Refinement by interpretation in \(\pi\)-institutions

César J. Rodrigues  
Dep. Informatics & CCTC,  
Minho University, Portugal  
cjr@di.uminho.pt

Manuel A. Martins  
Dep. Mathematics,  
Aveiro University, Portugal  
martins@ua.pt

Alexandre Madeira  
Dep. Informatics & CCTC,  
Minho University, Portugal  
Dep. Mathematics,  
Aveiro University, Portugal  
Critical Software S.A., Portugal  
madeira@ua.pt

Luís S. Barbosa  
Dep. Informatics & CCTC,  
Minho University, Portugal  
lsb@di.uminho.pt

The paper discusses the role of interpretations, understood as multifunctions that preserve and reflect logical consequence, as refinement witnesses in the general setting of \(\pi\)-institutions. This leads to a smooth generalization of the “refinement by interpretation” approach, recently introduced by the authors in more specific contexts. As a second, yet related contribution a basis is provided to build up a refinement calculus of structured specifications in and across arbitrary \(\pi\)-institutions.

1 Introduction

The expression refinement by interpretation was coined in [MMB09b] to refer to an alternative approach to refinement of equational specifications in which signature morphisms are replaced by logical interpretations as refinement witnesses.

Intuitively, an interpretation is a logic translation which preserves and reflects meaning. Actually, it is a central tool in the study of equivalent algebraic semantics (see, e.g., [Woj88, BP89, BP01, BR03, Cze01]), a paradigmatic example being the interpretation of the classical propositional calculus into the equational theory of boolean algebras (cf. [BP01, Example 4.1.2]). Interestingly enough, and in the more operational setting of formal software development, the notion of interpretation proved effective to capture a number of transformations difficult to deal with in classical terms. Examples include data encapsulation and the decomposition of operations into atomic transactions [MMB09b].

A typical refinement pattern that is not easily captured by the classical approach concerns refinement of a subset of operations into operations defined over more specialized sorts. This kind of transformation induces the loss of the functional property on the operations’ component of signature morphisms. For example, there is not a signature morphism \(\sigma\) to guide a refinement where a specification with operations \(g : s' \to s\) and \(f : s' \to s\) is transformed into one with operations \(g : s' \to s_{\text{new}}\) and \(f : s' \to s\), since this translation naturally induces a map \(\sigma_{\text{sort}}(s) = \{s, s_{\text{new}}\}\) which violates the definition of signature morphism.

The approach seems also promising in the context of new, emerging computing paradigms which entail the need for more flexible approaches to what is taken as a valid transformation of specifications, as in, for example, [BSR04]. Later, in [MMB09a], the whole framework was generalized from the original equational setting to address deductive systems of arbitrary dimension. This made possible, for example, to refine sentential into equational specifications and the latter into modal ones. Moreover, the restriction to logics with finite consequence relations was dropped which resulted in increased flexibility.
Refinement by interpretation in \( \pi \)-institutions

along the software development process. The interested reader is referred to both papers for a number of illustrative examples.

On the other hand, the notion of an institution [GB92], proposed by J. Goguen and R. Burstall in the late 1970s, has proven very successful in formalizing logical systems and their interrelations.

This paper aims at lifting the use of logic interpretations to witness refinement of specifications at an institutional level. This is made in the context of \( \pi \)-institutions [FS88] which deal directly with syntactic consequence relations rather than with semantical satisfaction, as in the original definition of an institution [GB92]. \( \pi \)-institutions are particularly useful in formalizing deductive systems with varying signatures, which are only indirectly handled by the methods of abstract algebraic logic, as in [BP01] on which our first generalization [MMB09a] is based. In general, \( \pi \)-institutions provide a more operational framework with no loss of expressiveness as any classical institution can be suitably translated.

Refinement by interpretation is proposed here at two different levels: a macro level relating different \( \pi \)-institutions, and the micro level of specifications inside a particular, although arbitrary, \( \pi \)-institution. The former discusses what is an interpretation of institutions and provides the envisaged generalization of this approach to refinement of arbitrary deductive systems. The latter, on the other hand, corresponds to a sort of local refinement witnessed by interpretations thought simply as multifunctions relating sentences generated by different signatures within the same institution.

As a second, although related, contribution, the paper lays the basis for a refinement-by-interpretation calculus of structured specifications in an arbitrary (and across) \( \pi \)-institution(s). That both levels can be addressed and related to each other comes to no surprise: a main outcome of institution theory is precisely to provide what [AN94] describes as effective mechanisms to manipulate theories in an analogous way as our deductive calculi manipulate formulas.

The remainder of this paper is organized as follows. \( \pi \)-institutions and a notion of interpretation between them are reviewed in section 2. Then, section 3 characterizes refinement by interpretation in this context, whereas the local view is discussed in section 4. The structure of a refinement calculus is discussed in section 5. Section 6 concludes and highlights some pointers to related work.

