

Zusammenfassung des Bisherigen

Ziel ist die Ableitung von Gleichungen aus gegebenen Gleichungen

- Gilt eine Gleichung in der von den gegebenen Gleichungen definierten Theory?

Beispiel: Ist eine bestimmte Gleichung ein Theorem der Gruppentheorie?

- Läßt sich eine Gleichung aus den gegebenen Gleichungen ableiten?

Vorgehen: Erzeugen eines *Termersetzungssystems* (TES) aus den gegebenen Gleichungen, mit dessen Hilfe die zweite – und damit auch die erste – Frage beantwortet werden kann.

Wichtige *Eigenschaften* von Termersetzungssystemen:

- Church-Rosser, Konfluenz, Terminierung, Vollständigkeit, irreduzibler Term, Normalform
- Bedeutung der *Terminierungsordnungen* für den Nachweis der Terminierung

Ein konfluentes, terminierendes, vollständiges Termersetzungssystem liefert eine *Entscheidungsprozedur* für die zu beantwortende Frage.

Vorgehen:

- linke und rechte Seite der zu beweisenden Gleichung werden mit TES auf Normalformen reduziert;
- die Frage, ob die Gleichung gilt, ist dann reduziert auf den Test, ob die beiden Normalformen syntaktisch identisch sind.

(Versuch der) Erzeugung eines solchen TES

- Umwandlung der vorgegebenen Gleichungen in Termersetzungsregeln
- Orientierung der Regeln mit Hilfe einer Termordnung: rechte Seite jeder Regel muss kleiner sein als die jeweilige linke Seite
- (Versuch der) Vervollständigung der Regelmenge mit Hilfe des Knuth-Bendix-Verfahrens:
 - Auffinden von kritischen Paaren, deren Bearbeitung entsprechend den gegebenen Regeln
 - Führt möglicherweise zur Erzeugung neuer Regeln
 - Verfahren terminiert, wenn keine neuen kritischen Paare mehr gefunden werden.

Termersetzung und Algebraische Spezifikation

Einige algebraische Grundbegriffe

Eine (einsortige) *Algebra* ist eine Menge mit Operationen auf der Menge.

Eine mehrsortige Algebra besteht entsprechend aus mehreren Mengen (jeweils eine pro Sorte) und Operationen auf den Mengen.

Eine Σ -*Algebra* ist eine Algebra, deren Operationen der Signatur Σ entsprechen.

D.h. Σ -*Algebren* sind die Strukturen, mit deren Hilfe Interpretationen von Termen und Gleichungen definiert werden.

Wie vorher setzen wir voraus, dass jede der Trägermengen nicht leer ist.

Die Termengen $(T_{\Sigma}^{(S)}(V))_{S \in \Sigma}$ bilden eine Σ -Algebra $T_{\Sigma}(V)$, die *Term-Algebra* zu Σ : die den Operationen zugeordneten Funktionen sind gerade die term-bildenden Operationen.

Für eine *sinnvolle* Signatur Σ , d.h. eine Signatur, die mindestens einen Grundterm für jede Sorte zulässt, bilden auch die Mengen der Grundterme $T_{\Sigma}^{(S)}(\emptyset)$ eine Σ -Termalgebra, die *Grundterm-Algebra* T_{Σ} .

Algebraische Grundbegriffe (2)

Ein Σ -*Homomorphismus* ist eine Abbildung zwischen Σ -Algebren, die die Sorten und Operationen der Signatur respektiert.

Ein Σ -*Isomorphismus* ist ein bijektiver Σ -*Homomorphismus*.

Die zu einer Σ -Algebra \mathcal{A} gehörende Interpretationsfunktion, die Terme auf Elemente der Trägermengen von \mathcal{A} abbildet, ist für jede Variablenbelegung $\mathcal{V} : V \rightarrow \mathcal{A}$ ein Σ -Homomorphismus von $T_\Sigma(V)$ nach \mathcal{A} ; der Homomorphismus ist durch \mathcal{V} und \mathcal{A} eindeutig bestimmt.

Für einen Grundterm t ist das Bild unter dem Homomorphismus bereits durch \mathcal{A} eindeutig bestimmt.

