

Kapitel 3b

Termalgebren

3.1 Formeln

3.2 Boolesche Algebra

3.3 Algebraische Strukturen
und Algebren

3.4 Abbildungen zwischen Algebren

3.5 Termalgebren

3.6 Termalgebren mit Variablen

3.7 Termersetzungssysteme



▪ Gegeben:

- Signatur Σ (also Menge von Operationen $\Sigma = \underbrace{\Sigma^{(0)}}_{\text{Konst.}} \cup \Sigma^{(1)} \cup \Sigma^{(2)} \cup \dots$)
- Elementaroperanden X
- Menge \mathcal{T} der korrekten Terme zu Σ und X
- Menge von Gesetzen (bzw. Axiome) Q , die bedeutungstreue Umformungen $f \rightarrow f'$ ($f, f' \in \Sigma$) definieren

Beispiele: die Halbgruppen- und Monoidgesetze HG1, HG2 (nur bei kommutativen HG), die Gesetze V1-V10 der booleschen Algebra

Das Tripel $\mathcal{A} = (\mathcal{T}, \Sigma, Q)$ bildet eine algebraische Struktur, man spricht auch von einer Abstrakten Algebra. Dabei gilt für zwei Terme $t, t' \in \mathcal{T}$: $t = t'$ gdw. t nach den Gesetzen Q in t' umgeformt werden kann.

Beispiele:

- Halbgruppen, Monoide, Verbände, Gruppen, Ringe, Körper, Vektorräume, boolesche Algebren
- alle Datenstrukturen der Informatik (abstrakte Datentypen)



Sei gegeben:

- $\Sigma = (S, F)$ eine Signatur
- $X = (\Sigma_{\varepsilon, s})$, $s \in S$ Familie der zur Signatur gehörigen Elementaroperanden

Grundterm der Sorte $s \in S$:

Term der Sorte s , wobei alle Elementaroperanden nur zur Signatur gehören (d.h. $X_s = \Sigma_{\varepsilon, s}$) für alle Sorten $s \in S$.

Notation: $G_0(\Sigma)$ ist die Menge aller Grundterme über der Signatur Σ .

Beispiel: Betrachte Signatur Σ mit Sorte \mathbb{N} und den Operationen

$$0: \quad \rightarrow \mathbb{N}$$

$$\text{succ}: \mathbb{N} \rightarrow \mathbb{N}$$

Dann ist $G_0(\Sigma) = \{0, \text{succ}(0), \text{succ}(\text{succ}(0)), \dots\}$

*Zusätzliche
Axiome ?*
↓

Grundtermalgebra (initiale Algebra): Σ -Algebra $G = (G_0(\Sigma), \emptyset)$

In der Informatik sind fast alle freien Algebren initiale Algebren



Satz: Sei $\Sigma = (S, F)$ eine Signatur und $\mathcal{A} = (\mathcal{I}, \Phi)$ eine Σ -Algebra. Dann existiert ein Homomorphismus $h: G_0(\Sigma) \rightarrow \mathcal{A}$.

Beweis:

- alle Konstanten $c \in \Sigma_0$ gehören zu \mathcal{I} , da \mathcal{A} Σ -Algebra
- alle Terme $t = f(t_1, \dots, t_n) \in G_0(\Sigma)$ gehören zu \mathcal{I}
- definiere $h: G_0(\Sigma) \rightarrow \mathcal{I}$ durch $h(t) = t$ (Identität)
- es gilt $h(t) = h(t')$, wenn in \mathcal{A} gilt $t = t'$ nach den Gesetzen Φ
 - h induziert eine Äquivalenzrelation \equiv in $G_0(\Sigma)$
- Anwendung des Homomorphiesatzes liefert das Ergebnis
 - $i_h(G_0(\Sigma)/\equiv) = \text{Bild}(h)$ ist Unter algebra von \mathcal{A}

- Einsicht: \mathcal{A} kann nur dann mehr Elemente als $\text{Bild}(h)$ umfassen, wenn es in \mathcal{A} Konstante gibt, die nicht Bild von Konstanten in $G_0(\Sigma)$ sind



- Gegeben sei eine Grundtermalgebra $G_0(\Sigma)$ und ein Homomorphismus $h: G_0(\Sigma) \rightarrow \mathcal{A}$ in eine Σ -Algebra \mathcal{A}

$$t, t', t'', \dots$$

$$h(t) = h(t') = h(t'')$$

- Fragen:

- Gibt es in $G_0(\Sigma)/\equiv$ in jeder Äquivalenzklasse $[t] = h(t)$ ein eindeutig bestimmtes Element t_0 , die **Normalform** von $[t]$, so, dass man jedes $t' \in [t]$ systematisch auf t_0 abbilden kann, um so die Äquivalenzklasse von t' zu ermitteln?
- Kann man die Normalform sogar so festlegen, dass für alle Operationen $\sigma \in \Sigma$ gilt: $\sigma(t_1, \dots, t_n) = t$ führt Normalformen t_1, \dots, t_n in die Normalform t des Ergebnisses über? Man spricht dann von **kanonischer Normalform**.
- Ist es bei der Anwendung von Operationen σ, τ, \dots zur Berechnung der Normalform gleichgültig, in welcher Reihenfolge die Operationen angewandt werden?
 - lautet die Antwort ja, so sagt man, die Algebra \mathcal{A} habe die **Church-Rosser-Eigenschaft** oder die Anwendung der Operationen sei **konfluent**



2.3 Noethersche Induktion

5/25

Ziel: Beweis von Aussagen über fundierte Halbordnungen

$$X_n = \{1, \dots, n\}$$

$$X_0 = \{1, \dots, 0\} = \emptyset$$

Sei (U, \leq) fundierte Halbordnung und $<$ zugehörige strenge Halbordnung.

Behauptung: Aussage $P(x)$ ist wahr, falls gilt:

z. zeigen $\left\{ \begin{array}{l} \text{Wenn } P(z) \text{ wahr für } \underline{\text{alle}} \ z < y, \text{ dann ist } P(y) \text{ wahr.} \\ \text{Induktionsschleife} \end{array} \right.$

Beweis: Sei $U_P = \{x \in U \mid P(x) \text{ wahr}\}$

Annahme: $M = U \setminus U_P \neq \emptyset$

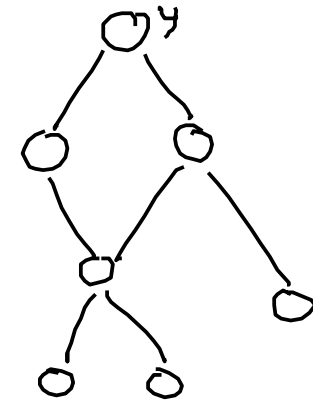
\Rightarrow Es gibt minimales Element $m \in M$, weil (U, \leq) fundiert ist

$\Rightarrow P(m)$ ist falsch, weil $m \in M$

$\Rightarrow P(z)$ ist wahr für alle $z \in U$ mit $z < m$, weil m minimal in M ist

$\Rightarrow P(m)$ ist wahr - **Widerspruch!**

Beobachtung: $P(y)$ muß auch gelten, wenn $\{z \in U \mid z < y\} = \emptyset$



- gegeben sei eine Termalgebra $\mathcal{A} = (\mathcal{T}, \Phi)$ zur Signatur Σ
 - jeder Term $t \in \mathcal{T}$ ist
 - entweder eine Konstante $t = k$
 - oder entsteht aus Konstanten durch sukzessive Anwendung von Operationen $f \in \Sigma$ auf einfachere Terme t_i : $t = f(t_1, \dots, t_n)$
 - „einfacher“: die t_i enthalten weniger Funktionsanwendungen als t
 - **Halbordnung auf \mathcal{T} : $t' \leq t$, wenn der Term t' als Operand in t vorkommt:**
 - $t' = t$
 - oder $t = f(\dots, t', \dots)$
 - oder (transitive Hülle) $t = f(\dots, t'', \dots)$ und t' ist Operand von t''
- $t' < t'' < t''' \dots < t$
endliche Kette
- Ein Term t enthält nur endlich viele Funktionsanwendungen (sonst könnte man ihn nicht hinschreiben)
 - wenn $t' \leq t$, dann ist t' einfacher als t
 - also: **die Halbordnung der Terme ist artinsch (und daher fundiert)**: jede absteigende Kette $\dots \leq t'' \leq t' \leq t$ bricht nach endlich vielen Schritten ab



Satz (Prinzip der strukturellen Induktion):