2 \( \pi \)-institutions and interpretations

In broad terms, an institution consists of an arbitrary category \( \text{Sign} \) of signatures together with two functors \( \text{SEN} \) and \( \text{MOD} \) that give, respectively, for each signature, a set of sentences and a category of models. For each signature, sentences and models are related via a satisfaction relation whose main axiom formalizes the popular aphorism truth is invariant under change of notation [Dia08]. Such a very generic way to capture a logical system was originally motivated by quite pragmatic concerns: to provide an abstract, language-independent framework for specifying and reasoning about software systems, in response to the explosion of specification logics. Several current specification formalisms, notably, CAFEOBJ [DF02], CASL [MHST03] and HETS [MML07] were designed to take advantage of such a general framework.

\( \pi \)-institutions, proposed by J. Fiadeiro and A. Sernadas in [FS88], fulfill a similar role, replacing semantical satisfaction by a syntactic consequence relation à la Tarski. Therefore, a \( \pi \)-institution introduces, for each signature, a closure operator on the set of its sentences capturing logical consequence. As remarked by G. Voutsadakis in [Vou13] \( \pi \)-institutions may be viewed as the natural generalization of the notion of a deductive system on which a categorical theory of algebraizability, generalizing the theory of [BP01] may be based. In the sequel we review the basic definition and adopt Voutsadakis’s notion of interpretation to define refinement by interpretation in such a general setting.
Definition 1 A $\pi$-institution $I$ is a tuple $\langle \text{Sign}, \text{SEN}, (C_\Sigma)_{\Sigma \in [\text{Sign}]} \rangle$ where

- $\text{Sign}$ is a category of signatures and signature morphisms;
- $\text{SEN} : \text{Sign} \to \text{Set}$ is a functor from the category of signatures to the category of small sets giving, for each $\Sigma \in [\text{Sign}]$, the set $\text{SEN}(\Sigma)$ of $\Sigma$-sentences and mapping each $f : \Sigma_1 \to \Sigma_2$ to a substitution $\text{SEN}(f) : \text{SEN}(\Sigma_1) \to \text{SEN}(\Sigma_2)$;
- for each $\Sigma \in [\text{Sign}]$, $C_\Sigma : \mathcal{P}(\text{SEN}(\Sigma)) \to \mathcal{P}(\text{SEN}(\Sigma))$ is a mapping, called $\Sigma$-closure, such that, for all $A, B \subseteq \text{SEN}(\Sigma)$ and $\Sigma_1, \Sigma_2 \in \text{Sign}$:
  - (a) $A \subseteq C_\Sigma(A)$
  - (b) $C_\Sigma(C_\Sigma(A)) = C_\Sigma(A)$
  - (c) $C_\Sigma(A) \subseteq C_\Sigma(B)$ for $A \subseteq B$
  - (d) $\text{SEN}(f)(C_\Sigma(A)) \subseteq C_{\Sigma'}(\text{SEN}(f)(A))$

Note that the $\Sigma$-closure operator of a $\pi$-institution is not required to be finitary.

Definition 2 A $\pi$-institution $I' = \langle \text{Sign}', \text{SEN}', (C_\Sigma')_{\Sigma \in [\text{Sign}']} \rangle$ is a sub-$\pi$-institution of $I = \langle \text{Sign}, \text{SEN}, (C_\Sigma)_{\Sigma \in [\text{Sign}]} \rangle$ if $\text{Sign}'$ is a sub-category of $\text{Sign}$ and, for each $\Sigma \in [\text{Sign}']$, $\text{SEN}'(\Sigma) \subseteq \text{SEN}(\Sigma)$ and the $\Sigma$-closure $C_\Sigma'$ is the restriction of $C_\Sigma$.

Roughly speaking, the notion of logical interpretation underlying [MB09a] is that of [BP89]: a multifunction (i.e., a set-valued function) relating formulas which preserves and reflects logical consequence. Note that the expressive flexibility of interpretations comes precisely from their definition as multifunctions. A corresponding definition, to be used in the sequel, was proposed, in the context of $\pi$-institutions, in [Vou03]:

Definition 3 Given two $\pi$-institutions $I = \langle \text{Sign}, \text{SEN}, (C_\Sigma)_{\Sigma \in [\text{Sign}]} \rangle$ and $I' = \langle \text{Sign}', \text{SEN}', (C_\Sigma')_{\Sigma \in [\text{Sign}']} \rangle$, a translation $\langle F, \alpha \rangle : I \to I'$ consists of a functor $F : \text{Sign} \to \text{Sign}'$ together with a natural transformation $\alpha : \text{SEN} \to \mathcal{P}\text{SEN}'$.

