Foundations of System Development

Prof. Dr. Martin Wirsing

04.10.2002

Data-Oriented System Development

Prof. Dr. Martin Wirsing

04.10.2002

MiS MIS

Functional Models: Interpretation of Interfaces through Structures

Goals

- Learn to understand the relationship between signature, term and mathematical structures
- Understand formulas and their interpretation in structures
- Understand the notions of Σ-homomorphisms
- Abstract data types, initial and reachable algebras
- Learn to put in relationship similar algebras through Σ-homomorphisms

Algebras and Structures

A Σ-algebra has for

- every sort a carrier set,
- every function symbol a function.

If signatures Σ also include predicate symbols, so you call them Σ-structures.

Definition 1 (Σ-Algebra):
Let $\Sigma = (S, F, P)$ be a signature.

1. A Σ-*algebra* A consists of
   (a) a family $(A_s)_{s \in S}$ of not empty carrier sets and
   (b) (total) functions $f^A : A_{s_1} \times \ldots \times A_{s_n} \to A_s$, for all $f \in F_{\langle\langle s_1, \ldots, s_n\rangle, s\rangle}$.
2. Moreover a Σ-structure has relations $p^A \subseteq A_{s_1} \times \ldots \times A_{s_n}$, for all $p \in P_{\langle s_1, \ldots, s_n\rangle}$
3. The class of all Σ-algebras is called $Alg(\Sigma)$, the class of all Σ-structures is called $Struct(\Sigma)$.

Example 1 (sig(BOOL0)-Algebras without "and", "or", "implies"):

1. The standard model B of boolean values

$$\begin{array}{ll} B_{Bool} = \{T, F\}, & \\ true^B = T, & false^B = F, \\ not^B(T) = F, & not^B(F) = T. \end{array}$$

2. The structure NB on the natural numbers with

$$\begin{array}{ll} NB_{Bool} = \mathbb{N}, & \\ true^{NB} = 1, & false^{NB} = 0, \\ not^{NB}(2i) = 2i+1, & not^{NB}(2i+1) = 2i \end{array}$$

3. The structure ZB on integers

$$\begin{array}{ll} ZB_{Bool} = \mathbb{Z}, & \\ true^{ZB} = 1, & false^{ZB} = 0, \\ not^{ZB}(1) = 0, & not^{ZB}(0) = 1, \\ not^{ZB}(i) = i, & \text{for } i \text{ different from } 0, 1. \end{array}$$

4. The structure $ZB1$ on integers with

$$
\begin{array}{ll}
ZB1_{Bool} = \mathbb{Z}, & \\
true^{ZB1} = 1, & false^{ZB1} = 0, \\
not^{ZB}(1) = 0, & not^{ZB}(0) = 1, \\
not^{ZB1}(i) = i + 1, & \text{for } i \text{ different from } 0, 1.
\end{array}
$$

5. The trivial structure UB with

$$
\begin{array}{l}
UB_{Bool} = 1, \\
true^{UB} = false^{UB} = 1, \\
not^{UB}(1) = 1,
\end{array}
$$

Example 2 (Algebras for SET0 (set signature)):

1. Finite sets on $\mathbb{Z}$: $P^{fin}(\mathbb{Z})$

$$\text{Elem}_{P^{fin}(\mathbb{Z})} =_{def} \mathbb{Z}$$
$$\text{Set}_{P^{fin}(\mathbb{Z})} =_{def} \{M | M \subseteq \mathbb{Z},\ M \text{ finite}\} \qquad \text{empty}^{P^{fin}(\mathbb{Z})} =_{def} \emptyset$$
$$\{z\}^{P^{fin}(\mathbb{Z})} =_{def} \{z\} \qquad M_1 \cup^{P^{fin}(\mathbb{Z})} M_2 =_{def} M_1 \cup M_2$$

2. Finite or infinite sets of integers: $P(\mathbb{Z})$

$$\text{Elem}_{P(\mathbb{Z})} =_{def} \mathbb{Z}$$
$$\text{Set}_{P(\mathbb{Z})} =_{def} \{M | M \subseteq \mathbb{Z}\}$$
for operations see previous example