Term-erzeugte Algebren

Satz: Ist Σ eine sinnvolle Signatur, so gilt für die Grundterm-Algebra T_Σ : Zu jeder Σ -Algebra \mathcal{A} gibt es genau einen Homomorphismus von T_Σ nach \mathcal{A} .

(In der Sprache der Kategorientheorie heißt dies, dass T_Σ ein *initiales Objekt* in der Kategorie der Σ -Algebren ist.)

Eine Σ -Algebra \mathcal{A} heißt *term-erzeugt* oder *erreichbar*, wenn es für jedes Element a einer Trägermenge A_S zur Sorte S einen Grundterm $t \in T_\Sigma^{(S)}$ gibt, dessen Interpretation in A_S das Element a ist.

Offensichtlich ist die Grundterm-Algebra T_Σ term-erzeugt.

Satz: Für eine Σ -Algebra \mathcal{A} sind die folgenden Aussagen äquivalent:

- \mathcal{A} ist term-erzeugt.
- Es gibt einen surjektiven Homomorphismus $h : T_\Sigma \rightarrow \mathcal{A}$

Gleichungsspezifizierte Algebren

Die Interpretation einer Σ -Gleichung ist ein *Modell* der Gleichung, wenn die Gleichung unter der Interpretation für *jede* Variablenbelegung erfüllt (d.h. wahr) ist; entsprechend für eine Menge von Gleichungen.

Jeder Interpretation entspricht eine Σ -Algebra (und umgekehrt), somit können wir auch von einer Algebra als einem Modell einer Menge von Gleichungen sprechen.

Eine Signatur Σ zusammen mit einer Menge E von Σ -Gleichungen über Σ kann aufgefasst werden als *Spezifikation* der Klasse derjenigen Algebren, die Modelle für die Gleichungen sind.

Die Spezifikation repräsentiert die *Theorie* der Klasse von Algebren, wobei die Gleichungen die “Axiome” der Theorie darstellen.

Gleichungsspezifizierte Algebren (2)

Beispiele:

- Die bereits angegebenen Gleichungen definieren *Gruppentheorie* als eine gleichungsspezifizierte algebraische Theorie.
- Analog lassen sich viele andere algebraische Strukturen (Theorien) mit Hilfe von Gleichungen spezifizieren.
- Wichtiger für die Informatik sind Spezifikationen von *algebraischen Datenstrukturen* oder *abstrakten Datentypen* (s. später).

Gleichungstheorien

Semantische Folgerung für Gleichungen:

$$E \models s = t \quad s = t \text{ folgt semantisch aus } E$$

d.h. in jedem Modell der Gleichungsmenge E ist auch die Gleichung $s = t$ erfüllt.

$Th(\Sigma, E)$ – Menge der Gleichungen, die aus E semantisch folgen

d.h. die von E definierte “Gleichungstheorie”.

Ist $Alg(\Sigma, E)$ die Klasse aller Σ -Algebren, die die Gleichungen E erfüllen (d.h. aller (Σ, E) -Algebren), dann ist $Th(\Sigma, E)$ die Menge der Gleichungen, die von allen Algebren $\mathcal{A} \in Alg(\Sigma, E)$ erfüllt sind.

Eine Gleichungsspezifikation (Σ, E) definiert in diesem Sinn eine algebraische Gleichungstheorie.

Bemerkung: Die Axiomatisierung einer Gleichungstheorie ist nicht eindeutig; es kann durchaus verschiedene Gleichungsmengen geben, die als Axiome dieselbe Theorie definieren.

Initiale Algebren

Eine Algebra \mathcal{A} heißt *initial* in einer Klasse \mathcal{K} von Algebren, wenn es genau einen Homomorphismus von \mathcal{A} zu jeder Algebra \mathcal{B} in \mathcal{K} gibt.

Aus dieser Eigenschaft ergibt sich, dass alle initialen Algebren einer Klasse isomorph sind; in einer Klasse von Algebren ist die initiale Algebra (sofern sie existiert) ‘bis auf Isomorphie’ eindeutig bestimmt.

