Logică pentru informatică - Săptămâna 14
Rezoluția pentru LP1

Rezoluția pentru LP1 este o optimizare a rezoluției de bază pe care am studiat-o în cursul precedent, fiind o metodă de demonstrare a nesatisfiabilității unei formule de ordinul I aflată în FNSC. Avantajul rezoluției (față de rezoluția de bază) este că nu este necesară alegerea "convenabilă" a unor substituții de bază, ci alegerea este făcută mecanic, printr-o metodă inventată de Robinson în anii 1960 numită unificare; așadar este mai ușor pretabilă spre a fi mecanizată (implementată într-un program pe calculator).

1 Unificare

Definiția 1.1 (Unificator)**.** *O substituție σ este unificator al termenilor t_1 și t_2 dacă $\sigma^\sharp(t_1) = \sigma^\sharp(t_2)$.*

Exemplul 1.1. *Fie termenii $t_1 = f(x, h(y))$ și $t_2 = f(h(z), z')$. Un unificator pentru t_1 și t_2 este:*

$$\sigma = \{z \mapsto a, x \mapsto h(a), z' \mapsto h(y)\} \qquad (\sigma^\sharp(t_1) = f(h(a), h(y)) = \sigma^\sharp(t_2)).$$

Un alt unificator al celor doi termeni este:

$$\sigma_1 = \{x \mapsto h(z), z' \mapsto h(y)\} \qquad (\sigma_1^\sharp(t_1) = f(h(z), h(y)) = \sigma_1^\sharp(t_2)).$$

Definiția 1.2 (Termeni unificabili)**.** *Doi termeni sunt* unificabili *dacă au cel puțin un unificator.*

Exemplul 1.2. *Termenii $t_1 = f(x, y)$ și $t_2 = h(z)$ nu au unificator, deci nu sunt unificabili. De ce?*

Pentru orice substituție σ avem $\sigma^\sharp(t_1) = \sigma^\sharp(f(x, y)) = f(\sigma^\sharp(x), \sigma^\sharp(y)) \neq h(\sigma^\sharp(z)) = \sigma^\sharp(h(z)) = \sigma^\sharp(t_2)$.

Termenii $t_1 = x$ și $t_2 = h(x)$ nu au unificator. De ce?

Să presupunem că ar exista un unificator al lor, σ. Din moment ce $\sigma^\sharp(t_1) = \sigma^\sharp(t_2)$, înseamnă că arborii abstracti corespunzatori termenilor $\sigma^\sharp(t_1)$ și $\sigma^\sharp(t_2)$ au același număr de noduri. Notăm cu $noduri(t)$ numărul de noduri ale arborelui corespunzator unui termen t.

Avem că noduri$(\sigma^\sharp(t_2))$ = *noduri*$(\sigma^\sharp(h(x)))$ = 1 + *noduri*$(\sigma^\sharp(x))$ = 1 + *noduri*$(\sigma^\sharp(t_1))$ > *noduri*$(\sigma^\sharp(t_1))$*, ceea ce reprezintă o contradicție, deoarece trebuia să avem noduri*$(\sigma^\sharp(t_2))$ = *noduri*$(\sigma^\sharp(t_1))$*. Prin urmare, presupusul unificator* σ *nu există.*

Definiția 1.3 (Compunerea a două substituții)**.** *Fie* σ_1, σ_2 *două substituții. Substituția* $\sigma_2 \circ \sigma_1 : \mathcal{X} \to \mathcal{T}$*, denumită* compunerea substituțiilor σ_1 și σ_2*, este definită astfel:*

- $(\sigma_2 \circ \sigma_1)(x) = \sigma_2^\sharp(\sigma_1(x))$*, pentru orice* $x \in \mathcal{X}$*.*

Exercițiul 1.1. *Verificați că funcția* $\sigma_2 \circ \sigma_1$ *este într-adevăr o substituție (adică că mulțimea acelor variabile* x *cu proprietatea că* $(\sigma_2 \circ \sigma_1)(x) \neq x$ *este finită).*

Exemplul 1.3. *Continuând exemplul anterior, fie substituțiile* $\sigma = \{z \mapsto a, x \mapsto h(a), z' \mapsto h(y)\}$*,* $\sigma_1 = \{x \mapsto h(z), z' \mapsto h(y)\}$ *și respectiv* $\sigma_2 = \{z \mapsto a\}$*. Avem că* $\sigma = \sigma_2 \circ \sigma_1$*.*

Exercițiul 1.2. *Arătați că într-adevăr substituțiile* σ *și respectiv* $\sigma_2 \circ \sigma_1$ *sunt egale (au același rezultat pentru orice variabilă).*

