

Fundamentele limbajelor de programare

CURS 5

Andrei Sipoș¹

Facultatea de Matematică și Informatică, DL Info, Anul II

¹Curs realizat împreună cu Traian Florin Șerbănuță.

Programare logică

În anul I, la disciplina „Logică matematică și computațională”, s-au studiat, pe de o parte, logica de ordinul I ca teorie matematică, iar, pe de alta, programarea logică din punct de vedere practic, sub forma limbajului Prolog. Asemănările dintre sintaxa limbajului și logica studiată la cursuri și seminare au fost evidențiate doar la modul intuitiv.

În continuare, vom arăta cum funcționarea acestui limbaj de programare poate fi modelată teoretic, extinzând teoria deja dezvoltată pentru logica de ordinul I. Vom recapitula, dintre lucrurile deja studiate din logică, pe cele care ne vor folosi acum, eventual introducând notații noi.

Vom fixa patru obiecte $\perp, \rightarrow, \forall, =$, diferite două câte două și o mulțime numărabilă (de **variabile logice**)

$$V = \{x_0, x_1, \dots\},$$

cu $V \cap \{\perp, \rightarrow, \forall, =\} = \emptyset$.

Signaturi și structuri

Definim o **signatură de ordinul I** ca fiind un triplet $\sigma = (F, R, r)$ astfel încât $F \cap R = \emptyset$, $(F \cup R) \cap (V \cup \{\perp, \rightarrow, \forall, =\}) = \emptyset$ și $r : F \cup R \rightarrow \mathbb{N}$.

Dacă $\sigma = (F, R, r)$ este o signatură de ordinul I, atunci numim elementele lui R **simbolurile de relație** ale lui σ , iar elementele lui F **simbolurile de funcție** ale lui σ ; pentru orice $s \in F \cup R$, numim $r(s)$ **aritatea** lui s ; în particular, acele $s \in F$ pentru care $r(s) = 0$ se numesc **constantele** lui σ . Mai definim și mulțimea

$$S_\sigma := \{\perp, \rightarrow, \forall, =\} \cup V \cup F \cup R.$$

Dacă $\sigma = (F, R, r)$ este o signatură de ordinul I, atunci o σ -**structură** va fi o pereche $(A, \{A_s\}_{s \in F \cup R})$, unde $A \neq \emptyset$ (și se va numi **universul**, **mulțimea suport** sau **mulțimea subiacentă** a structurii), pentru orice $s \in F$, $A_s : A^{r(s)} \rightarrow A$ și pentru orice $s \in R$, $A_s \subseteq A^{r(s)}$. Structurile vor reprezenta domeniile despre care vor vorbi formulele corespunzătoare signaturilor.

Exemple

Putem obține diverse semnături dacă punem $\sigma := (F, R, r)$, iar F , R , r sunt, pe rând:

- $F = \{\cdot, 0, 1\}$, $R = \emptyset$, $r(\cdot) = 2$, $r(0) = r(1) = 0$ – atunci σ -structurile vor fi tuplurile $(A, \cdot, 0, 1)$ unde $\cdot : A^2 \rightarrow A$, iar $0, 1 \in A$, de exemplu $(\mathbb{Z}, +, 2, 7)$. Observăm că nu impunem în definiția structurii ca ea să respecte anumite legi – acest lucru se va face eventual ulterior, după ce vom defini riguros formulele și satisfacerea lor.
- $F = \emptyset$, $R = \{\leq\}$, $r(\leq) = 2$ – atunci σ -structurile vor fi perechi $(A, \leq)$ unde $\leq$ este o relație binară pe A , de exemplu $(\mathbb{N}, >)$.
- $F = \emptyset$, $R = \{I, A, B\}$, $r(I) = r(A) = r(B) = 1$.

Dacă punem $F = R = \emptyset$, atunci obținem o semnătură care, dat fiind că singurele fapte pe care le vom putea exprima peste ea vor folosi semnul $=$, se va numi **semnătura egalității**.