Initiale Algebren haben spezifische Eigenschaften:

- Sie sind minimal, d.h. es gibt keine Elemente, deren Existenz nicht durch die Spezifikation gefordert wird (“*no junk*”).
- Es gelten keine Gleichungen, die nicht durch die Spezifikation erzwungen werden; es werden nur so viele Elemente identifiziert wie unbedingt nötig (“*no confusion*”).

Für Spezifikationen ohne Gleichungen bilden die Termalgebren die initialen Algebren; für Spezifikationen mit Gleichungen werden zur Konstruktion von initialen Algebren *Quotienten* gebildet.

Kongruenzen und Quotienten

Σ -Kongruenz \equiv auf T_Σ : Äquivalenzrelation, die mit allen Operationen aus Σ verträglich ist:

Sind $u_i \equiv v_i$ ($1 \leq i \leq n$) und f ein n -stelliges Operationssymbol aus Σ , so ist auch $f(u_1, \dots, u_n) \equiv f(v_1, \dots, v_n)$.

(Genauer: für jede Sorte S gibt es eine Relation \equiv_S , d.h. \equiv ist eine S -indizierte Familie von Relationen)

Quotient \mathcal{A}/\equiv einer Σ -Algebra \mathcal{A} nach einer Kongruenz-Relation \equiv auf \mathcal{A} :
besteht aus Äquivalenzklassen

$$[a]_{\equiv} := \{b \in A \mid b \equiv a\}$$

Ein Quotient wird zu einer Σ -Algebra durch folgende Interpretation der Operationen in Σ :

$$f_{\mathcal{A}/\equiv}([a_1], \dots, [a_n]) := [f_{\mathcal{A}}(a_1, \dots, a_n)]$$

wohldefiniert wegen Kongruenzeigenschaft.

Quotienten und Gleichungsspezifikationen

Die Gleichungen einer Gleichungsspezifikation (Σ, E) definieren eine Kongruenzrelation \equiv_E auf der Term-Algebra $T_\Sigma(V)$ und damit eine Quotientenalgebra $T_\Sigma(V)/\equiv_E$.

Satz: T_Σ/\equiv_E ist initial in der Klasse der (Σ, E) -Algebren.

Satz: Jede term-erzeugte (Σ, E) -Algebra \mathcal{A} lässt sich als Quotient von T_Σ/\equiv_E darstellen, d.h. jede term-erzeugte (Σ, E) -Algebra \mathcal{A} ist isomorph zu einer Quotientenalgebra von T_Σ/\equiv_E .

Aufgrund der Eigenschaften der Termalgebra und der Initialität ergibt sich, dass die Gleichungen, die in allen Algebren einer gleichungsspezifizierten Klasse gelten, genau diejenigen sind, die in der initialen Algebra gelten:

Satz: Für ein beliebige Σ -Grundgleichung e gilt $E \models e$ genau dann, wenn e in T_Σ/\equiv_E gilt.

Für eine Σ -Gleichung e gilt $E \models e$ genau dann, wenn e in $T_\Sigma(V)/\equiv_E$ gilt.

Kalkül für Gleichungslogik

im wesentlichen: Umschreiben der Eigenschaften der Gleichheitsrelation in der Form von Regeln

Reflexivität: (Axiomenschema)

$$x = x$$

Symmetrie:

$$\frac{x = y}{y = x}$$

Transitivität:

$$\frac{x = y \quad y = z}{x = z}$$

Substitutivität:

$$\frac{x = y}{\sigma(x) = \sigma(y)}$$

für jede Substitution σ .

Kalkül für Gleichungslogik (2)

Kongruenz:

Für jedes n -stellige Funktionssymbol f und alle Terme x_i und y_i ($1 \leq i \leq n$):

$$\frac{x_i = y_i \quad (1 \leq i \leq n)}{f(x_1, \dots, x_n) = f(y_1, \dots, y_n)}$$

Ableitbarkeit in diesem Kalkül:

$$E \vdash s = t$$

‘Gleichung $s = t$ ist in dem Kalkül aus der Gleichungsmenge E ableitbar’

Vollständigkeit und Korrektheit

Satz: Die folgenden Aussagen sind äquivalent

1. $E \models s = t$
2. $E \vdash s = t$
3. $s \leftrightarrow_R^* t$, wobei R das aus E entstehende Termersetzungssystem ist.

