Vergleich zweier semantischer Ansätze zur Unifikation

Unifikation in primalen Algebren aus monoidal-kommutativer Sicht

von
Martin Leucker

Angefertigt am
Lehr- und Forschungsgebiet für
Theoretische Informatik
bei
Professor Dr.-Ing. Franz Baader

Inhaltsverzeichnis

Kapitel 1

Einleitung

Die Unifikationstheorie beschäftigt sich mit der Frage, ob man in zwei gegebenen Termen s und t die Variablen uniform durch Terme ersetzen kann, so daß s und t *gleich* sind.

Dabei kann unter *gleich* einerseits syntaktische Gleicheit verstanden werden. Man kann aber auch Gleichheit modulo einer Gleichungstheorie $\mathcal{E}$ betrachten, was äquivalent dazu ist, Gleichheit in allen Algebren zu untersuchen, die den Gleichungen aus $\mathcal{E}$ genügen. Schließlich kann man *gleich* aber auch im Sinne von Gleichheit in einer Algebra $\mathcal{A}$ verstehen, das heißt, die betrachteten Terme müssen für alle Belegungen durch Elemente von $\mathcal{A}$ den gleichen Wert ergeben.

Für die Unifikation in Gleichungstheorien können zwei Ansätze zur Lösung von Unifikationsproblemen unterschieden werden. Der erste Ansatz, den man als „syntaktischen Ansatz“ bezeichnen könnte, benutzt in erster Linie die syntaktischen Eigenschaften der Identitäten, die eine Gleichungstheorie erzeugen. Der zweite Ansatz hingegen verwendet die Struktur der Algebren, die den gegebenen Identitäten genügen. Diesen kann man somit als „semantischen Ansatz“ bezeichnen.

Bei monoidalen/kommutativen Theorien (im folgenden monoidal-kommutativ genannt) wird ein semantischer Ansatz verwendet. Ein Unifikationsproblem wird in ein Gleichungssystem über einem Halbring transformiert. Jedes endliche Erzeugendensystem der Lösungsmenge des Gleichungssystems liefert nun einen allgemeinsten Unifikator für das Unifikationsproblem (vgl. Kapitel 5).

Interessiert man sich für Unifikation in primalen Algebren, so ist der syntaktische Ansatz nicht ratsam, da primale Algebren weder unter Verwendung einer festen Signatur noch durch Identitäten definiert werden. Somit ist es nicht verwunderlich, daß Unifikationsverfahren für primale Algebren ([Bü90], [Ni90], [KiRi94]) strukturelle Eigenschaften von primalen Algebren verwenden, das heißt, auch bei primalen Algebren verwendet man den semantischen Ansatz.

Vergleicht man nun Unifikationsalgorithmen für monoidal-kommutative Theorien und primale Algebren, so gewinnt man den Eindruck, daß es hier – über die reine Tatsache, daß beide „semantischer Natur" sind, hinaus – noch weitergehende Parallelen gibt.

Ziel dieser Arbeit ist daher, die Unifikation in primalen Algebren aus der Sicht der monoidal-kommutativer Theorien zu untersuchen, um die Gemeinsamkeiten und Unterschiede genauer herauszuarbeiten.

Es wird sich zeigen, daß die Unifikation in primalen Algebren zwar nicht *äquivalent* zu der Unifikation in monoidal-kommutativen Theorien ist, sich aber hierauf zurückführen läßt.

Nachdem in Kapitel 2 zunächst die in der Arbeit benötigten mathematischen Grundlagen bereitgestellt werden, folgt dann in Kapitel 3 die der jeweiligen Auffassung von *gleich* entsprechenden Begriffe „syntaktischer Unifikator", „$\mathcal{E}$-Unifikator" und „$\mathcal{A}$-Unifikator" definiert. Außerdem wird eine kategorientheoretische Sichtweise der Unifikation vorgestellt. Bisweilen können verschiedene Gleichungstheorien und Algebren hinsichtlich Unifikation identifiziert werden. Um dieses genauer zu formalisieren wird zum Schluß des Kapitels eine Äquivalenzrelation auf Gleichungstheorien und Algebren vorgestellt. Für diese wird gezeigt, daß äquivalente Gleichungstheorien oder Algebren vom gleichen Unifikationstyp sind und wie Unifiaktoren transformiert werden können.

Die Unifikation findet insbesondere im Bereich des *Constraint Solving* eine Anwendung (vgl. [BaaSi94]). Dabei interessiert weniger, durch welche Terme die Variablen von s und t ersetzt werden müssen, damit s und t gleich sind, sondern mehr die Frage, ob es eine Ersetzung gibt, so daß s und t gleich sind. Man fragt sich somit, ob $s = t$ *lösbar* ist. Zusammenhänge zwischen Lösbarkeit und Unifikation werden in Kapitel 4 untersucht.

In Kapitel 5 werden monoidale/kommutative Theorien zusammen mit einem Unifikationsalgorithmus vorgestellt. Monoidal-kommutative Theorien beschreiben Varietäten abelscher Monoide und verallgemeinern bzw. vereinheitlichen somit Unifikationsalgorithmen z.B. für die Theorie (idempotenter) abelscher Monoide oder Gruppen. Außerdem wird gezeigt, daß kommutative und monoidale Theorien äquivalent sind. Somit ist die Bezeichnung „monoidal-kommutativ" gerechtfertigt.

In Kapitel 6 werden zunächst primale Algebren, d.h. Algebren, bei denen jede Operation durch eine Termfunktion dargestellt werden kann, definiert und einige ihrer Eigenschaften hergeleitet. Insbesondere wird gezeigt, daß man Lösbarkeit in einer beliebigen endlichen Algebra mit Hilfe der Unifikation in primalen Algebren entscheiden kann. Außerdem wird gezeigt, daß primale Algebren und monoidale Theorien nicht äquivalent sind, man also einen Unifikationsalgorithmus für monoidale Theorien nicht direkt zur Unifikation in primalen Algebren verwenden kann.

Anschließend wird ein Algorithmus skizziert, der mit Hilfe eines Unifikationsalgorithmus für monoidale Theorien, Unifikatoren in primalen Algebren bestimmt. Dazu werden die zu untersuchenden Terme in eine bestimmte syntaktische Form gebracht und in Terme über einer monoidalen Theorie übersetzt. Hier wird ein Unifikator bestimmt, der nach kleineren Modifikationen in einen Unifikator für das ursprüngliche Problem übersetzt werden kann.

Kapitel 2

Grundlagen

Die Unifikationstheorie beschäftigt sich (vereinfacht ausgedrückt) mit der Frage, ob man zwei gegebene *Terme*, in denen *Variablen* enthalten sind, durch *Substitutionen gleich* machen kann. Dabei ist man in der Regel nicht an *irgendwelchen* Substitutionen interessiert, sondern an möglichst *allgemeinen*.

Wenngleich jeder eine intuitive Vorstellung von den gerade verwendeten Begriffen hat, ist es jedoch für die formale Definition des Unifikationsproblems unabdingbar, zunächst diese Begriffe zu klären.

Deshalb sollen zuerst einige Schreibweisen festgelegt und die für die weitere Arbeit benötigten Begriffe und Sätze zur Verfügung gestellt werden.

Die in diesem Kapitel angegebenen Definitionen und Sätze sind im wesentlichen (sofern nicht anders angegeben) den Büchern [Ih93], [We92] und [Grä79] entnommen. [Ih93] und [We92] bieten eine leicht verständliche Einführung in die universelle Algebra[1]. [We92] entwickelt die universelle Algebra aus der Anwendungssicht für den Informatiker, während [Ih93] eher allgemeine Resultate aus den wichtigen Bereichen der universellen Algebra beschreibt. [Grä79] bietet hingegen eine umfassende Darstellung zur universellen Algebra.

2.1 Ordnungen

Um von einer Substitution sagen zu können, sie sei allgemeiner als eine andere, ist es hilfreich, Substitutionen vergleichen zu können. Wir werden daher später auf Substitutionen eine Ordnung einführen. Daher zunächst einige Bemerkungen über Ordnungen:

Definition 2.1.1 (Quasiordnung)
Eine zweistellige Relation $\lesssim$ auf einer Menge A heißt ***Quasiordnung****, falls für alle $x, y, z \in A$ die folgenden Bedingungen gelten:*

[1] Dort finden sich auch die Beweise zu den hier angegebenen Sätzen, die der Übersichtlichkeit wegen hier nicht noch einmal angegeben wurden. Der interessierte Leser sollte, sofern ihm die Beweise nicht bekannt sind, an den angegebenen Stellen nachschlagen.

(O1)	$x \lesssim x$	*(Reflexivität)*
(O2)	$x \lesssim y$ *und* $y \lesssim z \Rightarrow x \lesssim z$	*(Transitivität)*

Eine Quasiordnung, die zudem noch antisymmetrisch ist, heißt *Halbordnung.*

Definition 2.1.2 (Halbordung; vgl. [Ih93, 2.2.1])
Eine zweistellige Relation $\leq$ *auf einer Menge* A *heißt* ***Halbordnung****, falls für alle* $x, y, z \in A$ *die folgenden Bedingungen gelten:*

(O1)	$x \leq x$	*(Reflexivität)*
(O2)	$x \leq y$ *und* $y \leq z \Rightarrow x \leq z$	*(Transitivität)*
(O3)	$x \leq y$ *und* $y \leq x \Rightarrow x = y$	*(Antisymmetrie)*

Man nennt dann A oder auch das Paar $(A, \lesssim)$ bzw. $(A, \leq)$ eine **quasigeordnete Menge** bzw. **halbgeordnete Menge**. Zwei Elemente $a, b \in A$ heißen **vergleichbar**, falls $a \lesssim b$ oder $b \lesssim a$ (bzw. $a \leq b$ oder $b \leq a$), und sonst **unvergleichbar**. a und b heißen **ähnlich**, falls $a \lesssim b$ und $b \lesssim a$ gilt.

Für Elemente a und b einer quasi- oder halbgeordneten Menge heißt a **kleiner** als b ($a < b$), falls $a \lesssim b$, aber nicht $b \lesssim a$ (bzw. $a \leq b$, aber nicht $b \leq a$)[2]. Die Relation $<$ als Teilmenge von $\lesssim$ (bzw. $< \ \subseteq \ \leq$) heißt der **strikte Teil** von $\lesssim$ (bzw. $\leq$).

Für Quasiordnungen definiert man fernerhin folgende Begriffe:

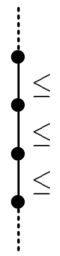
Definition 2.1.3 (Vollständigkeit; vgl. [Nutt92, 2.1])
Sei $(A, \lesssim)$ *eine quasigeordnete Menge. Ein Element* $a \in A$ *heißt* ***minimal****, falls kein* $b \in A$ *existiert mit* $b < a$*. Eine Menge* $B \subseteq A$ *heißt* ***vollständige Menge****, falls für jedes* $a \in A$ *ein* $b \in B$ *existiert mit* $b \lesssim a$*. Eine* ***minimal vollständige Menge*** *ist eine vollständige Menge* $B \subseteq A$*, so daß keine echte Teilmenge* $C \subset B$ *existiert, die vollständig ist. Ein* ***kleinstes Element*** *ist ein Element* $a \in A$ *mit* $a \lesssim a'$ *für alle* $a' \in A$*.*

Man beachte, daß ein minimales Element a kein kleinstes Element sein muß, da es Elemente geben könnte, die nicht mit a vergleichbar sind.

Unter einer vollständigen Menge versteht man also eine Teilmenge B einer Menge A, so daß zu jedem Element a aus A ein kleineres oder ähnliches Element in B existiert. Eine vollständige Menge einer Menge A existiert immer, da die Menge A selbst vollständig ist.

[2] also $a \leq b$ und $a \neq b$

Minimal vollständige Mengen einer quasigeordneten Menge müssen aber nicht existieren, wie man sich z.B. anhand von $\mathbb{Z}$ zusammen mit der üblichen Halb- und somit auch Quasiordnung $\leq$ (vgl. nebenstehende Abbildung) klar machen kann. Denn angenommen, es gäbe eine minimal vollständige Menge $B \subseteq \mathbb{Z}$. Dann gibt es zu einem beliebigen $b \in B$ ein $c \in \mathbb{Z}$ mit $c < b$. Da B vollständig ist, existiert zu c ein $d \in B$ mit $d \leq c$. Daher gilt $d < b$. Somit ist auch $C := B \backslash \{b\} \subset B$ eine vollständige Menge. Widerspruch!



Außerdem sind minimal vollständige Mengen in der Regel, sofern sie existieren, nicht eindeutig[3].

Nach Definition ist ein Element $a \in A$ genau dann ein kleinstes Element für A, wenn $\{a\}$ eine minimal vollständige Menge ist. Somit ist weder die Existenz noch die Eindeutigkeit eines kleinsten Elements gesichert.

Die Definitionen der obigen Begriffe lassen sich wörtlich auch auf Halbordnungen übertragen. Bei Halbordnungen ist jedoch aufgrund der Antisymmetrie die Eindeutigkeit minimal vollständiger Mengen gewährleistet. Deswegen ist es bisweilen hinderlich, auf die Antisymmetrie verzichten zu müssen. Jedoch ist es möglich, von einer quasigeordneten Menge zu einer halbgeordneten Menge zu gelangen, indem man ähnliche Elemente identifiziert. Dazu definiert man auf einer quasigeordneten Menge $(A, \lesssim)$ eine Äquivalenzrelation $\sim$ wie folgt:

$$\text{Für } a, b \in A \text{ sei } a \sim b :\Leftrightarrow a \lesssim b \text{ und } b \lesssim a$$

Dann ist mit $A' := A/\!\sim$ und $\leq$ definiert durch $\bar{a} \leq \bar{b} \;:\Leftrightarrow\; a \lesssim b$ für $a, b \in A$ das Paar $(A', \leq)$ eine halbgeordnete Menge, wobei $\bar{x}$ die Äquivalenzklasse von x bzgl. $\sim$ bezeichne (vgl. [We92, S. 34]).

2.2 Terme, Algebren, Termalgebra

Der Begriff eines *Terms* ist gebunden an den Begriff einer *Signatur*. Eine Signatur legt fest, welche *Symbole* man zum Aufbau von Termen verwenden darf. Die Angabe einer Signatur ist aber auch notwendig zur Beschreibung einer *Algebra*.

Definition 2.2.1 (Signatur)
Eine ***Signatur*** *ist ein Paar* (Σ, st)*, wobei* Σ *eine Menge, genannt die Menge der* ***Funktionssymbole*** *oder auch* ***Operationssymbole****, und* $st : \Sigma \rightarrow \mathbb{N}$ *eine Abbildung ist*[4]*, die jedem Funktionssymbol aus* Σ *eine* ***Stelligkeit*** *zuordnet.*

[3] Sei z.B. $\{a\} \subseteq A$ eine mininimal vollständige Menge für A und existiere ein $b \in B$ mit $b \lesssim a$ und $a \lesssim b$. Dann ist auch $\{b\}$ eine minimal vollständige Menge für A.

[4] $\mathbb{N} = \{0, 1, 2, \ldots\}$

Nullstellige Funktionssymbole werden auch **Konstantensymbole** genannt. Für Elemente aus Σ verwenden wir in der Regel die Zeichen $f, g, h, \ldots, f_1, f_2, \ldots$ oder auch $+, *, \underline{0}, \underline{1}$.

Im folgenden geben wir eine Signatur häufig nur durch Nennung von Σ an und weisen auf die Stelligkeit von $f \in \Sigma$ hin, wenn es notwendig ist.

Gruppiert man die Elemente von Σ gemäß ihrer Stelligkeit, z.B. $\Sigma^{(n)} := \{f \in \Sigma : st(f) = n\}$, so ist die Signatur eindeutig durch die Familie $(\Sigma^{(n)})_{n\in\mathbb{N}}$ bestimmt. Daher unterscheiden wir in der Regel nicht zwischen der Signatur Σ und der Familie $(\Sigma^{(n)})_{n\in\mathbb{N}}$ und schreiben statt $f \in \Sigma$, $st(f) = n$ kurz $f \in \Sigma^{(n)}$.

Bei gegebener Signatur Σ kann man erklären, was man unter einem Σ-*Term* versteht:

Definition 2.2.2 (Term; vgl. [Ih93, 6.2.1])
Sei (Σ, st) eine Signatur und X eine abzählbare[5] *Menge, deren Elemente* ***Variablen*** *genannt werden, mit $\Sigma \cap X = \emptyset$. Die Menge $T(\Sigma, X)$ wird durch folgende Rekursionsvorschrift definiert:*

1. *Für alle $x \in X$ ist $x \in T(\Sigma, X)$.*
2. *Für $f \in \Sigma^{(n)}$ und $t_1, \ldots, t_n \in T(\Sigma, X)$ ist auch $ft_1 \ldots t_n \in T(\Sigma, X)$.*

Die Elemente von $T(\Sigma, X)$ heißen ***Σ-Terme****.*

Mit $Var(t)$ bezeichnen wir die Menge aller bei der Bildung von t verwendeten Variablen, das heißt, $Var(t)$ ist rekursiv definiert durch $Var(x) = \{x\}$ für $x \in X$ und $Var(ft_1 \ldots t_n) = Var(t_1) \cup \cdots \cup Var(t_n)$ für $f \in \Sigma^{(n)}$. Für $t \in T(\Sigma, X)$ mit $Var(t) \subseteq \{x_1, \ldots, x_n\}$ schreibt man oft auch $t(x_1, \ldots, x_n)$ um anzudeuten, daß alle bei der Bildung von t verwendeten Variablen in der Menge $\{x_1, \ldots, x_n\}$ enthalten sind. Man nennt den Term dann **n-stellig**.

Der Übersichtlichkeit wegen werden wir bisweilen die Infixnotation verwenden und Klammern setzen, wo es sonst zu Mehrdeutigkeiten führen könnte. Zum Beispiel schreiben wir statt $++xyz$ einfach $(x + y) + z$.

Gilt für zwei Variablenmengen X, Y, daß $X \subseteq Y$, so ist $T(\Sigma, X) \subseteq T(\Sigma, Y)$, da man bei der Bildung von Termen (in $T(\Sigma, Y)$) nicht alle Variablen verwenden muß. Hat man insbesondere die Folge $(X_i)_{i\in\mathbb{N}}$ von Variablenmengen gegeben mit $X_0 := \{x_o\}$ und $X_{i+1} := X_i \cup \{x_{i+1}\}$, $i \in \mathbb{N}$, so folgt $T(\Sigma, X_i) \subseteq T(\Sigma, X_\omega)$ für $X_\omega := \{x_1, x_2, x_3, \ldots\} = \bigcup_{i\in\mathbb{N}} X_i$. Das heißt, für jeden Term t aus $T(\Sigma, X_i)$ gilt $t \in T(\Sigma, X_\omega)$. Andererseits gilt für $t \in T(\Sigma, X_\omega)$, daß $t \in T(\Sigma, X_i)$ für ein $i \in \mathbb{N}$, da ein Term ein endliches Wort ist und somit nur endlich viele Variablen enthalten kann. Bisweilen ist es daher „geschickt", mit $T(\Sigma, X_\omega)$ zu arbeiten, da man dann stets „ausreichend viele Variablen" hat, sich aber ggf. auf endlich viele Variablen beschränken kann.

[5] endliche oder unendliche

Terme sind wie die Elemente einer Signatur rein syntaktischer Natur. Man kann ihnen jedoch „eine Bedeutung geben“, wenn man sie in einer Struktur *interpretiert*. Dazu prägen wir den Begriff einer *Algebra*.

Unter einer **Realisation** eines n-stelligen Funktionssymbols f auf einer Menge A versteht man eine Funktion von A^n nach A, die wir mit f^A bezeichnen. Damit kann man für eine Signatur Σ den Begriff einer Σ-Algebra wie folgt definieren:

Definition 2.2.3 (Σ-Algebra)
*Sei Σ eine Signatur. Unter einer **Σ-Algebra** $\mathcal{A}$ versteht man ein Paar $\mathcal{A} = (A, \Sigma^A)$, wobei A eine Menge und Σ^A eine Familie $\Sigma^A = (f^A)_{f \in \Sigma}$ von Realisationen f^A von Funktionssymbolen f ist. Die Menge A wird **Universum** oder **Trägermenge** der Algebra $\mathcal{A}$ genannt, und die Abbildungen $f^{\mathcal{A}} := f^A$ heißen **fundamentale Operationen**.*

In der Sprache der mathemathischen Logik ist eine Σ-Algebra also nichts anderes als eine funktionale Σ-Struktur, also eine Σ-Struktur, deren Signatur nur Funktionssymbole und keine Relationssymbole enthält.

Im folgenden werden wir nicht immer typographisch zwischen $f \in \Sigma$ und der zugehörigen Abbildung $f^{\mathcal{A}}$ unterscheiden.

Definition 2.2.4 (Unteralgebra)
*Sei $\mathcal{A} = (A, \Sigma^A)$ eine Σ-Algebra. Dann heißt $\mathcal{B} = (B, \Sigma^B)$ **Unteralgebra** von $\mathcal{A}$ (in Zeichen: $\mathcal{B} \leq \mathcal{A}$), falls $B \subseteq A$ und die Einschränkung von f^A auf B $((f^A)|_B)$ eine Abbildung in B ist. Mit **Sub $\mathcal{A}$** wird die Menge aller Unteralgebren von $\mathcal{A}$ bezeichnet.*

Hat man zwei Σ-Algebren gegeben, so kann man Abbildungen zwischen ihnen betrachten. Wichtige Abbildungen sind insbesondere die, die die Struktur der betrachteten Algebren respektieren:

Definition 2.2.5 (Homomorphismus, Endomorphismus)
Es seien $\mathcal{A} = (A, \Sigma^A)$ und $\mathcal{B} = (B, \Sigma^B)$ zwei Σ-Algebren. Eine Abbildung $\varphi : A \to B$ heißt

- ***Homomorphismus**, falls für alle $f \in \Sigma$ und alle $a_1, \ldots, a_n$ $(n = st(f))$ gilt:*

  $$\varphi f^A(a_1, \ldots, a_n) = f^B(\varphi a_1, \ldots, \varphi a_n)$$

- ***Monomorphismus**, falls φ Homorphismus und φ injektiv*
- ***Epimorphismus**, falls φ Homorphismus und φ surjektiv*
- ***Isomorphismus**, falls φ Homorphismus und φ bijektiv*
- ***Endomorphismus**, falls φ Homorphismus und $\mathcal{A} = \mathcal{B}$.*

Ist $\varphi : \mathcal{A} \to \mathcal{B}$ ein Epimorphismus, so wird $\mathcal{B}$ **homomorphes Bild** *von $\mathcal{A}$ genannt. Die Menge aller Homomorphismen von $\mathcal{A}$ nach $\mathcal{B}$ wird mit* **$Hom(\mathcal{A}, \mathcal{B})$** *und die Menge der Endomorphismen von $\mathcal{A}$ mit* **$End\,\mathcal{A}$** *bezeichnet. Existiert ein Isomorphismus zwischen $\mathcal{A}$ und $\mathcal{B}$, so heißen $\mathcal{A}$ und $\mathcal{B}$* **isomorph** *(in Zeichen: $\mathcal{A} \cong \mathcal{B}$).*

Bisweilen möchte man Elemente einer Algebra identifizieren, d.h. zu einer Algebra übergehen, in der man statt mit einzelnen Elementen mit Klassen von Elementen rechnet. Genauer:

Definition 2.2.6 (Kongruenzrelation; vgl. [Ih93, 1.4.5])
Sei θ eine Äquivalenzrelation und $\mathcal{A} = (A, \Sigma^A)$ eine Σ-Algebra. Dann heißt θ **Kongruenzrelation**, *falls für alle $f \in \Sigma^{(n)}$ und alle $a_1, b_1, \ldots, a_n, b_n \in A$ mit $a_1\ \theta\ b_1, \ldots, a_n\ \theta\ b_n$ gilt*

$$f^A(a_1, \ldots, a_n)\ \theta\ f^A(b_1, \ldots, b_n).$$

Die **Kongruenzklasse** *von $a \in A$ ist die Menge $\{a' \in A : a'\ \theta\ a\}$ und wird mit $[a]\theta$ oder $[a]$ bezeichnet, falls θ aus dem Zusammenhang klar ist. Die Menge aller Kongruenzrelationen einer Algebra $\mathcal{A}$ wird mit $Con\,\mathcal{A}$ bezeichnet.*

Eine Kongruenzrelation ist also eine Äquivalenzrelation, die mit allen fundamentalen Operationen verträglich ist.

Definition 2.2.7 (Kern)
Es sei $\varphi : A \to B$ eine Abbildung. Dann ist der **Kern** *von φ definiert als*

$$Kern\,\varphi := \{(a, b) \in A^2 \ : \ \varphi a = \varphi b\}$$

Für den Kern eines Homomorphismus $\varphi : \mathcal{A} \to \mathcal{B}$ kann man leicht zeigen, daß $Kern\,\varphi$ eine Kongruenzrelation auf $\mathcal{A}$ ist, das heißt, es gilt $Kern\,\varphi \in Con\,\mathcal{A}$ (vgl. [Ih93, 1.4.11]). Außerdem kann man zeigen, daß $Con\,\mathcal{A}$ genau aus den Kernen von Homomorphismen von $\mathcal{A}$ besteht ([Ih93, 1.4.14]).

Definition 2.2.8 (Faktoralgebra; vgl. [Ih93, 1.4.9])
Sei $\mathcal{A}$ eine Σ-Algebra und $\theta \in Con\,\mathcal{A}$. Wir definieren die **Faktoralgebra** *$\mathcal{A}/\theta$ von $\mathcal{A}$ nach θ wie folgt: Das Universum von $\mathcal{A}/\theta$ sei A/θ, d.h. die Menge aller Kongruenzklassen von θ. Die fundamentalen Operationen von $\mathcal{A}/\theta$ werden aus denen von $\mathcal{A}$ gewonnen durch*

$$\begin{aligned} f^{\mathcal{A}/\theta} &: (A/\theta)^n \to A/\theta \\ f^{\mathcal{A}/\theta}([a_1]\theta, \ldots, [a_n]\theta) &:= [f^{\mathcal{A}}(a_1, \ldots, a_n)]\theta \end{aligned}$$

Aufgrund der Verträglichkeitsbedingung von θ ist $\mathcal{A}/\theta$ wohldefiniert. $\mathcal{A}$ läßt sich auf kanonische Weise homomorph in $\mathcal{A}/\theta$ einbetten:

Lemma 2.2.9 (Einbettungshomomorphismus; vgl. [Ih93, 1.4.12])
Es sei $\mathcal{A}$ eine Σ-Algebra und $\theta \in Con\,\mathcal{A}$. Dann ist die Abbildung ι definiert durch

$$\iota_\theta = \begin{cases} A \to A/\theta \\ a \mapsto [a]\theta \end{cases}$$

ein surjektiver Homomorphismus. ι_θ heißt ***kanonischer Einbettungshomomorphismus****.*

Die *Termalgebra* hat als Universum die Menge der Σ-Terme. Das Rechnen in der Termalgebra ist dem Aufbau von Termen nachempfunden:

Definition 2.2.10 (Termalgebra; vgl. [Ih93, 6.2.1])
Sei Σ eine Signatur und $T(\Sigma, X)$ eine Menge von Σ-Termen. Die ***Σ-Termalgebra*** *$\mathcal{T}(\Sigma, X)$ ist definiert als Σ-Algebra mit Universum $T(\Sigma, X)$ und den für jedes $f \in \Sigma^{(n)}$ durch*

$$f^{\mathcal{T}(\Sigma,X)}(t_1, \ldots, t_n) := f t_1 \ldots t_n$$

definierten fundamentalen Operationen.

Bisweilen identifizieren wir die Menge der Σ-Terme $T(\Sigma, X)$ mit der Σ-Termalgebra $\mathcal{T}(\Sigma, X)$.

Mit Hilfe der Termalgebra und dem Begriff eines Homomorphismus ist eine formale Beschreibung des Begriffs einer *Substitution* möglich:

Definition 2.2.11 (Substitution)
Sei V eine Variablenmenge. Ein Homomorphismus $\varphi : \mathcal{T}(\Sigma, V) \to \mathcal{T}(\Sigma, V)$ heißt ***Substitution****, falls $\varphi(v) \neq v$ nur für endlich viele $v \in V$. Die Menge der Substitutionen von $\mathcal{T}(\Sigma, V) \to \mathcal{T}(\Sigma, V)$ wird mit $Subs(\mathcal{T}(\Sigma, V), \mathcal{T}(\Sigma, V))$ bezeichnet.*

Ist $\varphi : \mathcal{T}(\Sigma, X) \to \mathcal{T}(\Sigma, Y)$ ein Homomorphismus und gilt $|X| < \infty$, so kann φ zu einer Substitution $\bar{\varphi} : \mathcal{T}(\Sigma, V) \to \mathcal{T}(\Sigma, V)$ für $V := X \cup Y$ erweitert werden. Definiere dazu

$$\bar{\varphi}(v) = \begin{cases} v & \text{für } v \in Y \backslash X \\ \varphi(v) & \text{für } v \in X \end{cases}$$

Offensichtlich ist $\bar{\varphi}|_X = \varphi$ und $\bar{\varphi}(v) \neq v$ nur für endlich viele $v \in V$. Somit ist $\bar{\varphi}$ eine Substitution. Wir wollen daher für endliches X bereits φ als Substitution bezeichnen. Die Menge der Substitutionen von $\mathcal{T}(\Sigma, X)$ nach $\mathcal{T}(\Sigma, Y)$ mit $Subs(\mathcal{T}(\Sigma, X), \mathcal{T}(\Sigma, Y))$ abgekürzt.

Satz 2.2.12 (Prinzip der endl. algebraischen Induktion; [Ih93, 6.2.5])
Sei $\mathcal{T}(\Sigma, X)$ die Σ-Termalgebra über X. Dann gibt es für jede Σ-Algebra $\mathcal{A}$ und jede Abbildung $\varphi : X \to A$ genau einen Homomorphismus $\bar{\varphi} : \mathcal{T}(\Sigma, X) \to \mathcal{A}$, der φ fortsetzt, d.h. mit $\bar{\varphi}|_X = \varphi$.

Will man also eine Σ-Termalgebra in eine Σ-Algebra $\mathcal{A}$ homomorph einbetten, so braucht man nur die Bilder der Variablen vorzugeben. Insbesondere sind auch Substitutionen eindeutig durch die Angabe der Bilder der Variablen bestimmt. Die Eindeutigkeit des Einbettungshomorphismus liefert fernerhin die Wohldefiniertheit von Termfunktionen:

Definition 2.2.13 (Termfunktion; [Ih93, 6.2.6])
Es sei t ein Σ-Term über $X = \{x_1, \ldots, x_n\}$ und $\mathcal{A}$ eine Σ-Algebra. Für $a_1, \ldots, a_n \in A$ sei $\varphi_{a_1,\ldots,a_n} : \mathcal{T}(\Sigma, X) \to \mathcal{A}$ der eindeutig bestimmte Homomorphismus mit $x_i \mapsto a_i$, $i = 1, \ldots, n$. Dann erhält man eine n-stellige Operation $t^{\mathcal{A}} : A^n \to A$ durch

$$t^{\mathcal{A}}(a_1, \ldots, a_n) := \varphi_{a_1,\ldots,a_n} t.$$

Die auf diese Weise aus den Termen gebildeten Operationen auf A heißen ***Termfunktionen****. Die Menge aller Termfunktionen von $\mathcal{A}$ wird mit $T(\mathcal{A})$ bezeichnet.*

Man nennt $t^{\mathcal{A}}$ auch die durch t **induzierte** Termfunktion und den eindeutig bestimmten Homomorphismus $\varphi_{a_1,\ldots,a_n} : \mathcal{T}(\Sigma, X) \to \mathcal{A}$ eine **Belegung**.[6] Die Belegung wir oft auch nur durch $a_1, \ldots, a_n$ angegeben.

Für $t \in T(\Sigma, X)$ und für jedes endliche $Y \supseteq X$ gilt offenbar $t \in T(\Sigma, Y)$. Da für die Belegungen $\varphi_{a_1,\ldots,a_n}$ und $\varphi_{a_1,\ldots,a_n,\ldots,a_{|Y|}}$

$$\varphi_{a_1,\ldots,a_n} t = \varphi_{a_1,\ldots,a_n,\ldots,a_{|Y|}} t$$

gilt, induziert t auch eine Termfunktion $t^{\mathcal{A}} : A^{|Y|} \to A$.

Für einen Term $t \in T(\Sigma, X)$, $X = \{x_1, \ldots, x_n\}$ mit induzierter Termfunktion $t^{\mathcal{A}} : A^n \to A$ heißt x_i **unwesentliche Variable** (bzgl. $\mathcal{A}$), falls für alle $(a_1, \ldots, a_n) \in A^n$ und für alle $a, b \in A$ gilt

$$t^{\mathcal{A}}(a_1, \ldots, a_{i-1}, a, a_{i+1}, \ldots, a_n) = t^{\mathcal{A}}(a_1, \ldots, a_{i-1}, b, a_{i+1}, \ldots, a_n)$$

Ansonsten heißt x_i **wesentliche Variable** von t (bzgl. $\mathcal{A}$). Offensichtlich ist für jede Algebra $\mathcal{A}$ die Menge der wesentlichen Variablen von t (bzgl. $\mathcal{A}$) eine Teilmenge von $Var(t)$.

[6] Da $\forall t \in T(\Sigma, X) : |Var(t)| < \infty$ gilt, ist $|X| < \infty$ keine wesentliche Einschränkung für die Begriffe Termfunktion und Belegung.

Besitzt ein Term t mindestens eine wesentliche Variable x, so kann man jede unwesentliche Variable durch x ersetzen und so zu einem Term t' übergehen, in dem jede Variable wesentlich ist und für den $t^{\mathcal{A}} = t'^{\mathcal{A}}$ gilt.

Besitzt t keine wesentliche Variable, d.h., für $t^{\mathcal{A}} : A^k \to A$ und alle $(a_1, \ldots, a_k) \in A^k$ ist $t^{\mathcal{A}}(a_1, \ldots, a_k)$ konstant, so kann man für t nur dann einen Term t' finden, für den gilt, daß t' nur wesentliche Variablen enthält und daß $t^{\mathcal{A}} = t'^{\mathcal{A}}$, wenn mindestens ein Konstantensymbol in der Signatur vorhanden ist, da ansonsten jeder Term mindestens eine Variable enthält. Ist keine Konstante in der Signatur vorhanden, wollen wir aber $t^{\mathcal{A}} : A \to A$ mit einer Abbildung $f_t : A^0 \to A$, $f_t = a \in A$ identifizieren, falls für jede Belegung b gilt $t^{\mathcal{A}}(b) = a$.

Wir sagen daher auch, daß ein Term t eine Familie von Termfunktionen $(t^{\mathcal{A}} : A^k \to A)_{k \in I}$ induziert, wobei $I := \{n \in \mathbb{N} : n \geq i\}$ und i die Anzahl der wesentlichen Variablen von t ist.

Ähnlich wie für die fundamentalen Operationen schreibt man auch bei den Termfunktionen oft einfach t anstelle von $t^{\mathcal{A}}$.

Da jede Variable $x_i \in X = \{x_1, \ldots, x_n\}$ ein Term ist, erhält man als Termfunktion für den Term $t = x_i$ die Projektionsabbildung $t^{\mathcal{A}}(a_1, \ldots, a_n) = a_i$. Die Termfunktionen einer Algebra sind genau die Abbildungen, die man durch Zusammensetzen aus den fundamentalen Operationen sowie den Projektionsabbildungen erhält (vgl. [Ih93, 6.2.7])[7].

Es sei noch erwähnt, daß sich alle Termfunktionen bzgl. Homomorphismen wie fundamentale Funktionen verhalten:

Satz 2.2.14 ([Ih93, 6.2.9])
Seien Σ eine Signatur, $\mathcal{A}, \mathcal{B}$ Σ-Algebren und t ein n-stelliger Σ-Term. Dann gilt für jeden Homomorphismus $\varphi : \mathcal{A} \to \mathcal{B}$ und alle $a_1, \ldots, a_n \in A$:

$$\varphi t^{\mathcal{A}}(a_1, \ldots, a_n) = t^{\mathcal{B}}(\varphi a_1, \ldots, \varphi a_n)$$

Wie oben bereits erwähnt sind Termfunktionen genau die Funktionen, die durch Zusammensetzen der fundamentalen Operationen und der Projektionsabbildungen entstehen. Die Grundmenge A einer Algebra $\mathcal{A}$ wird *nicht* bei der Definition von Termfunktionen verwendet. Läßt man beim Aufbau der Terme Elemente der Grundmenge als Konstanten zu, so spricht man von Polynomen:

Definition 2.2.15 (Polynome, Polynomfunktion; [Ih93, 6.2.10])
Es sei (Σ, st) eine Signatur und $\mathcal{A} = (A, \Sigma^A)$ eine Σ-Algebra. Werden zu Σ alle $a \in A$ als neue nullstellige Operationssymbole hinzugefügt, dann erhält man die neue Signatur $\Sigma' := \Sigma \cup A$ (mit den alten Stelligkeiten $st(f)$ für alle $f \in \Sigma$ und $st(a) = 0$ für alle $a \in A$). Ein Σ'-Term wird ***Polynom*** *genannt, die Menge der*

[7] Termen werden hier also – wie in der mathematischen Logik üblich – Termfunktionen zugeordnet.

Σ'-Terme über der Variablenmenge X wird mit $P_A(\Sigma, X)$ bezeichnet und die Elemente von $P_A(\Sigma, X)$ heißen ***Polynome****. Aus $\mathcal{A}$ wird nun eine Σ'-Algebra, indem man für jedes $a \in A$ eine nullstellige Operation f_a mit Wert a hinzufügt. Die Termfunktionen der so erhaltenen Algebra $\mathcal{A}_A := (A, \Sigma^A \cup \{f_a : a \in A\})$ heißen* ***Polynomfunktionen*** *von $\mathcal{A}$, und die Menge aller Polynomfunktionen von $\mathcal{A}$ wird mit $P(\mathcal{A})$ bezeichnet.*

Natürlich schreibt man oft einfacher $\underline{a}$ oder a anstelle von f_a.

Die Polynome einer Algebra $\mathcal{A}$ entstehen, indem in den Termen einige der Variablen durch Konstanten aus A ersetzt werden. Da man die Σ-Termalgebra problemlos in jede Σ-Algebra einbetten kann, betrachtet man häufig nicht die Polynome einer konkreten Σ-Algebra, sondern die Σ-Termalgebra über der Menge $X \cup \{c_1, \ldots, c_k\}$ und nennt die $c_1, \ldots, c_k$ **freie Konstanten**.

Wie weiter unten erläutert wird, sind Gleichungstheorien Kongruenzrelationen einer Algebra (vgl. [Ih93, S. 94 unten]). Deshalb sei folgendes Resultat genannt:

Satz 2.2.16 ([Ih93, 6.2.12])
Die Polynomfunktionen einer Algebra $\mathcal{A}$ sind mit allen Kongruenzrelationen von $\mathcal{A}$ verträglich, das heißt, aus $n \in \mathbb{N}$, $p \in P_A(x_1, \ldots, x_n)$, $\theta \in Con\,\mathcal{A}$ und $a_i \;\theta\; b_i$ für $i = 1, \ldots, n$ folgt:

$$p^{\mathcal{A}}(a_1, \ldots, a_n) \;\theta\; p^{\mathcal{A}}(b_1, \ldots, b_n)$$

2.3 Gleichungen

Ein wichtiger Begriff für die Unifikationstheorie ist der Begriff der Gleichung. Denn zu untersuchen, ob zwei Terme *gleich* sind, bedeutet hier zu überprüfen, ob eine Gleichung *gilt*.

