Podstawienia (ang. substitution)

podstawienie — skończony zbiór postaci $\{x_1/t_1, \ldots, x_n/t_n\}$,
gdzie: x_i — zmienne, t_i — termy różne od x_i,
wszystkie zmienne x_i są różne ($x_i \neq x_j$ dla $i \neq j$)

element podstawienia θ postaci x_i/t_i — dowiązanie zmiennej x_i

podstawienie identycznościowe (ε) — określone przez zbiór pusty

niech $\theta = \{x_1/t_1, \ldots, x_n/t_n\}$ — podstawienie

Dom(θ) $\stackrel{df}{=} \{x_1, \ldots, x_n\}$
Range(θ) $\stackrel{df}{=} \{t_1, \ldots, t_n\}$
Ran(θ) $\stackrel{df}{=}$ zbiór zmiennych występujących w t_i
Var(θ) $\stackrel{df}{=}$ Dom(θ) $\cup$ Ran(θ)

V — zbiór zmiennych
$\theta|V$ — podstawienie otrzymane z θ, ograniczenie dziedziny do V

podstawienie ustalone — jeśli wszystkie termy t_i są ustalone (stałe)
podstawienie zmiennych — jeśli wszystkie termy t_i są zmiennymi

wyrażenie — term, literał, koniunkcja lub alternatywa literałów, klauzula
wyrażenie proste — term lub atom

Niech $\theta = \{x_1/t_1, \ldots, x_n/t_n\}$ — podstawienie, E — wyrażenie

konkretyzacja wyrażenia E określona przez podstawienie θ — wyrażenie $E\theta$ powstałe z E poprzez jednoczesną zamianę każdego wystąpienia zmiennej x_i w E termem t_i ($i = 1, \ldots, n$)

Np. E = p(x, y, f(a)), θ = {x/b, y/x}
Eθ = p(b, x, f(a))

równoważna definicja $E\theta$ (indukcja strukturalna):

x — zmienna, x $\in$ Dom(θ), czyli x = x_i : $\quad \mathrm{x}\theta \stackrel{df}{=} \mathrm{t}_i$

x — zmienna, x $\notin$ Dom(θ) : $\quad \mathrm{x}\theta \stackrel{df}{=} \mathrm{x}$

a — stała : $\quad \mathrm{a}\theta \stackrel{df}{=} \mathrm{a}$

$f(t_1, \ldots, t_n)\theta \stackrel{df}{=} f(t_1\theta, \ldots, t_n\theta)$

Złożenie podstawień

Niech $\theta = \{x_1/s_1, \ldots, x_n/s_n\}$

$\sigma = \{y_1/t_1, \ldots, y_m/t_m\}$

podstawienie $\theta\sigma$ otrzymuje się z sekwencji dowiązań:

$$x_1/s_1\sigma,\ \ldots,\ x_n/s_n\sigma,\ \ y_1/t_1,\ \ldots,\ y_m/t_m$$

poprzez usunięcie:

— elementów $x_i/s_i\sigma$ takich, że $x_i = s_i\sigma$

— elementów y_j/t_j takich, że $y_j \in \{x_1, \ldots, x_n\}$

inaczej: x — zmienna, $(\theta\sigma)(x) \stackrel{df}{=} (x\theta)\sigma$

Przykład

niech $\theta = \{x/f(y), y/z, u/g(u)\}, \quad \sigma = \{x/a, y/b, z/y, u/c\}$

otrzymujemy: $x/f(b), y/y, u/g(c), \ \ x/a, y/b, z/y, u/c$

a zatem $\theta\sigma = \{x/f(b), u/g(c), z/y\}$

Właściwości podstawień

(a) $\theta\varepsilon = \varepsilon\theta = \theta$

(b) $(E\theta)\sigma = E(\theta\sigma)$ dla dowolnego wyrażenia E

(c) $(\theta\sigma)\gamma = \theta(\sigma\gamma)$

Przykład

$\theta = \{x/f(y), y/z\}, \quad \sigma = \{x/a, z/b\}, \quad E = p(x, y, g(z))$

$\theta\sigma = \{x/f(y), y/b, z/b\}$

$E\theta = p(f(y), z, g(z)), \quad (E\theta)\sigma = p(f(y), b, g(b)) = E(\theta\sigma)$

Niech E, F — wyrażenia.
Wyrażenia E i F są **wariantami**, jeśli istnieją podstawienia θ i σ takie, że $E = F\theta$ oraz $F = E\sigma$.
E jest wariantem F (i odwrotnie)

Np. E = p(f(x, y), g(z)),
F = p(f(y, x), g(u))
dla $\theta = \{x/y, y/x, z/u\}$ $\quad E\theta = F$
dla $\sigma = \{y/x, x/y, u/z\}$ $\quad F\sigma = E$

Czy p(x, x) jest wariantem p(x, y)? Nie.

podstawienie zmieniające nazwy (**przemianowanie**):
podstawienie zmiennych $\theta = \{x_1/y_1, \ldots, x_n/y_n\}$ takie, że
Dom(θ) = Range(θ)

Np. E = p(f(x), y, z)
$\theta = \{x/y, y/x\}$ $\quad$ Eθ = p(f(y), x, z) — przemianowanie
$\sigma = \{x/y\}$ $\quad$ Eσ = p(f(y), y, z) — nie

Twierdzenie
Jeśli E i F są wariantami, to istnieją podstawienia zmieniające nazwy zmiennych θ, σ takie, że
E = Fθ, F = Eσ.

