Zur Korrektheit

Sei spec $=$ (sig, R)
R bezüglich der Simplifikationsordnung $\succ$ simplifizierend.
$e/\pi = f(x_1, \ldots, x_n)$.
$l \to r \Leftarrow u = v$ in R, $f = \mathsf{top}(l)$.

Sei $\langle (s_1, \ldots, s_n), M, u = v \rangle \in C_f$, $(t_1^i, \ldots, t_n^i) \in M$.

Dies erzeugt das Teilziel

$$[u = v \wedge \bigwedge_{i=1}^{k} \tau_i(e)] \Rightarrow \sigma(e)$$

mit $\sigma(x_j) \equiv s_j$ und $\tau_i(x_j) \equiv t_j^i$ und es gilt
$l \equiv \sigma(f(x_1, \ldots, x_n))$ und die $\tau_i(f(x_1, \ldots, x_n))$ sind Teilterme von r.

Also gilt $\sigma(f(x_1, \ldots, x_n)) = l \succ r \succeq \tau_i(f(x_1, \ldots, x_n))$.

Definition 3.4

$\sigma \succ_i \tau \text{ gdw } \sigma(f(x_1, \ldots, x_n)) \succ \tau(f(x_1, \ldots, x_n))$ ist die durch spec, e, $f(x_1, \ldots, x_n)$ definierte Induktionsordnung.

Beachte

$\succ_i$ ist eine Noethersche Ordnung auf C-GSub(e).

Die Bedingung für die Korrektheit ist automatisch erfüllt.

Zur Vollständigkeit (1)

Sei spec $=$ (sig, R) und $C \subseteq F$ wie stets.

Definition 3.5

Das Coverset C_f für $f(x_1, \ldots, x_n)$, $f \in F - C$ heißt **vollständig**, falls es zu jedem $\hat{t} = (t_1, \ldots, t_n) \in \mathsf{Term}(C)^n$ ein $\langle \hat{s}, M, u = v \rangle \in C_f$ und ein σ gibt mit
$\sigma(\hat{s}) \equiv \hat{t}$ und $\sigma(u) =_R \sigma(v)$.

Beachte

a) Ist C_f für alle $f \in F$ vollständig, so ist jeder Grundterm der Form $f(t_1, \ldots, t_n)$ in R reduzierbar, es gilt also $f(t_1, \ldots, t_n) \xrightarrow{*}_R t_0$ für ein $t_0 \in \mathsf{Term}(C)$. Also ist f durch R total definiert.

b) Ist f durch R total definiert, so ist C_f vollständig.

c) In den bisherigen Beispielen war stets C_f vollständig.

d) Den Nachweis, dass f total definiert ist, kann man auch durch Induktion zeigen: Definiere das Prädikat $\mathrm{def}(t)$ auf $\mathcal{I} = \mathcal{I}(\mathsf{spec})$ durch $\mathcal{I} \models \mathrm{def}(t) \text{ gdw } \exists t' \in \mathsf{Term}(C) : t =_R t'$.
Zeige dann $\mathcal{I} \models \mathrm{def}(f(x_1, \ldots, x_n))$.

Zur Vollständigkeit (2)

Sei spec $= (\text{sig}, R)$
$e \equiv u = v \Rightarrow s = t$ und $e/\pi \equiv f(x_1, \ldots, x_n)$.

Lemma 3.1

Sei das Coverset C_f vollständig. Zu jedem $\varrho \in C\text{-GSub}(e)$ gibt es ein Teilziel

$$[u = v \wedge \bigwedge_{i=1}^{k} e_i] \Rightarrow e_0$$

im Induktionsschema zu spec, e, f und ein σ mit
$\sigma(u) =_R \sigma(v)$ und $\varrho(e) \equiv \sigma(e_0)$.

Beweis: Sei $\varrho(\hat{x}) \equiv \hat{t} = (t_1, \ldots, t_n)$. Da C_f vollständig ist, gibt es σ und $\langle \hat{s}, M, u = v\rangle \in C_f$ mit $\sigma(\hat{s}) \equiv \hat{t}$ und $\sigma(u) =_R \sigma(v)$. Dies $\langle \hat{s}, M, u = v\rangle$ erzeuge

$$[u = v \wedge \bigwedge_{i=1}^{k} e_i] \Rightarrow e_0.$$

Sei $\sigma_0(\hat{x}) = \hat{s}$, also $\varrho(\hat{x}) \equiv \hat{t} \equiv \sigma(\hat{s}) \equiv \sigma(\sigma_0(\hat{x}))$. Dann ist $\varrho(e) \equiv \sigma(\sigma_0(e)) \equiv \sigma(e_0)$.

Beachte

In $\langle \hat{s}, M, u = v\rangle$ kann sowohl M als auch $u = v$ leer sein. Ist $u = v$ leer, so entfällt im Teilziel $u = v \wedge \hat{e} \Rightarrow e_0$ die Vorbedingung „$u = v$“. Ist auch M leer, so entfällt „$u = v \wedge \hat{e}$“ .

Das Ergebnis

Sei spec $= (\text{sig}, R)$ konstruktor-basiert
sig $= (S, F, \alpha)$, $C \subseteq F$
R simplifizierend bezüglich $\succ$
$e \equiv u' = v' \Rightarrow s = t$ und $e/\pi \equiv f(x_1, \ldots, x_n)$

Satz 3.1.