Definition 2.3.1 (Gleichung; Gleichungssystem; vgl. [Ih93, 6.3.1])
Es sei $T(\Sigma, X)$ die Menge der Σ-Terme über X. Dann heißt jedes Paar $(s, t) \in T(\Sigma, X) \times T(\Sigma, X)$ eine ***Gleichung*** *über X. Eine Teilmenge $E \subseteq T(\Sigma, X) \times T(\Sigma, X)$ heißt* ***Gleichungssystem****.*

Anstelle von (s, t) wird im folgenden meist

$$s = t \text{ oder } s(x_1, \ldots, x_n) = t(x_1, \ldots, x_n)$$

geschrieben (letzteres, falls alle in s und t auftretenden Variablen in der Menge $\{x_1, \ldots, x_n\}$ enthalten sind.

Das heißt, eine Gleichung ist nichts anderes als ein Paar von Termen. Die Frage ist nun, wann eine Gleichung *gilt*.

Definition 2.3.2 (Modell; vgl. [Ih93, 6.3.1])
Eine Σ-Algebra $\mathcal{A}$ ***erfüllt*** *die Gleichung $s(x_1, \ldots, x_n) = t(x_1, \ldots, x_n)$ (oder ist* ***Modell*** *für $s = t$ oder die Gleichung* ***gilt*** *in $\mathcal{A}$), falls $s^{\mathcal{A}}(a_1, \ldots, a_n) = t^{\mathcal{A}}(a_1, \ldots, a_n)$ für jede Belegung $a_1, \ldots, a_n \in A$. In diesem Fall schreibt man*

$$\mathcal{A} \models s(x_1, \ldots, x_n) = t(x_1, \ldots, x_n)$$

oder kürzer

$$\mathcal{A} \models s = t \text{ oder } \mathcal{A} \models \forall X\, s = t,$$

wobei $\{x_1, \ldots, x_n\} \subseteq X$ gelte.

Ist $\mathcal{A}$ Modell für jede Gleichung eines Gleichungssystems E, so heißt $\mathcal{A}$ auch E-Algebra (der Signatur Σ), und wir sagen „$\mathcal{A}$ ist Modell für E“. Man schreibt dann bisweilen auch

$$\mathcal{A} \models E$$

Eine Algebra ist also Modell für eine Gleichung, wenn die durch die Gleichung gegebenen Terme in der Algebra die gleichen Termfunktionen induzieren.

Um den Begriff „$\mathcal{A}$ ist Modell für eine Gleichung $s = t$“ mit dem in der mathematischen Logik verwendeten Modellbegriff konform zu machen, könnte man eine Gleichung g als ein Tripel (X', s, t) definieren, wobei $X' := \{x_1, \ldots, x_m\}$ die in s und t auftretenden Variablen bezeichne, und der Gleichung g die logische Formel $g' := \forall x_1 \ldots \forall x_m\ s = t$ zuordnen und von $\mathcal{A} \models g'$ sprechen. Aus Gründen der Übersichtlichkeit haben wir hier darauf verzichtet.

Desweiteren existiert auch der Begriff der *Erfüllbarkeit*. Man drückt damit aus, daß es *mindestens eine* Belegung gibt, so daß die durch die Gleichung induzierten Termfunktionen dieselben Bilder für diese Belegung in der Algebra liefern.

Definition 2.3.3 (Erfüllbarkeit)
Eine Gleichung $s(x_1, \ldots, x_n) = t(x_1, \ldots, x_n)$ heißt ***erfüllbar*** *in der Σ-Algebra $\mathcal{A}$, falls eine Belegung $\alpha : X \to A$, $x_i \mapsto a_i$ für $i \in \{1, \ldots, n\}$ existiert mit $s^{\mathcal{A}}(a_1, \ldots, a_n) = t^{\mathcal{A}}(a_1, \ldots, a_n)$. Dabei sei $X = \{x_1, \ldots, x_n\}$. In diesem Fall schreibt man*

$$(\mathcal{A}, \alpha) \models s(x_1, \ldots, x_n) = t(x_1, \ldots, x_n)$$

oder kürzer

$$(\mathcal{A}, \alpha) \models s = t \text{ oder } \mathcal{A} \models \exists X\, s = t.$$

Wir erweitern nun den Modellbegriff für Algebren zu einem Modellbegriff für **Klassen** von Algebren:

Definition 2.3.4 (Modell; vgl. [Ih93, 6.3.1])
*Sei $\mathfrak{K}$ eine Klasse von Σ-Algebren. $\mathfrak{K}$ **erfüllt** eine Gleichung $s(x_1, \ldots, x_n) = t(x_1, \ldots, x_n)$ (oder die Gleichung **gilt** in $\mathfrak{K}$), falls $s = t$ in jeder Algebra $\mathcal{A} \in \mathfrak{K}$ gilt. Man schreibt dann*

$$\mathfrak{K} \models s = t.$$

Im folgenden wollen wir untersuchen, wie man vorgehen kann, um Aufschluß über die Gleichungen und deren erfüllende Algebren zu erhalten.

Dazu definieren wir die Operatoren M und G_X folgendermaßen:

Definition 2.3.5 (M, G_X; vgl. [Ih93, 6.3.2])
Sei Σ eine Signatur. Für jedes Gleichungssystem $E \subseteq T(\Sigma, X) \times T(\Sigma, X)$ über der Variablenmenge X ist

$$M(E) := \{\mathcal{A} : \mathcal{A} \models s = t \text{ für alle } (s,t) \in E\}$$

*die Klasse der Modelle von E und wird **Modellklasse von E** genannt. Umgekehrt ist für jede Klasse $\mathfrak{K}$ von Algebren*

$$G_X(\mathfrak{K}) := \{(s,t) \in T(\Sigma, X) \times T(\Sigma, X) \;:\; \mathcal{A} \models s = t \text{ für alle } \mathcal{A} \in \mathfrak{K}\}$$

die Menge aller in allen Algebren von $\mathfrak{K}$ gültigen Gleichungen über X.

Fernerhin betrachten wir die Operatoren S, H, P und I, die jede Klasse $\mathfrak{K}$ von Σ-Algebren wieder auf eine Klasse von Σ-Algebren abbilden. Es sei

Definition 2.3.6 (S, H, P, I; [Ih93, 6.1.1])

$S(\mathfrak{K})$	*die Klasse aller Unteralgebren von Algebren aus $\mathfrak{K}$*
$H(\mathfrak{K})$	*die Klasse aller homomorphen Bilder von Algebren aus $\mathfrak{K}$*
$P(\mathfrak{K})$	*die Klasse aller direkten Produkte von Familien von Algebren aus $\mathfrak{K}$*
$I(\mathfrak{K})$	*die Klasse aller zu Algebren aus $\mathfrak{K}$ isomorphen Algebren.*

Man sagt dann auch, $S(\mathfrak{K})$ ist der Abschluß von $\mathfrak{K}$ bzgl. Unteralgebrenbildung (für H, P, I entsprechend). Besteht die Klasse $\mathfrak{K}$ nur aus einem Element $\mathcal{A}$ (also $\mathfrak{K} = \{\mathcal{A}\}$), so schreibt man statt $H(\{\mathcal{A}\})$ kürzer $H(\mathcal{A})$ (für S, I, P entsprechend).

Für diese Klassen gilt:

Satz 2.3.7 ([Ih93, 6.3.17])
Es sei $\mathfrak{K}$ ein Klasse von Σ-Algebren. In jeder der Klassen $\mathfrak{K}$, $H(\mathfrak{K})$, $S(\mathfrak{K})$, $P(\mathfrak{K})$ und $I(\mathfrak{K})$ gelten dieselben Gleichungen über jeder Variablenmenge X.

Untersucht man die Gleichungen, die in einer Klasse $\mathfrak{K}$ gelten, so kann man also oBdA die Gleichungen des Abschlusses von $\mathfrak{K}$ unter den Operatoren S, H und P untersuchen.[8]

Definition 2.3.8 (abgeschlossen, Varietät; [Ih93, 6.1.4])
Eine Klasse $\mathfrak{K}$ von Σ-Algebren heißt unter H (bzw. S, bzw. P) ***abgeschlossen****, falls $H(\mathfrak{K}) \subseteq \mathfrak{K}$ (bzw. $S(\mathfrak{K}) \subseteq \mathfrak{K}$, bzw. $P(\mathfrak{K}) \subseteq \mathfrak{K}$) gilt. Eine unter allen drei Operatoren H, S, P abgeschlossene Klasse wird* ***Varietät*** *genannt.*

Man kann von jeder Klasse von Σ-Algebren zu einer Varietät gelangen, indem man den Abschluß unter den Operatoren H, S, P bildet. Die so erhaltene Klasse wird minimal (bzgl. $\subseteq$), wenn man die Operatoren in folgender Weise kombiniert:

Satz 2.3.9 ([Ih93, 6.1.5])
Für jede Klasse $\mathfrak{K}$ von Σ-Algebren ist $HSP(\mathfrak{K})$ die kleinste $\mathfrak{K}$ umfassende Varietät.

2.3.1 Freie Algebren

In diesem Abschnitt wollen wir untersuchen, ob es eine Algebra $\mathcal{F}$ in einer Klasse $\mathfrak{K}$ von Σ-Algebren gibt, die für eine feste Belegung φ stellvertretend bzgl. aller Gleichungen $s = t$ für die ganze Klasse ist, d.h. $(\mathcal{F}, \varphi) \models s = t \;\Leftrightarrow\; \mathfrak{K} \models s = t$. Da $\mathcal{F} \in \mathfrak{K}$ ist, folgt per Definition $\mathfrak{K} \models s = t \Rightarrow (\mathcal{F}, \varphi) \models s = t$. Es ist also eine Algebra $\mathcal{F}$ gesucht, für die $(\mathcal{F}, \varphi) \models s = t \Rightarrow \forall \mathcal{A} \in \mathfrak{K} : \mathcal{A} \models s = t$ gilt, in der also, anschaulich gesprochen, die *wenigsten* Gleichungen gelten.

Algebren, die in diesem Sinne für eine ganze Klasse charakteristisch sind, werden *freie Algebren* genannt:

Definition 2.3.10 (freie Algebra; [We92, 3.2, Def. 4])
Sei $\mathfrak{K}$ eine Klasse von Σ-Algebren. $\mathcal{F} = (F, \Sigma^F) \in \mathfrak{K}$ heißt ***freie Algebra bzgl. $\varphi : X \to F$*** *für $\mathfrak{K}$, wenn es zu jeder Algebra $\mathcal{A} \in \mathfrak{K}$ und jeder Abbildung $\alpha : X \to A$ genau einen Homomorphismus $\tilde{\alpha} : \mathcal{F} \to \mathcal{A}$ mit $\alpha = \varphi\tilde{\alpha}$ gibt.*

X wird dann auch **Erzeugermenge von $\mathcal{F}$** und die Elemente von X **Erzeuger** genannt.

Die Situation sei in Abbildung 2.1 erläutert.

Haben wir also eine Gleichung $s = t$ über $T(\Sigma, X)$ gegeben, so induziert

- die Einbettung von X in $\mathcal{T}(\Sigma, X)$ die Termfunktionen $s^{\mathcal{T}(\Sigma,X)}$ und $t^{\mathcal{T}(\Sigma,X)}$,
- φ die Termfunktionen $s^{\mathcal{F}}$ und $t^{\mathcal{F}}$ und
- α die Termfunktionen $s^{\mathcal{A}}$ und $t^{\mathcal{A}}$ (vgl. Abbildung 2.2).

$$\begin{tikzcd} X \arrow[r, "\varphi"] \arrow[dr, "\alpha"'] & F \arrow[d, "\tilde{\alpha}"] \\ & A \end{tikzcd}$$

Abbildung 2.1:

$$\begin{tikzcd} \mathcal{T}(\Sigma, X) \arrow[r, "\bar{\varphi}"] \arrow[dr, "\bar{\alpha}"] & \mathcal{F} \arrow[d, "\tilde{\alpha}"] \\ X \arrow[u, hook] \arrow[ur, "\varphi"] \arrow[r, "\alpha"'] & \mathcal{A} \end{tikzcd}$$

Abbildung 2.2:

Gilt nun $(\mathcal{F}, \varphi) \models s = t$, also $s\bar{\varphi} = t\bar{\varphi}$, wobei $\bar{\varphi}$ die homomorphe Fortsetzung von φ bezeichne, so folgt mit $\alpha = \varphi\tilde{\alpha}$ und dem Prinzip der endlichen algebraischen Induktion (Induktion über den Termaufbau) auch $s\bar{\varphi}\tilde{\alpha} = t\bar{\varphi}\tilde{\alpha}$ und somit $s\bar{\alpha} = t\bar{\alpha}$, was bedeutet, daß $\mathcal{A} \models s = t$. Da $\mathcal{A}$ beliebig ist, gilt also, daß jede in $\mathcal{F}$ bzgl. φ gültige Gleichung in jeder Algebra $\mathcal{A}$ von $\mathfrak{K}$ gilt.

Sind $\mathcal{F}_1$ und $\mathcal{F}_2$ freie Algebren für eine Klasse $\mathfrak{K}$ von Σ-Algebren mit Erzeugermenge X bzw. Y und gilt $|X| = |Y|$, so kann man zeigen, daß diese isomorph sind. Identifiziert man isomorphe Algebren (unproblematisch bei unter Isomorphismen abgeschlossenen Klassen von Algebren), so kann man von *der* freien Algebra von $\mathfrak{K}$ mit Erzeugermenge X sprechen.

Beispiel 2.3.11
Die freie Algebra der Klasse aller Σ-Algebren ist $\mathcal{T}(\Sigma, X)$, denn nach dem Prinzip der endlichen algebraischen Induktion (Satz 2.2.12) existiert die gewünschte Fortsetzung (vgl. Definition) und $\mathcal{T}(\Sigma, X)$ ist als Σ-Algebra in der Klasse aller Σ-Algebren enthalten. Wir haben also, daß eine Gleichung genau dann in allen Σ-Algebren gilt, wenn sie in $\mathcal{T}(\Sigma, X)$ gilt. Man beachte allerdings, daß für $s, t \in T(\Sigma, X)$ genau dann $\mathcal{T}(\Sigma, X) \models s = t$ gilt, wenn s syntaktisch gleich t ist.

Allgemein muß für eine Klasse $\mathfrak{K}$ von Algebren die freie Algebra von $\mathfrak{K}$ nicht existieren. Der nächste Satz liefert uns aber für gewisse Klassen von Σ-Algebren die Existenz einer freien Algebra:

[8] Man beachte, daß $I(\mathfrak{K}) \subseteq H(\mathfrak{K})$ und es deshalb ausreicht, den Abschluß unter H zu betrachten.

Satz 2.3.12 (Existenz freier Algebren; [We92, Satz 3.15])
Jede unter den Operatoren I, S und P abgeschlossene nichttriviale Klasse $\mathfrak{K}$ von Σ-Algebren (insbesondere jede Varietät) besitzt eine freie Algebra.

Wie sieht nun eine freie Algebra (bis auf Isomorphie) für solche Klassen aus? Das Beispiel legt uns nahe, die freie Algebra mit Hilfe der Termalgebra $\mathcal{T}(\Sigma, X)$ zu beschreiben.

Wir stellen folgende Überlegungen an:

Lemma 2.3.13 ([Ih93, 6.3.7])
Es sei $\mathfrak{K}$ eine Klasse von Σ-Algebren und $\mathcal{T}(\Sigma, X)$ die Σ-Termalgebra über der Variablenmenge X. Dann gilt

$$G_X(\mathfrak{K}) = \bigcap\{Kern\,\varphi \ : \ \varphi : \mathcal{T}(\Sigma, X) \to \mathcal{A},\ \mathcal{A} \in \mathfrak{K}\}$$

Das Lemma besagt insbesondere, daß $G_X(\mathfrak{K}) \in Con\,\mathcal{T}(\Sigma, X)$ ist, was einem erlaubt, die Faktoralgebra $\mathcal{T}(\Sigma, X)/G_X(\mathfrak{K})$ zu betrachten:

Satz 2.3.14 ([Ih93, 6.3.9])
Sei $\mathfrak{K}$ eine Klasse von Σ-Algebren, $\bar{x} := [x](G_X(\mathfrak{K}))$ und $\bar{X} := \{\bar{x} : x \in X\}$, wobei $[x](G_X(\mathfrak{K}))$ die Kongruenzklasse von x bzgl. $G_X(\mathfrak{K})$ bezeichne. Dann gibt es für jede Algebra $\mathcal{A} \in \mathfrak{K}$ und jede Abbildung $\alpha : \bar{X} \to A$ genau einen Homomorphismus $\tilde{\alpha} : \mathcal{T}(\Sigma, X)/G_X(\mathfrak{K}) \to \mathcal{A}$, der α fortsetzt, d.h. mit $\tilde{\alpha}|_{\bar{X}} = \alpha$.

Die Faktoralgebra $\mathcal{F}_{\mathfrak{K}}(X) := \mathcal{T}(\Sigma, X)/G_X(\mathfrak{K})$ ist also für eine unter I, S, P abgeschlossene Klasse $\mathfrak{K}$ eine freie Algebra, das heißt, für alle $s, t \in T(\Sigma, X)$ gilt

$$\mathfrak{K} \models s = t \ \Leftrightarrow\ \mathcal{F}_{\mathfrak{K}}(X) \models s = t.$$

$\mathcal{F}_{\mathfrak{K}}(X)$ wird die **freie Algebra** von $\mathfrak{K}$ über der Erzeugermenge X genannt.

2.3.2 Gleichungsdefinierte Klassen

Klassen, deren Elemente eindeutig durch Gleichungen beschrieben werden können, heißen *gleichungsdefinierte Klassen*:

Definition 2.3.15 (gleichungsdefinierte Klassen)
*Man nennt eine Klasse $\mathfrak{K}$ von Σ-Algebren **gleichungsdefiniert**, falls ein Gleichungssystem E mit $\mathfrak{K} = M(E)$ existiert.*

Erfüllt $\mathfrak{K}$ ein Gleichungssystem E, d.h. $\mathcal{A} \models E$ für alle $\mathcal{A} \in \mathfrak{K}$, so folgt $\mathcal{A} \in M(E)$ für alle $\mathcal{A} \in \mathfrak{K}$, d.h. $\mathfrak{K} \subseteq M(E)$. Die Frage ist nun, wann $M(E) \subseteq \mathfrak{K}$ gilt. Der folgende Satz von Birkhoff liefert die Antwort:

Satz 2.3.16 (Erster Hauptsatz der Gleichungstheorie; [Ih93, 6.3.18])
Eine Klasse $\mathfrak{K}$ von Algebren ist genau dann gleichungsdefiniert, wenn $\mathfrak{K}$ eine Varietät ist.

Dieser Satz rechtfertigt, daß die Menge $M(E)$ für eine gegebene Menge von Gleichungen E auch die **von E definierte Varietät** genannt wird.

2.3.3 Gleichungstheorien

In diesem Abschnitt wollen wir untersuchen, wie sich die Menge der in $\mathfrak{K}$ gültigen Gleichungen $G_X(\mathfrak{K})$ beschreiben läßt. Dazu definieren wir den Begriff der *Gleichungstheorie.*

Definition 2.3.17 (Gleichungstheorien)
Ein Gleichungssystem $E \subseteq T(\Sigma, X) \times T(\Sigma, X)$ heißt ***Gleichungstheorie*** *über X, falls es eine Klasse $\mathfrak{K}$ von Algebren mit $E = G_X(\mathfrak{K})$ gibt.*

Die Frage ist also, wie eine Menge von Gleichungen aussieht, die eine Gleichungstheorie ist.

Bemerkung 2.3.18 ([Ih93, S. 94 unten])
Für jede Gleichungstheorie $G_X(\mathfrak{K})$ gilt offenbar:

(G1)	*für $s \in T(\Sigma, X)$ gilt $s = s \in G_X(\mathfrak{K})$*	*(Reflexivität)*
(G2)	*für $s = t \in G_X(\mathfrak{K})$ folgt $t = s \in G_X(\mathfrak{K})$*	*(Symmetrie)*
(G3)	*für $s = t, t = u \in G_X(\mathfrak{K})$ folgt $s = u \in G_X(\mathfrak{K})$*	*(Transitivität)*
(G4)	*für $f \in \Sigma^{(n)}$ und $s_i = t_i \in G_X(\mathfrak{K})$ für $i = 1, \ldots, n$ folgt $f(s_1, \ldots, s_n) = f(t_1, \ldots, t_n) \in G_X(\mathfrak{K})$*	*(Verträglichkeit)*
(G5)	*aus $s(x_1, \ldots, x_n) = t(x_1, \ldots, x_n) \in G_X(\mathfrak{K})$ und $u_1, \ldots, u_n \in T(\Sigma, X)$ folgt $s(u_1, \ldots, u_n) = t(u_1, \ldots, u_n) \in G_X(\mathfrak{K})$*	*(Vollinvarianz)*

Die Regeln (G1) - (G4) sagen aus, daß jede Gleichungstheorie $G_X(\mathfrak{K})$ eine Kongruenzrelation von $\mathcal{T}(\Sigma, X)$ sein muß. Regel (G5) besagt, daß Gleichungen weiterhin gelten, wenn man Variablen durch Terme substituiert. Da Substitutionen spezielle Endomorphismen sind, kann (G5) auch folgendermaßen formuliert werden:

(G5') Aus $\varphi \in End\, \mathcal{T}(\Sigma, X)$ und $s = t \in G_X(\mathfrak{K})$ folgt $s\varphi = t\varphi \in G_X(\mathfrak{K})$

Definition 2.3.19 (vollinvariant; [Ih93, 6.3.20])
Eine Kongruenzrelation θ einer Algebra $\mathcal{A}$ heißt ***vollinvariant****, wenn sie mit allen Endomorphismen von $\mathcal{A}$ verträglich ist, das heißt, wenn aus $\varphi \in End\, \mathcal{A}$ und $a\ \theta\ b$ immer $a\varphi\ \theta\ b\varphi$ folgt. Die kleinste vollinvariante Kongruenzrelation*

$\mathcal{E}$, die eine Relation E enthält, heißt die ***von E erzeugte vollinvariante Kongruenzrelation*** *und wird mit $\langle E \rangle_{\mathsf{SC}}$ bezeichnet.*[9]

Das heißt, die in einer Klasse gültigen Gleichungen sind Obermenge einer vollinvarianten Kongruenzrelation. Daß jede vollinvariante Kongruenzrelation andererseits genau die Gleichungen einer Klasse beschreibt, sagt folgender Satz von Birkhoff.

Satz 2.3.20 (Vollständigkeitssatz der Gleichungslogik; [Ih93, 6.3.23])
Ein Gleichungssystem $E \subseteq T(\Sigma, X) \times T(\Sigma, X)$ ist genau dann eine Gleichungstheorie, wenn E eine vollinvariante Kongruenzrelation von $\mathcal{T}(\Sigma, X)$ ist.

Wir definieren daher:

Definition 2.3.21 (von E erzeugte Gleichungstheorie)
Sei E ein Gleichungssystem. Dann heißt $\mathcal{E} := \langle E \rangle_{\mathsf{SC}}$ die ***von E erzeugte Gleichungstheorie****.*

Satz 2.3.20 umformuliert besagt, daß die aus der mathematischen Logik stammenden Begriffe „folgern“ und „beweisen“ hier äquivalent sind.

Definition 2.3.22 (folgern, beweisen)

- *Eine Gleichung $s = t$* ***folgt*** *aus einem Gleichungssystem E (kurz: $E \models s = t$), falls für jede E-Algebra $\mathcal{A}$ gilt: $\mathcal{A} \models s = t$*
- *Eine Gleichung $s = t$ ist aus E* ***beweisbar*** *(kurz $E \vdash s = t$), wenn sie aus E mit Hilfe der Regeln (G1)-(G5) herleitbar ist.*

Für eine Gleichung $s = t$ und ein Gleichungssystem E gilt dann:

$$E \models s = t \;\Leftrightarrow\; s = t \in G_X(M(E)) \;\Leftrightarrow\; s = t \in \langle E \rangle_{\mathsf{SC}}.$$

Statt $s = t \in \mathcal{E}$ schreiben wir kürzer $s =_{\mathcal{E}} t$, wobei $\mathcal{E} = \langle E \rangle_{\mathsf{SC}}$.

2.4 Kategorien

Da wir im nächsten Kapitel Unifikation auch aus der Sicht der Kategorientheorie beschreiben, benötigen wir auch einige Kenntnisse über Kategorien. Die im folgenden genannten Ausführungen entstammen im wesentlichen [HeSt79], einer leicht verständlichen Einführung in die Kategorientheorie.

Kategorien bestehen im wesentlichen aus Objekten und Morphismen zwischen diesen Objekten:

[9] SC steht hierbei für *substitution invariant closure*

Definition 2.4.1 (Kategorie)
*Eine **Kategorie** ist ein Tupel $\mathfrak{C} = (\mathfrak{O}, \mathfrak{M}, dom, cod, \circ)$ mit folgenden Eigenschaften:*

1. *$\mathfrak{O}$ ist eine Klasse, deren Elemente $\mathfrak{C}$-**Objekte** genannt werden.*
2. *$\mathfrak{M}$ ist eine Klasse, deren Elemente $\mathfrak{C}$-**Morphismen** genannt werden.*
3. *dom, cod sind Funktionen von $\mathfrak{M}$ nach $\mathfrak{O}$. $dom\, f$ heißt **Domain** von f und $cod\, f$ heißt **Codomain** von f.*
4. *$\circ$ ist eine Funktion von*

$$D = \{(f, g) : f, g \in \mathfrak{M} \text{ und } cod\, f = dom\, g\}$$

*nach $\mathfrak{M}$. $\circ$ wird **Kompositionsfunktion** genannt. Statt $\circ(f, g)$ schreibt man $f \circ g$ und sagt $f \circ g$ ist genau dann definiert, wenn $(f, g) \in D$.*

Zusätzlich müssen die folgenden Bedingungen erfüllt sein:

1. *Falls $f \circ g$ definiert ist, so ist $dom\, f \circ g = dom\, f$ und $cod\, f \circ g = cod\, g$.*
2. *Falls $f \circ g$ und $g \circ h$ definiert sind, so gilt $(f \circ g) \circ h = f \circ (g \circ h)$.*
3. *Für jedes $\mathfrak{C}$-Objekt A existiert ein $\mathfrak{C}$-Morphismus e mit $dom\, e = A = cod\, e$ und*
   (a) $f \circ e = f$, falls $f \circ e$ definiert
   (b) $e \circ g = g$, falls $e \circ g$ definiert
4. *Für jedes Paar (A, B) von $\mathfrak{C}$-Objekten ist die Klasse*

$$Hom(A, B) = \{f : f \in \mathfrak{M}, dom\, f = A \text{ und } cod\, f = B\}$$

eine Menge.

Man kann leicht zeigen, daß das e aus 3. eindeutig ist, so daß wir statt $e : A \rightarrow A$ auch 1_A schreiben und von der **$\mathfrak{C}$-Identität** auf A sprechen.

Die recht allgemeine Definition erlaubt die Anwendung der Kategorientheorie in vielen Bereichen. In dieser Arbeit werden die Objekte freie Algebren und die Morphismen die Homomorphismen zwischen den freien Algebren sein (vgl. Kapitel 3.5).

Für eine gegebene Kategorie $\mathfrak{C}$ bezeichne $Ob\, \mathfrak{C}$ die Klasse der $\mathfrak{C}$-Objekte und $Mor\, \mathfrak{C}$ die Klasse der $\mathfrak{C}$-Morphismen. Obwohl Morphismen nicht notwendigerweise Funktionen sein müssen, schreiben wir für $f \in Hom(A, B)$ auch $f : A \rightarrow B$.

Für die weiteren Überlegungen benötigen wir noch einige Begriffe:

Definition 2.4.2 (initial, terminal, Nullobjekt)

- *Ein Objekt X einer Kategorie $\mathfrak{C}$ heißt* ***initial*** *für $\mathfrak{C}$, falls $|Hom(X,B)| = 1$ für alle $\mathfrak{C}$-Objekte B.*
- *Ein Objekt X einer Kategorie $\mathfrak{C}$ heißt* ***terminal*** *für $\mathfrak{C}$, falls $|Hom(B,X)| = 1$ für alle $\mathfrak{C}$-Objekte B.*
- *Ein Objekt X einer Kategorie $\mathfrak{C}$ heißt* ***Nullobjekt*** *für $\mathfrak{C}$, falls X initial und terminal ist.*

Definition 2.4.3 (konstant, cokonstant, Nullmorphismus)
Ein $\mathfrak{C}$-Morphismus $f : A \to B$ heißt

- ***konstant****, falls für jedes $C \in Ob\,\mathfrak{C}$ und für alle $r, s \in Hom(C,A)$ gilt $r \circ f = s \circ f$.*
- ***cokonstant****, falls für jedes $C \in Ob\,\mathfrak{C}$ und für alle $r, s \in Hom(B,C)$ gilt $f \circ r = f \circ s$.*
- ***Nullmorphismus****, falls f konstant und cokonstant ist.*

Definition 2.4.4 (punktierte Kategorie)
Eine Kategorie $\mathfrak{C}$ heißt punktiert, falls für alle $A, B \in Ob\,\mathfrak{C}$ gilt, daß $Hom(A,B)$ einen Nullmorphismus enthält.

Einen Nullmorphismus von A auf B schreiben wir oft als $0_{AB} : A \to B$ oder einfach als 0, wenn A und B aus dem Kontext bekannt sind.

Bisweilen möchte man sich nicht nur die *Struktur* einer Kategorie ansehen, sondern diese mit der einer anderen Kategorie vergleichen. Dazu bedient man sich „strukturerhaltender Abbildungen", die man sich ähnlich wie Homomorphismen bei Algebren vorstellen kann:

Definition 2.4.5 (Funktor)
Seien $\mathfrak{C}$ und $\mathfrak{D}$ Kategorien. Ein Funktor von $\mathfrak{C}$ nach $\mathfrak{D}$ ist ein Tripel $(\mathfrak{C}, F, \mathfrak{D})$, wobei F eine Abbildung von $Mor\,\mathfrak{C}$ nach $Mor\,\mathfrak{D}$ ist, die die folgenden Bedingungen erfüllt:

1. *Für jede $\mathfrak{C}$-Identität e ist $(e)F$ eine $\mathfrak{D}$-Identität.*
2. *Für alle $f, g \in Mor\,\mathfrak{C}$ gilt $(f \circ g)F = (f)F \circ (g)F$, falls $f \circ g$ definiert ist.*

Natürlich schreiben wir statt $(\mathfrak{C}, F, \mathfrak{D})$ auch $F : \mathfrak{C} \to \mathfrak{D}$.

Da für jedes Objekt eine eindeutige Identität existiert und ein Funktor Identiäten auf Identitäten abbildet, erhält man für jeden Funktor auch eine Abbildung der Objekte von $\mathfrak{C}$ auf Objekte von $\mathfrak{D}$. Hierfür schreiben wir kurz $F : Ob\,\mathfrak{C} \to Ob\,\mathfrak{D}$.

Definition 2.4.6 (Isomorphe Kategorien)
Ein Funktor $F : \mathfrak{C} \to \mathfrak{D}$ heißt ***Isomorphismus*** *von $\mathfrak{C}$ nach $\mathfrak{D}$, falls ein Funktor $G : \mathfrak{D} \to \mathfrak{C}$ existiert mit $F \circ G = 1_{\mathfrak{C}}$ und $G \circ F = 1_{\mathfrak{D}}$, d.h. $H \circ (F \circ G) = H$, $(F \circ G) \circ H = H$ und $H \circ (G \circ F) = H$, $(G \circ F) \circ H = H$ für alle Funktoren H, für die die Komposition definiert ist. Dabei ist $H \circ H'$ genau dann definiert, wenn $H : \mathfrak{C} \to \mathfrak{D}$ und $H' : \mathfrak{D} \to \mathfrak{C}$, und zwar durch $(f)(H \circ H') = ((f)H)H'$ für alle $f \in Mor\,\mathfrak{C}$.*

$\mathfrak{C}$ und $\mathfrak{D}$ heißen ***isomorph*** *($\mathfrak{C} \cong \mathfrak{D}$), falls es einen Isomorphismus zwischen ihnen gibt.*

Für Funktoren, die Isomorphismen sind, kann man folgendes Resultat zeigen, das wir im nächsten Kapitel benötigen:

Lemma 2.4.7 (vgl. [HeSt79, 14.3])
Sei $F : \mathfrak{C} \to \mathfrak{D}$ ein Funktor. Dann sind die folgenden Aussagen äquivalent.

1. *F ist ein Isomorphismus.*

2. *Die Abbildung $F : Mor\,\mathfrak{C} \to Mor\,\mathfrak{D}$ ist eine Bijektion.*

3. *Die Einschränkung von F auf $Hom(A, A')$, also F betrachtet als Abbildung von $Hom(A, A')$ auf $Hom(FA, FA')$, kurz*

   $$F|_{Hom(A,A')}^{Hom(FA,FA')}$$

   ist injektiv und surjektiv für jedes $A, A' \in \mathfrak{C}$ und die zugehörige Objektfunktion $F : Ob\,\mathfrak{C} \to Ob\,\mathfrak{D}$ ist eine Bijektion.

Definition 2.4.8 (Produkt, Coprodukt, Biprodukt)

- *Ein* ***$\mathfrak{C}$-Produkt*** *einer Familie $(A_i)_{i\in I}$ von $\mathfrak{C}$-Objekten ist ein Paar*

  $$\left(\prod(A_i)_{i\in I}, (\pi_i)_{i\in I}\right),$$

  welches die folgenden Bedingungen erfüllt

  1. *$\prod(A_i)_{i\in I}$ ist ein $\mathfrak{C}$-Objekt.*
  2. *für jedes $j \in I$ ist $\pi_j : \prod(A_i)_{i\in I} \to A_j$ ein $\mathfrak{C}$ Morphismus, der* ***Projektion*** *von $\prod(A_i)_{i\in I}$ auf A_j genannt wird.*
  3. *für jedes Paar $(C, (f_i)_{i\in I})$, wobei C ein $\mathfrak{C}$-Objekt ist und für jedes $j \in I$ gilt $f_j : C \to A_j$, existiert ein eindeutiger $\mathfrak{C}$-Morphismus $\langle f_i \rangle : C \to \prod(A_i)_{i\in I}$, so daß folgendes Diagramm*

  $$\begin{tikzcd}
  C \arrow[r, dashed, "\langle f_i \rangle"] \arrow[dr, "f_j"'] & \prod(A_i)_{i\in I} \arrow[d, "\pi_j"] \\
  & A_j
  \end{tikzcd}$$

kommutiert.

- *Ein* ***$\mathfrak{C}$-Coprodukt*** *einer Familie $(A_i)_{i \in I}$ von $\mathfrak{C}$-Objekten ist ein Paar $((\iota_i)_{i \in I}, \coprod(A_i)_{i \in I},)$, welches die folgenden Bedingungen erfüllt*

    1. *$\coprod(A_i)_{i \in I}$ ist ein $\mathfrak{C}$-Objekt.*
    2. *für jedes $j \in I$ ist $\iota_j : A_j \to \coprod(A_i)_{i \in I}$ ein $\mathfrak{C}$-Morphismus, der* ***Injektion*** *von A_j auf $\coprod(A_i)_{i \in I}$ genannt wird.*
    3. *für jedes Paar $((f_i)_{i \in I}, C)$, wobei C ein $\mathfrak{C}$-Objekt ist und für jedes $j \in I$ gilt $f_j : A_j \to C$, existiert ein eindeutiger $\mathfrak{C}$-Morphismus $[f_i] : \coprod(A_i)_{i \in I} \to A_j$, so daß folgendes Diagramm*

    $$\begin{tikzcd} \coprod(A_i)_{i \in I} \arrow[rr, dashed, "{[f_i]}"] & & C \\ A_j \arrow[u, "\iota_j"] \arrow[urr, "f_j"'] & & \end{tikzcd}$$

    kommutiert.

- *Sei $\mathfrak{C}$ eine punktierte Kategorie und $(A_i)_{i \in I}$ eine Familie von $\mathfrak{C}$-Objekten. Die Familie $(\iota_i, B, \pi_i)_{i \in I}$ heißt dann* ***$\mathfrak{C}$-Biprodukt*** *von $(A_i)_{i \in I}$, falls die folgenden Bedingungen erfüllt sind:*

    1. *$(B, \pi_i)_{i \in I}$ ist Produkt von $(A_i)_{i \in I}$,*
    2. *$(\iota_i, B)_{i \in I}$ ist Coprodukt von $(A_i)_{i \in I}$,*
    3. *$\iota_j \circ \pi_k = \delta_{jk}$ für alle $j, k \in I$,*

    wobei $\delta_{jk} : A_j \to A_k$ definiert ist durch

    $$\delta_{jk} = \begin{cases} 1_{A_j} & \text{falls } j = k \\ 0 & \text{sonst} \end{cases}$$

- *Eine Kategorie $\mathfrak{C}$ hat (endliche) Produkte, Coprodukte, Biprodukte, falls für jede (endliche) Familie von $\mathfrak{C}$-Objekten Produkte, Coprodukte bzw. Biprodukte existieren.*[10]

[10] Im letzten Fall muß $\mathfrak{C}$ natürlich punktiert sein.

Kapitel 3

Unifikation

Sei V eine abzählbar unendliche Menge von Variablen. Da einerseits eine Substitution nur endlich viele Variablen nicht festläßt und außerdem jeder Term und damit auch jede endliche Menge von Termen nur endlich viele Variablen enthält, ist es zweckmäßig, nur mit endlichen Variablenmengen zu rechnen. Es seien daher im folgenden X, Y, Z endliche Teilmengen von V, die wir meist schreiben als $X = \{x_1, \ldots, x_n\}$, $Y = \{y_1, \ldots, y_m\}$, $Z = \{z_1, \ldots, z_l\}$, und $\mathcal{T}(\Sigma, X)$, $\mathcal{T}(\Sigma, Y)$ bzw. $\mathcal{T}(\Sigma, Z)$ die Σ-Termalgebra über X, Y bzw. Z.

3.1 Syntaktische Unifikation

Unifikation im ursprünglichen Sinn wird definiert als Suche nach einer geeigneten endlichen Variablenmenge Y und einer Substitution $\sigma : \mathcal{T}(\Sigma, X) \rightarrow \mathcal{T}(\Sigma, Y)$ mit

$$s\sigma = t\sigma$$

für Terme $s, t \in \mathcal{T}(\Sigma, X)$, notiert als Gleichung $s \stackrel{?}{=} t$.[1] Ein derartiges σ wird Unifikator genannt.

Unifikatoren sind also Substitutionen, die ein Paar von Termen (s, t) auf (syntaktisch) gleiche Terme abbilden. Mit Satz 2.2.12 gilt

$$s\sigma = t\sigma \Leftrightarrow \emptyset \models \forall Y \;\; s\sigma = t\sigma,$$

wobei $\forall Y$ als Abkürzung für $\forall y_1 \ldots \forall y_m$ zu verstehen ist.

