PUC

ISSN 0103-9741

Monografias em Ciência da Computação
nº 38/92

On Extensions by Sorts

María Claudia Meré
Paulo A. S. Veloso

Departamento de Informática

PONTIFÍCIA UNIVERSIDADE CATÓLICA DO RIO DE JANEIRO
RUA MARQUÊS DE SÃO VICENTE, 225 - CEP 22453
RIO DE JANEIRO - BRASIL

PUC RIO - DEPARTAMENTO DE INFORMÁTICA

Monografias em Ciência da Computação, Nº 38/92 ISSN 0103-9741
Editor: Carlos J. P. Lucena December, 1992

On Extensions by Sorts *

María Claudia Meré

Paulo A. S. Veloso

* Research partly sponsored by the Brazilian agencies CNPq, RHAE and FAPERJ.

In charge of publications:
Rosane Teles Lins Castilho
Assessoria de Biblioteca, Documentação e Informação
PUC Rio — Departamento de Informática
Rua Marquês de São Vicente,225 — Gávea
22454970 — Rio de Janeiro, RJ
Brasil
Tel. +55-21-529 9386 Telex +55-21-31048 Fax +55-21-511 5645
E-mail: rosane@inf.puc-rio.br
techrep@inf.puc-rio.br (for publications only)

ON EXTENSIONS BY SORTS

María Claudia MERÉ
{e-mail: mere@inf.puc-rio.br}

Paulo A. S. VELOSO
{e-mail: veloso@inf.puc-rio.br}

PUCRioInf MCC 38/92

Abstract

The process of implementing a formal specification on another one is very important in formal software development and can be described in terms of simple logical concepts as an interpretation into a conservative extension. An extension consists of the addition of new symbols and axioms, a simple, but important, special case being the so-called extensions by definitions. The new symbols to be introduced correspond to sorts, functions or predicates. Extensions by the addition of function and predicate symbols are well studied in the literature.

Our purpose here is to analyse conservative extensions that introduce new sorts. This is of importance because it occurs often in implementing formal specifications, when new sorts are "constructed" from the concrete ones.

We specify and analyse some well-known sort introduction constructs akin to those found in programming languages, namely cartesian product, discriminated union, subsort and quotient. In each case the extension is shown to have unique, up to isomorphism, expandability and to be conservative; moreover the new sort is shown to exhibit the desired behaviour. Also, the new sort is connected to the old ones by means of conversion functions. Some derived properties are also established.

Key words:

Formal specifications, software development, formal methods, sort introduction, conservative extension, cartesian product, discriminated union, subsort, quotient, formal logic, universal property.

SOBRE EXTENSÕES POR SORTES

María Claudia MERÉ
{e-mail: mere@inf.puc-rio.br}

Paulo A. S. VELOSO
{e-mail: veloso@inf.puc-rio.br}

PUCRioInf MCC 38/92

Resumo

O processo de implementar uma especificação formal em outra é de grande importância no desenvolvimento formal de programas, podendo ser descrito em termos de conceitos lógicos simples como uma interpretação em uma extensão conservativa. Uma extensão consiste do acréscimo de novos símbolos e axiomas, um caso especial simples, porém importante, sendo as extensões por definições. Os novos símbolos a serem introduzidos correspondem a sortes, funções ou predicados. Extensões por acréscimo de símbolos de função e de predicado estão bem estudadas na literatura.

Nosso objetivo aqui é analisar extensões conservativas que introduzem novos sortes. Isto é importante pois ocorre com freqüência na implementação de especificações formais, quando novos sortes são "construídos" a partir dos concretos.

Alguns mecanismos de introdução de sortes similares aos encontrados em linguagens de programação - produto cartesiano, união discriminada, subsorte e quociente - são especificados e analisados. Em cada caso se mostra que a extensão tem a propriedade da expansividade única, a menos de isomorfismo, sendo conservativa; enquanto o novo sorte exibe o comportamento desejado. O novo sorte se liga aos antigos por meio de funções de conversão. Algumas propriedades derivadas são estabelecidas.

Palavras chave:

Especificações formais, desenvolvimento de programas, métodos formais, introdução de sortes, extensão conservativa, produto cartesiano, união discriminada, subsorte, quociente, lógica formal, propriedade universal.

Contents

1 Introduction

The process of implementing a formal specification on another one is very important in formal software development and it can be described in terms of simple basic logical concepts.

Formal specifications are presentations of theories in many-sorted logic, and an *implementation* of a formal specification A on another formal specification C amounts to an interpretation of A into a conservative extension B of C. The idea here is that the 'concrete' specification C is extended so as to incorporate versions to which the abstract symbols of A can then be mapped, [TM87, Vel87].

An *extension* consists of the addition of new symbols and axioms; a simple, but important, special case being the so-called *extensions by definitions*. The new symbols to be introduced correspond to sorts, functions or predicates. Extensions by the addition of function and predicate symbols are well studied in the literature. In particular, extensions by definitions of function and predicate symbols are characterized by the property of *unique expandability*, which entails *conservativeness* and *eliminability* [Sho67].

Our purpose here is to analyse **conservative extensions that introduce new sorts**. This is of importance because it occurs often in implementing formal specifications, when new sorts are "constructed" from the concrete ones. We first specify and analyse some well-known sort introduction constructs, akin to those found in programming languages ([Hoa74]), namely cartesian product, discriminated union, subsort and quotient. In each case the extension is shown to have unique, up to isomorphism, expandability and to be conservative, which corroborates the intuitive feeling that these amount to extensions by definition of a new sort. Moreover, the new sort is shown to exhibit the required behaviour. In the context of implementation of formal specifications, the new sorts introduced should be somehow 'connected' to the old ones. This is what our intuition requires and is what happens in the case of the four constructs examined.

In section 2 we shall provide formal specifications for each one of these four constructs by axiomatising their usual descriptions.

