Abstract

Traditional notions of refinement of algebraic specifications, based on signature morphisms, are often too rigid to capture a number of relevant transformations in the context of software design, reuse and adaptation. This paper proposes an alternative notion of specification refinement, building on recent work on logic interpretation. The concept is discussed, its theory partially developed, its use illustrated through a number of examples.

**Keywords:** Algebraic specification, refinement, logic interpretation.
Refinement via interpretation

Manuel A. Martins\textsuperscript{1}, Alexandre Madeira\textsuperscript{1,2} and L. S. Barbosa\textsuperscript{2}
\textsuperscript{1} Department of Mathematics, Aveiro University, Aveiro, Portugal \{martins, madeira\}@ua.pt
\textsuperscript{2} Department of Informatics & CCTC, Minho University, Portugal lsb@di.uminho.pt

Abstract

Traditional notions of refinement of algebraic specifications, based on signature morphisms, are often too rigid to capture a number of relevant transformations in the context of software design, reuse and adaptation. This paper proposes an alternative notion of specification refinement, building on recent work on logic interpretation. The concept is discussed, its theory partially developed, its use illustrated through a number of examples.

Keywords: Algebraic specification, refinement, logic interpretation.

1. Introduction

The industrial demand for high-assurance software opens a window of opportunity for mathematically based development methods, able to design complex systems at ever-increasing levels of reliability and security. The aphorism \textit{proofs pay V.A.T.} witnesses this change, which is re-shaping our understanding of what Informatics is about, after all.

Algebraic specification methods [STar, Tar03, MT92, Wir90], having played a pioneer role in this process, constitute a large and mature body of knowledge and active research in the triple dimension of foundations, methodologies and applications. Central to such methods, namely to CASL [MHST03], its landmark realisation, is the process of \textit{stepwise refinement} [ST88, BH06] through which a complex design is produced by incrementally adding details and reducing non determinism with respect to the original, high-level specifications. This is done step-by-step until the specification becomes a precise description of a concrete model, technically an algebra.

In the traditional framework of algebraic specification, \textit{signature morphisms} are used to translate a specification into another one over a different signature [San00]. This enables the possibility to rename, add, remove and group together various signature components which is very useful during the specification and development processes. In a number of situations, however, transformations based in \textit{signature morphisms} are too rigid to be useful. Such is the case in the context of software reuse. But also the emergence of new computing paradigms in which software composition and adaptation becomes essentially dynamic and distributed [Fia04], entails the need for more flexible approaches to what is taken as a valid transformation of specifications (see, for example, [BSR04]).

This paper is a step in that direction. It started from a challenge: that of looking for transformations supported by mappings which need not to be morphisms. Multi-functions, \textit{i.e.}, functions mapping an element to a set of elements, seemed a natural candidate. Unfortunately, in most cases, the price to be paid is rather high. In general it is no more possible to define the reduct of an algebra by these mappings, and consequently the traditional semantical treatment of the algebraic specification process does not apply.

The alternative put forward in this paper builds on top of recent works which apply tools and results from abstract algebraic logic to the specification of software systems (cf. [MP07]). The new concept of refinement proposed here, and referred to as \textit{refinement via interpretation}, is based on \textit{logic interpretation}, a central tool in the study of equivalence semantics (see, e.g., [BP89, BP, BR03, Cze01]). A definition of \textit{interpretation} can be found in [BP], where it is formulated, for \textit{k}-logical systems, as \((k - l)\)-mappings, translating a \textit{k}-dimensional sentence into a set of \textit{l}-dimensional sentences over the same signature. A paradigmatic example is the interpretation of the \textit{classical propositional calculus} into the \textit{equational theory of boolean algebras} (cf. [BP, Example 4.1.2]).

As a result we arrive at a very simple, but still quite expressive, notion of refinement. In particular, several crucial transformations is software development, \textit{e.g.}, data encapsulation or decomposition of operations into atomic transactions are captured in this framework. This increased flex-
ibility comes, essentially, from the possibility of mapping an equation into a set of equations, while signature morphisms map each formula into another one, preserving its structure.

The paper introduces this new concept, develops basic results in its theory and illustrates its relevance and applicability in a number of examples. Sections 3 and 4 contain the main results and examples. In order to keep exposition self-contained, section 2 provides the necessary background. This section can, naturally, be skipped by the informed reader. Finally, section 5 concludes and points out a few topics for future work.

2. Preliminaries

2.1. Universal (sorted) algebra

In this section, we recall some notions of universal sorted algebra. A detailed presentation of these concepts may be found in [Sta] and [MT92].

Let $S$ be a non empty set whose elements are called sorts. An $S$-sorted set is a $S$-indexed family of sets $A = (A_s)_{s \in S}$. $A$ is nonempty if $A_s \neq \emptyset$ for each $s \in S$. We say that a $S$-sorted set $A$ is locally finite (locally countable infinite) if, for any $s \in S$, $A_s$ is a finite (countable infinite, resp.) set, and we say that $A$ is globally finite if $A$ is locally finite and $A_s = \emptyset$ except for a finite number of sorts (observe that if $S$ is finite, then local implies global finiteness). The usual set operations are extended to many sorted componentwise (e.g., we say that $A \subseteq B$ if for any $s \in S$, $A_s \subseteq B_s$). The set of all $S$-sorted subsets of $A$ is denoted by $\mathcal{P}(A)$ and the set of all globally finite $S$-sorted subsets of $A$ by $\mathcal{P}_G(A)$.

Given two $S$-sorted sets $A$ and $B$, an $S$-sorted mapping from $A$ into $B$ is an $S$-sorted set $f = (f_s)_{s \in S}$ where $f_s : A_s \to B_s$; sometimes we write just $f$ for the components $f_s$ of $f$. An $S - S'$-sorted multi-function from an $S$-sorted set $A$ to an $S'$-sorted set $B$, denoted by $\tau : A \to B$, is an $S$-family of mappings $(\tau_s : A_s \to \mathcal{P}(B))_{s \in S}$. $\tau$ is said to be globally finite if for each $s \in S$ and for all $a \in A$, $\tau_s(a)$ is globally finite.

In the sequel, if $S$ is clear from the context, we may omit explicit reference to $S$ and we just say “sorted...” instead of “$S$-sorted...”.