Definiția 1.4 (Substituție mai generală)**.** *O substituție* σ_1 *este mai generală decât o substituție* σ *dacă* σ *se poate obține prin compunerea substituției* σ_1 *cu o altă substituție* σ_2*:* $\sigma = \sigma_2 \circ \sigma_1$*.*

Exemplul 1.4. *De exemplu,* $\sigma_1 = \{x \mapsto h(z), z' \mapsto h(y)\}$ *este mai generală decât* $\{z \mapsto a, x \mapsto h(a), z' \mapsto h(y)\}$*, deoarece* $\sigma = \sigma_2 \circ \sigma_1$*, unde* σ_2 *este definită în exemplul de mai sus.*

Definiția 1.5 (Cel mai general unificator)**.** *O substituție* σ *este* cel mai general unificator al termenilor t_1 și t_2 *dacă:*

1. σ *este unificator al termenilor* t_1, t_2 *și*
2. σ *este o substituție mai generală decât orice unificator al* t_1, t_2*.*

Exemplul 1.5. *Fie* $t_1 = f(x, a)$ *și* $t_2 = f(y, a)$*. Unificatorul* $\{y \mapsto x\}$ *este mai general decât* $\{x \mapsto a, y \mapsto a\}$*.*

Exemplul 1.6. *Substituția* $\sigma_1 = \{x \mapsto h(z), z' \mapsto h(y)\}$ *este cel mai general unificator al termenilor* $t_1 = f(x, h(y))$ *și* $t_2 = f(h(z), z')$*.*

Teorema 1.1 (Teorema existenței celui mai general unificator)**.** *Orice doi termeni unificabili au un cel mai general unificator.*

Observația 1.1. *În general, cel mai general unificator nu este unic.*

Exemplul 1.7. *Un unificator pentru termenii* $h(x)$ *și* $h(y)$ *este substituția* $\{x \mapsto a, y \mapsto a\}$ *(dar nu este cel mai general unificator).*

Un cel mai general unificator este $\{x \mapsto y\}$*. Un alt cel mai general unificator este* $\{y \mapsto x\}$*.*

În continuare, vom prezenta un algoritm pentru calculul unui cel mai general unificator.

În acest scop, avem nevoie de generalizarea noțiunii de unificare pentru mai multe perechi de termeni.

Definiția 1.6 (Problemă de unificare)**.** *O* problemă de unificare P *este:*

- *sau o mulțime*
$$P = \{t_1 \doteq t'_1, \ldots, t_n \doteq t'_n\}$$
formată din n perechi de termeni
- *sau simbolul special*
$$P = \perp \text{ (\textit{citit} bottom).}$$

Definiția 1.7 (Soluție a unei probleme de unificare)**.** *O substituție σ este o* soluție *a unei probleme de unificare P dacă:*

1. *problema este de forma $P = \{t_1 \doteq t'_1, \ldots, t_n \doteq t'_n\}$ și*
2. *σ este unificator pentru t_i și t'_i, pentru orice $i \in \{1, \ldots, n\}$.*

Definiția 1.8 (Mulțimea soluțiilor unei probleme de unificare)**.** *Cu unif(P) notăm mulțimea soluțiilor unei probleme de unificare P:*

$$\textit{unif}(P) = \{\sigma \mid \sigma \text{ \textit{este soluție a problemei} } P\}.$$

Observația 1.2. *Prin definiția noțiunii de soluție a unei probleme de unificare, dacă $P = \perp$, atunci unif(P) $= \emptyset$.*

Exemplul 1.8. *Fie $P = \{f(x, a) \doteq f(y, a)\}$. Avem că unif($P$) $= \{\{x \mapsto z, y \mapsto z\}, \{x \mapsto y\}, \ldots\}$.*

Definiția 1.9 (Cea mai generală soluție)**.** *Substituția σ este cea mai generală soluție pentru o problemă de unificare $P = \{t_1 \doteq t'_1, \ldots, t_n \doteq t'_n\}$ dacă:*

1. *σ este soluție pentru P: $\sigma^\sharp(t_i) = \sigma^\sharp(t'_i)$, pentru orice $1 \leq i \leq n$;*
2. *σ este mai generală decât orice altă soluție pentru P.*

Observația 1.3. *Observați că în cazul în care unif(P) $\neq \emptyset$ (problema de unificare are soluții), atunci există cel putin o cea mai generală soluție pentru P.*

Notație 1.1. *Cu mgu(P) notăm o cea mai generală soluție a problemei de unificare P (dacă problema P are soluție).*

Cu mgu(t_1, t_2) notăm un cel mai general unificator al termenilor t_1, t_2 (dacă termenii sunt unificabili).