Sei $\Sigma = (S, F)$ eine Signatur, \mathcal{A} eine Σ -Termalgebra mit Konstanten X .
Alle korrekten Terme $t \in \mathcal{T}$ besitzen die Eigenschaft $P(t)$, wenn gilt:

- ind. Vor-
ansetzung
- $P(k)$ gilt für alle Konstanten $k \in X$
- induktive-
Schritt
- Für alle Operationen $f: s_1 \times \dots \times s_n \rightarrow s$ gilt:
Wenn $P(t_1), \dots, P(t_n)$ für $t_1, \dots, t_n \in \mathcal{T}$ gilt, dann gilt auch $P(f(t_1, \dots, t_n))$

Beweis: Anwendung noetherscher Induktion auf die fundierte Halbordnung der Terme

- $$a \vee (\neg b \wedge c) \vee F$$
1. Beweis für a, b, c, F
 2. Beweise: falls Eigenschaft für Operanden gilt, dann auch für Ergebnis von \vee, \wedge, \neg



Beispiel: Betrachte Quotientenalgebra zu

▪ Signatur:

• 0: $\rightarrow \mathbb{N}$

• succ: $\mathbb{N} \rightarrow \mathbb{N}$

• plus: $\mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$

▪ Axiome:

• P1: $\text{plus}(m, 0) = m$

• P2: $\text{plus}(n, \text{succ}(m)) = \text{succ}(\text{plus}(n, m))$

▪ Es gibt Homomorphismus in das Monoid der natürlichen Zahlen.

Gilt auch in der Quotientenalgebra das Assoziativgesetz ?



Ausgangspunkt:

Sei $\mathcal{T} = (\Sigma, \rightarrow)$ Semi-Thue-System, so daß \Rightarrow^* azyklisch

Beispiele:

(modifizierte Kaffeedose)

+ | \rightarrow | +

+ \rightarrow ε

schwarz schwarz \rightarrow schwarz

weiß weiß \rightarrow schwarz

weiß schwarz \rightarrow weiß

schwarz weiß \rightarrow schwarz weiß?

- Warum terminieren diese Semi-Thue Systeme?
- Warum ergibt sich bei der Addition immer dasselbe Ergebnis, aber bei der modifizierten Kaffeedose nicht?



Beobachtung:

$\mathcal{T} = (\Sigma, \rightarrow)$ terminiert genau dann für alle $x \in \Sigma^*$,
wenn \Rightarrow^* noethersche Halbordnung ist

$$x \Rightarrow x' \Rightarrow x'' \Rightarrow \dots \Rightarrow X$$

Spezialfall: Reduktion von $w \in \Sigma^*$ auf Z einer anständigen kontextfreien Grammatik $G = (\Sigma, N, P, Z)$

- Produktionen sind terminierend oder rechte Seite ist länger als linke Seite

$$X \rightarrow x$$

$$\begin{array}{l} |x| = 0 \quad \varepsilon \text{ ausgesch.} \\ |x| = 1 \quad \Rightarrow x = a \in \Sigma \\ |x| \geq 2 \end{array}$$

Aber: Endet Semi-Thue-System immer mit demselben Wort?

In einer Halbordnung \leq heißt ein Wort w Normalform eines Worts x ,
wenn es maximal ist, wenn es also kein w' mit $w \leq w'$, $w \neq w'$ gibt.

Also ist jedes Wort w mit dem eine Ableitung $x \Rightarrow^* w$ endet, auf das
also keine weiteren Regeln mehr anwendbar sind, eine Normalform
von x



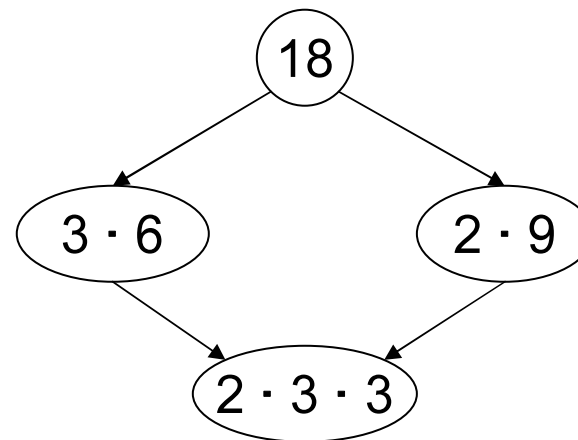
2.3 Beispiel: Faktorzerlegung

11/25

Formales System: $(\{n \in \mathbb{N} \mid n > 1\}, \rightarrow)$ mit

- $n \rightarrow p \cdot q$ genau dann, wenn $n = p \cdot q$ ist
verbunden *mal*
- \Rightarrow^* definiert Halbordnung