Definition 1 (Signature) A signature $\Sigma$ is a pair $(S, \Omega)$, where:

- $S$ is a set (of sort names);
- $\Omega$ is a $(S^* \times S)$-sorted set (of operation names),

where $S^*$ is the set of all the finite sequences of $S$ elements.

The symbols in $\Omega_{s_1, \ldots, s_n, s}$, $n \geq 1$, are called operation symbols with arguments of sort $s_1, \ldots, s_n$ and range sort $s$.

The elements of $\Omega_{s, s}$, $s \in S$, are called constants of sort $s$ ($\epsilon$ denotes the empty sequence).

We write $f : s_1, \ldots, s_n \to s \in \Sigma$ to mean that $s_1, \ldots, s_n, s \in S$ and $f \in \Omega_{s_1, \ldots, s_n, s}$, $s_1, \ldots, s_n \to s$ is the type of $f$.

Definition 2 ($\Sigma$-algebra) Let $\Sigma = (S, \Omega)$ be a signature. A $\Sigma$-algebra $A$ consists of

- an $S$-sorted set $A = (A_s)_{s \in S}$, where for all $s \in S$, $A_s \neq \emptyset$;
- for any $f \in \Omega_{s_1, \ldots, s_n, s}$, a function $f^A : A_{s_1} \times \cdots \times A_{s_n} \to A_s$;

$A$ is called the carrier set of the algebra. We will denote as usually the algebra and its carrier set with the same roman letter.

An homomorphism between two $\Sigma$-algebras $A$ and $B$ is an $S$-sorted mapping $h : A \to B$ between the correspondent carrier sets, satisfying for each $f : s_1, \ldots, s_n \to s \in \Sigma$, $h_s(f^A(a_1, \ldots, a_n)) = f^B(h_{s_1}(a_1), \ldots, h_{s_n}(a_n))$ for all $a_i \in A_{s_i}, 1 \leq i \leq n$. An injective homomorphism $f$ is called a monomorphism. If $f$ is surjective, it is called an epimorphism. We say that $h$ is an isomorphism if it is both an injective and a surjective homomorphism.

A set of variables for a signature $\Sigma = (S, \Omega)$ is a nonempty $S$-sorted set $X$ of pairwise disjoint sets. The elements in $X_s$ are called $s$-variables. To denote that a variable $x$ is of sort $s$ we write $x : s$. Throughout the paper we take the usual assumption that the variables and the symbols in $\Omega$ have different denotations.

Definition 3 $(T_\Sigma(X))$ Let $\Sigma$ be a signature and $X$ a set of variables for $\Sigma$. The set of $\Sigma$-terms in the variables $X$ is the smallest set $T_\Sigma(X)$ such that:

- for any $s \in S$, $X_s \subseteq (T_\Sigma(X))_s$;
- if $f : X \to \Sigma$ then $f \in (T_\Sigma(X))_s$;
- if $f : s_1, \ldots, s_n \to s \in \Sigma$ and $t_1 \in T_\Sigma(X)_{s_1}, \ldots, t_n \in T_\Sigma(X)_{s_n}$, then $f(t_1, \ldots, t_n) \in T_\Sigma(X)_s$;

The elements in $T_\Sigma(X)_s$ are called $\Sigma$-terms of sort $s$. We write $t(x_1, \ldots, x_n)$ to mean that the variables which occur in $t$ are among $x_1, \ldots, x_n$. The terms without variables are called ground terms. A signature is said to be standard if there is a ground term for every sort $S$.

It is well known that we can define, in a standard way, operations over $T_\Sigma(X)$ to obtain a $\Sigma$-algebra which is called term algebra over $\Sigma$. An endomorphism $\sigma : T_\Sigma(X) \to T_\Sigma(X)$ is called a substitution.

Definition 4 (Assignment) Let $\Sigma = (S, \Omega)$ be a signature, $X$ be a set of variables for $\Sigma$ and $A$ be a $\Sigma$-algebra. An assignment $h : X \to A$ is a $S$-family of mappings
functions respecting the sorts of operations names in
the sequel we will simply write
to a
conditional equation
for shortt if
wise disjointt an
important tools on the implementation procedure of softu
Γ
( t
, equation may be seen as a conditional equau
will be written as
Σ
′
and
and
Σ
σ
, signaturesw ?
By note by
the following well known result is the basis of the tradiu
Therefore, we can extend, in an uniquely way, σ (more precisely σ together with the inclusion on the variables) to a homomorphism from \( T_2(X) \) into \( T_{2\Sigma}(X') \) that we will denote by σ too (see [Star]).

The following well known result is the basis of the tradi
cenement procedure.

**Lemma 1 (Satisfaction Lemma [GB92])** Let \( \Sigma \) and \( \Sigma' \) be signatures, \( \sigma : \Sigma \to \Sigma' \) a signature morphism, \( A' \) a \( \Sigma' \)-algebra and \( \xi \) a conditional equation. Then,

\[
A' \models \sigma(\xi) \iff A' \models \sigma(\xi).
\]

**2.2. Specification logic**

Given a signature \( \Sigma \), a locally countable infinite \( S \)-sorted set of variables for \( \Sigma \) and a class \( K \) of \( \Sigma \)-algebras, the **equational consequence relation** determined by \( K \) w.r.t \( X \) is the relation between sets of \( \Sigma \)-equations and individual \( \Sigma \)-equations in \( \text{Eq}_{12}(X) \) defined by

\[
\{ t_i \approx t'_i | i \in I \} \vdash_K t \approx t' \text{ if, for all } A \in K \text{ and every valuation } \alpha : X \to A, \\
\alpha(t_i) = \alpha(t'_i) \text{ for every } i \in I \text{ implies } \alpha(t) = \alpha(t').
\]

The relation \( \vdash_K \) is said to be **finitary** if \( \{ t_i \approx t'_i | i \in I \} \vdash_K t \approx t' \) implies \( \{ t_i \approx t'_i | i \in J \} \vdash_K t \approx t' \) for some finite \( J \subseteq I \).

Let \( A \) a \( \Sigma \)-algebra, and \( \xi = t_1 \approx t'_1 \land \cdots \land t_n \approx t'_n \vdash \in \text{Eq}_{12}(X) \). It is easy to see that \( A \) is a model of \( \xi \) if \( \{ t_i \approx t'_i | i \leq n \} \vdash_A t \approx t' \).