A translation $\langle F, \alpha \rangle : I \to I'$ is a semi-interpretation if, for all $\Sigma \in [\text{Sign}]$, $\Phi \cup \{\phi\} \subseteq \text{SEN}(\Sigma)$,

$$\phi \in C_\Sigma(\Phi) \implies \alpha_\Sigma(\phi) \subseteq C_{\Phi(\Sigma)}(\alpha_\Sigma(\Phi))$$

(1)

It is an interpretation if,

$$\phi \in C_\Sigma(\Phi) \iff \alpha_\Sigma(\phi) \subseteq C_{\Phi(\Sigma)}(\alpha_\Sigma(\Phi))$$

(2)

Finally, we say that a translation $\langle F, \alpha \rangle$ interprets a $\pi$-institution $I$, if there is a $\pi$-institution $I^0 = \langle \text{Sign}^0, \text{SEN}^0, (C_\Sigma^0)_{\Sigma \in [\text{Sign}^0]} \rangle$ for which $\langle F, \alpha \rangle$ is an interpretation.

Note that a translation depends only on the categories of signatures and the sentence functors involved, but not on the family of closure operators. A translation is a self-translation if $F$ is the identity functor Id. On the other hand, it is said to be a functional translation if, for every $\Sigma \in [\text{Sign}]$, $\phi \in \text{SEN}(\Sigma)$, $|\alpha_\Sigma(\phi)| = 1$. Additionally, it is an identity translation, if for every $\Sigma \in [\text{Sign}]$, $\phi \in \text{SEN}(\Sigma)$,

$$\alpha_\Sigma(\phi) = \{\phi\}$$

(3)
3 Refining \( \pi \)-institutions by interpretation

In software development the process of **stepwise refinement** [ST88b] encompasses a chain of successive transformations of a specification

\[
S_0 \leadsto S_1 \leadsto S_2 \leadsto \cdots \leadsto S_{n-1} \leadsto S_n
\]

through which a complex design is produced by incrementally adding details and reducing under-specification. This is done step-by-step until the class of models becomes restricted to such an extent that a program can be easily manufactured. The discussion on what counts for a valid refinement step, represented by \( S_i \leadsto S_j \), is precisely the starting point of this line of research.

The minimal requirement to be placed on a refinement relation, besides being a pre-order to allow stepwise construction, is preservation of logical consequence. In the framework of \( \pi \)-institutions this corresponds to the following definition:

**Definition 4 (Syntactic refinement)** Let \( I = \langle \text{Sign}, \text{SEN}, (C_\Sigma)_{\Sigma \in \text{Sign}} \rangle \) and \( I' = \langle \text{Sign}', \text{SEN}', (C'_{\Sigma})_{\Sigma \in \text{Sign'}} \rangle \) be two \( \pi \)-institutions. \( I' \) is a syntactic refinement of \( I \) if Sign is a sub-category of \( \text{Sign}' \) and, for each \( \Sigma \in \text{Sign} \), \( \text{SEN}(\Sigma) \subseteq \text{SEN}'(\Sigma) \) and \( C_\Sigma(\Phi) \subseteq C'_{\Sigma}(\Phi) \) for \( \Phi \subseteq \text{SEN}'(\Sigma) \).

Clearly, a \( \pi \)-institution is a syntactic refinement of any of its \( \pi \)-sub-institutions. Refinement by interpretation, on the other hand, goes a step further:

**Definition 5 (Refinement by interpretation)** Consider two \( \pi \)-institutions \( I = \langle \text{Sign}, \text{SEN}, (C_\Sigma)_{\Sigma \in \text{Sign}} \rangle \) and \( I' = \langle \text{Sign}', \text{SEN}', (C'_{\Sigma})_{\Sigma \in \text{Sign'}} \rangle \) and let \( \langle F, \alpha \rangle : I \longrightarrow I' \) be a translation. \( I' \) is a refinement by interpretation of \( I \) via \( \langle F, \alpha \rangle \), written as \( I \leadsto_{\langle F, \alpha \rangle} I' \), if

- there is a \( \pi \)-institution \( I^0 = \langle \text{Sign}', \text{SEN}', (C^0_{\Sigma})_{\Sigma \in \text{Sign'}} \rangle \) that interprets \( I \) under translation \( \langle F, \alpha \rangle \):

\[
\sigma \in C_{\Sigma}(\Phi) \quad \Rightarrow \quad \sigma|_{\Sigma}(\Phi) \subseteq C'_{\Sigma}(\Phi)
\]

Clearly, a syntactic refinement is a refinement by interpretation for a self, identity, functional interpretation, with \( F = \text{Id} \). The following Lemma establishes an useful characterization of refinement via interpretation:

**Lemma 1** Let \( I = \langle \text{Sign}, \text{SEN}, (C_\Sigma)_{\Sigma \in \text{Sign}} \rangle \) and \( I' = \langle \text{Sign}', \text{SEN}', (C'_{\Sigma})_{\Sigma \in \text{Sign'}} \rangle \) be two \( \pi \)-institutions and \( \langle F, \alpha \rangle : I \longrightarrow I' \) a translation. Then, \( I \leadsto_{\langle F, \alpha \rangle} I' \) if \( I' \) is a syntactic refinement of some interpretation of \( I \) through \( \langle F, \alpha \rangle \).

