Program Verification: Lecture 11

José Meseguer

Computer Science Department
University of Illinois at Urbana-Champaign

Unsorted Homomorphisms

Given unsorted Σ-algebras $\mathbb{A} = (A, \_\_{}_{\mathbb{A}})$ and $\mathbb{B} = (B, \_\_{}_{\mathbb{B}})$, a Σ-homomorphism h from $\mathbb{A}$ to $\mathbb{B}$, written $h : \mathbb{A} \to \mathbb{B}$, is a function $h : A \to B$ that preserves the operations Σ, i.e.,

- for each constant $a : \epsilon \to s$ in Σ, $h(a_{\mathbb{A}}) = a_{\mathbb{B}}$ (preservation of constants)
- for each $f : s \overset{n}{\ldots} s \to s$ in Σ, $n \geq 1$, and each $(a_1, \ldots, a_n) \in A^n$, we have $h(f_{\mathbb{A}}(a_1, \ldots, a_n)) = f_{\mathbb{B}}(h(a_1), \ldots, h(a_n))$ (preservation of (non-constant) operations).

Example of Unsorted Homomorphism

Ex.11.1. The natural numbers $\mathbb{N}$, and the natural numbers modulo k, $\mathbb{N}_k$ (for any $k \geq 1$) are all $\Sigma_{\texttt{NAT-MIXFIX}}$-algebras (Lecture 3, pages 3–4). Prove in detail that (for any $k \geq 1$) we have a $\Sigma_{\texttt{NAT-PREFIX}}$-homomorphism:

$$res_k : \mathbb{N} \longrightarrow \mathbb{N}_k$$

where res_k sends each number to its residue after dividing by k. For example, $res_7(23) = 2$, and $res_5(23) = 3$.

Note that $\Sigma_{\texttt{NAT-MIXFIX}} = \{0, s, +, *\}$. So you have to prove the $\Sigma_{\texttt{NAT-PREFIX}}$-homomorphism property of res_k for 0 and for the operations $\{s, +, *\}$.

Examples of Unsorted Homomorphisms (II)

Ex.11.2. Recall (Lecture 3, pgs. 6–8) the powerset algebra $\mathbb{P}(A) = (\mathcal{P}(A), \_\mathbb{P}(A))$ over the Boolean signature Σ_{BOOL}. Let A and B be any sets, and let $f : A \longrightarrow B$ be any function. Prove in detail that the function:

$$f^{-1}[\_] : \mathcal{P}(B) \to \mathcal{P}(A)$$

defined for any $B' \subseteq B$ by: $f^{-1}[B'] = \{a \in A \mid f(a) \in B'\}$, is a Σ_{BOOL}-homomorphism $f^{-1}[\_] : \mathbb{P}(B) \to \mathbb{P}(A)$. Consider also a function $g : B \longrightarrow C$. Prove that we have the identity $(f;g)^{-1}[\_] = g^{-1}[\_]; f^{-1}[\_]$, and therefore that $g^{-1}[\_]; f^{-1}[\_] : \mathcal{P}(C) \longrightarrow \mathcal{P}(A)$ is also a Σ_{BOOL}-homomorphism from $\mathbb{P}(C)$ to $\mathbb{P}(A)$.

Many-Sorted Homomorphisms

Given (many-sorted) Σ-algebras $\mathbb{A} = (A, \_\_{\mathbb{A}})$ and $\mathbb{B} = (B, \_\_{\mathbb{B}})$, a Σ-homomorphism h from $\mathbb{A}$ to $\mathbb{B}$, written $h : \mathbb{A} \longrightarrow \mathbb{B}$, is an S-indexed family of functions $h = \{h_s : A_s \to B_s\}_{s \in S}$ such that:

- for each constant $a : \epsilon \to s$, $h_s(a_{\mathbb{A}}^{nil,s}) = a_{\mathbb{B}}^{nil,s}$ (preservation of constants)

- for each $f : w \to s$ with $w = s_1 \ldots s_n$, $n \geq 1$, and each $(a_1, \ldots, a_n) \in A^w$, we have $h_s(f_{\mathbb{A}}^{w,s}(a_1, \ldots, a_n)) = f_{\mathbb{B}}^{w,s}(h_{s_1}(a_1), \ldots, h_{s_n}(a_n))$ (preservation of (non-constant) operations).