Note that if \( I \) is finite, \( \{ t_i \approx t'_i | i \in I \} \vdash_K t \approx t' \) if and only if for every \( A \in K \) \( A \models t_1 \approx t'_1 \land \cdots \land t_n \approx t'_n \vdash \approx t \).

The relation \( \vdash_K \) is a Tarski consequence relation on the set of equations, that is, it satisfies the following conditions for all \( \Delta, \Delta' \subseteq \text{Eq}_1(X) \) and \( t \approx t' \in \text{Eq}_1(X) \):

\[
\text{(i) } \Delta \subseteq \text{Eq}_1(X) \text{ and } t \approx t' \in \text{Eq}_1(X) \implies \Delta \vdash_K t \approx t'.
\]

\[
\text{(ii) } \Delta, \Delta' \subseteq \text{Eq}_1(X) \text{ and } t \approx t' \in \text{Eq}_1(X) \implies \Delta \cup \Delta' \vdash_K t \approx t'.
\]

\[
\text{(iii) } \Delta \subseteq \text{Eq}_1(X) \text{ and } t \approx t' \in \text{Eq}_1(X) \implies \Delta \vdash t \implies t'.
\]

\[
\text{(iv) } \Delta \subseteq \text{Eq}_1(X) \text{ and } t \approx t' \in \text{Eq}_1(X) \implies \Delta \vdash t \implies t'.
\]
1. \( t \approx t' \in \Gamma \) implies \( \Gamma \models K t \approx t' \).
2. \( \Gamma \models K t \approx t' \) and \( \Gamma \subseteq \Delta \) imply \( \Delta \models K t \approx t' \).
3. \( \Gamma \models K t \approx t' \) and \( \Delta = \{ u \approx u' \text{ for every } u \approx u' \in \Gamma \} \) imply \( \Delta \models K t \approx t' \).
4. \( \Gamma \models K t \approx t' \) implies \( \sigma(\Gamma) \models K \sigma(t \approx t') \) for every substitution \( \sigma \).

It can be proved that, if \( K \) is a class of \( \Sigma \)-algebras axiomatized by a set of \( \Sigma \)-conditional equations then the relation \( \models K \) is finitary (cf. BR03 for the one-sorted case). In this case the relation can be defined in the Hilbert style by considering the set of \( \Sigma \)-equations in \( \Phi \) together with the reflexivity axioms as the set of axioms, and the \( \Sigma \)-conditional equations in \( \Phi \) together with the symmetry, transitivity and congruence rules as the inference rules. This is established in the following proposition.

**Proposition 1** [BR03] Let \( \Gamma \cup \{ t \approx t' \} \subseteq \text{Eq}_{\Sigma}(X) \) and \( K \) be the class of \( \Sigma \)-algebras axiomatized by \( \Phi \). We have that \( \Gamma \models K t \approx t' \) if and only if, there is a finite sequence of equations \( t_1 \approx t'_1, \ldots, t_n \approx t'_n \) called a proof of \( t \approx t' \) from \( \Gamma \) in \( \models K \), such that \( t_n \approx t'_n \) is \( t \approx t' \) and for every \( i = 1, \ldots, n \) one of the following conditions holds:

1. \( t_i \approx t'_i \in \Gamma \);
2. there is an axiom \( v \approx v' \) and a substitution \( \sigma \) such that \( t_i \approx t'_i = \sigma(v \approx v') \);
3. there is an inference rule \( v_1 \approx v'_1 \land \cdots \land v_m \approx v'_m \rightarrow v \approx v' \) and a substitution \( \sigma \) such that \( t_i \approx t'_i = \sigma(v \approx v') \) and \( \{ \sigma(v_i \approx v'_i) | l < m \} \subseteq \{ t_j \approx t'_j | j < i \} \).

2.3. Algebraic specification

To specify a software system, we should define an adequate signature, taking into account the sorts and functions of the intended system, and we express, in an appropriated logical system, the desired functional behaviour of the signature operations.

An algebraic specification \( SP \) is a pair \( \langle \Sigma, [SP] \rangle \) where \( \Sigma \) is a signature, denoted by \( \text{Sig}(SP) \) and \([SP]\) is a class of \( \Sigma \)-algebras. This class of \( \Sigma \)-algebras is called the model class of \( SP \), and an individual \( \text{Sig}(SP) \)-algebra in \([SP]\) a model of \( SP \). If \( \xi \) is the conditional equation \( \langle \Gamma, e \rangle \), we write \( SP \models \xi \) for \( \Gamma \models \text{[SP]} e \). We say that a specification \( SP \) is \( X \)-flat if there is a sorted set of variables \( X \) for \( \Sigma \) and a set \( \Phi \subseteq \text{Eq}_{\Sigma}(X) \) such that \( [SP] = \{ A \in \text{Alg}(\Sigma) | A \models \Phi \} \). We represent an axiomatised specification \( SP = \langle \Sigma, [SP] \rangle \) as a pair \( SP = \langle \Sigma, \Phi \rangle \) omitting explicit reference to the variables \( X \); \( X \) is assumed to be a set of variables for \( \Sigma \) such that \( \Phi \subseteq \text{Eq}_{\Sigma}(X) \) and \( [SP] = \{ A \in \text{Alg}(\Sigma) | A \models \Phi \} \). When \( \Phi \) is a set of equations, the specification \( SP = \langle \Sigma, \Phi \rangle \) is called an equation specification.

2.4. Refinement

Given a specification \( SP \) of a software system, the implementation process consists in building a correct realization (a program) of \( SP \), i.e., built an algebra \( P \) such that \( P \in [SP] \), or at least a class of \( \text{Sig}(SP) \)-algebras \( SP' \) such that \( [SP'] \subseteq [SP] \), and with \( SP' \) small enough for the desired work. During this process, we enrich \( SP \) with implementation decisions, in order to obtain a complete description of the intended program (desired algebra).

The stepwise refinement process (see [Star, ST97, Mar06]) is the systematic process by which, from an initial abstract specification \( SP_0 \) more concrete specifications are built by introducing new requirements leading to

\[ SP_0 \Rightarrow SP_1 \Rightarrow SP_2 \Rightarrow \cdots \Rightarrow SP_{n-1} \Rightarrow SP_n, \]

where for all \( 1 \leq i \leq n \), \( SP_{i-1} \Rightarrow SP_i \) means \([SP_i] \subseteq [SP_{i-1}]\). Each step of this process is called a refinement step or simply a refinement. Note that if \( SP \Rightarrow SP' \) and \( SP' \Rightarrow SP'' \) then \( SP \Rightarrow SP'' \), since \( \text{Sig}(SP) = \text{Sig}(SP') = \text{Sig}(SP'') \) and \([SP'] \subseteq [SP] \subseteq [SP] \subseteq [SP] \).