Beispiel: Ableitungen von 18:



Beobachtungen:

- alle Wege führen zum selben Ziel (Konfluenz)
- Maximales Element: Primfaktorzerlegung (Normalform)
- Primzahlen selbst sind maximal (irreduzibel)



2.3 Reduktionen bei Grammatiken

12/25

Gegeben: kontextfreie Grammatik $G = (\Sigma, N, P, Z)$

Beobachtung:

- Reduktionsbeziehung \Rightarrow^* ist Halbordnung, wenn nicht $A \Rightarrow^+ A$ gilt.
- Z ist Normalform und $w \in L(G)$ genau dann, wenn $w \Rightarrow^+ Z$

Beispiel:

A	\rightarrow	F A + F	a + a	\Rightarrow	F + a	a + a \Rightarrow	F + a
F	\rightarrow	bez (A)		\Rightarrow	A + a	\Rightarrow	A + a
				\Rightarrow	A + F	\Rightarrow	A + F
				\Rightarrow	A	\Rightarrow	A + A

Problem: Es gibt auch andere Normalformen y von w

- $w \Rightarrow^+ y$ ist eine Sackgasse

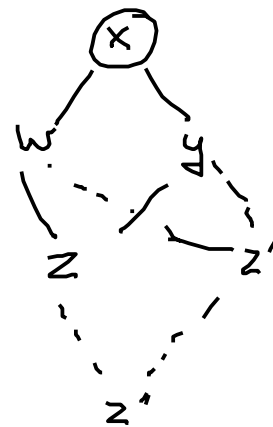
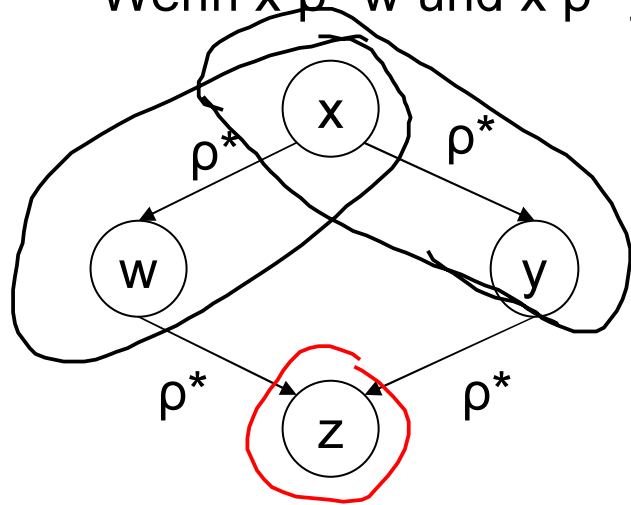


2.3 Konfluenz

13/25

konfluente Relation $\rho \subseteq U \times U$:

Wenn $x \rho^* w$ und $x \rho^* y$, dann gibt es ein z mit $w \rho^* z$ und $y \rho^* z$



Konfluenz: $f(g(h), t)$
Reihenfolge Anw. f, g
gleichgültig

Einsicht: Wenn es für konfluente Relation ρ eine Normalform gibt, dann ist diese eindeutig.

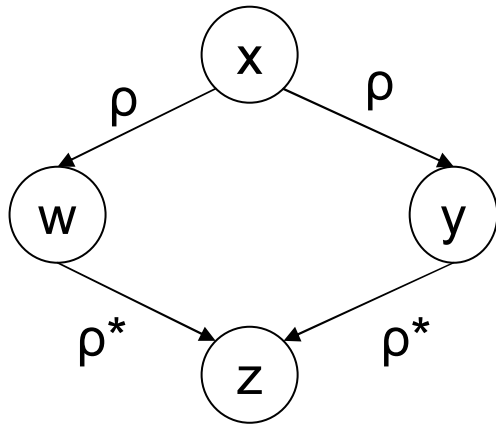
⇒ Noethersche Halbordnung konfluent genau dann, wenn maximales Element einer Kette eindeutig ist.