De asemenea, vom defini **signatura aritmeticii** ca fiind

$$\sigma_{\text{ar}} := (\{\dot{+}, \dot{\times}, \dot{S}, \dot{0}\}, \{\dot{<}\}, r),$$

unde $r(\dot{+}) = r(\dot{\times}) = r(\dot{<}) = 2$, $r(\dot{S}) = 1$, iar $r(\dot{0}) = 0$. Dacă definim funcția $S : \mathbb{N} \rightarrow \mathbb{N}$, pentru orice $n \in \mathbb{N}$, prin $S(n) := n + 1$, iar

$$\mathcal{N} := (\mathbb{N}, (N_s)_{s \in F \cup R}),$$

unde $N_{\dot{+}} = +$, $N_{\dot{\times}} = \cdot$, $N_{\dot{S}} = S$, $N_{\dot{0}} = 0$, iar $N_{\dot{<}} = <$, avem că $\mathcal{N}$ este o σ_{ar} -structură.

De remarcat că există și alte σ_{ar} -structuri, de exemplu putem înzestra mulțimea $\{0, 1\}$ cu $\wedge$, $\vee$, $\neg$, 0 și $<$ pentru a obține o altă σ_{ar} -structură.

Formulele corespunzătoare unei semnături $\sigma = (F, R, r)$ vor fi cuvinte peste alfabetul S_σ . Înainte de a defini formulele, va trebui să definim **termenii**. Ei se definesc ca fiind cea mai mică mulțime A de șiruri de simboluri din S_σ astfel încât:

- $V \subseteq A$;
- pentru orice $s \in F$ și orice $t_1, \dots, t_{r(s)} \in A$, avem $st_1 \dots t_{r(s)} \in A$ (în particular, dacă $r(s) = 0$, $s \in A$).

Mulțimea termenilor peste σ se va nota cu T_σ .

Inducție și recursie pe termeni

Principiul inducției pe termeni

Fie $B \subseteq T_\sigma$ astfel încât:

- $V \subseteq B$;
- pentru orice $s \in F$ și orice $t_1, \dots, t_{r(s)} \in B$, avem $st_1 \dots t_{r(s)} \in B$.

Atunci $B = T_\sigma$.

Principiul recursiei pe termeni

Fie A o mulțime și $G_0 : V \rightarrow A$, iar pentru orice $s \in F$, $G_s : A^{r(s)} \rightarrow A$. Atunci există și este unică $F : T_\sigma \rightarrow A$ astfel încât:

- pentru orice $x \in V$, $F(x) = G_0(x)$;
- pentru orice $s \in F$ și orice $t_1, \dots, t_{r(s)} \in T_\sigma$,
 $F(st_1 \dots t_{r(s)}) = G_s(F(t_1), \dots, F(t_{r(s)}))$.

Mulțimea variabilelor unui termen

Ca exemplu, putem defini recursiv mulțimea variabilelor unui termen. Practic, definim funcția $Var : T_\sigma \rightarrow \mathcal{P}(V)$, prin:

- pentru orice $x \in V$, $Var(x) := \{x\}$;
- pentru orice $s \in F$ și orice $t_1, \dots, t_{r(s)} \in T_\sigma$,
 $Var(st_1 \dots t_{r(s)}) := Var(t_1) \cup \dots \cup Var(t_{r(s)})$ (în particular, dacă $r(s) = 0$, $Var(s) = \emptyset$).

Notăm cu $\tilde{T}_\sigma$ mulțimea termenilor fără variabile.

Fie $\mathcal{A} = (A, (A_s)_{s \in FUR})$ o σ -structură. Atunci pentru orice $v : V \rightarrow A$ există și este unică o funcție $(\cdot)_v^{\mathcal{A}} : T_\sigma \rightarrow A$ astfel încât

- pentru orice $x \in V$, $x_v^{\mathcal{A}} = v(x)$;
- pentru orice $s \in F$ și orice $t_1, \dots, t_{r(s)} \in T_\sigma$,
 $(st_1 \dots t_{r(s)})_v^{\mathcal{A}} = A_s((t_1)_v^{\mathcal{A}}, \dots, (t_{r(s)})_v^{\mathcal{A}})$ (în particular, dacă $r(s) = 0$, $s_v^{\mathcal{A}} = A_s$).