**Proof.** Suppose \( I' \) is a syntactic refinement of an arbitrary interpretation \( I^0 \) of \( I \) along \( \langle F, \alpha \rangle \). Clearly the first condition in the definition of refinement by interpretation is met. For the second, let \( \Sigma \in \text{Sign} \) and \( \Phi \cup \{ \phi \} \subseteq \text{SEN}(\Sigma) \). Assume \( \phi \in C_{\Sigma}(\Phi) \). Then

\[
\alpha_{\Sigma}(\phi) \subseteq C^0_{F(\Sigma)}(\alpha_{\Sigma}(\Phi))
\]

because \( \langle F, \alpha \rangle \) is an interpretation. On the other hand, \( I' \) being a syntactic refinement of \( I^0 \),

\[
C^0_{F(\Sigma)}(\alpha_{\Sigma}(\Phi)) \subseteq C'_{F(\Sigma)}(\alpha_{\Sigma}(\Phi))
\]

Thus, \( \alpha_{\Sigma}(\phi) \subseteq C'_{F(\Sigma)}(\alpha_{\Sigma}(\Phi)) \).

\[\Box\]

**Definition** subsumes the corresponding notion introduced in [MMB09a] for \( k \)-dimensional deductive systems, because every \( k \)-dimensional deductive system \( \langle \mathcal{L}, \vdash_{\mathcal{L}} \rangle \) over a countable set of variables \( V \), gives rise to a specific \( \pi \)-institution \( I_{\mathcal{L}} = \langle \text{Sign}_{\mathcal{L}}, \text{SEN}_{\mathcal{L}}, (C_{\Sigma})_{\Sigma \in \text{Sign}_{\mathcal{L}}} \rangle \), built in [Vou02] as follows:
Proof. Given an interpretation \( \tau : \mathcal{F}m_{\mathcal{L}}(V) \longrightarrow \mathcal{P}(\mathcal{F}m_{\mathcal{L}}(V')) \), we define an interpretation \( \tau \). Composition \( g \cdot f \) is defined by \( \tau \cdot f = \tau \cdot f \cdot g \), where \( \tau \cdot f : \mathcal{F}m_{\mathcal{L}}(V) \longrightarrow \mathcal{F}m_{\mathcal{L}}(V) \) denotes the translation extended uniquely by \( g \) to \( \mathcal{F}m_{\mathcal{L}}(V) \).

(ii) \( \mathcal{S} \mathcal{E} \mathcal{N}_{\mathcal{L}} : \mathcal{S} \mathcal{E} \mathcal{N} \rightarrow \mathcal{S} \mathcal{E} \mathcal{N} \) maps \( V \) to \( \mathcal{F}m_{\mathcal{L}}(V) \) and \( f : V \longrightarrow \mathcal{F}m_{\mathcal{L}}(V) \) \( (f^*)^k : \mathcal{F}m_{\mathcal{L}}^k(V) \longrightarrow \mathcal{F}m_{\mathcal{L}}^k(V) \). It is easy to see that \( \mathcal{S} \mathcal{E} \mathcal{N}_{\mathcal{L}} \) is a functor.

(iii) Finally, \( \mathcal{C}_{\mathcal{L}} \) is the standard closure operator \( \mathcal{C} : \mathcal{P}(\mathcal{F}m_{\mathcal{L}}(V)) \longrightarrow \mathcal{P}(\mathcal{F}m_{\mathcal{L}}(V)) \) associated with \( \langle \mathcal{L}, \vdash \rangle \), i.e., \( \mathcal{C}(\Phi) = \{ \phi \in \mathcal{F}m_{\mathcal{L}}^k(V) : \Phi \vdash \phi \} \) for all \( \Phi \subseteq \mathcal{F}m_{\mathcal{L}}^k(V) \).

