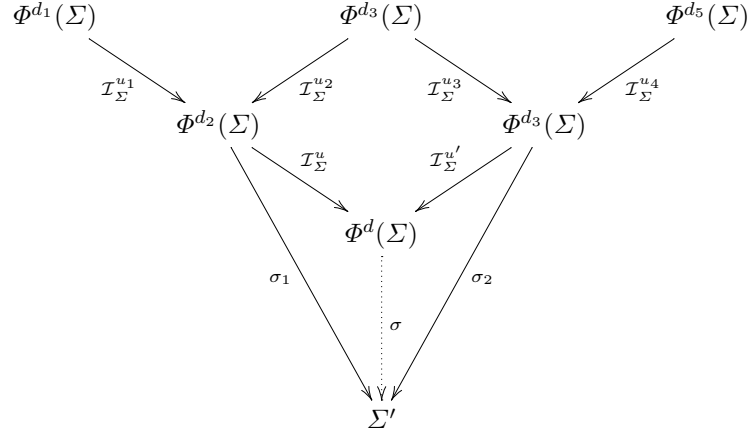
Proof of Prop. 22: It is easy to see that the above relation is contain in the relation generated by (1): just apply (1) twice. It remains to show that the above relation is a congruence. Reflexivity and symmetry are clear. Concerning transitivity, assume that

$$(d_1, \sigma_1 \circ \mathcal{I}_\Sigma^{u_1}) \equiv (d_3, \sigma_1 \circ \mathcal{I}_\Sigma^{u_2}) = (d_3, \sigma_2 \circ \mathcal{I}_\Sigma^{u_3}) \equiv (d_5, \sigma_2 \circ \mathcal{I}_\Sigma^{u_4}),$$

the first relation being witnessed by  $u_1 : d_2 \Rightarrow d_1, u_2 : d_2 \Rightarrow d_3$ , and the second by  $u_3 : d_4 \Rightarrow d_3, u_4 : d_4 \Rightarrow d_5$ . Take the pullback in  $\mathbf{Ind}(j, i)$  of the two spans



By the construction of pushouts of 2-cells in **CoIns** (see Prop.16), the middle square in



is a pushout, and the mediating morphism  $\sigma$  leads to the desired form

$$(d_1, \sigma_1 \circ \mathcal{I}_{\Sigma}^{u_1}) = (d_1, \sigma \circ \mathcal{I}_{\Sigma}^{u_1 \circ u}) \equiv (d_5, \sigma \circ \mathcal{I}_{\Sigma}^{u_4 \circ u'}) = (d_5, \sigma_2 \circ \mathcal{I}_{\Sigma}^{u_4}).$$

Concerning composition, assume that

$$(d_1, \sigma \circ \mathcal{I}_{\Sigma}^{u_1}) \equiv (d_2, \sigma \circ \mathcal{I}_{\Sigma}^{u_2})$$

via  $u_1 : d \Rightarrow d_1, u_2 : d \Rightarrow d_2$ , and

$$(e_1, \tau \circ \mathcal{I}_{\Sigma'}^{v_1}) \equiv (e_2, \tau \circ \mathcal{I}_{\Sigma'}^{v_2})$$

via  $v_1 : e \Rightarrow e_1, v_2 : e \Rightarrow e_2$ . Then for  $k = 1, 2$ ,

$$\begin{aligned} & (e_k, \sigma \circ \mathcal{I}_{\Sigma}^{u_k}) \circ (d_k, \tau \circ \mathcal{I}_{\Sigma'}^{v_k}) \\ &= (d_k \circ e_k, \sigma \circ \mathcal{I}_{\Sigma}^{u_k} \circ \Phi^{e_k}(\tau) \circ \Phi^{e_k}(\mathcal{I}_{\Sigma'}^{v_k})) && \text{(def. Grothendieck composition)} \\ &= (d_k \circ e_k, \sigma \circ \Phi^{e_k}(\tau) \circ \Phi^{e_k}(\mathcal{I}_{\Sigma'}^{v_k}) \circ \mathcal{I}_{\Phi^{e_k}(\Sigma')}^{u_k}) && \text{(naturality of } \mathcal{I}^{u_k} \text{)} \\ &= (d_k \circ e_k, \sigma \circ \Phi^{e_k}(\tau) \circ \mathcal{I}_{\Sigma'}^{v_k \cdot u_k}) && \text{(functoriality of } \mathcal{I} \text{)} \end{aligned}$$

which shows that we arrive at the desired form.  $\square$

Proof of Thm. 26: Apply Theorem 1 of [22] with  $C_i = \mathbf{Sign}^i$  and  $C_m = \Phi^m$ . Note that  $\mathbf{Sign}^\#$  is then  $Flat(C^{op})^{op}$ .  $\square$