In section 3 we establish the adequacy of these specifications by showing that they capture the intended behaviour; this is done by characterising their models and showing that the extensions are conservative, monomorphic, invariant under isomorphisms and present the functorial character to be expected from these constructs.

2 Constructs for introducing new sorts

In this section we present formal specifications for the four usual constructs for sort introduction: cartesian product, subsort, discriminated union and quotient.

The specifications for the first three constructs are axiomatisations of their usual

description [Hoa74, Vel87]. While the specification for the last one axiomatises the construction of the quotient with its natural projection.

Later on we shall establish some properties of these specifications.

2.1 Cartesian Product

Let T be a specification with two sorts S_1, S_2. Then, a specification of the cartesian product of these two sorts is:

T' = T +

sort C

operations $p_1 : C \to S_1$

$p_2 : C \to S_2$

axioms

- $\forall x_1 : S_1 \forall x_2 : S_2 \ \exists y : C \ \ p_1(y) = x_1 \wedge p_2(y) = x_2$
- $\forall y, y' : C \ \ p_1(y) = p_1(y') \wedge p_2(y) = p_2'(y) \Longrightarrow y = y'$

These axioms make C behave as the cartesian product of S_1 and S_2, as will be shown.

Indeed, in the next section, we will show that, in any model of T', the new sort may be regarded as consisting of the ordered pairs $< a_1, a_2 >$ of elements of the given sorts.

2.2 Subsort

Let T be a specification with a sort S and an unary (relativisation) predicate r over S (**r** points which elements of **S** are in the subset N of S) such that $T \models \exists x : S \ r(x)$. Then, a specification of the subsort N of the sort S in according with r is:

T' = T +

sort N

operations $j : N \to S$

axioms

- $\forall x : S \ \ r(x) \iff \exists y : N \ \ x = j(y)$
- $\forall y, y' : N \ \ j(y) = j(y') \Longrightarrow y = y'$

These axioms force N to behave as the set of elements of S selected by r.

In fact, as will be shown in the next section, in any model of T', the new sort can be regarded as consisting of those elements of sorts that satisfy the relativisation predicate.

Note that if we already have the sorts S, N and the function symbol j then we can introduce the predicate symbol r by definition (as the image of the function j). But we cannot define N solely from S and r.

2.3 Discriminated Union

Let T be a specification with two sorts S_1 and S_2. Then, a specification of the (discriminated) union of these two sorts is:

T' = T +

sort U

operations $i_1 : S_1 \to U$

$i_2 : S_2 \to U$

axioms

- $\forall u : U \;\; (\exists x_1 : S_1 \;\; u = i_1(x_1)) \vee (\exists x_2 : S_2 \;\; u = i_2(x_2))$
- $\forall x_1 : S_1 \; \forall x_2 : S_2 \; i_1(x_1) \neq i_2(x_2)$
- $\forall x, x' : S_1 \;\; i_1(x) = i_1(x') \Rightarrow x = x'$
- $\forall y, y' : S_2 \;\; i_2(y) = i_2(y') \Rightarrow y = y'$

These axioms make U exhibit the behaviour of the discriminated union of S_1 and S_2, as will be shown.

Indeed, in the next section we will show that the new sort in a model of T' may be viewed as the discriminated union of the given sorts.

2.4 Quotient sort

Let T be a specification with a sort S and a binary predicate q over S, which is proved in T to be an equivalence relation. Then, a specification of the quotient sort Q of the sort S by the relation q is:

T' = T +

sort Q

operations $p : S \to Q$

axioms

- $\forall x, x' : S \;\; q(x, x') \iff p(x) = p(x')$
- $\forall y : Q \;\; \exists x : S \;\; p(x) = y$

The axioms state that q is the kernel of the function p and also p is onto.

We will show in the next section that the new sort in a model of T' can be regarded as consisting of the equivalence classes of the elements of the given sort under the equivalence relation.

Note that if we have sorts S and Q and a surjective $p : S \to Q$ then we can introduce q by definition via the first axiom, but we cannot define sort Q only from S and q.

Also, by introducing such a quotient sort one can normalise any equivalence relation q over sort S to true identity over Q.

3 Adequacy of the specifications

In this section we establish some model theoretic properties of the specifications presented in Section 2.

For each one of the four specifications, we examine their models, which leads to:

- their characterisation, showing that the new sort indeed exhibits the desired behaviour.
- the invariance under isomorphism and the functorial character ([HS73]) of the constructs specified.

These results indicate the adequacy of the specifications in capturing behaviour that is to be expected from the intuitive view of these sort introducing constructs.

We shall examine each construct in turn in the following four subsection.

We shall use T to stand for the specification of the given theory, where a new sort is to be introduced, and T' for the extended theory, with the new sort and its accompanying conversion functions. Also, L stands for the language of the specification T, and L' for the language of T'. Given a structure $\mathcal{A}'$ for the language L', we use $\mathcal{A} = \mathcal{A}'/L$ to denote its reduct to the sublanguage L.

Finally, given a function h defined on a many-sorted structure $\mathcal{A}$, we use h_S to denote its restriction to sort $S^{\mathcal{A}}$.

3.1 Cartesian product

In this subsection, T and T' are the specifications in subsection 2.1.

The next result characterises the models of T'. It shows that the new sort may be regarded as consisting of the desired ordered pairs and behaves as (categorical) product ([HS73]) of the given sorts.

