Substitutionen

Eine verallgemeinerte Substitution σ ist eine Abbildung der Menge der Variablen in die Menge aller Terme, so daß nur endlich viele Variable x existieren mit $\sigma(x) \neq x$.

Sei $\mathrm{Def}(\sigma) = \{x \text{ Variable} \mid x \neq \sigma(x)\}$ der Definitionsbereich der verallgemeinerten Substitution σ.

Für einen Term t definieren wir den Term $t\,\sigma$ (Anwendung der verallgemeinerten Substitution σ auf den Term t) wie folgt induktiv:

- $x\,\sigma = \sigma(x)$
- $\big[f(t_1, \ldots, t_k)\big]\,\sigma = f(t_1\,\sigma, \ldots, t_k\,\sigma)$ für Terme $t_1, \ldots, t_k$, $f \in \mathrm{Fun}$ und $k = \mathrm{ar}(f)$

Für eine atomare Formel $\alpha = P(t_1, \ldots, t_k)$ (d.h. $P \in \mathrm{Rel}$, $\mathrm{ar}(P) = k$, $t_1, \ldots, t_k$ Terme) sei

$$\alpha\,\sigma \quad = \quad P(t_1\,\sigma, \ldots, t_k\,\sigma)$$

Verknüpfung von verallgemeinerten Substitutionen: Sind σ_1 und σ_2 verallgemeinerte Substitutionen, so definieren wir eine neue verallgemeinerte Substitution $\sigma_1\sigma_2$ durch

$$(\sigma_1\sigma_2)(x) = (x\,\sigma_1)\,\sigma_2\,.$$

Beispiel

Sei x Variable und t Term. Dann ist σ mit

$$\sigma(y) = \begin{cases} t & \text{falls } x = y \\ y & \text{sonst} \end{cases}$$

eine verallgemeinerte Substitution. Für alle Terme s und alle atomaren Formeln α gilt

$$s\,\sigma = s[x := t] \text{ und } \alpha\,\sigma = \alpha[x := t]\,.$$

Substitutionen sind also ein Spezialfall der verallgemeinerten Substitutionen.

Beispiel: Die verallgemeinerte Substitution σ mit $\mathrm{Def}(\sigma) = \{x, y, z\}$ und

$$\sigma(x) = f\big(h(x')\big), \quad \sigma(y) = g\big(a, h(x')\big), \quad \sigma(z) = h(x')$$

ist gleich der verallgemeinerten Substitution

$$\begin{aligned} & \Big[x := f\big(h(x')\big)\Big] \Big[y := g\big(a, h(x')\big)\Big] \big[z := h(x')\big] \\ = \quad & \big[x := f(z)\big] \big[y := g(a, z)\big] \big[z := h(x')\big] . \end{aligned}$$

Es kann sogar jede verallgemeinerte Substitution σ als Verknüpfung von Substitutionen der Form $[x := t]$ geschrieben werden.

Vereinbarung: Wir sprechen ab jetzt nur von „Substitutionen“, auch wenn wir „verallgemeinerte Substitutionen“ meinen.

Unifikator/Allgemeinster Unifikator

Definition

1. Ein Unifikator eines Paars von Termen (s, t) ist eine Substitution σ mit $s\,\sigma = t\,\sigma$.
2. Ein Unifikator einer Menge $E = \{(s_i, t_i) \mid 1 \leq i \leq n\}$ von Termpaaren ist eine Substitution σ mit $s_i\,\sigma = t_i\,\sigma$ für alle $1 \leq i \leq n$.
3. Ein Unifikator eines Paars (α, β) von Atomformeln ist eine Substitution σ mit $\alpha\,\sigma = \beta\,\sigma$.
4. Ein allgemeinster Unifikator von X ist ein Unifikator σ von X, so daß für jeden Unifikator τ von X eine Substitution σ' existiert mit $\tau = \sigma\,\sigma'$.

Existiert ein Unifikator?