This transitivity, named vertical composition, assures that \( SP_0 \Rightarrow SP_n \).

The introduction of new requirements mentioned above is achieved through the specification of suitable signature morphisms. Supported on the Satisfaction Lemma (Lemma 1), we have the following generalisation of the refinement concept:

**Definition 7 (\( \sigma \)-Refinement)** Let \( \sigma : \Sigma \rightarrow \Sigma' \) be a signature morphism. The specification \( SP' \) over \( \Sigma' \) is a \( \sigma \)-refinement of \( SP \), in symbols \( SP \Rightarrow \sigma SP' \), if

\[ [SP'] =_{\sigma} [SP] \]

where \([SP'] =_{\sigma} [A | A \in [SP'] \}.

Note that a refinement is just a \( \text{id} \)-refinement with \( \text{id} \) the identity morphism. Since the composition of two signature morphisms is a signature morphism, we have, by Satisfaction Lemma (Lemma 1), that the vertical composition holds. I.e., if \( SP_0 \Rightarrow_{\sigma_1} SP_1 \) and \( SP_1 \Rightarrow_{\sigma_2} SP_2 \) we have \( SP_0 \Rightarrow_{\sigma_2 \circ \sigma_1} SP_2 \), and for the case with \( n \) steps, we have \( SP_0 \Rightarrow_{\sigma_n \circ \cdots \circ \sigma_1} SP_n \).

It follows an important characterisation of \( \sigma \)-refinements.

**Theorem 1** Let \( \sigma : \Sigma \rightarrow \Sigma' \) be a signature morphism, \( SP = \langle \Sigma, \Phi \rangle \) a \( X \)-flat specification and \( SP' \) a specifications over \( \Sigma' \). Then, \( SP \Rightarrow \sigma SP' \) if \( SP' \models \Phi \).

3. Refinement via interpretation

This section introduces, exemplifies and discusses the concept of refinement via interpretation — the core con-
tribution of this paper. As mentioned in the Introduction, this new perspective on algebraic specification refinement is based on the notion of logic interpretation, a central concept in the abstract algebraic theory of deductive systems [BP98, BP, BR03, Cez01]. In such a context, an interpretation is a particular kind of translation, both notions being discussed in the next two sub-sections. Then, sub-section 3.3 introduces our notion of refinement and illustrates its suitability through a number of examples. Finally, its theory is (partially) developed in sub-section 3.4.

3.1. Translations

A number of notions of translation between logical systems have been proposed in the literature (see, for example, [Fei97, FD01, BP, MDT09]). In the sequel we adopt the following definition, assuming that all sets of variables are locally countable infinite.

Definition 8 (Translation) Let $\Sigma = (S, \Omega)$ and $\Sigma' = (S', \Omega')$ be two signatures, and $X$ and $X'$ sets of variables for $\Sigma$ and $\Sigma'$ respectively. A translation from $\Sigma$ to $\Sigma'$ with respect to (w.r.t) the set of variables $X$ and $X'$ is a globally finite $S - S'$-sorted multi-function from $\text{Eq}_{\Sigma}(X)$ to $\text{Eq}_{\Sigma'}(X')$.

When $\Sigma = \Sigma'$ and $X = X'$, we call $\tau$ a self translation of $\Sigma$ w.r.t. the set of variables $X$. And, in this case, we say that $\tau$ commutes with substitutions if for every substitution $s$ and every equation $e \in \text{Eq}_{\Sigma}(X) \tau(s(e)) = s(\tau(e))$.

We extend, in a natural way, a translation $\tau : \text{Eq}_{\Sigma}(X) \rightarrow \text{Eq}_{\Sigma'}(X')$ to a multi-function $\tau^* : \text{Ce}_{\Sigma}(X) \rightarrow \text{Ce}_{\Sigma'}(X')$ as follows:

$$\tau^*(\xi) = \{ (\bigcup_{t \approx t' \in \Gamma} \tau(t \approx t'), e') : e' \in \tau(e) \}.$$ 

for any conditional equation $\xi = (\Gamma, e)$. In the sequel, we will identify $\tau^*$ with $\tau$. Notice how the reason for requiring $\tau_s(x)$ to be global finite becomes clear from the definition of $\tau^*$. We may now prove the following result.

Proposition 2 Let $\Sigma = (S, \Omega)$ be a standard signature, $X$ a set of variables for $\Sigma$ and $\tau$ a self translation of $\Sigma$ w.r.t $X$. Then the following conditions are equivalent:

1. $\tau$ commutes with substitutions.

2. There exists an $S$-sorted set of equations $E(x, y) \subseteq \text{Eq}_{\Sigma}(X)$ such that, for any $t \approx t' \in \text{Eq}_{\Sigma}(X)$, $\tau_s(t \approx t') = E_s(t, t')$.

Proof. Assume $\tau$ commutes with arbitrary substitutions. We fix distinct variables $p, q$ and we define $E(p, q) := \tau(p \approx q)$. Suppose $\text{Var}(E(p, q)) \subseteq \{p, q, r_1, r_2, \ldots\}$. Let $e$ be a substitution such that $e(p) = p, e(q) = q$ and $e(r_i) = p$ for all $i \in I$. By assumption, $E(p, q, p, \ldots) = e(E(p, q)) = \tau(e(p \approx q)) = \tau(p \approx q) = E(p, q, r_1, r_2, \ldots)$. Hence, $\{r_1, r_2, \ldots\} \subseteq \{p, q\}$. Thus $\text{Var}(E(p, q)) \subseteq \{p, q\}$. Now, let $\varphi \approx \psi \in \text{Eq}$ and $e$ a substitution such that $e(p) = \varphi$ and $e(q) = \psi$. We have that $\tau(\varphi \approx \psi) = \tau(e(p) \approx e(q)) = e(\tau(p \approx q)) = E(e(p, q)) = E(e(p), e(q)) = E(\tau(p), \tau(q))$.