Theorem 3.1.1 (Characterisation of Mod T') *$\mathcal{A}' \models T'$ iff, with $\mathcal{A}'/L = \mathcal{A}$,*

1. *$\mathcal{A} \models T$, and*
2. *there exists a bijection $h : C^{\mathcal{A}'} \rightarrow S_1^{\mathcal{A}} \times S_2^{\mathcal{A}}$ such that $h(c) =< p_1^{\mathcal{A}'}(c), p_2^{\mathcal{A}'}(c) >$.*

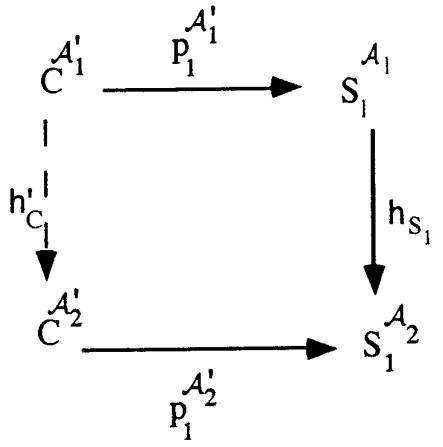
Proof:

- To prove the direction left-to-right assume $\mathcal{A}' \models T'$ and $\mathcal{A} = \mathcal{A}'/L$.
  1. Clearly $\mathcal{A} \models T$
  2. Consider the function $h : C^{\mathcal{A}'} \rightarrow S_1^{\mathcal{A}} \times S_2^{\mathcal{A}}$ defined by the given assignment. The two axioms of T' establish its surjectivity and injectivity.
- To prove the direction right-to-left assume $\mathcal{A} \models$ T. Consider its expansion $\mathcal{A}^{\times}$ to a structure of L' with $C^{\mathcal{A}^{\times}} = S_1^{\mathcal{A}} \times S_2^{\mathcal{A}}$ and its projections. Then, clearly $\mathcal{A}^{\times} \models$ T'. The requirement in (2) implies that $\mathcal{A}' \cong \mathcal{A}^{\times}$, as L'-structures. Therefore, $\mathcal{A}' \models$ T'.

Corollary 3.1.2 (Expansiveness) *The extension $T \subseteq T'$ is expansive.*

Corollary 3.1.3 (Conservativeness) *The extension $T \subseteq T'$ is conservative.*

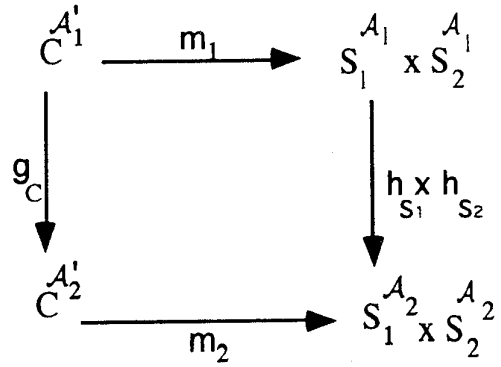
Proposition 3.1.4 (Invariance under isomorphism) *Given $\mathcal{A}'_1, \mathcal{A}'_2 \models T'$, each isomorphism between their reducts $h : \mathcal{A}_1 \to \mathcal{A}_2$ extends (uniquely) to an isomorphism $h' : \mathcal{A}'_1 \to \mathcal{A}'_2$, i.e. the following diagram for the first projection and the analogous one for the second projection commute*



Proof:
For $j = 1, 2$, since $\mathcal{A}'_j \models$ T', the characterisation result in theorem 3.1.1 states that the mediating $m_j =< p_1^{\mathcal{A}'_j}, p_2^{\mathcal{A}'_j} >: C^{\mathcal{A}'_j} \to S_1^{\mathcal{A}_j} \times S_2^{\mathcal{A}_j}$ is a bijection extending the identity $1 : \mathcal{A}_j \to \mathcal{A}_j$ to an isomorphism $h_j : \mathcal{A}'_j \to \mathcal{A}_j^{\times}$. The given (iso)morphism $h : \mathcal{A}_1 \to \mathcal{A}_2$ can be extended to an (iso)morphism $h^{\times} : \mathcal{A}_1^{\times} \to \mathcal{A}_2^{\times}$ by the addition of $h_{S_1} \times h_{S_2} : S_1^{\mathcal{A}_1} \times S_2^{\mathcal{A}_1} \to S_1^{\mathcal{A}_2} \times S_2^{\mathcal{A}_2}$, with $h_{S_1} \times h_{S_2}(< a_1, a_2 >) =< h_{S_1}(a_1), h_{S_2}(a_2) >$.

Existence: The composite $h_2^{-1}.h^{\times}.h_1$ is an isomorphism $h' : \mathcal{A}'_1 \to \mathcal{A}'_2$ with the required commutativity.

Uniqueness: Given any $g : \mathcal{A}'_1 \to \mathcal{A}'_2$ with the required commutativity on the new sort, we have



whence g agrees with h over the new sort, in view of the bijectivity of m_1 and m_2.

Corollary 3.1.5 (Monomorphic character) *Given $\mathcal{A}'_1, \mathcal{A}'_2 \models T'$ with $\mathcal{A}'_1/L = \mathcal{A} = \mathcal{A}'_2/L$, there exists a (unique) bijection $h_C : C^{\mathcal{A}'_1} \to C^{\mathcal{A}'_2}$ extending the identity to an isomorphism $\mathcal{A}'_1 \cong \mathcal{A}'_2$.*

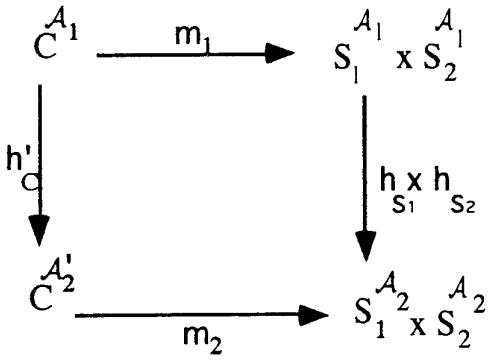
Notice that in the previous corrollary one cannot conclude $\mathcal{A}'_1 = \mathcal{A}'_2$ because the objects of the new sort may have distinct representations in the two structures.

In fact we can extract a more general result from the construction in the proof of Proposition 3.1.4.