Um die Analogie zur Definition von E- und $\mathcal{A}$-Unifikatoren zu verdeutlichen, benutzen wir obige Eigenschaft zur Definition von Unifikatoren, die wir zu deren Unterscheidung von E- und $\mathcal{A}$-Unifikatoren als syntaktische Unifikatoren

[1] Y erhält man, indem man $\sigma' : \mathcal{T}(\Sigma, X) \rightarrow \mathcal{T}(\Sigma, V)$ sucht und auf $\sigma : \mathcal{T}(\Sigma, X) \rightarrow \mathcal{T}(\Sigma, Y)$ einschränkt, wobei $Var(X\sigma') \subseteq Y$ gelte.

bezeichnen. Weiterhin machen wir von der Konvention Gebrauch, daß ungebundene Variablen allquantifiziert sein sollen. Außerdem wird die Definition dahingehend erweitert, daß man statt einer Gleichung eine Menge Γ von Gleichungen, ein sogenanntes **Gleichungssystem**, betrachtet:

Definition 3.1.1 (Syntaktischer Unifikator)
Sei $\Gamma := \{(s_1, t_1), \ldots, (s_k, t_k)\}$ *mit* $s_i, t_i \in \mathcal{T}(\Sigma, X), i \in \{1, \ldots, k\}$.

- *Dann heißt* $\sigma \in Subs(\mathcal{T}(\Sigma, X), \mathcal{T}(\Sigma, Y))$ ***syntaktischer Unifikator*** *von* Γ, *falls für alle* $i \in \{1, \ldots, k\}$

  $$\emptyset \models s_i\sigma = t_i\sigma.$$

- *Mit* $U_\emptyset(\Gamma)$ *bezeichnen wir die Menge aller Unifikatoren von* Γ.

- *Das Paar* $(\Gamma, \emptyset)$ *wird* ***Unifikationsproblem*** *genannt.*

3.2 Unifikation in Gleichungstheorien

Bei der Unifikation in Gleichungstheorien hat man Gleichungen E, **Identitäten** genannt, auf der Menge der Terme gegeben. Statt eine Susbstitution σ zu finden, so daß zu gegebenen Termen s und t jede Σ-Algebra die Formel $\forall Y \; s\sigma = t\sigma$ erfüllt, verlangt man dies nur von jeder E-Algebra, also jeder Σ-Algebra, die den Identitäten aus E genügt.

Im vorherigen Kapitel wurde gezeigt, daß man dazu stellvertretend in der Termalgebra faktorisiert nach der von E erzeugten vollinvarianten Kongruenzrelation rechnen kann. Wir definieren daher:

Definition 3.2.1 (E-Unifikator)
Seien E *eine Menge von Identitäten und* $\Gamma := \{(s_1, t_1), \ldots, (s_k, t_k)\}$ *mit* $s_i, t_i \in \mathcal{T}(\Sigma, X), i \in \{1, \ldots, k\}$.

- *Dann heißt* $\sigma \in Subs(\mathcal{T}(\Sigma, X), \mathcal{T}(\Sigma, Y)/\mathcal{E})$ ***E-Unifikator*** *von* Γ, *falls*[2]

  $$E \models s_i\sigma = t_i\sigma$$

  für alle $i \in \{1, \ldots, k\}$, *wobei* $\mathcal{E} = \langle E \rangle_{\mathsf{SC}}$.

- *Mit* $U_E(\Gamma)$ *bezeichnen wir die Menge aller Unifikatoren von* Γ.

- *Das Paar* (Γ, E) *wird* ***Unifikationsproblem*** *genannt.*

[2] zur Bedeutung von $E \models s_i\sigma = t_i\sigma$ vergleiche nachfolgende Bemerkung

Zunächst ist nicht klar, was $E \models s_i\sigma = t_i\sigma$ bedeuten soll, da $s_i\sigma$ und $t_i\sigma$ Elemente von $\mathcal{T}(\Sigma, Y)/\mathcal{E}$ sind und daher $s_i\sigma = t_i\sigma$ nicht direkt als syntaktischer Ausdruck behandelt werden kann, falls $E \neq \emptyset$. Wir wollen unter $s_i\sigma$ bzw. $t_i\sigma$ beliebige Repräsentanten aus $\mathcal{T}(\Sigma, Y)$ von $s_i\sigma$ bzw. $t_i\sigma$ verstehen. Der Ausdruck $E \models s_i\sigma = t_i\sigma$ ist unabhängig von der Wahl der Repräsentanten, da jedes Modell von E per Definition nicht zwischen verschiedenen Repräsentanten unterscheidet. $E \models s_i\sigma = t_i\sigma$ ist auf diese Weise wohldefiniert.

Ein Unifikator $\sigma : \mathcal{T}(\Sigma, X) \rightarrow \mathcal{T}(\Sigma, Y)/\mathcal{E}$ kann oBdA auch mit einem Unifikator $\hat{\sigma} : \mathcal{T}(\Sigma, X)/\mathcal{E} \rightarrow \mathcal{T}(\Sigma, Y)/\mathcal{E}$ auf folgende Weise identifiziert werden:

Lemma 3.2.2

1. *Sei eine Substitution $\sigma : \mathcal{T}(\Sigma, X) \rightarrow \mathcal{T}(\Sigma, Y)/\mathcal{E}$ gegeben. Dann existiert eine Substitution $\hat{\sigma} : \mathcal{T}(\Sigma, X)/\mathcal{E} \rightarrow \mathcal{T}(\Sigma, Y)/\mathcal{E}$ mit*

$$t\sigma = [t]\hat{\sigma}$$

für alle $t \in T(\Sigma, X)$, wobei $[t]$ die Kongruenzklasse von t bzgl. $\mathcal{E}$ bezeichnet.

2. *Sei eine Substitution $\hat{\sigma} : \mathcal{T}(\Sigma, X)/\mathcal{E} \rightarrow \mathcal{T}(\Sigma, Y)/\mathcal{E}$ gegeben. Dann existiert eine Substitution $\sigma : \mathcal{T}(\Sigma, X) \rightarrow \mathcal{T}(\Sigma, Y)/\mathcal{E}$ mit*

$$[t]\hat{\sigma} = t\sigma$$

für alle $t \in T(\Sigma, X)$.

Beweis

zu 1) Sei σ gegeben durch $x_i \mapsto [t_i]$, $i \in \{1, \ldots, n\}$. $\iota : \mathcal{T}(\Sigma, X) \rightarrow \mathcal{T}(\Sigma, X)/\mathcal{E}$ wird dann als kanonischen Einbettungshomomorphismus definiert durch $x_i \mapsto [x_i]$ und $\hat{\sigma} : \mathcal{T}(\Sigma, X)/\mathcal{E} \rightarrow \mathcal{T}(\Sigma, Y)/\mathcal{E}$ durch $[x_i] \mapsto [t_i]$.[3] Da $x_i\sigma = [t_i] = [x_i]\hat{\sigma} = x_i\iota\hat{\sigma}$ ist, gilt $\sigma = \iota\hat{\sigma}$. Mit $t\iota = [t]$ (vgl. Lemma 2.2.9) folgt dann

$$t\sigma = t\iota\hat{\sigma} = [t]\hat{\sigma}$$

für alle $t \in \mathcal{T}(\Sigma, X)$.

zu 2) Sei $\hat{\sigma}$ gegeben durch $[x_i] \mapsto [t_i]$, $i \in \{1, \ldots, n\}$. Definiere den Homomorphismus $\sigma : \mathcal{T}(\Sigma, X) \rightarrow \mathcal{T}(\Sigma, Y)/\mathcal{E}$ durch

$$x_i \mapsto [t_i]$$

[3] beachte, daß $\mathcal{T}(\Sigma, X)/\mathcal{E}$ frei auf $\bar{X} := \{[x] : x \in X\}$ für die durch $\mathcal{E}$ erzeugte Varietät ist. Somit ist $\hat{\sigma}$ wohldefiniert.

Dadurch ist σ wohldefiniert. Zu zeigen ist, daß

$$[t]\hat{\sigma} = t\sigma$$

für alle $t \in \mathcal{T}(\Sigma, X)$. Wir zeigen dies per Induktion über den Termaufbau.
Induktionsanfang:
Sei $t = x_i$. $x_i\sigma = [t_i] = [x_i]\hat{\sigma}$.
Sei $t = fx_1 \ldots x_n$, $f \in \Sigma^{(n)}$. Dann ist

$$\begin{aligned}
t\sigma &= f^{\mathcal{T}(\Sigma,X)/\mathcal{E}}(x_1\sigma, \ldots, x_n\sigma) \\
&= f^{\mathcal{T}(\Sigma,X)/\mathcal{E}}([t_1], \ldots, [t_n]) \\
&= f^{\mathcal{T}(\Sigma,X)/\mathcal{E}}([x_1]\hat{\sigma}, \ldots, [x_n]\hat{\sigma}) \\
&= f^{\mathcal{T}(\Sigma,X)/\mathcal{E}}([x_1], \ldots, [x_n])\hat{\sigma} \\
&= [f^{\mathcal{T}(\Sigma,X)}(t_1, \ldots, t_n)]\hat{\sigma} \\
&= [t]\hat{\sigma}
\end{aligned}$$

Induktionsschritt:
Sei $t = fs_1 \ldots s_n$, $f \in \Sigma^{(n)}$. Dann ist

$$\begin{aligned}
t\sigma &= f^{\mathcal{T}(\Sigma,X)/\mathcal{E}}(s_1\sigma, \ldots, s_n\sigma) \\
&\overset{\text{IV}}{=} f^{\mathcal{T}(\Sigma,X)/\mathcal{E}}([s_1]\hat{\sigma}, \ldots, [s_n]\hat{\sigma}) \\
&= f^{\mathcal{T}(\Sigma,X)/\mathcal{E}}([s_1], \ldots, [s_n])\hat{\sigma} \\
&= [f^{\mathcal{T}(\Sigma,X)}(s_1, \ldots, s_n)]\hat{\sigma} \\
&= [t]\hat{\sigma}
\end{aligned}$$

Somit ist die Behauptung gezeigt.

□

Wir werden daher in Zukunft einen E-Unifikator je nach Anwendung als einen Homomorphismus von $\mathcal{T}(\Sigma, X)$ oder von $\mathcal{T}(\Sigma, X)/\mathcal{E}$ betrachten, insbesondere identifizieren wir x_i und $[x_i]$.[4]

Setzen wir $E = \emptyset$ und damit $\mathcal{E} := \langle E\rangle_{\mathsf{SC}} = \{(t,t) : t \in \mathcal{T}(\Sigma, X)\}$, so erhalten wir den Spezialfall des syntaktischen Unifikators. Also werden im folgenden syntaktische Unifikatoren nicht gesondert untersucht.

Abkürzend für $\mathcal{T}(\Sigma, X)/\langle E\rangle_{\mathsf{SC}}$ schreiben wir außerdem $\mathcal{F}_{\mathcal{E}}(X)$.

[4] was keine Probleme bei einer nichttrivialen, d.h. nicht 0- oder 1-elementigen, Algebra bedeutet.

3.3 Unifikation in Algebren

Während bei syntaktischen Unifikatoren das Rechnen in der Klasse aller Σ-Algebren bzw. stellvertretend dazu das Rechnen in der Σ-Termalgebra und bei der E-Unifikation das Rechnen in der Klasse aller E-Algebren bzw. stellvertretend dazu das Rechnen in einem Faktor der Termalgebra im Vordergrund steht, betrachtet man bei der Unifikation in Algebren *eine* konkrete Σ-Algebra $\mathcal{A}$.

Um die bisher gewonnenen Definitionen und Techniken verwenden zu können, stellt sich auch hier zunächst die Frage nach einer Termalgebra, die es erlaubt, in ihr weitestgehend stellvertretend für die Algebra $\mathcal{A}$ rechnen zu können. Dazu halten wir fest:

Satz 3.3.1
Sei $\mathcal{A}$ eine Σ-Algebra und $s = t$ eine Gleichung über $T(\Sigma, X)$. Dann gilt:

$$\mathcal{A} \models s = t \;\Leftrightarrow\; \mathcal{T}(\Sigma, X)/G_X(\{\mathcal{A}\}) \models s = t$$

Beweis
Zunächst zeigen wir, daß $\mathcal{A} \models s = t \Leftrightarrow \mathfrak{K} := HSP(\mathcal{A}) \models s = t$: Falls $\mathfrak{K} \models s = t$, so folgt mit $\mathcal{A} \in \mathfrak{K}$ per Definition auch $\mathcal{A} \models s = t$. Sei andererseits $\mathcal{A} \models s = t$. Nach Satz 2.3.7 gilt damit $H(\mathcal{A}) \models s = t$, $S(\mathcal{A}) \models s = t$ und $P(\mathcal{A}) \models s = t$.

$$\begin{aligned} P(\mathcal{A}) \models s = t \quad &\Rightarrow \quad \forall \mathcal{A}' \in P(\mathcal{A})\; \mathcal{A}' \models s = t \\ &\Rightarrow \quad \forall \mathcal{A}' \in P(\mathcal{A})\; S(\mathcal{A}') \models s = t \\ &\Rightarrow \quad \bigcup_{\mathcal{A}' \in P(\mathcal{A})} S(\mathcal{A}') \models s = t \\ &\Rightarrow \quad SP(\mathcal{A}) \models s = t \end{aligned}$$

Analog ergibt sich $\mathfrak{K} = HSP(\mathcal{A}) \models s = t$.

Nach Satz 2.3.9 ist $\mathfrak{K}$ Varietät und besitzt somit nach Satz 2.3.12 eine freie Algebra über X, die nach der Bemerkung zu Satz 2.3.14 isomorph zu $\mathcal{F} := \mathcal{T}(\Sigma, X)/G_X(\mathfrak{K}) = \mathcal{T}(\Sigma, X)/G_X(\{\mathcal{A}\})$ ist. Da $\mathcal{F}$ frei ist, gilt für alle $s', t' \in T(\Sigma, X)$, daß $\mathcal{F} \models s' = t' \Leftrightarrow \mathfrak{K} \models s' = t'$, also insbesondere $\mathcal{F} \models s = t \Leftrightarrow \mathfrak{K} \models s = t$. Insgesamt gilt also $\mathcal{A} \models s = t \Leftrightarrow \mathfrak{K} \models s = t \Leftrightarrow \mathcal{F} \models s = t$. □

Wir definieren daher:

Definition 3.3.2 ($\mathcal{A}$-Unifikator)
Sei $\mathcal{A}$ eine Σ-Algebra, $\Gamma = \{(s_1, t_1), \ldots, (s_k, t_k)\} \subseteq T(\Sigma, X)^2$.

- *Sei W eine Variablenmenge. Dann heißt die Algebra*

  $$\mathcal{F}_{\mathcal{A}}(W) := \mathcal{T}(\Sigma, W)/G_W(\{\mathcal{A}\})$$

  freie Algebra zu $\mathcal{A}$ *(über W).*

- *Eine Substitution* $\sigma : \mathcal{F}_{\mathcal{A}}(X) \to \mathcal{F}_{\mathcal{A}}(Y)$ *heißt* ***$\mathcal{A}$-Unifikator*** *von* Γ, *falls*

  $$\mathcal{F}_{\mathcal{A}}(Y) \models s_i\sigma = t_i\sigma$$

  für alle $i \in \{1, \ldots, k\}$.

- *Mit* $U_{\mathcal{A}}(\Gamma)$ *bezeichnen wir die Menge aller Unifikatoren von* Γ.

- *Das Paar* $(\Gamma, \mathcal{A})$ *wird dann auch* ***$\mathcal{A}$-Unifikationsproblem*** *genannt.*

Wir haben gesehen, daß unabhängig von E- oder $\mathcal{A}$-Unifikation stellvertretend für die durch E erzeugte Varietät bzw. für die Algebra $\mathcal{A}$ in einer freien Termalgebra gerechnet werden kann, da sich diese in Bezug auf die Gültigkeit von Gleichungen nicht unterscheiden. Daher wird im folgenden mit $\mathcal{F}(X)$ die Termalgebra $\mathcal{F}_{\mathcal{E}}(X) := \mathcal{T}(\Sigma, X)/\langle E\rangle_{\mathsf{SC}}$ oder $\mathcal{F}_{\mathcal{A}}(X) := \mathcal{T}(\Sigma, X)/G_X(\{\mathcal{A}\})$ bezeichnet, das heißt, wir verzichten auf die Angabe des Index E bzw. $\mathcal{A}$, sofern dieser aus dem Kontext hervorgeht.

Im Vorgriff auf Kapitel 4 sei bereits erwähnt, daß $\mathcal{F}(X)$ nur eingeschränkt stellvertretend für eine Algebra $\mathcal{A}$ in Bezug auf Lösbarkeit von Gleichungen ist.

3.4 Unifikationstypen

In der Regel ist man nicht an allen Unifikatoren eines Unifikationsproblems Γ interessiert, sondern nur an möglichst *aussagekräftigen*, *allgemeinen*. Dabei nennt man einen Unifikator σ allgemeiner als einen Unifikator τ, falls sich τ als *Spezialisierung* bzw. *Instanz* von σ ergibt. Beisweilen sagt man auch, daß sich τ durch σ faktorisieren läßt. Formal können wir dieses fassen, indem wir auf der Menge der Unifikatoren eine Quasiordnung einführen und möglichst kleine Elemente suchen:

Definition 3.4.1 (Allgemeinster Unifikator)
Seien $\sigma \in Subs(\mathcal{F}(X), \mathcal{F}(Y))$, $\tau \in Subs(\mathcal{F}(Y), \mathcal{F}(Z))$ *und* Γ *ein Unifikationsproblem mit* $X_0 := Var(\Gamma)$.

- τ *heißt* ***Instanz*** *oder* ***Spezialisierung*** *von* σ *bzgl.* Γ, *bzw.* τ *läßt sich bzgl.* Γ *durch* σ ***faktorisieren***, *falls es ein* $\lambda \in Subs(\mathcal{F}(Y), \mathcal{F}(Z))$ *gibt mit*

  $$\sigma\lambda|_{X_0} = \tau|_{X_0} \quad \text{d.h. } \forall x \in X_0 : x\sigma\lambda = x\tau$$

- *Die Quasiordnung* $\lesssim_\Gamma$ *sei definiert durch*

  $$\sigma \lesssim_\Gamma \tau \;:\Leftrightarrow\; \tau \text{ läßt sich bzgl. } \Gamma \text{ durch } \sigma \text{ faktorisieren.}$$

- *Für ein Unifikationsproblem (Γ, E) bzw. $(\Gamma, \mathcal{A})$ bezeichne $\mu U_E(\Gamma)$ bzw. $\mu U_{\mathcal{A}}(\Gamma)$ (kurz: $\mu U(\Gamma)$) eine* ***minimal vollständige Menge der Unifikatoren*** *von Γ (bzgl. $\lesssim_\Gamma$). σ heißt* ***allgemeinster Unifikator (mgu, most general unifier)****, falls σ kleinstes Element in $U_E(\Gamma)$ bzw. $U_A(\Gamma)$ (bzgl. $\lesssim_\Gamma$) ist.*

Sicherlich interessieren uns bei einem Unifikator nur die Bilder der in Γ vorkommenden Variablen, so daß in obiger Definition die Gleichheit von $\sigma\lambda = \tau$ auf die in Γ vorkommenden Variablen eingeschränkt worden ist. Fordert man die Gleichheit auf ganz X, so ändert sich die Ordnung, so daß sich unter Umständen andere minimal vollständige Mengen und somit ein anderer *Unifikationstyp* (Definition siehe unten) ergeben (vgl. hierzu [Baa91]).

Zur Vereinfachung der Schreibweise gehen wir im folgenden oBdA davon aus, daß X gleich der Menge der in Γ vorkommenden Variablen ist und wir schreiben statt $\lesssim_\Gamma$ kürzer $\lesssim$, sofern Γ aus dem Kontext hervorgeht.

Wir haben in Kapitel 2.1 gesehen, daß minimal vollständige Mengen und kleinste Elemente einer quasigeordneten Menge nicht immer existieren müssen. Dieses gilt auch für die Menge der Unifikatoren[5].

Anhand der Existenz und der Mächtigkeit minimal vollständiger Mengen kann man eine Einteilung von Unifikationsproblemen vornehmen:

Definition 3.4.2 (Unifikationstyp)
Je nach Existenz und Mächtigkeit der minimal vollständigen Menge $\mu U(\Gamma)$ von Unifikatoren für Gleichungssysteme Γ sei der ***Unifikationstyp*** *einer Menge E von Identitäten definiert als*

Typ 1	*(unitär)*	*$\mu U(\Gamma)$ existiert für alle Γ und $\lvert\mu U(\Gamma)\rvert \leq 1$*
Typ ω	*(finitär)*	*$\mu U(\Gamma)$ existiert für alle Γ und $\lvert\mu U(\Gamma)\rvert < \infty$*
Typ ∞	*(infinitär)*	*$\mu U(\Gamma)$ existiert für alle Γ und es gibt ein Γ*
	mit $\lvert\mu U(\Gamma)\rvert = \infty$	
Typ 0	*(null)*	*es gibt ein Γ, so daß $\mu U(\Gamma)$ nicht existiert*

Für jeden der obengenannten Typen existieren Beispiele:

Beispiel 3.4.3 (aus [BaaSi94])

- Die leere Theorie $\emptyset$, d.h. die durch eine leere Menge von Identitäen erzeugte Gleichungstheorie, ist unitär ([Ro65]).
- Die durch die Gleichung $f(x, y) = f(y, x)$ („Kommutativtät") erzeugte Gleichungstheorie C ist finitär (z.B. [Si79]).
- Die durch die Gleichung $f(f(x, y), z) = f(x, f(y, z))$ („Assoziativität") erzeugte Gleichungstheorie A ist infinitär ([Pl72]).

[5] Eine ausführliche Darstellung über notwendige und hinreichende Bedingungen für die Existenz minimal vollständiger Mengen, insbesondere im Hinblick auf Mengen von Unifikatoren findet main in [Baa89a]

- Die durch die Gleichungen $f(f(x,y),z) = f(x,f(y,z))$ („Assoziativität") und $f(x,x) = x$ („Idempotenz") erzeugte Gleichungstheorie AI ist vom Typ 0 ([Baa86]).

3.5 Unifikation aus kategorientheoretischer Sicht

Unifikation kann statt als Suche nach einer Substitution, die Paare von Termen gleich macht, auch auf folgende Weise als die Suche nach einer Substitution, die Substitutionen gleich macht, verstanden werden.

Sei $\Gamma := \{(s_1,t_1),\ldots,(s_k,t_k)\}$ ein Gleichungssystem über $\mathcal{F}(X)$ und $W := \{x_1,\ldots,x_k\}$. Definiere $\eta,\nu : \mathcal{F}(W) \to \mathcal{F}(X)$ durch $\eta : x_i \mapsto s_i$, $\nu : x_i \mapsto t_i$, $i \in \{1,\ldots,k\}$.

Lemma 3.5.1
Mit obiger Bezeichnung gilt:

$$\eta\sigma = \nu\sigma \Leftrightarrow s_i\sigma = t_i\sigma \quad \forall i \in \{1,\ldots,k\}$$

für $\sigma : \mathcal{F}(X) \to \mathcal{F}(Y)$.

Beweis
$\eta\sigma = \nu\sigma \Leftrightarrow x_i\eta\sigma = x_i\nu\sigma \ \forall i \in 1,\ldots,k \Leftrightarrow s_i\sigma = t_i\sigma \ \forall i \in \{1,\ldots,k\}$. □

Wir wollen daher auch (η,ν) als Unifikationsproblem verstehen (vgl. Abbildung 3.5).

$$\begin{tikzcd}
 & & & \mathcal{F}(Z') \\
\mathcal{F}(W) \arrow[r, bend left, "\eta"] \arrow[r, bend right, "\nu"'] & \mathcal{F}(X) \arrow[r, "\sigma"] \arrow[urr, "\tau'"] \arrow[drr, "\tau"'] & \mathcal{F}(Y) \arrow[ur, "\lambda'"'] \arrow[dr, "\lambda"] & \\
 & & & \mathcal{F}(Z)
\end{tikzcd}$$

$\eta\sigma = \nu\sigma$
$\sigma \lesssim \tau, \tau'$

Abbildung 3.1:

Beachte, daß X nach Konvention genau aus den in Γ vorkommenden Variablen besteht.

Diese Sichtweise erlaubt uns, Unifikationsprobleme im Rahmen der Kategorientheorie auszudrücken.

Definition 3.5.2 (kanonische Kategorie)
Sei $\mathcal{E}$ eine Gleichungstheorie bzw. $\mathcal{A}$ eine Σ-Algebra mit zugehörigen freien Algebren $\mathcal{F}(W) = \mathcal{F}_\mathcal{E}(W)$ bzw. $\mathcal{F}(W) = \mathcal{F}_\mathcal{A}(W)$ für alle $W \subseteq V$. Dann wird $\mathfrak{C} = \mathfrak{C}(\mathfrak{O}, \mathfrak{M}, dom, cod, \circ)$, $\mathfrak{C} = \mathfrak{C}_\mathcal{E}$ bzw. $\mathfrak{C} = \mathfrak{C}_\mathcal{A}$ definiert durch

- $\mathfrak{O} = \{\mathcal{F}(W) \ : \ W \subseteq V, |W| < \infty\}$
- $\mathfrak{M} = \{\sigma : \mathcal{F}(W) \to \mathcal{F}(W') \ : \ \sigma \textit{ Hom.}, W, W' \subseteq V \textit{ endlich}\}$
- *dom, cod entsprechend dem Quell- und Zielbereichs der $\sigma \in \mathfrak{M}$*
- *$\circ$ sei die gewöhnliche Komposition von Homomorphismen.*

$\mathfrak{C}$ heißt die zu $\mathcal{E}$ bzw. $\mathcal{A}$ ***kanonische Kategorie****.*

Ein Unifikationsproblem ist also ein Paar von Morphismen η, ν und ein Unifikator ist ein Morphismus σ, so daß $\eta \circ \sigma = \nu \circ \sigma$ gilt.

Für die kanonische Kategorie einer Gleichungstheorie gilt, daß endliche Coprodukte existieren:

Lemma 3.5.3
Sei $\mathfrak{C}_\mathcal{E}$ kanonische Kategorie einer Gleichungstheorie $\mathcal{E}$. Dann existiert zu jeder endlichen Familie $(\mathcal{F}(X_i))_{i \in I}$ von $\mathfrak{C}_\mathcal{E}$-Objekten ein Coprodukt.

Beweis
Beachte, daß möglicherweise $\bigcap X_i \neq \emptyset$. Setze daher $X := \dot{\bigcup} X_i$, $X = \{x_{ij} \ : \ i \in I, j \in \{1, \ldots, |X_i|\}\}$. Für $X_i = \{x_{i_1}, \ldots, x_{i_{|X_i|}}\}$ sei $\iota_i : \mathcal{F}(X_i) \to \mathcal{F}(X)$ definiert durch $x_{i_j} \mapsto x_{ij}$. Dann ist $((\iota_i)_{i \in I}, \mathcal{F}(X))$ ein Coprodukt. Dazu ist zu zeigen:

1. $\mathcal{F}(X)$ ist ein $\mathfrak{C}_\mathcal{E}$-Objekt
2. Die ι_i sind Morphismen
3. Für jedes Tupel $((\varphi_i)_{i \in I}, \mathcal{F}(Y))$ mit $\varphi_i : \mathcal{F}(X_i) \to \mathcal{F}(Y)$ gibt es genau ein $\varphi : \mathcal{F}(X) \to \mathcal{F}(Y)$ mit $\varphi_i = \iota_i \varphi$.

1. und 2. sind offensichtlich erfüllt. Für $\varphi_i : \mathcal{F}(X_i) \to \mathcal{F}(Y)$ definiert durch $x_{i_j} \mapsto t_{i_j}$, $j \in \{1, \ldots, |X_i|\}$, sei $\varphi : \mathcal{F}(X) \to \mathcal{F}(Y)$ definiert durch $x_{ij} \mapsto t_{i_j}$. Da $x_{i_j} \iota \varphi = x_{ij} \varphi = t_{i_j} = x_{i_j} \varphi_i$ für alle $x_{i_j} \in X_i$, gilt $\varphi_i = \iota_i \varphi$ für alle $i \in I$. Für φ' : $\mathcal{F}(X) \to \mathcal{F}(Y)$ mit $x_{ij} \varphi' \neq t_{i_j}$ für ein Paar i, j gilt offensichtlich $x_{i_j} \iota_i \varphi' \neq t_{i_j} = x_{i_j} \varphi_i$, so daß φ eindeutig bestimmt ist. □

Kanonische Kategorien, wo obiges Coprodukt zu einem Biprodukt erweitert werden kann, werden in Kapitel 5 untersucht.

3.6 Äquivalente Algebren

Für gewisse Anwendungen, insbesondere der Unifikation, ist es hilfreich, *nicht* zwischen zwei verschiedenen Algebren zu unterscheiden, falls sie *ineinander überführt* werden können:[6]

Beispiel 3.6.1
Seien $\Sigma = \{\vee, ^-\}$, $\Sigma' = \{\wedge, ^-\}$, $\mathcal{A} = (\{0,1\}, \Sigma^{\mathcal{A}})$, $\mathcal{B} = (\{0,1\}, \Sigma'^{\mathcal{B}})$, wobei $^{-\mathcal{A}} = {}^{-\mathcal{B}}$ dem logischen *nicht*, $\vee^{\mathcal{A}}$ dem logischen *oder* und $\wedge^{\mathcal{B}}$ dem logischen *und* entspreche. Dann sind $\mathcal{A}$ und $\mathcal{B}$ aufgrund der unterschiedlichen Signaturen zwar nicht isomorph, doch es gilt $(x \vee y)^{\mathcal{A}} = (\overline{\overline{x} \wedge \overline{y}})^{\mathcal{B}}$. Versteht man die Gleichung als Abbildung, das heißt, Teilterme der Form $(x \vee y)$ werden durch $(\overline{\overline{x} \wedge \overline{y}})^{\mathcal{B}}$ ersetzt, so kann jeder Term t der Signatur Σ in einen Term t' der Signatur Σ' mit $t^{\mathcal{A}} = t'^{\mathcal{B}}$ umgewandelt werden. Hat man also einen Unifikator σ für eine Σ-Gleichung (s,t) gegeben mit $\mathcal{A} \models s\sigma = t\sigma$, d.h. $(s\sigma)^{\mathcal{A}} = (t\sigma)^{\mathcal{A}}$, so wird man einen Unifikator σ' für (s',t') finden, falls man in (s,t) und dem Bild von σ jedes Auftreten von $\vee$ gemäß der obigen Gleichung ersetzt. Aufgrund der Gleichung $(x \wedge y)^{\mathcal{A}} = (\overline{\overline{x} \vee \overline{y}})^{\mathcal{B}}$ gilt obige Argumentation umgekehrt auch für Σ' und Σ, so daß wir $\mathcal{A}$ und $\mathcal{B}$ bzgl. der Unifikationseigenschaften identifizieren wollen.[7]

Wir definieren daher (vgl. [BaNu90]):

Definition 3.6.2 (Signaturtransformation, äquivalente Algebren)

1. *Seien Σ, Σ' zwei Signaturen. Eine Abbildung $\Delta : \mathcal{T}(\Sigma, X) \to \mathcal{T}(\Sigma', X)$ heißt* ***Signaturtransformation*** *von Σ zu Σ', falls für alle $x \in X$*

   $$x\Delta = x$$

   und für alle $f \in \Sigma^{(k)}$ und alle $x_1, \ldots, x_k \in X$, paarweise verschieden

   $$(ft_1 \ldots t_k)\Delta = (fx_1 \ldots x_k)\Delta \circ \{x_1 \mapsto t_1\Delta, \ldots, x_k \mapsto t_k\Delta\}$$

   mit $Var(fx_1 \ldots x_k\Delta) = \{x_1, \ldots, x_k\}$ gilt.

2. *Eine Σ-Algebra $\mathcal{A}$ heißt* ***äquivalent*** *zu einer Σ'-Algebra $\mathcal{B}$ ($\mathcal{A} \sim \mathcal{B}$), falls eine Signaturtransformation Δ von Σ zu Σ' und eine Signaturtransformation Δ' von Σ' zu Σ existieren mit*

   (A1) $s^{\mathcal{A}} = t^{\mathcal{A}} \Rightarrow (s\Delta)^{\mathcal{B}} = (t\Delta)^{\mathcal{B}}$
   (A2) $s'^{\mathcal{B}} = t'^{\mathcal{B}} \Rightarrow (s'\Delta')^{\mathcal{A}} = (t'\Delta')^{\mathcal{A}}$

[6] Bei isomorphen Algebren ist einem diese Vorgehensweise sehr vertraut, da man in vielen Fällen isomorphe Algebren identifiziert. Wie das Beispiel zeigt, wollen wir aber unter gewissen Voraussetzungen auch nichtisomorphe Algebren identifizieren.

[7] Im folgenden wird genauer erläutert, wie sich allgemeinste Unifikatoren usw. bei der Übersetzung verhalten.

(A3) $(s\Delta\Delta')^{\mathcal{A}} = s^{\mathcal{A}}$, $(s'\Delta'\Delta)^{\mathcal{B}} = s'^{\mathcal{B}}$

für alle $s, t \in T(\Sigma, X)$, $s', t' \in T(\Sigma', X)$.

3. *Zwei Gleichungstheorien* $\mathcal{E}, \mathcal{E}'$ *über der Signatur* Σ *bzw.* Σ' *heißen äquivalent* ($\mathcal{E} \sim \mathcal{E}'$), *falls eine Signaturtransformation* Δ *von* Σ *zu* Σ' *und eine Signaturtransformation* Δ' *von* Σ' *zu* Σ *existieren mit*

   (A1) $s =_{\mathcal{E}} t \Rightarrow s\Delta =_{\mathcal{E}'} t\Delta$

   (A2) $s' =_{\mathcal{E}'} t' \Rightarrow s'\Delta' =_{\mathcal{E}} t'\Delta'$

   (A3) $s\Delta\Delta' =_{\mathcal{E}} s$, $s'\Delta'\Delta =_{\mathcal{E}'} s'$

   für alle $s, t \in T(\Sigma, X)$, $s', t' \in T(\Sigma', X)$.

4. *Seien* $\mathcal{A}$ *und* $\mathcal{B}$ ($\mathcal{E}$ *und* $\mathcal{E}'$) *äquivalente Algebren (Theorien) mit Signaturtransformationen* Δ *und* Δ'. *Zwei Unifikationsprobleme* $(\Gamma, \mathcal{A})$ *und* $(\Gamma, \mathcal{B})$ ($(\Gamma, \mathcal{E})$ *und* $(\Gamma, \mathcal{E}')$) *heißen* ***äquivalent***, *falls* $\Gamma\Delta = \Gamma'$ *und* $\Gamma'\Delta' = \Gamma$, *wobei* $\hat{\Gamma}\hat{\Delta} = \{(s\hat{\Delta}, t\hat{\Delta}) \ : \ (s,t) \in \hat{\Gamma}\}$ *für* $(\hat{\Gamma}, \hat{\Delta}) = (\Gamma, \Delta)$ *bzw.* $(\hat{\Gamma}, \hat{\Delta}) = (\Gamma', \Delta')$.

Bei einer Signaturtransformation wird also jedem Funktionssymbol, genauer jedem **flachen Term**[8] der Signatur Σ mit k Variablen ein Term der Signatur Σ' mit k Variablen zugeordnet und die Zuordnung auf alle Σ-Terme kanonisch erweitert.

Zwei Algebren $\mathcal{A}$ und $\mathcal{B}$ werden dann äquivalent genannt, falls es zwischen ihnen jeweils eine Signaturtransformation gibt, so daß für in $\mathcal{A}$ gleiche Terme s und t auch die Bilder von s und t unter der Signaturtransformation in $\mathcal{B}$ gleich sind und umgekehrt.

Daß man bzgl. Unifikation äquivalente Algebren oder Theorien identifizieren kann, zeigt der letzte Satz des Kapitels, für den wir einige Vorarbeit leisten.

Die Überlegungen in Kapitel 2 ergeben direkt:

Lemma 3.6.3
Seien $\mathcal{E}$, $\mathcal{E}'$ *zwei Gleichungstheorien und* $\mathcal{F}_{\mathcal{E}}(X)$ *bzw.* $\mathcal{F}_{\mathcal{E}'}(X)$ *die zugehörigen freien Algebren. Dann gilt:*

$$\mathcal{E} \sim \mathcal{E}' \ \Leftrightarrow \ \mathcal{F}_{\mathcal{E}}(X) \sim \mathcal{F}_{\mathcal{E}'}(X)$$

Wir werden daher im folgenden nur Eigenschaften äquvialenter Algebren untersuchen.

Folgendes Lemma zeigt, daß der Äquivalenzbegriff für Algebren verträglich mit dem der zugehörigen freien Algebra ist:

[8] d.h. jeder Teilterm ist eine Variable

Lemma 3.6.4
Sei $\mathcal{A}$ eine Σ-Algebra, $\mathcal{B}$ eine Σ'-Algebra. Dann gilt:

$$\mathcal{A} \sim \mathcal{B} \;\Leftrightarrow\; \mathcal{F}_\mathcal{A} \sim \mathcal{F}_\mathcal{B}$$

Beweis

$$\begin{array}{lcl}
\mathcal{A} \sim \mathcal{B} & \Leftrightarrow & \exists \Delta : \mathcal{T}(\Sigma, X) \to \mathcal{T}(\Sigma', X), \Delta' : \mathcal{T}(\Sigma', X) \to \mathcal{T}(\Sigma, X) \text{ mit} \\
& & s^\mathcal{A} = t^\mathcal{A} \;\Rightarrow\; (s\Delta)^\mathcal{B} = (t\Delta)^\mathcal{B} \\
& & s'^\mathcal{B} = t'^\mathcal{B} \;\Rightarrow\; (s'\Delta')^\mathcal{A} = (t'\Delta')^\mathcal{A} \\
& & (s\Delta\Delta')^\mathcal{A} = s^\mathcal{A}, (s'\Delta'\Delta)^\mathcal{B} = s'^\mathcal{B} \\
& \overset{\text{Satz 3.3.1}}{\Leftrightarrow} & \exists \Delta : \mathcal{T}(\Sigma, X) \to \mathcal{T}(\Sigma', X), \Delta' : \mathcal{T}(\Sigma', X) \to \mathcal{T}(\Sigma, X) \text{ mit} \\
& & s^{\mathcal{F}_\mathcal{A}} = t^{\mathcal{F}_\mathcal{A}} \;\Rightarrow\; (s\Delta)^{\mathcal{F}_\mathcal{B}} = (t\Delta)^{\mathcal{F}_\mathcal{B}} \\
& & s'^{\mathcal{F}_\mathcal{B}} = t'^{\mathcal{F}_\mathcal{B}} \;\Rightarrow\; (s'\Delta')^{\mathcal{F}_\mathcal{A}} = (t'\Delta')^{\mathcal{F}_\mathcal{A}} \\
& & (s\Delta\Delta')^{\mathcal{F}_\mathcal{A}} = s^{\mathcal{F}_\mathcal{A}}, (s'\Delta'\Delta)^{\mathcal{F}_\mathcal{B}} = s'^{\mathcal{F}_\mathcal{B}} \\
& \Leftrightarrow & \mathcal{F}_\mathcal{A} \sim \mathcal{F}_\mathcal{B}
\end{array}$$

□

Insbesondere sind zwei Algebren äquivalent, falls sie die gleichen Termfunktionen besitzen:

Lemma 3.6.5
Sei $\mathcal{A} = (A, \Sigma^A)$ eine Σ-Algebra, $\mathcal{B} = (A, \Sigma'^A)$ eine Σ'-Algebra. Aus $T(\mathcal{A}) = T(\mathcal{B})$ folgt $\mathcal{A} \sim \mathcal{B}$.