Suppose now that 2 holds. Let $\alpha$ be a substitution in $\Sigma$. Then, for any $t \approx t' \in \Sigma$,

$$\alpha(\tau(t \approx t')) = \alpha(E_s(t, t')) = E_s(\alpha(t), \alpha(t')) = \tau(\alpha(t \approx \alpha(t'))) = \tau(\alpha(t \approx t')).$$

$\square$

3.2. Interpretations

Defined as a multi-function, a translation maps a term into a set of terms, and this is what makes translations interesting to establish relationships between specification. Recall that, on the other hand, a signature morphism maps a term into just another term.

Not all translations, however, are suitable to capture the meaning of interpreting a specification into another one. The following definition singles out the relevant ones:

Definition 9 (Interpretation) Let $\tau$ be a translation from $\Sigma$ to $\Sigma'$ w.r.t. the set of variables $X$ and $X'$. Let $SP$ be a specification over $\Sigma$. We say that $\tau$ interprets $SP$ if there is a specification $SP'$ over $\Sigma'$ such that, for any $\xi \in \text{Ce}_{\Sigma}(X)$, $SP \models \xi$ if and only if $SP' \models \tau(\xi)$. In this case we say that $\tau$ interprets $SP$ in $SP'$ and $SP'$ is a $\tau$-interpretation of $SP$.

Example 1 The interpretation of the class $HA$ of Heyting algebras in the class $BA$ of (the specification of) Boolean algebras is a classical example of an interpretation. Let $X$ be a numerable set of variables and $\Sigma$ the usual signature for boolean algebras (and for Heyting algebras). Consider the well known duple negation (propositional) translation 1:

$$\iota : \text{T}_{\Sigma}(X) \rightarrow \text{T}_{\Sigma}(X) \quad t \mapsto \iota(t) = \neg \neg t$$

Let $\tau$ be the a self translation of $\Sigma$ w.r.t. $X$ defined by

$$\tau(t \approx t') = \{ \iota(t) \approx \iota(t') \}.$$ 

It can be shown that $\tau$ interprets the specification $BA$ of the boolean algebras in the specification $HA$ of the Heyting algebras (cf. [BR03]).

It is not difficult to see that

---

1 This translation is known by Glivenko’s interpretation. This translation establishes a strict relation between classical derivability and intuitionistic derivability, namely

If $\varphi$ is a theorem in CPC then $\neg \neg \varphi$ is a theorem in IPC (cf. [BR03]). This result establishes the bridge between the algebraic semantics of the classical propositional calculus and the algebraic semantics intuitionistic propositional calculus.
Theorem 2 Let $SP$ and $SP'$ be two algebraic specifications over a signature $\Sigma$ and $\tau$ a recursive self translation of $\Sigma$ w.r.t a set of variables $X$ that commutes with arbitrary substitutions and interprets $SP$ in $SP'$. If $SP$ is decidable then $SP'$ is decidable.

Definition 10 ($\tau$-model) Let $\tau$ be a translation from $\Sigma$ to $\Sigma'$ w.r.t the set of variables $X$ and $X'$, and $SP$ a specification over $\Sigma$. A $\Sigma'$-algebra $A'$ is a $\tau$-model of $SP$ if for any $\xi \in Ceq_{\Sigma}(X)$, $SP |= \xi$ implies $A' |= \tau(\xi)$. We define the $\tau$-model class of $SP$, denoted by $Mod_{\tau}(SP)$, as the class of all $\tau$-models of $SP$. We will denote the specification over $\Sigma'$ whose models are $Mod_{\tau}(SP)$ by $SP'$.

Observe that for all conditional equation $\xi$, $SP |= \xi \rightarrow SP' |= \tau(\xi)$.

Theorem 3 Let $\tau$ be a translation from $\Sigma$ to $\Sigma'$ w.r.t the set of variables $X$ and $X'$, and $SP$ a specification over $\Sigma$. If $\tau$ interprets $SP$, then the specification $SP'$ is the largest $\tau$-interpretation of $SP$, i.e., with the largest class of models.

Proof. Suppose that $\tau$ interprets $SP$. Let $SP'$ be a specification that is a $\tau$-interpretation of $SP$. Then for any $\xi \in Ceq_{\Sigma}(X)$, $SP |= \xi$ if and only if $SP' |= \tau(\xi)$. Hence all models of $SP'$ are $\tau$-models of $SP$. Thus, $[SP'] \subseteq [SP']$.

So, we only need to prove that $SP'$ is a $\tau$-interpretation of $SP$. Let $\xi \in Ceq_{\Sigma}(X)$. It is clear that $SP |= \xi$ implies $SP' |= \tau(\xi)$. Suppose now that $SP' |= \tau(\xi)$. Let $SP'$ be a specification that is a $\tau$-interpretation of $SP$ (it exists since $\tau$ interprets $SP$). Since, $[SP'] \subseteq [SP']$, $SP' |= \tau(\xi)$. Since $SP'$ is a $\tau$-interpretation of $SP$, $SP' |= \xi$.

Next theorem states that $SP'$ is finitely axiomatized whenever $SP$ is:

Theorem 4 Let $\tau$ be a self translation of $\Sigma$ w.r.t $X$ and $SP = \langle \Sigma, \Phi \rangle$ be a X-flat specification. If $\tau$ commutes with substitutions then $SP'$ is also X-flat and $SP' = \langle \Sigma', \tau(\Phi) \rangle$. Moreover, if $\Phi$ is finite then $SP'$ is finitely axiomatizable, i.e. X-flat.

Proof. On the one hand, we have that for any $A' \in [SP']$ and for any $\xi \in Ceq(X)$, $SP |= \xi$ implies $A' |= \tau(\xi)$. In particular, since $SP |= \Phi$, we have that $SP' = \tau(\Phi)$ and hence, $[SP'] = [\langle \Sigma', \tau(\Phi) \rangle]$.

On the other hand, let $A = \langle \Sigma', \tau(\Phi) \rangle$ and $\xi = \langle \Gamma, e \rangle$ be a conditional equation over $X$ such that $SP' \models \xi$ (i.e., $\Gamma \models e \in SP \Gamma$). Then, it can be proved by induction on the length of a proof of $\Gamma$ that $A \models \tau(\xi)$. Therefore $A$ is a $\tau$-model of $SP'$ and, so, $[\langle \Sigma', \tau(\Phi) \rangle] \subseteq [SP']$.