3. AVL-Trees on natural numbers

$$\text{Elem}_{AVL} =_{def} \mathbb{N}$$
$$\text{Set}_{AVL} =_{def} \text{"all AVL-Trees"} \qquad \{z\}^{AVL} =_{def} \text{"one element AVL-Trees"}$$
$$\text{empty}^{AVL} =_{def} \text{"empty AVL-Tree"} \qquad AV_1 \cup^{AVL} AV_2 =_{def} \text{"unification of AVL-Trees"}$$

4. The one element structure U for Set

$$\begin{array}{ll}
\mathsf{Elem}_U =_{def} \mathbb{Z} & \\
\mathsf{Set}_U =_{def} \{\bullet\} & \mathsf{empty}^U =_{def} \bullet \\
\{z\}^U =_{def} \bullet & M_1 \cup^U M_2 =_{def} \bullet
\end{array}$$

5. Numbers for set

$$\begin{array}{ll}
\mathsf{Elem}_{ZZ} =_{def} \mathbb{Z} & \\
\mathsf{Set}_{ZZ} =_{def} \mathbb{Z} & \mathsf{empty}^{ZZ} =_{def} 0 \\
\{z\}^{ZZ} =_{def} z & z_1 \cup^{ZZ} z_2 =_{def} z_1 + z_2
\end{array}$$

Term Algebra

Let $\Sigma = (S, F)$ be a sensible signature.
The term algebra structure: We use T for $T(\Sigma, X)$.
The carrier sets of T are the sets $T(\Sigma, X)_s$ for $s \in S$. The interpretation of function symbols is defined by:

$$f^T(a_1, \ldots, a_n) =_{def} f(a_1, \ldots, a_n) \quad \text{for } a_i \in T_{s_i}$$

Example 3 (Term algebra T):
Ground term algebra $T = T(\text{BOOL0})$ with

$$\begin{array}{ll} T_{\text{Bool}} = T(\text{BOOL0})_{Bool} & \{\text{true}, \text{false}\} \\ \text{true}^T = \text{true} & \text{false}^T = \text{false} \\ \text{not}^T(t) = \text{not}(t) & \text{and so on.} \end{array}$$

Interpretation of Terms

Definition 2 (Term Interpretation):
Given Σ, X, Σ-algebra A

1. A assignment from X to A is a family of mappings $(v_s : X_s \to A_s)_{s \in S}$, written $v : X \to A$.
2. The interpretation $I_v : T(\Sigma, X) \to A$ of terms in A concerning v defines the following family of mappings:
   (a) $(I_{v_s})(x) = v_s(x)$ for $s \in S$
   (b) $I_{v_s}(f(t_1, \ldots, t_n)) = f^A(I_{v_{s1}}(t_1), \ldots, I_{v_{sn}}(t_n))$,
   for all $f \in F_{\langle\langle s_1, \ldots, s_n\rangle, s\rangle}, t_1 \in T(\Sigma, X)_{s1, \ldots, t_n} \in T(\Sigma, X)_{sn}$

   Instead of I_{v_s} we write I_v
   For $t \in T(\Sigma, \{\emptyset\})$ we write t^B.

Σ-Formulas

Definition 3 (Σ-Formulas):
Let $\Sigma = (S, F, P)$ be a signature and X be a S-sorted family of variables.

1. An atomic Σ-formula has the form

   $$p(t_1, \ldots, t_n) \quad \text{for } p \in P_{\langle s_1,\ldots,s_n\rangle}, t_1 \in T(\Sigma, X)_{s_1}, \ldots, t_n \in T(\Sigma, X)_{s_n}$$

   Moreover for every sort $s \in S$ and all terms $t_1, t_2 \in T(\Sigma, X)_s$,
   $t_1 =_s t_2$
   is an atomic formula.
2. The set of Σ-formulas $WFF(\Sigma)$ (well-formed formula) is the smallest set, that fulfils following properties (inductive definition):
   (a) every atomic Σ-formula is in $WFF(\Sigma)$,
   (b) if G_1, G_2 in $WFF(\Sigma)$, so $(\neg G_1)$ and $(G_1 \wedge G_2)$ as well,
   (c) if G in $WFF(\Sigma)$, $x \in X_s$, so $(\forall x : s.\ G)$ in $WFF(\Sigma)$.