Proof of Lemma 28: Easy induction over the definition of  $(d_1, \sigma_1) \equiv (d_2, \sigma_2)$ .  $\square$

Proof of Prop. 29: Analogous to the proof of Prop. 22.  $\square$

Proof of Thm. 30: The proof idea follows that of Theorem 1 in [22], the necessary modifications being caused by the congruences. By assumption 2, we can always choose representatives  $d \in Ind$  of congruence classes  $[d] \in Ind/\equiv$  in such a way that  $d$  is a canonical weakly terminal object. Similarly, we can always choose representatives  $(d, \sigma)$  of congruence classes  $[(d, \sigma)]$  in  $\mathbf{Sign}^\#/\equiv$  in such a way that  $d$  is the canonical weakly terminal object in its connected component: given an arbitrary  $(d, \sigma: \Phi^d(\Sigma) \rightarrow \Sigma')$  in  $\mathbf{Sign}^\#$ , let  $u: d \rightrightarrows t$  be a 2-cell into the canonical weakly terminal object. Then  $(t, \sigma \circ \mathcal{I}_\Sigma^u)$  is equivalent to  $(d, \sigma)$ .

Given a diagram  $D: K \rightarrow \mathbf{Sign}^\#/\equiv$ , we introduce the notation  $(i_k, \Sigma_k)$  for  $D(k)$  ( $k \in |K|$ ) and  $[(d_m, \sigma_m)]: (i_k, \Sigma_k) \rightarrow (i_{k'}, \Sigma_{k'})$  for  $D(m)$  ( $m: k \rightarrow k' \in K$ ). Let  $\bar{D}: K \rightarrow Ind/\equiv$  be the projection of  $D$  to the first component; by Lemma 28 this is a well-defined diagram in  $Ind/\equiv$ . By assumption 1,  $\bar{D}$  has a limit  $[(m_k]: i \rightarrow i_k)_{k \in |K|}$ .

Let the diagram  $G: K \rightarrow \mathbf{Sign}^i$  be defined by

$$\begin{aligned} G(k) &= \Phi^{m_k}(\Sigma_k) \quad (k \in |K|) \\ G(m) &= \Phi^{m_k}(\sigma_m) \quad (m: k' \rightarrow k \in K) \end{aligned}$$

Note that  $m_k$  is chosen to be canonical weakly terminal in  $[m_k]$ . By assumption 5,  $G$  has a colimit  $(\sigma_k: G(k) \rightarrow \Sigma)_{k \in |K|}$ . We show that  $([(m_k, \sigma_k)]: (i_k, \Sigma_k) \rightarrow (i, \Sigma))_{k \in |K|}$  is a colimit of  $D$ .

Since equality implies congruence,  $([(m_k, \sigma_k)])_{k \in |K|}$  is a cocone of  $D$ . Let  $([(n_k, \theta_k)]: (i_k, \Sigma_k) \rightarrow (i', \Sigma'))_{k \in |K|}$  be another cocone. By Lemma 28,  $([n_k]: i' \rightarrow i_k)_{k \in |K|}$  is a cocone for  $\bar{D}$ . Hence there is a unique  $[d]: i' \rightarrow i$  with  $[m_k] \circ [d] = [n_k]$ . Since we choose representatives canonically in a way closed under composition,  $m_k \circ d = n_k$ .