Sei C_f vollständig und jedes Teilziel

$$u = v \wedge \hat{e} \Rightarrow e_0$$

aus dem Induktionsschema zu spec, e, $f(x_1, \ldots, x_n)$ gelte in $\mathcal{I}(\text{spec})$. Dann gilt auch e in $\mathcal{I}(\text{spec})$.

Beweis zu Satz 3.1

Sei $\varrho \in C$-GSub(e); zu zeigen ist, dass $\varrho(e)$ in $\mathcal{I}(\text{spec})$ gilt.

Wir führen Noethersche Induktion nach $\succ_i$.

Zu ϱ gibt es nach Lemma 3.1 ein Teilziel

$$[u = v \wedge \bigwedge_{j=1}^{k} \tau_j(e)] \Rightarrow \sigma(e)$$

und ein σ' mit $\varrho = \sigma' \circ \sigma$ auf Var(e) und $\sigma'(u) =_R \sigma'(v)$.

Es ist $\sigma \succ_i \tau_j$, also auch $\varrho \succ_i \varrho_j$ mit $\varrho_j = \sigma' \circ \tau_j$.

Also gilt nach IV $\varrho_j(e)$ in $\mathcal{I}(\text{spec})$ für $j = 1, \ldots, k$.

Da das Teilziel in $\mathcal{I}(\text{spec})$ gilt und wegen $\sigma'(u) =_R \sigma'(v)$ gilt $\varrho(e) \equiv \sigma'(\sigma(e))$ in $\mathcal{I}(\text{spec})$.

Ein Beweis zur Ackermann-Funktion (1)

Sei $F = \{\text{true}, \text{false}, 0, s, +, a, \leq\}$, $C = \{0, s, \text{true}, \text{false}\}$.

R:

$$\begin{array}{ll} x + 0 \to x & a(0, y) \to s(y) \\ x + s(y) \to s(x + y) & a(s(x), 0) \to a(x, s(0)) \\ 0 \leq y \to \text{true} & a(s(x), s(y)) \to a(x, a(s(x), y)) \\ s(x) \leq 0 \to \text{false} & \\ s(x) \leq s(y) \to x \leq y & \end{array}$$

$e \equiv s(x + y) \leq a(x, y)$

Behauptung

e gilt in $\mathcal{I}(\text{spec})$.

Es gelten folgende Lemmata in $\mathcal{I}$ (o. Beweis)

L1: $0 + y = y$
L2: $s(x) + y = s(x + y)$
L3: $x + (y + z) = (x + y) + z$
L4: $x \leq y = \text{true}, y \leq z = \text{true} \Rightarrow x \leq z = \text{true}$
L5: $x \leq y = \text{true} \Rightarrow s(x) \leq s(y) = \text{true}$
L6: $x \leq y = \text{true} \Rightarrow z + x \leq z + y = \text{true}$
L7: $x \leq x = \text{true}$

Es gilt

$$\begin{aligned} C_a = \{ & \langle (0, y), \varnothing, \varnothing \rangle, \langle (s(x), 0), \{x, s(0)\}, \varnothing \rangle, \\ & \langle (s(x), s(y)), \{(x, a(s(x), y)), (s(x), y)\}, \varnothing \rangle \} \end{aligned}$$

Ein Beweis zur Ackermann-Funktion (2)

Das Coverset C_a liefert die **Teilziele** (ohne „= true")

1. $\Rightarrow s(0+y) \leq a(0,y)$
2. $s(x+s(0)) \leq a(x,s(0)) \Rightarrow s(s(x)+0) \leq a(s(x),0)$
3. $s(s(x)+y) \leq a(s(x),y)$,
   $s(x+a(s(x),y)) \leq a(x,a(s(x),y))$
   $\Rightarrow s(s(x)+s(y)) \leq a(s(x),s(y))$

Zu 1. Umschreiben mit R und L1 liefert
$\Rightarrow s(y) \leq s(y)$
Dies gilt in $\mathcal{I}$.

Zu 2. Umschreiben mit R und L2 liefert
$s^2(x) \leq a(x,s(0)) \Rightarrow s^2(x) \leq a(x,s(0))$
Dies gilt in $\mathcal{I}$.

Zu 3. Umschreiben mit R und L2 liefert
$s^2(x+y) \leq a(s(x),y)$,
$s(x+a(s(x),y)) \leq a(x,a(s(x),y))$
$\Rightarrow s^3(x+y) \leq a(x,a(s(x),y))$

Die Behauptung folgt mit den Lemmata L1-L7 aus der Voraussetzung.

Ein Beweis zur Ackermann-Funktion (3)

Sei
$s^2(x+y) \leq a(s(x),y)$
$s(x+a(s(x),y)) \leq a(x,a(s(x),y))$

Dann

$x+s^2(x+y) \leq x+a(s(x),y)$	nach L6
$s(x+s^2(x+y)) \leq s(x+a(s(x),y))$	nach L5
$s(x+s^2(x+y)) \leq a(x,a(s(x),y))$	nach L4
$s^3(x+(x+y)) \leq a(x,a(s(x),y))$	nach R
$x+y \leq x+(x+y)$	nach L6 und R
$s^3(x+y) \leq s^3(x+(x+y))$	nach L5
$s^3(x+y) \leq a(x,a(s(x),y))$	nach L4

Beachte
Im Beweis zu e

- sind die Variablen in e „beliebig aber fest",
- können Lemmata mit beliebiger Instanziierung der Variablen benutzt werden.