Atenție, din nou: funcția v din definiția de mai sus **nu** are un rol similar cu cel al funcțiilor $e : Q \rightarrow 2$ din logica propozițională, cu toate că ar putea părea astfel.

Fie $\sigma = (F, R, r)$ o semnătură. Numim **formulă atomică** peste σ un șir de forma $=tu$, cu $t, u \in T_\sigma$ (numită formulă atomică **ecuațională** sau doar **ecuație**) sau un șir de forma $st_1 \dots t_n$ cu $s \in R$, $n = r(s)$ și $t_1, \dots, t_n \in T_\sigma$ (numită formulă atomică **relațională**). Mulțimea formulelor atomice peste σ se va nota cu Fa_σ . Mulțimea **formulelor** peste σ se definește ca fiind cea mai mică mulțime A de șiruri de simboluri din S_σ astfel încât:

- formulele atomice aparțin lui A ;
- $\perp \in A$;
- dacă $\varphi, \psi \in A$, atunci $\rightarrow \varphi\psi \in A$;
- dacă $\varphi \in A$ și $x \in V$, atunci $\forall x\varphi \in A$.

Mulțimea formulelor peste σ se va nota cu F_σ .

De asemenea, vom defini **formulele relaționale** în același mod, cu excepția că acceptăm în cadrul lor doar formule atomice relaționale.

Notăție infixată și conectori derivați

Vom folosi aceeași metodă pe care am folosit-o la logica propozițională pentru a putea nota formulele infixat – pentru orice $\varphi, \psi \in F_\sigma$, $\varphi \rightarrow \psi$ în loc de $\rightarrow \varphi \psi$, dar și, pentru orice $t, u \in T_\sigma$, $t = u$ în loc de $= tu$.

De asemenea, vom nota, ca mai înainte, pentru orice $\varphi, \psi \in F_\sigma$,

$$\top := \perp \rightarrow \perp, \quad \neg\varphi := \varphi \rightarrow \perp, \quad \varphi \wedge \psi := \neg(\varphi \rightarrow \neg\psi),$$

$$\varphi \vee \psi := (\neg\varphi) \rightarrow \psi, \quad \varphi \leftrightarrow \psi := (\varphi \rightarrow \psi) \wedge (\psi \rightarrow \varphi).$$

dar și, pentru orice $x \in V$ și $\varphi \in F_\sigma$,

$$\exists x\varphi := \neg\forall x\neg\varphi.$$

Principiul inducției pe formule

Fie $B \subseteq F_\sigma$ astfel încât:

- formulele atomice aparțin lui B ;
- $\perp \in B$;
- dacă $\varphi, \psi \in B$, atunci $\varphi \rightarrow \psi \in B$;
- dacă $\varphi \in B$ și $x \in V$, atunci $\forall x \varphi \in B$.

Atunci $B = F_\sigma$.

Principiul recursiei pe formule

Fie A o mulțime și $G_0 : Fa_\sigma \rightarrow A$, $G_\perp \in A$, $G_\rightarrow : A^2 \rightarrow A$, $G_\forall : V \times A \rightarrow A$. Atunci există și este unică $F : F_\sigma \rightarrow A$ astfel încât:

- pentru orice $\varphi \in Fa_\sigma$, $F(\varphi) = G_0(\varphi)$;
- $F(\perp) = G_\perp$;
- pentru orice $\varphi, \psi \in F_\sigma$, $F(\varphi \rightarrow \psi) = G_\rightarrow(F(\varphi), F(\psi))$;
- pentru orice $\varphi \in F_\sigma$ și $x \in V$, $F(\forall x \varphi) = G_\forall(x, F(\varphi))$.

Mulțimea variabilelor libere ale unei formule

Ca exemplu, putem defini recursiv mulțimea variabilelor **libere** ale unei formule. Definim funcția $FV : F_\sigma \rightarrow \mathcal{P}(V)$, prin:

- pentru orice $t, u \in T_\sigma$, $FV(t = u) := Var(t) \cup Var(u)$;
- pentru orice $s \in R$ și orice $t_1, \dots, t_{r(s)} \in T_\sigma$,
 $FV(st_1 \dots t_{r(s)}) := Var(t_1) \cup \dots \cup Var(t_{r(s)})$;
- $FV(\perp) := \emptyset$;
- pentru orice $\varphi, \psi \in F_\sigma$, $FV(\varphi \rightarrow \psi) := FV(\varphi) \cup FV(\psi)$;
- pentru orice $\varphi \in F_\sigma$ și $x \in V$, $FV(\forall x \varphi) := FV(\varphi) \setminus \{x\}$.