Beweisidee für die Äquivalenz der Aussagen (2) und (3): Induktion über die Länge der Ableitung.

Nach dem vorhergehenden Satz reicht es für (1) aus zu zeigen, dass die Gleichung $s = t$ in dem initialen Modell erfüllt ist.

Aussage (3) macht die Bedeutung konfluenten TES für Gleichungstheorien explizit.

Erweiterungen der Termersetzung

- *Termersetzung modulo Gleichungen:*
Bestimmte Gleichungen werden speziell behandelt – in der Regel in den Unifikationsprozess integriert.
- *Bedingte Termersetzung:*
Jede Regel ist mit einer Vorbedingung (Anwendbarkeitsbedingung) verbunden.
- *“Narrowing”:*
Verfahren zum Auffinden von *Lösungen* einer oder mehrerer Gleichungen mit Hilfe von Termersetzung.
D.h. es wird nicht versucht nachzuweisen, dass eine gegebene Gleichung in einer Gleichungstheorie liegt, sondern dass eine *Instanz* (= Lösung) einer Gleichung ableitbar ist.

Termersetzung modulo Gleichungen

Termersetzung relativ zu einer Gleichungstheorie: Von der Grundmenge der Gleichungen wird eine (kleine) Teilmenge E abgetrennt, z.B. weil es für sie kein konfluentes TES geben kann (Beispiel: Kommutativität).

Der Rest der Gleichungen wird in ein Regelsystem für “Termersetzung modulo E ” entwickelt.

Wichtigster Fall: AC – Assoziativität und Kommutativität binärer Operationen

In Definitionen (der Konfluenz usw.) wird \doteq durch \approx_E , die von E erzeugte Kongruenz auf Termen, ersetzt.

Termersetzung modulo E : TES R/E

$$s \rightarrow_{R/E} t \quad \text{falls} \quad \begin{array}{l} l \rightarrow r \text{ eine Regel in } R, s \approx_E u, \\ w \text{ Teilterm von } u \text{ mit } w = \sigma(l), \\ t \approx_E u[w \leftarrow \sigma(r)]. \end{array}$$

Termersetzung modulo Gleichungen (2)

D.h. R operiert auf Äquivalenzklassen der Kongruenzrelation, also dem Quotienten $T/\approx_E = \{[t]_{\approx_E} \mid t \in T\}$.

Vereinfachung: Anwendung von \approx_E nur auf zu ersetzenden Teilterm:

$$\begin{aligned} s \rightarrow_{R/E} t \quad & \text{falls } l \rightarrow r \text{ Regeln in } R, \\ & w \text{ Teilterm von } s \text{ mit } w \approx_E \sigma(l), \\ & t \doteq s[w \leftarrow \sigma(r)]. \end{aligned}$$

In allen Fällen ist Matching bzw. Unifikation modulo E (E-Matching, E-Unifikation) erforderlich.

Termersetzungssystem für Aussagenlogik

Umsetzung aussagenlogischer Formeln in Polynome (Zhegalkin 1927), mit “*” für Konjunktion, “+” für exklusives Oder, 1 für “wahr”, 0 für “falsch”.

Kanonisches TES BA:

$$\begin{array}{ll} \neg X & \rightarrow X + 1 \\ X \vee Y & \rightarrow (X * Y) + X + Y \\ X \Rightarrow Y & \rightarrow (X * Y) + X + 1 \\ X * 1 & \rightarrow X \\ X * X & \rightarrow X \\ X * 0 & \rightarrow 0 \\ X + 0 & \rightarrow X \\ X + X & \rightarrow 0 \\ (X + Y) * Z & \rightarrow (X * Z) + (Y * Z) \end{array}$$

Zusätzlich: “*” und “+” sind assoziativ und kommutativ (AC).

Ergibt eindeutige Normalform (modulo AC) für aussagenlogische Formeln. d.h. eine Entscheidungsprozedur für Aussagenlogik.