Proposition 3.1.6 (Functorial character) *Given $\mathcal{A}'_1, \mathcal{A}'_2 \models T'$, each homomorphism $h : \mathcal{A}_1 \to \mathcal{A}_2$ between their reducts to L has a unique extension to an homomorphism $h' : \mathcal{A}'_1 \to \mathcal{A}'_2$*

Proof:
It suffices to use the construction in the proof of proposition 3.1.4 and notice that the assumed bijectivity of h was relied upon only for concluding that the resulting h' is bijective.

Indeed, the following commutative diagram



defines h' uniquely on the new sort, because the mediating $m_j =< p_1^{\mathcal{A}'_j}, p_2^{\mathcal{A}'_j} >$ are bijective .

3.2 Subsort

In this subsection T and T' refer to the specifications in subsection 2.2. Notice the precondition $T \models \exists x : S\ r(x)$

Theorem 3.2.1 (Characterisation of Mod T') *$\mathcal{A}' \models T'$ iff, with $\mathcal{A}'/L = \mathcal{A}$,*

1. *$\mathcal{A} \models T$, and*

2. *there exists a bijection* $h : N^{\mathcal{A}'} \to r^{\mathcal{A}}$, *where* $r^{\mathcal{A}} = \{a \in S^{\mathcal{A}} \;/\; \mathcal{A} \models r(x)[a]\}$, *such that* $h(c) = j^{\mathcal{A}'}(c)$.

Proof:

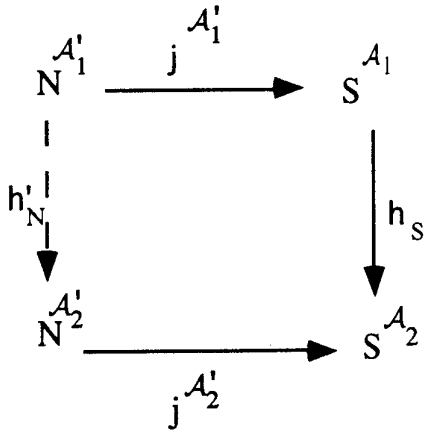
- To prove the direction left-to-right assume $\mathcal{A}' \models T'$ and $\mathcal{A} = \mathcal{A}'/L$.
  1. Clearly $\mathcal{A} \models T$
  2. Consider the function $h : N^{\mathcal{A}'} \to S^{\mathcal{A}}$ defined by the given assignment. The two axioms of T' establish that, since $h = j^{\mathcal{A}'}$, h is injective and its image is the extension $r^{\mathcal{A}}$ of r in $\mathcal{A}$
- To prove the direction right-to-left assume $\mathcal{A} \models$ T, so $r^{\mathcal{A}} \neq \emptyset$. Consider its expansion $\mathcal{A}^r$ to a structure of L' with $N^{\mathcal{A}^r} = r^{\mathcal{A}}$ and its inclusion. Then, clearly $\mathcal{A}^r \models$ T'. The requirement in (2) implies that $\mathcal{A}' \cong \mathcal{A}^r$, as L'-structures. Therefore, $\mathcal{A}' \models$ T'.

This result establishes that the new sort may be thought of as consisting of those elements that satisfy the relativisation predicate. But, the elements of the new sort may very well have a different representation. This possibly different representation is one reason for the conversion fuction $j : N \to S$. This is illustrated by the (unsigned) naturals as a subsort of the (signed) integers.

Corollary 3.2.2 (Expansiveness) *The extension* $T \subseteq T'$ *is expansive.*

Corollary 3.2.3 (Conservativeness) *The extension* $T \subseteq T'$ *is conservative.*

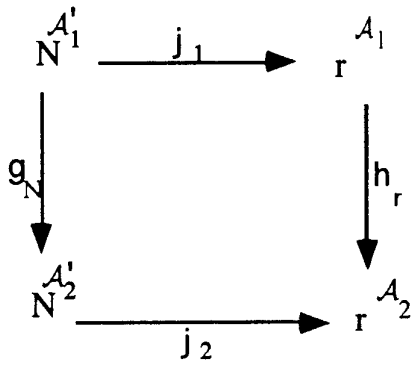
Proposition 3.2.4 (Invariance under isomorphism) *Given* $\mathcal{A}'_1, \mathcal{A}'_2 \models T'$, *each isomorphism between their reducts* $h : \mathcal{A}_1 \to \mathcal{A}_2$ *extends (uniquely) to an isomorphism* $h' : \mathcal{A}'_1 \to \mathcal{A}'_2$, *i.e. the following diagram commutes*



Proof:
For $k = 1, 2$, since $\mathcal{A}'_k \models$ T', the characterisation result in theorem 3.2.1 states that the restriction $j_k : N^{\mathcal{A}'_k} \to r^{\mathcal{A}_k}$ is a bijection extending the identity $1 : \mathcal{A}_k \to \mathcal{A}_k$ to an isomorphism $g_k : \mathcal{A}'_k \to \mathcal{A}^r_k$. The given (iso)morphism $h : \mathcal{A}_1 \to \mathcal{A}_2$ can be extended to an (iso)morphism $h^r : \mathcal{A}^r_1 \to \mathcal{A}^r_2$ by the addition of $h_r : r^{\mathcal{A}_1} \to r^{\mathcal{A}_2}$, well defined as the restriction of h (because $\mathcal{A}_k \models$ T).

Existence: The composite $g_2^{-1}.h^r.g_1$ is an isomorphism $h' : \mathcal{A}'_1 \to \mathcal{A}'_2$ with the required commutativity.

Uniqueness: Given any $g : \mathcal{A}'_1 \to \mathcal{A}'_2$ with the required commutativity on the new sort, we have



whence g agrees with h' over the new sort.