Beweis
Sei $T(\mathcal{A}) = T(\mathcal{B})$. Definiere Signaturtransformationen $\Delta : \mathcal{T}(\Sigma, X) \to \mathcal{T}(\Sigma', X)$ und $\Delta' : \mathcal{T}(\Sigma', X) \to \mathcal{T}(\Sigma, X)$ folgendermaßen: Sei $f \in \Sigma^{(k)}$. Zu $f^\mathcal{A} : A^k \to A$ gibt es dann ein $t_f \in \mathcal{T}(\Sigma', X)$ mit $t_f^\mathcal{B} : A^k \to A$, $t_f^\mathcal{B} = f^\mathcal{A}$ und oBdA $Var(t_f) = \{x_1, \ldots, x_k\}$. Setze $fx_1 \ldots x_k\Delta = t_f$, $x\Delta = x$. Analog wird Δ' definiert. Beh.: Δ und Δ' liefern die Äquivalenz von $\mathcal{A}$ und $\mathcal{B}$, das heißt, für alle $s, t \in T(\Sigma, X)$, s', t' gilt:

(A1) $s^\mathcal{A} = t^\mathcal{A} \Rightarrow (s\Delta)^\mathcal{B} = (t\Delta)^\mathcal{B}$

(A2) $s'^\mathcal{B} = t'^\mathcal{B} \Rightarrow (s'\Delta')^\mathcal{A} = (t'\Delta')^\mathcal{A}$

(A3) $(s\Delta\Delta')^\mathcal{A} = s^\mathcal{A}$, $(s'\Delta'\Delta)^\mathcal{B} = s'^\mathcal{B}$

Zunächst beweisen wir per Induktion über den Termaufbau, daß für alle $s \in \mathcal{T}(\Sigma, X)$ und $s' \in \mathcal{T}(\Sigma', X)$ gilt:

$$s^\mathcal{A} = (s\Delta)^\mathcal{B}, s'^\mathcal{B} = (s'\Delta')^\mathcal{A}$$

Der Induktionsanfang ist klar nach Definition von Δ und Δ'.
Sei $s = fs_1 \ldots s_k$.

$$(s\Delta)^\mathcal{B} \;=\; (fs_1 \ldots s_k\Delta)^\mathcal{B}$$

$$\begin{aligned}
&= ((fx_1 \dots x_k)\Delta[x_1/s_1\Delta, \dots, x_k/s_k\Delta])^{\mathcal{B}} \\
&= (t_f[x_1/s_1\Delta, \dots, x_k/s_k\Delta])^{\mathcal{B}} \\
&= ((s_1\Delta)^{\mathcal{B}}, \dots, (s_k\Delta)^{\mathcal{B}})t_f^{\mathcal{B}} \\
&= (s_1^{\mathcal{A}}, \dots, s_k^{\mathcal{A}})t_f^{\mathcal{B}} \\
&= (s_1^{\mathcal{A}}, \dots, s_k^{\mathcal{A}})f^{\mathcal{A}} \\
&= (fs_1 \dots s_k)^{\mathcal{A}}
\end{aligned}$$

Analog zeigt man $s'^{\mathcal{B}} = (s'\Delta')^{\mathcal{A}}$.
Dann gilt:

$$s^{\mathcal{A}} = t^{\mathcal{A}} \Leftrightarrow (s\Delta)^{\mathcal{B}} = (t\Delta)^{\mathcal{B}}$$

$$s'^{\mathcal{B}} = t'^{\mathcal{B}} \Leftrightarrow (s'\Delta')^{\mathcal{A}} = (t'\Delta')^{\mathcal{A}}$$

$$(s\Delta\Delta')^{\mathcal{A}} = ((s\Delta)\Delta')^{\mathcal{A}} = (s\Delta)^{\mathcal{B}} = s^{\mathcal{A}},$$

$$(s'\Delta'\Delta)^{\mathcal{B}} = ((s'\Delta')\Delta)^{\mathcal{B}} = (s'\Delta')^{\mathcal{A}} = s'^{\mathcal{B}}$$

Somit sind insbesondere (A1), (A2) und (A3) erfüllt. □

Daß äquivalente Algebren nicht die gleichen Termfunktionen besitzen müssen, zeigt folgendes Beispiel:

Beispiel 3.6.6
Seien $A = \{0, 1\}$, $\Sigma = \{\underline{0}\}$ und $\Sigma' = \{\underline{1}\}$. Die Signaturtransformationen $\Delta : \mathcal{T}(\Sigma, X) \to \mathcal{T}(\Sigma', X)$ und $\Delta' : \mathcal{T}(\Sigma', X) \to \mathcal{T}(\Sigma, X)$ definiert durch

$$\begin{aligned}
\underline{0}\Delta &= \underline{1} \\
\underline{1}\Delta' &= \underline{0}
\end{aligned}$$

Dann sind die Algebren $\mathcal{A} = (A, \Sigma^{A})$ und $\mathcal{B} = (A, \Sigma'^{\mathcal{A}})$ mit der natürlichen Interpretation von Σ bzw. Σ' über A äquivalent.[9] Dennoch besitzt $\mathcal{A}$ nur die Termfunktionen, die konstant das Element 0 liefern, während $\mathcal{B}$ nur Termfunktionen besitzt, die konstant 1 liefern.

Der folgende Satz zeigt, daß der etwas „technische" Äquivalenzbegriff im Rahmen der Kategorientheorie „recht einfach" beschrieben werden kann.

Satz 3.6.7
Seien $\mathcal{F}(V)$ und $\mathcal{F}'(V)$ zwei freie Algebren über der abzählbar unendlichen Variablenmenge V mit zugehörigen kanonischen Kategorien $\mathfrak{C}_{\mathcal{F}}$ bzw. $\mathfrak{C}_{\mathcal{F}'}$. Dann gilt:

$$\mathcal{F}(V) \sim \mathcal{F}'(V) \Rightarrow \mathfrak{C}_{\mathcal{F}} \cong \mathfrak{C}_{\mathcal{F}'}$$

[9] (A1) und (A2) sind trivialerweise erfüllt, da es keine verschiedenen Terme s und t bzw. s' und t' in $\mathcal{T}(\Sigma, X)$ bzw. in $\mathcal{T}(\Sigma', X)$ gibt. Wegen $\underline{0}\Delta\Delta' = \underline{0}$ und $\underline{1}\Delta'\Delta = \underline{1}$ gilt insbesondere $(\underline{0}\Delta\Delta')^{A} = \underline{0}^{A}$ und $(\underline{1}\Delta'\Delta)^{B} = \underline{1}^{B}$ und somit (A3).

Beweis
„$\Rightarrow$“: Wegen $\mathcal{F}(V) \sim \mathcal{F}'(V)$ existieren Signaturtransformationen Δ, Δ' mit den Eigenschaften (A1), (A2), (A3). Die Abbildung $I : Mor\,\mathfrak{C}_{\mathcal{F}} \rightarrow Mor\,\mathfrak{C}_{\mathcal{F}'}$ wird wie folgt definiert: Sei $\sigma \in Mor\,\mathfrak{C}_{\mathcal{F}}$ mit $\sigma : \mathcal{F}(X) \rightarrow \mathcal{F}(Y)$ gegeben durch $x_1 \mapsto t_1, \ldots, x_n \mapsto t_n$. Definiere $\sigma' : \mathcal{F}'(X) \rightarrow \mathcal{F}'(Y)$ durch $x_1 \mapsto t_1\Delta, \ldots, x_n \mapsto t_n\Delta$. Da $Var(t_i\Delta) \subseteq Y$, ist σ' wohldefiniert.

Analog ordnen wir jedem $\sigma' : \mathcal{F}'(X) \rightarrow \mathcal{F}'(Y)$ einen Homomorphismus $\sigma'' : \mathcal{F}'(X) \rightarrow \mathcal{F}'(Y)$ zu und nennen diese Abbildung $I^{-1} : Mor\,\mathfrak{C}_{\mathcal{F}'} \rightarrow Mor\,\mathfrak{C}_{\mathcal{F}}$.

Per Induktion zeigen wir zunächst, daß für $s \in \mathcal{F}(X)$ gilt:

$$(s\sigma)\Delta = (s\Delta)\sigma'$$

Induktionsanfang:
Sei $x_i \in X$: $x_i\sigma\Delta = t_i\Delta = x_i\sigma' = x_i\Delta\sigma'$
Sei $f \in \Sigma^{(k)}$:

$$\begin{aligned}
(fx_1 \ldots x_k)\sigma\Delta &= (ft_1 \ldots t_k)\Delta \\
&= (fx_1 \ldots x_k\Delta)[x_1/t_1\Delta, \ldots, x_k/t_k\Delta] \\
&= fx_1 \ldots x_k\Delta\sigma'
\end{aligned}$$

Induktionsschritt:
Sei $s = fs_1 \ldots s_k \in \mathcal{F}(X)$

$$\begin{aligned}
(fs_1 \ldots s_k\sigma)\Delta &= (fs_1\sigma \ldots s_k\sigma)\Delta \\
&= (fx_1 \ldots x_k)\Delta[x_1/s_1\sigma\Delta, \ldots, x_k/s_k\sigma\Delta] \\
&\overset{\text{IV}}{=} (fx_1 \ldots x_k)\Delta[x_1/s_1\Delta\sigma', \ldots, x_k/s_k\Delta\sigma'] \\
&= (fx_1 \ldots x_k)\Delta[x_1/s_1\Delta, \ldots, x_k/s_k\Delta]\sigma' \\
&= (fs_1 \ldots s_k)\Delta\sigma'
\end{aligned}$$

Analog zu obiger Argumentation erhalten wir auch für $s' \in \mathcal{F}'(X)$

$$(s'\sigma')\Delta' = (s'\Delta')\sigma''$$

Nun zeigen wir, daß $\sigma II^{-1} = \sigma$ und $\sigma' I^{-1} I = \sigma$ für alle $\sigma \in Hom(\mathcal{F}(X), \mathcal{F}(Y))$ und $\sigma' \in Hom(\mathcal{F}'(X), \mathcal{F}'(Y))$.

Sei $s \in \mathcal{F}(X)$ beliebig. Nach (A3) gilt $(s\sigma)\Delta\Delta' = (s\sigma)$.

$$\begin{aligned}
s\sigma\Delta\Delta' = s\sigma \quad &\Rightarrow \quad s\Delta\sigma'\Delta' = s\sigma \\
&\Rightarrow \quad s\Delta\Delta'\sigma'' = s\sigma \\
&\overset{(A3)}{\Rightarrow} \quad s\sigma'' = s\sigma
\end{aligned}$$

Da s beliebig ist, gilt $\sigma'' = \sigma$. Analog zeigt man $\sigma' I^{-1} I = \sigma'$. Somit ist I eine Bijektion von $Hom(\mathcal{F}(X), \mathcal{F}(Y))$ auf $Hom(\mathcal{F}'(X), \mathcal{F}'(Y))$ für alle $X, Y \subseteq V$, $|X|, |Y| < \infty$.

Da die eindeutige Identität $e_{\mathcal{F}(Y)}$ von $\mathcal{F}(Y)$ (bzw. $e_{\mathcal{F}'(Y)}$ von $\mathcal{F}'(Y)$) definiert ist durch $y \mapsto y$ für alle $y \in Y$ (bzw. $y \mapsto y$ für alle $y \in Y$) und $y\Delta = y$ (bzw. $y\Delta' = y$), gilt:

$$e_{\mathcal{F}(Y)} I = e_{\mathcal{F}'(Y)} \quad \text{bzw. } e_{\mathcal{F}'(Y)} I^{-1} = e_{\mathcal{F}(Y)}$$

Somit gilt:

1. $\mathfrak{C}_{\mathcal{F}}$-Identitäten werden unter I abgebildet auf $\mathfrak{C}_{\mathcal{F}'}$-Identitäten und umgekehrt.
2. Die zu I, I^{-1} gehörigen Objektfunktionen sind bijektiv auf $Ob\,\mathfrak{C}_{\mathcal{F}}$ bzw. $Ob\,\mathfrak{C}_{\mathcal{F}'}$.

Falls I Funktor ist, folgt mit Lemma 2.4.7, daß I ein Isomorphismus von $\mathfrak{C}_{\mathcal{F}}$ auf $\mathfrak{C}_{\mathcal{F}'}$ ist.

Zeigen wir daher noch, daß I ein Funktor ist. Da wir bereits gesehen haben, daß $\mathfrak{C}_{\mathcal{F}}$-Identitäten unter I auf $\mathfrak{C}_{\mathcal{F}'}$-Identitäten abgebildet werden, ist nur noch zu zeigen, daß

$$(\sigma_1 \circ \sigma_2) I = (\sigma_1 I) \circ (\sigma_2 I)$$

für alle $\sigma_1, \sigma_2 \in Mor\,\mathfrak{C}_{\mathcal{F}}$.

Seien $\sigma_1 : \mathcal{F}(X) \to \mathcal{F}(Y)$ und $\sigma_2 : \mathcal{F}(Y) \to \mathcal{F}(Z)$ gegeben. Für $s \in \mathcal{F}(X)$ gilt

$$\begin{aligned}
(s\Delta)((\sigma_1\sigma_2)I) &= (s\Delta)(\sigma_1\sigma_2)' \\
&= (s(\sigma_1\sigma_2))\Delta \\
&= ((s\sigma_1)\sigma_2)\Delta \\
&= ((s\sigma_1)\Delta)\sigma_2' \\
&= ((s\Delta)\sigma_1')\sigma_2' \\
&= ((s\Delta)(\sigma_1 I))(\sigma_2 I)
\end{aligned}$$

Insbesondere gilt die Gleichung für alle $s \in X$ (also $s = s\Delta \in X$), so daß

$$(\sigma_1 \circ \sigma_2) I = (\sigma_1 I) \circ (\sigma_2 I)$$

gilt.

Damit ist die Behauptung gezeigt. □

Aus dem Beweis des letzten Satzes ergibt sich die wichtige Folgerung, daß aus der Sicht der Unifikation äquivalente Algebren oder Theorien gemeinsam behandelt werden können:

Satz 3.6.8
Seien V eine abzählbar unendliche Variablenmenge, $\mathcal{F}(V)$ und $\mathcal{F}'(V)$ äquivalente Algebren der Signaturen Σ bzw. Σ', $(\Gamma, \mathcal{F}(V))$ und $(\Gamma', \mathcal{F}'(V))$ äquivalente Unifikationsprobleme über $\mathcal{F}(V)$ bzw. $\mathcal{F}'(V)$. Dann gilt: $\mathcal{F}(V)$ und $\mathcal{F}'(V)$ sind von gleichem Unifikationstyp.

Beweis
Wegen $\mathcal{F}(V) \sim \mathcal{F}'(V)$ existieren Signaturtransformationen Δ, Δ' mit den Eigenschaften (A1), (A2), (A3) über V.

Seien $\mathfrak{C}_{\mathcal{F}}$ und $\mathfrak{C}_{\mathcal{F}'}$ die zu $\mathcal{F}(V)$ bzw. $\mathcal{F}'(V)$ kanonischen Kategorien.

Analog wie im Beweis des letzten Satzes definieren wir eine Abbildung $I : Mor\,\mathfrak{C}_{\mathcal{F}} \rightarrow Mor\,\mathfrak{C}_{\mathcal{F}'}$ wie folgt: Sei $\sigma \in Mor\,\mathfrak{C}_{\mathcal{F}}$ mit $\sigma : \mathcal{F}(X) \rightarrow \mathcal{F}(Y)$ gegeben durch $x_1 \mapsto t_1, \ldots, x_n \mapsto t_n$. Definiere $\sigma' : \mathcal{F}'(X) \rightarrow \mathcal{F}'(Y)$ durch $x_1 \mapsto t_1\Delta$, …, $x_n \mapsto t_n\Delta$. Wegen $Var(t_i\Delta) \subseteq Y$ ist σ' wohldefiniert.

Analog ordnen wir jedem $\sigma' : \mathcal{F}'(X) \rightarrow \mathcal{F}'(Y)$ einen Homomorphismus $\sigma'' : \mathcal{F}'(X) \rightarrow \mathcal{F}'(Y)$ zu und nennen diese Abbildung $I^{-1} : Mor\,\mathfrak{C}_{\mathcal{F}'} \rightarrow Mor\,\mathfrak{C}_{\mathcal{F}}$.

Per Induktion zeigt man wie im letzten Beweis, daß für $s \in \mathcal{F}(X)$ und $s' \in \mathcal{F}'(X)$

$$\begin{aligned} (s\sigma)\Delta &= (s\Delta)\sigma' \\ (s'\sigma')\Delta' &= (s'\Delta')\sigma'' \end{aligned}$$

gilt und daß I ein Funktor ist.

Für $(s,t) \in \Gamma$ gilt somit $(s\sigma)^{\mathcal{F}(Y)} = (t\sigma)^{\mathcal{F}(Y)} \overset{(A1)}{\Rightarrow} (s\sigma\Delta)^{\mathcal{F}'(Y)} = (t\sigma\Delta)^{\mathcal{F}'(Y)} \Leftrightarrow (s\Delta\sigma')^{\mathcal{F}'(Y)} = (t\Delta\sigma')^{\mathcal{F}'(Y)} \Leftrightarrow (s'\sigma')^{\mathcal{F}'(Y)} = (t'\sigma')^{\mathcal{F}'(Y)}$ für die (s,t) entsprechende Gleichung $(s', t') \in \Gamma'$.

Das heißt, Unifikatoren von Γ werden unter I auf Unifikatoren von Γ' abgebildet und mit I^{-1} folgt auch die Umkehrung.

Da I eine Bijektion von den Morphismen von $\mathfrak{C}_{\mathcal{F}}$ auf die Morphismen von $\mathfrak{C}_{\mathcal{F}'}$ ist, gilt somit, daß $I|_{U_{\mathcal{F}(X)}(\Gamma)}$ eine Bijektion der Unifikatoren von Γ auf die Unifikatoren von Γ' ist.

Damit $\mathcal{F}(X)$ und $\mathcal{F}'(X)$ den gleichen Unifikationstyp haben, ist noch zu zeigen, daß die Zuordnung verträglich mit der Ordnung $\lesssim_\Gamma$ und $\lesssim'_\Gamma$ ist.

Seien $\sigma : \mathcal{F}(X) \rightarrow \mathcal{F}(Y)$ und $\tau : \mathcal{F}(X) \rightarrow \mathcal{F}(Z)$ mit $\sigma \lesssim \tau$ gegeben.

$$\begin{aligned} \sigma \lesssim \tau \quad &\Leftrightarrow \quad \exists\, \lambda : \mathcal{F}(Y) \rightarrow \mathcal{F}(Z) \text{ mit } \sigma\lambda = \tau \\ &\Leftrightarrow \quad \exists\, \lambda : \mathcal{F}(Y) \rightarrow \mathcal{F}(Z) \text{ mit } (\sigma\lambda)I = \tau I \\ &\Leftrightarrow \quad \exists\, \lambda : \mathcal{F}(Y) \rightarrow \mathcal{F}(Z) \text{ mit } (\sigma I)(\lambda I) = \tau I \\ &\Leftrightarrow \quad \sigma I \lesssim \tau I \end{aligned}$$

Somit ist die Behauptung gezeigt. □

Kapitel 4

Eine Anwendung: Lösbarkeit von Gleichungen

In diesem Kapitel werden wir mit Hilfe der Unifikation untersuchen, ob eine Gleichung *lösbar* ist und wie man *Lösungen beschreiben* kann. Dabei wird deutlich, daß der Begriff des $\mathcal{A}$-Unifikators sich nur bedingt für diese Aufgabe verwenden läßt.

4.1 Lösbarkeit

Definition 4.1.1 (Lösbarkeit)
Seien $s = t$ eine Gleichung über $\mathcal{T}(\Sigma, X)$, E eine Menge von Identitäten und $\mathcal{A}$ eine Σ-Algebra. $s = t$ heißt

1. ***lösbar**, falls für alle Σ-Algebren $\mathcal{B}$ gilt: $\mathcal{B} \models \exists X \;\; s = t$*

2. ***lösbar in E**, falls für alle E-Algebren $\mathcal{B}$ gilt: $\mathcal{B} \models \exists X \;\; s = t$*

3. ***lösbar in $\mathcal{A}$**, falls gilt: $\mathcal{A} \models \exists X \;\; s = t$*

Satz 4.1.2 (Lösbarkeit)
Seien $s = t$ eine Gleichung über $\mathcal{T}(\Sigma, X)$, E eine Menge von Identitäten und $\mathcal{A}$ eine Σ-Algebra. $s = t$ ist

1. *genau dann lösbar, wenn es einen syntaktischen Unifikator zu $s = t$ gibt.*

2. *genau dann lösbar in E, wenn es einen E-Unifikator zu $s = t$ gibt.*

3. *lösbar in $\mathcal{A}$, falls es einen $\mathcal{A}$-Unifikator zu $s = t$ gibt.*

Beweis

zu 1.) „$\Rightarrow$“: $s = t$ lösbar $\Leftrightarrow$ für alle Σ-Algebren $\mathcal{A}$ gilt $\mathcal{A} \models \exists X\ s = t$.
$\Rightarrow$ $\mathcal{T}(\Sigma, Y) \models \exists X\ s = t$
$\Rightarrow$ $\exists$ Belegung $\varphi : X \rightarrow \mathcal{T}(\Sigma, Y)$ mit $(\mathcal{T}(\Sigma, Y), \varphi) \models s = t$
$\Rightarrow$ für $\hat{\varphi} : \mathcal{T}(\Sigma, X) \rightarrow \mathcal{T}(\Sigma, Y)$ als kanonische Fortsetzung von φ gilt: $s\hat{\varphi} = t\hat{\varphi}$
$\Rightarrow$ $\hat{\varphi}$ ist Unifikator

„$\Leftarrow$“: Sei andererseits $\hat{\varphi} : \mathcal{T}(\Sigma, X) \rightarrow \mathcal{T}(\Sigma, Y)$ Unifikator. Dann gilt $s\hat{\varphi} = t\hat{\varphi}$ in $\mathcal{T}(\Sigma, X)$ und damit auch in allen Σ-Algebren $\mathcal{A}$, da $\mathcal{T}(\Sigma, X)$ frei für die Klasse aller Σ-Algebren ist. Sei $\alpha : Y \rightarrow A$ Belegung der in $s\hat{\varphi}$ freien Variablen, wobei A das Universum einer Σ-Algebra $\mathcal{A}$ bezeichne. Dann ist $\varphi\hat{\alpha} : X \rightarrow A$ eine erfüllende Belegung der Variablen aus s bzw. t, wobei $\varphi = \hat{\varphi}|_X$ und $\hat{\alpha}$ die kanonische Fortsetzung von α auf $\mathcal{T}(\Sigma, Y)$ bezeichne.

zu 2.) anolog zu 1.

zu 3.) Sei $\hat{\varphi} : \mathcal{F}_{\mathcal{A}}(X) \rightarrow \mathcal{F}_{\mathcal{A}}(Y)$ $\mathcal{A}$-Unifikator. Dann gilt $\mathcal{A} \models s\hat{\varphi} = t\hat{\varphi}$. Sei $\mathcal{A} = (A, \Sigma^A)$, $\alpha : Y \rightarrow A$ beliebige Abbildung, $\varphi = \hat{\varphi}|_X$. Dann ist $\varphi\hat{\alpha} : X \rightarrow A$ mit $s\varphi\hat{\alpha} = t\varphi\hat{\alpha}$ (in A), also erfüllende Belegung. Hierbei bezeichne $\hat{\alpha}$ die kanonische Fortsetzung von α auf $\mathcal{T}(\Sigma, Y)$. Beachte, daß $\hat{\varphi} : \mathcal{F}_{\mathcal{A}}(X) \rightarrow \mathcal{F}_{\mathcal{A}}(Y)$ als Homomorphismus $\hat{\varphi}' : \mathcal{T}(\Sigma, X) \rightarrow \mathcal{T}(\Sigma, Y)$ aufgefaßt werden kann.

$\square$

Man beachte, daß aus der Lösbarkeit einer Gleichung in einer Algebra $\mathcal{A}$ nicht die Existenz eines $\mathcal{A}$-Unifikators folgt. Der Grund hierfür ist, daß nicht in Analogie zu den Fällen 1 und 2 aus der Lösbarkeit in $\mathcal{A}$ auch die Lösbarkeit in $\mathcal{F}_{\mathcal{A}}(X)$ folgt.

Beispiel 4.1.3
Sei die Signatur $\Sigma = \{+, \underline{0}, \underline{2}, \underline{3}\}$, $\mathcal{A} = (\mathbb{N}, \Sigma^{\mathbb{N}})$, wobei $+^{\mathbb{N}}$ die Addition auf den natürlichen Zahlen, $\underline{0}^{\mathbb{N}}$, $\underline{2}^{\mathbb{N}}$, $\underline{3}^{\mathbb{N}}$ die entsprechenden natürlichen Zahlen bedeuten möge. Betrachtet sei die Gleichung $x + \underline{2} = \underline{3}$. Es ist offensichtlich, daß $\alpha : \{x\} \rightarrow \mathbb{N}$, $x \mapsto 1$ eine erfüllende Belegung ist, die Gleichung also insbesondere lösbar ist. Dennoch existiert kein $\mathcal{A}$-Unifikator. Denn angenommen, $\sigma : \mathcal{F}_{\mathbb{N}}(\{x\}) \rightarrow \mathcal{F}_{\mathbb{N}}(\{x\})$ definiert durch $x \mapsto t$ sei ein Unifikator, so ist

$$(x + \underline{2})\sigma =_{\mathcal{F}_{\mathbb{N}}(\{x\})} \underline{3}\sigma \Leftrightarrow x\sigma + \underline{2} =_{\mathcal{F}_{\mathbb{N}}(\{x\})} \underline{3} \Leftrightarrow t + \underline{2} =_{\mathcal{F}_{\mathbb{N}}(\{x\})} \underline{3}.$$

Aufgrund von Satz 3.3.1 gilt daher $\mathcal{A} \models t + \underline{2} = \underline{3}$ und somit $t^{\mathcal{A}} = 1$. Andererseits kann nur $t^{\mathcal{A}} = 0$ ($t = \underline{0} + \cdots + \underline{0}$), $t^{\mathcal{A}} \geq 2$ ($t = \cdots + \underline{2} + \cdots$, $t = \cdots + \underline{3} + \cdots$) oder $t^{\mathcal{A}}$ nicht konstant aufgrund freier Variablen in t sein. Widerspruch!

Im obigen Beispiel existiert für die betrachtete Gleichung kein Unifikator, da 1 nicht durch einen Term *erreichbar* ist:

Definition 4.1.4 (Erreichbarkeit)
Sei $\mathcal{A} = (A, \Sigma)$ eine Algebra. Ein Element $a \in A$ heißt **erreichbar**, *falls es einen Term $t \in \mathcal{T}(\Sigma, V)$ mit $t^{\mathcal{A}} = a$ gibt.*

Man beachte, daß $t^{\mathcal{A}} = a$ bedeutet, daß $t^{(\mathcal{A},\alpha)} = a$ unabhängig von der Belegung α ist.

Lemma 4.1.5 (Lösbarkeit)
Seien $s = t$ eine Gleichung über $\mathcal{T}(\Sigma, X)$ und $\mathcal{A}$ eine Σ-Algebra, deren Elemente erreichbar sind. Dann gilt:

$$s = t \text{ lösbar } \Leftrightarrow \exists\ \mathcal{A}\text{-Unifikator zu } s = t$$

Beweis
Noch zu zeigen „$\Rightarrow$“:
$s = t$ lösbar $\Rightarrow \mathcal{A} \models \exists X\ s = t \Rightarrow \exists\ \alpha : X \to A$ mit $(\mathcal{A}, \alpha) \models s = t$
α sei definiert duch $x_i \mapsto a_i$. Dann gibt es t_i mit $t_i^{\mathcal{A}} = a_i$, $t_i \in \mathcal{T}(\Sigma, Y)$ für geeignetes $Y \subseteq V$.
Sei $\sigma : \mathcal{T}(\Sigma, X) \to \mathcal{F}_{\mathcal{A}}(Y)$ definiert durch $x \mapsto t_i$
Offensichtlich gilt $s\sigma = t\sigma$. □

Etwas anders ausgedrückt liegt das Problem an folgender Tatsache: $\mathcal{F}_{\mathcal{A}}(X)$ ist logisch äquivalent[1] zu $\mathcal{A}$ bzgl. allquantifizierter Gleichungen (vgl. Satz 3.3.1), jedoch nicht logisch äquivalent bzgl. existenzquantifizierter Gleichungen. Sieht man sich noch einmal den Beweis von Satz 3.3.1 an, so kann man bei existenzquantifizierten Gleichungen nicht schließen, daß aus der Erfüllbarkeit in $\mathcal{A}$ auch die Erfüllbarkeit in $H(\{\mathcal{A}\})$ oder $S(\{\mathcal{A}\})$ folgt.
Wir halten also fest:

1. Untersucht man Gleichungen auf Lösbarkeit in $\mathcal{A}$ durch Prüfung, ob ein $\mathcal{A}$-Unifikator existiert, so ist dies vollständig, falls alle Elemente von $\mathcal{A}$ erreichbar sind.

2. Ist $\mathcal{A} = (A, \Sigma^A)$ eine Σ-Algebra, in der nicht alle Elemente von A erreichbar sind, so kann man zu einer Σ'-Algebra $\mathcal{A}'$ übergehen, in der alle Elemente erreichbar sind, indem man alle nicht erreichbaren Elemente aus A als nullstellige Funktionssymbole zu Σ hinzufügt.[2]

4.2 Symbolische Lösungen

Mit $\mathcal{A}$-Unifikatoren läßt sich nicht nur die Lösbarkeit in $\mathcal{A}$ testen, sondern sie eignen sich auch zum *Beschreiben* von Lösungen. Wir definieren zunächst, was ein Lösung ist:

[1] d.h. $\mathcal{F}_{\mathcal{A}}(X) \models \varphi \Leftrightarrow \mathcal{A} \models \varphi$

[2] In vielen Arbeiten wird daher der $\mathcal{A}$-Unifikator direkt als Homomorphismus über der Termalgebra der Signatur $\Sigma \cup A$ definiert. Dies führt aber z.B. bei $\mathbb{N}$ als Universum zu einer unendlichen Signatur, obwohl bereits mit $\Sigma = \{+, \underline{0}, \underline{1}\}$ alle Elemente aus $\mathbb{N}$ erreichbar sind.

Definition 4.2.1 (exakte Lösung)
Sei $\mathcal{A}$ eine Σ-Algebra, $s = t$ eine Gleichung über $\mathcal{T}(\Sigma, X)$ und $\alpha : \mathcal{T}(\Sigma, X) \to \mathcal{A}$ eine Belegung. Dann heißt α ***exakte Lösung*** *von $s = t$, falls $(\mathcal{A}, \alpha) \models s = t$.*

Beispiel 4.2.2
Sei die Signatur $\Sigma := \{+, \underline{0}\}$ gegeben und betrachten wir als Σ-Algebra die natürlichen Zahlen, aufgefaßt als additiven Monoid. Für die Gleichung $x + x + x + x = y + y$ (abkürzend schreiben wir dafür $4x = 2y$) sind die exakten Lösungen die Homomorphismen $\{x \mapsto 0, y \mapsto 0\}$, $\{x \mapsto 1, y \mapsto 2\}$, $\{x \mapsto 2, y \mapsto 4\}$ usw.

Möchte man in diesem Beispiel alle Lösungen endlich repräsentieren, so ist klar, daß man dies nur *symbolisch* erreichen kann, da es unendlich viele Lösungen gibt. Offensichtlich ist die im obigen Beispiel betrachtete Gleichung äquivalent zur Gleichung $2x = y$.

Diese Gleichung kann als Substitution σ, $x \mapsto x, y \mapsto 2x$ (genauer $x \mapsto x, y \mapsto x + x$) aufgefaßt werden. Wendet man diese Substitution auf die Ausgangsgleichung an, so gilt für jede Belegung α der Variablen x durch ein Element aus $\mathbb{N}$, daß $(x + x + x + x)\sigma\alpha = (y + y)\sigma\alpha$. Wir definieren daher:

Definition 4.2.3 (symbolische Lösung)
Seien $\mathcal{A}$ eine Σ-Algebra, $s = t$ eine Gleichung über $\mathcal{T}(\Sigma, X)$ und σ eine Substitution, $\sigma : \mathcal{T}(\Sigma, X) \to \mathcal{T}(\Sigma, Y)$. Dann heißt σ ***symbolische Lösung*** *von $s = t$, falls $\mathcal{A} \models s\sigma = t\sigma$.*

Auch hier werden wir $\sigma : \mathcal{T}(\Sigma, X) \to \mathcal{T}(\Sigma, Y)$ mit $\sigma : \mathcal{F}_{\mathcal{A}}(X) \to \mathcal{F}_{\mathcal{A}}(Y)$ identifizieren, so daß unter der Beachtung der Äquivalenz

$$\mathcal{A} \models s\sigma = t\sigma \Leftrightarrow \mathcal{F}_{\mathcal{A}}(Y) \models s\sigma = t\sigma$$

symbolische Lösungen genau die $\mathcal{A}$-Unifikatoren von (s, t) sind.

Eine symbolische Lösung ist also eine Substitution, bei der für alle Belegungen der abgebildeten Terme die Gleichung in der betrachteten Algebra $\mathcal{A}$ gilt, d.h. $(s\sigma)\alpha = (t\sigma)\alpha$ für jede Belegung $\alpha : \mathcal{T}(\Sigma, X) \to \mathcal{A}$. Klammert man in obiger Gleichung anders, also $s(\sigma\alpha) = t(\sigma\alpha)$, d.h. $\sigma\alpha : \mathcal{T}(\Sigma, X) \to \mathcal{A}$, so sieht man, daß man exakte Lösungen als *Instanzen* symbolischer Lösungen erhält.

Im obigen Beispiel erhält man für die symbolische Lösung $\{x \mapsto x, y \mapsto x + x\}$ und die Belegung $\{x \mapsto 1\}$ die exakte Lösung $\{x \mapsto 1, y \mapsto 2\}$, die wir oben bereits als solche erkannt haben.

Beispiel 4.1.3 zeigt, daß in der Regel nicht alle exakten Lösungen durch symbolische beschrieben werden können.

Definition 4.2.4 (Symbolisierbarkeitseigenschaft)
Eine Σ-Algebra $\mathcal{A}$ hat die ***Symbolisierbarkeitseigenschaft****, falls alle exakten Lösungen Instanzen symbolischer Lösungen sind.*

Satz 4.2.5
In einer Σ-Algebra $\mathcal{A}$ sind alle exakten Lösungen Instanzen symbolischer Lösungen, falls alle Elemente von $\mathcal{A}$ erreichbar sind.

Beweis
Sei $s = t$ eine Gleichung über $T(\Sigma, X)$ und $\alpha : \mathcal{T}(\Sigma, X) \rightarrow \mathcal{A}$ eine exakte Lösung, d.h. $s\alpha = t\alpha$. Dann ist α eindeutig bestimmt durch $x_1 \mapsto a_1, \ldots, x_n \mapsto a_n$ mit $\{x_1, \ldots, x_n\}$ die in s und t auftretenden Variablen und $a_i \in A$ für $i \in \{1, \ldots, n\}$. Da jedes Element a_i von $\mathcal{A}$ erreichbar ist, gibt es Terme $t_1, \ldots, t_n$ mit $t_i^{\mathcal{A}} = a_i$ für $i \in \{1, \ldots, n\}$. Dann gilt für $\sigma : \mathcal{T}(\Sigma, X) \rightarrow \mathcal{A}$ definiert durch $x_i \mapsto t_i$, daß $(s\sigma)^{\mathcal{A}} = (t\sigma)^{\mathcal{A}}$ und $\alpha = \sigma\beta$ für beliebiges $\beta : \mathcal{T}(\Sigma, X) \rightarrow \mathcal{A}$. $\square$

Folgerung 4.2.6
Sind alle Elemente einer Σ-Algebra erreichbar, so besitzt sie die Symbolisierbarkeitseigenschaft.

Auch hier kann man bei einer endlichen Σ-Algebra $\mathcal{A}$ leicht zu einer endlichen Algebra $\mathcal{A}'$ mit endlicher Signatur Σ' übergehen, in der jedes Element erreichbar ist, indem man die Elemente $a_1, \ldots, a_n$ des Universums als 0-stellige Funktionsymbole $\underline{a}_1, \ldots, \underline{a}_n$ zur Signatur hinzunimmt.

Kapitel 5

Unifikation in monoidal-kommutativen Gleichungstheorien

Statt einen Unifikationsalgorithmus[1] für eine einzelne Gleichungstheorie zu entwickeln, ist man bestrebt, Algorithmen direkt für eine ganze Klasse von Theorien zu entwickeln. In diesem Kapitel soll eine Klasse von Gleichungstheorien, sogenannte monoidale bzw. kommutative Theorien, zusammen mit einem einheitlichen Unifikationsalgorithmus vorgestellt werden.

In Kapitel 6 wird anschließend gezeigt, wie sich die Unifikation in primalen Algebren auf die Unifikation in monoidalen Theorien zurückführen läßt.

Monoidale Theorien wurden von W. Nutt untersucht und z.B. in [Nutt92] vorgestellt. Kommutative Theorien wurden von F. Baader definiert und u.a. in [Baa89] betrachtet. Die folgenden Ausführungen wurden im wesentlichen diesen beiden Quellen entnommen.

5.1 Monoidale/kommutative Theorien

Definition 5.1.1 (monoidale Theorie)
Seien Σ eine Signatur und E eine Menge von Identitäten über $\mathcal{T}(\Sigma, X)$. Dann heißt die von E erzeugte Gleichungstheorie $\mathcal{E} = \langle E \rangle_{\mathsf{SC}}$ ***monoidal****, falls gilt:* [2]

1. $\Sigma = \Sigma^{(0)} \dot\cup \Sigma^{(1)} \dot\cup \Sigma^{(2)}$ *mit* $\Sigma^{(2)} = \{+\}$, $\Sigma^{(0)} = \{0\}$, $\Sigma^{(1)}$ *beliebig.*

[1] d.h. einen Algorithmus zur Berechnung minimal vollständiger Mengen von Unifikatoren (evtl. *eines mgu*), falls existent

[2] Zur Erinnnerung: $s =_{\mathcal{E}} t$ ist Kurzschreibweise für $(s, t) \in \mathcal{E}$.

2. *+ ist assoziativ und kommutativ:*

$$\begin{aligned} (x+y)+z &=_{\mathcal{E}} x+(y+z) \\ x+y &=_{\mathcal{E}} y+x \end{aligned}$$

3. *0 ist neutrales Element bzgl. +:*

$$0+x =_{\mathcal{E}} x$$

4. *Jedes $h \in \Sigma^{(1)}$ ist Homomorphismus für + und 0:*

$$\begin{aligned} h(x+y) &=_{\mathcal{E}} h(x)+h(y) \\ h(0) &=_{\mathcal{E}} 0 \end{aligned}$$

Monoidale Theorien beschreiben also Varietäten abelscher Monoide mit Homomorphismen.

Beispiel 5.1.2
Sei $+$ ein zweistelliges und 0 ein nullstelliges Funktionssymbol. Als Signaturen seien gegeben: $\Sigma := \{+, 0\}$, $\Sigma' := \Sigma \cup \{h\}$, wobei h einstellig ist, $\Delta := \{+, 0, -\}$, wobei $-$ einstellig ist, $\Delta' := \Delta \cup \{h\}$, wobei h einstellig ist und $\Omega := \{+, 0, i\}$, wobei i einstellig ist. Dann sind die folgenden Gleichungstheorien offensichtlich monoidal:

$AC = \langle E_{AC} \rangle_{\mathsf{SC}}$, wobei E_{AC} aus den Identitäten über Σ für Assoziativität, Kommutativität und Neutralität der 0 bzgl. + besteht. AC beschreibt die **Theorie abelscher Monoide** und ist die kleinste monoidale Theorie in dem Sinne, daß keine weiteren Homomorphismensymbole oder weitere als die in der Definition verlangten Identitäten gelten.