Example 1 The \( \pi \)-institution of modal logic \( \mathcal{S}^G \) forms a (syntactic) refinement of the one for classical propositional calculus (CPC). Actually, consider the modal signature \( \Sigma = \{ \neg, \land, \lor, \top, \bot, \Box \} \). Modal logic \( K \) is defined as an extension of CPC by adding the axiom \( \Box(p \implies q) \implies (\Box p \implies \Box q) \) and the inference rule \( \Box \). Logic \( \mathcal{S}^G \), on the other hand, enriches the signature of \( K \) with the symbol \( \Diamond \), and \( K \) itself with the axioms \( \Box p \implies p \), \( \Box p \implies \Box \Box p \) and \( \Diamond p \implies \Box \Diamond p \), cf. [BP01]. Hence, since the signature of both systems contains the signature of CPC and their presentations extend that of CPC with extra axioms and inference rules, we have \( CPC \sim K \) and \( CPC \sim \mathcal{S}^G \) (actually, \( CPC \sim K \sim \mathcal{S}^G \)). Hence, through these refinements, one may capture more complex, modally expressed requirements introduced along the refinement process.

Corollary 1 An \( \ell \)-deductive system \( \langle \mathcal{L}', \vdash \rangle \) is a refinement of a \( k \)-deductive system \( \langle \mathcal{L}, \vdash \rangle \) through an interpretation \( \tau \), iff \( \langle \mathcal{F}_x, \tau \rangle \) interprets the \( \pi \)-institution \( I_{\mathcal{L}} \) in \( I_{\mathcal{L}'} \).

According to the construction of \( I_{\mathcal{L}} \), detailed above, this is equivalent to

\[
\phi \in \mathcal{C}_V(\Gamma) \iff \tau(\phi) \subseteq \mathcal{C}_{V'}(\tau(\Gamma))
\]  

\( \Box \)

Hence, it is immediate to check that

As a final remark, note that, in a very precise sense, Definition 5 also covers the case of classical institutions. Actually, a \( \pi \)-institution corresponding to a classical one can always be defined: for each signature \( \Sigma \) and set of formulas \( \Psi \), take \( \mathcal{C}_E(\Psi) \) as the set of sentences satisfied in all models validating \( \Psi \).
4 The local view

Having discussed refinement by interpretation of π-institutions, we address now the same sort of refinement applied to specifications inside an arbitrary π-institution. Such is the local view. Given an arbitrary π-institution \( I = \langle \text{Sign}, \text{SEN}, (C_\Sigma)_{\Sigma \in \text{Sign}} \rangle \), a basic, or flat specification is defined as

\[
SP = \langle \Sigma, \Phi \rangle
\]

where \( \Sigma \in \text{Sign} \) and \( \Phi \subseteq \text{SEN}(\Sigma) \). Its meaning is the closure of \( \Phi \), i.e., \( C_\Sigma(\Phi) \). D. Sannella and A. Tarlecki in [ST88a] define specification over an arbitrary institution along similar lines, but taking, as semantic domain, classes of models instead of logical consequence relations.

As expected, any morphism \( \sigma : \Sigma \rightarrow \Sigma' \) in \( \text{Sign} \) entails a notion of local refinement \( \sim_\sigma \) in \( I \) given by

\[
\langle \Sigma, \Phi \rangle \sim_\sigma \langle \Sigma', \Phi' \rangle \text{ if } \sigma(\Phi) \subseteq C_{\Sigma'}(\Phi')
\]

For \( \sigma \) an inclusion, this may be regarded as a form of syntactic refinement.

Specifications may also be connected by interpretations which, again, correspond to multifunctions preserving and reflecting consequence. Formally,

**Definition 6.** Let \( \langle \Sigma, \Phi \rangle \) and \( \langle \Sigma', \Phi' \rangle \) be two specifications over a π-institution \( I = \langle \text{Sign}, \text{SEN}, (C_\Sigma)_{\Sigma \in \text{Sign}} \rangle \) and \( i : \text{SEN}(\Sigma) \rightarrow \mathcal{P}(\text{SEN}(\Sigma')) \) a multifunction from \( \text{SEN}(\Sigma) \) to \( \text{SEN}(\Sigma') \). Then \( i \) is a (local) semi-interpretation of \( \langle \Sigma, \Phi \rangle \) in \( \langle \Sigma', \Phi' \rangle \) if, for all \( \phi \in \text{SEN}(\Sigma) \),

\[
\phi \in C_\Sigma(\Phi) \Rightarrow i(\phi) \subseteq C_{\Sigma'}(\Phi')
\]

It is a (local) interpretation of \( \langle \Sigma, \Phi \rangle \) in \( \langle \Sigma', \Phi' \rangle \) if,

\[
\phi \in C_\Sigma(\Phi) \iff i(\phi) \subseteq C_{\Sigma'}(\Phi')
\]

Finally, we say that \( i \) (locally) interprets \( \langle \Sigma, \Phi \rangle \), if there is a specification \( \langle \Sigma^0, \Phi^0 \rangle \) on which \( \langle \Sigma, \Phi \rangle \) is interpreted by \( i \).