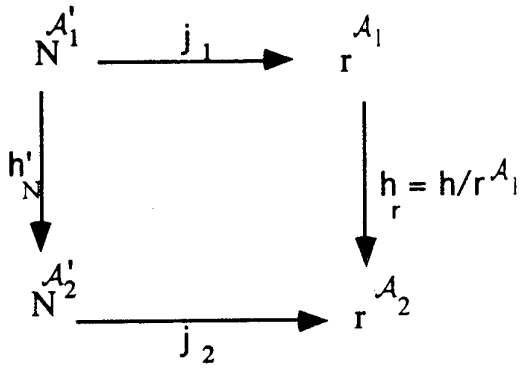
Corollary 3.2.5 (Monomorphic character) *Given $\mathcal{A}'_1, \mathcal{A}'_2 \models T'$ with $\mathcal{A}'_1/L = \mathcal{A} = \mathcal{A}'_2/L$, there exists a (unique) bijection $h_N : N^{\mathcal{A}'_1} \to N^{\mathcal{A}'_2}$ extending the identity to an isomorphism $\mathcal{A}'_1 \cong \mathcal{A}'_2$.*

Again, notice that we cannot conclude $\mathcal{A}'_1 = \mathcal{A}'_2$ because of possibly different representations.

Proposition 3.2.6 (Functorial character) *Given $\mathcal{A}'_1, \mathcal{A}'_2 \models T'$ each homomorphism $h : \mathcal{A}_1 \to \mathcal{A}_2$ between their reducts to L has a unique extension to an homomorphism $h' : \mathcal{A}'_1 \to \mathcal{A}'_2$*

Proof:
It suffices to notice that the construction in the proof of proposition 3.2.4 does not really need the bijectivity of h.

Indeed, the following commutative diagram



defines h' uniquely on the new sort because the restrictions $j_k : N^{\mathcal{A}'_k} \to r^{\mathcal{A}_k}$ are well defined bijections.

3.3 Discriminated Union

In this subsection, T and T' stand for the specifications in subsection 2.3.

The next result characterises the models of T'. It shows that the new sort may be viewed as the disjoint union of the given sorts, as desired, and exhibits the behaviour of their (categorical) coproduct ([HS73]).

Theorem 3.3.1 (Characterisation of Mod T') *$\mathcal{A}' \models T'$ iff, with $\mathcal{A}'/L = \mathcal{A}$,*

1. *$\mathcal{A} \models T$, and*
2. *there exists a bijection $h : S_1^{\mathcal{A}} + S_2^{\mathcal{A}} \to U^{\mathcal{A}'}$ such that $h(a) = i_1^{\mathcal{A}'}(a)$ for each $a \in S_1^{\mathcal{A}}$ and $h(b) = i_2^{\mathcal{A}'}(b)$ for each $b \in S_2^{\mathcal{A}}$.*

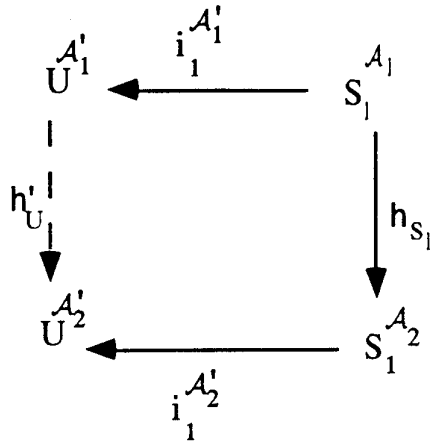
Proof:

- To prove the direction left-to-right assume $\mathcal{A}' \models T'$ and $\mathcal{A} = \mathcal{A}'/L$.
  1. Clearly $\mathcal{A} \models T$
  2. Consider the function $h : S_1^{\mathcal{A}} + S_2^{\mathcal{A}} \to U^{\mathcal{A}'}$ defined by the given assignment. The four axioms of T' establish its bijectivity.
- To prove the direction right-to-left assume $\mathcal{A} \models$ T. Consider its expansion $\mathcal{A}^+$ to a structure of L' with $U^{\mathcal{A}^+} = S_1^{\mathcal{A}} + S_2^{\mathcal{A}}$ and its insertions. Then, clearly $\mathcal{A}^+ \models$ T'. The requirement in (2) implies that $\mathcal{A}' \cong \mathcal{A}^+$, as L'-structures. Therefore, $\mathcal{A}' \models$ T'.

Corollary 3.3.2 (Expansiveness) *The extension $T \subseteq T'$ is expansive.*

Corollary 3.3.3 (Conservativeness) *The extension $T \subseteq T'$ is conservative.*

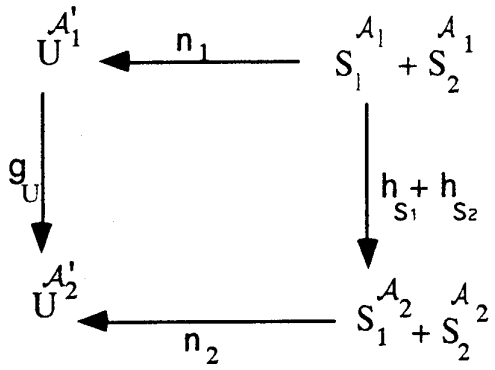
Proposition 3.3.4 (Invariance under isomorphism) *Given $\mathcal{A}'_1, \mathcal{A}'_2 \models T'$, each isomorphism between their reducts $h : \mathcal{A}_1 \to \mathcal{A}_2$ extends (uniquely) to an isomorphism $h' : \mathcal{A}'_1 \to \mathcal{A}'_2$,i.e. the following diagram for the first insertion and the analogous one for the second insertion commute*



Proof:
For $k = 1, 2$, since $\mathcal{A}'_k \models$ T', the characterisation result in theorem 3.3.1 states that the mediating $n_k = [i_1^{\mathcal{A}'_k} | i_2^{\mathcal{A}'_k}] : S_1^{\mathcal{A}_j} + S_2^{\mathcal{A}_k} \to U^{\mathcal{A}'_k}$ is a bijection extending the identity $1 : \mathcal{A}_k \to \mathcal{A}_k$ to an isomorphism $h_k : \mathcal{A}'_k \to \mathcal{A}_k^+$. The given (iso)morphism $h : \mathcal{A}_1 \to \mathcal{A}_2$ can be extended to an (iso)morphism $h^+ : \mathcal{A}_1^+ \to \mathcal{A}_2^+$ by the addition of $h_{S_1} + h_{S_2} : S_1^{\mathcal{A}_1} + S_2^{\mathcal{A}_1} \to S_1^{\mathcal{A}_2} + S_2^{\mathcal{A}_2}$, with $(h_{S_1} + h_{S_2})(a_k) = h_k(a_k)$, if $a_k \in S_k^{\mathcal{A}_1}$ for $k = 1, 2$.