3. Further operators are defined as abreviations:

$$
\begin{aligned}
(G_1 \vee G_2) &=_{def} \neg((\neg G_1) \wedge (\neg G_2)) \\
(G_1 \implies G_2) &=_{def} ((\neg G_1) \vee G_2) \\
(G_1 \equiv G_2) &=_{def} ((G_1 \implies G_2) \wedge (G_2 \implies G_1) \\
(\exists x : s.\ G) &=_{def} (\neg(\forall x : s.\ (\neg G)))
\end{aligned}
$$

   The set of free variables of G is called $FV(G)$. A formula G is called closed, if $FV(G) = \emptyset$.

4. A quantifier free formula is a Σ-formula without quantors.
5. A Horn formula has the form

$$\forall x_1 : s_1, \ldots, \forall x_m : s_m.\ G_1 \wedge \ldots \wedge G_n \implies G$$

   for atomic formulas G_i and G. If all G and G_i are equations we speak of a conditional equational formula or short of conditional equation.

Example 4 (Σ-Formulas):

1. $\forall x, y, z$: Elem. $(x \circ y) \circ z = x \circ (y \circ z)$
   is an universally quantified equation for the description of associativity.
2. $\forall x, y$: Nat. $\text{succ}(x) = \text{succ}(y) \implies x = y$
   is a conditional equation for the description of injectivity of succ.
3. $\forall x$: Bool. $x = \text{true} \lor x = \text{false}$
   defines, that the sort Bool has at most two elements.
4. $\forall x$: Bool. $\text{not}(\text{not}(x)) = x$
   describes the idempotency of not.

Properties of Algebras: Homomorphism, initial and reachable Structures

Definition 4 (Σ-Homomorphism):
Let Σ = (S, F) be the signature and let A, B be Σ-algebras

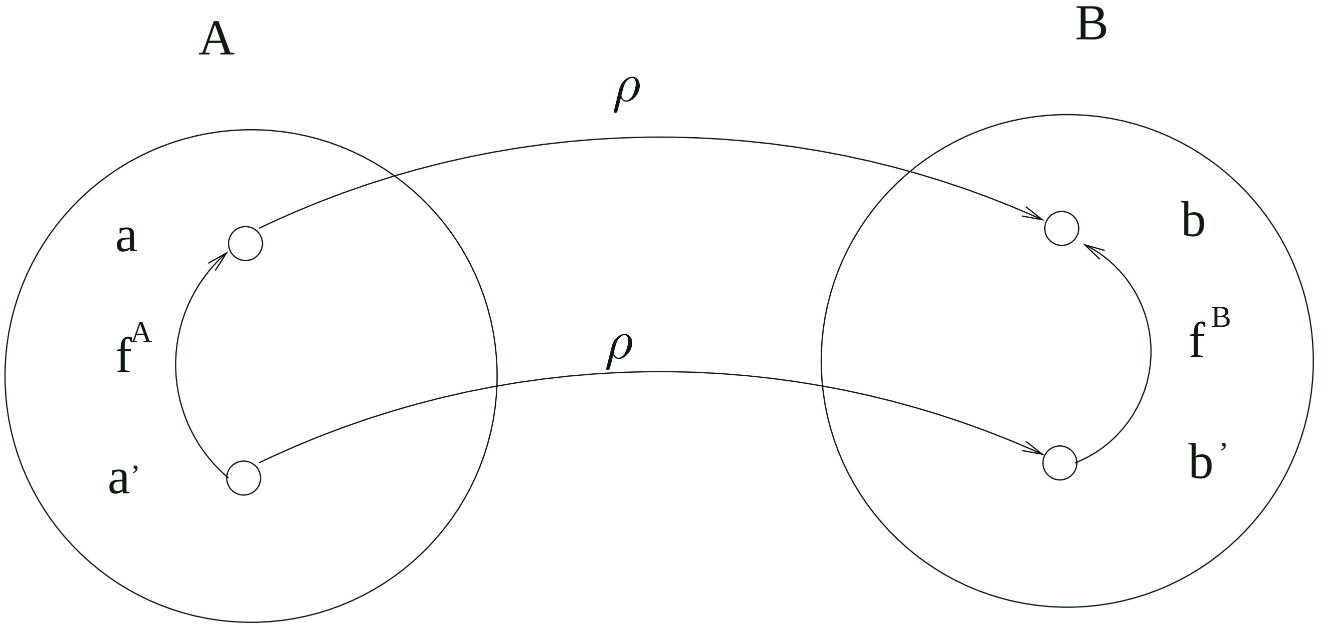
1. A Σ-homomorphism $(\rho : A \;\rightarrow B)$ is a family of mappings