Adopting expression “\( \phi \) is true in specification \( \langle \Sigma, \Phi \rangle \)” to abbreviate the fact that \( \phi \in C_\Sigma(\Phi) \), definition (6) can be read as \( \phi \) is true in \( \langle \Sigma, \Phi \rangle \) iff \( i(\phi) \) is true in \( \langle \Sigma', \Phi' \rangle \).

**Definition 7.** Let \( SP = \langle \Sigma, \Phi \rangle \) be a specification and \( i : \text{SEN}(\Sigma) \rightarrow \mathcal{P}(\text{SEN}(\Sigma')) \) a translation which interprets \( SP \). A specification \( SP' = \langle \Sigma', \Phi' \rangle \) refines \( SP \) via local interpretation \( i \), written as \( SP \sim_i SP' \), if for all \( \phi \in \text{SEN}(\Sigma) \),

\[
\phi \in C_\Sigma(\Phi) \Rightarrow i(\phi) \subseteq C_{\Sigma'}(\Phi')
\]

Given a \( \sigma : \Sigma \rightarrow \Sigma' \in \text{Sign} \), \( \text{SEN}(\sigma) : \text{SEN}(\Sigma) \rightarrow \text{SEN}(\Sigma') \) induces a translation that maps each \( \phi \in \text{SEN}(\Sigma) \) into \( \{ \text{SEN}(\sigma)(\phi) \} \). In the sequel we identify this translation simply with \( \text{SEN}(\sigma) \).

**Definition 8.** A signature morphism \( \sigma : \Sigma \rightarrow \Sigma' \in \text{Sign} \) is conservative if for any \( \Phi \subseteq \text{SEN}(\Sigma) \), \( \text{SEN}(\sigma) \) interprets \( \langle \Sigma, \Phi \rangle \) in \( SP' = \langle \Sigma', \text{SEN}(\sigma)(\Phi) \rangle \).

Observe that \( \text{SEN}(\sigma) \) is always a semi-interpretation from \( SP \) to \( SP' \). Moreover, note that conservativeness is a stronger notion than that of interpretability.
Theorem 1 Let \( \sigma : \Sigma \to \Sigma' \in \text{Sign} \) be a conservative signature morphism, \( SP = \langle \Sigma, \Phi \rangle \) a specification over \( I \) and \( \Phi' \in \text{SEN}(\Sigma') \). Then,

\[
\text{SEN}(\sigma)(\Phi) \subseteq C_{\Sigma'}(\Phi') \text{ implies that } SP \rightarrow_{\text{SEN}(\sigma)} \langle \Sigma', \Phi' \rangle
\]  

(10)

In practice, new specifications are built from old through application of a number of specification constructors. As a minimum set we consider operators to join two specifications, to translate one into another, and to derive one from another going backward along a signature morphism. The following definition characterizes along these lines a notion of structured specification in an arbitrary \( \pi \)-institution.

Definition 9 Structured specifications over an arbitrary \( \pi \)-institution \( I = \langle \text{Sign}, \text{SEN}, (C_{\Sigma})_{\Sigma \in \text{Sign}} \rangle \) are defined inductively as follows, taking flat specifications as the base case.

- For a signature \( \Sigma \), the union of specifications \( SP_1 = \langle \Sigma, \Phi_1 \rangle \) and \( SP_2 = \langle \Sigma, \Phi_2 \rangle \) is defined as
  \[
  \text{union}(SP_1, SP_2) = \langle \Sigma, \Phi_1 \cup \Phi_2 \rangle
  \]

- The translation of specification \( SP = \langle \Sigma, \Phi \rangle \) through a morphism \( \sigma : \Sigma \to \Sigma' \) in \( \text{Sign} \) is defined as
  \[
  \text{translate } SP \text{ through } \sigma = \langle \Sigma', \text{SEN}(\sigma)(\Phi) \rangle
  \]

- The derivation of a \( \Sigma \) specification from \( SP' = \langle \Sigma', \Phi' \rangle \) through a morphism \( \sigma : \Sigma \to \Sigma' \) in \( \text{Sign} \) is defined as
  \[
  \text{derive } SP' \text{ through } \sigma = \langle \Sigma, \Psi \rangle
  \]

where \( \Psi = \{ \psi | \text{SEN}(\sigma)(\psi) \in C_{\Sigma'}(\Phi') \} \).

Of course, it is desirable that refinement be preserved by horizontal composition of specifications. In particular, refinement by interpretation should be preserved by all specification constructors in Definition 9. The result is non trivial. For union we have,

Lemma 3 Let \( i : \text{SEN}(\Sigma) \longrightarrow \mathcal{P}(\text{SEN}(\Sigma')) \) be a local interpretation, and \( SP_1 = \langle \Sigma, \Phi_1 \rangle \), \( SP_2 = \langle \Sigma, \Phi_2 \rangle \) specifications such that \( SP_1 \approx_i SP'_1 \) and \( SP_2 \approx_i SP'_2 \). If \( i \) interprets \( \text{union}(SP_1, SP_2) \), then \( \text{union}(SP_1, SP_2) \approx_i \text{union}(SP'_1, SP'_2) \).

