Beispiel zu $\mathcal{T}(\text{spec})$ (Forts.)

c) $\mathcal{B} = (\{0,1,2\}, \{0^\mathcal{B}, s^\mathcal{B}, +^\mathcal{B}, *^\mathcal{B}\})$
mit

$$\begin{array}{ll} 0^\mathcal{B} = 0 & n +^\mathcal{B} m = n + m \bmod 3 \\ s^\mathcal{B}(n) = n + 1 \bmod 3 & n *^\mathcal{B} m = n \cdot m \bmod 3 \end{array}$$

Es gilt $\mathcal{B} \in \text{Mod}(\text{spec})$, aber $\mathcal{B}$ ist nicht initial in Mod(spec).
Denn: Es gibt keinen sig-Homomorphismus $\varphi : \mathcal{B} \to \mathcal{A}$.
Sonst gilt in $\mathcal{A}$ (also in $\mathbb{N}$):
$0 = \varphi(0^\mathcal{B}) = \varphi(s^3(0)^\mathcal{B}) = s^\mathcal{A}(\varphi(s^2(0)^\mathcal{B}) = 2 + 1 = 3$
$\lightning$

Standardmodelle

Bezeichnung

$\mathcal{A} \in \text{Mod}(\text{spec})$ heißt ein **Standardmodell** zu spec, falls $\mathcal{A}$ termerzeugt ist.

Frage:

Sei $t_1, t_2 \in \text{Term}(F, V)$.

Wann gilt $t_1 = t_2$ in allen Standardmodellen von spec?

Beachte

a) $\mathcal{A} \models t_1 = t_2$ steht für $\mathcal{A} \models \forall x_1, \ldots, x_n : t_1 = t_2$.
b) Für Grundterme t_1, t_2 gilt: Aus $\mathcal{I}(\text{spec}) \models t_1 = t_2$ folgt $\mathcal{A} \models t_1 = t_2$ für alle $\mathcal{A} \in \text{Mod}(\text{spec})$.
c) Vermutung: Gilt $\mathcal{I}(\text{spec}) \models \sigma(t_1) = \sigma(t_2)$ für alle $\sigma \in \text{GSub}(t_1 = t_2)$, so gilt $\mathcal{A} \models t_1 = t_2$ für alle Standardmodelle $\mathcal{A}$.

Bezeichnung

$\text{GSub}(t_1 = t_2) = \{\sigma \mid \sigma(x) \in \text{Term}(F) \text{ für alle } x \in \text{Var}(t_1, t_2)\}$.

Gültigkeit in allen Standardmodellen (1)

Sei $\text{spec} = (\text{sig}, E), \text{sig} = (S, F, \alpha)$.

Erinnerung

Eine Evaluierungsfunktion zur sig-Algebra $\mathcal{A}$ ist $\text{eval} : V \to A$, fortgesetzt zu $\text{eval} : \text{Term}(F, V) \to A$.

$\mathcal{A} \models t_1 = t_2$ gdw $\text{eval}(t_1) = \text{eval}(t_2)$ in $\mathcal{A}$ für alle eval.

Lemma 2.5

Sei $\mathcal{I} = \mathcal{I}(\text{spec})$.

a) Zu jedem $\text{eval} : V \to I$ gibt es eine Grundsubstitution σ_{eval} mit $\text{eval}(t) = [\sigma_{\text{eval}}(t)]$ für alle $t \in \text{Term}(F, V)$.

b) Zu jeder Grundsubstitution σ gibt es ein $\text{eval}_\sigma : V \to I$ mit $\text{eval}_\sigma(t) = [\sigma(t)]$ für alle $t \in \text{Term}(F, V)$.

Beweis-Idee:

a) Sei $\text{eval}(x) = [t_x], t_x \in \text{Term}(F)$. Setze $\sigma(x) = t_x$.

b) Setze $\text{eval}_\sigma(x) = [\sigma(x)]$.

Induktion über den Aufbau von t liefert die Behauptung.

Gültigkeit in allen Standardmodellen (2)

Satz 2.4.

Für alle $s, t \in \text{Term}(F, V)$ sind äquivalent.

1. $s = t$ ist gültig in $\mathcal{I} = \mathcal{I}(\text{spec})$.
2. $\sigma(s) =_E \sigma(t)$ für alle $\sigma \in \text{GSub}(s = t)$.
3. $s = t$ ist gültig in allen Standardmodellen $\mathcal{A}$ von spec.

