SEMINARUL 2 DE PROGRAMARE LOGICA

Claudia Mureşan

Ignorati diferenta dintre literele drepte si literele italice din acest document!

Sa consideram urmatorul modul CafeObj:

mod! NATF{

[Nat]

op 0 : $->$ Nat
ops s f : Nat $->$ Nat
op _<_ : Nat Nat $->$ Bool

vars X Y : Nat

eq 0 $<$ s(X) = true .
eq s(X) $<$ 0 = false .
eq s(X) $<$ s(Y) = X $<$ Y .
eq X $<$ X = false .

eq f(0) = s(0) .
ceq f(X) = s(s(X)) if 0 $<$ X .
}

Desigur, ultima ecuatie din specificatia de mai sus putea fi scrisa ca ecuatie neconditionata sub forma:

eq f(s(X)) = s(s(s(X))) .

Dar, pentru a ilustra tratarea ecuatiilor conditionate in demonstratii de tipul celei de mai jos, am ales sa scriem acea ecuatie conditionata.

Specificatia descrisa este:

- signatura (Σ):
  - sorturile: N, B;

  - operatiile:
    * 0 : → N;
    * true, false : → B;
    * s, f : N → N;
    * < : N N → B;

- ecuatiile (Γ):
  - $(\forall X : N)0 < s(X) = true$;
  - $(\forall X : N)s(X) < 0 = false$;
  - $(\forall X, Y : N)s(X) < s(Y) = X < Y$;
  - $(\forall X : N)X < X = false$;
  - $f(0) = s(0)$;
  - $(\forall X : N)f(X) = s(s(X))$ if $0 < X$.

Vom demonstra ca $\mathcal{N} = (\mathbb{N}, \{true, false\}, 0, true, false, s, f, <)$, unde 0 este primul numar natural, $<$ este relatia de ordine stricta pe $\mathbb{N}$, definita, ca orice relatie, sub forma unei operatii $<: \mathbb{N} \times \mathbb{N} \to \{true, false\}$, care ia valoarea *true* exact pe perechile de numere naturale aflate in aceasta relatie, iar operatiile unare $s, f : \mathbb{N} \to \mathbb{N}$ sunt definite prin: pentru orice $n \in \mathbb{N}$, $s(n) = n+1$ (s este operatia succesor pe $\mathbb{N}$) si $f(n) = \begin{cases} 1, & \text{daca } n = 0, \\ n+2, & \text{daca } n > 0, \end{cases}$ este model initial pentru specificatia de mai sus, adica este $\Gamma-$algebra initiala.

Evident, $\mathcal{N}$ satisface specificatia.

Fie $\mathcal{A} = (A_N, A_B, 0_A, true_A, false_A, s_A, f_A, <_A)$ un alt model pentru aceasta specificatie, adica o alta $\Gamma-$algebra.

Ramane de demonstrat ca exista un unic $\Gamma-$morfism $h : \mathcal{N} \to \mathcal{A}$. Un astfel de morfism este de forma: $h = (h_N, h_B)$, cu $h_N : \mathbb{N} \to A_N$ si $h_B : \{true, false\} \to A_B$.

Unicitatea:

Fie $h, g : \mathcal{N} \to \mathcal{A}$ doua $\Gamma-$morfisme. Rezulta, din comutarea acestor morfisme cu operatiile zeroare: $h_N(0) = 0_A = g_N(0)$, $h_B(true) = true_A = g_B(true)$ si $h_B(false) = false_A = g_B(false)$. Pentru a arata egalitatea lui h cu g, ramane de demonstrat ca, pentru orice $n \in \mathbb{N}^*$, $h_N(n) = g_N(n)$.

Demonstram prin inductie matematica dupa n ca, pentru orice $n \in \mathbb{N}$, $h_N(n) = g_N(n)$.

Pasul de verificare: Conform celor de mai sus, $h_N(0) = g_N(0) = 0_A$.

Pasul de inductie: Presupunem ca $h_N(n) = g_N(n)$ pentru un anumit n natural, arbitrar, fixat.

Folosind definitia lui s, comutarea cu s si ipoteza de inductie, rezulta: $h_N(n+1) = h_N(s(n)) = s_A(h_N(n)) = s_A(g_N(n)) = g_N(s(n)) = g_N(n+1)$.

Asadar, pentru orice $n \in \mathbb{N}$, $h_N(n) = g_N(n)$, deci $h_N = g_N$.

Conform egalitatilor pe operatiile zeroare de sort B, avem $h_B = g_B$.

Prin urmare, $h = g$.

Existenta:

Fie $h : \mathcal{N} \to \mathcal{A}$, definita prin:

$$\begin{cases} h_B(true) = true_A; \\ h_B(false) = false_A; \\ h_N(0) = 0_A; \\ (\forall n \in \mathbb{N}^*) h_N(n) = \underbrace{s_A \circ \ldots \circ s_A}_{\text{de } n \text{ ori } s_A}(0_A). \end{cases}$$

De ce definim pe $h_N(n)$ astfel? Pentru ca trebuie sa avem comutarea lui h cu 0 si cu s, prin urmare trebuie sa avem: pentru orice n natural nenul, $h_N(n) = h_N(\underbrace{s \circ \ldots \circ s}_{\text{de } n \text{ ori } s}(0)) = \underbrace{s_A \circ \ldots \circ s_A}_{\text{de } n \text{ ori } s_A}(h_N(0)) = \underbrace{s_A \circ \ldots \circ s_A}_{\text{de } n \text{ ori } s_A}(0_A)$.

