8 SPRE ABSTRACTIZAREA TIPURILOR DE DATE

Virgil Emil Căzănescu

March 22, 2008

1 Ecuaţii

Să analizăm conceptul de axiomă aşa cum apare el în algebră. De exemplu comutativitatea şi asociativitatea se scriu

$$(\forall x \forall y) x?y = y?x \qquad (\forall x \forall y \forall z) x?(y?z) = (x?y)?z.$$

Ce sunt acestea? Sunt egalităţi de două expresii cuantificate universal prin mulţimea variabilelor conţinute în cele două expresii. Deci o astfel de axiomă are forma

$$(\forall X) l \doteq r$$

unde l şi r sunt din algebra liber generată de mulţimea X de variabile.

Ce înseamnă că o axiomă este adevărată într-o algebră $\mathcal{D}$? Intuitiv este necesar ca rezultatul evaluării celor două expresii l şi r în algebra $\mathcal{D}$ să fie acelaşi indiferent de valorile date în $\mathcal{D}$ variabilelor din X. Această idee intuitivă conduce la:

Definiţia 1.1 Axioma $(\forall X) l \doteq r$ este satisfăcută în algebra $\mathcal{D}$ dacă şi numai dacă pentru orice morfism $h : T_\Sigma(X) \longrightarrow \mathcal{D}$ este adevărată egalitatea $h(l) = h(r)$.

În continuare vom folosi pentru $(\forall X) l \doteq r$ termenul de *ecuaţie* în locul celui de axiomă, pentru a ne conforma cu terminologia internaţională.

În plus vor intra în joc şi aşa zisele *ecuaţii condiţionate*. De exemplu

$$(\forall x \forall y \forall z)(x * y = x * z \Rightarrow y = z)$$

ceea ce corespunde axiomei de simplificare la stânga care este adevărată în orice grup sau în orice monoid liber.

2 Ecuaţii condiţionate

În logica ecuaţională o axiomă este o implicaţie

$$a_1 = c_1, a_2 = c_2, \ldots, a_n = c_n \Rightarrow a = c$$

unde ipoteza este o conjuncţie de egalităţi formale şi concluzia o egalitate formală. Toată implicaţia este cuantificată universal, fapt care nu apare scris mai sus. În acest cadru o axiomă, numită în continuare şi ecuaţie condiţionată a logicii ecuaţionale, poate fi scrisă sub forma

$$(\forall X)\ a \doteq_s c \ \textbf{if}\ H$$

unde a şi c sunt elemente de acelaşi sort s, iar H este o mulţime **finită** de egalităţi formale din algebra liber generată de mulţimea X de variabile. Ipoteza implicaţiei este dată de mulţimea H.

Pentru a verifica dacă o algebră $\mathcal{D}$ satisface axioma de mai sus se dau valori arbitrare variabilelor din X în $\mathcal{D}$ fapt ce poate fi făcut printr-o funcţie arbitrară $f : X \longrightarrow \mathcal{D}$ sau echivalent printr-un morfism arbitrar $h : T_\Sigma(X) \longrightarrow \mathcal{D}$. Apoi se evaluează expresiile din H pentru a se verifica dacă rezultatul evaluarii conduce la egalităţi adevărate, caz în care trebuie ca $h_s(a) = h_s(c)$. Deci Σ-algebra $\mathcal{D}$ satisface ecuaţia condiţionată $(\forall X) a \doteq_s c$ **if** H fapt notat prin

$$\mathcal{D} \models_\Sigma (\forall X)\ a \doteq_s c \ \textbf{if}\ H$$

dacă şi numai dacă

$$(\forall h : T_\Sigma(X) \longrightarrow \mathcal{D})\ (\forall u =_t v \in H) h_t(u) = h_t(v) \text{ implică } h_s(a) = h_s(c).$$

Credem că este bine să menţionăm diferenţa esenţială între semnele $\doteq_s$ şi $=$, diferenţă care va fi menţinută constant pe parcursul întregului text. Egalul peste care s-a pus un punct ($\doteq_s$) indică o egalitate formală care poate fi adevărată sau falsă. Egalul $=$ are semnificaţia uzuală indicând deobicei o egalitate adevărată.