By assumption 4,  $(\Phi^d(\sigma_k))_{k \in |K|}$  is a colimit of  $\Phi^d \circ G$ . Note that the source of  $\Phi^d(\sigma_k)$  is  $\Phi^d(G(k)) = \Phi^d(\Phi^{m_k}(\Sigma_k)) = \Phi^{n_k}(\Sigma_k)$ . By the cocone property of  $([(n_k, \theta_k)])_{k \in |K|}$ ,  $(n_k, \theta_k) \equiv (d_m \circ n_{k'}, \theta_{k'} \circ \Phi^{n_{k'}}(\sigma_m))$  for  $m: k \rightarrow k' \in K$ . By the assumption of weakly terminal canonical representatives,  $n_k = d_m \circ n_{k'}$ . By assumption 3,  $\theta_k = \theta_{k'} \circ \Phi^{n_{k'}}(\sigma_m)$ . This shows that  $(\theta_k: \Phi^{n_k}(\Sigma_k) \rightarrow \Sigma')_{k \in |K|}$  is a cocone for  $\Phi^d \circ G$ . Hence, there is a unique  $\tau: \Phi^d(\Sigma) \rightarrow \Sigma'$  with  $\tau \circ \Phi^d(\sigma_k) = \theta_k$ . Then  $[(d, \tau)]: (i, \Sigma) \rightarrow (i', \Sigma')$  is a unique morphism in  $\mathbf{Sign}^\#/\equiv$  such that  $[(d, \tau)] \circ [(m_k, \sigma_k)] = [(n_k, \theta_k)]$ .  $\square$

Proof of Prop. 31: Clearly,  $emb^i$  is injective on objects. Faithfulness follows from assumption 3. Preservation of colimits can be seen by inspecting the construction of the proof of Theorem 30: if the indices are all  $i$ , then the colimit is just that in  $\mathbf{Sign}^i$ .  $\square$

Proof of Thm. 32: “Only if”, 1: Following Prop. 2 in [5], it is easy to see that for each  $i \in |Ind|$ , the model functor  $\mathbf{Mod}^i$  is the restriction  $\mathbf{Mod}^\#(i, -)$  of the model functor of the Grothendieck institution to the subcategory  $\mathbf{Sign}^i$  of the Grothendieck signature category  $\mathbf{Sign}^\#/\equiv$ .

$$\begin{array}{ccc}
 (\mathbf{Sign}^i)^{op} & \xrightarrow{emb^i} & (\mathbf{Sign}^\#/\equiv)^{op} \\
 & \searrow \mathbf{Mod}^i & \downarrow \mathbf{Mod}^\# \\
 & & \mathcal{CAT}
 \end{array}$$

By Prop. 31, the canonical injection  $emb^i: \mathbf{Sign}^i \rightarrow \mathbf{Sign}^\#$  preserves colimits, hence  $\mathbf{Mod}^i$  takes pushouts to (weak) pullbacks because  $\mathbf{Mod}^\#$  does so.

“Only if”, 2: Given a pullback in  $Ind/\equiv$

$$\begin{array}{ccc}
 & i & \xleftarrow{[d_1]} & j1 \\
 [d_2] \uparrow & & & \uparrow [e_1] \\
 & j2 & \xleftarrow{[e_2]} & k
 \end{array}$$

choose  $d_1, d_2, e_1, e_2$  canonically. By the construction of colimits in Theorem 30, for any signature  $\Sigma$  in  $\mathbf{Sign}^i$ ,

$$\begin{array}{ccc}
 (i, \Sigma) & \xrightarrow{[(d_1, id)]} & (j1, \Phi^{d_1}(\Sigma)) \\
 \downarrow [(d_2, id)] & & \downarrow [(e_1, id)] \\
 (j2, \Phi^{d_2}(\Sigma)) & \xrightarrow{[(e_2, id)]} & (k, \Phi^{e_1}(\Phi^{d_1}(\Sigma))) = (k, \Phi^{e_2}(\Phi^{d_2}(\Sigma)))
 \end{array}$$

is a pushout in  $\mathbf{Sign}^\#/\equiv$  and is therefore mapped to a (weak) pullback by the model functor. This gives exactly the desired property.

“Only if”, 3: Let  $d: j \rightarrow i$  by canonical and  $\sigma: \Sigma_1 \rightarrow \Sigma_2$  a signature morphism in  $\mathbf{Sign}^i$ . By the construction of colimits in Theorem 30,

$$\begin{array}{ccc}
 (i, \Sigma_1) & \xrightarrow{[(id, \sigma)]} & (i, \Sigma_2) \\
 \downarrow [(d, id)] & & \downarrow [(d, id)] \\
 (j, \Phi^d(\Sigma_1)) & \xrightarrow{[(id, \Phi^d(\sigma))]} & (j, \Phi^d(\Sigma_2))
 \end{array}$$

is a pushout in  $\mathbf{Sign}^\#/\equiv$  and is therefore mapped to a (weak) pullback by the model functor. Again, this gives exactly the desired property.