$$(\rho_s : A_s \rightarrow B_s)_{s\in\ S}$$

   with following properties:
   For all function symbols $f \in F_{\langle\langle s_1,\ldots,s_n\rangle s\rangle}$, and all $a_i \in A_{s_i}$, $i = 1, \ldots, n$:

$$\rho_s(f^A(a_1, \ldots, a_n)) = f^B(\rho_{s_1}(a_1), \ldots, \rho_{s_n}(a_n))$$

2. A bijective Σ-homomorphism is called Σ-isomorphism. Two Σ-algebras A, B are called isomorphic, if there is a Σ-isomorphism from A to B.


A
B
ρ
a
b
f^A
ρ
f^B
a'
b'

Notice:

1. The equality is preserved by Σ-homomorphisms:

$$a_1 =^A a_2 \Rightarrow \rho_s(a_1) =^B \rho_s(a_2)$$

   but not the inequality:

$$a_1 \neq^A a_2 \Rightarrow \rho_s(a_1) \neq^B \rho_s(a_2)$$

2. For structures a Σ-homomorphism requires additionally, that predicates are preserved:
   for $p \in P_{\langle s_1,\ldots,s_n\rangle}$ and $a_i \in A_{s_i}$, $i = 1, \ldots, n$:

$$(a_1, \ldots, a_n) \in p^A \Rightarrow (\rho_{s_1}(a_1), \ldots, \rho_{s_n}(a_n)) \in p^B$$

Example 5 (NAT0-Algebras):
Let

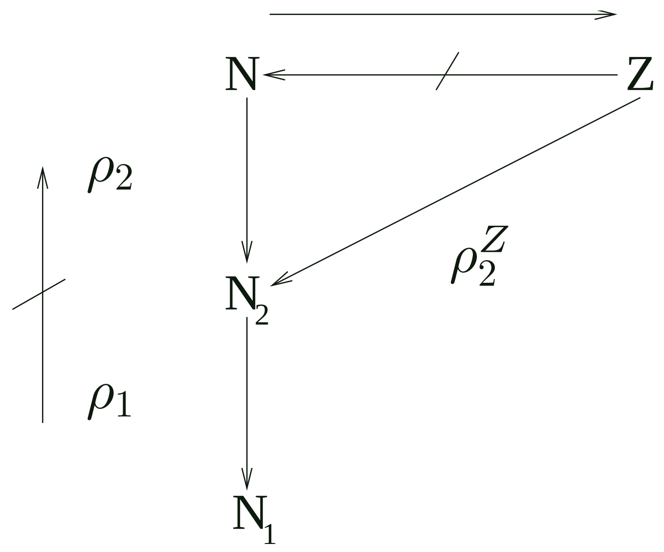
- $N = \langle \mathbb{N}, 0, \_ + 1 \rangle$ the standard model of natural numbers.
- $Z = \langle \mathbb{Z}, 0, \_ + 1 \rangle$ the standard model of integers
- $N_2 = \langle \{0, 1\}, 0, \_ + 1(\mathrm{mod} 2) \rangle$
- $N_1 = \langle \{0\}, 0, id \rangle$.

be given. Then

- $in : N \to Z$ with $in(x) = x$ "Embedding Homomorphism"
- $\rho_2 : N \to N_2$ resp. $\rho_2^Z : Z \to N_2$ with $\rho_2(x) = \rho_2^Z(x) = x \bmod 2$
- $\rho_1 : N_2 \to N_1$ with $\rho_1(x) = 0$

are homomorphisms.