Problem: Nachweis der Konfluenz erfordert Untersuchung beliebig langer Ketten $x \rho^* w$ und $x \rho^* y$



lokal konfluente Relation $\rho \subseteq U \times U$

Wenn $x \rho w$ und $x \rho y$, dann gibt es ein z mit $w \rho^* z$ und $y \rho^* z$



- Aus Konfluenz folgt lokale Konfluenz
- lokale Konfluenz ist einfacher nachzuweisen

Problem: Reicht lokale Konfluenz aus?



2.3 Diamantenlemma

15/25

(Newman 1942) Eine noethersche Halbordnung (U, ρ) ist genau dann konfluent, wenn sie lokal konfluent ist.

Beweis: „lokal konfluent“ impliziert „konfluent“

Noethersche Induktion auf $\rho^T = \{(x, y) \mid (y, x) \in \rho\}$

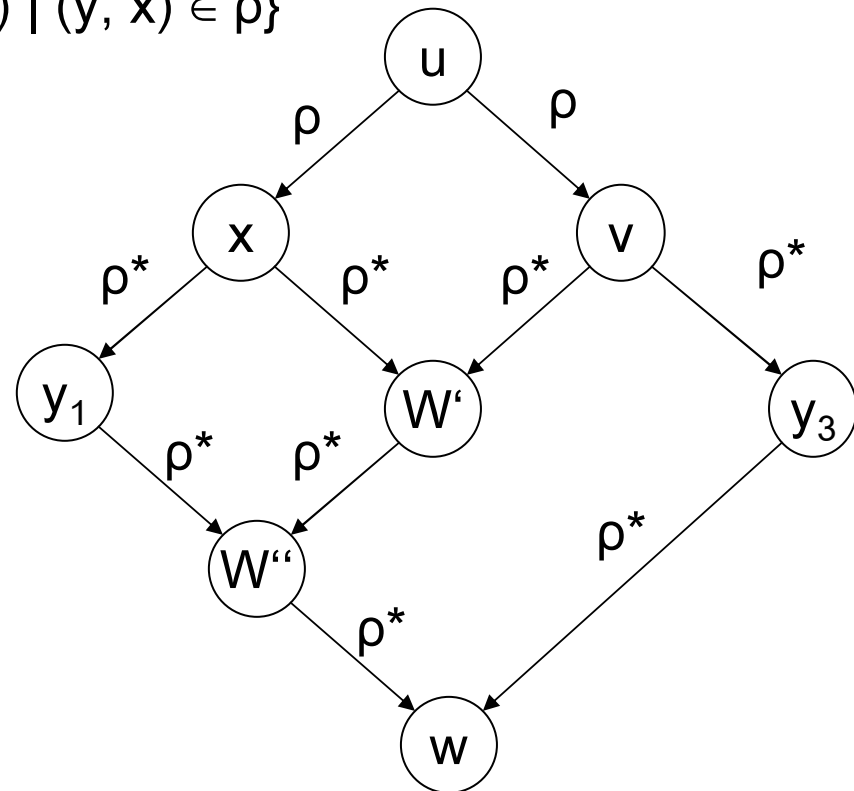
$\Rightarrow \rho^T$ ist artinsch, also fundiert,
weil ρ noethersch ist

Es gelte $y_1 \rho^{T*} u$ und $y_3 \rho^{T*} u$

Zu zeigen:

Es gibt w mit $w \rho^{T*} y_1$

und $w \rho^{T*} y_3$



Beweis (Fortsetzung):

- O.b.d.A. sei $y_1 \neq u$ und $y_3 \neq u$, sonst wähle $w = y_1$ bzw. $w = y_3$
 - ⇒ Es gibt x und v mit $y_1 \rho^T * x \rho^T u$ und $y_3 \rho^T * v \rho^T u$
- ρ ist lokal konfluent
 - ⇒ es gibt w' mit $w' \rho^T * x$ und $w' \rho^T * v$
- Induktionshypothese für x
 - ⇒ Es gibt w'' mit $w'' \rho^T * y_1$ und $w'' \rho^T * w'$
- Induktionshypothese für v (Wege $w'' \rho^T * w' \rho^T * v$ und $y_3 \rho^T * v$)
 - ⇒ Es gibt w mit $w \rho^T * w''$ und $w \rho^T * y_3$
 - ⇒ $w \rho^T * w'' \rho^T * y_1$ und $w \rho^T * y_3$