$ACI = \langle E_{ACI} \rangle_{\mathsf{SC}}$, die **Theorie idempotenter abelscher Monoide**. Dabei ist $E_{ACI} := E_{AC} \,\dot{\cup}\, \{x + x = x\}$.

$ACN = \langle E_{ACN} \rangle_{\mathsf{SC}}$, die **Theorie n-kongruenter abelscher Monoide**. Dabei ist $E_{ACN} := E_{AC} \,\dot{\cup}\, \{\underbrace{x + \cdots + x}_{n} = x\}$. Für $n = 2$ erhält man die Theorie idempotenter abelscher Monoide.

$ACH = \langle E_{ACH} \rangle_{\mathsf{SC}}$, die **Theorie abelscher Monoide mit Homomorphismus** (über der Signatur Σ'). Dabei ist E_{ACH} die Vereinigung von E_{AC} mit den Identitäten, die besagen, daß h ein Homomorphismus ist.

$AG = \langle E_{AG} \rangle_{\mathsf{SC}}$, die **Theorie abelscher Gruppen**. E_{AG} ist definiert über der Signatur Δ und umfaßt Identitäten, die festlegen, daß + die binäre Operation einer abelschen Gruppe mit neutralem Element 0 und Inversersionsoperation $-$ ist.

$AGH = \langle E_{AGH} \rangle_{\mathsf{SC}}$, die **Theorie abelscher Gruppen mit Homomorphismus** (über Δ') erweitert AG um „Homomorphismengleichungen“ für h.

Monoidale Theorien sind also mit expliziter Bezugnahme auf die Signatur definiert. Primale Algebren hingegen, die wir später definieren, werden unabhängig von der Signatur definiert. Um die zugehörigen freien Algebren hinsichtlich der Unifikationseigenschaften vergleichen zu können, ist es hilfreich, die Struktur freier Algebren einer monoidalen Theorie genauer zu untersuchen. Dazu benötigen wir einige Begriffe:

Definition 5.1.3 (Semiadditive Kategorie)

1. *Eine **semiadditive Struktur** auf einer punktierten Kategorie $\mathfrak{C}$ ist eine Abbildung $+$, die jedem Paar $(f, g) \in \mathfrak{M}^2$ mit $f, g : A \to B$ einen Morphismus $h := f + g$ mit $h : A \to B$ zuordnet, wobei $+$ folgende Bedingungen erfüllt:*

   (SA1) Für jedes Paar (A, B) von $\mathfrak{C}$-Objekten ist

   $$(Hom(A, B), 0_{AB}, +|_{Hom(A,B)})$$

   ein kommutativer Monoid.

   (SA2) Die Komposition ist links- und rechtsdistributiv bzgl. $+$, das heißt, für $\mathfrak{C}$-Morphismen $f : A \to B$, $g, h : B \to C$, $k : C \to D$ gilt

   $$f \circ (g + h) = f \circ g + f \circ h$$

   und

   $$(g + h) \circ k = g \circ k + h \circ k$$

2. *Eine Kategorie $\mathfrak{C}$ heißt genau dann **semiadditive Kategorie**, wenn*

   (a) $\mathfrak{C}$ ein Nullobjekt enthält und

   (b) auf $\mathfrak{C}$ eine semiadditive Struktur $+$ existiert.[3]

Statt $\mathfrak{C}$ schreiben wir dann auch $(\mathfrak{C}, +)$, falls $+$ eine semiadditive Struktur auf $\mathfrak{C}$ ist.

Lemma 5.1.4
Die kanonische Kategorie $\mathfrak{C}_{\mathcal{E}}$ einer monoidalen Theorie $\mathcal{E}$ ist semiadditiv.

Beweis
$\mathcal{F}_{\mathcal{E}}(\emptyset)$ ist ein Nullobjekt für $\mathfrak{C}_{\mathcal{E}}$: Das Universum von $\mathcal{F}_{\mathcal{E}}(\emptyset)$ besteht offensichtlich nur aus dem Term 0, d.h. $|\mathcal{F}_{\mathcal{E}}(\emptyset)| = 1$. Für $\sigma : \mathcal{F}_{\mathcal{E}}(X) \to \mathcal{F}_{\mathcal{E}}(\emptyset)$ gilt somit $x \mapsto 0$ für alle $x \in X$. Andererseits existiert durch die Definition $x \mapsto 0$ für alle $x \in X$ ein Homomorphismus von $\mathcal{F}_{\mathcal{E}}(X)$ auf $\mathcal{F}_{\mathcal{E}}(\emptyset)$. Somit ist $\mathcal{F}_{\mathcal{E}}(\emptyset)$ terminal. Da $\mathcal{F}_{\mathcal{E}}(\emptyset)$

[3] Beachte, daß aus der Existenz eines Nullobjekts in $\mathfrak{C}$ folgt, daß $\mathfrak{C}$ punktiert ist.

auf genau eine Weise in $\mathcal{F}_\mathcal{E}(X)$ eingebettet werden kann, ist $\mathcal{F}_\mathcal{E}(\emptyset)$ auch initial und somit Nullobjekt.

Somit ist $\mathfrak{C}_\mathcal{E}$ punktiert, genauer: Seien $\mathcal{F}_\mathcal{E}(X), \mathcal{F}_\mathcal{E}(Y) \in Ob\,\mathfrak{C}_\mathcal{E}$. Definiere den Morphismus $0_{\mathcal{F}_\mathcal{E}(X)\mathcal{F}_\mathcal{E}(Y)} : \mathcal{F}_\mathcal{E}(X) \to \mathcal{F}_\mathcal{E}(Y)$ durch $x \mapsto 0$ für $x \in X$. Offensichtlich ist $0_{\mathcal{F}_\mathcal{E}(X)\mathcal{F}_\mathcal{E}(Y)}$ konstant und cokonstant, also Nullmorphismus.

Sei $\sigma, \tau \in Hom(\mathcal{F}_\mathcal{E}(X), \mathcal{F}_\mathcal{E}(Y))$ gegeben durch $x_i \mapsto t_i$ bzw. $x_i \mapsto s_i$, $i \in \{1, \ldots, n\}$. Definiere $+ : Mor\,\mathfrak{C}_\mathcal{E} \times Mor\,\mathfrak{C}_\mathcal{E} \to Mor\,\mathfrak{C}_\mathcal{E}$ durch

$$+|_{Hom(\mathcal{F}_\mathcal{E}(X), \mathcal{F}_\mathcal{E}(Y))} : (\sigma, \tau) \mapsto (\sigma + \tau) \text{ mit } (\sigma + \tau) : x_i \mapsto s_i + t_i$$

Dann ist + offensichtlich wohldefiniert, und es gilt:

1. $0_{\mathcal{F}_\mathcal{E}(X)\mathcal{F}_\mathcal{E}(Y)} + \sigma = \sigma + 0_{\mathcal{F}_\mathcal{E}(X)\mathcal{F}_\mathcal{E}(Y)} = \sigma$ (aufgrund der Kommutativität von + auf $\mathcal{F}_\mathcal{E}(Y)$ und der Neutralität der $0 \in \mathcal{F}_\mathcal{E}(Y)$ bzgl. +).

2. Für $t \in \mathcal{F}_\mathcal{E}(X)$ gilt $t(\sigma + \tau) = (t\sigma) + (t\tau)$. Denn:

   Für $t = x_i$ gilt $x_i(\sigma + \tau) = s_i + t_i = x_i\sigma + x_i\tau$.

   Per Induktion gilt dann:
   Für $t = h(t')$

$$\begin{aligned} h(t')(\sigma + \tau) &= h(t'(\sigma + \tau)) \\ &\overset{IV}{=} h(t'\sigma + t'\tau) \\ &= h(t'\sigma) + h(t'\tau) \\ &= h(t')\sigma + h(t')\tau \end{aligned}$$

   Für $t = t_1 + t_2$ gilt

$$\begin{aligned} (t_1 + t_2)(\sigma + \tau) &= t_1(\sigma + \tau) + t_2(\sigma + \tau) \\ &\overset{IV}{=} t_1\sigma + t_1\tau + t_2\sigma + t_2\tau \\ &= t_1\sigma + t_2\sigma + t_1\tau + t_2\tau \\ &= (t_1 + t_2)\sigma + (t_1 + t_2)\tau \end{aligned}$$

   Per Induktion folgt die Behauptung für alle $t \in \mathcal{F}_\mathcal{E}(X)$.

3. Für $\lambda : \mathcal{F}_\mathcal{E}(Y) \to \mathcal{F}_\mathcal{E}(Z)$ und $\lambda' : \mathcal{F}_\mathcal{E}(Z) \to \mathcal{F}_\mathcal{E}(X)$ gilt

$$(\sigma + \tau)\lambda = \sigma\lambda + \tau\lambda$$

   da $(x(\sigma + \tau))\lambda = (x\sigma + x\tau)\lambda = x\sigma\lambda + x\tau\lambda = x(\sigma\lambda + \tau\lambda)$ und

$$\lambda'(\sigma + \tau) = \lambda'\sigma + \lambda'\tau$$

   da $x\lambda'(\sigma + \tau) \overset{2.}{=} x\lambda'\sigma + x\lambda'\tau = x(\lambda'\sigma + \lambda'\tau)$.

$+$ ist also eine semiadditive Struktur auf $\mathfrak{C}_{\mathcal{E}}$, so daß insgesamt $\mathfrak{C}_{\mathcal{E}}$ eine semiadditive Kategorie ist. □

Da für die semiadditive Struktur $+$ gilt, daß sie kommutativ ist, definieren wir:

Definition 5.1.5 (Kommutative Theorie)
*Eine Gleichungstheorie $\mathcal{E}$ heißt **kommutative Theorie**, falls die zu $\mathcal{E}$ kanonische Kategorie $\mathfrak{C}_{\mathcal{E}}$ semiadditiv ist.*

Folgerung 5.1.6
Jede monoidale Theorie ist eine kommutative Theorie.

5.2 Monoidale und kommutative Theorien sind äquivalent

Ziel dieses Abschnitts ist es zu zeigen, daß das Konzept der kommutativen Theorien nicht *allgemeiner* ist. Sicherlich können wir schon allein aufgrund der Signatur(einschränkung) bei monoidalen Theorien nicht eine direkte Umkehrung der letzten Folgerung erwarten, d.h. wir werden nicht zeigen können, daß jede kommutative Theorie eine monoidale Theorie ist. Aus der Sicht der Unifikation reicht es aber aus zu zeigen, daß zu jeder kommutativen Theorie eine äquivalente monoidale Theorie existiert (vgl. Kapitel 3.6).

Dazu einige Vorarbeit:

Definition 5.2.1 (idempotent)
*Sei $\mathcal{E}$ eine Gleichungstheorie über Σ. Ein Konstantensymbol $e \in \Sigma^{(0)}$ heißt **idempotent** in $\mathcal{E}$, wenn für alle $f \in \Sigma$ gilt: $fe\ldots e =_{\mathcal{E}} e$.*

Für $f \in \Sigma^{(0)}$ bedeutet dies $f =_{\mathcal{E}} e$.

Lemma 5.2.2 (vgl. [Baa89])
Sei $\mathcal{E}$ eine Gleichungstheorie über Σ mit kanonischer Kategorie $\mathfrak{C}_{\mathcal{E}}$. Dann sind folgende Aussagen äquivalent:

1. *$\mathfrak{C}_{\mathcal{E}}$ enthält ein Nullobjekt*
2. *$|\mathcal{F}_{\mathcal{E}}(\emptyset)| = 1$*
3. *$\exists\, e \in \Sigma^{(0)}$ mit e ist idempotent*

Beweis
Offensichtlich sind 2. und 3. äquivalent.

Da $\mathcal{F}_{\mathcal{E}}(\emptyset)$ freie Algebra ist, ist $\mathcal{F}_{\mathcal{E}}(\emptyset)$ initial in $\mathfrak{C}_{\mathcal{E}}$. Gilt zusätzlich $|\mathcal{F}_{\mathcal{E}}(\emptyset)| = 1$, so ist $\mathcal{F}_{\mathcal{E}}(\emptyset)$ auch terminal in $\mathfrak{C}_{\mathcal{E}}$, also Nullobjekt von $\mathfrak{C}_{\mathcal{E}}$. Dies zeigt „2. $\Rightarrow$ 1.“

Besitze nun $\mathfrak{C}_{\mathcal{E}}$ ein Nullobjekt $\mathcal{N}$. Da $\mathcal{F}_{\mathcal{E}}(\emptyset)$ initial ist, existiert genau ein Homomorphismus von $f : \mathcal{F}_{\mathcal{E}}(\emptyset) \to \mathcal{N}$ und, da $\mathcal{N}$ initial ist, existiert genau ein Homomorphismus von $g : \mathcal{N} \to \mathcal{F}_{\mathcal{E}}(\emptyset)$. Aufgrund der Eindeutigkeit gilt $f \circ g = 1_{\mathcal{F}_{\mathcal{E}}(\emptyset)}$ und $g \circ f = 1_{\mathcal{N}}$. Somit sind $\mathcal{F}_{\mathcal{E}}(\emptyset)$ und jedes Nullobjekt isomorph. Für $|\mathcal{F}_{\mathcal{E}}(\emptyset)| > 1$ existieren mindestens zwei Morphismen von $\mathcal{F}_{\mathcal{E}}(\{x\})$ nach $\mathcal{F}_{\mathcal{E}}(\emptyset)$. Für $|\mathcal{F}_{\mathcal{E}}(\emptyset)| = 0$ existiert kein Morphismus von $\mathcal{F}_{\mathcal{E}}(\{x\})$ nach $\mathcal{F}_{\mathcal{E}}(\emptyset)$. Dies zeigt „1. $\Rightarrow$ 2. “ □

Definition 5.2.3 (implizite Operation)
Es sei $\mathfrak{K}$ ein Klasse von Σ-Algebren. Eine n-stellige implizite Operation in $\mathfrak{K}$ ist eine Familie $f = (f_{\mathcal{A}})_{\mathcal{A} \in \mathfrak{K}}$ von Abbildungen $f^{\mathcal{A}} : A^n \to A$, die mit allen Homomorphismen verträglich ist, das heißt, für jeden Homomorphismus $h : \mathcal{A} \to \mathcal{B}$ mit $\mathcal{A}, \mathcal{B} \in \mathfrak{K}$ und alle $a_1, \ldots, a_n \in A$ ist $f^{\mathcal{A}}(a_1, \ldots, a_n)h = f^{\mathcal{B}}(a_1 h, \ldots, a_n h)$.

Offenbar induziert jeder Σ-Term eine implizite Operation in jeder Klasse von Σ-Algebren. Sei umgekehrt $\mathcal{E}$ eine Gleichungstheorie. Dann gilt für die durch $\mathcal{E}$ erzeugte Varietät und für die zu $\mathcal{E}$ kanonische Kategorie $\mathfrak{C}_{\mathcal{E}}$, daß alle impliziten Operationen durch Σ-Terme definiert werden können (vgl. [La63]).

Satz 5.2.4
$\mathfrak{C}_{\mathcal{E}}$ enthalte ein Nullobjekt, e sei idempotentes Konstantensymbol. Dann sind die folgenden Aussagen äquivalent:

1. *$\mathfrak{C}_{\mathcal{E}}$ ist semiadditiv*
2. *Es gibt eine binäre implizite Operation $*$ in $Ob\,\mathfrak{C}_{\mathcal{E}}$ mit*
   (a) *Die Konstante e ist neutrales Element für $*$ in jeder Algebra $\mathcal{F} \in Ob\,\mathfrak{C}_{\mathcal{E}}$.*
   (b) *Für jedes $f \in \Sigma^{(n)}$ und jede Algebra $\mathcal{F} \in Ob\,\mathfrak{C}_{\mathcal{E}}$ und alle $s_1, \ldots, s_n$, $t_1, \ldots, t_n \in \mathcal{F}$ gilt*
   $$f(s_1 * t_1, \ldots, s_n * t_n) = f(s_1, \ldots, s_n) * f(t_1, \ldots, t_n)$$

Beweis
Siehe [Baa89, S. 74]. □

Wir kommen nun zu dem angekündigten Satz:

Satz 5.2.5 (vgl. [BaNu90])
Zu jeder kommutativen Theorie $\mathcal{E}$ über der Signatur Σ existiert eine Signatur Σ' und eine monoidale Theorie $\mathcal{E}'$ über der Signatur Σ' mit

$$\mathcal{E} \sim \mathcal{E}'$$

Beweis

Wir geben die Signatur Σ' und eine Signaturtransformation an: Σ' enthalte neben dem zweistelligen $+$ und der Konstanten 0 zu jedem $f \in \Sigma^{(n)}$ einstellige $f_1, \ldots, f_n$. Sei e die idempotente Konstante von $\mathcal{E}$ und $t_*(x,y)$ Term der impliziten Operation $*$ (vgl. Satz 5.2.4). Sei $\Delta' : \mathcal{T}(\Sigma', X) \to \mathcal{T}(\Sigma, X)$ definiert durch

$$\begin{aligned} 0\Delta' &= e \\ (x+y)\Delta' &= t_* \\ f_i(x)\Delta' &= f(\underbrace{e, \ldots, e}_{i-1}, \underbrace{x}_{i-\text{te Pos.}}, \underbrace{e, \ldots, e}_{n-i}) \end{aligned}$$

und $E' := \{s' = t' \ : \ s'\Delta' =_{\mathcal{E}} t'\Delta'\}$. Sei $\Delta : \mathcal{T}(\Sigma, X) \to \mathcal{T}(\Sigma', X)$ definiert durch

$$\begin{aligned} e\Delta &= 0 \\ f(x_1, \ldots, x_n)\Delta &= f_1(x_1) + \ldots + f_n(x_n) \end{aligned}$$

Eine leichte Rechnung zeigt, daß $\mathcal{E}' := \langle E' \rangle_{\mathsf{SC}}$ eine monoidale Theorie ist und daß $\mathcal{E}$ und $\mathcal{E}'$ äquivalent sind (vgl. [BaNu90, S. 11f.]). $\square$

Wir wollen daher im folgenden auch von monoidal-kommutativen Theorien sprechen.

Eine wichtige Eigenschaft monoidaler und somit auch kommutativer Theorien, die für die Unifikation verwendet wird, ist die Existenz von Biprodukten in der zugehörigen kanonischen Kategorie:

Satz 5.2.6

Sei $\mathcal{E}$ eine monoidale Theorie mit zugehöriger kanonischer Kategorie $\mathfrak{C}_{\mathcal{E}}$. Dann existiert zu jeder endlichen Familie $(\mathcal{F}_{\mathcal{E}}(X_i))_{i \in I}$ ein Biprodukt.

Beweis

Nach Lemma 3.5.3 existiert zu der Familie $(\mathcal{F}_{\mathcal{E}}(X_i))_{i \in I}$ ein Coprodukt

$$((\iota_i)_{i \in I}, \mathcal{F}_{\mathcal{E}}(X)) .$$

Analog zum Beweis von Lemma 3.5.3 sei $X_i = \{x_{i_1}, \ldots, x_{i_{|X_i|}}\}$ für $i \in I$, $X := \dot{\bigcup} X_i = \{x_{ij} \ : \ i \in I, j \in \{1, \ldots, |X_i|\}\}$, $\iota_i : \mathcal{F}_{\mathcal{E}}(X_i) \to \mathcal{F}_{\mathcal{E}}(X)$, $x_{i_j} \mapsto x_{ij}$. Sei $\pi_i : \mathcal{F}_{\mathcal{E}}(X) \to \mathcal{F}_{\mathcal{E}}(X_i)$ definiert durch $x_{ij} \mapsto x_{i_j}$ und $x_{kl} \mapsto 0$ für $k \neq i$, $j \in \{1, \ldots, |X_i|\}$, $l \in \{1, \ldots, |X_k|\}$. Dann gilt offensichtlich $\iota_i \pi_j = \delta_{ij}$ und $\pi_i \iota_j = \delta_{ij}$. Noch zu zeigen: $(\mathcal{F}_{\mathcal{E}}(X), (\pi_i)_{i \in I})$ ist ein Produkt. Sei $(\psi_i)_{i \in I}$, $\psi_i : \mathcal{F}_{\mathcal{E}}(Y) \to \mathcal{F}_{\mathcal{E}}(X_i)$ zu $Y = \{x_1, \ldots, x_m\}$ gegeben durch $\psi_i : x_j \mapsto t_{ij}$. Setze $\psi : \mathcal{F}_{\mathcal{E}}(Y) \to \mathcal{F}_{\mathcal{E}}(X)$ als $\psi := \sum_i \psi_i \iota_i$. Dann ist $\psi \pi_i = (\sum_k \psi_k \iota_k) \pi_i = \sum_k (\psi_k \iota_k \pi_i) = \sum_k (\psi_k \delta_{ki}) = \psi_i$ für alle $i \in I$. Dies zeigt, daß $((\iota_i)_{i \in I}, \mathcal{F}_{\mathcal{E}}(X), (\pi_i)_{i \in I})$ ein Biprodukt ist. $\square$

Eine etwas abstraktere Art, obige Aussage zu bestätigen, liefert folgendes Lemma:

Lemma 5.2.7
Sei $(\mathfrak{C}, +)$ eine semiadditive Kategorie, $((\iota_i)_I, \mathcal{B})$ ein Coprodukt der endlichen Familie $(\mathcal{A}_i)_I$. Dann kann $((\iota_i)_I, \mathcal{B})$ auf eindeutige Weise zu einem Biprodukt $((\iota_i)_I, \mathcal{B}, (\pi_i)_I)$ erweitert werden.

Beweis
Nach Definition eines Coproduktes existiert zu jedem $j \in I$ ein eindeutig bestimmtes $\pi_j : \mathcal{B} \rightarrow \mathcal{A}_j$ mit $\delta_{ij} = \iota_i \pi_j$.
Für $(\mathcal{A}, (f_j)_{j \in I})$, $f_j : \mathcal{A} \rightarrow \mathcal{A}_j$ sei $f = \sum_{j \in I} f_j \iota_j$. Dann ist $f\pi_k = \left(\sum_j f_j \iota_j\right) \pi_k = \sum_j f_j \iota_j \pi_k = \sum_j f_j \delta_{jk} = \begin{cases} f_j & k = j \\ 0 & \text{sonst} \end{cases}$

$$\begin{tikzcd} \mathcal{A}_i \arrow[d, "\iota_i"'] \arrow[dr, "\delta_{ij}"] & \\ \mathcal{B} \arrow[r, "\pi_j"'] & \mathcal{A}_j \end{tikzcd}$$

Somit ist $((\iota_i)_I, \mathcal{B}, (\pi_i)_I)$ ein Biprodukt. $\square$

5.3 Unifikation in monoidalen/kommutativen Theorien

Im folgenden wird kurz die Idee bei der Unifikation in monoidalen Theorien geschildert. Für eine umfassende Darstellung sei auf [Nutt92] verwiesen.

Bei der Unifikation in monoidalen Theorien wird einer Theorie $\mathcal{E}$ ein *Halbring* $\mathcal{S}_\mathcal{E}$ zugeordnet. Ein Unifikationsproblem Γ über $\mathcal{E}$ wird dann in ein lineares Gleichungssystem über dem Halbring $\mathcal{S}_\mathcal{E}$ transformiert, das Gleichungsystem gelöst und die Lösung in eine Substitution zurückübersetzt. Diese ist dann ein allgemeinster Unifikator für Γ. Schematisch sei der Sachverhalt noch einmal in Abbildung 5.1 dargestellt.

$$\begin{array}{ccc} \text{Unifikationsproblem} & \longleftrightarrow & \text{lin. Gleichungssystem} \\ \downarrow & & \downarrow \\ \text{Monoidale Theorie} & \longleftrightarrow & \text{Halbring} \end{array}$$

Abbildung 5.1:

Definition 5.3.1 (Halbring)
*Ein **Halbring** ist eine Menge $\mathcal{S}$ mit verschiedenen Elementen 0 und 1 und zwei zweistelligen Operationen $+$ und $\cdot$, so daß $(\mathcal{S}, +, 0)$ ein kommutativer Monoid und $(\mathcal{S}, \cdot, 1)$ ein Monoid ist und für alle $a, b, c \in \mathcal{S}$ gilt:*

1. $(a + b) \cdot c = a \cdot c + b \cdot c$
2. $a \cdot (b + c) = a \cdot b + a \cdot c$

3. $0 \cdot a = a \cdot 0 = 0$

Im Gegensatz zu Ringen besitzen Halbringe also nicht notwendigerweise ein Inverses bzgl. der Addition.

Beispiel 5.3.2

- *Die natürlichen Zahlen* $\mathbb{N}$ *zusammen mit* $+$, $\cdot$, 0 *und* 1 *sind offensichtlich ein Halbring.*
- *Jeder Ring (mit 1) ist ein Halbring.*

Für monoidale Theorien gilt:

Satz 5.3.3
Seien $\mathcal{E}$ *eine monoidale Theorie und* $\mathcal{A}$ *eine* $\mathcal{E}$*-Algebra. Dann ist*

$$(End\ A, +, 0_{\mathcal{A}}, \circ, id_{\mathcal{A}})$$

ein Halbring, wobei $id_{\mathcal{A}}$ *die Identität auf* $\mathcal{A}$ *bezeichne und die Addition* $+$ *zweier Endomorphismen* $\sigma, \tau \in End\ A$ *durch*

$$a(\sigma + \tau) := a\sigma + a\tau$$

für alle $a \in A$ *definiert ist.*

Beweis
Der Beweis ergibt sich durch einfaches Nachrechnen der Halbring-Gesetze, vgl. [Nutt92, 6.3]. □

Für eine monoidale Theorie $\mathcal{E}$ definieren wir nun den kanonischen Halbring $\mathcal{S}_{\mathcal{E}}$:

Definition 5.3.4 (kanonischer Halbring)
Sei $\mathcal{E}$ *eine monoidale Theorie. Dann ist der* ***kanonische Halbring*** $\mathcal{S}_{\mathcal{E}}$ *definiert als:*

$$\mathcal{S}_{\mathcal{E}} := (end\ \mathcal{F}_{\mathcal{E}}(u), +, 0_{\mathcal{F}_{\mathcal{E}}(u)}, \circ, id_{\mathcal{F}_{\mathcal{E}}(u)})$$

für eine Variable u.

Beispiel 5.3.5
Sei $\Sigma := \Sigma^{(0)} \dot\cup \Sigma^{(2)} \dot\cup \Sigma^{(1)}$ mit $\Sigma^{(0)} = \{0\}$, $\Sigma^{(1)} = \{-\}$, $\Sigma^{(2)} = \{+\}$ und $\mathcal{E} := AG = \langle E_{AG} \rangle_{\mathsf{SC}}$ die Theorie abelscher Gruppen. Zur Erinnerung sei erwähnt, daß E_{AG} über der Signatur Σ definiert ist und aus den Identitäten, die festlegen, daß $+$ die binäre Operation einer abelschen Gruppe mit neutralem Element 0 und Inversionsoperation $-$ ist, besteht.

In $\mathcal{F}_{\mathcal{E}}(\{u\})$ gibt es offensichtlich nur die folgenden Kongruenzklassen von Termen:

$$[0], [u], [u+u], [u+u+u], \ldots$$

kurz

$$[0u], [1u], [2u], [3u], \ldots$$

Somit sind die Endomorphismen von $\mathcal{F}_{\mathcal{E}}(\{u\})$ die Homomorphismen, die eindeutig bestimmt sind durch

- $u \mapsto [0u]$
- $u \mapsto [1u]$
- $u \mapsto [2u]$
- $u \mapsto [3u]$

  $\vdots$

Die Addition zweier Endomorphismen $\sigma, \tau \in End\,\mathcal{F}_{\mathcal{E}}(\{u\})$ ergibt sich somit folgendermaßen: seien σ, τ bestimmt durch

$$\sigma : u \mapsto [mu] \qquad \tau : u \mapsto [nu]$$

Dann ist $\sigma + \tau$ der Endomorphismus, der eindeutig bestimmt ist durch

$$(\sigma + \tau) : u \mapsto [(m+n)u] \qquad (*)$$

Offensichtlich kann man σ und τ mit m bzw. n in $\mathbb{Z}$ identifizieren. $(*)$ liefert dann, daß für $\sigma+\tau$ entsprechend $m+n$ gilt. Man kann sogar zeigen, daß $\mathcal{S}_{\mathcal{E}} \cong \mathbb{Z}$ gilt (vgl. [Nutt92, 6.4]).

Moduln über Halbringen sind Verallgemeinerungen von Vektorräumen über Körpern. Da die Multiplikation in einem Halbring jedoch nicht kommutativ sein muß, muß zwischen Links- und Rechtsmoduln unterschieden werden:

Definition 5.3.6 (Modul)
*Ein **Linksmodul** (bzw. **Rechtsmodul**) über einem Halbring $\mathcal{S}$ ist ein kommutativer Monoid $(\mathcal{M}, +, 0)$ mit einer Skalarmultiplikation*

$$\mathcal{S} \times \mathcal{M} \rightarrow \mathcal{M} \quad \textit{bzw.} \quad \mathcal{M} \times \mathcal{S} \rightarrow \mathcal{M},$$

so daß für alle $a, b \in \mathcal{S}$ und $v, w \in \mathcal{M}$ gilt:

$$\begin{array}{lll}
(ab)v = a(bv) & \text{bzw.} & v(ab) = (va)b \\
(a+b)v = av + bv & \text{bzw.} & v(a+b) = va + vb \\
a(v+w) = av + aw & \text{bzw.} & (v+w)a = va + vb \\
a0 = 0 & \text{bzw.} & 0a = 0 \\
1v = v & \text{bzw.} & v1 = v \\
0v = 0 & \text{bzw.} & v0 = 0
\end{array}$$

Für eine endliche Menge X bezeichne $\mathcal{S}^X$ die Menge der Tupel über $\mathcal{S}$ indiziert durch Elemente von X. $\mathcal{S}^X$ wird zu einem $\mathcal{S}$-Linksmodul bzw. Rechtsmodul indem wir die Addition komponentenweise und die Skalarmultiplikation durch $a(b_x)_{x\in X} := (ab_x)_{x\in X}$ bzw. $((b_x)_{x\in X})a := (b_x a)_{x\in X}$ definieren. Der **Einheitsvektor** $e_y \in \mathcal{S}^X$ ist das Tupel $(a_x)_{x\in X}$ mit $a_y = 1$ und $a_x = 0$ für $x \neq y$.

Analog wie bei Vektorräumen definiert man lineare Abbildungen, wobei man hier zwischen linkslinearen und rechtslinearen Abbildungen unterscheiden muß.

Seien $\mathcal{M}, \mathcal{N}$ Linksmoduln (Rechtsmoduln). Eine Abbildung $\sigma : \mathcal{M} \to \mathcal{N}$ heißt **linkslinear** (**rechtslinear**), falls für alle $a \in \mathcal{S}$ und alle $v, w \in \mathcal{M}$ gilt:

$$\begin{array}{c}
(v+w)\sigma = v\sigma + w\sigma \\
(av)\sigma = a(v\sigma) \quad \text{bzw.} \quad (va)\sigma = (v\sigma)a \\
0\sigma = 0
\end{array}$$

Ein Linksmodul (Rechtsmodul) $\mathcal{M}$ heißt **frei über einer Menge von Erzeugern $\boldsymbol{X \subseteq \mathcal{M}}$**, falls für jeden Linksmodul (Rechtsmodul) $\mathcal{N}$ und jede Abbildung $g : X \to \mathcal{N}$ eine eindeutige linkslineare (rechtslineare) Abbildung $\sigma_g : \mathcal{M} \to \mathcal{N}$ existiert, so daß $x\sigma_g = xg$ für alle $x \in X$.

Lemma 5.3.7 ([Nutt92, 5.3])
Für endliches X ist $\mathcal{S}^X$ mit skalarer Links- bzw. Rechtsmultiplikation ein freier Links- bzw. Rechtsmodul über $\{e_x : x \in X\}$.

Analog wie bei Vektorräumen kann man bei freien Moduln lineare Abbildungen durch Matrizen darstellen. Eine linkslineare Abbildung $\sigma : \mathcal{S}^X \to \mathcal{S}^Y$ kann durch eine $X \times Y$-Matrix $C_\sigma = (\sigma_{xy})_{x\in X, y\in Y}$ mit Einträgen aus $\mathcal{S}$ beschrieben werden, indem man die Zeile x von C_σ auf $e_x\sigma$ setzt. Umgekehrt führt jede $X \times Y$-Matrix C zu einer linkslinearen Abbildung $\sigma_C : \mathcal{S}^X \to \mathcal{S}^Y$ durch $v\sigma_c := vC$.

Analog kann man bei rechtslinearen Abbildungen vorgehen. Insbesondere kann man jede Matrix einer linkslinearen Abbildung σ auch als Matrix einer rechtslinearen Abbildung σ^* verstehen und umgekehrt. Man spricht dann von der zu σ **dualen Abbildung** σ^* (vgl. [Nutt92, Abschnitt 5.3]).

Beispiel 5.3.8
Sei $\mathcal{S} = \mathbb{Z}$. Betrachte die $\mathbb{Z}$-Moduln $\mathbb{Z}^k$ für $k = 2, 3$. Dann entspricht der Matrix

$$\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix}$$

die linkslineare Abbildung $\sigma : \mathbb{Z}^2 \to \mathbb{Z}^3$ mit

$$(x, y) \mapsto (1x + 4y, 2x + 5y, 3x + 6y)$$

und die rechtslineare Abbildung $\sigma^* : \mathbb{Z}^3 \to \mathbb{Z}^2$ mit

$$(x, y, z) \mapsto (1x + 2y + 3z, 4x + 5y + 6z).$$

Wir wollen nun mittels zweier Abbildungen die Σ-Homomorphismen zwischen freien $\mathcal{E}$-Algebren in Bezug zu linkslinearen Abbildungen zwischen freien $\mathcal{S}_\mathcal{E}$-Moduln setzen. Da man ein Unifikationsproblem als Unifikation von Σ-Homomorphismen verstehen kann (vgl. Lemma 3.5.1), kann auf diese Weise ein Unifikationsproblem in ein algebraisches Problem übersetzt werden.

Zu einem Homomorphismus $\sigma : \mathcal{F}_\mathcal{E}(X) \to \mathcal{F}_\mathcal{E}(Y)$ definieren wir eine linkslineare Abbildung $\sigma^{lin} : \mathcal{S}_\mathcal{E}^X \to \mathcal{S}_\mathcal{E}^Y$ wie folgt:

Für $x \in X$ seien $\iota_x : \mathcal{F}_\mathcal{E}(u) \to \mathcal{F}_\mathcal{E}(X)$ definiert durch

$$u \mapsto x$$

und $\pi_x : \mathcal{F}_\mathcal{E}(X) \to \mathcal{F}_\mathcal{E}(u)$ durch

$$\begin{aligned} x &\mapsto u \\ x' &\mapsto 0 \text{ für } x \neq x'. \end{aligned}$$

Für $\sigma : \mathcal{F}_\mathcal{E}(X) \to \mathcal{F}_\mathcal{E}(Y)$ sei

$$\sigma_{xy} := \iota_x \sigma \pi_y$$

und $\sigma^{lin} : \mathcal{S}_\mathcal{E}^X \to \mathcal{S}_\mathcal{E}^Y$ sei definiert durch

$$(\sigma_{xy})_{x \in X, y \in Y}.$$

Zu einer linkslinearen Abbildung $\sigma : \mathcal{S}_\mathcal{E}^X \to \mathcal{S}_\mathcal{E}^Y$ geg. durch die Matrix $(\sigma_{xy})_{x \in X, y \in Y}$ definieren wir einen Σ-Homomorphismus $\sigma^{hom} : \mathcal{F}_\mathcal{E}(X) \to \mathcal{F}_\mathcal{E}(Y)$ durch

$$\sigma^{hom} := \sum_{x \in X, y \in Y} \pi_x \sigma_{xy} \iota_y$$

Beispiel 5.3.9 (Fortsetzung von Beispiel 5.3.5 und 5.3.8)
Identifizieren wir, wie oben beschrieben, $\mathcal{S}_\mathcal{E}$ und $\mathbb{Z}$, so ist für die linkslineare Abbildung σ, gegeben durch die Matrix

$$M = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix}$$

$\sigma^{hom} : \mathcal{S}^{\{x_1,x_2\}} \to \mathcal{S}^{\{y_1,y_2,y_3\}}$ eindeutig bestimmt durch

$$\begin{aligned} x_1 &\mapsto 1y_1 + 2y_2 + 3y_3 \\ x_2 &\mapsto 4y_1 + 5y_2 + 6y_3. \end{aligned}$$

Andersherum ergibt sich für σ^{hom} gerade M als Matrix der entsprechenden linkslinearen Abbildung $(\sigma^{hom})^{lin}$.

Für $\cdot^{lin}$ kann man zeigen, daß es ein Isomorphismus (mit Inverser $\cdot^{hom}$) von der kanonischen Kategorie $\mathfrak{C}_\mathcal{E}$ auf die Kategorie der endlich erzeugten $\mathcal{S}_\mathcal{E}$-Linksmoduln ist (vgl. [Nutt92, Abschnitt 6.2]).
Für linkslineare Abbildungen $\sigma, \tau : \mathcal{S}^X \to \mathcal{S}^Y$ sei

$$ker(\sigma, \tau) := \{v \in \mathcal{S}^X : v\sigma = v\tau\}$$

und

$$im\,\sigma := \mathcal{S}^X\sigma = \{b \in \mathcal{S}^Y : \exists v \in \mathcal{S}^X \text{ mit } v\sigma = b\}$$

Dann gilt:

Satz 5.3.10 ([Nutt92, 7.2])
Seien $\sigma, \tau : \mathcal{S}_\mathcal{E}^X \to \mathcal{S}_\mathcal{E}^Y$ und $\delta : \mathcal{S}_\mathcal{E}^Y \to \mathcal{S}_\mathcal{E}^Z$ linkslineare Abbildungen. Dann gilt:

1. *δ ist Unifikator von σ und τ $\Leftrightarrow$ $im\,\delta^* \subseteq ker(\sigma^*, \tau^*)$*
2. *δ ist allgemeinster Unifikator von σ und τ $\Leftrightarrow$ $im\,\delta^* = ker(\sigma^*, \tau^*)$*

Ist der Kern von σ^* und τ^* endlich erzeugt, so kann man ein endliches Erzeugendensystem (aufgefaßt als Matrix) mittels $\cdot^{hom}$ in einen allgemeinsten Unifikator übersetzen.

Folgerung 5.3.11 (vgl. [Nutt92, 7.11])
Sei $\mathcal{E}$ eine monoidale Theorie und $\mathcal{S}_\mathcal{E}$ sei endlich. Dann ist $\mathcal{E}$ unitär.

Beweis
Da $\mathcal{S}_\mathcal{E}$ endlich ist, ist jeder Kern von σ^* und τ^* endlich erzeugt. □

Wir verdeutlichen die obigen Überlegungen an einem Beispiel:

Beispiel 5.3.12 (Fortsetzung von Beispiel 5.3.9)
Seien $Y = \{y_1, y_2\}$, $s = y_1 + y_1 + y_2$ und $t = y_1 + y_1 + y_2 + y_2$. Definiere η, $\nu : \mathcal{F}_{\mathcal{E}}(\{x\}) \to \mathcal{F}_{\mathcal{E}}(Y)$ durch

$$x\eta = y_1 + y_1 + y_2 \qquad x\nu = y_1 + y_1 + y_2 + y_2$$

kurz

$$x\eta = 2y_1 + 1y_2 \qquad x\nu = 2y_1 + 2y_2.$$

Betrachte im folgenden η, ν als Unifikationsproblem (im Sinne von Lemma 3.5.1).