Demonstram ca h astfel definit este $\Gamma-$morfism, adica $\Sigma-$morfism, adica demonstram ca h comuta cu operatiile din signatura Σ.

Conform definitiei sale, h comuta cu operatiile zeroare din Σ.

Demonstram ca h comuta cu s.

Pentru orice $n \in \mathbb{N}$, $h_N(s(n)) = h_N(n+1) = \underbrace{s_A \circ \ldots \circ s_A}_{\text{de } n+1 \text{ ori } s_A}(0_A) = s_A(\underbrace{s_A \circ \ldots \circ s_A}_{\text{de } n \text{ ori } s_A}(0_A)) = s_A(h_N(n))$. Asadar, $h_N \circ s = s_A \circ h_N$, deci h comuta cu s.

Demonstram ca h comuta cu $<$. Avem de aratat ca, pentru orice $n, k \in \mathbb{N}$, $h_B(n < k) = h_N(n) <_A h_N(k)$. Fie, asadar, $n, k \in \mathbb{N}$, arbitrare, fixate. Avem de analizat cazurile: $n < k$, $k < n$ si $n = k$.

Cazul 1: $n < k$. In acest caz, $k - n - 1 \in \mathbb{N}$. Din faptul ca $\mathcal{A}$ verifica ecuatiile din specificatia Γ si din definitia lui h rezulta ca: $h_B(n < k) = h_B(0 < k - n) = h_B(0 < s(k-n-1)) = h_B(true) = true_A = 0_A <_A s_A(h_N(k - n - 1)) = 0_A <_A s_A(\underbrace{s_A \circ \ldots \circ s_A}_{\text{de } k-n-1 \text{ ori } s_A}(0_A)) = 0_A <_A \underbrace{s_A \circ \ldots \circ s_A}_{\text{de } k-n \text{ ori } s_A}(0_A) = s_A(0_A) <_A \underbrace{s_A \circ \ldots \circ s_A}_{\text{de } k-n+1 \text{ ori } s_A}(0_A) = \ldots = \underbrace{s_A \circ \ldots \circ s_A}_{\text{de } n \text{ ori } s_A}(0_A) <_A \underbrace{s_A \circ \ldots \circ s_A}_{\text{de } k \text{ ori } s_A}(0_A) = h_N(n) <_A h_N(k)$.

Cazul 2: $k < n$. Analog cazului 1.

Cazul 3: $n = k$. Atunci: $h_B(n < k) = h_B(n < n) = h_B(false) = false_A = h_N(n) <_A h_N(n) = h_N(n) <_A h_N(k)$. Am folosit faptul ca $\mathcal{A}$ verifica ecuatiile din specificatia Γ.

Asadar, h comuta si cu $<$.

Ramane de demonstrat ca h comuta cu f. Adica avem de demonstrat ca $h_N \circ f = f_A \circ h_N$, i. e., pentru orice $n \in \mathbb{N}$, $h_N(f(n)) = f_A(h_N(n))$.

$h_N(f(0)) = h_N(s(0)) = s_A(h_N(0)) = s_A(0_A) = f_A(0_A) = f_A(h_N(0))$, conform comutarii lui h cu s, definitiei lui h in 0 si faptului ca $\mathcal{A}$ verifica ecuatiile din specificatia Γ.

Fie $n \in \mathbb{N}^*$.

Sa ne amintim din curs faptul ca $\mathcal{A}$ satisface ecuatia $(\forall X : N) f(X) = s(s(X))$ if $0 < X$ daca si numai daca, pentru orice $x \in A_N$, daca $0_A <_A x = true_A$, atunci $f_A(x) = s_A(s_A(x))$ (observati ca acest fapt este echivalent cu definitia cu morfismul de la $\Sigma-$algebra libera generata de X la $\mathcal{A}$, pentru ca un astfel de morfism duce pe 0 din $\Sigma-$algebra libera generata de X in 0_A si comuta cu $<$; mai precis, conform definitiei, $\mathcal{A}$ satisface ecuatia $(\forall X : N) f(X) = s(s(X))$ if $0 < X$ daca si numai daca, oricare ar fi $\Sigma-$morfismul $\alpha : T_\Sigma(X) \to \mathcal{A}$, daca $\alpha_B(0 < X) = true_A$, atunci $\alpha_N(f(X)) = \alpha_N(s(s(X)))$, adica, oricare ar fi $\Sigma-$morfismul $\alpha : T_\Sigma(X) \to \mathcal{A}$, daca $0_A <_A \alpha_N(X) = true_A$, atunci $f_A(\alpha_N(X)) = s_A(s_A(\alpha_N(X)))$, si acum notam $x = \alpha_N(X) \in A_N$).

Avem ca $0 < n$, prin urmare: $h_N(f(n)) = h_N(s(s(n))) = s_A(s_A(h_N(n))) = f_A(h_N(n))$, pentru ca h comuta cu s, $\mathcal{A}$ satisface Γ si $0_A <_A h_N(n) = h_N(0) <_A h_N(n) = h_B(0 < n) = h_B(true) = true_A$, datorita definitiei lui h in 0 si $true$ si comutarii lui h cu $<$, care a fost deja demonstrata.

Deci h comuta si cu f.

Rezulta ca h este $\Gamma-$morfism.

Rezulta ca exista un unic $\Gamma-$morfism $h : \mathcal{N} \to \mathcal{A}$, prin urmare $\mathcal{N}$ este $\Gamma-$algebra initiala, adica obiect initial in categoria $\Gamma-$algebrelor, adica model initial pentru specificatia Γ.