Beweis:

1. $\leadsto$ 2.:

Sei $\sigma \in \text{GSub}(s = t)$. Nach Lemma 2.5 gibt es eval_σ mit $[\sigma(s)] = \text{eval}_\sigma(s)$ und $\text{eval}_\sigma(t) = [\sigma(t)]$. Wegen $\mathcal{I} \models s = t$ gilt $\text{eval}_\sigma(s) = \text{eval}_\sigma(t)$, also $[\sigma(s)] = [\sigma(t)]$, also $\sigma(s) =_E \sigma(t)$.

3. $\leadsto$ 1.:

Dies ist trivial, da $\mathcal{I}$ ein Standardmodell ist.

Gültigkeit in allen Standardmodellen (3)

2. $\rightsquigarrow$ 3.:

Sei $\mathcal{A}$ Standardmodell und eval : $V \to A$.

Zu zeigen ist eval$(s) =$ eval(t) in $\mathcal{A}$.

Es gibt $t_x \in$ Term(F) mit eval$(x) = t_x^{\mathcal{A}}$. Sei $\sigma \in$ GSub$(s = t)$ gegeben durch $\sigma(x) = t_x$.

a) Es gilt stets eval$(t_0) = \sigma(t_0)^{\mathcal{A}}$ (Induktion über t_0).

b) Aus $t_1^{\mathcal{I}} = t_2^{\mathcal{I}}$ und $t_1, t_2 \in$ Term(F) folgt stets $t_1^{\mathcal{A}} = t_2^{\mathcal{A}}$ (nach Lemma 2.1).

c) Aus $\sigma(s) =_E \sigma(t)$ folgt $[\sigma(s)] = [\sigma(t)]$,
also $\sigma(s)^{\mathcal{I}} = \sigma(t)^{\mathcal{I}}$, also $\sigma(s)^{\mathcal{A}} = \sigma(t)^{\mathcal{A}}$ nach b).

d) Nach Voraussetzung gilt $\sigma(s)^{\mathcal{A}} = \sigma(t)^{\mathcal{A}}$ wegen c),
also folgt eval$(s) = \sigma(s)^{\mathcal{A}} = \sigma(t)^{\mathcal{A}} =$ eval(t).

Also (Ergebnis über Standardmodellen)

Die Gültigkeit von $s = t$ in $\mathcal{I}$(spec) impliziert die Gültigkeit von $s = t$ in allen Standardmodellen.

2.2 Hilfsmittel für Beweise in der induktiven Theorie

Problem

Gegeben: spec $=$ (sig, E), $s = t$.

Frage: Gilt $\mathcal{I}$(spec) $\models s = t$?

Definition 2.8

ITh(spec) $= \{s = t \mid \mathcal{I}$(spec) $\models s = t\}$ heißt die **induktive Theorie** zu spec.

Beachte

Sei $\mathcal{I} = \mathcal{I}$(spec).

a) Es gilt $\mathcal{I} \models s = t$ gdw $\sigma(s) =_E \sigma(t)$ für alle $\sigma \in$ GSub$(s = t)$. Dies ist i. Allg. ein unendlicher Test.

b) Induktion hilft häufig, den Test endlich zu machen. Daher der Name „induktive Theorie“.

Hier

Hilfsmittel entwickeln, um Beweise einfacher zu gestalten.

spec-Konstruktoren (1)

Sei $\quad \text{spec} = (\text{sig}, E), \text{sig} = (S, F, \alpha)$.

Beachte

Es gibt verschiedene Definitionen von Konstruktor.

1. Ansatz: Man zeichnet $C \subseteq F$ aus, nennt die $f \in C$ Konstruktoren und definiert auf der „Datenmenge“ $\text{Term}(C)$ Funktionen $g \in F - C$.

2. Ansatz: Man wählt $C \subseteq F$ möglichst klein, so dass jeder F-Grundterm E-gleich zu einem C-Grundterm ist.

Also

Sind alle $g \in F - C$ total definiert, so stimmen beide Ansätze überein.

Hier

Wir wählen den 2. Ansatz.

Definition 2.9

$C \subseteq F$ heißt eine **Konstruktormenge** zu $\text{spec} = (\text{sig}, E)$, falls zu jedem $t \in \text{Term}(F)$ ein $t' \in \text{Term}(C)$ existiert mit $t =_E t'$.
C heißt **frei**, falls für alle $t_1, t_2 \in \text{Term}(C)$ gilt: $t_1 =_E t_2 \text{ gdw } t_1 \equiv t_2$.

spec-Konstruktoren (2)

Frage

Wie findet man eine sinnvolle Konstruktormenge?

Lemma 2.6

Sei $\text{spec} = (\text{sig}, R)$ terminierend. Gilt $t \in \text{Term}(C)$ für jeden irreduziblen Term $t \in \text{Term}(F)$, so ist C eine Konstruktormenge.

Beweis: klar.