Niech $S = \{E_1, \ldots, E_n\}$ — zbiór wyrażeń (skończony)
θ — podstawienie

$S\theta$ oznacza zbiór wyrażeń $\{E_1\theta, \ldots, E_n\theta\}$

Niech S - skończony zbiór wyrażeń prostych

podstawienie uzgadniające S — podstawienie θ takie, że $S\theta$ jest zbiorem jednoelementowym podstawienie θ jest **podstawieniem bardziej ogólnym** od σ, jeśli istnieje podstawienie ω takie, że $\sigma = \theta\omega$

najbardziej ogólne podstawienie uzgadniające S — podstawienie uzgadniające S bardziej ogólne od wszystkich podstawień uzgadniających S (ozn. mgu; ang. most general unifier)
(θ jest mgu, jeśli dla każdego podstawienia uzgadniającego σ zbioru S istnieje γ takie, że $\sigma = \theta\gamma$)

Przykład
S_1 = { p(f(x), a), p(y, f(w)) } — nie istnieje podst. uzgadn.
S_2 = { p(f(x), z), p(y, a) }
σ = { y/f(a), x/a, z/a } — podstawienie uzgadniające
θ = { y/f(x), z/a } — mgu ($\sigma = \theta\,\{x/a\}$)

Twierdzenie
Niech θ, σ — najbardziej ogólne podstawienia uzgadniające dla zbioru S.
Wówczas istnieją podstawienia zmieniające nazwy zmiennych δ i ω takie, że:

$$\theta = \sigma\omega \quad \text{oraz} \quad \sigma = \theta\delta.$$

(mgu są identyczne z dokładnością do nazw zmiennych)

Niech S - skończony zbiór wyrażeń.

Zbiór niezgodności dla S — zbiór podwyrażeń rozpoczynających się od pierwszej skrajnie lewej pozycji wyrażeń S, na której nie we wszystkich wyrażeniach z S występuje ten sam symbol.

Np. S = { p(f(x), h(y), a), p(f(x), z, a), p(f(x), h(y), b)}
zbiór niezgodności = { h(y), z }

Algorytm uzgadniania (J.A. Robinson)

Niech S — skończony zbiór wyrażeń prostych

1. Niech k = 0, $\sigma_0 = \varepsilon$.
2. Jeśli zbiór $S\sigma_k$ jest zbiorem jednoelementowym, to koniec: σ_k jest najbardziej ogólnym podstawieniem uzgadniającym dla S, wpp. znajdź zbiór niezgodności D_k dla zbioru wyrażeń $S\sigma_k$.
3. Jeśli zbiór D_k zawiera zmienną v oraz term t nie zawierający zmiennej v, to niech $\sigma_{k+1} = \sigma_k \cdot \{v/t\}$, zwiększ k o jeden, idź do p.2,
   wpp. koniec: zbioru wyrażeń S nie można uzgodnić. □

(algorytm niedeterministyczny: w p.3 wybór zmiennej oraz termu)

Przykłady

$$S_1 = \{\ \mathrm{p(f(a), g(x))}, \quad \mathrm{p(y, y)}\}$$

— $\sigma_0 = \varepsilon$
— $D_0 = \{\mathrm{f(a), y}\}$, $\sigma_1 = \{\mathrm{y/f(a)}\}$,
$S_1\sigma_1 = \{\ \mathrm{p(f(a), g(x))}, \quad \mathrm{p(f(a), f(a))}\ \}$
— $D_1 = \{\mathrm{g(x), f(a)}\}$, koniec: S_1 nie jest uzgadnialny

$$S_2 = \{\ \mathrm{p(a, x, h(g(z)))}, \quad \mathrm{p(z, h(y), h(y))}\ \}$$

— $\sigma_0 = \varepsilon$
— $D_0 = \{\mathrm{a, z}\}$, $\sigma_1 = \{\mathrm{z/a}\}$
$S_2\sigma_1 = \{\ \mathrm{p(a, x, h(g(a)))}, \quad \mathrm{p(a, h(y), h(y))}\ \}$
— $D_1 = \{\mathrm{x, h(y)}\}$, $\sigma_2 = \{\mathrm{z/a, x/h(y)}\}$
$S_2\sigma_2 = \{\ \mathrm{p(a, h(y), h(g(a)))}, \quad \mathrm{p(a, h(y), h(y))}\ \}$
— $D_2 = \{\mathrm{g(a), y}\}$, $\sigma_3 = \{\mathrm{z/a, x/h(g(a)), y/g(a)}\}$
$S_2\sigma_3 = \{\ \mathrm{p(a, h(g(a)), h(g(a)))}\ \}$