“If”: Consider an arbitrary pushout in  $\mathbf{Sign}^\# / \equiv$

$$\begin{array}{ccc} (i, \Sigma_0) & \xrightarrow{[(d_1, \sigma_1)]} & (j_1, \Sigma_1) \\ \downarrow [(d_2, \sigma_2)] & & \downarrow [(e_1, \theta_1)] \\ (j_2, \Sigma_2) & \xrightarrow{[(e_2, \theta_2)]} & (k, \Sigma') \end{array}$$

and assume that representatives are chosen canonically. By the construction of colimits in Theorem 30, the above pushout can be expressed as the following composition of four pushout squares:

$$\begin{array}{ccccc} (i, \Sigma_0) & \xrightarrow{[(d_1, id)]} & (j_1, \Phi^{d_1}(\Sigma_0)) & \xrightarrow{[(id, \sigma_1)]} & (j_1, \Sigma_1) \\ \downarrow [(d_2, id)] & & \downarrow [(e_1, id)] & & \downarrow [(e_1, id)] \\ (j_2, \Phi^{d_2}(\Sigma_0)) & \xrightarrow{[(e_2, id)]} & (k, \Phi^{e_1}(\Phi^{d_1}(\Sigma_0))) = (k, \Phi^{e_2}(\Phi^{d_2}(\Sigma_0))) & \xrightarrow{[(id, \Phi^{e_1} \sigma_1)]} & (k, \Phi^{e_1}(\Sigma_1)) \\ \downarrow [(id, \sigma_2)] & & \downarrow [(id, \Phi^{e_2} \sigma_2)] & & \downarrow [(id, \theta_1)] \\ (j_2, \Sigma_2) & \xrightarrow{[(e_2, id)]} & (k, \Phi^{e_2}(\Sigma_2)) & \xrightarrow{[(id, \theta_2)]} & (k, \Sigma') \end{array}$$

Now the model functor of the quotient Grothendieck institution maps the upper left pushout to a (weak) pullback because the 2-indexed coinstitution is (weakly) semi-exact, maps the lower right pushout to a (weak) pullback because the 2-indexed coinstitution is (weakly) locally semi-exact, and maps the remaining two squares to (weak) pullbacks because the comorphisms for canonical index morphisms are (weakly) exact. Since (weak) pullback squares compose, the result follows.  $\square$

Proof of Thm. 36:

Let a diagram  $(j_1, \Sigma_1) \xleftarrow{(d_1, \sigma_1)} (i, \Sigma) \xrightarrow{(d_2, \sigma_2)} (j_2, \Sigma_2)$  in  $\mathbf{Sign}^\#$  be given. Let

$$\begin{array}{ccccc} & & i & & \\ & d_2 \nearrow & \uparrow & \nwarrow d_1 & \\ j_2 & \xrightarrow{u_2} & & \xleftarrow{u_1} & j_1 \\ & e_2 \searrow & d \downarrow & \nearrow e_1 & \\ & & k & & \end{array}$$

be a weakly amalgamable square of two lax triangles with  $\mathcal{I}^k$  quasi-semi-exact. By the latter property, there are  $\theta_1, \theta_2$  such that

$$\begin{array}{ccccc}
\Phi^d(\Sigma) & \xrightarrow{\mathcal{I}_\Sigma^{u_1}} & \Phi^{e_1}(\Phi^{d_1}(\Sigma)) & \xrightarrow{\Phi^{e_1}\sigma_1} & \Phi^{e_1}(\Sigma_1) \\
\downarrow \mathcal{I}_\Sigma^{u_2} & & & & \downarrow \theta_1 \\
\Phi^{e_2}(\Phi^{d_2}(\Sigma)) & & & & \downarrow \\
\downarrow \Phi^{e_2}\sigma_2 & & & & \downarrow \\
\Phi^{e_2}(\Sigma_2) & \xrightarrow{\theta_2} & & & \Sigma'
\end{array}$$