3 Necesitatea utilizării cuantificatorilor în ecuaţii

Vom ilustra printr-un exemplu necesitatea utilizării cuantificatorilor în ecuaţiile logicii ecuaţionale multisortate.

Fie signatura $S = \{a, bool\}$ şi $\Sigma = \{g, F, T\}$. Rangurile simbolurilor de operaţii sunt date prin desenul următor :

$$a \xrightarrow{g} bool \underset{T}{\overset{F}{\leftleftarrows}} .$$

Vom lucra cu două Σ–algebre.

Σ–algebra iniţială este $\mathcal{I} = (\emptyset, \{F, T\}, I_g, I_F, I_T)$ unde $F \neq T$, $I_F = F$, $I_T = T$ şi $I_g : \emptyset \longrightarrow \{F, T\}$ este funcţia incluziune.

Pentru orice variabilă x de sort a, Σ-algebra liber generată de această variabilă $T_\Sigma(\{x\}, \emptyset)$ are suporturile $\{x\}$ şi {g(x),F,T}.

Are loc relaţia $\mathcal{I} \models_\Sigma F = T$? Sau mai intuitiv: este egalitatea $F = T$ adevărată în algebra $\mathcal{I}$? Vom arăta că raspunsul depinde de algebra liberă în care este scrisă egalitatea.

Sunt posibile cel puţin două variante.

1. $\mathcal{I} \models_\Sigma (\forall\emptyset)T = F \quad \Leftrightarrow \quad \forall h : \mathcal{I} \longrightarrow \mathcal{I}$ morfism, $h_{bool}(F) = h_{bool}(T)$,
   ceea ce este *fals* deoarece $h_{bool}(F) = F \neq T = h_{bool}(T)$.

2. $\mathcal{I} \models_\Sigma (\forall x)T = F \quad \Leftrightarrow \quad \forall h : T_\Sigma(\{x\}, \emptyset) \longrightarrow \mathcal{I}$ morfism, $h_{bool}(F) = h_{bool}(T)$,
   ceea ce este *adevărat* deoarece nu există nici un morfism $h : T_\Sigma(\{x\}, \emptyset) \longrightarrow \mathcal{I}$.

Am arătat că $\mathcal{I} \models_\Sigma (\forall\emptyset)T = F$ este falsă şi că $\mathcal{I} \models_\Sigma (\forall x)T = F$ este adevărată. Dacă omitem cuantificatorii obţinem: "$\mathcal{I} \models_\Sigma T = F$ este falsă şi $\mathcal{I} \models_\Sigma T = F$ este adevărată."

Contradicţia obţinută prin omiterea cuantificatorilor din faţa egalităţii $F = T$ arată că în logica ecuaţională multisortată prezenţa cuantificatorilor în ecuaţii este necesară.

4 In primul rând semantica

Pentru orice algebră $\mathcal{D} = (D_s, D_\sigma)$ notăm cu

$$Sen(\mathcal{D}) = \{a \doteq_s c : s \in S,\ a, c \in D_s\}$$

mulţimea *propoziţiilor* sale. Propoziţiile sunt de fapt egalităţi formale care pot fi adevărate sau false.

Să observăm că $Sen(\mathcal{D})$ se poate identifica cu produsul cartezian $D \times D$. Poate cea mai bună reprezentare a unei propoziţii din $\mathcal{D}$ este un triplet format dintr-un sort s si două elemente de sort s din $\mathcal{D}$.