Die zugehörigen linkslinearen Abbildungen lauten dann (in Matrixdarstellung über $\mathbb{Z}$):

$$C_{\eta^{lin}} = (2,1) \qquad C_{\nu^{lin}} = (2,2)$$

Der Kern von $(\eta^{lin})^*$ und $(\nu^{lin})^*$, d.h. die Menge

$$\left\{ \begin{pmatrix} z_1 \\ z_2 \end{pmatrix} \in \mathbb{Z}^2 \;:\; (2,1)\begin{pmatrix} z_1 \\ z_2 \end{pmatrix} = (2,2)\begin{pmatrix} z_1 \\ z_2 \end{pmatrix} \right\}$$

ist dann durch den Vektor $v = (1,0)^{tr}$ erzeugt. Als als Matrix einer linkslinearen Abbildung aufgefaßt entspricht v der Substitution $\delta : \mathcal{F}_{\mathcal{E}}(Y) \to \mathcal{F}_{\mathcal{E}}(Z)$ definiert durch $y_1 \mapsto z$ und $y_2 \mapsto 0$ mit $Z = \{z\}$. δ ist nach dem vorigen Satz allgemeinster Unifikator.

Es sei noch folgendes Resultat genannt, welches dahingehend interpretiert werden kann, daß das Konzept der monoidalen Theorien alle Unifikationsprobleme umfaßt, bei denen Unifikatoren durch Lösen von linearen Gleichungssystemen bestimmt werden können.

Lemma 5.3.13 ([Nutt92, 6.3])
Für jeden Halbring $\mathcal{S}$ existiert eine monoidale Theorie $\mathcal{E}$, so daß $\mathcal{S}$ und $\mathcal{S}_{\mathcal{E}}$ isomorph sind.

Kapitel 6

Unifikation in primalen Algebren

Ziel dieses Kapitels ist es, die Unifikation in primalen Algebren auf die Unifikation in monoidalen Theorien zurückzuführen, statt Verfahren vorzustellen, die direkt für primale Algebren entwickelt worden sind.

Dazu werden im ersten Abschnitt primale Algebren und einige ihrer Eigenschaften vorgestellt. Insbesondere wird gezeigt, daß primale Algebren und monoidale Theorien nicht äquivalent sind, so daß man nicht direkt Unifikationsalgorithmen für monoidale Theorien für die Unifikation in primalen Algebren übernehmen kann.

Im zweiten Abschnitt wird allerdings ein Übersetzungsschritt vorgestellt, der es erlaubt, die Unifikation in primalen Algebren auf die Unifikation in monoidalen Theorien zurückzuführen.

6.1 Primale Algebren

Zunächst die Definition einer primalen und zur Verdeutlichung die einer funktionalvollständigen Algebra:

Definition 6.1.1 (Primale/funktionalvollständige Algebren)
Eine Algebra $\mathcal{A} = (A, \Sigma)$ heißt ***primal*** *(bzw.* ***funktional vollständig****) $:\Leftrightarrow$ $\forall n \in \mathbb{N}\ \ \forall f : A^n \to A$ gibt es eine Termfunktion $t^{\mathcal{A}}$ (bzw. Polynomfunktion $p^{\mathcal{A}}$) mit*

$$f(a_1, \ldots, a_n) = t^{\mathcal{A}}(a_1, \ldots, a_n) \ \ \forall a_1, \ldots, a_n \in A$$

bzw.

$$f(a_1, \ldots, a_n) = p^{\mathcal{A}}(a_1, \ldots, a_n) \ \ \forall a_1, \ldots, a_n \in A$$

Beispiel 6.1.2
Betrachten wir folgende boolesche Algebren:

- $\mathcal{B} = (\{0,1\}, \{xor, \wedge\})$ mit der üblichen Interpretation von xor und $\wedge$ ist funktional vollständig aber nicht primal, da man das Element 1 nicht durch eine Termfunktion darstellen kann.
- $\mathcal{B} = (\{0,1\}, \{xor, \wedge, 1\})$ ist daher primal.
- $\mathcal{B} = (\{0,1\}, \{\vee, ^{-}\})$ ist primal. Das heißt, primale Algebren haben nicht notwendigerweise Konstanten in der Signatur.

Bisweilen bereitet es jedoch Probleme, keine Konstante in der Signatur zu haben (betrachte $\mathcal{F}_{\mathcal{A}}(\emptyset)$), so daß wir uns in diesen Fällen die Signatur temporär um ein Konstantensymbol erweitert denken.

Die nächsten beiden Resultate liefern einige Aussagen über die Struktur primaler Algebren.

Lemma 6.1.3
Eine primale Algebra $\mathcal{A}$ ist einfach, das heißt, sie besitzt nur die trivialen Kongruenzen, und hat keine echten Unteralgebren.

Beweis
Sei θ Kongruenzrelation von $\mathcal{A} = (A, \Sigma^A)$, $a \equiv b\ (\theta)$, $a \neq b$, und $c, d \in A$. Sei die Operation p so, daß $ap = c$ und $bp = d$. Aus $a \equiv b\ (\theta)$ folgt dann $c = ap \equiv bp = d\ (\theta)$. Somit ist $\theta = A \times A$. Sei $\mathcal{A}' = (A', \Sigma^{A'}) \leq \mathcal{A}$. Für $a \in \mathcal{A}$ sei p_a derart, daß $bp_a = a$ für alle $b \in \mathcal{A}$. Dann ist $\bigcup_{a \in A} A'p_a \supseteq A$, also $\mathcal{A} \leq \mathcal{A}'$. □

Lemma 6.1.4
Jede primale Algebra $\mathcal{A}$ ist gleichungsvollständig, das heißt, nimmt man zu den in $\mathcal{A}$ gültigen Gleichungen weitere hinzu, so erfüllt nur noch die triviale Algebra die erhaltene Menge von Gleichungen.

Beweis
Sei $\mathfrak{K} = HSP(\mathcal{A})$. Dann ist $\mathcal{F}_{\mathfrak{K}}(\emptyset) \cong \mathcal{A}$. Falls $\mathfrak{K}_1 \subseteq \mathfrak{K}$ und $\mathfrak{K}_1$ gleichungsdefiniert ist, dann ist $\mathcal{F}_{\mathfrak{K}_1}(\emptyset)$ homomorphes Bild von $\mathcal{F}_{\mathfrak{K}}(\emptyset)$. Wegen der Einfachheit folgt die Behauptung. □

Lemma 6.1.5
Jede primale Algebra ist endlich.

Beweis
Über unendlichem Universum existieren überabzählbar viele Funktionen, die Menge der Termfunktionen ist aber abzählbar. □

Gemäß Kapitel 3.3 betrachten wir bei der Unifikation in Algebren statt der Algebra selbst die zugehörige freie Algebra. Für diese gilt:

Lemma 6.1.6
Seien $\mathcal{A} = (A, \Sigma^A)$ eine primale Algebra, $f : A^n \to A$, $g_i : A^{m_i} \to A$ und $l := \max\{n, m_1, \ldots, m_n\}$ für $i \in \{1, \ldots, n\}$.

1. *Dann existieren $t_f, t_{g_i} \in \mathcal{T}(\Sigma, X)$ für $X := \{x_1, \ldots, x_l\}$ mit $Var(t_f) = \{x_1, \ldots, x_n\}$, $Var(t_{g_i}) = \{x_1, \ldots, x_{m_i}\}$ und*

$$t_f^{\mathcal{A}} = f, t_{g_i}^{\mathcal{A}} = g_i$$

   für $i \in \{1, \ldots, n\}$.

2. *Für $h : A^m \to A$, $h : (a_1, \ldots, a_l) \mapsto f(g_1(a_1, \ldots, m_1), \ldots, g_n(a_1, \ldots, a_{m_n}))$ und $t_h := t_f\{x \mapsto t_{g_1}, \ldots, x_n \mapsto t_{g_n}\}$ gilt*

$$h^{\mathcal{A}} = t_h^{\mathcal{A}}$$

Beweis
einfaches Nachrechnen. □

Daher schreiben wir statt $t_f\{x_1 \mapsto t_{g_1}, \ldots, x_n \mapsto t_{g_n}\}$ suggestiver

$$t_h(x_1, \ldots, x_l) = t_f(t_{g_1}(x_1, \ldots, x_{m_1}), \ldots, t_{g_n}(x_1, \ldots, x_{m_n})).$$

Da in einer primalen Algebra $\mathcal{A}$ jede Funktion als Termfunktion darstellbar ist und jedes Element $a \in \mathcal{A}$ eine konstante Funktion definiert, gibt es zu jedem Element $a \in \mathcal{A}$ einen Term t_a mit $t_a^{\mathcal{A}} = a$. Also gilt:

Lemma 6.1.7 (Erreichbarkeit)
Jedes Element a einer primalen Algebra $\mathcal{A}$ ist erreichbar.

Mit Folgerung 4.2.6 besitzt also jede primale Algebra die Symbolisierbarkeitseigenschaft. Insbesondere ist also Lösbarkeit durch Unifikation zu entscheiden (vgl. Kapitel 4).

Die folgenden Überlegungen zeigen, daß man sogar die Lösbarkeit einer Gleichung (über der Signatur Σ) in einer beliebigen endlichen Σ-Algebra mit Hilfe der Unifikation in primalen Algebren entscheiden kann.

Wie bereits in Kapitel 3 erwähnt, kann man jede endliche Σ-Algebra zu einer Σ'-Algebra erweitern, in der jedes Element erreichbar ist, indem man jedes Element des Universums als nullstelliges Funktionssymbol zur Signatur hinzunimmt und geeignet interpretiert. Fügt man weitere Funktionen hinzu, so kann man sogar jede endliche Algebra zu einer primalen Algebra erweitern:

Definition 6.1.8 (primale Erweiterung)
Für eine Algebra $\mathcal{A} = (A, \Sigma)$ mit $A = \{0, \ldots, q-1\}$ sei $\bar{\mathcal{A}} := (A, \bar{\Sigma})$ definiert durch

$$\bar{\Sigma} := \Sigma \,\dot{\cup}\, \{\underline{0}, \ldots, \underline{q-1}, C_0, \ldots, C_{q-1}, +, *\}$$

mit folgender Interpretation in $\bar{\mathcal{A}}$:

- $\forall i \in A:\ \underline{i}^{\bar{\mathcal{A}}} = i$
- $\forall i \in A, \forall x \in A:\ C_i^{\bar{\mathcal{A}}}(x) = \begin{cases} q-1 & \textit{falls } x = i \\ 0 & \textit{sonst} \end{cases}$
- $\forall (x,y) \in A^2:\ x +^{\bar{\mathcal{A}}} y = \max(x,y)$
- $\forall (x,y) \in A^2:\ x *^{\bar{\mathcal{A}}} y = \min(x,y)$
- $\forall f \in \Sigma$ *sei* $f^{\bar{\mathcal{A}}} = f^{\mathcal{A}}$

$\bar{\mathcal{A}}$ heißt die **primale Erweiterung** *von $\mathcal{A}$.*

Lemma 6.1.9
Sei $\bar{\mathcal{A}}$ die primale Erweiterung einer endlichen Algebra $\mathcal{A}$. Dann ist $\bar{\mathcal{A}}$ primal.

Beweis
Analog zu Beweis von Lemma 6.2.1. □

Satz 6.1.10
Sei $\mathcal{A} = (A, \Sigma^A)$ eine endliche Σ-Algebra und $\bar{\mathcal{A}}$ die primale Erweiterung von $\mathcal{A}$. Für eine Gleichung $s = t$ über der Signatur Σ gilt dann:

$$s = t \textit{ lösbar in } \mathcal{A} \ \Leftrightarrow\ \textit{Es gibt einen } \bar{\mathcal{A}}\textit{-Unifikator für } s = t$$

Beweis
Sei $X := \{x_1, \ldots, x_n\} = Var(s) \cup Var(t)$. $s = t$ ist genau dann lösbar in $\mathcal{A}$, wenn

$$(\mathcal{A}, \alpha) \models s = t$$

für eine Belegung $\alpha : X \to A$.

„$\Rightarrow$": Sei $s = t$ lösbar und $\alpha : X \to A$ erfüllende Belegung, definiert durch $x_i \mapsto a_i$ für $i \in \{1, \ldots, n\}$. Da $\bar{\mathcal{A}}$ primal ist, existieren $t_{a_i} \in \mathcal{T}(\bar{\Sigma}, X)$ mit $t_{a_i}^{\bar{\mathcal{A}}} = a_i$. Definiere $\sigma : \mathcal{T}(\bar{\Sigma}, X) \to \mathcal{T}(\bar{\Sigma}, Y)$ durch $x_i \mapsto t_{a_i}$ für $i \in \{1, \ldots, n\}$. Dann gilt $\bar{\mathcal{A}} \models s\sigma = t\sigma$, so daß σ Unifikator ist.

„$\Leftarrow$": Sei $\sigma : \mathcal{F}_{\bar{\mathcal{A}}}(X) \to \mathcal{F}_{\bar{\mathcal{A}}}(Y)$ ein $\bar{\mathcal{A}}$-Unifikator für $s = t$ mit $Y = \{y_1, \ldots, y_m\} = Var(X\sigma)$ gegeben durch $x_i \mapsto t_i$ für $i \in \{1, \ldots, n\}$. Dann ist auch jede Instanz von σ ein Unifikator von $s = t$. Sei $\lambda : \mathcal{F}_{\bar{\mathcal{A}}}(Y) \to \mathcal{F}_{\bar{\mathcal{A}}}(Z)$ gegeben durch $y_i \mapsto \underline{0}$. Dann gilt für $\sigma\lambda$, daß $x_i\sigma\lambda = s_i$ mit $s_i^{\bar{\mathcal{A}}} \in A$. Dann ist $\alpha : X \to A$ definiert durch $x_i \mapsto s_i^{\bar{\mathcal{A}}}$ offensichtlich eine erfüllende Belegung. □

Wir zeigen nun, daß sich die die Unifikation in einer primalen Algebra sich i.a. nicht direkt auf die Unifikation in einer monoidalen Theorie zurückführen läßt, d.h. die freie Algebra einer primalen Algebra i.a. nicht äquivalent zu der einer monoidalen Theorie ist.

Satz 6.1.11
Sei $\mathcal{A} = (A, \Sigma^A)$ eine primale Algebra mit $|A| \geq 2$, $\mathcal{F}_\mathcal{A}(V)$ freie Algebra zu $\mathcal{A}$. Dann existiert keine *monoidale Theorie $\mathcal{E}$, so daß*

$$\mathcal{F}_\mathcal{A}(V) \sim \mathcal{F}_\mathcal{E}(V)$$

Beweis
OBdA sei $A = \{0, 1, \ldots\} \subseteq \mathbb{N}$. Falls Σ keine idempotente Konstante e enthält, besitzt $\mathfrak{C}_\mathcal{A}$ kein Nullobjekt (vgl. Satz 5.2.2) und kann somit keine semiadditive Kategorie sein. Besitze Σ daher im folgenden eine idempotente Konstante e. OBdA sei $e^\mathcal{A} = 0$. Betrachte die Operation $\alpha : A \to A$ definiert durch $x \mapsto 1$ für alle $x \in A$.

Da $\mathcal{A}$ primal ist, existiert $t_\alpha \in T(\Sigma, X)$ für $X := \{x\}$ mit

$$t_\alpha^\mathcal{A} = \alpha$$

t_α kann jedoch nicht existieren, denn

1. falls $Var(t_\alpha) = \emptyset$ wäre, würde, da e idempotent ist, $t_\alpha =_{\mathcal{F}_\mathcal{A}(X)} e$ und somit $(t_\alpha)^\mathcal{A} = e^\mathcal{A} = 0 \neq 1$ gelten, Widerspruch!

2. falls $Var(t_\alpha) = \{x\}$ wäre, würde $(t_\alpha \circ \{x \mapsto e\})^\mathcal{A} = 1 \neq 0 = e^\mathcal{A}$ und somit $t_\alpha \circ \{x \mapsto e\} \neq_{\mathcal{F}_\mathcal{A}(X)} e$ im Widerspruch zur Idempotenz von e gelten.

□

Mit Lemma 5.3.13 folgt somit, daß man ein Unifikationsproblem über einer primalen Algebra (mit mehr als zwei Elementen) *nicht* in ein lineares Gleichungssystem über einem Halbring übersetzen kann, so daß ein allgemeinster Unifikator genau der Homomorphismus ist, der durch ein Erzeugendensystem des Kerns definiert wird.

Im nächsten Abschnitt überlegen wir uns jedoch, daß man ein Unifikationsproblem über einer primalen Algebra in ein lineares Gleichungssystem über einem Halbring übersetzen kann, so daß ein allgemeinster Unifikator durch ein Erzeugendensystem des Kerns bestimmt werden kann.

6.2 Unifikation in primalen Algebren durch Unifikation in monoidalen Theorien

In diesem Abschnitt soll ein Algorithmus für die Unifikation in primalen Algebren vorgestellt werden, der einen Unifikationsalgorithmus für monoidale Theorien verwendet. Dieser Algorithmus soll einen allgemeinsten Unifikator für ein gegebenes Unifikationsproblem bestimmen. Er basiert auf dem in [Bü90] vorgestellten Verfahren.

Die Überlegungen aus dem letzten Abschnitt zeigen, daß es i.a. nicht möglich ist, das Unifikationsproblem über der primalen Algebra mittels einer Signaturtransformation in ein äquivalentes Problem über einer monoidalen Theorie zu transformieren und hier den Unifikator mit dem gegebenen Algorithmus zu bestimmen. Wir werden daher anders vorgehen:

1. Das gegebene Unifikationsproblem über der primalen Algebra wird zunächst in eine bestimmte syntaktische Form gebracht, in die sog. *Post-Normalform.*

2. Anschließend wird das Unifikationsproblem in ein (nicht äquivalentes) Unifikationsproblem über einer monoidalen Theorie übersetzt. Für dieses wird ein Unifikator mit Hilfe eines gegebenen Algorithmus für monoidale Theorien berechnet.

3. Dieser wird *geeignet modifiziert* und genau dann in einen allgemeinsten Unifikator für das ursprüngliche Unifikationsproblem übersetzt, wenn dieses unifizierbar ist.

Zunächst jedoch einige Vorüberlegungen.

Lemma 6.2.1
Sei $\mathcal{A} = (A, \Sigma^A)$ primale Algebra mit (oBdA) $A = \{0, \ldots, q-1\}$ und sei $\mathcal{A}' = (A, \Sigma'^A)$ mit $\Sigma' = \{\underline{0}, \ldots, \underline{q-1}, C_0, \ldots, C_{q-1}, +, *\}$ mit folgender Interpretation in $\mathcal{A}'$:

- $\forall i \in A : \ \underline{i}^{\mathcal{A}'} = i$
- $\forall i \in A, \forall x \in A : \ C_i^{\mathcal{A}'}(x) = \begin{cases} q-1 & \textit{falls } x = i \\ 0 & \textit{sonst} \end{cases}$
- $\forall (x, y) \in A^2 : \ x +^{\mathcal{A}'} y = \max(x, y)$
- $\forall (x, y) \in A^2 : \ x *^{\mathcal{A}'} y = \min(x, y)$

Dann ist $\mathcal{A}'$ primal.

Beweis
Wir müssen zeigen, daß jede Funktion $f : A^k \to A$ als Termfunktion darstellbar ist. Sei $f : A^k \to A$ gegeben durch

$$\begin{array}{rcl} (0, \ldots, 0) & \mapsto & i_1 \\ (0, \ldots, 1) & \mapsto & i_2 \\ \vdots & \vdots & \vdots \\ (q-1, \ldots, q-1) & \mapsto & i_{q^k} \end{array}$$

Setze $t_f = \underline{i_1} * C_0(x_1) * \cdots * C_0(x_k) + \cdots + \underline{i_{q^k}} * C_{q-1}(x_1) * \cdots * C_{q-1}(x_k)$. Dann ist offensichtlich $t_f^{\mathcal{A}} = f$ („t_f kodiert die Wertetabelle von f“). □

Folgerung 6.2.2
Seien $\mathcal{A}$ und $\mathcal{A}'$ wie im vorigen Lemma. Dann sind $\mathcal{A}$ und $\mathcal{A}'$ äquivalent.

Beweis
Da $\mathcal{A}$ und $\mathcal{A}'$ als primale Algebren über gleichem Universum die gleichen Termfunktionen haben, folgt die Aussage direkt aus Lemma 3.6.5. □

Sei daher im folgenden $\mathcal{A} = (A, \Sigma^A)$ eine primale Σ-Algebra mit

$$\begin{aligned} A &= \{0, \ldots, q-1\} \\ \Sigma &= \{\underline{0}, \ldots, \underline{q-1}, C_0, \ldots, C_{q-1}, +, *\} \end{aligned}$$

mit Σ^A wie in Lemma 6.2.1. Wir schreiben statt $a * b$ kurz ab und setzen (je nach Kontext) $\bot := \underline{0}$ oder $\bot := 0$ und $\top := \underline{q-1}$ oder $\top := q-1$.

6.2.1 Atome

Sei im folgenden Γ ein Unifikationsproblem über der primalen Algebra $\mathcal{A}$ mit $X_{\mathcal{A}} := Var(\Gamma) = \{x_1, \ldots, x_k\}$.

Definition 6.2.3 (Atome, Post-Normalform)

- *Die Menge der Atome von $\mathcal{A}$ bzgl. $X_{\mathcal{A}}$ ist definiert durch*

$$At(\mathcal{A}, X_{\mathcal{A}}) := \{C_{i_1}(x_1) \ldots C_{i_k}(x_k) \ : \ (i_1, \ldots, i_k) \in A^k\}$$

- *Sei $t \in \mathcal{F}_{\mathcal{A}}(X_{\mathcal{A}})$. Zu t definieren wir $\hat{t} \in \mathcal{T}(\Sigma, X_{\mathcal{A}})$ durch*[1]

$$\hat{t} = \sum_{(i_1,\ldots,i_k) \in A^k} \underline{(i_1, \ldots, i_k)t^{\mathcal{A}}} C_{i_1}(x_1) \ldots C_{i_k}(x_k)$$

Dann heißt $\hat{t}$ ***Post-Normalform*** *oder* ***vollständige disjunktive Normalform*** *von t, kurz $\hat{t} := PN(t)$.*

- *Für ein Gleichungssystem Γ ist $PN(\Gamma)$ definiert durch*

$$PN(\Gamma) := \{PN(s) = PN(t) \ : \ s = t \in \Gamma\}$$

Die Post-Normalform eines Terms $t \in \mathcal{F}_{\mathcal{A}}(X_{\mathcal{A}})$, genauer die Post-Normalform einer Kongruenzklasse $t \in \mathcal{F}_{\mathcal{A}}(X_{\mathcal{A}})$, ist ein Vertreter $\hat{t} \in \mathcal{T}(\Sigma, X_{\mathcal{A}})$ von t:

[1] Genaugenommen ist t eine Kongruenzklasse von Termen. Mit t^A ist die induzierte Termfunktion eines beliebigen Vertreters von t gemeint. Da für je zwei Vertreter t_1 und t_2 der Klasse gilt, daß $t_1^A = t_2^A$ ist, ist t^A wohldefiniert.

Lemma 6.2.4
Sei $t \in \mathcal{F}_\mathcal{A}(X_\mathcal{A})$ *und* $\hat{t} := PN(t)$. *Dann gilt:*

$$t =_{\mathcal{F}_\mathcal{A}(X_\mathcal{A})} \hat{t}$$

Beweis
Für alle $(j_1, \ldots, j_k) \in A^k$ gilt

$$\begin{aligned}(j_1, \ldots, j_k)\hat{t}^\mathcal{A} &= \sum_{(i_1,\ldots,i_k)\in A^k} \underline{(i_1, \ldots, i_k)t^\mathcal{A}}^\mathcal{A} C^\mathcal{A}_{i_1}(j_1) \ldots C^\mathcal{A}_{i_k}(j_k) \\ &= (j_1, \ldots, j_k)t^\mathcal{A}\end{aligned}$$

Somit gilt $\hat{t}^\mathcal{A} = t^\mathcal{A}$, und mit Satz 3.3.1 folgt die Behauptung. □

Im folgenden werden wir des öfteren – wie im obigen Beweis – Gleichheit von Termen in $\mathcal{F}_\mathcal{A}(Y_\mathcal{A})$ durch Gleichheit der induzierten Termfunktionen zeigen (vgl. Satz 3.3.1), ohne explizit darauf hinzuweisen.

Wir überlegen uns nun, wie Atome mittles Homomorphismen abgebildet werden:

Lemma 6.2.5
Sei $\sigma : \mathcal{F}_\mathcal{A}(X_\mathcal{A}) \to \mathcal{F}_\mathcal{A}(Y_\mathcal{A})$ *ein Homomorphismus. Dann gilt*

(H1) $(a\sigma)(b\sigma) = \bot$ *für alle* $a, b \in At(\mathcal{A}, X_\mathcal{A})$, $a \neq b$.

(H2) $\sum_{a\in At(\mathcal{A},X_\mathcal{A})} a\sigma = \top$

(H3) $(i_1, \ldots, i_l)(a\sigma)^\mathcal{A} \in \{\bot, \top\}$ *für jedes* $a \in At(\mathcal{A}, X_\mathcal{A})$ *und jede Belegung* $(i_1, \ldots, i_l) \in A^l$, $l := |Y_\mathcal{A}|$.

Beweis
Für jede Belegung $\alpha : X_\mathcal{A} \to \mathcal{A}$ nimmt genau ein Atom aus $At(\mathcal{A}, X_\mathcal{A})$ den Wert $\top$ an. Mit Satz 3.3.1 folgt dann, daß $ab =_{\mathcal{F}_\mathcal{A}(X_\mathcal{A})} \bot$ für unterschiedliche Atome $a, b \in At(\mathcal{A}, X_\mathcal{A})$ und $\sum_{a\in At(\mathcal{A},X_\mathcal{A})} a =_{\mathcal{F}_\mathcal{A}(X_\mathcal{A})} \top$.

(H1) $(a\sigma)(b\sigma) =_{\mathcal{F}_\mathcal{A}(Y_\mathcal{A})} (ab)\sigma =_{\mathcal{F}_\mathcal{A}(Y_\mathcal{A})} \bot\sigma =_{\mathcal{F}_\mathcal{A}(Y_\mathcal{A})} \bot$ für alle $a, b \in At(\mathcal{A}, X_\mathcal{A})$, $a \neq b$.

(H2) $\sum_{a\in At(\mathcal{A},X_\mathcal{A})} a\sigma =_{\mathcal{F}_\mathcal{A}(Y_\mathcal{A})} (\sum_{a\in At(\mathcal{A},X_\mathcal{A})} a)\sigma =_{\mathcal{F}_\mathcal{A}(Y_\mathcal{A})} \top\sigma =_{\mathcal{F}_\mathcal{A}(Y_\mathcal{A})} \top$

(H3) Sei $a \in At(\mathcal{A}, X_\mathcal{A})$, $a = C_{j_1}(x_1) \ldots C_{j_k}(x_k)$ und $(i_1, \ldots, i_l) \in A^l$. Dann ist

$$\begin{aligned}&(i_1, \ldots, i_l)(a\sigma)^\mathcal{A} \\ &= (i_1, \ldots, i_l)((C_{j_1}(x_1) \ldots C_{j_k}(x_k))\sigma)^\mathcal{A} \\ &= (i_1, \ldots, i_l)(C_{j_1}(x_1\sigma) \ldots C_{j_k}(x_k\sigma))^\mathcal{A} \\ &= C^\mathcal{A}_{j_1}((i_1, \ldots, i_l)(x_1\sigma)^\mathcal{A}) \ldots C^\mathcal{A}_{j_k}((i_1, \ldots, i_l)(x_k\sigma)^\mathcal{A})\end{aligned}$$

Da $C^\mathcal{A}_{j_r}(i) \in \{\bot, \top\}$ für alle $r \in \{1, \ldots, k\}$ und $i \in A$ ist die Behauptung klar.

□

(H1) besagt, daß Produkte der Bilder von Atomen konstant $\perp$ sein müssen.

(H2) besagt, daß die Summe der Bilder aller Atome konstant $\top$ sein muß.

(H3) besagt, daß die den Atomen zugeordneten Terme, interpretiert als Termfunktion über $\mathcal{A}$, Funktionen sind, die evaluiert in $\mathcal{A}$ lediglich die Bilder $\top$ und $\perp$ haben.

Gelten andererseits für eine Abbildung der Atome die Bedingungen (H1) – (H3), so definiert diese Abbildung auf eindeutige Weise einen Homomorphismus:

Satz 6.2.6
Seien $X_\mathcal{A} := \{x_1, \ldots, x_k\}$, $\mathcal{A} = (\{0, \ldots, q-1\}, \Sigma^\mathcal{A})$ und $\varphi : At(\mathcal{A}, X_\mathcal{A}) \to \mathcal{F}_\mathcal{A}(Y_\mathcal{A})$ mit

(H1) $(a\varphi)(b\varphi) = \perp$, *für alle* $a, b \in At(\mathcal{A}, X_\mathcal{A})$, $a \neq b$.

(H2) $\sum_{a \in At(\mathcal{A}, X_\mathcal{A})} a\varphi = \top$

(H3) $(i_1, \ldots, i_l)(a\varphi)^\mathcal{A} \in \{\perp, \top\}$ *für jedes* $a \in At(\mathcal{A}, X_\mathcal{A})$ *und jede Belegung* $(i_1, \ldots, i_l) \in A^l$, $l := |Y_\mathcal{A}|$.

Dann gilt für $\sigma : \mathcal{T}(\Sigma, X_\mathcal{A}) \to \mathcal{F}_\mathcal{A}(Y_\mathcal{A})$ definiert durch

$$\sigma : x_j \mapsto \sum_{(i_1, \ldots, i_k) \in A^k} \underline{i_j}(C_{i_1}(x_1) \ldots C_{i_k}(x_k))\varphi$$

für $j \in \{1, \ldots, k\}$, daß

$$a\sigma = a\varphi \qquad \forall a \in At(\mathcal{A}, X_\mathcal{A})$$

Gilt für einen Homomorphismus $\sigma' : \mathcal{T}(\Sigma, X_\mathcal{A}) \to \mathcal{F}_\mathcal{A}(Y_\mathcal{A})$, daß $a\sigma' = a\varphi\ \forall a \in At(\mathcal{A}, X_\mathcal{A})$, so ist $\sigma' = \sigma$, das heißt, die Bilder der Atome bestimmen auf eindeutige Weise einen Homomorphismus.

Beweis
Zunächst überlegen wir uns, daß

$$(i_1, \ldots, i_l)(a\varphi)^\mathcal{A} = \top \Rightarrow (i_1, \ldots, i_l)(b\varphi)^\mathcal{A} = \perp \quad (*)$$

für alle $b \in At(\mathcal{A}, X_\mathcal{A})$, $b \neq a$ und $l := |Var(a\varphi) \cup Var(b\varphi)|$ und ein $(i_1, \ldots, i_l) \in A^l$, das heißt, ist für eine Belegung $(a\varphi)^\mathcal{A} = \top$, so gilt für jedes andere Atom b, daß $(b\varphi)^\mathcal{A} = \perp$ für diese Belegung ist. Denn angenommen, es gäbe $(i_1, \ldots, i_l)$ mit

$$(i_1, \ldots, i_l)(a\varphi)^\mathcal{A} = \top = (i_1, \ldots, i_l)(b\varphi)^\mathcal{A}$$

für ein $b \neq a$, dann gilt nicht

$$(a\varphi)(b\varphi) = \bot$$

im Widerspruch zu (H1). Also muß gelten $(i_1, \ldots, i_l)(b\varphi)^{\mathcal{A}} \neq \top$ und mit (H3) sogar $(i_1, \ldots, i_l)(b\varphi)^{\mathcal{A}} = \bot$.

Betrachten wir nun $C_h(x_j)\sigma = C_h(x_j\sigma)$.

Die folgende Rechnung betrachtet die zu den Termen gehörigen Termfunktionen angewendet auf eine Belegung. Zur Vereinfachung der Schreibweise werden jedoch Terme anstelle der Termfunktionen geschrieben.[2]

$$\begin{aligned} C_h(x_j\sigma) &= C_h\left(\sum_{(i_1,\ldots,i_k)\in A^k} \underline{i_j}(C_{i_1}(x_1)\ldots C_{i_k}(x_k))\varphi\right) \\ &= \begin{cases} \top & \text{falls } \sum_{(i_1,\ldots,i_k)\in A^k} \underline{i_j}(C_{i_1}(x_1)\ldots C_{i_k}(x_k))\varphi = h \\ \bot & \text{sonst} \end{cases} \end{aligned}$$

Wir untersuchen jetzt, wann $\sum_{(i_1,\ldots,i_k)\in A^k} \underline{i_j}(C_{i_1}(x_1)\ldots C_{i_k}(x_k))\varphi = h$ gilt:

$$\begin{aligned} & \sum_{(i_1,\ldots,i_k)\in A^k} \underline{i_j}(C_{i_1}(x_1)\ldots C_{i_k}(x_k))\varphi = h \\ \Leftrightarrow \quad & \sum_{\substack{(i_1,\ldots,i_k)\in A^k \\ i_j \geq h}} \underline{i_j}(C_{i_1}(x_1)\ldots C_{i_k}(x_k))\varphi = h, \end{aligned}$$

da für $i_j < h$ das Produkt $\underline{i_j} \cdot (\ldots) < h$ ist und somit nichts zum Maximum beiträgt.

1. Fall: $h > 0$:

$$\begin{aligned} & \sum_{\substack{(i_1,\ldots,i_k)\in A^k \\ i_j \geq h}} \underline{i_j}(C_{i_1}(x_1)\ldots C_{i_k}(x_k))\varphi = h \\ \Leftrightarrow \quad & \text{a)} \sum_{(i_1,\ldots,i_{j-1},h,i_{j+1},\ldots,i_k)\in A^k} \underline{h}(C_{i_1}(x_1)\ldots C_{i_{j-1}}(x_{j-1})C_h(x_j)C_{i_{j+1}}(x_{j+1})\ldots C_{i_k}(x_k))\varphi = h \\ & \text{und} \\ & \sum_{\substack{(i_1,\ldots,i_k)\in A^k \\ i_j > h}} \underline{i_j}(C_{i_1}(x_1)\ldots C_{i_k}(x_k))\varphi \leq h \\ & \text{oder} \\ & \text{b)} \sum_{(i_1,\ldots,i_{j-1},h,i_{j+1},\ldots,i_k)\in A^k} \underline{h}(C_{i_1}(x_1)\ldots C_{i_{j-1}}(x_{j-1})C_h(x_j)C_{i_{j+1}}(x_{j+1})\ldots C_{i_k}(x_k))\varphi < h \\ & \text{und} \end{aligned}$$

[2] Wir schreiben z.B. $C_h(x_j\sigma)$ anstelle von $(i_1, \ldots, i_l)(C_h(x_1\sigma))^{\mathcal{A}}$.

$$\sum_{\substack{(i_1,\ldots,i_k)\in A^k \\ i_j>h}} \underline{i_j}\, \underbrace{(C_{i_1}(x_1)\ldots C_{i_k}(x_k))\varphi}_{\in\{\top,\bot\}} = h$$

b) ist nicht möglich, da die zweite Bedingung von b) aufgrund von (H3) nicht erfüllbar ist, also

$$\sum_{\substack{(i_1,\ldots,i_k)\in A^k \\ i_j\geq h}} \underline{i_j}(C_{i_1}(x_1)\ldots C_{i_k}(x_k))\varphi = h$$

$$\Leftrightarrow \quad \sum_{(i_1,\ldots,i_{j-1},h,i_{j+1},\ldots,i_k)\in A^k} \underline{h}(C_{i_1}(x_1)\ldots C_{i_{j-1}}(x_{j-1})C_h(x_j)C_{i_{j+1}}(x_{j+1})\ldots C_{i_k}(x_k))\varphi = h$$

und

$$\sum_{\substack{(i_1,\ldots,i_k)\in A^k \\ i_j>h}} \underline{i_j}(C_{i_1}(x_1)\ldots C_{i_k}(x_k))\varphi \leq h$$

$$\overset{\text{(H3)}}{\Leftrightarrow} \quad \sum_{(i_1,\ldots,i_{j-1},h,i_{j+1},\ldots,i_k)\in A^k} (C_{i_1}(x_1)\ldots C_{i_{j-1}}(x_{j-1})C_h(x_j)C_{i_{j+1}}(x_{j+1})\ldots C_{i_k}(x_k))\varphi = \top$$

und

$$\sum_{\substack{(i_1,\ldots,i_k)\in A^k \\ i_j>h}} \underline{i_j}(C_{i_1}(x_1)\ldots C_{i_k}(x_k))\varphi = \bot$$

$$\overset{(*)}{\Leftrightarrow} \quad \sum_{(i_1,\ldots,i_{j-1},h,i_{j+1},\ldots,i_k)\in A^k} (C_{i_1}(x_1)\ldots C_{i_{j-1}}(x_{j-1})C_h(x_j)C_{i_{j+1}}(x_{j+1})\ldots C_{i_k}(x_k))\varphi = \top$$

Beachte bei der letzten Umformung, daß die Aussage von $(*)$ gerade besagt, daß die erste Bedingung die zweite impliziert, so daß diese weggelassen werden kann.