Examples of Many-Sorted Homomorphisms

Ex.11.3. Recall the module `NAT-LIST` in Lecture 2, and the two $\Sigma_{\texttt{NAT-LIST}}$-algebras, let us call them $\mathbb{A}$ and $\mathbb{B}$, defined on pages 4–5 of Lecture 4, namely $\mathbb{A}$ = lists of natural numbers and $\mathbb{B}$ = (finite) sets of natural numbers. Show that there cannot be any $\Sigma_{\texttt{NAT-LIST}}$-homomorphim $h : \mathbb{A} \longrightarrow \mathbb{B}$.

Ex.11.4. For Σ the signature in picture 4.1, consider the first family of algebras for it described in point 1, pages 5–6 of Lecture 4, namely n-dimensional vector spaces on the rational, the real, or the complex numbers. Let us be specific and fix the reals. Let $\mathbb{A}$ be the 3-dimensional real vector space, and $\mathbb{B}$ the 2-dimensional real vector space. What is then a Σ-homomorphism $h : \mathbb{A} \longrightarrow \mathbb{B}$? Prove that any such homomorphism h can be completely described by a 2×3 matrix M_h with real coefficients, so that applying to a

3-dimensionsl vector $\vec{v}$ the homomorphims h, that is, computing $h(\vec{v})$ exactly corresponds to computing the matrix multiplication $\vec{v} \circ M_h$. Generalize this to $\mathbb{A}$ and $\mathbb{B}$ real vector spaces of arbitrary finite dimensions n and m. Generalize it further to rational, resp. complex, vector spaces of any pair of finite dimensions n and m.

Now generalize this even further to characterize by means of matrices all Σ-homomorphims between Σ-algebras in cases 2–3 in page 6 of Lecture 4. Give for each of these cases specific examples of $h : \mathbb{A} \longrightarrow \mathbb{B}$ showing how this works and how h is thus applied to specific elements in the corresponding algebra $\mathbb{A}$.

Order-Sorted Homomorphisms

For $\Sigma = ((S, <), F, \Sigma)$ an order-sorted signature, and $\mathbb{A}$ and $\mathbb{B}$ order-sorted Σ-algebras, a Σ-homomorphism h from $\mathbb{A}$ to $\mathbb{B}$, written $h : \mathbb{A} \to \mathbb{B}$, is an S-indexed family of functions $h = \{h_s : A_s \to B_s\}_{s \in S}$ such that:

- $h : \mathbb{A} \to \mathbb{B}$ is a many-sorted (S, F, Σ)-homomorphism; and
- if $[s] = [s']$ and $a \in A_s \cap A_{s'}$, then $h_s(a) = h_{s'}(a)$ (agreement on data in the same connected component)

Examples of Order-Sorted Homomorphisms

Ex.11.5. Consider the order-sorted signature Σ of the `NAT-LIST-II` exampe in Lecture 2, the two algebras on such a signature, let us call them $\mathbb{A}$ and $\mathbb{B}$, defined on page 8 of Lecture 4, with $\mathbb{A}$ case (1), and $\mathbb{B}$ case (2). Show that there is exactly one order-sorted Σ-homomorphim $h : \mathbb{A} \to \mathbb{B}$. Describe such a homomorphism h in complete detail. Show that there cannot be any other Σ-homomorphims $h' : \mathbb{A} \to \mathbb{B}$ with $h \neq h'$.

What is a Pocket Calculator?