Definiţia 4.1 O *ecuaţie condiţionată* este

$$(\forall X)l \doteq_s r \textbf{ if } H$$

unde X este o mulţime S-sortată de variabile, l şi r sunt două elemente de sort s din $T_\Sigma(X)$ iar H o mulţime **finită** de egalităţi formale din $T_\Sigma(X)$. $\square$

O ecuaţie condiţionată în care $H = \emptyset$ devine necondiţionată şi este numită pe scurt *ecuaţie*. În acest caz scriem doar $(\forall X)l \doteq_s r$ în loc de $(\forall X)l \doteq_s r$ **if** $\emptyset$.

Definiţia 4.2 Algebra $\mathcal{D}$ *satisface* ecuaţia condiţionată $(\forall X)l \doteq_s r$ **if** H, fapt notat prin

$$\mathcal{D} \models_\Sigma (\forall X)l \doteq_s r \textbf{ if } H$$

dacă pentru orice morfism $h : T_\Sigma(X) \longrightarrow \mathcal{D}$ pentru care $h_{s'}(u) = h_{s'}(v)$ pentru orice $u \doteq_{s'} v \in H$, avem $h_s(l) = h_s(r)$. $\square$

În cele ce urmează indicele Σ din $\models_\Sigma$ va fi omis. El va fi menţionat atunci când este pericol de confuzie.

Observăm că $\mathcal{D} \models (\forall X)l \doteq_s r$ dacă şi numai dacă $h_s(l) = h_s(r)$ pentru orice morfism $h\colon T_\Sigma(X) \longrightarrow \mathcal{D}$.

În continuare fixăm o mulţime Γ de ecuaţii condiţionate, numite axiome.

Definiţia 4.3 Spunem că algebra $\mathcal{D}$ satisface Γ sau că $\mathcal{D}$ e o Γ-algebră şi scriem $\mathcal{D} \models \Gamma$ dacă $\mathcal{D}$ satisface toate ecuaţiile condiţionate din Γ.

Un morfism de Σ-algebre între două Γ-algebre se numeşte morfism de Γ-algebre sau mai scurt Γ-morfism. $\square$

5 Punctul de vedere local

Fixăm o algebră $\mathcal{A}$ şi lucrăm cu propoziţii din $Sen(\mathcal{A})$. Acesta este punctul *local* de vedere al logicii ecuaţionale. Cazul în care ne interesează propoziţii din algebre diferite este numit *global* dar va fi puţin folosit în acest curs. În cazul global o propoziţie din $\mathcal{D}$ va fi scrisă $(\forall \mathcal{D})a \doteq_s c$ în loc de $a \doteq_s c$. Notaţia fără cuantificatori folosită în cazul local nu contrazice ceea ce am scris despre necesitatea utilizării cuantificatorilor în ecuaţii. Pur si simplu nu scriem cuantificatorul pentru că fixând algebra $\mathcal{A}$ el va fi mereu acelaşi $(\forall \mathcal{A})$ şi deci îl ştim chiar dacă nu-l vedem scris.

O altă idee pe care dorim să o subliniem este folosirea unei algebre arbitrare $\mathcal{A}$ în locul unei algebre libere. Principalele rezultate privind rescrierile, care se referă atât la rescrierile de termeni cât şi la rescrierile modulo ecuaţii, rămân valabile în acest cadru mai general. Aceasta prezentare unitară a diverselor tipuri de rescriere este de fapt contribuţia autorului la modernizarea lecţiilor despre rescriere. Există în lume trei cărţi privind rescrieriile. Cea mai veche este Term Rewriting and All That, scrisă de Franz Baader şi Tobias Nipkow.

Menţionăm că algebra $\mathcal{A}$ nu are legătură cu algebra $T_\Sigma(X)$ folosită în vreo axiomă $(\forall X)l =_s r$ **if** H din Γ. Menţionăm şi că în axiome diferite putem folosi algebre libere diferite. Aceasta corespunde cazului practic, de exemplu scriem comutativitatea $xy = yx$ într-o algebră liberă cu doi generatori x şi y iar asociativitatea $(xy)z = x(yz)$ într-o algebră liberă cu trei generatori x, y şi z.