Also gilt für $h > 0$ (in $\mathcal{F}_{\mathcal{A}}(Y_{\mathcal{A}})$)

$$C_h(x_j\sigma) = \sum_{(i_1,\ldots,i_{j-1},h,i_{j+1},\ldots,i_k)\in A^k} (C_{i_1}(x_1)\ldots C_{i_{j-1}}(x_{j-1})C_h(x_j)C_{i_{j+1}}(x_{j+1})\ldots C_{i_k}(x_k))\varphi$$

2. Fall: $h = 0$

$$\sum_{\substack{(i_1,\ldots,i_k)\in A^k \\ i_j\geq 0}} \underline{i_j}(C_{i_1}(x_1)\ldots C_{i_k}(x_k))\varphi = 0$$

$$\Leftrightarrow \quad \text{a)} \quad \sum_{(i_1,\ldots,i_{j-1},0,i_{j+1},\ldots,i_k)\in A^k} (C_{i_1}(x_1)\ldots C_{i_{j-1}}(x_{j-1})C_0(x_j)C_{i_{j+1}}(x_{j+1})\ldots C_{i_k}(x_k))\varphi = \top$$

und

$$\sum_{\substack{(i_1,\ldots,i_k)\in A^k \\ i_j>0}} (C_{i_1}(x_1)\ldots C_{i_k}(x_k))\varphi = \bot$$

oder

$$\text{b)} \quad \sum_{(i_1,\ldots,i_k)\in A^k} (C_{i_1}(x_1)\ldots C_{i_k}(x_k))\varphi = \bot$$

b) ist nach (H2) nicht möglich, also

$$\sum_{\substack{(i_1,\dots,i_k)\in A^k\\ i_j\geq 0}} \underline{i_j}(C_{i_1}(x_1)\dots C_{i_k}(x_k))\varphi = 0$$

$$\Leftrightarrow \sum_{(i_1,\dots,i_{j-1},0,i_{j+1},\dots,i_k)\in A^k} (C_{i_1}(x_1)\dots C_{i_{j-1}}(x_{j-1})C_0(x_j)C_{i_{j+1}}(x_{j+1})\dots C_{i_k}(x_k))\varphi = \top$$

und

$$\sum_{\substack{(i_1,\dots,i_k)\in A^k\\ i_j>0}} (C_{i_1}(x_1)\dots C_{i_k}(x_k))\varphi = \bot$$

$$\overset{(*)}{\Leftrightarrow} \sum_{(i_1,\dots,i_{j-1},0,i_{j+1},\dots,i_k)\in A^k} (C_{i_1}(x_1)\dots C_{i_{j-1}}(x_{j-1})C_0(x_j)C_{i_{j+1}}(x_{j+1})\dots C_{i_k}(x_k))\varphi = \top$$

Also gilt auch für $h = 0$ (in $\mathcal{F}_\mathcal{A}(Y_\mathcal{A})$)

$$C_h(x_j\sigma) = \sum_{(i_1,\dots,i_{j-1},h,i_{j+1},\dots,i_k)\in A^k} (C_{i_1}(x_1)\dots C_{i_{j-1}}(x_{j-1})C_h(x_j)C_{i_{j+1}}(x_{j+1})\dots C_{i_k}(x_k))\varphi$$

Somit gilt für

$$\begin{aligned}
&(C_{h_1}(x_1)\dots C_{h_k}(x_k))\sigma\\
&= C_{h_1}(x_1\sigma)\dots C_{h_k}(x_k\sigma)\\
&= \prod_{h_j\in\{h_1,\dots,h_k\}} \sum_{(i_1,\dots,i_{j-1},h_j,i_{j+1},\dots,i_k)\in A^k} (C_{i_1}(x_1)\dots C_{i_{j-1}}(x_{j-1})C_{h_j}(x_j)C_{i_{j+1}}(x_{j+1})\dots C_{i_k}(x_k))\varphi
\end{aligned}$$

Multipliziert man dieses Produkt aus, so erhält man eine Summe über Glieder der Form

$$(C_{h_1}(x_1)Rest_1)\varphi\cdot(C_{h_2}(x_2)Rest_2)\varphi\cdot\ldots\cdot(C_{h_k}(x_k)Rest_2)\varphi$$

Nach (H1) ist dieses Produkt nur dann ungleich $\bot$, wenn die $C_{h_i}(x_i)Rest_i$ dieselben Atome sind also gleich dem Atom $C_{h_1}(x_1)\dots C_{h_k}(x_k)$ sind. Somit gilt:

$$(C_{h_1}(x_1)\dots C_{h_k}(x_k))\sigma = (C_{h_1}(x_1)\dots C_{h_k}(x_k))\varphi$$

Es ist noch die Eindeutigkeit von σ zu zeigen: Sei $\sigma' : \mathcal{T}(\Sigma, X_\mathcal{A})\to\mathcal{F}_\mathcal{A}(Y_\mathcal{A})$ Homomorphismus mit $a\sigma' = a\varphi$ für alle $a\in At(\mathcal{A}, X_\mathcal{A})$. Dann gilt:

$$\begin{aligned}
x_j\sigma &= \sum_{(i_1,\dots,i_k)\in A^k} \underline{i_j}(C_{i_1}(x_1)\dots C_{i_k}(x_k))\varphi\\
&= \sum_{(i_1,\dots,i_k)\in A^k} \underline{i_j}(C_{i_1}(x_1)\dots C_{i_k}(x_k))\sigma'\\
&= \left(\sum_{(i_1,\dots,i_k)\in A^k} \underline{i_j}C_{i_1}(x_1)\dots C_{i_k}(x_k)\right)\sigma'\\
&= x_j\sigma'
\end{aligned}$$

für alle $j \in \{1, \ldots, k\}$ und somit $\sigma = \sigma'$. □

Folgerung 6.2.7
Eine Substitution $\sigma : \mathcal{F}_\mathcal{A}(X_\mathcal{A}) \to \mathcal{F}_\mathcal{A}(Y_\mathcal{A})$ ist eindeutig durch die Bilder der Atome $a\sigma$ für $a \in At(\mathcal{A}, X_\mathcal{A})$ bestimmt.

6.2.2 q-max-Theorie

Wir betrachten nun die Gleichungstheorie, in die wir unser Unifikationsproblem übersetzen wollen:

Definition 6.2.8 (q-max-Theorie)
Seien $q \in \mathbb{N}$, $\Omega^{(0)} = \{\underline{0}\}, \Omega^{(2)} = \{+\}, \Omega^{(1)} = \{h_0, \ldots, h_{q-1}\}, \Omega = \Omega^{(0)} \cup \Omega^{(2)} \cup \Omega^{(1)}$. Sei $X_\mathcal{E}$ eine Menge von Variablen, $E_q \subseteq T(\Omega, X_\mathcal{E})^2$ enthalte neben den Identitäten, die besagen, daß $+$ kommutativ, assoziativ und 0 neutral für $+$ ist, genau die folgenden:

$$\begin{array}{lrcl}
 & y + y & = & y \\
\forall h \in \Omega^{(1)} & h(\underline{0}) & = & \underline{0} \\
\forall h \in \Omega^{(1)} & h(y_1 + y_2) & = & h(y_1) + h(y_2) \\
 & h_0(y) & = & \underline{0} \\
\forall h_i, h_j \in \Omega^{(1)}, j > 0 & h_i(h_j(y)) & = & h_i(y) \\
\forall h_i, h_j \in \Omega^{(1)} & h_i(y) + h_j(y) & = & h_{\max\{i,j\}}(y)
\end{array}$$

*wobei $y, y_1, y_2 \in X_\mathcal{E}$. Dann heißt $\mathcal{E}_q = \langle E_q \rangle_{\mathsf{SC}}$ **q-max-Theorie**.*

Die q-max-Theorie ist offensichtlich eine monoidale Theorie. Sie ist so konstruiert, daß die Homomorphismensymbole $h_i \in \Omega^{(1)}$ sich wie die Elemente i der primalen Algebra bzgl. $+$ verhalten.

Offensichtlich gibt es in der q-max-Theorie bzgl. einer Variablen y nur die folgenden Äquivalenzklassen von Termen:

$$[\underline{0}], [y], [h_i(y)], [y + h_i(y)] \quad (i \in A \backslash \{0\})$$

Hieraus ergeben sich direkt die Äquivalenzklassen von Termen über beliebiger Variablenmenge. Analog wie bei Termen über primalen Algebren (Post-Normalform) möchten wir besondere Vertreter dieser Klassen auszeichnen:

Definition 6.2.9 (H-Normalform)
Sei $\mathcal{E}_q$ eine q-max-Theorie über der Signatur Ω und der Variablenmenge $X_\mathcal{E}$ mit $\Omega^{(1)} = \{h_0, \ldots, h_{q-1}\}$ und $X_\mathcal{E} = \{y_1, \ldots, y_n\}$. Sei $t \in \mathcal{F}_{\mathcal{E}_q}(X_\mathcal{E})$ gegeben durch

$$t = [\underline{0}] \quad \textit{oder} \quad t = [\sum_{j \in J, i \in I_j} h_j(y_i) + \sum_{r \in R} y_r]$$

für geeignete Indexmengen J, R und -familie $(I)_{j\in J}$ mit $J \cup R \neq \emptyset$ und $I_j \neq \emptyset$ für alle $j \in J$.

Dann definieren wir $\check{} : \mathcal{F}_{\mathcal{E}_q}(X_{\mathcal{E}}) \rightarrow \mathcal{T}(\Omega, X_{\mathcal{E}})$ *durch*

$$\check{t} = \underline{0} \quad bzw. \quad \check{t} = \sum_{j\in J, i\in I_j} h_j(y_i) + \sum_{r\in R} y_r$$

*und nennen $\check{t}$ die **H-Normalform** von t.*

Wir zeigen nun, daß eine q-max-Theorie $\mathcal{E}_q$ unitär ist. Dazu betrachten wir den zu $\mathcal{E}_q$ kanonischen Halbring $\mathcal{S}_{\mathcal{E}_q}$. Zur Wiederholung sei erwähnt, daß der kanonische Halbring einer monoidalen Theorie aus den Endomorphismen der zugehörigen freien Algebra über einer Variablen y besteht. Da die betreffenden Homomorphismen eindeutig durch das Bild t von y bestimmt sind, betrachten wir die Terme t über einer Variablen y. Wie oben bereits erwähnt existieren hier nur die folgenden Äquivalenzklassen von Termen:

$$[\underline{0}], [y], [h_i(y)], [y + h_i(y)] \quad (i \in A\backslash\{0\})$$

Das heißt, die Menge aller Endomorphismen $\tilde{\sigma} \in End\, \mathcal{F}_{\mathcal{E}_q}(\{y\})$ ist die Menge der Homomorphismen, die eindeutig bestimmt sind durch

- $y \mapsto [\underline{0}]$
- $y \mapsto [y]$
- $y \mapsto [h_i(y)] \quad (i \in A\backslash\{0\})$
- $y \mapsto [y + h_i(y)] \quad (i \in A\backslash\{0\})$

Insbesondere ist $|\mathcal{S}_{\mathcal{E}_q}| < \infty$, so daß mit Folgerung 5.3.11 gilt:

Satz 6.2.10
Die q-max-Theorie $\mathcal{E}_q$ ist unitär.

Da bei monoidalen Theorien immer ein Unifikator existiert (ersetze jede Variable durch $\underline{0}$), bedeutet dies, daß bei der q-max-Theorie immer ein allgemeinster Unifikator existiert.

Aus Gründen der Übersichtlichkeit kürzen wir ab:

$$\begin{array}{lllll} 0 & := & y & \mapsto & [\underline{0}] \\ 1 & := & y & \mapsto & [y] \\ h_i & := & y & \mapsto & [h_i(y)] \qquad (i \in A\backslash\{0\}) \\ h_i^y & := & y & \mapsto & [y + h_i(y)] \quad (i \in A\backslash\{0\}) \end{array}$$

Anstelle von 0 verwenden wir auch die Bezeichnung h_0. Schreibt man für die Addition auf $\mathcal{F}_{\mathcal{E}_q}(\{y\})$ + und für die Komposition von Homomorphismen auf $\mathcal{F}_{\mathcal{E}_q}(\{y\})$ $\cdot$, so gelten die folgenden Gleichungen in $\mathcal{S}_q := \mathcal{S}_{\mathcal{E}_q}$, wie man durch leichtes Nachrechnen bestätigt:

Für alle $r \in \mathcal{S}_q$ und $i, j \in \{0, \ldots, q-1\}$ ist

$$\begin{array}{rclcl} r + r & = & r & & \\ 0 + r & = & r + 0 & = & r \\ 1 + h_i & = & h_i + 1 & = & h_i^y \\ h_i + h_j & = & h_{\max(i,j)} & & \\ 0 \cdot r & = & r \cdot 0 & = & 0 \\ r \cdot 1 & = & 1 \cdot r & = & r \\ h_i \cdot h_j & = & \left\{ \begin{array}{ll} 0 & j = 0 \\ h_i & j > 0 \end{array} \right. & & \end{array}$$

6.2.3 $\mathcal{A}/\mathcal{E}$-Transformation

Ähnlich wie bei der Signaturtransformation setzen wir eine primale Algebra $\mathcal{A}$ in Beziehung zu einer q-max-Theorie $\mathcal{E}_q$. Statt jedoch jedem *flachen Term* in $\mathcal{F}_{\mathcal{A}}(X_{\mathcal{A}})$ einen Term in $\mathcal{F}_{\mathcal{E}_q}(X_{\mathcal{E}})$ zuzuordnen, bilden wir ein Atom, genauer ein *Atom mit Vorfaktor*, auf einen Term in $\mathcal{F}_{\mathcal{E}_q}(X_{\mathcal{E}})$ ab:

Definition 6.2.11 (Δ, Δ')
Sei $X_{\mathcal{A}} = \{x_1, \ldots, x_k\}$ und $X_{\mathcal{E}} = \{y_1, \ldots, y_n\}$ mit $n = |\mathcal{A}|^k$.

- $\Delta : \mathcal{F}_{\mathcal{A}}(X_{\mathcal{A}}) \to \mathcal{F}_{\mathcal{E}_q}(X_{\mathcal{E}})$ *wird folgendermaßen definiert: Sei $t \in \mathcal{F}_{\mathcal{A}}(X_{\mathcal{A}})$ und*

$$\hat{t} = \sum_{(i_1,\ldots,i_k) \in A^k} \underline{j_{(i_1,\ldots,i_k)}} C_{i_1}(x_1) \ldots C_{i_k}(x_k)$$

die Post-Normalform von t. Dann ist

$$t\Delta = \sum_{(i_1,\ldots,i_k) \in A^k} h_{j_{(i_1,\ldots,i_k)}}(y_{(i_1,\ldots,i_k)})$$

wobei $y_{(i_1,\ldots,i_k)} := y_i$ mit $i = \sum_{r=1}^{k} i_r q^{k-r} + 1$.

- $\Delta' : \mathcal{F}_{\mathcal{E}_q}(X_{\mathcal{E}}) \to \mathcal{F}_{\mathcal{A}}(X_{\mathcal{A}})$ *wird folgendermaßen definiert: Sei $t' \in \mathcal{F}_{\mathcal{E}_q}(X_{\mathcal{E}})$ und*

$$\check{t}' = \underline{0} \quad \text{oder} \quad \check{t}' = \sum_{j \in J, i \in I_j} h_j(y_i) + \sum_{r \in R} y_r$$

für geeignete Indexmengen J, I_j und R. Dann ist

$$t'\Delta' = \perp$$

bzw.

$$t'\Delta' = \sum_{j\in J, i\in I_j} \underline{j}C_{i_1}(x_1)\dots C_{i_k}(x_k) + \sum_{r\in R} C_{r_1}(x_1)\dots C_{r_k}(x_k)$$

wobei $(i_1,\dots,i_k)$ und $(r_1,\dots,r_k)$ derart seien, daß $i = \sum_{v=1}^k i_v q^{k-v} + 1$ und $r = \sum_{v=1}^k r_v q^{k-v} + 1$.

Das heißt, die Atome $C_{i_1}(x_1)\dots C_{i_k}(x_k)$ werden mittels Δ der Variablen y_i zugeordnet, wobei i dem um 1 erhöhten q-nären Wert von $i_1 \dots i_k$ entspricht. Dann wird die Konstante j vor einem Atom auf den entsprechenden Homomorphismus $h_j(y_i)$ abgebildet. Wir erhalten also mittels Δ nur Terme, deren H-Normalform entweder nur aus der $\underline{0}$ oder aus Summen von Homomorphismen besteht. Δ' macht im wesentlichen das Umgekehrte von Δ. Allerdings wird eine Variable y genau wie auch der Term $h_{q-1}(y)$ auf denselben Term in $\mathcal{F}_\mathcal{A}(X_\mathcal{A})$ abgebildet.

Beachte, daß aufgrund der Definiton von Δ' eine Eigenschaft für alle Term $t'\Delta'$ per Induktionsprinzip nur für alle Terme der Form $\underline{0}, h_j(y_i)$ und y_r gezeigt werden muß.

Lemma 6.2.12

1. *Für $t \in \mathcal{F}_\mathcal{A}(X_\mathcal{A})$ gilt $t\Delta\Delta' =_{\mathcal{F}_\mathcal{A}(X_\mathcal{A})} t$.*
2. *Für $t, s \in \mathcal{F}_\mathcal{A}(X_\mathcal{A})$ mit $t \neq_{\mathcal{F}_\mathcal{A}(X_\mathcal{A})} s$ gilt $t\Delta \neq_{\mathcal{F}_{\mathcal{E}_q}(X_\mathcal{E})} s\Delta$.*

Beweis

zu 1) Sei $\hat{t} = \sum \underline{t_i} C_{i_1}(x_1)\cdots C_{i_k}(x_k)$ mit $i = \sum_{v=1}^k i_v q^{k-v} + 1$. Dann ist $t\Delta = [\sum h_{t_i}(y_i)]$. $t\check{\Delta} = \underline{0} \Leftrightarrow \forall i\ t_i = 0 \Leftrightarrow t = \perp$. Somit folgt aus $t = \perp$ insbesondere $t\Delta\Delta' = \perp$. Gilt andererseits $t \neq \perp$, so ist $t\check{\Delta} = \sum h_{t_i}(y_i)$ und somit $t\Delta\Delta' = \sum \underline{t_i} C_{i_1}(x_1)\cdots C_{i_k}(x_k)$.

zu 2) Sei $\hat{t} = \sum \underline{t_i} C_{i_1}(x_1)\cdots C_{i_k}(x_k)$ und $\hat{s} = \sum \underline{s_i} C_{i_1}(x_1)\cdots C_{i_k}(x_k)$. Aufgrund von $s \neq_{\mathcal{F}_\mathcal{A}(X_\mathcal{A})} t$ gibt es ein $j \in \{1,\dots,q^k\}$ mit $t_j \neq s_j$, also $h_{t_j}(y_j) \neq_{\mathcal{F}_{\mathcal{E}_q}(X_\mathcal{E})} h_{s_j}(y_j)$. Somit ist $t\Delta = [\sum_i h_{t_i}(y_i)] \neq_{\mathcal{F}_{\mathcal{E}_q}(X_\mathcal{E})} [\sum_i h_{s_i}(y_i)] = s\Delta$.

□

Analog können wir einer Substitution $\sigma : \mathcal{F}_\mathcal{A}(X_\mathcal{A}) \to \mathcal{F}_\mathcal{A}(Y_\mathcal{A})$ eine Substitution $\sigma' : \mathcal{F}_{\mathcal{E}_q}(X_\mathcal{E}) \to \mathcal{F}_{\mathcal{E}_q}(Y_\mathcal{E})$ mittels einer Abbildung, die wir ebenfalls Δ nennen, zuordnen.

Definition 6.2.13 (Δ)
Seien $X_{\mathcal{A}}, Y_{\mathcal{A}}, X_{\mathcal{E}}, Y_{\mathcal{E}}$ Variablenmengen mit $|X_{\mathcal{E}}| = |A|^{|X_{\mathcal{A}}|}$ und $|Y_{\mathcal{E}}| = |A|^{|Y_{\mathcal{A}}|}$. $\Delta : Subs(\mathcal{F}_{\mathcal{A}}(X_{\mathcal{A}}), \mathcal{F}_{\mathcal{A}}(Y_{\mathcal{A}})) \rightarrow Subs(\mathcal{F}_{\mathcal{E}_q}(X_{\mathcal{E}}), \mathcal{F}_{\mathcal{E}_q}(Y_{\mathcal{E}}))$ wird folgendermaßen definiert: Sei $|X_{\mathcal{A}}| = k$ und $\sigma \in Subs(\mathcal{F}_{\mathcal{A}}(X_{\mathcal{A}}), \mathcal{F}_{\mathcal{A}}(Y_{\mathcal{A}}))$ definiert durch

$$x_j \mapsto t_j \quad (j \in \{1, \ldots, k\}).$$

Dann ist $\sigma\Delta$ definiert durch

$$y_i \mapsto s_i\Delta \quad (y_i \in X_{\mathcal{E}} = \{y_1, \ldots, y_{|A|^k}\}),$$

wobei $s_i = C_{i_1}(t_1) \ldots C_{i_k}(t_k) = (C_{i_1}(x_1) \ldots C_{i_k}(x_k))\sigma$ und $(i_1, \ldots, i_k)$ die q-näre Darstellung von $i - 1$ bezeichne.

Δ ist also folgendermaßen definiert:

Lemma 6.2.14
Für $t' \in \mathcal{F}_{\mathcal{E}_q}(X_{\mathcal{E}})$ und $\sigma : \mathcal{F}_{\mathcal{A}}(X_{\mathcal{A}}) \rightarrow \mathcal{F}_{\mathcal{A}}(Y_{\mathcal{A}})$ gilt

$$t'(\sigma\Delta) =_{\mathcal{F}_{\mathcal{E}_q}(Y_{\mathcal{E}})} ((t'\Delta')\sigma)\Delta$$

Beweis
Für $y_i \in X_{\mathcal{E}}$ gilt

$$\begin{aligned} y_i(\sigma\Delta) &\stackrel{\text{Def}}{=} ((C_{i_1}(x_1) \ldots C_{i_k}(x_k))\sigma)\Delta \\ &= ((y_i\Delta')\sigma)\Delta \end{aligned}$$

Per Induktion folgt die Behauptung. □

Somit erhalten wir:

Lemma 6.2.15
Seien $\sigma : \mathcal{F}_{\mathcal{A}}(X_{\mathcal{A}}) \rightarrow \mathcal{F}_{\mathcal{A}}(Y_{\mathcal{A}})$ und $\lambda : \mathcal{F}_{\mathcal{A}}(Y_{\mathcal{A}}) \rightarrow \mathcal{F}_{\mathcal{A}}(Z_{\mathcal{A}})$ Substitutionen.

1. *Für alle $t \in \mathcal{F}_{\mathcal{A}}(X_{\mathcal{A}})$ gilt $(t\sigma)\Delta = (t\Delta)(\sigma\Delta)$.*
2. *$(\sigma\lambda)\Delta = (\sigma\Delta)(\lambda\Delta)$.*

Beweis
zu 1) Für alle $t \in \mathcal{F}_{\mathcal{A}}(X_{\mathcal{A}})$ gilt

$$\begin{aligned} (t\Delta)(\sigma\Delta) &\stackrel{6.2.14}{=} (((t\Delta)\Delta')\sigma)\Delta \\ &\stackrel{6.2.12}{=} (t\sigma)\Delta \end{aligned}$$

zu 2) Für alle $y_i \in X_{\mathcal{E}} = \{y_1, \ldots, y_{|At(\mathcal{A}, X_{\mathcal{A}})|}\}$ gilt:

$$\begin{aligned} y_i((\sigma\lambda)\Delta) &\overset{6.2.14}{=} ((y_i\Delta')(\sigma\lambda))\Delta \\ &= (((y_i\Delta')\sigma)\lambda)\Delta \\ &\overset{1.}{=} (((y_i\Delta')\sigma)\Delta)(\lambda\Delta) \\ &\overset{6.2.14}{=} (y_i(\sigma\Delta))(\lambda\Delta) \end{aligned}$$

Somit gilt $(\sigma\lambda)\Delta = (\sigma\Delta)(\lambda\Delta)$. □

Ziel ist es nun, eine Abbildung Δ' zu definieren, die einer Substitution $\sigma : \mathcal{F}_{\mathcal{E}_q}(X_{\mathcal{E}}) \rightarrow \mathcal{F}_{\mathcal{E}_q}(Y_{\mathcal{E}})$ eine Substitution $\sigma : \mathcal{F}_{\mathcal{A}}(X_{\mathcal{A}}) \rightarrow \mathcal{F}_{\mathcal{A}}(Y_{\mathcal{A}})$ zuordnet.

Definition 6.2.16 (Λ)
Seien $X_{\mathcal{A}}, Y_{\mathcal{A}}, X_{\mathcal{E}}, Y_{\mathcal{E}}$ Variablenmengen mit $|X_{\mathcal{E}}| = |A|^{|X_{\mathcal{A}}|}$ und $|Y_{\mathcal{E}}| = |A|^{|Y_{\mathcal{A}}|}$. Betrachte die Abbildung

$$\Lambda : Subs(\mathcal{F}_{\mathcal{E}_q}(X_{\mathcal{E}}), \mathcal{F}_{\mathcal{E}_q}(Y_{\mathcal{E}})) \rightarrow \{\varphi : At(\mathcal{A}, X_{\mathcal{A}}) \rightarrow \mathcal{F}_{\mathcal{A}}(Y_{\mathcal{A}})\},$$

die wie folgt definiert wird. Sei $|X_{\mathcal{E}}| = n$ und $\sigma \in Subs(\mathcal{F}_{\mathcal{E}_q}(X_{\mathcal{E}}), \mathcal{F}_{\mathcal{E}_q}(Y_{\mathcal{E}}))$ definiert durch

$$y_i \mapsto t_i \quad (i \in \{1, \ldots, n\})$$

Dann wird $\varphi = \sigma\Lambda$ definiert durch

$$y_i\Delta' \mapsto t_i\Delta' = (y_i\sigma)\Delta'$$

Beachte, daß $t_i\Delta'$ wohldefiniert ist, da $|Y_{\mathcal{E}}| = |A|^{|Y_{\mathcal{A}}|}$ vorausgesetzt wurde.

$\varphi = \sigma\Lambda$ ist also auf $At(\mathcal{A}, X_{\mathcal{A}})$ definiert. Falls φ die Eigenschaften (H1) – (H3) erfüllt, läßt sich φ gemäß Satz 6.2.6 zu einem Homomorphismus auf $\mathcal{F}_{\mathcal{A}}(X_{\mathcal{A}})$ fortsetzen. Da wir einer Substitution $\sigma : \mathcal{F}_{\mathcal{E}_q}(X_{\mathcal{E}}) \rightarrow \mathcal{F}_{\mathcal{E}_q}(Y_{\mathcal{E}})$ eine Substitution zuordnen wollen, untersuchen wir daher zunächst, unter welchen Voraussetzungen $\sigma\Lambda$ die Voraussetzungen (H1) – (H3) erfüllt.

Definition 6.2.17 (variablenreduziert, variablenexpandiert)
*Sei eine Substitution $\sigma : \mathcal{F}_{\mathcal{E}_q}(X_{\mathcal{E}}) \rightarrow \mathcal{F}_{\mathcal{E}_q}(Y_{\mathcal{E}})$ gegeben. Dann heißt σ **variablenreduziert** falls*

$$D := \bigcup_{\substack{y_i, y_j \in X_{\mathcal{E}} \\ y_i \neq y_j}} (Var(y_i\sigma) \cap Var(y_j\sigma)) = \emptyset$$

und

$$H := \{y : \exists y_i \in X_{\mathcal{E}} \exists h_j \in \Omega^{(1)} \text{ mit } \check{y_i}\sigma = \cdots + h_j(y) + \cdots\} = \emptyset$$

*gilt. Ist $Var(X_{\mathcal{E}}\sigma) = Y_{\mathcal{E}}$, so heißt σ **variablenexpandiert**.*

Eine Substitution heißt also variablenreduziert, falls in den Bildern der Variablen aus $X_\mathcal{E}$, genauer in der H-Normalform der Bilder aller Variablen, keine gleichen Variablen (aus $Y_\mathcal{E}$) und keine Homomorphismen vorkommen.[3] Somit gilt:

Bemerkung 6.2.18
Sei $\sigma : \mathcal{F}_{\mathcal{E}_q}(X_\mathcal{E}) \to \mathcal{F}_{\mathcal{E}_q}(Y_\mathcal{E})$ eine variablenreduzierte Substitution. Setzen wir $\sum_{r\in\emptyset} y_r := \underline{0}$, so gilt

$$y_i\sigma = \sum_{r\in R_i} y_r$$

für geeignete, paarweise verschiedene Indexmengen R_i, $i \in \{1,\ldots,|X_\mathcal{E}|\}$.

Lemma 6.2.19
Seien $X_\mathcal{A}, Y_\mathcal{A}, X_\mathcal{E}, Y_\mathcal{E}$ Variablenmengen mit[4] $|X_\mathcal{E}| = |A|^{|X_\mathcal{A}|}$ und $|Y_\mathcal{E}| = |A|^{|Y_\mathcal{A}|}$ und eine Substitution $\sigma : \mathcal{F}_{\mathcal{E}_q}(X_\mathcal{E}) \to \mathcal{F}_{\mathcal{E}_q}(Y_\mathcal{E})$ gegeben. Ist σ variablenreduziert und variablenexpandiert, so erfüllt $\sigma\Lambda$ die Bedingungen (H1) – (H3).

Beweis
Da $|X_\mathcal{E}| = |A|^{|X_\mathcal{A}|}$ und $|Y_\mathcal{E}| = |A|^{|Y_\mathcal{A}|}$ gilt $X_\mathcal{E}\Delta' = At(\mathcal{A}, X_\mathcal{A})$ bzw. $Y_\mathcal{E}\Delta' = At(\mathcal{A}, Y_\mathcal{A})$ und $\Delta'|_{X_\mathcal{E}}$ ist eine Bijektion.

Es ist zu zeigen:

(H1) $(a\sigma)(b\sigma) = \bot$ für alle $a, b \in At(\mathcal{A}, X_\mathcal{A})$, $a \neq b$.

(H2) $\sum_{a\in At(\mathcal{A},X_\mathcal{A})} a\sigma = \top$

(H3) $(i_1,\ldots,i_l)(a\sigma)^\mathcal{A} \in \{\bot, \top\}$ für jedes $a \in At(\mathcal{A}, X_\mathcal{A})$ und jede Belegung $(i_1,\ldots,i_l) \in A^l$, $l := |Y_\mathcal{A}|$.

Sei für $i \in \{1,\ldots,|X_\mathcal{E}|\}$ und geeigneter Indexfamilie $(R_i)_{i\in\{1,\ldots,|X_\mathcal{E}|\}}$ σ gegeben durch $y_i\sigma = \sum_{r\in R_i} y_r$.

Dann ist $(\sum_{r\in R_i} y_r)\Delta' = \sum_{r\in R_i} C_{r_1}(x_1)\ldots C_{r_l}(x_l)$, wobei $(r_1,\ldots r_l)$ die q-näre Darstellung von $r-1$ bezeichne und $l = |Y_\mathcal{A}|$ sei.

Das heißt, die Bilder von $(y_i\sigma)\Delta'$ sind Summen von paarweise verschiedenen Atomen. Somit ist $a(\sigma\Lambda) = (y_i\Delta')(\sigma\Lambda) = (y_i\sigma)\Delta'$ eine Summe von paarweise verschiedenen Atomen. Daher gelten offensichtlich (H1) und (H3). Da σ variablenexpandiert ist, gilt $Var(X_\mathcal{E}\sigma) = Y_\mathcal{E}$, so daß alle Atome als Summanden im Bild von $X_\mathcal{A}(\sigma\Lambda)$ vorkommen. Somit gilt (H3). □

[3] Wir werden im folgenden – wie hier – einfachheitshalber von syntaktischen Eigenschaften eines Terms aus $\mathcal{F}_{\mathcal{E}_q}(X_\mathcal{E})$ sprechen, obwohl natürlich genauer von syntaktischen Eigenschaften des entsprechenden Terms in H-Normalform $\check{t}$ die Rede ist.

[4] Beachte, daß hierdurch implizit $|Y_\mathcal{E}| > 0$ vorausgesetzt wird.

Da für eine Variable $y\Delta' =_{\mathcal{F}_\mathcal{A}(X_\mathcal{A})} h_\top(y)\Delta'$ ist, gilt andererseits auch für Homomorphismen $\sigma : \mathcal{F}_{\mathcal{E}_q}(X_\mathcal{E}) \to \mathcal{F}_{\mathcal{E}_q}(Y_\mathcal{E})$, wo die Bilder von Variablen aus Summen von $h_\top(y)$ bestehen, daß diese die Bedingungen (H1) – (H3) erfüllen. Genauer:

Sei $\sigma_0 : \mathcal{F}_{\mathcal{E}_q}(X_\mathcal{E}) \to \mathcal{F}_{\mathcal{E}_q}(Y_\mathcal{E})$ eine variablenreduzierte und -expandierte Substitution, dann erfüllt $\sigma : \mathcal{F}_{\mathcal{E}_q}(X_\mathcal{E}) \to \mathcal{F}_{\mathcal{E}_q}(Y_\mathcal{E})$ für $\sigma = \sigma_0\lambda$ mit $\lambda : \mathcal{F}_{\mathcal{E}_q}(Y_\mathcal{E}) \to \mathcal{F}_{\mathcal{E}_q}(Y_\mathcal{E})$ definiert durch $y \mapsto h_\top(y)$ die Bedingungen (H1) – (H3). Wir nennen ein derartiges σ **Atom-Substitution**.

Wir definieren daher:

Definition 6.2.20 (Δ')
Seien $X_\mathcal{A}, Y_\mathcal{A}, X_\mathcal{E}, Y_\mathcal{E}$ Variablenmengen mit $|X_\mathcal{E}| = |A|^{|X_\mathcal{A}|}$ und $|Y_\mathcal{E}| = |A|^{|Y_\mathcal{A}|}$. Dann ist $S_{REA}(\mathcal{F}_{\mathcal{E}_q}(X_\mathcal{E}), \mathcal{F}_{\mathcal{E}_q}(Y_\mathcal{E})) \subseteq Subs(\mathcal{F}_{\mathcal{E}_q}(X_\mathcal{E}), \mathcal{F}_{\mathcal{E}_q}(Y_\mathcal{E}))$ die Menge aller variablenreduzierten und variablenexpandierten Substitutionen vereinigt mit allen Atom-Substitutionen von $\mathcal{F}_{\mathcal{E}_q}(X_\mathcal{E})$ nach $\mathcal{F}_{\mathcal{E}_q}(Y_\mathcal{E})$. Man beachte, daß die Menge $S_{REA}(\mathcal{F}_{\mathcal{E}_q}(X_\mathcal{E}), \mathcal{F}_{\mathcal{E}_q}(Y_\mathcal{E}))$ nur für nicht leeres $Y_\mathcal{E}$ definiert ist. Wir definieren weiterhin

$$\Delta' : S_{REA}(\mathcal{F}_{\mathcal{E}_q}(X_\mathcal{E}), \mathcal{F}_{\mathcal{E}_q}(Y_\mathcal{E})) \to Subs(\mathcal{F}_\mathcal{A}(X_\mathcal{A}), \mathcal{F}_\mathcal{A}(Y_\mathcal{A}))$$

folgendermaßen: Sei $\sigma \in S_{REA}(\mathcal{F}_{\mathcal{E}_q}(X_\mathcal{E}), \mathcal{F}_{\mathcal{E}_q}(Y_\mathcal{E}))$ gegeben und φ_σ die durch $\sigma\Lambda$ gemäß Satz 6.2.6 eindeutig bestimmte Substitution mit $\sigma\Lambda = \varphi_\sigma|_{At(\mathcal{A},X_\mathcal{A})}$. Dann sei

$$\sigma\Delta' = \varphi_\sigma.$$

Seien im folgenden $X_\mathcal{A}, Y_\mathcal{A}, Z_\mathcal{A}, X_\mathcal{E}, Y_\mathcal{E}, Z_\mathcal{E}$ Variablenmengen mit $|X_\mathcal{E}| = |A|^{|X_\mathcal{A}|}$, $|Y_\mathcal{E}| = |A|^{|Y_\mathcal{A}|}$ und $|Z_\mathcal{E}| = |A|^{|Z_\mathcal{A}|}$.

Lemma 6.2.21
Für alle $t \in \mathcal{F}_{\mathcal{E}_q}(X_\mathcal{E})$ und alle $\sigma' \in S_{REA}(\mathcal{F}_{\mathcal{E}_q}(X_\mathcal{E}), \mathcal{F}_{\mathcal{E}_q}(Y_\mathcal{E}))$ gilt

$$(t\sigma')\Delta' = (t\Delta')(\sigma'\Delta')$$

Beweis
Zunächst zeigen wir, daß

1. $(\underline{0}\Delta')(\sigma'\Delta') = (\underline{0}\sigma')\Delta'$
2. $(y_i\Delta')(\sigma'\Delta') = (y_i\sigma')\Delta'$ und
3. $(h_j(y_i)\Delta')(\sigma'\Delta') = (h_j(y_i)\sigma')\Delta'$ gilt.

$(\underline{0}\Delta')(\sigma'\Delta') = \bot(\sigma'\Delta') = \bot = \underline{0}\Delta' = \underline{0}\sigma'\Delta'$. Somit gilt 1. Per Definition gilt 2. Die Gültigkeit von 3. sieht man folgendermaßen ein:

$$\begin{aligned}
((h_j(y_i))\Delta')(\sigma'\Delta') &= (\underline{j}a_i)(\sigma'\Delta') \quad \text{für ein } a_i \in At(\mathcal{A}, X_{\mathcal{A}}) \\
&= \underline{j}(a_i(\sigma'\Delta')) \\
&= \underline{j}((y_i\Delta')(\sigma'\Delta')) \\
&\stackrel{1.}{=} \underline{j}((y_i\sigma')\Delta') \\
&\stackrel{(*)}{=} h_j(y_i\sigma')\Delta' \\
&= (h_j(y_i)\sigma')\Delta'
\end{aligned}$$

Dabei besagt $(*)$, daß $\underline{j}(y_i\Delta') = \underline{j}(h_\top(y_i)\Delta') = h_j(y_i)\Delta'$. Per Induktionsprinzip folgt nun die Behauptung für beliebige Terme $t' \in \mathcal{F}_{\mathcal{E}_q}(X_{\mathcal{E}})$. □

Lemma 6.2.22

Sei $\sigma : \mathcal{F}_{\mathcal{A}}(X_{\mathcal{A}}) \rightarrow \mathcal{F}_{\mathcal{A}}(Y_{\mathcal{A}})$ gegeben. Dann ist $(\sigma\Delta)\Delta'$ definiert und es gilt

$$(\sigma\Delta)\Delta' = \sigma$$

Beweis

Sei $t \in \mathcal{F}_{\mathcal{A}}(X_{\mathcal{A}})$ beliebig. Dann ist

$$\begin{aligned}
t((\sigma\Delta)\Delta') &\stackrel{6.2.12}{=} ((t\Delta)\Delta')((\sigma\Delta)\Delta') \\
&\stackrel{6.2.21}{=} ((t\Delta)(\sigma\Delta))\Delta' \\
&\stackrel{6.2.15}{=} ((t\sigma)\Delta)\Delta' \\
&\stackrel{6.2.12}{=} t\sigma
\end{aligned}$$

□

Lemma 6.2.23

Seien $\sigma \in S_{REA}(\mathcal{F}_{\mathcal{E}_q}(X_{\mathcal{E}}), \mathcal{F}_{\mathcal{E}_q}(Y_{\mathcal{E}}))$ und $\lambda \in S_{REA}(\mathcal{F}_{\mathcal{E}_q}(Y_{\mathcal{E}}), \mathcal{F}_{\mathcal{E}_q}(Z_{\mathcal{E}}))$ gegeben. Dann ist $(\sigma\lambda)\Delta'$ definiert und es gilt

$$(\sigma\lambda)\Delta' = (\sigma\Delta')(\lambda\Delta')$$

Beweis

Man rechnet leicht nach, daß die Komposition

- zweier variablenreduzierter und variablenexpandierter Substitutionen wieder eine variablenreduzierte und -expandierte Abbildung ergibt.
- einer variablenreduzierten und -expandierten Substitution mit einer Atom-Substitution eine Atom-Substitution ergibt.

Daher ist $(\sigma\lambda)\Delta'$ wohldefiniert.

Dann ist

$$\begin{array}{rcl} t((\sigma\lambda)\Delta') & \stackrel{6.2.12}{=} & ((t\Delta)\Delta')((\sigma\lambda)\Delta') \\ & \stackrel{6.2.21}{=} & ((t\Delta)(\sigma\lambda))\Delta' \\ & = & (((t\Delta)\sigma)\lambda)\Delta' \\ & \stackrel{6.2.21}{=} & (((t\Delta)\sigma)\Delta')(\lambda\Delta') \\ & \stackrel{6.2.21}{=} & (((t\Delta)\Delta')(\sigma\Delta'))(\lambda\Delta') \\ & = & (t(\sigma\Delta'))(\lambda\Delta') \\ & = & t((\sigma\Delta')(\lambda\Delta')) \end{array}$$

□

6.2.4 Unifikation in primalen Algebren durch Unifikation in der q-max-Theorie

Wir beschreiben nun, wie man mit Hilfe der Unifikation in einer monoidalen q-max-Theorie einen allgemeinsten Unifikator, sofern existent, bestimmen kann. Seien im folgenden $X_{\mathcal{A}}, X_{\mathcal{E}}$ Variablenmengen mit $|X_{\mathcal{E}}| = |A|^{|X_{\mathcal{A}}|}$. und Γ ein Unifikationsproblem über einer primalen Algebra $\mathcal{A}$ gegeben.