Consider a pocket calculator for expressions on the signature $\Sigma = \{0, 1, \_ + \_, \_ * \_\}$, evaluated on the integers $\mathbb{Z} = (\mathbb{Z}, \_\mathbb{Z})$.

Q: What is a pocket calculator as a computable function?

A: A function, say, $\_\mathbb{Z} : T_\Sigma \to \mathbb{Z}$. Call it evaluation in $\mathbb{Z}$.

Q: What is the recursive definition of $\_\mathbb{Z} : T_\Sigma \to \mathbb{Z}$?

A: It is defined by the recursive equations: $0_\mathbb{Z} = 0$, $1_\mathbb{Z} = 1$, $(t + t')_\mathbb{Z} = t_\mathbb{Z} +_\mathbb{Z} t'_\mathbb{Z}$, $(t * t')_\mathbb{Z} = t_\mathbb{Z} *_\mathbb{Z} t'_\mathbb{Z}$.

Q: What is the essential property of the function $\_\mathbb{Z} : T_\Sigma \to \mathbb{Z}$?

A: It is a Σ-homomorphism $\_\mathbb{Z} : \mathbb{T}_\Sigma \to \mathbb{Z}$ because, for example,

$$(0_{\mathbb{T}_\Sigma})_\mathbb{Z} = (0)_\mathbb{Z} = 0_\mathbb{Z} = 0, \qquad (t +_{\mathbb{T}_\Sigma} t')_\mathbb{Z} = (t + t')_\mathbb{Z} = t_\mathbb{Z} +_\mathbb{Z} t'_\mathbb{Z}.$$

What is a Pocket Calculator? (II)

In the same way we also have pocket calculators for the ground terms of $\Sigma = \{0, 1, \_+\_, \_*\_\}$, evaluated on the natural numbers $\mathbb{N} = (\mathbb{N}, \_\mathbb{N})$, the natural numbers modulo $k \geq 1$, $\mathbb{N}_k = (\mathbb{N}_k, \_\mathbb{N}_k)$, or the rational numbers $\mathbb{Q} = (\mathbb{Q}, \_\mathbb{Q})$.

More generally, we shall see shortly, that for Σ a sensible order-sorted signature and any order-sorted Σ-algebra $\mathbb{A} = (A, \_\mathbb{A})$ there is a unique pocket calculator evaluating the terms T_Σ in $\mathbb{A}$, that is, a unique Σ-homomorphism $\_\mathbb{A} : \mathbb{T}_\Sigma \to \mathbb{A}$, defined by the recursive equations:

- $(a)_\mathbb{A} = a_\mathbb{A}$ for each constant a in Σ, and
- $f(t_1, \ldots, t_n)_\mathbb{A} = f_\mathbb{A}(t_{1\mathbb{A}}, \ldots, t_{n\mathbb{A}})$ for each $f : s_1 \ldots s_n \to s$ in Σ.

Term Algebras on Sensible Signatures

If a signature is sensible, then different terms denote different things. In the argot of algebraic specifications, this is expressed by saying that the term algebra $\mathbb{T}_\Sigma$ has no confusion.

Furthermore, the term algebra $\mathbb{T}_\Sigma$ is in some sense minimal, since it has only the elements it needs to have to be an algebra: the constants, and the terms needed so that the operations can yield a result; that is why this minimality is expressed saying that it has no junk.

The key intuition of why there is a unique pocket calculator $\_\_{\mathbb{A}} : \mathbb{T}_\Sigma \to \mathbb{A}$ for any Σ-algebra $\mathbb{A}$, is that: (i) no junk ensures uniqueness of $\_\_{\mathbb{A}}$, and (ii) no confusion ensures the existence of $\_\_{\mathbb{A}}$.

No Pocket Calculators for Term Algebras on Non-sensible Signatures

The intuition that no confusion ensures the existence of $\_{\mathbb{A}} : \mathbb{T}_\Sigma \to \mathbb{A}$ suggests that confusion/ambiguity in $\mathbb{T}_\Sigma$, i.e., Σ non-sensible, will prevent/block the existence of $\_{\mathbb{A}} : \mathbb{T}_\Sigma \to \mathbb{A}$. Let us see an example.