Dacă $\varphi \in F_\sigma$ cu $FV(\varphi) = \emptyset$, atunci φ se numește **enunț**.

Mulțimea enunțurilor peste σ se notează cu E_σ .

Spre evaluarea formulelor

Fie $\mathcal{A} = (A, (A_s)_{s \in \text{FUR}})$ o σ -structură. Pentru orice $v : V \rightarrow A$, $x \in V$, $a \in A$, definim $v_{x \leftarrow a} : V \rightarrow A$, pentru orice $y \in V$, prin

$$v_{x \leftarrow a}(y) := \begin{cases} v(y), & \text{dacă } y \neq x, \\ a, & \text{dacă } y = x. \end{cases}$$

Observăm că pentru orice variabile x, y cu $x \neq y$, orice $v : V \rightarrow A$ și orice $a, b \in A$, avem că

$$(v_{y \leftarrow b})_{x \leftarrow a} = (v_{x \leftarrow a})_{y \leftarrow b}.$$

În acest caz, notăm valoarea lor comună cu $v_{x \leftarrow a, y \leftarrow b}$. Așadar, pentru orice $z \in V$,

$$v_{x \leftarrow a, y \leftarrow b}(z) = \begin{cases} v(z) & \text{dacă } z \neq x \text{ și } z \neq y, \\ a & \text{dacă } z = x, \\ b & \text{dacă } z = y. \end{cases}$$

Avem că există și este unică o funcție $\|\cdot\|^{\mathcal{A}} : F_{\sigma} \rightarrow \{0, 1\}^{A^V}$ astfel încât, pentru orice $v : V \rightarrow A$, avem:

- pentru orice $t, u \in T_{\sigma}$, $\|t = u\|_v^{\mathcal{A}} = 1 \Leftrightarrow t_v^{\mathcal{A}} = u_v^{\mathcal{A}}$;
- pentru orice $s \in R$ și orice $t_1, \dots, t_{r(s)} \in T_{\sigma}$,
 $\|st_1 \dots t_{r(s)}\|_v^{\mathcal{A}} = 1 \Leftrightarrow ((t_1)_v^{\mathcal{A}}, \dots, (t_{r(s)})_v^{\mathcal{A}}) \in A_s$;
- $\|\perp\|_v^{\mathcal{A}} = \perp = 0$;
- pentru orice $\varphi, \psi \in F_{\sigma}$, $\|\varphi \rightarrow \psi\|_v^{\mathcal{A}} = \|\varphi\|_v^{\mathcal{A}} \rightarrow \|\psi\|_v^{\mathcal{A}}$;
- pentru orice $\varphi \in F_{\sigma}$ și $x \in V$,
 $\|\forall x \varphi\|_v^{\mathcal{A}} = 1 \Leftrightarrow$ pentru orice $a \in A$, $\|\varphi\|_{v_{x \leftarrow a}}^{\mathcal{A}} = 1$.

Dacă $\varphi \in F_{\sigma}$ este astfel încât pentru orice $\mathcal{A}$ și v , $\|\varphi\|_v^{\mathcal{A}} = 1$, spunem că φ este **validă**.