Proof. For all \( \phi \in \text{SEN}(\Sigma) \), we reason

\[
SP_1 \approx_i SP'_1 \land SP_2 \approx_i SP'_2
\]
\[
\Leftrightarrow \quad \{ \text{definition} \}
\]
\[
\phi \in C_{\Sigma}(\Phi_1) \Rightarrow i(\phi) \subseteq C_{\Sigma'}(\Phi'_1) \land \phi \in C_{\Sigma}(\Phi_2) \Rightarrow i(\phi) \subseteq C_{\Sigma'}(\Phi'_2)
\]
\[
\Leftrightarrow \quad \{ \text{C. C. monotonic} \}
\]
\[
\phi \in (C_{\Sigma}(\Phi_1) \cup C_{\Sigma}(\Phi_2)) \Rightarrow i(\phi) \subseteq (C_{\Sigma'}(\Phi'_1) \cup C_{\Sigma'}(\Phi'_2))
\]
\[
\Leftrightarrow \quad \{ \text{definition} \}
\]
\[
\text{union}(SP_1, SP_2) \approx_i \text{union}(SP'_1, SP'_2)
\]

\( \Box \)

The remaining cases are not straightforward. Actually, achieving compatibility entails the need for imposing some non trivial conditions on morphisms.
5 Towards a refinement calculus

Having defined refinement by interpretation across π-institutions and inside an arbitrary π-institution, this section sketches their interconnections. Our first step is to define how a specification in an institution I translates to I' along an interpretation.

**Definition 10** Let \( \rho = \langle F, \alpha \rangle : I \rightarrow I' \) be a translation between π-institutions I and I' and \( SP = \langle \Sigma, \Phi \rangle \) a specification in I. The translation \( \hat{\rho}(SP) \) of SP through \( \rho \) is defined by

\[
\hat{\rho} \langle \Sigma, \Phi \rangle = \langle F(\Sigma), \alpha(\Phi) \rangle
\]  (11)

Next lemma answers the following question: is refinement by interpretation over arbitrary π-institutions preserved by the specification constructors?

**Lemma 4** The definition of specification translation is structural over the specification constructors given in definition 9, i.e.

\[
\begin{align*}
\hat{\rho} \left( \text{union}(SP_1, SP_2) \right) &= \text{union}(\hat{\rho}(SP_1), \hat{\rho}(SP_2)) \\
\hat{\rho} \left( \text{translate } SP \text{ through } \sigma \right) &= \text{translate } \hat{\rho}(SP) \text{ through } F(\sigma) \\
\hat{\rho} \left( \text{derive } SP' \text{ through } \sigma \right) &= \text{derive } \hat{\rho}(SP') \text{ through } F(\sigma)
\end{align*}
\]

**Proof.** For the first case let \( SP_1 = \langle \Sigma_1, \Phi_1 \rangle \) and \( SP_2 = \langle \Sigma_2, \Phi_2 \rangle \). Then,

\[
\begin{align*}
\hat{\rho} \left( \text{union}(SP_1, SP_2) \right) &= \{ \text{ definition of union} \} \\
\hat{\rho} \langle \Sigma, \Phi_1 \cup \Phi_2 \rangle &= \{ \text{ definition of } \hat{\rho} \} \\
\langle F(\Sigma), \alpha(\Phi_1 \cup \Phi_2) \rangle &= \{ \alpha \text{ is a natural transformation} \} \\
\langle F(\Sigma), \alpha(\Phi_1) \cup \alpha(\Phi_2) \rangle &= \{ \text{ definition of union} \} \\
\text{union}(\langle F(\Sigma), \alpha(\Phi_1) \rangle, \langle F(\Sigma), \alpha(\Phi_2) \rangle) &= \{ \text{ definition of } \hat{\rho} \} \\
\text{union}(\hat{\rho}(SP_1), \hat{\rho}(SP_2))
\end{align*}
\]
Consider now the second case (the third being similar):

\[
\hat{\rho} \left( \text{translate } SP \text{ through } \sigma \right) = \left\{ \text{ definition of translate} \right\}
\]

\[
\hat{\rho} \left( \Sigma', \sigma(\Phi) \right) = \left\{ \text{ definition of } \hat{\rho} \right\}
\]

\[
\langle F(\Sigma'), \alpha_{\Sigma'}(\sigma(\Phi)) \rangle = \left\{ \alpha \text{ is a natural transformation} \right\}
\]

\[
\langle F(\Sigma'), \mathcal{P}(\sigma)(\alpha_{\Sigma}(\Phi)) \rangle = \left\{ \text{ definition of translate} \right\}
\]

\[
\text{translate } \langle F(\Sigma'), \alpha_{\Sigma}(\Phi) \rangle \text{ through } F(\sigma)
\]

\[
\left\{ \text{ definition of } \hat{\rho} \right\}
\]

\[
\text{translate } \hat{\rho}(SP) \text{ through } F(\sigma)
\]

Note a slight abuse of notation: the extension of \( \hat{\rho}(SP) \) in the conclusion is actually through the powerset extension of \( F(\sigma) \).