Proof Homomorphism condition for $\rho_2 : N \to N_2$:
$\rho_2(\text{zero}^N) = 0 = \text{zero}^{N2}$
$\rho_2(\text{succ}^N(x)) = \rho_2(x + 1) = (x + 1) \bmod 2$
$\text{succ}^{N2}(\rho_2(x)) = \text{succ}^{N2}(x \bmod 2) =$
$((x \bmod 2) + 1) \bmod 2 = (x + 1) \bmod 2$


N
Z
ρ_2
N_2
ρ_2^Z
ρ_1
N_1

Lemma 1 (Σ-Homomorphism)
Let be $\rho : A \to B$ a Σ-homomorphism. Then for any ground term $t \in T(\Sigma)$:

$$\rho(t^A) = t^B$$

Proof :
By structural induction

Example 6 (Non-Existence of Homomorphisms):

1. There is no Nat0-homomorphism $\rho : N_2 \to N$.

   Proof by contradiction
   Assume there is such a homomorphism. Then according to Lemma 1 we would have

$$\rho(\mathsf{succ}(\mathsf{succ}(\mathsf{zero}))^{N_2}) = \mathsf{succ}(\mathsf{succ}(\mathsf{zero}))^{N} = 2, \quad \rho(\mathsf{zero}^{N_2}) = \mathsf{zero}^{N} = 0$$

   and

$$\mathsf{succ}(\mathsf{succ}(\mathsf{zero}))^{N_2} = \mathsf{zero}^{N_2}$$

   thus we obtain a contradiction:

$$2 = \rho(\mathsf{succ}(\mathsf{succ}(\mathsf{zero}))^{N_2}) = \rho(\mathsf{zero}^{N_2}) = 0.$$

   So there is no homomorphism $\rho : N_2 \to N$.

Definition 5 (Initiality):
A Σ-algebra I is called initial in K, if

1. $I \in K$
2. for all $B \in K$ there exists exactly one Σ-homomorphism $\rho : I \to B$.

Example 7 (Initiality):
Let Σ be a sensible signature.

1. The ground term algebra $T(\Sigma)$ is initial in $Alg(\Sigma)$: Let $A \in Alg(\Sigma)$. The family of mappings $eval_s : T(\Sigma)_s \to A_s$ with $eval(t) = t^A$ is a Σ-homomorphism. Because of $eval(f(t_1, \ldots, t_n)) = f^A(eval(t_1), \ldots, eval(t_n))$ $eval$ is a Σ-homomorphism.
2. The standard model $N = \langle \mathbb{N}, 0, \_ + 1 \rangle$ of natural numbers is initial in $Alg(NAT0)$.

$\mathbb{N} =$	0	1	2	$\ldots$
	$\updownarrow$	$\updownarrow$	$\updownarrow$	
	zero	succ(zero)	succ(succ(zero))	

3. Other interpretations of $sig(NAT0)$ like Z, N_2, N_1 are not initial in $Alg(NAT0)$.

Theorem 1 (Equality in initial algebras)
Let $\Sigma = (S, F)$ be a sensible signature, K a class of Σ-algebras and $I \in K$ initial in K. Then for all ground terms $t_1, t_2 \in T(\Sigma)_s$, $s \in S$ the following holds:

$$I \models t_1 = t_2 \qquad \text{iff} \qquad K \models t_1 = t_2$$

Proof Initiality

"$\Rightarrow$" Let $I \models t_1 = t_2$ and $A \in K$. By definition $t_1^I = t_2^I$ holds. As I is initial, there is exactly one Σ-homomorphism $\rho : I \to A$. Thus Lemma 1 implies:

$$t_1^A = \rho(t_1^I) = \rho(t_2^I) = t_2^A$$

"$\Leftarrow$" Let $K \models t_1 = t_2$. Because of $I \in K$ we have $I \models t_1 = t_2$.