Fie $\mathcal{A} = (A, (A_s)_{s \in \text{FUR}})$ o σ -structură. Este acum imediat că pentru orice $v : V \rightarrow A$, avem:

- $\|\top\|_v^{\mathcal{A}} = \top = 1$;
- pentru orice $\varphi, \psi \in F_\sigma$, $\|\varphi \wedge \psi\|_v^{\mathcal{A}} = \|\varphi\|_v^{\mathcal{A}} \wedge \|\psi\|_v^{\mathcal{A}}$;
- pentru orice $\varphi, \psi \in F_\sigma$, $\|\varphi \vee \psi\|_v^{\mathcal{A}} = \|\varphi\|_v^{\mathcal{A}} \vee \|\psi\|_v^{\mathcal{A}}$;
- pentru orice $\varphi, \psi \in F_\sigma$, $\|\varphi \leftrightarrow \psi\|_v^{\mathcal{A}} = \|\varphi\|_v^{\mathcal{A}} \leftrightarrow \|\psi\|_v^{\mathcal{A}}$;
- pentru orice $\varphi \in F_\sigma$ și $x \in V$,
 $\|\exists x \varphi\|_v^{\mathcal{A}} = 1 \Leftrightarrow \text{există } a \in A \text{ cu } \|\varphi\|_{v_{x \leftarrow a}}^{\mathcal{A}} = 1$.

Așadar, dacă $\mathcal{A} = (A, (A_s)_{s \in \text{FUR}})$ este o σ -structură și φ este enunț, pentru orice $v_1, v_2 : V \rightarrow A$, avem $\|\varphi\|_{v_1}^{\mathcal{A}} = \|\varphi\|_{v_2}^{\mathcal{A}}$, deci este echivalent faptul că pentru orice $v : V \rightarrow A$, $\|\varphi\|_v^{\mathcal{A}} = 1$ cu faptul că există $v : V \rightarrow A$ cu $\|\varphi\|_v^{\mathcal{A}} = 1$. Numim această stare de fapt cu

$$\mathcal{A} \models \varphi$$

și spunem că $\mathcal{A}$ **satisface** φ sau că $\mathcal{A}$ este **model** pentru φ .

Iată, deci, că structurile de ordinul I reprezintă analogul funcțiilor de evaluare întâlnite în logica propozițională. De aici provine și numele acelei ramuri a logicii care studiază structurile de ordinul I în conjuncție cu enunțurile satisfăcute de ele: **teoria modelelor**.

Semnul $\models$ în logica de ordinul I

Vom defini următoarele concepte, precum și noi semnificații ale semnelui $\models$, prin analogie cu logica propozițională:

- Dacă $\varphi \in E_\sigma$ și φ este valid, vom scrie $\models \varphi$.
- Spunem că $\varphi \in E_\sigma$ este **satisfiabil** dacă există $\mathcal{A}$ cu $\mathcal{A} \models \varphi$.
- Spunem că un enunț φ este **nesatisfiabil** dacă φ nu este satisfiabil.
- Fie $\varphi, \psi \in E_\sigma$. Spunem că din φ **se deduce semantic** ψ și scriem $\varphi \models \psi$ dacă pentru orice $\mathcal{A}$ cu $\mathcal{A} \models \varphi$ avem $\mathcal{A} \models \psi$.

Clar, $\perp$ este enunț, iar pentru orice σ -structură $\mathcal{A}$, avem $\mathcal{A} \not\models \perp$, i.e. $\perp$ este nesatisfiabil.

Complet analog celor din logica propozițională, vom introduce noțiuni de satisfiabilitate pentru mulțimi de formule, precum și semnificații corespunzătoare ale semnului $\models$.

Fie $\Gamma \subseteq E_\sigma$. Pentru orice σ -structură $\mathcal{A}$, spunem că $\mathcal{A}$ **satisfacă** Γ sau că $\mathcal{A}$ este **model** pentru Γ , și scriem $\mathcal{A} \models \Gamma$, dacă pentru orice $\varphi \in \Gamma$, $\mathcal{A} \models \varphi$.

Spunem că Γ este **satisfiabilă** dacă există o σ -structură $\mathcal{A}$ cu $\mathcal{A} \models \Gamma$; că este **nesatisfiabilă** dacă nu este satisfiabilă.

Următoarele proprietăți se demonstrează perfect analog celor din logica propozițională.

Proprietăți

Fie $\Gamma \subseteq E_\sigma$, $\Delta \subseteq \Gamma$ și $\mathcal{A}$ o σ -structură. Avem următoarele:

- Dacă $\mathcal{A} \models \Gamma$, atunci $\mathcal{A} \models \Delta$.
- Dacă Δ este nesatisfiabilă, atunci Γ este nesatisfiabilă.
- Avem că $\mathcal{A} \models \Gamma$ dacă și numai dacă pentru orice $\Sigma \subseteq \Gamma$ finită, $\mathcal{A} \models \Sigma$.