For example, $\_{\mathbb{K}} : \mathbb{T}_\Sigma \to \mathbb{K}$ cannot be defined for Σ the non-sensible signature we showed in pg. 16 of Lecture 4 and the Σ-algebra $\mathbb{K} = (K, \_{\mathbb{K}})$ with: $K_A = \{a\}$, $K_B = \{b\}$, $K_C = \{c\}$, $K_D = \{d, d'\}$, and with $f_{\mathbb{K}}^{A,B}(a) = b$, $f_{\mathbb{K}}^{A,C}(a) = c$, $g_{\mathbb{K}}^{B,D}(b) = d$, and $g_{\mathbb{K}}^{C,D}(c) = d'$. Indeed, there in no Σ-homomorphism $h : \mathbb{T}_\Sigma \longrightarrow \mathbb{K}$ at all, since $h_D(g(f(a))$ must be either d or d'. But if $h_D(g(f(a)) = d$, then h fails to preserve the operation $g : C \longrightarrow D$, and if $h_D(g(f(a)) = d'$, then h fails to preserve the operation $g : B \longrightarrow D$.

Initiality of the Term Algebra $\mathbb{T}_\Sigma$ when Σ Sensible

In summary, the claim is that, if Σ is sensible, then for any Σ-algebra $\mathbb{A}$ there is a unique pocket calculator for $\mathbb{A}$, i.e., a unique Σ-homomorphism $\_{\mathbb{A}} : \mathbb{T}_\Sigma \longrightarrow \mathbb{A}$. This is called the initiality property of $\mathbb{T}_\Sigma$. This unique Σ-homomorphism $\_{\mathbb{A}}$ is the obvious evaluation function, mapping each term t to the result of evaluating it in $\mathbb{A}$. As already mentioned, $\_{\mathbb{A}}$ is defined inductively as follows:

- for a constant a we define $(a)_{\mathbb{A}} = a_{\mathbb{A}}$, and
- for a term $f(t_1, \ldots, t_n)$ we define $(f(t_1, \ldots, t_n))_{\mathbb{A}} = f_{\mathbb{A}}((t_1)_{\mathbb{A}}, \ldots, (t_n)_{\mathbb{A}})$.

Let us prove it in detail.

Theorem. If Σ is a sensible order-sorted signature, then $\mathbb{T}_\Sigma$ satisfies the initiality property.

Proof of the Initiality Theorem

Proof: For $\mathbb{A}$ any Σ-algebra Let us first prove the uniqueness of $\_\_{\mathbb{A}}$, and then its existence.

Proof of uniqueness. Let us suppose that we have two different homomorphisms $h, h' : \mathbb{T}_{\Sigma} \rightarrow \mathbb{A}$. We can prove that $h = h'$ by induction on the depth of the terms.

For terms of depth 0 let a be a constant in $T_{\Sigma,s}$. That means that there is a sort $s' \leq s$ with an operator declaration $a : nil \longrightarrow s'$ and therefore, by h and h' being Σ-homomorphisms we must have $h_s(a) = h'_s(a) = a_{\mathbb{A}}^{nil,s'}$.

Proof of the Initiality Theorem (II)

Assume that the equality $h = h'$ holds for terms of depth less or equal to n, and let $f(t_1, \ldots, t_n) \in T_{\Sigma,s}$ have depth $n+1$. That means that there is an operator declaration $f : s_1 \ldots s_n \to s'$ with $s' \leq s$ and $t_i \in T_{\Sigma,s_i}$, $1 \leq i \leq n$. Again, by h and h' being Σ-homomorphisms we must have:

$h_s(f(t_1, \ldots, t_n)) =$
$= f_{\mathbb{A}}^{s_1 \ldots s_n, s'}(h_{s_1}(t_1), \ldots, h_{s_n}(t_n))$ (h homomorphism and $s' \leq s$)
$= f_{\mathbb{A}}^{s_1 \ldots s_n, s'}(h'_{s_1}(t_1), \ldots, h'_{s_n}(t_n))$ (induction hypothesis)
$= h'_s(f(t_1, \ldots, t_n))$ (h' homomorphism and $s' \leq s$).