Existence: The composite $h_2^{-1}.h^+.h_1$ is an isomorphism $h' : \mathcal{A}'_1 \to \mathcal{A}'_2$ with the required commutativity.

Uniqueness: Given any $g : \mathcal{A}'_1 \to \mathcal{A}'_2$ with the required commutativity on the new sort, we have

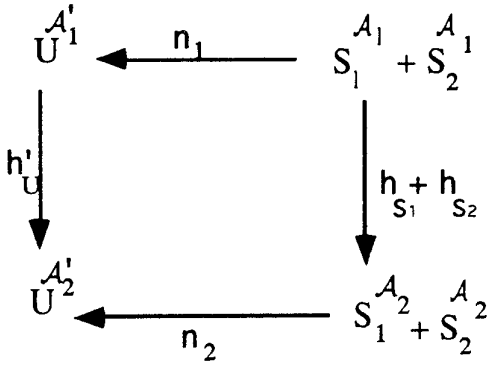


whence g agrees with h over the new sort, since n_1 and n_2 are bijective .

Corollary 3.3.5 (Monomorphic character) *Given $\mathcal{A}'_1, \mathcal{A}'_2 \models T'$ with $\mathcal{A}'_1/L = \mathcal{A} = \mathcal{A}'_2/L$, there exists a (unique) bijection $h_U : U^{\mathcal{A}'_1} \to U^{\mathcal{A}'_2}$ extending the identity to an isomorphism $\mathcal{A}'_1 \cong \mathcal{A}'_2$.*

Proposition 3.3.6 (Functorial character) *Given $\mathcal{A}'_1, \mathcal{A}'_2 \models T'$ each homomorphism $h : \mathcal{A}_1 \to \mathcal{A}_2$ between their reducts to L has a unique extension to an homomorphism $h' : \mathcal{A}'_1 \to \mathcal{A}'_2$*

Proof:
It suffices to notice that the actual construction in the proof of proposition 3.3.4 did not rely on the bijectivity of h. Indeed, the following commutative diagram



defines h' uniquely on the new sort, because the mediating $n_k = [i_1^{\mathcal{A}'_k} | i_2^{\mathcal{A}'_k}]$ are bijections.

3.4 Quotient

In this subsection T and T' are to be understood as the specifications in subsection 2.4. Notice the precondition on T: reflexivity, symmetry and transitivity of q must be theorems of T.

The next resultcharacterises the models of T' by showing that the new sort can be thought to consist of the desired equivalence classes, or representatives for them.

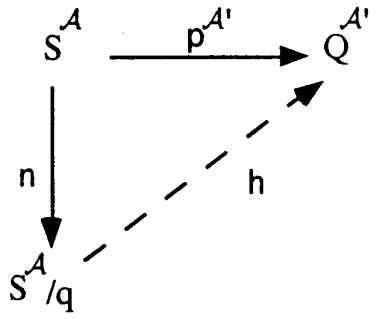
Theorem 3.4.1 (Characterisation of Mod T') *$\mathcal{A}' \models T'$ iff, with $\mathcal{A}'/L = \mathcal{A}$,*

1. *$\mathcal{A} \models T$, and*
2. *there exists a bijection $h : S^{\mathcal{A}}/q^{\mathcal{A}} \to Q^{\mathcal{A}'}$ such that $h([a]) = p^{\mathcal{A}'}(a)$, where $[a]$ is the equivalence class of $a \in S$ under q.*

Proof:

- To prove the direction left-to-right assume $\mathcal{A}' \models T'$ and $\mathcal{A} = \mathcal{A}'/L$.

  1. Clearly $\mathcal{A} \models T$, whence $q^{\mathcal{A}}$ is an equivalence relation on $S^{\mathcal{A}}$.
  2. Consider the function $p^{\mathcal{A}'} : S^{\mathcal{A}} \to Q^{\mathcal{A}'}$. The two axioms of T' show that $p^{\mathcal{A}'}$ is surjective with $\mathrm{Ker}(p^{\mathcal{A}'}) = q^{\mathcal{A}}$, where $\mathrm{Ker}(p^{\mathcal{A}'}) = \{< a_1, a_2 > \in S^{\mathcal{A}} \times S^{\mathcal{A}} \;/\; p^{\mathcal{A}'}(a_1) = p^{\mathcal{A}'}(a_2)\}$. Hence, there exists a bijection h such that the following diagram commutes



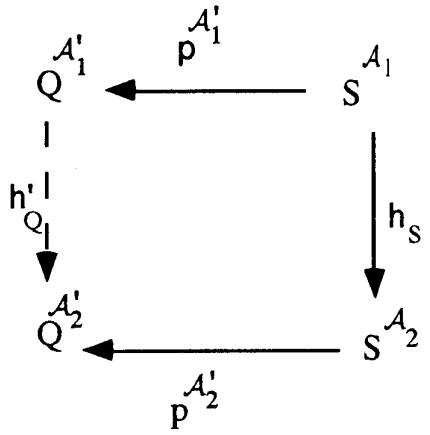
  with $n : S^{\mathcal{A}} \to S^{\mathcal{A}}/q^{\mathcal{A}}$ given by $n(a) = [a]$.