Deducție semantică din mulțimi

Fie $\Gamma \subseteq E_\sigma$ și $\varphi \in E_\sigma$. Spunem că din Γ **se deduce semantic** φ , și scriem $\Gamma \models \varphi$, dacă pentru orice σ -structură $\mathcal{A}$ cu $\mathcal{A} \models \Gamma$ avem $\mathcal{A} \models \varphi$. Această noțiune are următoarele proprietăți analoge celor din logica propozițională și demonstrabile similar.

Proprietăți

Fie $\Gamma \subseteq E_\sigma$, $\Delta \subseteq \Gamma$ și $\varphi, \psi \in E_\sigma$. Avem următoarele:

- Dacă $\Delta \models \varphi$, atunci $\Gamma \models \varphi$.
- Mulțimea Γ este nesatisfiabilă dacă și numai dacă $\Gamma \models \perp$.
- Avem $\Gamma \models \varphi$ dacă și numai dacă $\Gamma \cup \{\neg\varphi\}$ este nesatisfiabilă.

Vom numi **substituție** o funcție $\theta : V \rightarrow T_\sigma$. Folosind Principiul de recursie pe termeni, ea se extinde natural în mod unic la o funcție $\tilde{\theta} : T_\sigma \rightarrow T_\sigma$.

Se observă, folosind unicitatea, că, pentru orice două substituții θ, θ' ,

$$\widetilde{\theta' \circ \theta} = \tilde{\theta'} \circ \tilde{\theta}.$$

Dacă avem o formulă φ , $n \in \mathbb{N}$ și $k_1 < \dots < k_n$ cu $FV(\varphi) = \{x_{k_1}, \dots, x_{k_n}\}$, notăm cu $\forall \varphi$ enunțul $\forall x_{k_1} \dots \forall x_{k_n} \varphi$.

Numim **literal** o formulă de forma φ sau $\neg \varphi$, unde φ este o formulă atomică relațională (literalul este, respectiv, **pozitiv** sau **negativ**). Numim **clauză** o formulă de forma $\forall(L_1 \vee \dots \vee L_m)$, unde $L_1, \dots, L_m$ sunt literali. Numim **clauză definită** o clauză unde apare exact un literal pozitiv, anume pe prima poziție. Dacă $A_0, \dots, A_m$ sunt formule atomice relaționale, atunci clauza

$$\forall(A_0 \vee \neg A_1 \vee \dots \vee \neg A_m)$$

se scrie și sub forma (cunoscută din limbajul Prolog)

$$A_0 \leftarrow A_1, \dots, A_m.$$

Un **program** va fi o mulțime finită de clauze definite. Un **scop definit** este o clauză în care apar doar literalii negativi.

Să zicem că avem un program Prolog care conține regula

$$p(f(x), y) \leftarrow p(x, y)$$

și vrem să interogăm $p(z, f(t))$. Pentru a găsi o soluție a acestei interogări folosind regula de mai sus, trebuie să substituim $x \mapsto z$, $z \mapsto f(x)$, $y \mapsto f(t)$, $t \mapsto t$, interogarea devenind $p(f(x), f(t))$, care este redusă, conform regulii, la $p(x, f(t))$, care devine practic o nouă interogare.

Observăm că o parte esențială a procesului de rulare a unui program Prolog (pe care îl vom studia data viitoare, când vom vedea exact care este legătura dintre regulile/interogările afișate mai sus și teoria prezentată astăzi) este găsirea acelei substituții. Acest procedeu se va numi **unificare**.

Unificatori

Dacă $\mathcal{E}$ este o mulțime de ecuații, numim **unificator** pentru ea o substituție θ astfel încât, pentru orice $(s = t) \in \mathcal{E}$, avem $\tilde{\theta}(s) = \tilde{\theta}(t)$; el se numește **cel mai general unificator (cgu; most general unifier, mgu)** dacă, pentru orice unificator θ' pentru $\mathcal{E}$, avem că există o substituție ω cu $\theta' = \tilde{\omega} \circ \theta$.