Proof of the Initiality Theorem (III)

Proof of Existence. Before defining $\_{\mathbb{A}}$, recall the notation $T_\Sigma^\circ =_{def} \bigcup_{s\in S} T_{\Sigma_s}$. Likewise, for $\mathbb{A} = (A, \_{\mathbb{A}})$ a Σ-algebra define $A^\circ =_{def} \bigcup_{s\in S} A_s$. Recall also from STACS that $[T_\Sigma^\circ \rightharpoonup A^\circ]$ denotes the set of partial functions from T_Σ° to A°. Define the subset $[T_\Sigma^\circ \rightharpoonup A^\circ]_S \subseteq [T_\Sigma^\circ \rightharpoonup A^\circ]$ as follows:

$$[T_\Sigma^\circ \rightharpoonup A^\circ]_S =_{def} \{h \in [T_\Sigma^\circ \rightharpoonup A^\circ] \mid \forall s \in S, \forall t \in T_{\Sigma,s}\ (t,a) \in h \Rightarrow a \in A_s\}$$

that is, $[T_\Sigma^\circ \rightharpoonup A^\circ]_S$ is the subset of sort-preserving partial functions from T_Σ° to A°. One such function in $[T_\Sigma^\circ \rightharpoonup A^\circ]_S$ is:

$$\_{\mathbb{A}}^{0} =_{def} \{(a, a_{\mathbb{A}}) \mid (\epsilon \to a) \in G\}$$

Now define the function:

$$next : [T_\Sigma^\circ \rightharpoonup A^\circ]_S \to [T_\Sigma^\circ \rightharpoonup A^\circ]_S$$

by the lambda expression: $next = \lambda h \in [T_\Sigma^\circ \rightharpoonup A^\circ]_S.\ h \uplus s(h)$, where

Proof of the Initiality Theorem (IV)

$s(h) = \{(f(t_1, \ldots, t_n), f_{\mathbb{A}}(h(t_1), \ldots, h(t_n)) \mid f(t_1, \ldots, t_n) \in T_{\Sigma}^{\circ} \setminus dom(h) \wedge t_i \in dom(h),\ 1 \leq i \leq n\}$

Since in order-sorted algebras overloaded operators agree on common data and Σ is sensible, the result $f_{\mathbb{A}}(h(t_1), \ldots, h(t_n))$ does not depend on the specific typing chosen for f in G and therefore $s(h)$ and $next(h)$ are both indeed partial functions in $[T_{\Sigma}^{\circ} \rightharpoonup A^{\circ}]_S$.

Now define

$$\_^{\circ}_{\mathbb{A}} =_{def} \bigcup_{n \in \mathbb{N}} rec(\_^{0}_{\mathbb{A}}, next)(n)$$

Recall from STACS §6.1, Thm 3, that $rec(\_^{0}_{\mathbb{A}}, next)$ is the function

$$rec(\_^{0}_{\mathbb{A}}, next) : \mathbb{N} \to [T_{\Sigma}^{\circ} \rightharpoonup A^{\circ}]_S$$