Example 8 (SETNATI):
Let SETNATI be following signature:

sig SETNATI =
  sorts Set, Nat
  ops empty : Set
   $\{\_\}$: Nat $\longrightarrow$ Set
   $\_ \cup \_$: Set $\times$ Set $\longrightarrow$ Set
   zero : Nat
   succ : Nat $\longrightarrow$ Nat
end

and let $K \subseteq Alg(\text{SETNATI})$ be the class of algebras, that fulfil following properties:

1. $G \cup (H \cup K) = (G \cup H) \cup K$
2. $G \cup H = H \cup G$
3. $G \cup G = G$
4. $G \cup \text{empty} = G$

Then the algebra of finite sets of natural numbers is initial and satisfies exactly the properties of K.

Lemma 2 (Let K be a class of Σ-algebras and $I \in K$ initial in K.)
If $I' \in K$ is isomorphic to I, then I' is also initial in K.

Proof :
Let $A \in K$ be given. As $I' \in K$ is isomorphic to I there is exactly one Σ-homomorphism $\phi : I' \rightarrow I$.
As I is initial, there is exactly one Σ-homomorphism $\rho : I \rightarrow A$.
So $\rho \circ \phi : I' \rightarrow A$ is a unique Σ-homomorphism from $I^{'} \rightarrow A$.

Definition 6 (Abstract Data Type):
A class K of Σ-algebras is called abstract data type, if K is closed under isomorphism, i.e. if $A \in K$ and B is isomorphic to A, so $B \in K$ as well.

Example 9 (Abstract Data Type):

1. The class of initial algebras of K forms an abstract data type.
2. The stroke number model and the binary number model form two isomorphic elements of the class of initial algebras from NAT0.

Definition 7 (Σ-reachable):
A Σ-algebra A is called Σ-reachable,if every element of A is the interpretation of a ground term, i.e. for all $s \in S$ and $a \in A_s$ there is a ground term $t \in T(\Sigma)$ with $t^A = a$.

Example 10 (Σ-reachable):

1. The standard model $N = (\mathbb{N}, 0, \_ + 1)$ is NAT0-reachable.

$$\begin{array}{cccc} 0 & 1 & 2 & \dots \\ \updownarrow & \updownarrow & \updownarrow & \\ \mathsf{zero}^N & \mathsf{succ}(\mathsf{zero})^N & \mathsf{succ}(\mathsf{succ}(\mathsf{zero}))^N & \dots \end{array}$$

2. N_2 is NAT0-reachable.

$$\begin{array}{cc} 0 & 1 \\ \uparrow & \uparrow \\ \mathsf{zero}^N & \mathsf{succ}(\mathsf{zero})^N \end{array}$$

3. Z is not NAT0-reachable (because there is no surjective NAT0-homomorphism of the term algebra of signature NAT0 to Z).

$$\underbrace{\ldots \quad -2 \qquad -1}_{\text{"junk" (Burstall, Goguen ca. 1980)}} \qquad \begin{matrix} 0 \\ \updownarrow \\ \mathsf{zero}^N \end{matrix} \qquad \begin{matrix} 1 \\ \updownarrow \\ \mathsf{succ}(\mathsf{zero})^N \end{matrix} \qquad \begin{matrix} 2 \\ \updownarrow \\ \mathsf{succ}(\mathsf{succ}(\mathsf{zero}))^N \end{matrix}$$

Lemma 3 (Characterisation of Σ-reachability)
A Σ-algebra A is Σ-reachable, iff there is a surjective Σ-homomorphism from $T(\Sigma)$ to A.

Proof :
Let $\rho : T(\Sigma) \rightarrow A$ be a Σ-homomorphism. Obviously the surjectivity of ρ is equivalent to the reachability of A.