6 Semantică şi Corectitudine

Vom lucra într-o Σ-algebră $\mathcal{A}$. Vom grupa într-o relaţie toate tautologiile(propoziţiile valide) din algebră ale logicii ecuaţionale.

Fie $\equiv_\Gamma^\mathcal{A}$ relaţia pe A definită prin

$$a \equiv_\Gamma^\mathcal{A} c \text{ dacă şi numai dacă } (\forall h : \mathcal{A} \longrightarrow \mathcal{M} \models \Gamma)h_s(a) = h_s(c).$$

Dacă nu există pericol de confuzie vom prefera să scriem $\equiv_\Gamma$ în loc de $\equiv_\Gamma^\mathcal{A}$.

Observăm că

$$\equiv_\Gamma = \bigcap\{Ker(h) \mid h : \mathcal{A} \longrightarrow \mathcal{M} \models \Gamma\}.$$

Deoarece nucleul unui morfism este o relaţie de congruenţă şi deoarece orice intersecţie de relaţii de congruenţe este o relaţie de congruenţă, deducem că $\equiv_\Gamma$ este o relaţie de congruenţă.

$\equiv_\Gamma$ este numită **congruenţă semantică.**

Definim regula de deducţie a substituţiei utilizată atât în logica ecuaţională cât şi în rescrierea termenilor.

Sub$_\Gamma$ Pentru orice $(\forall X)\, l \doteq_s r$ **if** $H \in \Gamma$ şi orice morfism $h\colon T_\Sigma(X) \longrightarrow \mathcal{A}$
$(\forall u \doteq_{s'} v \in H)h_{s'}(u) \doteq_{s'} h_{s'}(v)$ implică $h_s(l) \doteq_s h_s(r)$.

Lemă 6.1 *Pentru orice morfism* $f : \mathcal{A} \longrightarrow \mathcal{M} \models \Gamma$*,* $Ker(f)$ *este închis la* **Sub**$_\Gamma$.

Demonstraţie: Fie $(\forall X)l \doteq_s r$ **if** H în Γ şi $h : T_\Sigma(X) \longrightarrow \mathcal{A}$ un morfism cu proprietatea că $h_t(u)\ Ker(f)\ h_t(v)$ pentru orice $u \doteq_t v \in H$. Prin urmare $(h; f)_t(u) = (h; f)_t(v)$ pentru orice $u \doteq v \in H$. Deoarece $h; f\colon T_\Sigma(X) \longrightarrow \mathcal{M} \models \Gamma$ rezultă că $(h; f)_s(l) = (h; f)_s(r)$, deci $h_s(l)\ Ker(f)\ h_s(r)$.□

Propoziţie 6.2 *Congruenţă semantică este închisă la substituţie.*

Demonstraţie: Congruenţa semantică este o intersecţie de congruenţe închise la substituţie. Deoarece o intersecţie de congruenţe închise la substituţii este o congruenţă închisă la substituţii rezultă că $\equiv_\Gamma$ este o congruenţă închisă la substituţie. □

Propoziţie 6.3 *Dacă* $\sim$ *este o congruenţă închisă la substituţii, atunci* $\mathcal{A}/\!\sim\ \models \Gamma$.

Demonstraţie: Notăm cu $\rho : \mathcal{A} \longrightarrow \mathcal{A}/\!\sim$ morfismul de factorizare canonic.

Fie $(\forall X)l \doteq_s r$ **if** H în Γ şi $h : T_\Sigma(X) \longrightarrow \mathcal{A}/\!\sim$ un morfism astfel încât $h_t(u) = h_t(v)$ pentru orice $u \doteq_t v \in H$. Cum $T_\Sigma(X)$ este algebră proiectivă există un morfism $f : T_\Sigma(X) \longrightarrow \mathcal{A}$ astfel încât $f; \rho = h$. Pentru orice $u \doteq_t v \in H$ deoarece $\rho_t(f_t(u)) = \rho_t(f_t(v))$ deducem $f_t(u) \sim f_t(v)$.