defined by simple recursion from $\_^{0}_{\mathbb{A}}$ and $next$. Note that: (i) $\_^{\circ}_{\mathbb{A}}$ is a partial function in $[T_{\Sigma}^{\circ} \rightharpoonup A^{\circ}]$ because $\{rec(\_^{0}_{\mathbb{A}}, next)(n)\}_{n \in \mathbb{N}}$ is a chain in the subset order $\subseteq$ and $[T^{\circ}_{\Sigma} \rightharpoonup A^{\circ}]$ is closed under limits of chains (see STACS §7.5); (ii) furthermore, $\_^{\circ}_{\mathbb{A}}$ belongs to $[T^{\circ}_{\Sigma} \rightharpoonup A^{\circ}]_S$ because for each $n \in \mathbb{N}$, $rec(\_^{0}_{\mathbb{A}}, next)(n)$ does so; and (iii) $\_^{\circ}_{\mathbb{A}}$ is a total function $\_^{\circ}_{\mathbb{A}} : T^{\circ}_{\Sigma} \to A^{\circ}$, since $next(\_^{\circ}_{\mathbb{A}}) = \_^{\circ}_{\mathbb{A}}$.

Now define the S-sorted function:

$$\_{}_{\mathbb{A}} = \{\_^{\circ}_{\mathbb{A}}|_{T_{\Sigma,s}} : T_{\Sigma,s} \to A_s\}_{s \in S}$$

This is our desired Σ-homomorphism $\_{}_{\mathbb{A}} : \mathbb{T}_{\Sigma} \to \mathbb{A}$ because for each $n \in \mathbb{N}$, $rec(\_^{0}_{\mathbb{A}}, next)(n)$ (viewed as an S-sorted partial function) is a partial Σ-homomorphism, i.e., by construction it satisfies the Σ-homomorphism requirements for all terms in $dom(rec(\_^{0}_{\mathbb{A}}, next)(n))$, i.e., for all constants a in Σ and for all $f(t_1, \ldots, t_n) \in T^{\circ}_{\Sigma}$ of tree depth n or less. q.e.d.

The Pocket Calculator of a Canonical Term Algebra

Ex.11.6. Recall the canonical term algebra $\mathbb{C}_{\Sigma/E,B} = (C_{\Sigma/E,B}, \_\_{\mathbb{C}_{\Sigma/E,B}})$, defined in page 17 of Lecture 6 for a functional `fmod` $(\Sigma, E \cup B)$ `endfm`, where Σ is B-preregular and satisfies the Unique Termination, Sufficient Completeness and Sort Preservation requirements.[a] What is the pocket calculator of $\mathbb{C}_{\Sigma/E,B}$?

By the Initiality Theorem, it is the unique Σ-homomorphism $\_\_{\mathbb{C}_{\Sigma/E,B}} : \mathbb{T}_\Sigma \longrightarrow \mathbb{C}_{\Sigma/E,B}$. Prove that, as an S-sorted function on S-sorted sets, $\_\_{\mathbb{C}_{\Sigma/E,B}} : T_\Sigma \rightarrow C_{\Sigma/E,B}$ is exactly the S-sorted function: $\{T_{\Sigma,s} \ni t \mapsto [t!_{E/B}] \in C_{\Sigma/E,B,s}\}_{s \in S}$ (what Maude's `red` command implements!!), which we used in defining $\mathbb{C}_{\Sigma/E,B}$.

[a] Which of course can be checked by checking sort-decreasingness, local confluence and termination of $\vec{E}$ modulo B, and sufficient completeness w.r.t. the constructors Ω.

More on Homomorphisms

Ex.11.7. Prove that homomorphisms compose. That is, if $h : \mathbb{A} \to \mathbb{B}$ and $g : \mathbb{B} \to \mathbb{C}$ are Σ-homomorphisms, then $h; g = \{h_s; g_s\}_{s \in S}$ is a Σ-homomorphism $h; g : \mathbb{A} \to \mathbb{C}$.

Ex.11.8. Prove that identities are homomorphisms. That is, given a Σ-algebra $\mathbb{A} = (A, \_\_{\mathbb{A}})$, the family of identity functions $id_A = \{id_{A_s}\}$ is a Σ-homomorphim $id_A : \mathbb{A} \to \mathbb{A}$.