- To prove the direction right-to-left assume $\mathcal{A} \models$ T, so $q^{\mathcal{A}}$ is an equivalence relation on $S^{\mathcal{A}}$. Consider its expansion $\mathcal{A}^q$ to a structure of L' with $Q^{\mathcal{A}^q} = S^{\mathcal{A}}/q^{\mathcal{A}}$ together with its natural projection onto the quotient. Then, clearly $\mathcal{A}^q \models$ T'. The requirement in (2) implies that $\mathcal{A}' \cong \mathcal{A}^q$, as L'-structures. Therefore, $\mathcal{A}' \models$ T'.

Corollary 3.4.2 (Expansiveness) *The extension $T \subseteq T'$ is expansive.*

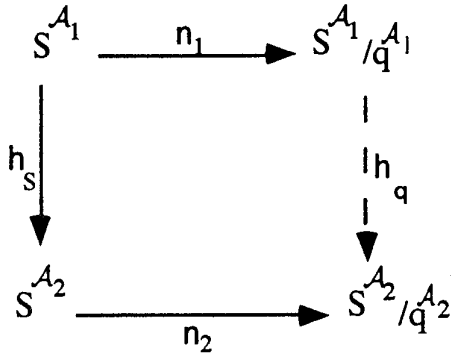
Corollary 3.4.3 (Conservativeness) *The extension $T \subseteq T'$ is conservative.*

Proposition 3.4.4 (Invariance under isomorphism) *Given $\mathcal{A}'_1, \mathcal{A}'_2 \models T'$, each isomorphism between their reducts $h : \mathcal{A}_1 \to \mathcal{A}_2$ extends (uniquely) to an isomorphism $h' : \mathcal{A}'_1 \to \mathcal{A}'_2$,i.e. the following diagram commutes*



Proof:
For $j = 1, 2$, since $\mathcal{A}'_j \models$ T', the characterisation result in theorem 3.4.1 gives a bijection $\tilde{p}_j : S^{\mathcal{A}_j}/q^{\mathcal{A}_j} \to Q^{\mathcal{A}'_j}$ extending the identity $1 : \mathcal{A}_j \to \mathcal{A}_j$ to an isomorphism $g_j : \mathcal{A}'_j \to \mathcal{A}^q_j$.

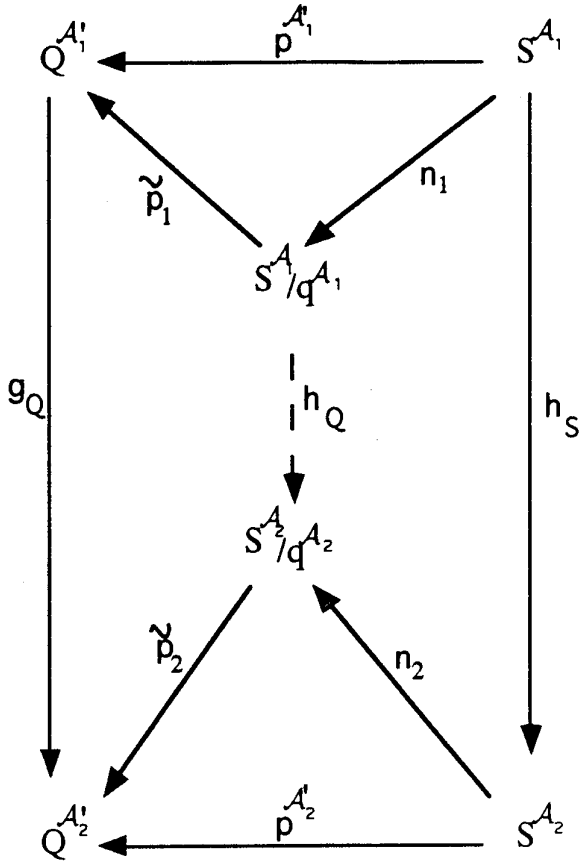
Now consider the given (iso)morphism $h : \mathcal{A}_1 \to \mathcal{A}_2$. Since $\mathcal{A}_1, \mathcal{A}_2 \models$ T, we have $< h(a), h(a') > \in q^{\mathcal{A}_2}$ whenever $< a, a' > \in q^{\mathcal{A}_1}$. Thus, since $\mathcal{A}'_1, \mathcal{A}'_2 \models$ T' , $< h(a), h(a') > \in \mathrm{Ker}(p^{\mathcal{A}'_2})$ whenever $< a, a' > \in \mathrm{Ker}(p^{\mathcal{A}'_1})$ and there exists $h_q : S^{\mathcal{A}_1}/q^{\mathcal{A}_1} \to S^{\mathcal{A}_2}/q^{\mathcal{A}_2}$ such that the following diagram commutes



The addition of $h_q : S^{\mathcal{A}_1}/q^{\mathcal{A}_1} \to S^{\mathcal{A}_2}/q^{\mathcal{A}_2}$ to the given $h : \mathcal{A}_1 \to \mathcal{A}_2$, extends it to an isomorphism $h^q : \mathcal{A}^q_1 \to \mathcal{A}^q_2$.

Existence: The composite $g_2^{-1}.h^q.g_1$ is an isomorphism $h' : \mathcal{A}'_1 \to \mathcal{A}'_2$ with the required commutativity.

Uniqueness: Given any $g : \mathcal{A}'_1 \to \mathcal{A}'_2$ with the required commutativity we have, on the new sort



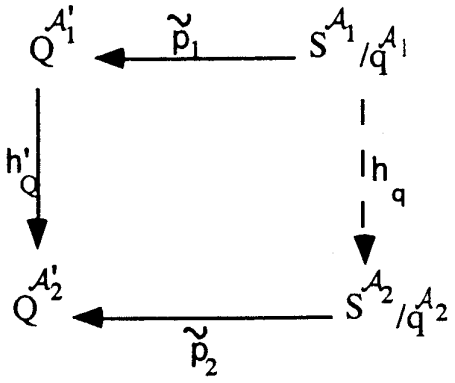
which shows that g agrees with h' over the new sort, since $\tilde{p}_1$ and $\tilde{p}_2$ are bijections.