Propoziție

Fie $n \in \mathbb{N}$, $z_1, \dots, z_n \in V$ (diferite două câte două) și $t_1, \dots, t_n \in T_\sigma$ astfel încât, pentru orice i, j , $z_i \notin \text{Var}(t_j)$. Atunci substituția θ care duce, pentru orice i , z_i în t_i este cgu pentru $\{z_i = t_i \mid i \in \{1, \dots, n\}\}$.

Demonstrație

Faptul că este unificator este evident. Fie acum θ' un unificator. Vrem ω cu $\theta' = \tilde{\omega} \circ \theta$. Luăm $\omega := \theta'$. Avem, într-adevăr, că, pentru orice i , $(\tilde{\theta}' \circ \theta)(z_i) = \tilde{\theta}'(t_i) = \tilde{\theta}'(z_i) = \theta'(z_i)$ și, pentru orice altă variabilă y , $(\tilde{\theta}' \circ \theta)(y) = \tilde{\theta}'(y) = \theta'(y)$.

Algoritm de unificare

Vom descrie acum un algoritm de unificare. El are ca intrare o mulțime de ecuații $\mathcal{E}$, iar la ieșire, un cgu dat de o mulțime de ecuații ca în propoziția precedentă, sau „eșec”, dacă un cgu nu există. Algoritmul trece printr-un ciclu care, la fiecare pas, verifică dacă există vreo ecuație în mulțime căruia i se poate aplica vreuna dintre următoarele operații – în caz contrar, el se oprește:

- o ecuație de forma $f(s_1, \dots, s_n) = f(t_1, \dots, t_n)$ este înlocuită de ecuațiile $s_1 = t_1, \dots, s_n = t_n$;
- o ecuație de forma $f(s_1, \dots, s_n) = g(t_1, \dots, t_m)$, unde $f \neq g$, produce „eșec”;
- o ecuație de forma $x = x$, cu $x \in V$, este eliminată;
- o ecuație de forma $t = x$ cu $x \in V$ și $t \notin V$ este înlocuită cu $x = t$;
- o ecuație de forma $x = t$ cu $x \in V$, $t \neq x$ și $x \in \text{Var}(t)$ produce „eșec”;
- o ecuație de forma $x = t$ cu $x \in V$, $t \neq x$, $x \notin \text{Var}(t)$, dar cu x apărând și în alte ecuații din mulțime, face ca toate celelalte sale apariții să fie substituite cu t .

Teoremă

Algoritmul de unificare prezentat se termină mereu și produce rezultatul corect.

Demonstrație

Pentru terminare, observăm că doar ultimul pas crește numărul de simboluri, dar acela poate fi aplicat doar o dată pentru fiecare variabilă.

Pentru corectitudine, observăm întâi că mulțimile care produc „eșec” nu au unificator și că, atunci când algoritmul se termină, mulțimea are exact forma din propoziția precedentă (numită **formă rezolvată**). Apoi, trebuie să arătăm că la fiecare pas, mulțimea rezultantă are aceiași unificatori ca cea precedentă. Tratăm ultimul caz doar. Notând cu ψ substituția $x \mapsto t$, avem că ecuațiile $s = u$ care nu sunt $x = t$ sunt înlocuite de $\tilde{\psi}(s) = \tilde{\psi}(u)$.

Demonstrație (cont.)

Fie θ un unificator pentru mulțimea inițială, în particular $\theta(x) = \tilde{\theta}(t)$. Fie $s = u$ o ecuație din ea care nu este $x = t$. Vrem $\tilde{\theta}(\tilde{\psi}(s)) = \tilde{\theta}(\tilde{\psi}(u))$. Se arată ușor că $\tilde{\theta} \circ \psi = \theta$, de unde rezultă concluzia.

Fie acum θ un unificator pentru mulțimea rezultată, în particular (din nou) $\theta(x) = \tilde{\theta}(t)$. Se arată, din nou, ușor, că $\tilde{\theta} \circ \psi = \theta$, iar concluzia rezultă analog, scriind egalitățile invers.