Also

Sei R terminierend und grundkonfluent und sei
$\text{Irr}(R) = \{t \in \text{Term}(F) \mid t \text{ irreduzibel}\}$. Sei $C \subseteq F$ minimal mit $\text{Irr}(R) \subseteq \text{Term}(C)$. Dann ist C eine minimale Konstruktormenge.
Für $t_1, t_2 \in \text{Irr}(R)$ gilt $t_1 =_R t_2 \text{ gdw } t_1 \equiv t_2$.

Gilt also $\text{Irr}(R) = \text{Term}(C)$, so ist C eine Menge von freien Konstruktoren.

Beispiele

1. Beispiel

$F = \{0, s, +, -\}$.

R: (1) $x + 0 \to x$ (3) $x - 0 \to x$
(2) $x + s(y) \to s(x + y)$ (4) $0 - y \to 0$
(5) $s(x) - s(y) \to x - y$

Sei spec $=$ (sig, R). Dann ist R konvergent und $C = \{0, s\}$ ist Menge von freien Konstruktoren.

Sei R' das System R ohne (4) und spec$' =$ (sig, R'). Dann ist $t \equiv (0 - s(0)) + (0 - s(0))$ irreduzibel, also F die kleinste Konstruktormenge. Sie ist nicht frei.

2. Beispiel

$F = \{0, s, \mathsf{nil}, ., \mathsf{app}, \mathsf{rev}\}$.

R: $\mathsf{app}(\mathsf{nil}, l_2) \to l_2$ $\mathsf{app}(x.l_1, l_2) \to x.\mathsf{app}(l_1, l_2)$
$\mathsf{rev}(\mathsf{nil}) \to \mathsf{nil}$ $\mathsf{rev}(x.l) \to \mathsf{app}(\mathsf{rev}(l), x.\mathsf{nil})$

Sei spec $=$ (sig, R). Dann ist R konvergent und $C = \{0, s, \mathsf{nil}, .\}$ eine Menge von freien Konstruktoren.

Verwendung von Konstruktormengen

Sei spec $=$ (sig, E), sig $= (S, F, \alpha)$ und $C \subseteq F$.

Definition 2.10

σ heißt eine **C-Substitution**, falls $\sigma(x) \in \mathsf{Term}(C, V)$ für alle $x \in V$.

Sei C-GSub$(s = t) = \{\sigma \mid \sigma(x) \in \mathsf{Term}(C)$ für alle $x \in \mathsf{Var}(s, t)\}$.

Satz 2.5.

Sei $\mathcal{I} = \mathcal{I}(\text{spec})$, $s, t \in \mathsf{Term}(F, V)$ und C eine Konstruktormenge. Es gilt $\mathcal{I} \models s = t \text{ gdw } \sigma(s) =_E \sigma(t)$ für alle $\sigma \in C$-GSub$(s = t)$.

Beweis:

„$\curvearrowright$“ klar, wegen Satz 2.4.

„$\curvearrowleft$“ Sei $\tau \in$ GSub$(s = t)$. Es gibt $\sigma \in C$-GSub$(s = t)$ mit $\sigma(x) =_E \tau(x)$ für alle $x \in \mathsf{Var}(s, t)$, da C Konstruktormenge.

Also $\tau(s) =_E \sigma(s) =_E \sigma(t) =_E \tau(t)$.

Also $\mathcal{I} \models s = t$, wegen Satz 2.4.

Berechnung einer Konstruktormenge

Sei spec $=$ (sig, R), sig $= (S, F, \alpha)$.

Ziel wegen Satz 2.5:

Berechnung einer **kleinen** Konstruktormenge.

Lemma 2.7

Berechne $C_0, C_1, \dots \subseteq F$ so

$C_0 = \{c \mid c \in F$ ist irreduzible Konstante$\}$.

$C_{i+1} = C_i \cup \{f \in F - C_i \mid$ es gibt $t_1, \dots, t_n \in \mathrm{Term}(C_i)$,
so dass $f(t_1, \dots, t_n)$ irreduzibel$\}$.

Es gibt $k \in \mathbb{N}$ mit $C_k = C_{k+1}$. Sei $C = C_k$, dann ist $C = C_i$ für alle $i \geq k$. Ist R terminierend, so ist C eine Konstruktormenge zu spec.

Beweis:

Wegen $C_0 \subseteq C_1 \subseteq \cdots \subseteq F$ und F endlich gibt es solch ein k. Es gilt $t \in \mathrm{Term}(C)$, falls $t \in \mathrm{Term}(F)$ irreduzibel ist (Induktion nach $>_{TT}$).

Also: Zu jedem $t \in \mathrm{Term}(F)$ gibt es $t' \in \mathrm{Term}(C)$ mit $t \xrightarrow{*} t'$.