2.3 Anwendung des Diamantenlemmas

17/25

$+ | \rightarrow | +$

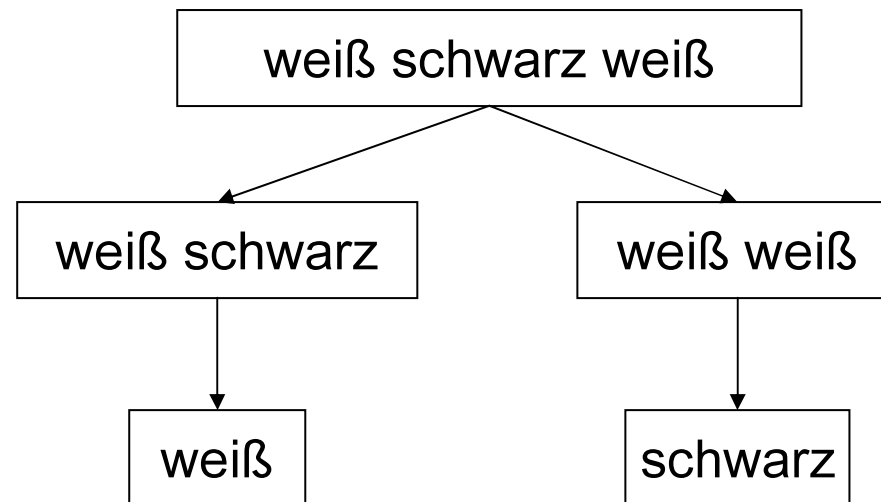
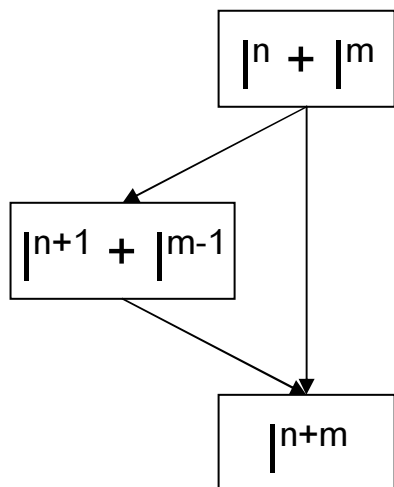
$+ \rightarrow \varepsilon$

schwarz schwarz \rightarrow schwarz

weiß weiß \rightarrow schwarz

weiß schwarz \rightarrow weiß

schwarz weiß \rightarrow schwarz



▪ **Beispiel Keller:**

- Definiere $x \prec y$ genau dann, wenn x aus y durch Anwenden eines der Gesetze K1-K4 entsteht.

⇒ x enthält weniger Operationen als y

⇒ \prec^* ist eine noethersche Halbordnung

▪ \prec^* ist lokal konfluent (Übung)

⇒ Jeder Term der Sorte $\text{stack}(T)$ hat eindeutige **Normalform**, da aufgrund des Diamantenlemmas \prec^* konfluent ist.

⇒ Normalformen der Sorte „Keller“

- enthalten keine der Operationen: `pop`, `top`, `isEmpty`
- haben die Form: `push(...(push(createStack, n_1), ...), n_k)`
- repräsentieren Keller



- Das Beispiel ist leider nicht beliebig verallgemeinerbar:
 - die durch die Gesetze induzierte Ordnungsrelation $x < y$ ist
 - oft nicht noethersch
 - oft nicht konfluent (mehrere oder keine Normalform)
- Beispiele:
 - arithmetische Ausdrücke im Körper der rationalen oder reellen Zahlen
 - Datentypen mit Gesetzen wie Assoziativität, Kommutativität, die die Länge nicht reduzieren



Konstruktoren: Operationen, die in Normalformen vorkommen.

Beispiel: createStack, push

Hilfskonstrukturen: Operationen, die Datenstrukturen verändern, aber nicht in Normalformen vorkommen.

Beispiel: pop

Projektoren: Operationen, die Informationen über eine Datenstruktur berechnen (und ein Ergebnis anderer Sorte liefern)

Beispiel: top, isEmpty



Problem: Terme wie $\text{top}(\text{createStack})$ und $\text{pop}(\text{createStack})$ sind auch Normalformen.

Diese sind jedoch unerwünscht, da in einem leeren Keller kein oberstes Element existiert bzw. entfernt werden kann.

Lösung: Man erklärt top und pop zu partiellen Operationen und die obigen Terme zu einem Fehler \perp (lies: bottom).