Twierdzenie o uzgadnianiu

Niech S — skończony zbiór wyrażeń prostych.
Jeśli zbiór wyrażeń S można uzgodnić, to algorytm uzgadniania kończy się i przekazuje najbardziej ogólne podstawienie uzgadniające dla S.
Jeśli zbioru S nie można uzgodnić, to algorytm kończy się informując o niemożności uzgodnienia.

dowód:

(i) algorytm kończy się
- — zbiór S zawiera skończoną liczbę zmiennych
- — jednokrotne wykonanie p.3 algorytmu powoduje zmniejszenie zbioru zmiennych o jedną zmienną

(ii) załóżmy, że S nie można uzgodnić
algorytm kończy się, ale nie kończy się w p.2 (wówczas S byłby uzgadnialny), a zatem kończy się w p.3

(iii) załóżmy, że S można uzgodnić
niech θ — dowolne podstawienie uzgadniające S
udowodnimy, że:
dla $k \geq 0$, jeśli σ_k — podstawienie obliczone w k-krokach, to istnieje podstawienie γ_k takie, że $\theta = \sigma_k \gamma_k$
(dowód indukcyjny)

wiemy, że:
S — można uzgodnić, algorytm kończy się w p.2 po k-krokach iteracji oraz $\theta = \sigma_k \gamma_k$ dla pewnego podstawienia γ_k
i σ_k — podstawienie uzgadniające S
θ — dowolne podstawienie uzgadniające, a zatem σ_k jest mgu

$\square$

Lemat

S — skończony zbiór uzgadnialnych wyrażeń prostych

θ — dowolne podstawienie uzgadniające S

k $\geq$ 0, σ_k — podstawienie uzyskane po k krokach algorytmu

Wówczas: istnieje γ_k t.że $\theta = \sigma_k \gamma_k$

dowód:

— k = 0, $\sigma_0 = \epsilon$, niech $\gamma_0 = \theta$, czyli $\theta = \sigma_0 \gamma_0$

— k $\geq$ 0, niech $\theta = \sigma_k \gamma_k$

$S\sigma_k$ — zbiór nie jednoelementowy

należy pokazać, że istnieje γ_{k+1} t.że $\theta = \sigma_{k+1} \gamma_{k+1}$

niech D_k — zbiór niezgodności Sσ_k

θ uzgadnia S, a zatem γ_k uzgadnia D_k,

czyli D_k zawiera zmienną (v) i term (t)

ponieważ vγ_k = tγ_k, stąd v nie występuje w t

niech { v/t } — wybrane podstawienie, czyli $\sigma_{k+1} = \sigma_k$ { v/t }

niech $\gamma_{k+1} = \gamma_k -$ { v/vγ_k }

(i) γ_k zawiera dowiązanie dla v

wówczas: γ_k = { v/vγ_k } $\cup\ \gamma_{k+1}$

= { v/tγ_k } $\cup\ \gamma_{k+1}$

= { v/tγ_{k+1} } $\cup\ \gamma_{k+1}$

= { v/t } γ_{k+1}

(ii) γ_k nie zawiera dowiązania dla v

wówczas: $\gamma_{k+1} = \gamma_k$ i każdy element D_k jest zmienną,

czyli również γ_k = { v/t } γ_{k+1} (v = tγ_k)

a zatem: $\theta = \sigma_k \gamma_k = \sigma_k \{v/t\} \gamma_{k+1} = \sigma_{k+1} \gamma_{k+1}$

□

Przykład

$$S_3 = \{\ \mathrm{p(x,\ x),\ p(y,\ f(y))}\ \}$$

— $\sigma_0 = \varepsilon$

— $D_0 = \{\mathrm{x,\ y}\}$, $\sigma_1 = \{\mathrm{x/y}\}$

$$S_3\sigma_1 = \{\ \mathrm{p(y,\ y),\ p(y,\ f(y))}\ \}$$

— $D_1 = \{\mathrm{y,\ f(y)}\}$

zgodnie z p.3: S_3 nie jest uzgadnialny, gdyż term f(y) zawiera zmienną y

jest to tzw. problem **occur check**

(nieskończone dowiązanie: $\{\mathrm{y/f}(\infty)\}$)

□

podstawienie θ nazywamy **idempotentnym** jeśli $\theta\theta = \theta$

podstawienie θ — mgu termów s i t nazywamy **mocnym** jeśli dla każdego podstawienia η uzgadniającego termy s i t zachodzi:

$$\eta = \theta\eta$$

Twierdzenie

Podstawienie θ jest idempotentne wiw gdy

$$\mathrm{Dom}(\ \theta\ ) \cap \mathrm{Ran}(\ \theta\ ) = \emptyset$$

Twierdzenie

Podstawienie θ będące mgu jest mocne wiw gdy jest idempotentne.

Twierdzenie

Jeśli zbiór wyrażeń S można uzgodnić, to algorytm uzgadniania kończy się i przekazuje najbardziej ogólne mocne podstawienie uzgadniające dla S.