Also: C ist Konstruktormenge, falls R terminierend ist.

Bemerkung/Beispiel

Bezeichnung

$C = C_R$ aus Lemma 2.7 heißt die durch R definierte Konstruktormenge.

Beispiel

$F = \{0, s, +, -\}$.

R: (1) $x + 0 \to x$ (3) $x - 0 \to x$
(2) $x + s(y) \to s(x + y)$ (4) $0 - y \to 0$
(5) $s(x) - s(y) \to x - y$

a) Sei spec $=$ (sig, R). Es ergibt sich
$C_0 = \{0\}$ $C_1 = \{0, s\} = C_2$ Also $C = \{0, s\}$.

b) R' sei R ohne (4). Sei spec$'$ $=$ (sig, R').
Es ergibt sich
$C_0 = \{0\}$, $C_1 = \{0, s\}$, $C_2 = \{0, s, -\}$,
$C_3 = \{0, s, -, +\} = F$.
Also gilt $C = F$.

Beachte

R definiert $+$ und $-$ total (über $\mathrm{Term}(C)$).

Beispiel für nicht freie Konstruktoren

Sei $S = \{\mathsf{INT}\}$, $F = \{0, s, p, +, -\}$.

$$
\begin{array}{lll}
R\text{:} & s(p(x)) \to x & x + 0 \to x \\
 & p(s(x)) \to x & x + s(y) \to s(x+y) \\
 & & x + p(y) \to p(x+y) \\
 & x - 0 \to x & \\
 & x - s(y) \to p(x-y) & \\
 & x - p(y) \to s(x-y) &
\end{array}
$$

spec $= (\mathsf{sig}, R)$.

Es gilt

$C = \{0, s, p\}$ ist die von R definierte Konstruktormenge.

C ist nicht frei, denn es gilt z. B. $p(s(0)) =_R s(p(0))$.

Verwendung von Lemmata

Sei spec $= (\mathsf{sig}, E)$.

Definition 2.11

$s = t \in ITh(\text{spec})$ heißt ein **Lemma** zu spec.

Lemma 2.8

Gilt $L \subseteq ITh(\text{spec})$ und spec$' = (\mathsf{sig}, L \cup E)$, so gilt $ITh(\text{spec}) = ITh(\text{spec}')$.

Beweis:

„$\subseteq$“: Sei $s = t \in ITh(\text{spec})$. Dann gilt für alle $\sigma \in \mathsf{GSub}(s = t)$ $\sigma(s) =_E \sigma(t)$, also auch $\sigma(s) =_{E \cup L} \sigma(t)$.

Also gilt $s = t \in ITh(\text{spec}')$.

„$\supseteq$“: Sei $s = t \in ITh(\text{spec}')$, $\sigma \in \mathsf{GSub}(s = t)$, also $\sigma(s) =_{E \cup L} \sigma(t)$. Jeder Beweisschritt $\tau(u) \vdash\!\!\!\longrightarrow\!\!\dashv \tau(v)$ mit $u = v \in L$ in diesem Beweis kann ersetzt werden durch den Beweis zu $\tau(u) =_E \tau(v)$. Also gilt $\sigma(s) =_E \sigma(t)$.

Also: $s = t \in ITh(\text{spec})$.

Zusammenfassung

Satz 2.6.

Sei spec $=$ (sig, E), sig $= (S, F, \alpha)$, $C \subseteq F$ eine Konstruktormenge und $L \subseteq ITh$(spec) eine Menge von Lemmata zu spec.

Gibt es zu jedem $\sigma \in C$-GSub$(s = t)$ einen Beweis zu $\sigma(s) =_{E \cup L} \sigma(t)$, so gilt $s = t \in ITh$(spec).

Beweis: Dies folgt aus Satz 2.5 und Lemma 2.8.

Beachte

Beide Prinzipien sind von entscheidender Wichtigkeit für das induktive Beweisen:

1. Verwendung von Konstruktoren: Dies schränkt die zu betrachtenden σ ein.
2. Verwendung von Lemmata: Dies hilft beim Beweisen von $\sigma(s) =_E \sigma(t)$.

Ein Beispiel

Sei spec $=$ (sig, R), $S = \{$NAT$\}$, $F = \{0, s, +\}$.

$R : x + 0 \to x \qquad x + s(y) \to s(x + y)$

Beh.: $x + y = y + x \in ITh$(spec).

Es gilt $C = \{0, s\}$ ist eine Konstruktormenge.

Beweis-Prinzip

Induktion über den Aufbau von $\sigma(x)$ bzw. $\sigma(y)$.

Lemmata

$L1 : 0 + y = y \qquad L2 : s(x) + y = s(x + y)$