Beispiel: Keller

- Ergänze Menge der Axiome um
 - K5: $\text{top}(\text{createStack}) = \perp$
 - K6: $\text{pop}(\text{createStack}) = \perp$

Problem: Sind Werte wie $\text{push}(\perp, 3)$ auch vernünftige Normalformen?

Antwort: Strikte Operationen f erfüllen immer die Gleichung

$$f(\dots, \perp, \dots) = \perp$$

⇒ Wenn alle Operationen strikt sind, dann sind die Normalformen \perp und $\text{push}(\dots(\text{push}(\text{createStack}, n_1), \dots), n_k)$.



Termersetzungsregel $\ell \rightarrow \varkappa$:

ℓ, \varkappa sind Terme gleicher Sorte über einer Signatur Σ mit Variablen V .

Forderung: Alle Variablen, die in ℓ auftreten müssen auch in \varkappa auftreten.

Termersetzungssystem:

Menge \mathcal{E} von Termersetzungsregeln $\ell \rightarrow \varkappa$ über einer Signatur Σ .

Anwendung einer Termersetzungsregel $\ell \rightarrow \varkappa$ auf Term t :

1. finde Unterterm t' von t , der auf ℓ paßt, d.h. es gibt Substitution σ mit $\ell\sigma = t'$.
2. ersetze t' durch $\varkappa\sigma$
(entspricht der Anwendung eines Axioms)

Ableitung $t \Rightarrow^* t'$:

t' entsteht aus t durch Anwendung von Termersetzungsregeln.

Direkte Ableitung $t \Rightarrow t'$:

t' entsteht aus t durch Anwendung genau einer Termersetzungsregel.



Terminaler Term:

- Term t heißt terminal bzgl. des Termersetzungssystem \mathcal{E} , wenn keine weitere Regel mehr angewandt werden kann.

Normalform:

- Menge der terminalen Grundterme zu einem Termersetzungssystem \mathcal{E}
- Einem vorgegebenen Term t wird ein terminaler Term t' als Normalform zugeordnet, falls existent

Sei gegeben:

- Σ eine Signatur
- $\mathcal{A} = (\mathcal{I}, \Sigma, Q)$ eine abstrakte Σ -Algebra
- Q Axiome, dargestellt durch Gleichungen

Beobachtung:

Wenn alle Gleichungen von links nach rechts gerichtet werden, dann entsteht ein Termersetzungssystem \mathcal{E} .



$$t \equiv s \quad t' \equiv s \quad > \quad t \equiv s \equiv t'$$

Eigenschaften von \mathcal{E} :

- Wenn $t \Rightarrow^* t'$, dann ist $t \equiv t'$ bzgl. der Axiome Q.
- Wenn $t \Rightarrow^* s$ und $t' \Rightarrow^* s$, dann ist $t \equiv t'$ bzgl. der Axiome Q.
- Wenn \mathcal{E} noethersch und konfluent, dann Normalformen eindeutig
 $\Rightarrow t \equiv t'$ kann entschieden werden, indem man die Normalformen von t und t' bestimmt und prüft, ob diese identisch sind.

Beobachtung:

Alle diese Überlegungen erfordern nur den Übergang zur Quotiententermalgebra, nicht aber zu einer konkreten Algebra.

\Rightarrow Man kann bereits vor der Realisierung im Rechner prüfen, ob eine Spezifikation das Gewünschte leistet.



- partielle Korrektheit

- R: Termersetzungssystem
A: Termalgebra (Datenstruktur) der Signatur Σ
- Eine Termersetzungsregel $t \rightarrow r$ über der Signatur heißt partiell korrekt bzgl. der Termalgebra A, falls für jede Belegung β in A gilt:

$$I_{\beta}^A[t] = I_{\beta}^A[r]$$

- R heißt partiell korrekt bezüglich A, falls jede Regel partiell korrekt bezüglich A ist
- vollständige oder totale Korrektheit
 - Ein partiell korrektes Termersetzungssystem R heißt total korrekt bezüglich A, wenn
 - für Grundterme t, mit $t^A \neq \perp$, keine nichtterminierenden Berechnungen existieren
 - für bezüglich R terminale, verschiedene Grundterme t_1, t_2 mit $t_1^A \neq \perp$ und $t_2^A \neq \perp$ stets gilt $t_1^A \neq t_2^A$