Bedingte Termersetzung

(*conditional term rewriting*)

Bedingte Gleichung: $C \Rightarrow s = t$

benutzt z.B. bei der Spezifikation von abstrakten Datentypen, funktionalen Programmen

erlauben häufig klarere und knappere Spezifikation als mit einfachen Gleichungen für vorgegebene Signatur ausdrückbarer als einfache Gleichungen

C kann im Prinzip eine beliebige Bedingung (prädikatenlogische Formel) sein, wird aber i.a. auf eine Konjunktion von Gleichungen eingeschränkt:

$$s_1 = t_1 \wedge \dots \wedge s_n = t_n \Rightarrow s = t$$

Bedingte Gleichungen werden wie üblich als implizit universell quantifiziert angesehen.
 \Rightarrow Horn-Klauseln

Bedingte Termersetzung (2)

Operationalisierung eines Systems bedingter Gleichungen:

bedingtes Termersetzungssystem (mit Orientierung $s \rightarrow t$)

Im allgemeinen wird gefordert, dass alle in C oder t vorkommenden Variablen auch in der linken Seite der Regel (d.h. s) vorkommen.

Je nach Art der Auswertung von der Bedingung C ergeben sich unterschiedliche Relationen “ \rightarrow ”

- Falls $s_i = t_i$ als $s_i \leftrightarrow^* t_i$ ausgewertet wird, kann die Relation \rightarrow unentscheidbar werden.
- Alternative Interpretation von $s_i = t_i$: Es gibt ein u_i mit $s_i \rightarrow^* u_i$ und $t_i \rightarrow^* u_i$
 s_i und t_i sind “verbindbar” (*joinable*) – Notation: $s_i \downarrow t_i$

Damit: $u \rightarrow v$ g.d.w. es für eine Regel $s_1 = t_1 \wedge \dots \wedge s_n = t_n \Rightarrow s \rightarrow t$ und einen Teilterm w von u eine Substitution σ gibt, so dass $w \doteq \sigma(s)$, $\sigma(s_i) \downarrow \sigma(t_i)$ (f.a. i),
 $v \doteq u[w \leftarrow \sigma(t)]$.

Bedingte Termersetzung (3)

Bemerkung: Die angegebene Definition für \rightarrow ist rekursive, kann also schon in einem Termersetzungsschritt zu unendlicher Entwicklung führen. Daher wird Existenz einer Simplifikationsordnung $>$ gefordert mit $s > t$, $s > s_i$, $s > t_i$ (f.a. i), was die Relation \rightarrow entscheidbar und das TES terminierend macht.

Bedingtes kritisches Paar: Für zwei bedingte Regeln $C \Rightarrow l_1 \rightarrow r_1$, $D \Rightarrow l_2 \rightarrow r_2$ sei u Teilterm von l_1 , $\sigma := mgu(u, l_2)$.

Mit $v \doteq \sigma(l_1[u \leftarrow r_1])$, $w \doteq \sigma(r_2)$ ist $\sigma(C) \wedge \sigma(D) : (v, w)$ ein bedingtes (oder kontextuelles) kritisches Paar.

Ein bedingtes kritisches Paar $s_1 = t_1 \wedge \dots \wedge s_n = t_n : (v, w)$ ist verbindbar (*joinable*), falls für jede Substitution σ mit $\sigma(s_i) \downarrow \sigma(t_i)$ (f.a. i) auch $\sigma(v) \downarrow \sigma(w)$ gilt.

Satz: Ein terminierendes bedingtes Termersetzungssystem mit einer wie oben angegebenen Simplifikationsordnung ist konfluent genau dann, wenn jedes seiner bedingten kritischen Paare verbindbar ist.

Beispiel für bedingtes Gleichungssystem:

ganze Zahlen mit Nachfolger s , Vorgänger p , Ordnungsrelation $<$.

Regeln:

$$(1) \quad 0 < 0 = F$$

$$(2) \quad 0 < s(0) = W$$

$$(3) \quad s(x) < y = x < p(y)$$

$$(4) \quad p(x_4) < y_4 = x_4 < s(y_4)$$

$$(5) \quad x < y = W \Rightarrow x < s(y) = W$$

$$(6) \quad y_6 < x_6 = F \Rightarrow y_6 < p(x_6) = F$$

$$(7) \quad s(p(x)) = x$$

$$(8) \quad p(s(x)) = x$$

Kritisches Paar mit Regeln (4), (6):

$$p(x_4) < x_6 = F : (x_4 < s(p(x_6)), F)$$

mit Substitution $\{y_6 \leftarrow p(x_4), y_4 \leftarrow p(x_6)\}$

Spezifikation des ggT als bedingtes Gleichungssystem:

$$(0 < 0) = F$$

$$(0 < s(x)) = W$$

$$(s(x) < s(y)) = (x < y)$$

$$(s(x) < 0) = F$$

$$(s(x) - s(y)) = (x - y)$$

$$0 - x = 0$$

$$x - 0 = x$$

Bemerkung: Subtraktion ist *nicht* die normale Integer-Subtraktion!