Corollary 3.4.5 (Monomorphic character) *Given $\mathcal{A}'_1, \mathcal{A}'_2 \models T'$ with $\mathcal{A}'_1/L = \mathcal{A} = \mathcal{A}'_2/L$, there exists a (unique) bijection $h_Q : Q^{\mathcal{A}'_1} \to Q^{\mathcal{A}'_2}$ extending the identity to an isomorphism $\mathcal{A}'_1 \cong \mathcal{A}'_2$.*

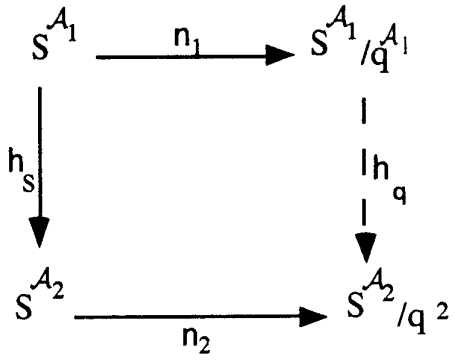
In this case it is quite clear why we cannot conclude $\mathcal{A}'_1 = \mathcal{A}'_2$: one may use different representatives for the equivalence classes.

Proposition 3.4.6 (Functorial character) *Given $\mathcal{A}'_1, \mathcal{A}'_2 \models T'$ each homomorphism $h : \mathcal{A}_1 \to \mathcal{A}_2$ between their reducts to L has a unique extension to an homomorphism $h' : \mathcal{A}'_1 \to \mathcal{A}'_2$*

Proof:
The construction presented in the proof of proposition 3.4.4 yields the desired extension, because it does not actually rely on the bijectivity of h. Indeed, the following commutative diagram



defines h' uniquely on the new sort because each $\tilde{p}_j$ is a bijection and h_q is uniquely defined by



4 Conclusions

We have examined four sort introducing constructs: cartesian product, subsort, discriminated union and quotient.

Introduction of new sorts is of interest because it occurs often in implementing formal specifications. In constrast to the introduction of new function or predicate symbols [Sho67], the case of new sorts is not extensively studied.

The four constructs examined correspond to natural constructions of new sets. Three of them have found their way as data structuring constructs in programming languages [Hoa74]. The quotient construct is of importance in developing and verifying correct implementations [TM87, Vel87].

In section 2 we have provided formal specifications for these four constructs by axiomatising their usual descriptions as extensions of specifications. In each case, in addition to the new sort, we also introduce appropriate conversion functions, connecting it to the old sorts.

In section 3 we have established the adequacy of these specifications in the sense of exhibiting the intented behaviour. We have first characterised their models, up

to isomorphism, as expansions by addition of a new sort as desired. In fact, we have shown that up to a unique isomorphism,

- a model of the cartesian product of S_1 and S_2 is the expansion with new sort $S_1^{\mathcal{A}} \times S_2^{\mathcal{A}}$ with the cartesian projections, which makes it a categorical product (see 3.1);
- a model of the subsort of S defined by relativisation predicate r is the expansion with new sort $\{a \in S^{\mathcal{A}} \mid \mathcal{A} \models r(x)[a]\}$ with its inclusion (see 3.2);
- a model of the discriminated union of S_1 and S_2 is the expansion with new sort the disjoint union of $S_1^{\mathcal{A}}$ and $S_2^{\mathcal{A}}$ with their inclusions, which makes it a categorical coproduct (see 3.3);
- a model of the quotient of S by equivalence relation q is the expansion with new sort consisting of the equivalence classes under q together with its natural projection onto the quotient (see 3.4).

From these characterisation theorems we have derived other desired properties of the specifications:

- the extensions are expansive, hence conservative;
- invariance under isomorphisms and monomorphic character;
- functorial character: each homomorphism between basic models has a unique extension to a homomorphism between models with new sorts and their conversion functions.

In each case the new sort is unique, but only up to isomorphism; this contrasts with the case of introduction of new function or predicate symbols by definitions, when we have unique expandability of models. Also, these more familiar extensions by definitions exhibit eliminability: any formula of the extended language is equivalent to some formula inthe original language.

In our case of introduction of new sorts one should not expect full eliminability, because of the new variables ranging over the sort introduced. Nevertheless, a kind of generalised eliminability is still possible, as we shall examine in a forthcoming paper.

References

[End72] H.B. Enderton. *A Mathematical Introduction to Logic.* Academic Press, Inc., New York, 1972.

[Eri82] H.D. Erich. On the theory of specification, implementation and parametrization of abstract data types. *Journal of the Association for Computing Machinery*, 29(1):206–227, January 1982.

[GB83] J.A. Goguen and R.M. Burstall. Introducing institutions. *Proceedings, Logics of Programming Workshop. Lecture Notes in Computer Science*, 164:221–256, 1983.

[Hoa74] C.A.R. Hoare. Notes on data structuring. In O.J. Dahl, E.W. Dijkstra, and C.A.R. Hoare, editors, *Structured Programming*, pages 83–174. Academic Press, 1974.

[HS73] H. Herrlich and G. E. Strecker. *Category Theory.* Ally and Bacon Inc., Boston, 1973.

[MD85] B. Möller and W. Dosch. On the algebraic specification of domains. In H.J. Kreowski, editor, *Recent Trends in Data Type Specification. Informatik Fachberichte 116*, pages 178–195. Springer-Verlag, 1985.

[Sho67] J.R. Shoenfield. *Mathematical Logic.* Addison-Wesley Publishing Company, 1967.

[TM87] W.M. Turski and T.S.E. Maibaum. *The Specification of Computer Programs.* Addison-Wesley Publishing Company, 1987.

[Vel87] P.A.S Veloso. *Estruturação e Verificação de Programas com Tipos de Dados.* Editora E. Blücher ltda., 1987.