Observația 1.4. *mgu(t_1, t_2) $=$ mgu($\{t_1 \doteq t_2\}$).*

Definiția 1.10 (Formă rezolvată)**.** *O problemă de unificare P* este în formă rezolvată *dacă $P = \bot$ sau $P = \{x_1 \doteq t'_1, \ldots, x_n \doteq t'_n\}$ și $x_i \notin vars(t_j)$ pentru orice $i, j \in \{1, \ldots, n\}$.*

De ce este utilă forma rezolvată a problemelor de unificare?

Lema 1.1. *Dacă $P = \{x_1 \doteq t'_1, \ldots, x_n \doteq t'_n\}$ este în formă rezolvată, atunci $\{x_1 \mapsto t'_1, \ldots, x_n \mapsto t'_n\}$ este cea mai generală soluție a problemei P.*

Următoarele reguli pot fi folosite pentru aducerea unei probleme de unificare în formă rezolvată:

Ștergere	$P \cup \{t \doteq t\} \Rightarrow P$
Descompunere	$P \cup \{f(t_1, \ldots, t_n) \doteq f(t'_1, \ldots, t'_n)\} \Rightarrow$ $P \cup \{t_1 \doteq t'_1, \ldots, t_n \doteq t'_n\}$
Orientare	$P \cup \{f(t_1, \ldots, t_n) \doteq x\} \Rightarrow P \cup \{x \doteq f(t_1, \ldots, t_n)\}$
Eliminare	$P \cup \{x \doteq t\} \Rightarrow \sigma^\sharp(P) \cup \{x \doteq t\}$ dacă $x \notin vars(t), x \in vars(P)$(unde $\sigma = \{x \mapsto t\}$)
Conflict	$P \cup \{f(t_1, \ldots, t_n) \doteq g(t'_1, \ldots, t'_m)\} \Rightarrow \bot$
Occurs check	$P \cup \{x \doteq f(t_1, \ldots, t_n)\} \Rightarrow \bot$ dacă $x \in vars(f(t_1, \ldots, t_n))$

Transformările de mai sus au următoarele proprietăți:

Lema 1.2 (Progres)**.** *Dacă P nu este în formă rezolvată, atunci există P' astfel încât $P \Rightarrow P'$.*

Lema 1.3 (Păstrarea soluțiilor)**.** *Dacă $P \Rightarrow P'$, atunci $unif(P) = unif(P')$.*

Lema 1.4 (Terminare)**.** *Nu există o secvență infinită $P \Rightarrow P_1 \Rightarrow P_2 \Rightarrow \ldots \Rightarrow P_i \Rightarrow \ldots$.*

Corolarul 1.1. *Regulile precedente constituie un algoritm de calcul al unei cele mai generale soluții pentru o problemă de unificare, dacă aceasta există.*

Exemplul 1.9.

$$P = \{f(g(x_1, a), x_2) \doteq x_3, f(x_2, x_2) \doteq f(a, x_1)\} \overset{\text{Descompunere}}{\Rightarrow}$$

$$\{f(g(x_1, a), x_2) \doteq x_3, x_2 \doteq a, x_2 \doteq x_1\} \overset{\text{Eliminare}}{\Rightarrow}$$

$$\{f(g(x_1, a), a) \doteq x_3, x_2 \doteq a, a \doteq x_1\} \overset{\text{Orientare}}{\Rightarrow}$$

$$\{f(g(x_1, a), a) \doteq x_3, x_2 \doteq a, x_1 \doteq a\} \overset{\text{Eliminare}}{\Rightarrow}$$

$$\{f(g(a, a), a) \doteq x_3, x_2 \doteq a, x_1 \doteq a\} \overset{\text{Orientare}}{\Rightarrow}$$

$$\{x_3 \doteq f(g(a, a), a), x_2 \doteq a, x_1 \doteq a\}.$$

Concluzie: $\{x_3 \mapsto f(g(a, a), a), x_2 \mapsto a, x_1 \mapsto a\}$ *este cea mai generală soluție a problemei de unificare inițiale.*

Exemplul 1.10.

$$P = \{f(g(x_1, a), x_2) \doteq x_3, f'(x_2) \doteq f'(x_3)\} \overset{\text{Descompunere}}{\Rightarrow}$$

$$\{f(g(x_1, a), x_2) \doteq x_3, x_2 \doteq x_3\} \overset{\text{Orientare}}{\Rightarrow}$$

$$\{x_3 \doteq f(g(x_1, a), x_2), x_2 \doteq x_3\} \overset{\text{Eliminare}}{\Rightarrow}$$

Explicati de ce nu se mai poate aplica orientare

$$\{x_3 \doteq f(g(x_1, a), x_3), x_2 \doteq x_3\} \overset{\text{Occurs check}}{\Rightarrow}$$

$$\perp.$$

Concluzie: *unif*$(P) = \emptyset$.