	Ja	Nein
$\Big(P\big(f(x)\big), P\big(g(y)\big)\Big)$		
$\Big(P(x), P\big(f(y)\big)\Big)$		
$\Big\{\big(x, f(u)\big), \big(f(y), z\big)\Big\}$		
$\Big\{\big(x, f(u)\big), \big(f(y), f(z)\big)\Big\}$		
$\Big\{\big(x, f(y)\big), \big(f(x), y\big)\Big\}$		
$\Big\{\big(x, f(y)\big), \big(g(x), z\big), \big(g^2(x), g(z)\big)\Big\}$		

Beobachtungen

(B1) σ ist genau dann Unifikator von $\big(P(s_1, \ldots, s_k), P(t_1, \ldots, t_k)\big)$ bzw. $\big(f(s_1, \ldots, s_k), f(t_1, \ldots, t_k)\big)$, wenn σ Unifikator von $\big\{(s_1, t_1), (s_2, t_2), \ldots, (s_k, t_k)\big\}$ ist.

(B2) Sei x eine Variable und t ein Term.
Kommt x in t nicht vor, so ist $[x := t]$ ein allgemeinster Unifikator von (x, t).
Kommt x in t vor und gilt $x \neq t$, so existiert kein Unifikator von (x, t).

(B3) Seien $X \subseteq E$ Mengen von Termpaaren und sei σ ein allgemeinster Unifikator von X.
Eine Subsitution τ ist Unifikator von E genau dann, wenn die Menge

$$(E \setminus X)\,\sigma = \big\{(s_1\,\sigma, s_2\,\sigma) \;\big|\; (s_1, s_2) \in E \setminus X\big\}$$

einen Unifikator σ' mit $\tau = \sigma\,\sigma'$ hat.

Unifikationsalgorithmus

Eingabe: endliche Menge von Termpaaren E_0

Sei id die Substitution mit $\mathrm{id}(x) = x$ für alle Variable x.

Setze $E = E_0$ und $\sigma = \mathrm{id}$.
solange möglich, mache eine der folgenden Transformationen:

(1) wähle $(t, t) \in E$ und setze $E := E \setminus \{(t, t)\}$.

(2) wähle $(s, t) = \big(f(s_1, \ldots, s_k), f(t_1, \ldots, t_k)\big) \in E$ und setze
$E := E \setminus \{(s, t)\} \cup \{(s_i, t_i) \mid 1 \leq i \leq n\}$.

(3) wähle $(x, t) \in E$, wobei x nicht in t vorkommt, und setze
$E := \Big(E \setminus \{(x, t)\}\Big)[x := t]$ und $\sigma := \sigma\,[x := t]$.

(4) wähle $(s, x) \in E$, wobei x nicht in s vorkommt, und setze
$E := \Big(E \setminus \{(s, x)\}\Big)[x := s]$ und $\sigma := \sigma\,[x := s]$.

$\mathrm{if}\ E = \emptyset$
then Ausgabe „σ ist allgemeinster Unifikator von E_0“
else Ausgabe „E_0 hat keinen Unifikator“

Beispiel

$E_0 = \{(x, f(y)), (g(x), z), (g^2(x), g(z))\}$

Modifikation (3) mit $(x, t) = (x, f(y))$:
$E = \{(gf(y), z), (g^2 f(y), g(z))\}, \quad \sigma = [x := f(y)]$

Modifikation (2) mit $(s, t) = (g^2 f(y), g(z))$:
$E = \{(gf(y), z)\}, \quad \sigma = [x := f(y)]$

Modifikation (4) mit $(s, x) = (gf(y), z)$:
$E = \emptyset \quad \sigma = [x := f(y)]\,[z := gf(y)]$

Es gilt

$$E_0\,\sigma = \left\{ \big(f(y), f(y)\big), \big(gf(y), gf(y)\big), \big(g^2 f(y), g^2 f(y)\big) \right\},$$

d.h. σ ist tatsächlich ein Unifikator von E_0.

Beispiel

$E_0 = \{(x, f(y)), (f(x), y)\}$

Modifikation (3) mit $(x, t) = (x, f(y))$:
$E = \{(f^2(y), y)\}$, $\sigma = [x := f(y)]$

Hier sind keine weiteren Modifikationen möglich. Wegen $E \neq \emptyset$ behauptet der Unifikationsalgorithmus, daß E_0 keinen Unifikator hat (und tatsächlich gibt es auch keinen).

Behauptung

Beim Eintritt in die Schleife und beim Austritt aus der Schleife gilt folgende Invariante:

$$\tau \text{ unifiziert } E_0 \iff \text{es gibt } \sigma' \text{ mit } \tau = \sigma\,\sigma' \text{ und } \sigma' \text{ unifiziert } E.$$

Beweis: Beim ersten Eintritt in die Schleife gilt Invariante wegen $(E, \sigma) = (E_0, \mathrm{id})$.