More on Homomorphisms (II)

A Σ-homomorphim $h : \mathbb{A} \to \mathbb{B}$ is called an isomorphim if there is another Σ-homomorphism $g : \mathbb{B} \to \mathbb{A}$ such that $h; g = id_A$ and $g; h = id_B$. We then may use the notation $g = h^{-1}$ and $h = g^{-1}$.

We call a Σ-homomorphism $h : \mathbb{A} \to \mathbb{B}$

- injective (resp. surjective) if for each sort $s \in S$ the function h_s is injective (resp. surjective)
- a monomorphism if for any pair of Σ-homomorphisms $g, q : \mathbb{C} \to \mathbb{A}$, if $g; h = q; h$ then $g = q$
- an epimorphism if for any pair of Σ-homomorphisms $g, q : \mathbb{B} \to \mathbb{C}$, if $h; g = h; q$ then $g = q$.

More on Homomorphisms (III)

For example, if $\mathbb{N}_{bin}$, resp. $\mathbb{N}_{dec}$, denote the natural numbers with 0, successor, and addition in binary, resp. decimal, representation, we have an obvious binary-to-decimal isomorphism $b2d : \mathbb{N}_{bin} \to \mathbb{N}_{dec}$ preserving all operations, whose inverse is the decimal-to-binary isomorphism, $d2b : \mathbb{N}_{bin} \to \mathbb{N}_{dec}$. Of course, $d2b; b2d = id_{\mathbb{N}_{dec}}$, and $b2d; d2b = id_{\mathbb{N}_{bin}}$.

For $\mathbb{N}_n$ the residue classes modulo n, the reminder function $\mathbb{N} \stackrel{rem_n}{\longrightarrow} \mathbb{N}_n$ is a surjective homomorphism for Σ containing, say, 0, 1, $+$, $\times$.

Similarly, for $\mathbb{Z}_{dec}$ the integers in decimal notation, the inclusion $j : \mathbb{N}_{dec} \hookrightarrow \mathbb{Z}_{dec}$ is an injective homomorphism preserving all shared operations: 0, 1, $+$, $\times$, etc.

Theorem: All Initial Algebras Are Isomorphic

Proof: Suppose $\mathbb{I}$ and $\mathbb{J}$ are Σ-algebras and both satisfy the initiality property of having a unique Σ-homomorphism to any other Σ-algebra. In particular, we have unique homomorphisms,

$$h : \mathbb{I} \longrightarrow \mathbb{J} \qquad g : \mathbb{J} \longrightarrow \mathbb{I}$$

and therefore a composed homomorphism

$$\mathbb{I} \xrightarrow{h} \mathbb{J} \xrightarrow{g} \mathbb{I}$$

but we also have the identity homomorphism $id_{\mathbb{I}}$, which by uniqeness forces $h; g = id_{\mathbb{I}}$. Interchanging the role of $\mathbb{I}$ and $\mathbb{J}$ we also get, $g; h = id_{\mathbb{J}}$. q.e.d.

Exercises

Ex.11.9. Show that a homomorphism is injective iff it is a monomorphism. Prove that every surjective homomorphism is an epimorphism. Construct an epimorphism that is not surjective.

Ex.11.10. Show that any many-sorted Σ-homomorphism that is surjective and injective is an isomorphism.

Construct an order-sorted homomorphism that is surjective and injective but is not an isomorphism. Give a sufficient condition on the poset $(S, \leq)$ (more general of course than being a discrete poset, since that is the many-sorted case) so that h is an isomorphism iff h is surjective and injective.

Exercises (II)

Ex.11.11. Prove that an algebra $\mathbb{J}$ initial iff it is isomorphic to an initial algebra $\mathbb{I}$.

Ex.11.12. Show that the natural numbers in Peano notation (zero and successor) and in base 2 are isomorphic Σ-algebras (both initial) for Σ the signature with one sort `Natural` and zero and successor operations.