Clearly, if $\Phi$ is finite then $\tau(\Phi)$ is also finite. Moreover, one can prove that $\tau(\Phi)$ constitutes an axiomatization for $SP'$. ∎

3.3. Refinement via interpretation

Logic interpretations provide the basic tool for the following definition:

Definition 11 (Refinement via interpretation) Let $SP$ be a specifications over $\Sigma$ and $\tau$ a translation from $\Sigma$ to $\Sigma'$ w.r.t. the set of variables $X$ and $X'$ which interprets $SP$. We say that a specification $SP'$ over $\Sigma'$ refines the specification $SP$ via the interpretation $\tau$, in symbols $SP \rightarrow_\tau SP'$, if for any $\xi \in Ceq_{\Sigma}(X)$

$$SP \models \xi \Rightarrow SP' \models \tau(\xi)$$

Let us now discuss some examples of refinements via interpretations. The first one is mainly of theoretical interest: it shows how (a specification of) an Heyting algebra can be regarded as a refinement of (a specification of) a Boolean algebra.

Example 2 Consider the following specifications of Boolean and Heyting algebras:

$\text{SPEC } BOOL = \text{ enrich DIST} - \text{ LATTICE by } [AX]$

(1) $p \lor \neg p \approx tt$
(2) $p \land \neg p \approx ff$
(3) $p \lor tt \approx tt$
(4) $p \land ff \approx ff$

and

$\text{SPEC } HEYTING = \text{ enrich DIST} - \text{ LATTICE by } [GEN]$

$bool$

$[OP]$

$tt : \longrightarrow bool$
$ff : \longrightarrow bool$
$neg : bool \longrightarrow bool$
$\land : bool \times bool \longrightarrow bool$
$\lor : bool \times bool \longrightarrow bool$
$\Rightarrow : bool \times bool \longrightarrow bool$

$[AX]$

(1) $p \lor tt \approx tt$
(2) $p \land ff \approx ff$
(3) $p \Rightarrow p \approx tt$
(4) $p \Rightarrow (q \lor r) \approx (p \Rightarrow q)$
(5) $(p \Rightarrow q) \land q \approx q$
(6) $p \land (p \Rightarrow q) \approx p \land q$
(7) $(p \Rightarrow q) \land (p \Rightarrow r) \approx (p \Rightarrow q) \land (p \Rightarrow r)$
(8) $(p \land q) \Rightarrow r \approx (p \Rightarrow r) \land (q \Rightarrow r)$

where $DIST - LATTICE$ is the specification of the distributive lattices (cf. [BS81]).

As in Example 1, multi-function $\tau$ defined by

$$\tau(t \approx t') = \{\neg t \approx \neg t'\}$$

interprets $BOOL$ in $HEYTING$. To show that $BOOL \rightarrow_\tau HEYTING$ just observe that for any axiom $\varphi$ of $BOOL$, $HEYTING \models \tau(\varphi)$. 


Our next example, although quite elementary, illustrates a key point. It shows how refinement via interpretation is able to capture data encapsulation, i.e., the process of hiding a specific sort in a specification. This is a relevant issue in algebraic specification, in particular when the implementation target is an object-oriented framework; hidden sorts become the state space of object implementations, as discussed in, e.g., [Fav98, DD05]. It is interesting to have such sort of transformations integrated in a stepwise refinement process.

Example 3 Consider the following specification of the natural numbers:

\[
\text{SPEC} \quad \text{NAT} = \\
\text{[SORT]} \\
\qquad \text{nat} \\
\text{[OP]} \\
\qquad s : \text{nat} \rightarrow \text{nat} \\
\text{[AX]} \\
\qquad (1) s(x) \approx s(y) \rightarrow x \approx y
\]

Consider now an alternative specification which introduces an equality test predicate \( \text{eq} \) axiomatised with the congruence property:

\[
\text{SPEC} \quad \text{NATEQ} = \text{enrich BOOL by} \\
\text{[SORT]} \\
\qquad \text{nat} \\
\text{[OP]} \\
\qquad s : \text{nat} \rightarrow \text{nat} \\
\quad \text{eq} : \text{nat} \times \text{nat} \rightarrow \text{bool} \\
\text{[AX]} \\
\quad (1) \text{eq}(x, x) \approx \text{tt} \\
\quad (2) \text{eq}(x, y) \approx \text{tt} \rightarrow \text{eq}(y, x) \approx \text{tt} \\
\quad (3) \text{eq}(x, y) \approx \text{tt} \land \text{eq}(y, z) \approx \text{tt} \rightarrow \text{eq}(x, z) \approx \text{tt} \\
\quad (4) \text{eq}(x, y) \approx \text{tt} \rightarrow \text{eq}(s(x), s(y)) \approx \text{tt} \\
\quad (5) \text{eq}(s(x), s(y)) \approx \text{tt} \rightarrow \text{eq}(x, y) \approx \text{tt}
\]

Consider multi-function \( \tau \) such that

\[
\tau(x : \text{nat} \approx y : \text{nat}) = \{\text{eq}(x : \text{nat}, y : \text{nat}) \approx \text{true}\}
\]

\( \text{NATEQ} \) interprets \( \text{NAT} \) by \( \tau \). First note that for any equation \( t \approx t' \) such that \( \text{NAT} \models t \approx t' \), we have that \( \text{NATEQ} \models \text{eq}(t, t') \approx \text{tt} \), where the interpretation of the proof of \( \text{NAT} \models t \approx t' \) (in sense of proposition 1) is a proof of \( \text{NATEQ} \models \text{eq}(t, t') \approx \text{tt} \). The converse may be verified by induction on the length of the proof of \( \text{NATEQ} \models \text{eq}(t, t') \approx \text{tt} \).

The example shows how a specification of the natural numbers is interpreted into another one axiomatised exclusively by equations of sort \( \text{bool} \). Sort \( \text{nat} \) became hidden, or encapsulated, after refinement.

Other useful design transformations in algebraic specification can similarly be captured as refinements. Our last example illustrates one of them relating specifications to implementations in which some operations are decomposed or mapped to transactions, i.e., sequences of operations to be executed atomically.