Exemplul 1.11.

$$P = \{f(g(x_1, a), x_2) \doteq x_3, f(g(x_4, x_5)) \doteq f(x_3)\} \overset{\text{Descompunere}}{\Rightarrow}$$

$$\{f(g(x_1, a), x_2) \doteq x_3, g(x_4, x_5) \doteq x_3\} \overset{\text{Orientare}}{\Rightarrow}$$

$$\{f(g(x_1, a), x_2) \doteq x_3, x_3 \doteq g(x_4, x_5)\} \overset{\text{Eliminare}}{\Rightarrow}$$

$$\{f(g(x_1, a), x_2) \doteq g(x_4, x_5), x_3 \doteq g(x_4, x_5)\} \overset{\text{Conflict}}{\Rightarrow}$$

$$\perp.$$

Concluzie: $unif(P) = \emptyset$.

2 Rezoluție de ordinul I

Rezoluția pentru logica de ordinul I este un sistem deductiv alcătuit din următoarele două reguli de inferență:

$$\text{REZOLUȚIE BINARĂ}\ \frac{P(t_1,\ldots,t_n)\vee C_1 \quad \neg P(t'_1,\ldots,t'_n)\vee C_2}{\sigma^\flat(C_1\vee C_2)}\ \begin{array}{l} V_1\cap V_2=\emptyset \\ \sigma = mgu(\{t_1 \doteq t'_1,\ldots,t_n\doteq t'_n\})\end{array}$$

unde $V_1 = vars(P(t_1,\ldots,t_n)\vee C_1)$ și $V_2 = vars(\neg P(t'_1,\ldots,t'_n)\vee C_2)$.

$$\text{FACTORIZARE POZITIVĂ}\ \frac{P(t_1,\ldots,t_n)\vee P(t'_1,\ldots,t'_n)\vee C}{\sigma^\flat(P(t_1,\ldots,t_n)\vee C)}\ \sigma = mgu(\{t_1 \doteq t'_1,\ldots,t_n\doteq t'_n\})$$

Observația 2.1.

- *În cazul în care clauzele care reprezintă ipotezele regulii* REZOLUȚIE BINARĂ *au variabile în comun ($V_1\cap V_2 \neq \emptyset$), variabilele uneia dintre clauze trebuie redenumite înainte de a aplica regula (vezi exemplul de mai jos);*
- *În cazul în care problema de unificare care apare în regula de rezoluție nu are soluție, regula nu poate fi aplicată.*
- *Regula de factorizare pozitivă are o singură ipoteză.*
- *În cazul în care problema de unificare care apare în regula de factorizare nu are soluție, regula nu poate fi aplicată.*
- *Regula de factorizare pozitivă este necesară pentru completitudine (vezi exerciții seminar).*

Teorema 2.1 (Teorema rezoluției)**.** *O formulă $\varphi = \forall x_1.\ldots.\forall x_n.(C_1\wedge C_2\wedge \ldots C_m)$, aflată în FNSC, este nesatisfiabilă dacă și numai dacă $\Box$ se poate obține din clauzele $C_1,\ldots,C_m$, aplicând regulile* REZOLUȚIE BINARĂ *și* FACTORIZARE POZITIVĂ.

Exemplul 2.1. *Să demonstrăm că $\forall x.(P(x)\wedge(\neg P(h(x))\vee Q(f(x)))\wedge(\neg Q(f(g(a)))))$ este nesatifiabilă, prin rezoluție de ordinul I:*

1. $P(x)$
2. $\neg P(h(x))\vee Q(f(x))$
3. $\neg Q(f(g(a)))$
4. $Q(f(x))$ *rezoluție binară între* 1 *și* 2*:*

$$\frac{P(x') \qquad \neg P(h(x))\vee Q(f(x))}{\sigma^\flat(Q(f(x)))}\ \sigma = \{x'\mapsto h(x)\} = mgu(\{x'\doteq h(x)\})$$

5. $\square$ *rezoluție între* 3 *și* 4*:*

$$\frac{Q(f(g(a))) \qquad Q(f(x))}{\sigma^\flat(\square)} \; \sigma = \{x \mapsto g(a)\} = mgu(\{f(g(a)) \doteq f(x)\})$$

Exercițiul 2.1. *Arătați că* $\Big(\forall x.(P(x) \rightarrow Q(x))\Big) \land P(s) \rightarrow Q(s)$ *este validă, folosind rezoluția de ordinul I.*