Gelte nun Invariante für (E_1, σ_1) und sei (E_2, σ_2) Ergebnis eines Schleifendurchlaufs, d.h. einer der Modifikationen (1)-(4).

- Anwendung der Modifikation (1): (E_2, σ_2) erfüllt Invariante, da $\sigma_2 = \sigma_1$ und da $E_2 = E_1 \setminus \{(t, t)\}$ und E_1 dieselben Unifikatoren haben.
- Anwendung der Modifikation (2): (E_2, σ_2) erfüllt Invariante, da $\sigma_2 = \sigma_1$ und da E_2 und E_1 nach Beobachtung (B1) von Folie 14.6 dieselben Unifikatoren haben.

- Anwendung der Modifikation (3): Sei τ beliebige Substitution.

  Nach IV unifiziert τ die Menge E_0 genau dann, wenn es eine Substitution σ' gibt mit $\tau = \sigma\,\sigma'$, die E_1 unifiziert.

  Nach Beobachtungen (B2) und (B3) von Folie 14.6 unifiziert σ' die Menge E_1 genau dann, wenn es Subsitution σ'' gibt mit $\sigma' = [x := t]\,\sigma''$, die $\big(E_1 \setminus \{(x,t)\}\big)[x := t] = E_2$ unifiziert.

  also: τ unifiziert E_0 gdw. es Substitution σ'' gibt mit $\tau = \underbrace{\sigma\,[x := t]}_{=\sigma_2}\,\sigma''$, die E_2 unifiziert.

(4) symmetrisch

□

Behauptung

Wenn, bei Eingabe von E_0, der Unifikationsalgorithmus die Substitution σ ausgibt, so ist σ ein allgemeinster Unifikator von E_0.

Beweis:
Da der Algorithmus σ ausgibt, erfüllt $(\emptyset, \sigma)$ die Invariante. Also gilt für alle Substitutionen τ:

$$\begin{aligned} \tau \text{ unifiziert } E_0 &\iff \exists \sigma' : \tau = \sigma\,\sigma' \text{ und } \sigma' \text{ unifiziert } \emptyset \\ &\iff \exists \sigma' : \tau = \sigma\,\sigma' \end{aligned}$$

σ ist also tatsächlich ein allgemeinster Unifikator. □

Behauptung

Wenn, bei Eingabe von E_0, der Unifikationsalgorithmus ausgibt, es gäbe keinen Unifikator, so ist E_0 tatsächlich nicht unifizierbar.

Beweis:
Da der Algorithmus behauptet, es gäbe keinen Unifikator, existieren (E, σ) mit $E \neq \emptyset$, die die Invariante erfüllen und keine der Modifikationen (1)-(4) erlauben. Wegen $E \neq \emptyset$ existiert also ein Paar $(s, t) \in E$. Da keine Modifikation anwendbar ist, gelten die folgenden Aussagen:

- Falls $s = f(s_1, \ldots, s_k)$ und $t = g(t_1, \ldots, t_\ell)$, so gilt $f \neq g$.
- Falls s Variable ist, so kommt s in t vor und $s \neq t$.
- Falls t Variable ist, so kommt t in s vor und $s \neq t$.

In all diesen Fällen hat (s, t) keinen Unifikator. Also hat E keinen Unifikator. Da (E, σ) die Invariante erfüllt, hat also auch E_0 keinen Unifikator. □

Behauptung

Der Unifikationsalgorithmus terminiert bei Eingabe von E_0.

Beweis:

Für eine Menge E von Termpaaren sei die Norm $||E||$ die Summe der Größe aller Terme:

$$||E|| = \sum_{(s,t)\in E} |s| + |t| \,.$$

In jedem Schleifendurchlauf sinkt

- die Anzahl der vorkommenden Variablen (Modifikationen (3) und (4)) oder
- die Norm der Formelmenge, wobei die Anzahl der vorkommenden Variablen nicht steigt (Modifikationen (1) und (2)).

Da die Anzahl der vorkommenden Variablen nur endlich oft sinken kann, und da, von (E, σ) ausgehend, nur $||E||$ oft die Modifikationen (1) und (2) angewandt werden können, terminiert der Algorithmus. □

Satz

Bei Eingabe einer Menge E_0 entscheidet der Unifikationsalgorithmus, ob E_0 einen Unifikator hat. In diesem Fall gibt er einen allgemeinsten Unifikator aus.