Example 4 Consider the following fragment of a specification of a bank account management system (BaMS), involving account deposits (operation deposit), withdrawals (withdraw) and a balance query (bal). Assume variables \( s : \text{BaMS}, i : \text{AccountId} \) and \( n : \mathbb{N} \), where \( \mathbb{N} \) stands for the natural numbers, with the usual arithmetic operators.

\[
\text{SPEC} \quad B_1 = \\
\text{[AX]} \\
\quad (1) \text{bal}(\text{deposit}(s, i, n)) \approx \text{bal}(s, i) + n \\
\quad (2) \text{bal}(\text{withdraw}(s, i, n)) \approx \text{max}(\text{bal}(s, i) - n, 0)
\]

Consider, now, an implementation \( B_2 \), where all transactions are previously validated (through predicate \( \text{val} \)). Its axioms include,

\[
\begin{align*}
(3) \, & \text{val}(\text{bal}(\text{val}(\text{deposit}(s, i, n)))) \approx \text{val}(\text{bal}(s, i)) + n \\
(4) \, & \text{val}(\text{bal}(\text{val}(\text{withdraw}(s, i, n)))) \\
& \approx \text{max}(\text{bal}(\text{bal}(s, i)) - n, 0)
\end{align*}
\]

Interpretation

\[
\tau_1 : \text{Eq}(\Sigma_1) \rightarrow \text{Eq}(\Sigma_2) \\
= \{(\text{op}(x) \approx y) \rightarrow \{\text{val}(\text{op}(x)) \approx y\} | \text{op} \in \Sigma_1\}
\]

witnesses a refinement in which isolated calls to the operations are mapped to transactions which necessarily include a validation step. The situation where only a given subset of such operations (for example the ones directly affecting an account balance) requires validation is captured by the following axioms in another implementation \( B_3 \):

\[
\begin{align*}
(5) \, & \text{bal}(\text{val}(\text{deposit}(s, i, n))) \approx \text{bal}(s, i) + n \\
(6) \, & \text{bal}(\text{val}(\text{withdraw}(s, i, n))) \approx \text{max}(\text{bal}(s, i) - n, 0)
\end{align*}
\]

Clearly,

\[
\tau_2 : \text{Eq}(\Sigma_1) \rightarrow \text{Eq}(\Sigma_3) = \\
\{(\text{op}(x) \approx y) \rightarrow \{\text{val}(\text{op}(x)) \approx y\} | \text{op} \in \text{userOp}\}
\]

where \( \text{userOp} = \{\text{deposit}, \text{withdraw}\} \), is the required interpretation. Notice, however, that multi-function

\[
\tau'_2 : \text{Eq}(\Sigma_1) \rightarrow \text{Eq}(\Sigma_3) = \\
\{(\text{op}(x) \approx y) \rightarrow \{\text{val}(\text{op}(x)) \approx y, \text{op}(x) \approx y\} | \text{op} \in \Sigma_1\}
\]

is not an interpretation: most of the possible translations of (1) are not valid in \( B_3 \).
Finally, the reader is invited to check that $B_4$ is a refinement of $B_3$ through interpretation $\tau_3$:

$$\tau_3 : Eq(\Sigma_1) \longrightarrow Eq(\Sigma_1) \quad = \quad \{\{\text{val}(\text{op}(x)) \approx y\} \mid \text{op} \in \Sigma_1 \setminus \{\text{withdraw}\}\} \cup \{\text{withdraw}(x) \approx y\} \rightarrow \{\text{conf}(\text{val}(\text{withdraw}(x))) \approx y\}\}
$$

where specification $B_4$ forces all operations to be validated, but also requires for some of them a previous authorisation, therefore decomposing such operations in three step transactions:

1. $\text{val}(\text{bal}(\text{val}(\text{deposit}(s, i, n)))) \approx \text{val}(\text{bal}(s, i)) + n$
2. $\text{val}(\text{bal}(\text{conf}(\text{val}(\text{withdraw}(s, i, n))))))$ 

\[ \approx \max(\text{val}(\text{bal}(s, i)) - n, 0) \]

### 3.4. Stepwise refinement revisited

Having illustrated some typical applications of the notion of refinement put forward in this paper, it is legitimate to ask now how does it relate to the traditional one, based on signature morphisms.

**Theorem 5** Let $SP$ be a specifications over $\Sigma$ and $\tau$ a translation from $\Sigma$ to $\Sigma'$ w.r.t. the set of variables $X$ and $X'$ which interprets $SP$. Then, for every $SP'$ specification over $\Sigma'$, if $SP' \rightarrow \tau$ $SP'$ then $SP \rightarrow \tau SP'$.

**Proof.** Suppose $SP' \rightarrow \tau SP'$, i.e., that $[SP'] \subseteq [SP]$. Thus, all the algebras $A' \in [SP']$ are $\tau$-models of $SP$. Therefore for any $\xi \in \text{Ceq}_1(X), SP \models \xi$ implies $SP' \models \tau(\xi)$. I.e., $SP \rightarrow \tau SP'$.

**Theorem 6** Let $SP = (\Sigma, \Phi)$ be a $X$-flat specification and $\tau$ a translation from $\Sigma$ to $\Sigma'$ w.r.t. the set of variables $X$ and $X'$. If $\tau$ interprets $SP$, then the following conditions are equivalent:

$$SP \rightarrow \tau SP' \quad (1)$$

$$SP' \rightarrow \tau SP' \quad (2)$$

**Proof.** Theorem 3 justifies implication (1) to (2). The converse implication is just Theorem 5.

As a corollary we have:

**Corollary 1** Let $SP = (\Sigma, \Phi)$ be a $X$-flat specification and $\tau$ a translation from $\Sigma$ to $\Sigma'$ w.r.t. the set of variables $X$ and $X'$ which interprets $SP$. Then, $SP' \models \tau(\Phi)$ implies $SP \rightarrow \tau SP'$.

We may now try the following question: given that any mapping $\bar{f}$ can be regarded as a multifunction, when does a traditional refinement via signature morphism become a refinement via interpretation? We start with the following lemma:

**Lemma 2** Let $SP$ be a specification over $\Sigma$ and $\sigma : \Sigma \rightarrow \Sigma'$ be an injective signature morphism. Let $\tau$ be the translation induced by the signature morphism $\sigma$. Then $\tau$ interprets $SP$.