is a weakly amalgamable square, which leads to weak amalgamability of the lower right square in

$$\begin{array}{ccccc}
(i, \Sigma) & \xrightarrow{(d_1, id)} & (j_1, \Phi^{d_1}(\Sigma)) & \xrightarrow{(id, \sigma_1)} & (j_1, \Sigma_1) \\
\downarrow (d, id) & \searrow (d, id) & \downarrow (e_1, id) & & \downarrow (e_1, id) \\
(j_2, \Phi^{d_2}(\Sigma)) & \xrightarrow{(d_2, id)} & (k, \Phi^d(\Sigma)) & \xrightarrow{(id, \mathcal{I}_\Sigma^{u_1})} & (k, \Phi^{e_1}(\Phi^{d_1}(\Sigma))) & \xrightarrow{(id, \Phi^{e_1}(\sigma_1))} & (k, \Phi^{e_1}(\Sigma_1)) \\
\downarrow (d_2, id) & & \downarrow (id, \mathcal{I}_\Sigma^{u_2}) & & \downarrow (id, \theta_1) \\
(j_2, \Phi^{d_2}(\Sigma)) & \xrightarrow{(e_2, id)} & (k, \Phi^{e_2}(\Phi^{d_2}(\Sigma))) & & \downarrow (id, \theta_1) \\
\downarrow (id, \sigma_2) & & \downarrow (id, \Phi^{e_2}(\sigma_2)) & & \downarrow (id, \theta_1) \\
(j_2, \Sigma_2) & \xrightarrow{(e_2, id)} & (k, \Phi^{e_2}(\Sigma_2)) & \xrightarrow{(id, \theta_2)} & (k, \Sigma')
\end{array}$$

The upper right and lower left squares are weakly amalgamable by weak exactness of  $\mathcal{I}^{e_1}$  and  $\mathcal{I}^{e_2}$ . The pair of the remaining two squares is jointly weakly amalgamable since it is induced by a weakly amalgamable square of two lax triangles (and note that squares in  $\mathbf{Sign}^\# / \equiv$  induced by lax triangles in  $\mathbf{Ind}$  commute by definition of  $\equiv$ ). Since weakly amalgamable squares can be pasted together, we get a weakly amalgamable cocone for the original diagram.  $\square$

**Proof of Corollary 37:** In the sequel, we will use terms like “connected”, “maximal”, “lower bound” for small categories, when we really mean the pre-order obtained from the category by collapsing the hom-sets into singletons. A maximal element in a pre-order is an element which is equivalent to any element above it.

Let  $D: J \rightarrow \mathbf{Sign}^\#$  be a connected diagram and let  $Max$  be the set of maximal nodes in  $J$ . We successively construct new diagrams out of  $J$ . Take two nodes in  $Max$  that have a common lower bound (if two such nodes do not exist, the diagram is not connected). By Theorem 36, there is a weak amalgamating cocone for the sub-diagram consisting of the two maximal nodes and the lower bound (together with the arrows from the lower bound into the maximal nodes).

Extend the diagram with the cocone. The diagram thus obtained now has a set of maximal nodes whose size is decreased by one. By iterating this construction, we get a diagram with one maximal node. The maximal node then is just the tip of a weakly amalgamating cocone for the original diagram.  $\square$

Proof of Prop. 38:

A model  $M_1 \in |\mathbf{Mod}(\sigma_1)^{-1}(\mathbf{Mod}(\sigma_2(\mathbf{Mod}(\Sigma_2, \Psi_2))))|$  is nothing but a pair  $(M_1, M_2)$  of models  $M_1 \in |\mathbf{Mod}(\Sigma_1)|$ ,  $M_2 \in |\mathbf{Mod}(\Sigma_2, \Psi_2)|$  with common reduct to  $\Sigma$ . This pair can be amalgamated to a model  $M_3 \in |\mathbf{Mod}(\Sigma_3)|$ . Since  $M_3|_{\theta_2} = M_2$ , by the satisfaction condition,  $M_3 \models_{\Sigma_3} \theta_2(\Psi_2)$ . By the assumption, also  $M_3 \models_{\Sigma_3} \theta_1(\Psi_1)$ . But this means  $M_1 = M_3|_{\theta_1} \models_{\Sigma_1} \Psi_1$ .  $\square$