\( \square \)

6 Conclusions and related work

In software development, one often has to resort to a number of different logical systems to capture contrasting aspects of systems’ requirements and programming paradigms. This paper uses \( \pi \)-institutions to formalize arbitrary logical systems and lifts to such level a recently proposed \[\text{MMB09b, MMB09a}\] approach to refinement based on logical interpretation.

Refinement by interpretation is formulated at both a global (i.e., across \( \pi \)-institutions) and local (i.e., between specifications inside an arbitrary \( \pi \)-institution) level. The paper introduces a notion of structured specification and shows that, at both levels, refinement by interpretation respects the proposed specification constructors. Actually, the institutional setting not only makes it possible to go a step further from \[\text{MMB09a}\] in generalizing the concept to arbitrary logics, but also provides a basis to build up a refinement calculus of “institution-independent”, structured specifications.

We close the paper with a few remarks on refinement by interpretation in itself and some pointers to related work.

The idea of relaxing what counts as a valid refinement of an algebraic specification, by replacing signature morphisms by logic interpretations is, to the best of our knowledge, new. The piece of research initiated with \[\text{MMB09b}\] up to the present paper was directly inspired by the second and third author’s work on algebraic logic as reported, respectively, in \[\text{Mar06}\] and \[\text{Mad08}\], where the notion of an interpretation plays a fundamental role (see, e.g., \[\text{BP89, BP01, BR03, Cze01}\]) and occurs in different variants. In particular, the notion of conservative translation intensively studied by Feitosa and Ottaviano \[\text{FD01}\] is the closest to our own approach.

Refinement by interpretation should also be related to the extensive work of Maibaum, Sadler and Veloso in the 70’s and the 80’s, as documented, for example, in \[\text{MSV84, MVS85}\]. The authors resort
Refinement by interpretation in $\pi$-institutions

to interpretations between theories and conservative extensions to define a syntactic notion of refinement according to which a specification $SP'$ refines a specification $SP$ if there is an interpretation of $SP'$ into a conservative extension of $SP$. It is shown that these refinements can be vertically composed, therefore entailing stepwise development. This notion is, however, somehow restrictive since it requires all maps to be conservative, whereas in program development it is usually enough to guarantee that requirements are preserved by the underlying translation. Moreover, in that approach the interpretation edge of a refinement diagram needs to satisfy a number of extra properties.

Related work also appears in [FM93, Vou05] where interpretations between theories are studied, as in the present paper, in the abstract framework of $\pi$-institutions. The first reference is a generalization of the work of Maibaum and his collaborators, whereas the second generalizes to $\pi$-institutions the abstract algebraic logic treatment of algebraic semantics on sentential logics. Notions of interpretation between institutions also appear in [Bor02] and [Tar95] under the designation of institution representation. Differently from the one used in this paper, borrowed from [Vou03], they are not defined as multifunctions. The work of José Meseguer [Mes89] on general logics, where a theory of interpretations between logical systems is developed, should also be mentioned.

We believe this approach to refinement through logical interpretation has a real application potential, namely to deal with specifications spanning through different specification logics. Particularly deserving to be considered, but still requiring further investigation, are observational logic [BHK03], hidden logic [Ros00] MP07 and behavioral logic [Hen97]. As remarked above, the study of refinement preservation by horizontal composition remains a challenge and a topic of current research.

Other research topics arise concerns the ways in which global and local levels interrelate. For example, we are still studying to what extent a local refinement by interpretation of a specification in a $\pi$-institution $I$, lifts to another local refinement of its translation induced by a global interpretation from $I$ to another $\pi$-institution $I'$.

Acknowledgments

This research was partially supported by Fct (the Portuguese Foundation for Science and Technology) under contract PTDC/EIA-CCO/108302/2008 — the MONDRIAN project, and the CIDMA research center. M. A. Martins was further supported by project Nociones de Completud, reference FFI2009-09345 (MICINN - Spain). Finally, A. Madeira was also supported by SFRH/BDE/33650/2009, a joint PhD grant by FCT and Critical Software S.A., Portugal.

References


Refinement by interpretation in $\pi$-institutions