**Proof.** Let $SP'$ be the specification over $\Sigma'$ such that $[SP'] = \{A' \mid A \in [SP]\}$. Suppose $SP \models \xi$. Let $A' \in [SP']$. Since $A' \models \sigma(\xi)$ we have that $A' \models \xi$ and, by Lemma 1, $A' \models \sigma(\xi)$. Therefore $SP' \models \tau(\xi)$. Suppose now $SP' \models \tau(\xi)$ and let $A \in [SP]$. Since $\sigma$ is injective there is $B \in [SP']$ such $B \models \xi$. Hence $B \models \tau(\xi)$. Therefore $SP' \models \xi$. Hence $SP' \models \xi$. Therefore $\sigma$ interprets $SP'$.

Next theorem shows that our notion actually is a generalization of the standard one in the special case when the signature morphism is injective.

**Theorem 7** Let $SP$ and $SP'$ be two specifications over $\Sigma$ and $\Sigma'$ respectively, and $\sigma : \Sigma \rightarrow \Sigma'$ an injective signature morphism. Let $\tau$ be the translation induced by the signature morphism $\sigma$. Then, $SP \rightarrow \sigma SP'$ implies $SP \rightarrow \tau SP'$.

**Proof.** By previous theorem $\tau$ interprets $SP$. Suppose $SP \rightarrow \sigma SP'$, i.e., $[SP'] \subseteq [SP]$. Let $\xi \in \text{Ceq}_1(X)$ such that $SP \models \xi$. Let $A' \in [SP']$. Then $A' \models [SP']$ and so $A' \models [SP]$. By Lemma 1, $A' \models [SP]$. Hence $SP' \models \sigma(\xi)$. Therefore $SP' \models \tau(\xi)$. Hence $SP' \models \sigma(\xi)$. Therefore $SP \rightarrow \tau SP'$.

Now, we show that, in the flat case, the two concepts of refinement coincide:

**Theorem 8** Let $\sigma : \Sigma \rightarrow \Sigma'$ be an injective signature morphism, $SP = (\Sigma, \Phi)$ a $X$-flat specification and $SP$ a specification over $\Sigma'$. Let $\tau$ be the translation induced by the signature morphism $\sigma$. Then $SP \rightarrow \sigma SP'$ if $SP \rightarrow \tau SP'$.

**Proof.** Suppose $SP \rightarrow \tau SP'$. By Theorem 5, $SP' \rightarrow \tau SP'$. On the other hand, since $[SP'] \subseteq [\Sigma']$, by Theorem 1, $SP \rightarrow \sigma SP'$. Since we can vertically compose $\sigma$-refinements we have $SP \rightarrow \sigma SP'$.

The discussion concerning the composition of refinements via interpretation is not straightforward. For vertical composition an additional property has to be imposed on the components’ interpretations. Formally.

**Theorem 9** Let $SP$, $SP'$ and $SP''$ be three specifications over $\Sigma$, $\Sigma'$ and $\Sigma''$ respectively. Let $\tau$ be a translation from $\Sigma$ to $\Sigma'$ w.r.t. the set of variables $X$ and $X'$ and $\rho$ a translation from $\Sigma'$ to $\Sigma''$ w.r.t. the set of variables $X'$ and $X''$. Suppose that $SP \rightarrow \tau SP'$, $SP' \rightarrow \rho SP''$ and $\rho$ interprets $SP''$. Then $SP \rightarrow \rho \tau SP''$.

**Proof.** Suppose $\xi \in \text{Ceq}_1(X)$. Suppose $SP \models \xi$. Since $SP \rightarrow \tau SP'$, $SP' \models \tau(\xi)$. And, from $SP' \rightarrow \rho SP''$, we have $SP'' \models \rho(\tau(\xi))$. By hypothesis, $\tau$ interprets $SP$ and $\rho$ interprets $SP''$. In particular, $SP''$ is a $\rho$-interpretation of $SP$ and $(SP'')^\rho$ is a $\rho$-interpretation of $SP''$. Hence, for any $\xi \in \text{Ceq}_1(X), SP \models \xi \models SP'' \models \tau(\xi)$ and for any $\zeta \in \text{Ceq}_1(X'), SP' \models \zeta \models (SP')^\rho \models \tau(\zeta)$. Therefore, for any $\xi \in \text{Ceq}_1(X), SP \models \xi \models (SP'')^\rho \models \rho(\tau(\xi))$. That is, $\rho \circ \tau$ interprets $SP$.

On the other hand, horizontal composition of refinements via interpretations is still a topic of current research. To illustrate the kind of results we are investigating suppose, for example, that $\tau$ interprets $SP$ in $SP'$. The challenge is to prove that $\tau$ also interprets any axiomatic extension of $SP$ in an appropriate subclassification of $SP'$. 
4. Conclusions and further work

The paper introduced a new notion of refinement and started to set the way towards the development of a consistent algebraic theory of refinements via interpretations. The results, characterizations and applications obtained are promising, in the sense that a number of useful transformations of specifications become captured as refinement steps. Although the paper raises more questions than it gives answers, the path seems to be clear, although the paper raises more questions than it gives answers.

The main focus of our current work is the integration of the refinements via interpretation within the standard refinement process of algebraic specifications. A first step in this direction concerns the study of hybrid notions like $SP \rightarrow_{\tau} SP'$ iff $SP^\tau \rightarrow_{\sigma} SP'$, for $\tau$ a translation and $\sigma$ a signature morphism. In this context, our $\tau \circ \sigma$-models would consist of algebras of the class $[SP^\sigma]_\tau$.

Another topic to explore is the equivalence of algebraic specification up to logical interpretations. As a starting point, it would be worth to explore relation $\equiv$ defined as follows: $SP \equiv SP'$ if there are interpretations $\tau$ and $\rho$ such that $SP \rightarrow_{\tau} SP'$ and $SP' \rightarrow_{\rho} SP$. It is not difficult to see that $SP \models \xi$ implies $SP' \models \rho(\tau(\xi))$ and $SP' \models \eta$ implies $SP' \models \tau(\rho(\eta))$. More challenging seems to be a stronger equivalence, studied in the context of equivalence between logical systems [CG05, BP89], which requires interpretations to be mutually inverse, that is inverses of one another.

Acknowledgements. This research was supported by FCT (the Portuguese Foundation for Science and Technology) under contracts PTDC/EIA/73252/2006, at Minho University, and PTDC/MAT/68723/2006 at the Unidade de Investigação Matemática e Aplicações of University of Aveiro.

References