Deoarece $\sim$ este o congruenţă închisă la substituţii obţinem $f_s(l) \sim f_s(r)$. Prin urmare $\rho_s(f_s(l)) = \rho_s(f_s(r))$, de unde $h_s(l) = h_s(r)$. □

Fie $\mathcal{A}_\Gamma$ factorizarea lui $\mathcal{A}$ prin congruenţa $\equiv_\Gamma$ şi fie $\eta\colon \mathcal{A} \longrightarrow \mathcal{A}_\Gamma$ morfismul cât.

Teorema 6.4 $\mathcal{A}_\Gamma \models \Gamma$

Demonstraţie: Se aplică propoziţiile 6.2 şi 6.3. $\Box$

Teorema 6.5 *Pentru orice* Γ*-algebră* $\mathcal{B}$ *şi pentru orice morfism* $h\colon \mathcal{A} \longrightarrow \mathcal{B}$ *există şi este unic un morfism* $h^\# : \mathcal{A}_\Gamma \longrightarrow \mathcal{B}$ *astfel încât* $\eta; h^\# = h$.

Demonstraţie: Este suficient să arătăm că $a \equiv_\Gamma c$ implică $h(a) = h(c)$ şi aplicăm proprietatea de universalitate a algebrei cât. Într-adevăr $a \equiv_\Gamma c$ implică $h(a) = h(c)$ deoarece $h\colon \mathcal{A} \longrightarrow \mathcal{B} \models \Gamma$. $\Box$

Corolar 6.6 *Dacă* $\mathcal{A}$ *este* Σ*-algebră iniţială, atunci* $\mathcal{A}_\Gamma$ *este* Γ*-algebră iniţială.*

Corolar 6.7 *Pentru orice signatură* Σ *şi pentru orice mulţime* Γ *de ecuaţii condiţionate există o* Γ*-algebră iniţială.*

Propoziţie 6.8 *Fie* $h : \mathcal{A} \longrightarrow \mathcal{B}$ *un morfism. Dacă* $a \equiv_\Gamma^{\mathcal{A}} c$*, atunci* $h(a) \equiv_\Gamma^{\mathcal{B}} h(c)$.

Demonstraţie: Fie $f : \mathcal{B} \longrightarrow \mathcal{C} \models \Gamma$. Din $a \equiv_\Gamma^{\mathcal{A}} c$ folosind morfismul $h; f : \mathcal{A} \longrightarrow \mathcal{C} \models \Gamma$ deducem $(h; f)(a) = (h; f)(c)$, prin urmare $f(h(a)) = f(h(c))$. Deci $h(a) \equiv_\Gamma^{\mathcal{B}} h(c)$.

7 Problema programării prin rescriere

Principala problemă este : "poate o maşină să demonstreze că $a \equiv_\Gamma c$*?".*

Se ştie că în unele cazuri rescrierile ne dau o soluţie.

8 Tipuri abstracte de date

Am văzut în lecţiile precedente că orice signatură determină prin algebra sa iniţială un tip abstract de date. Tipul abstract de date al numerelor naturale a fost determinat de signatura formată din constanta 0 şi operaţia unară cunoscută sub numele de succesor.

Acum am pus în evidenţă un instrument mai puternic deoarece orice signatură împreună cu o mulţime Γ de ecuaţii condiţionate determină prin Γ-algebra iniţială, a cărei existenţă am dovedit-o mai sus, un tip abstract de date.

8.1 Tipul abstract al numerelor naturale - continuare

Considerăm signatura cu un singur sort *nat*, o singură constantă de sort nat şi o singură operaţie unară cu argument şi rezultat de sort nat:

sort nat .
op 0 : $\longrightarrow$ nat .
op s : nat $\longrightarrow$ nat .

Elementele algebrei iniţiale sunt

0, s(0), s(s(0)), s(s(s(0))), s(s(s(s(0)))), ...

şi ele reprezintă numerele naturale 0 1 2 3 4 ...