Corollary (Uniqueness of Σ-homomorphism)
Let A be Σ-reachable. Then there is at most one Σ-homomorphism $\rho : A \rightarrow B$ from A to B, which is defined by $\rho(t^A) = t^B$.

Proof :
Let $\rho : A \rightarrow B$ be a Σ-homomorphism. According to Lemma 1, $\rho(t^A) = t^B$ for any ground term t. As A is Σ-reachable, ρ is uniquely defined for all elements of carrier sets of A.

Theorem 2 (Characterisation of Initiality)
Let Σ be a sensible signature, K a class of Σ-algebras, that are characterised by a set E of axioms of the form:

$$\forall x_1 : s_1 \dots x_n : s_n.\ G \qquad \text{G without quantifiers}$$

A Σ-algebra I is initial in K iff

1. E holds in I,
2. I is Σ-reachable,
3. for all ground terms $t_1, t_2 \in T(\Sigma)_s$, $s \in S$ we have:

$$I \models t_1 = t_2 \quad \text{iff} \quad K \models t_1 = t_2$$

Theorem 3 (Existence of initial algebras)
Let Σ be a sensible signature, K a class of Σ-algebras, which is characterised by a set E of conditional equations of the form:

$$u_1 = v_1 \wedge \ldots \wedge u_n = v_n \implies u = v.$$

Then there exists an initial algebra $I \in K$ such that for all ground Σ-terms t_1, t_2

$$I \models t_1 = t_2 \quad \text{iff} \quad E \vdash t_1 = t_2.$$

Theorem 4 (Structural Induction)
Let $\Sigma = (S, C)$, G first order Σ-formula, K be a class of reachable Σ-algebras and $s \in S$. If

1. $K \models G[c/x]$ for all $c \in C_{\epsilon,s}$ ("G holds for all constants") and
2. $K \models \forall y_1 : s_1 \ldots \forall x_1, \ldots, x_n : s.\ G[x_1] \wedge \ldots \wedge G[x_n] \implies G[f(x_1, \ldots, x_n, y_1, \ldots)]$ for all $f \in C_{\langle\langle s,\ldots,s,s_1,..,\rangle s\rangle}$

holds, then: $K \models \forall x : s.\ G[x]$ holds.

Example 11 (Structural Induction):

1. The structural induction schema for natural numbers is:

$$\frac{G(\mathsf{zero}) \qquad \forall x : \mathsf{Nat}.\ G[x] \implies G[\mathsf{succ}(x)]}{\forall x : \mathsf{Nat}.\ G[x]}$$

   (Signature $\mathsf{NAT0} = (\{\mathsf{Nat}\}, \{\mathsf{zero}, \mathsf{succ}\}))$
2. The structural induction schema for boolean values is:

$$\frac{G[\mathsf{true}] \qquad G[\mathsf{false}]}{\forall x : \mathsf{Bool}.\ G[x]}$$

3. The structural induction schema for the sort list of LISTNATI is:

$$\frac{G[\mathsf{nil}] \qquad \forall y : \mathsf{Nat}.\ \forall s : \mathsf{List}.\ G[s] \implies G[\mathsf{cons}(y, s)]}{\forall s : \mathsf{List}.\ G[s]}$$

Notice, that this induction schema does not refer to the function symbols for natural numbers and therefore applies to the signature LIST0:

sig LIST0 =

sorts List, Elem

ops nil : List

cons : Elem $\times$ List $\rightarrow$ List

end

LIST0 is not sensible, because there is no ground term for Elem. Therefore, the notion of initiality can not be used.