$$ggT(x, x) = x$$

$$(y < x) = W \Rightarrow ggT(x, y) = ggT(x - y, y)$$

$$(x < y) = W \Rightarrow ggT(x, y) = ggT(x, y - x)$$

Terminierung?

Narrowing

Verfahren, Lösungen von Gleichungen zu finden mit Hilfe von Termersetzung.
D.h. es wird nicht versucht nachzuweisen, dass eine gegebene Gleichung in einer Gleichungstheorie liegt, sondern dass eine Instanz einer Gleichung ableitbar ist.

Beispiel: $x * x = s(0)$ ist nicht ableitbar (allgemein wahr), aber hat eine Lösung $\sigma = \{x \leftarrow s(0)\}$.

Für ein TES R und eine Gleichungsmenge E ist eine Substitution σ eine *Lösung von E bzgl. R* , falls für jede Gleichung $s = t$ in E gilt $\sigma(s) \leftrightarrow_R^* \sigma(t)$.

Das Narrowing-Verfahren kann durch Regeln auf einem Paar (Gleichungsmenge, Substitution) beschrieben werden:

$$(N1) \quad \frac{E \cup \{s = t\}, \tau}{\sigma(E) \cup \{\sigma(s = t[u \leftarrow r])\}}, \sigma \cdot \tau$$

falls u Teilterm von t ist, $l \rightarrow r$ eine Regel aus R , σ MGU von l und u

Narrowing (2)

$$(N2) \quad \frac{E \cup \{s = t\}, \tau}{\sigma(E), \sigma \cdot \tau}$$

falls σ MGU von s und t ist.

Narrowing-Verfahren:

Ausgangssituation: Ausgangsmenge von Gleichungen und identische (= leere) Substitution.

Sukzessive Anwendung (nichtdeterministische Auswahl) einer Regel

Verfahren terminiert, wenn leere Gleichungsmenge erreicht ist: die Substitution ist dann die gewünschte Lösung.

Narrowing (3)

Eine Substitution σ heißt *normalisiert* (bzgl. des TES R), wenn $\sigma(x)$ für jede Variable x in Normalform bzgl. R ist.

Satz (Korrektheit von Narrowing):

(1) Jede mit Narrowing aus $(E, \{\})$ abgeleitete Substitution ist eine Lösung von E bzgl. R .

(2) Ist R konfluent, so lässt sich für jede normalisierte Lösung σ von E bzgl. R mit Narrowing aus $(E, \{\})$ eine Lösungssubstitution τ ableiten, die spezieller als σ ist.

$$\tau \leq \sigma \iff \exists \tau'. \tau = \tau' \cdot \sigma$$

Beispiel für Narrowing

Regeln:

...

$$(2) \quad p(s(x)) \rightarrow x$$

$$(3a) \quad 0 + x \rightarrow x$$

$$(3b) \quad x + 0 \rightarrow x$$

$$(4a) \quad s(x) + y \rightarrow s(x + y)$$

$$(4b) \quad x + s(y) \rightarrow s(x + y)$$

$$(5) \quad 0 * x \rightarrow 0$$

$$(6) \quad s(x) * y \rightarrow y + (x * y)$$

Lösung der Gleichung $x * y = p(x + z)$

mit Regel (6), Subst. $x \leftarrow s(v)$: $y + (v * y) = p(s(v) + z)$

mit Regel (5), Subst. $v \leftarrow 0$: $y + 0 = p(s(0) + z)$

mit Regeln (3b), (4a): $y = p(s(0 + z))$

mit Regeln (3a), (2): $y = z$

Ergebnis-Substitution: $\{x \leftarrow s(0), z \leftarrow y\}$