Propoziţie 8.1 *Algebra* $(N, 0_N, s_N)$ *definită prin:* N *este mulţimea numerelor naturale,* 0_N *este numărul natural zero şi* $s_N(n) = n + 1$ *pentru orice număr natural* n*; este iniţială.*

Propoziţia anterioară ne arată cum pot fi definite numerele naturale prim metoda algebrei iniţiale ca tip abstract de date.

Deocamdată prin signatura de mai sus calculatorul învaţă numerele naturale dar nu ştie încă să calculeze. Să-l învăţăm să adune şi să înmulţească. La cele de mai sus adăugăm.

op _+_ : nat nat $\longrightarrow$ nat .
var X Y : nat .
eq X + 0 = 0 .

eq X + s(Y) = s(X+Y) .
op _*_ : nat nat ⟶ nat .
eq X * 0 = 0 .
eq X * s(Y) = X*Y + X .

Trebuie să menţionăm că egalităţiile de mai sus sunt folosite în două moduri:
a) ca ecuaţii care împreună cu signatura de patru operaţii formează o mulţime Γ pentru a defini o structură algebrică şi
b) ca reguli de rescriere în timpul execuţiei programelor.

Propoziţie 8.2 *Algebra* $\mathcal{N} = (N, 0_N, s_N, +_N, *_N)$ *este* Γ*-algebră iniţială.*

Demonstraţie: Fie $\mathcal{A} = (A, O_A, s_A, +_A, *_A)$ o Γ-algebră. Menţionăm că algebra $\mathcal{A}$ satisfac ecuaţiile din Γ, adică

1) $a +_A 0_A = a$ pentru orice a din A,
2) $a +_A s_A(b) = s_A(a + b)$ pentru orice a, b din A,
3) $a *_A 0_A = 0_A$ pentru orice a din A,
4) $a *_A s_A(b) = a *_A b +_A a$ pentru orice a, b din A.

Vom proba că există un unic morfism de Γ-algebre de la $\mathcal{N}$ la $\mathcal{A}$.
Să începem cu unicitatea. Dacă $h : \mathcal{N} \longrightarrow \mathcal{A}$ este un Γ-morfism, atunci $h : (N, 0_N, s_N) \longrightarrow (A, 0_A, s_A)$ este morfism prin urmare coincide cu unicul morfism dat de propoziţia de mai sus.
Pentru a demonstra existenţa nu avem decât o singură şansă şi anume să dovedim că unicul morfism $h : (N, 0_N, s_N) \longrightarrow (A, 0_A, s_A)$ este şi morfism de Γ-algebre. Reamintim că

$$h(0_N) = 0_A \text{ şi pentru orice } n \text{ număr natural } h(n+1) = s_A(h(n)).$$

Probăm că $h(n +_N m) = h(n) +_A h(m)$ prin inducţie după m

$h(n +_N 0_N) = h(n) = h(n) +_A 0_A = h(n) +_A h(0_N)$ şi
$h(n +_N (m+1)) = h(s_N(n +_N m)) = s_A(h(n +_N m)) = s_A(h(n) +_A h(m)) = h(n) +_A s_A(h(m)) = h(n) +_A h(m+1)$.

Probăm că $h(n *_N m) = h(n) *_A h(m)$ prin inducţie după m

$h(n *_N 0_N) = h(0_N) = 0_A = h(n) *_A 0_A = h(n) *_A h(0_N)$ şi
$h(n *_N (m+1)) = h(n *_N m +_N n) = h(n *_N m) +_A h(n) = (h(n) *_A h(m)) +_A h(n) = h(n) *_A s_A(h(m)) = h(n) *_A h(m+1)$. $\square$

Propoziţia anterioară demonstrează corectitudinea definiţiei de mai sus. Deoarece algebra $\mathcal{N}$ este iniţială rezultă că ea este izomorfă cu Γ-algebra iniţială, deci specificaţia de mai sus caracterizează prin Γ-algebra sa iniţială tipul de date al numerelor naturale.