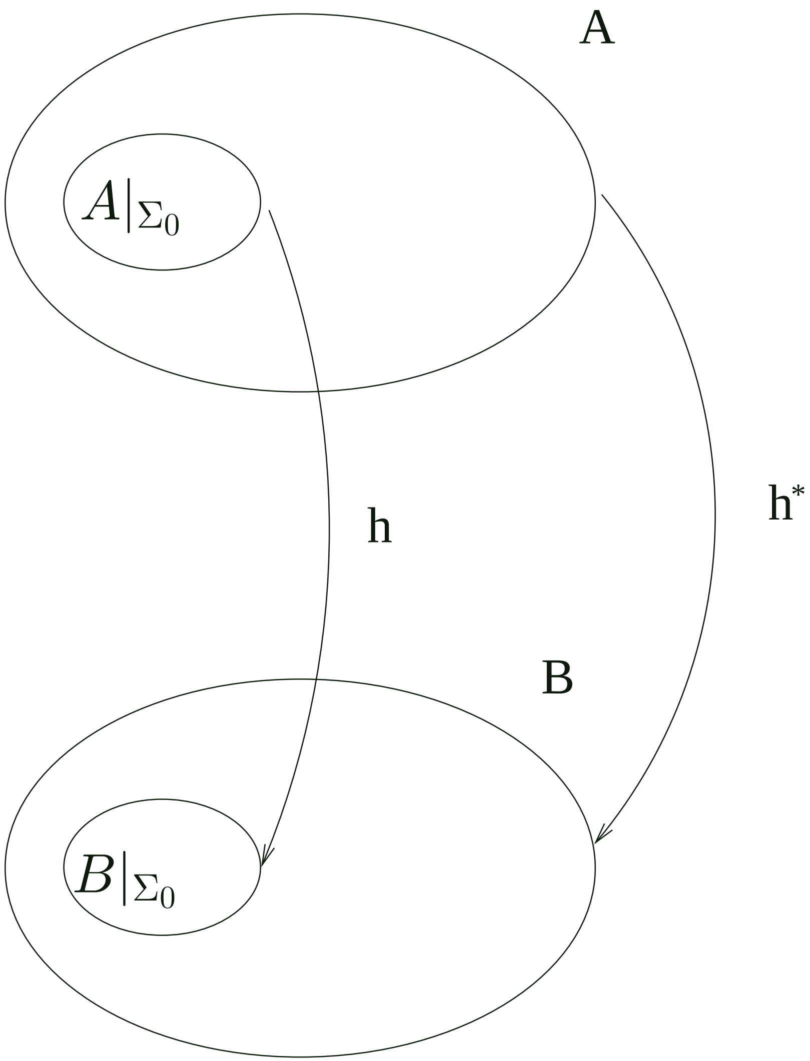
The Generalisation of Initiality: Free Extension

Definition 8 (Free Extension):
Let $\Sigma_0 = (S_0, F_0), \Sigma_1$ be signatures with $\Sigma_0 \subseteq \Sigma_1$.

1. Let A be a Σ_1-algebra. The Σ_0-Reduct $A|_{\Sigma_0}$ of A is constructed by leaving out the sorts and function symbols of A, that do not occur in Σ_0, formally:

$$\begin{array}{rcll} (A|_{\Sigma_0})_s & =_{def} & A_s & \text{for all } s \in S_0 \\ f^{A|_{\Sigma_0}} & =_{def} & f^A & \text{for all } f \in F_0 \end{array}$$

2. Let K be a class of Σ_1-algebras. A is called free extension of $A|_{\Sigma_0}$, if for every $B \in K$ and every Σ_0-homomorphism $h : A|_{\Sigma_0} \to B|_{\Sigma_0}$ there is exactly one Σ_1-homomorphism $h^* : A \to B$ with $h^*|_{\Sigma_0} = h$.


A
$A|_{\Sigma_0}$
h
h*
B
$B|_{\Sigma_0}$

Summary

- Signatures are a formal approach to describe interfaces. A signature consists of sorts, function symbols and predicate symbols.
- Interpretations can be given to interfaces by Σ-algebras and Σ-structures.
- Properties of interfaces resp. structures are described by Σ-formulas. We distinguish propositional logic formulas, equations, conditional equations and general formulas of predicate first order logic.
- In the class of Σ-algebras, initial and reachable algebras are of particular interest. Reachability implies the validity of structural induction. Initiality describes an abstract data type, that fulfils exactly the required equations and is executable.
- The free extension generalizes the initiality theorem for generic data types.