Der erste Schritt unseres Algorithmus besteht darin, das gegebene Problem Γ in ein Problem der q-max-Theorie zu übersetzen. Dazu bedienen wir uns der Abbildung Δ.

Definition 6.2.24
$\tilde{\Gamma} := \Gamma\Delta = \{(s\Delta, t\Delta) : (s,t) \in \Gamma\}$ *heißt das **zu Γ gehörige** Unifikationsproblem in der q-max-Theorie.*

Beispiel 6.2.25
Seien $\mathcal{A} = (A, \Sigma^A)$, $A = \{0,1,2\}$, $\Sigma = \{+, *, \underline{0}, \underline{1}, \underline{2}, C_0, C_1, C_2\}$ mit gewohnter Interpretation und $X_{\mathcal{A}} := \{x_1, x_2\}$, $q := |A| = 3$.

Beachte, daß Δ mittels der Post-Normalform der Terme in Γ definiert ist.

1. Seien $s_1 := 2C_0(x_1) + 2C_1(x_1) + 2C_2(x_1)C_0(x_2)$, $t_1 := 1C_0(x_1)C_0(x_2)$ und $\Gamma_1 := \{(s_1, t_1)\}$. Dann ist

$$\begin{array}{rcl} \hat{s}_1 & := & PN(s_1) \\ & = & 2C_0(x_1)C_0(x_2) + 2C_0(x_1)C_1(x_2) + 2C_0(x_1)C_2(x_2)+ \\ & & 2C_1(x_1)C_0(x_2) + 2C_1(x_1)C_1(x_2) + 2C_1(x_1)C_2(x_2)+ \\ & & 2C_2(x_1)C_0(x_2) + 0C_2(x_1)C_1(x_2) + 0C_2(x_1)C_2(x_2) \\ \hat{t}_1 & := & PN(t_1) \\ & = & 1C_0(x_1)C_0(x_2) + 0C_0(x_1)C_1(x_2) + 0C_0(x_1)C_2(x_2)+ \\ & & 0C_1(x_1)C_0(x_2) + 0C_1(x_1)C_1(x_2) + 0C_1(x_1)C_2(x_2)+ \\ & & 0C_2(x_1)C_0(x_2) + 0C_2(x_1)C_1(x_2) + 0C_2(x_1)C_2(x_2) \end{array}$$

und somit $\hat{\Gamma} := PN(\Gamma) = \{(\hat{s}_1, \hat{t}_1)\}$.

2. Seien

$$\begin{aligned} s_2 &:= 1C_0(x_1)C_0(x_2) \\ t_2 &:= 0C_0(x_1)C_0(x_2) + 1C_0(x_1)C_1(x_2) + 2C_0(x_1)C_2(x_2) + \\ & 2C_1(x_1)C_0(x_2) + 2C_1(x_1)C_1(x_2) + 2C_1(x_1)C_2(x_2) + \\ & 2C_2(x_1)C_0(x_2) + 2C_2(x_1)C_1(x_2) + 2C_2(x_1)C_2(x_2) \end{aligned}$$

$\Gamma_2 := \{(s_2, t_2)\}$. Dann ist

$$\begin{aligned} \hat{s}_2 &:= PN(s_2) \\ &= 1C_0(x_1)C_0(x_2) + 0C_0(x_1)C_1(x_2) + 0C_0(x_1)C_2(x_2) + \\ & 0C_1(x_1)C_0(x_2) + 0C_1(x_1)C_1(x_2) + 0C_1(x_1)C_2(x_2) + \\ & 0C_2(x_1)C_0(x_2) + 0C_2(x_1)C_1(x_2) + 0C_2(x_1)C_2(x_2) \\ \hat{t}_2 &:= PN(t_2) \\ &= 0C_0(x_1)C_0(x_2) + 1C_0(x_1)C_1(x_2) + 2C_0(x_1)C_2(x_2) + \\ & 2C_1(x_1)C_0(x_2) + 2C_1(x_1)C_1(x_2) + 2C_1(x_1)C_2(x_2) + \\ & 2C_2(x_1)C_0(x_2) + 2C_2(x_1)C_1(x_2) + 2C_2(x_1)C_2(x_2) \end{aligned}$$

und somit $\hat{\Gamma}_1 := PN(\Gamma_1) = \{(\hat{s}_2, \hat{t}_2)\}$.

Da für die Belegung $\alpha : X_{\mathcal{A}} \to \mathcal{A}$ definiert durch $x_1 \mapsto 2$, $x_2 \mapsto 1$ gilt, daß $s_1\alpha = t_1\alpha$, existiert mit der Bemerkung nach 6.1.7 ein Unifikator für das erste Beispiel.

Da sich im zweiten Beispiel die Koeffizienten der sich entsprechenden Atome von $\hat{s}_2$ und $\hat{t}_2$ unterscheiden und bei einer Auswertung genau ein Atom den Wert $\top$ annehmen muß, existiert keine Belegung α mit $\hat{s}_2\alpha = \hat{t}_2\alpha$, so daß mit der Bemerkung nach Lemma 6.1.7 kein Unifikator für das zweite Beispiel existieren kann.

Betrachten wir nun die Umwandlung in die entsprechende q-max-Theorie.

Wegen $q = |A| = 3$ und $k = |X_{\mathcal{A}}| = 2$ setzen wir $X_{\mathcal{E}} := \{y_1, \ldots, y_9\}$. Dann gilt

1. für das erste Beispiel

$$\begin{aligned} \tilde{s}_1 = s_1\Delta &:= h_2(y_1) + h_2(y_2) + h_2(y_3) + \\ & h_2(y_4) + h_2(y_5) + h_2(y_6) + \\ & h_2(y_7) + h_0(y_8) + h_0(y_9) \\ \tilde{t}_1 = t_1\Delta &:= h_1(y_1) + h_0(y_2) + h_0(y_3) + \\ & h_0(y_4) + h_0(y_5) + h_0(y_6) + \\ & h_0(y_7) + h_0(y_8) + h_0(y_9) \end{aligned}$$

und $\tilde{\Gamma} = \{\tilde{s}_1, \tilde{t}_1\}$.

2. für das zweite Beispiel

$$\begin{aligned}\tilde{s}_2 = s_2\Delta \quad &:= \quad h_1(y_1) + h_0(y_2) + h_0(y_3) + \\ & \quad\;\; h_0(y_4) + h_0(y_5) + h_0(y_6) + \\ & \quad\;\; h_0(y_7) + h_0(y_8) + h_0(y_9) \\ \tilde{t}_2 = t_2\Delta \quad &:= \quad h_0(y_1) + h_1(y_2) + h_2(y_3) + \\ & \quad\;\; h_2(y_4) + h_2(y_5) + h_2(y_6) + \\ & \quad\;\; h_2(y_7) + h_2(y_8) + h_2(y_9)\end{aligned}$$

und $\tilde{\Gamma} = \{\tilde{s}_2, \tilde{t}_2\}$.

Für das Unifikationsproblem $\tilde{\Gamma} = \Gamma\Delta$ wird nun ein allgemeinster Unifikator bestimmt. Beachte, daß dieser nach der Bemerkung zu Satz 6.2.10 existiert.

Dieser heiße $\tilde{\sigma} : \mathcal{F}_{\mathcal{E}_q}(X_{\mathcal{E}}) \to \mathcal{F}_{\mathcal{E}_q}(Y_{\mathcal{E}})$.

Beispiel 6.2.26 (Fortsetzung von Beispiel 6.2.25)
Die zu den Termen gehörigen Matrizen (über $\mathcal{S}_q$) lauten (vgl. Kapitel 5.3)

1. für das erste Beispiel

$$\begin{aligned} m_{\tilde{s}_1} \quad &:= \quad (h_2, h_2, h_2, h_2, h_2, h_2, h_2, h_0, h_0) \\ m_{\tilde{t}_1} \quad &:= \quad (h_1, h_0, h_0, h_0, h_0, h_0, h_0, h_0, h_0)\end{aligned}$$

Ist in einem Vektor eine der ersten sieben Komponenten ungleich 0, so erhält man bei der Multiplikation mit $m_{\tilde{s}_1}$ den Wert h_2. Diesen kann man aber durch Multiplikation mit $m_{\tilde{t}_1}$ nicht erreichen. Daher müssen die ersten sieben Komponenten eines Lösungsvektor gleich 0 sein. Die Komponenten 8 und 9 können dagegen beliebig sein. Somit wird der Kern von den Vektoren

$$(0, 0, 0, 0, 0, 0, 0, 1, 0)^{tr}$$

und

$$(0, 0, 0, 0, 0, 0, 0, 0, 1)^{tr}$$

erzeugt. Also ist ein allgemeinster Unifikator $\tilde{\sigma}_1 : \mathcal{T}(\Omega, X_{\mathcal{E}}) \to \mathcal{F}_{\mathcal{E}_q}(Y_{\mathcal{E}})$ definiert durch

$$\begin{aligned} y_i \quad &\mapsto \quad \underline{0} \quad i \in \{1, \ldots, 7\} \\ y_8 \quad &\mapsto \quad y_1 \\ y_9 \quad &\mapsto \quad y_2 \end{aligned}$$

2. für das zweite Beispiel

$$\begin{aligned} m_{\tilde{s}_2} &:= (h_1, h_0, h_0, h_0, h_0, h_0, h_0, h_0, h_0) \\ m_{\tilde{t}_2} &:= (h_0, h_1, h_2, h_2, h_2, h_2, h_2, h_2, h_2) \end{aligned}$$

Man überlegt sich leicht, daß hier neben dem Nullvektor nur solche Vektoren v im Kern liegen für die $m_{\tilde{s}_2} v = m_{\tilde{t}_2} v = (h_1)$ gilt. Somit wird der Kern von den folgenden Vektoren (als Spalten einer Matrix geschrieben) erzeugt:

$$\begin{pmatrix} 1 & h_1 & h_2 & 1 & 1 \\ 1 & 1 & 1 & h_1 & h_2 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Somit ergibt sich der allgemeinste Unifikator $\tilde{\sigma}_2 : \mathcal{T}(\Omega, X_{\mathcal{E}}) \rightarrow \mathcal{F}_{\mathcal{E}_q}(Y_{\mathcal{E}})$, der definiert ist durch

$$\begin{aligned} y_1 &\mapsto y_1 + h_1(y_2) + h_2(y_3) + y_4 + y_5 \\ y_2 &\mapsto y_1 + y_2 + y_3 + h_1(y_4) + h_2(y_5) \\ y_i &\mapsto \underline{0} \quad i \in \{3, \ldots, 9\} \end{aligned}$$

Ziel ist nun zu zeigen, daß der Unifikator $\tilde{\sigma}$ für $\tilde{\Gamma}$ mittels Δ' auf einem Unifikator für Γ abgebildet werden kann.

Lemma 6.2.27
Seien $|X_{\mathcal{E}}| = |A|^{|X_{\mathcal{A}}|}$ und $|Y_{\mathcal{E}}| = |A|^{|Y_{\mathcal{A}}|}$ und $\tilde{\sigma} \in S_{REA}(\mathcal{F}_{\mathcal{E}_q}(X_{\mathcal{E}}), \mathcal{F}_{\mathcal{E}_q}(Y_{\mathcal{E}}))$ Unifikator eines Problems $\tilde{\Gamma} = \Gamma\Delta$. Dann ist $\tilde{\sigma}\Delta'$ Unifikator für Γ.

Beweis
Da $\tilde{\sigma} \in S_{REA}(\mathcal{F}_{\mathcal{E}_q}(X_{\mathcal{E}}), \mathcal{F}_{\mathcal{E}_q}(Y_{\mathcal{E}}))$ ist $\tilde{\sigma}\Delta'$ definiert.
Betrachte $(s,t) \in \Gamma$. Da $\tilde{\sigma}$ Unifikator für $\tilde{\Gamma}$ ist, gilt mit $\tilde{s} = s\Delta$ und $\tilde{t} = t\Delta$

$$\tilde{s}\tilde{\sigma} =_{\mathcal{F}_{\mathcal{E}_q}(Y_{\mathcal{E}})} \tilde{t}\tilde{\sigma}$$

Dann gilt (in $\mathcal{F}_{\mathcal{A}}(Y_{\mathcal{A}})$)

$$\begin{aligned} & (\tilde{s}\tilde{\sigma})\Delta' = (\tilde{t}\tilde{\sigma})\Delta' \\ \stackrel{6.2.21}{\Rightarrow} \quad & (\tilde{s}\Delta')(\tilde{\sigma}\Delta') = (\tilde{t}\Delta')(\tilde{\sigma}\Delta') \\ \Rightarrow \quad & (s\Delta\Delta')(\tilde{\sigma}\Delta') = (t\Delta\Delta')(\tilde{\sigma}\Delta') \\ \stackrel{6.2.12}{\Rightarrow} \quad & s(\tilde{\sigma}\Delta') = t(\tilde{\sigma}\Delta') \end{aligned}$$

Somit ist $\tilde{\sigma}\Delta'$ Unifikator für Γ. $\square$

Im allgemeinen gilt jedoch für einen (allgemeinsten) Unifikator eines Unifikationsproblems über der q-max-Theorie nicht, daß $|Y_{\mathcal{E}}| = |A|^{|Y_A|}$ und $\tilde{\sigma} \in S_{REA}(\mathcal{F}_{\mathcal{E}_q}(X_{\mathcal{E}}), \mathcal{F}_{\mathcal{E}_q}(Y_{\mathcal{E}}))$.

Wir werden daher zwei Modifikationen an einem Unifikator vornehmen, so daß er die obigen Voraussetzungen erfüllt und wir den letzten Satz anwenden können.

Definition 6.2.28 (Variablenreduktion, Variablenexpansion)

- *Sei eine Substitution $\tilde{\sigma} : \mathcal{F}_{\mathcal{E}_q}(X_{\mathcal{E}}) \to \mathcal{F}_{\mathcal{E}_q}(Y_{\mathcal{E}})$ gegeben und seien*

$$D := \bigcup_{\substack{y_i, y_j \in X_{\mathcal{E}} \\ y_i \neq y_j}} (Var(y_i\sigma) \cap Var(y_j\sigma))$$

und

$$H := \{y : \exists y_i \in X_{\mathcal{E}} \exists h_j \in \Omega \text{ mit } \check{y_i}\sigma = \cdots + h_j(y) + \cdots\}.$$

Dann heißt $\mu_{1,\tilde{\sigma}}$ (kurz $\mu_1 : \mathcal{F}_{\mathcal{E}_q}(Y_{\mathcal{E}}) \to \mathcal{F}_{\mathcal{E}_q}(Y_{\mathcal{E}})$) definiert durch

$$\begin{array}{ll} y \mapsto \underline{0} & \text{für } y \in D \cup H \\ y \mapsto y & \text{für } y \in Y_{\mathcal{E}} \backslash (D \cup H) \end{array}$$

***Variablenreduktion** bzgl. $\tilde{\sigma}$.*

- *Seien $\mathcal{A}$ eine primale Algebra mit Universum A und eine variablenreduzierte Substitution $\tilde{\sigma} : \mathcal{F}_{\mathcal{E}_q}(X_{\mathcal{E}}) \to \mathcal{F}_{\mathcal{E}_q}(Y_{\mathcal{E}})$ und $Y = \{y_{j_1}, \ldots, y_{j_r}\} = Var(X_{\mathcal{E}}\tilde{\sigma})$ gegeben. Falls $r = 0$ ist, setzen wir $Z_{\mathcal{E}} = \emptyset$, sonst sei $|Z_{\mathcal{E}}| = \min\{|A|^j : |A|^j \geq |Y|\}$. OBdA sei $Z_{\mathcal{E}} = \{y_{j_1}, \ldots, y_{j_r}\} \dot{\cup} \{y_{j_{r+1}}, \ldots, y_{j_l}\}$ mit $l = |Z_{\mathcal{E}}|$. Wir definieren $\mu_2 : \mathcal{F}_{\mathcal{E}_q}(Y_{\mathcal{E}}) \to \mathcal{F}_{\mathcal{E}_q}(Z_{\mathcal{E}})$ folgendermaßen. Falls $r = 0$ ist, sei für alle $y \in Y_{\mathcal{E}}$ $y\mu_2 = \perp$. Ansonsten sei μ_2 definiert durch*

$$\begin{array}{rcll} y_{j_1} & \mapsto & y_{j_1} + y_{j_{r+1}} + \cdots + y_{j_l} & \\ y_j & \mapsto & y_j & \text{für alle } y_j \in Y_{\mathcal{E}} \backslash \{y_{j_1}\} \end{array}$$

*Dann heißt μ_2 **Variablenexpansion** bzgl. $\tilde{\sigma}$ und $\mathcal{A}$.*

Bemerkung 6.2.29
Sei $\tilde{\sigma} : \mathcal{F}_{\mathcal{E}_q}(X_{\mathcal{E}}) \to \mathcal{F}_{\mathcal{E}_q}(Y_{\mathcal{E}})$ Unifikator eines Unifikationsproblems $\tilde{\Gamma}$ über der q-max-Theorie. Dann gilt offensichtlich:

- *$\tilde{\sigma}\mu_1$ ist variablenreduziert.*
- *$\tilde{\sigma}\mu_1$ ist als Instanz von $\tilde{\sigma}$ Unifikator von $\tilde{\Gamma}$.*

Gilt für $Var(X_{\mathcal{E}}\sigma\tilde{\mu}_1) \neq \emptyset$, so gilt außerdem

- *$\tilde{\sigma}\mu_1\mu_2$ ist variablenreduziert und variablenexpandiert.*
- *$\tilde{\sigma}\mu_1\mu_2 \in S_{REA}(\mathcal{F}_{\mathcal{E}_q}(X_{\mathcal{E}}), \mathcal{F}_{\mathcal{E}_q}(Z_{\mathcal{E}}))$.*
- *$\tilde{\sigma}\mu_1\mu_2$ ist als Instanz von $\tilde{\sigma}$ Unifikator von $\tilde{\Gamma}$.*

Mit obiger Bemerkung gilt:

Satz 6.2.30
Sei $\mathcal{A}$ eine primale Algebra und Γ ein Unifikationsproblem über $\mathcal{F}_{\mathcal{A}}(X_{\mathcal{A}})$. Seien $|X_{\mathcal{E}}| = |A|^{|X_{\mathcal{A}}|}$ und $\tilde{\sigma} : \mathcal{F}_{\mathcal{E}_q}(X_{\mathcal{E}}) \rightarrow \mathcal{F}_{\mathcal{E}_q}(Y_{\mathcal{E}})$ Unifikator eines Problems $\tilde{\Gamma} = \Gamma\Delta$. Ist $Var(X_{\mathcal{E}}\sigma\tilde{\mu}_1) \neq \emptyset$, so ist $(\tilde{\sigma}\mu_1\mu_2)\Delta'$ Unifikator für Γ.

Ziel ist es, zu zeigen, daß falls

1. $Var(X_{\mathcal{E}}\tilde{\sigma}\mu_1) = \emptyset$ ist, kein Unifikator für Γ existiert und
2. ansonsten $(\tilde{\sigma}\mu_1\mu_2)\Delta'$ allgemeinster Unifikator für Γ ist.

Sei $\tau : \mathcal{F}_{\mathcal{A}}(X_{\mathcal{A}}) \rightarrow \mathcal{F}_{\mathcal{A}}(Z_{\mathcal{A}}')$ ein Unifikator für Γ. Wir zeigen unter dieser Voraussetzung gilt, daß $Var(X_{\mathcal{E}}\tilde{\sigma}\mu_1) \neq \emptyset$ ist und daß ein $\lambda : \mathcal{F}_{\mathcal{A}}(Z_{\mathcal{A}}) \rightarrow \mathcal{F}_{\mathcal{A}}(Z_{\mathcal{A}}')$ existiert mit

$$((\tilde{\sigma}\mu_1\mu_2)\Delta')\lambda = \tau$$

Zunächst überlegen wir uns, daß ein Unifikator für Γ mittels Δ auf einen Unifikator für $\tilde{\Gamma}$ abgebildet wird:

Lemma 6.2.31
Seien $|X_{\mathcal{E}}| = |A|^{|X_{\mathcal{A}}|}$ und $|Y_{\mathcal{E}}| = |A|^{|Y_{\mathcal{A}}|}$ und $\sigma \in Subs(\mathcal{F}_{\mathcal{A}}(X_{\mathcal{A}}), \mathcal{F}_{\mathcal{A}}(Y_{\mathcal{A}}))$ Unifikator eines Problems Γ. Dann ist $\sigma\Delta$ Unifikator für $\tilde{\Gamma} = \Gamma\Delta$.

Beweis
Da σ Unifikator ist, gilt für alle $(s,t) \in \Gamma$, daß $s\sigma =_{\mathcal{F}_{\mathcal{A}}(X_{\mathcal{A}})} t\sigma$ ist.

$$\begin{aligned} & s\sigma = t\sigma \\ \Rightarrow \quad & (s\sigma)\Delta = (t\sigma)\Delta \\ \overset{6.2.15}{\Rightarrow} \quad & (s\Delta)(\sigma\Delta) = (t\Delta)(\sigma\Delta) \end{aligned}$$

Somit ist $\sigma\Delta$ Unifikator für $\tilde{\Gamma}$. □

Somit ist $\tau\Delta = \tilde{\tau} : \mathcal{F}_{\mathcal{E}_q}(X_{\mathcal{E}}) \rightarrow \mathcal{F}_{\mathcal{E}_q}(Z_{\mathcal{E}}')$ ein Unifikator für $\tilde{\Gamma}$ und es existiert ein $\tilde{\nu} : \mathcal{F}_{\mathcal{E}_q}(Y_{\mathcal{E}}) \rightarrow \mathcal{F}_{\mathcal{E}_q}(Z_{\mathcal{E}}')$ mit $\tilde{\sigma}\tilde{\nu} = \tilde{\tau}$, da $\tilde{\sigma}$ allgemeinster Unifikator ist.

Lemma 6.2.32
Unter den obigen Bezeichnungen gilt

$$y\tilde{\sigma}\mu_1\mu_2 = \perp \Rightarrow y\tilde{\tau} = \perp$$

für alle $y \in X_{\mathcal{E}}$.

Beweis
Falls $y\tilde{\sigma} = \perp$ ist, so gilt auch $y\tilde{\sigma}\tilde{\nu} = \perp$, d.h. $y\tilde{\tau} = \perp$.

Betrachten wir nun den Fall, daß $y\tilde{\sigma} = \sum_{j\in J, i\in I_j} h_j(y_i) + \sum_{r\in R} y_r \neq \perp$ und $y\tilde{\sigma}\mu_1\mu_2 = \perp$ ist. Aufgrund der Definition von μ_2 gilt dann bereits $y\tilde{\sigma}\mu_1 = \perp$ ist. D.h.

1. Es gibt $y, y' \in X_\mathcal{E}$ mit $Var(y\tilde{\sigma}) \cap Var(y'\tilde{\sigma}) \neq \emptyset$ oder
2. $J \neq \emptyset$.

Angenommen es gibt $y, y' \in X_\mathcal{E}$ mit $y \neq y'$ und es gäbe ein $z \in Y_\mathcal{E}$ mit $z \in Var(y\tilde{\sigma}) \cap Var(y'\tilde{\sigma})$, also $z\mu_1 = \perp$. Angenommen $z\tilde{\nu} \neq \perp$, so würde $Var(y\tilde{\sigma}\tilde{\nu}) \cap Var(y'\tilde{\sigma}\tilde{\nu}) = Var(y\tilde{\tau}) \cap Var(y'\tilde{\tau}) \neq \emptyset$ gelten, im Widerspruch zu $\tilde{\tau} \in S_{REA}(\mathcal{F}_{\mathcal{E}_q}(X_\mathcal{E}), \mathcal{F}_{\mathcal{E}_q}(Z_\mathcal{E}'),)$.

Betrachten wir nun den Fall, daß für $y\tilde{\sigma} = \sum_{j\in J, i\in I_j} h_j(y_i) + \sum_{r\in R} y_r$ gilt, daß $J \neq \emptyset$ ist. Ist für ein $j \in J$ und für ein $i \in I_j$ die Variable $y_i \in Y_\mathcal{E}$ im Bild einer Variablen $y' \neq y$ unter $\tilde{\sigma}$ enthalten, so wird diese mittels $\tilde{\nu}$ auf $\perp$ abgebildet, wie im ersten Teil gezeigt wurde.

Betrachten wir daher noch den Fall, daß ein i und ein j gibt, mit $i \in I_j$ und für alle $y' \in X_\mathcal{E}$ mit $y \neq y'$ gilt $y_i \notin Var(y'\tilde{\sigma})$. Sei $J_i = \{j \in J : y_i \in I_j\}$. Nach Voraussetzung ist $J_i \neq \emptyset$. Wir führen dieses zu einem Widerspruch. Sei $\tilde{\sigma}' : \mathcal{F}_{\mathcal{E}_q}(X_\mathcal{E}) \to \mathcal{F}_{\mathcal{E}_q}(Y_\mathcal{E})$ definiert durch

$$\tilde{\sigma}'|_{X_\mathcal{E}\setminus\{y\}} = \tilde{\sigma}|_{X_\mathcal{E}\setminus\{y\}}$$

und

$$y\tilde{\sigma}' = \sum_{j\in J, i'\in I_j'} h_j(y_{i'}) + \sum_{r\in R} y_r + y_i$$

wobei für alle $j \in J$ $I_j' = I_j\setminus\{y_i\}$ sei. Dann ist offensichtlich $\tilde{\sigma}'$ ein Unifikator für $\tilde{\Gamma}$ (vergleiche Rechstmultiplikation in $\mathcal{S}_{\mathcal{E}_q}$) und es gilt $\tilde{\sigma}' \lesssim \tilde{\sigma}$ aber nicht $\tilde{\sigma} \lesssim \tilde{\sigma}'$, im Widerspruch dazu, daß $\tilde{\sigma}$ allgemeinster Unifikator ist.

Somit gilt die Behauptung. □

Folgerung 6.2.33
Gilt für $\tilde{\sigma}\mu_1\mu_2$, daß $y\tilde{\sigma} = \perp$ für alle $y \in X_\mathcal{E}$ ist, so existiert kein Unifikator für Γ.

Beweis
Angenommen es gäbe einen Unifikator $\tau : \mathcal{F}_\mathcal{A}(X_\mathcal{A}) \to \mathcal{F}_\mathcal{A}(Z_\mathcal{A}')$. Dann ist $\tilde{\tau} = \tau\Delta$ ein Unifikator für $\tilde{\Gamma}$. Gilt für alle $y \in X_\mathcal{E}$, daß $y\tilde{\sigma}\mu_1\mu_2 = \perp$, so gilt mit obigem Lemma auch für alle y, $y\tilde{\tau} = \perp$ ist, im Widerspruch dazu, daß $\tilde{\tau}$ eine Atom-Substitution ist. Daher kann τ nicht existieren. □

Im folgenden schreiben wir für $\tilde{\sigma}\mu_1\mu_2$ kürzer $\tilde{\sigma}'$. Betrachten wir nun den Fall, daß $Var(X_{\mathcal{E}}\tilde{\sigma}') = Z_{\mathcal{E}} \neq \emptyset$ gilt.

Lemma 6.2.32 liefert uns außerdem die Möglichkeit, ein $\tilde{\lambda}$ mit $\tilde{\sigma}'\tilde{\lambda} = \tilde{\tau}$ zu konstruieren. Denn gilt für ein $y_i \in X_{\mathcal{E}}$, daß $y_i\tilde{\sigma}' \neq \perp$ ist, so ist $y_i\tilde{\sigma}' = \sum_{r\in R_i} y_r$ mit $R_i \neq \emptyset$ und für $y_j \neq y_i$ gilt $R_j \cap R_i = \emptyset$, da $\tilde{\sigma}'$ variablenreduziert und -expandiert ist. Sei $R_i = \{r_{i_1}, \ldots, r_{i_v}\}$. Dann ist die Abbildung $\tilde{\lambda} : \mathcal{F}_{\mathcal{E}_q}(Z_{\mathcal{E}}) \rightarrow \mathcal{F}_{\mathcal{E}_q}(Z_{\mathcal{E}}')$ definiert durch

$$\begin{aligned} y_{r_{i_1}}\tilde{\lambda} &= y_i\tilde{\tau} \\ y_{r_k}\tilde{\lambda} &= \perp \quad \text{für alle } r_k \neq r_{i_1} \end{aligned}$$

wohldefiniert. Außerdem gilt offensichtlich $\tilde{\sigma}'\tilde{\lambda} = \tilde{\tau}$.

Wir zeigen nun, daß $\tilde{\lambda} \in S_{REA}(\mathcal{F}_{\mathcal{E}_q}(Z_{\mathcal{E}}), \mathcal{F}_{\mathcal{E}_q}(Z_{\mathcal{E}}'))$ gilt: Zunächst gilt nach Definition von μ_2, daß $|Z_{\mathcal{E}}| = |A|^{Z_{\mathcal{A}}}$ für ein geeignetes $Z_{\mathcal{A}}$. Nach Definition von τ gilt $|Z_{\mathcal{E}}'| = |\mathcal{A}|^{Z_{\mathcal{A}}'}$. Da $\tilde{\tau}$ eine Atom-Abbildung ist, ist auch $\tilde{\lambda}$ eine Atomabbildung.

Somit ist $\tilde{\lambda}\Delta'$ definiert.

Wir schließen unsere Überlegungen mit der Feststellung, daß $\tilde{\sigma}'\Delta'$ ein allgemeinster Unifikator für Γ ist:

Lemma 6.2.34
Unter den obigen Bezeichnungen gilt: $\tilde{\sigma}'\Delta' = (\tilde{\sigma}\mu_1\mu_2)\Delta'$ ist ein allgemeinster Unifikator für Γ.

Beweis
Es gilt $\tilde{\sigma}' \in S_{REA}(\mathcal{F}_{\mathcal{E}_q}(X_{\mathcal{E}}), \mathcal{F}_{\mathcal{E}_q}(Z_{\mathcal{E}}))$ und $\tilde{\tau} \in S_{REA}(\mathcal{F}_{\mathcal{E}_q}(X_{\mathcal{E}}), \mathcal{F}_{\mathcal{E}_q}(Z_{\mathcal{E}}'))$. Nach obigen Überlegungen existiert ein $\tilde{\lambda} \in S_{REA}(\mathcal{F}_{\mathcal{E}_q}(Z_{\mathcal{E}}), \mathcal{F}_{\mathcal{E}_q}(Z_{\mathcal{E}}'))$ mit $\tilde{\sigma}'\tilde{\lambda} = \tilde{\tau}$. Dann gilt:

$$\begin{aligned} & \tilde{\sigma}'\tilde{\lambda} = \tilde{\tau} \\ \Rightarrow\quad & (\tilde{\sigma}'\tilde{\lambda})\Delta' = \tilde{\tau}\Delta' \\ \stackrel{6.2.23}{\Rightarrow}\quad & (\tilde{\sigma}'\Delta')(\tilde{\lambda}\Delta') = \tilde{\tau}\Delta' \\ \stackrel{6.2.22}{\Rightarrow}\quad & (\tilde{\sigma}'\Delta')(\tilde{\lambda}\Delta') = \tau \end{aligned}$$

Somit existiert ein $\lambda : \mathcal{F}_{\mathcal{A}}(Z_{\mathcal{A}}) \rightarrow \mathcal{F}_{\mathcal{A}}(Z_{\mathcal{A}}')$ mit $(\tilde{\sigma}'\Delta')\lambda = \tau$, d.h. $\tilde{\sigma}'\Delta'$ ist allgemeiner als τ. □

Wir fassen Folgerung 6.2.33 und die Aussage des letzten Lemmas zusammen:

Satz 6.2.35
Sei Γ ein Unifikationsproblem über einer primalen Algebra $\mathcal{A}$ und sei $\tilde{\sigma}$ allgemeinster Unifikator für das Problem $\tilde{\Gamma} = \Gamma\Delta$. Gilt für $\tilde{\sigma}' = \tilde{\sigma}\mu_1\mu_2$, daß $Var(X_{\mathcal{E}}\tilde{\sigma}') = \emptyset$, so existiert kein Unifikator für Γ. Ansonsten ist $\tilde{\sigma}'\Delta'$ allgemeinster Unifikator für Γ.

Beispiel 6.2.36 (Fortsetzung von Beispiel 6.2.26)

1. Da σ' variablenreduziert ist, ist μ_1 die identische Abbildung. Wegen $Y_{\mathcal{E}} = \{y_1, y_2\}$ und $|A|^1 = 3$ setzen wir $Z_{\mathcal{E}} := \{y_1, y_2, y_3\}$ und $Y_{\mathcal{A}} := \{x_1\}$. $\mu_2 : \mathcal{F}_{\mathcal{E}_q}(Y_{\mathcal{E}}) \to \mathcal{F}_{\mathcal{E}_q}(Z_{\mathcal{E}})$ ergibt sich zu $y_1 \mapsto y_1 + y_3$ und $\tilde{\sigma}'_1 := \tilde{\sigma}_1 \mu_1 \mu_2$ ist definiert durch

$$\begin{array}{lll} y_i & \mapsto & \underline{0} \quad i \in \{1, \ldots, 7\} \\ y_8 & \mapsto & y_1 + y_3 \\ y_9 & \mapsto & y_2 \end{array}$$

Somit ist $\tilde{\sigma}'\Lambda : At(\mathcal{A}, X_{\mathcal{A}}) \to \mathcal{F}_{\mathcal{A}}(Y_{\mathcal{A}})$ definiert durch

$$\begin{array}{ccl} C_0(x_1)C_0(x_2) & \mapsto & \perp \\ \vdots & \mapsto & \vdots \\ C_2(x_1)C_0(x_2) & \mapsto & \perp \\ C_2(x_1)C_1(x_2) & \mapsto & C_0(x_1) + C_2(x_1) \\ C_2(x_1)C_2(x_2) & \mapsto & C_1(x_1) \end{array}$$

Aufgrund der allgemeinen Form

$$x_j \mapsto \sum_{(i_1,\ldots,i_k)\in A^k} \underline{i_j}(C_{i_1}(x_1)\ldots C_{i_k}(x_k))\varphi$$

wird $\tilde{\sigma}'\Delta' = \sigma' : \mathcal{T}(\Sigma, X_{\mathcal{A}}) \to \mathcal{F}_{\mathcal{A}}(Y_{\mathcal{A}})$ definiert durch

$$\begin{array}{lll} x_1 & \mapsto & 2(C_0(x_1) + C_2(x_1)) + 2C_1(x_1) \quad (=_{\mathcal{F}_{\mathcal{A}}(Y_{\mathcal{A}})} \top) \\ x_2 & \mapsto & 1C_0(x_1) + 1C_2(x_1) + 2C_1(x_1) \end{array}$$

Eine kleine Rechnung zeigt, daß (wie nicht anders zu erwarten)

$$s\sigma' =_{\mathcal{F}_{\mathcal{A}}(Y_{\mathcal{A}})} t\sigma'.$$

2. Aus $\tilde{\sigma}_2 : \mathcal{T}(\Omega, X_{\mathcal{E}}) \to \mathcal{F}_{\mathcal{A}}(Y_{\mathcal{E}})$ definiert durch

$$\begin{array}{lll} y_1 & \mapsto & y_1 + h_1(y_2) + h_2(y_3) + y_4 + y_5 \\ y_2 & \mapsto & y_1 + y_2 + y_3 + h_1(y_4) + h_2(y_5) \\ y_i & \mapsto & \underline{0} \quad i \in \{3, \ldots, 9\} \end{array}$$

ergibt sich zunächst, daß die in Homomorphismen enthalten Variablen y_2, y_3, y_4 und y_5 unter μ_1 auf $\perp$ abgebildet werden müssen. Außerdem muß auch y_1 auf $\perp$ abgebildet werden, da y_1 Summand sowohl im Bild von y_1 als auch im Bild von y_2 unter $\tilde{\sigma}$ ist. Somit ist $\mu_1 : \mathcal{F}_{\mathcal{E}_q}(X_{\mathcal{E}}) \to \mathcal{F}_{\mathcal{E}_q}(Z_{\mathcal{E}})$ definiert durch $y \mapsto \perp$ für alle $y \in X_{\mathcal{E}}$. Daher ist $\mu_2 : \mathcal{F}_{\mathcal{E}_q}(Z_{\mathcal{E}}) \to \mathcal{F}_{\mathcal{E}_q}(Z_{\mathcal{E}}')$ für $Z_{\mathcal{E}}' = \emptyset$ der Homomorphismus bestimmt durch $y \mapsto \perp$ für alle $y \in Z_{\mathcal{E}}$. Nach Satz 6.2.35 ist Γ_2 somit nicht unifizierbar ist.

Abschließend sei das Unifikationsverfahren noch einmal schematisch dargestellt:

1. Das gegebene Unifikationsproblem Γ über der primalen Algebra wird in Post-Normalform übersetzt.
2. Anschließend wird das Unifikationsproblem in ein (nicht äquivalentes) Unifikationsproblem $\tilde{\Gamma}$ über der q-max- Theorie übersetzt.
3. Hier wird ein allgemeinster Unifikator $\tilde{\sigma}$ berechnet.
4. $\tilde{\sigma}$ wird mittels μ_1 und μ_2 zu $\tilde{\sigma}' = \tilde{\sigma}\mu_1\mu_2$ abgeändert.
5. Ist $Var(X_{\mathcal{E}}\tilde{\sigma}') = \emptyset$, so existiert kein Unifikator für Γ, ansonsten ist Δ' für $\tilde{\sigma}'$ definiert und es gilt, daß $\tilde{\sigma}'\Delta'$ ein allgemeinster Unifikator für Γ ist.

6.2.5 Bemerkungen

Analysiert man die Modifikation μ_1 genauer, so stellt man fest, daß eine Variable y_j unter μ_1 immer dann auf $\perp$ abgebildet wird, falls sich in der Matrix, die aus den Vektoren eines Erzeugendensystems des Kerns des entsprechenden Gleichungssystems besteht, in der Spalte j mehr als ein Eintrag gleich 1 befindet. (vgl. das zweite Beispiel in 6.2.36).

Steht z.B. in dieser Matrix in der Spalte j in Zeile i der Wert t und in Zeile i' der Wert t' mit $t, t' \neq \perp$, so gilt für $\tilde{\sigma}$, daß

$$\begin{aligned} x_i &\mapsto \cdots + t(y_j) + \cdots \\ x_{i'} &\mapsto \cdots + t'(y_j) + \cdots \end{aligned}$$

wobei $t(y_j)$ bedeute, daß in dem Term t nur die Variable y_j vorkommt. Somit wird mittels μ_1 die Variable y_j auf $\perp$ abgebildet, sei es, weil t oder t' nur aus Summen von Homomorphismen $(h_k(y_j))_{k\in K}$ bestehen oder weil $t = t' = y_j$ gilt und somit y_j sowohl im Bild von x_i als auch im Bild von $x_{i'}$ als Variable vorkommt.

Ist in der Spalte j genau ein Eintrag ungleich 0 und ist dieser ungleich 1, so ist dieser gleich einem Homomorphismus h_i oder gleich h_i^y und wird deshalb durch die Variablenreduktion auf $\perp$ abgebildet.

Um daher einen Unifikator für Γ zu erhalten, braucht man nur solche Vektoren aus dem Erzeugendensystem zu betrachten, die genau einen Eintrag gleich 1 und sonst nur Einträge gleich 0 haben. Dieses sind aber gerade die Einheitsvektoren e_i, die an der Stelle i den Eintrag 1 und sonst 0 haben.

Offensichtlich ist aber der Vektor e_i genau dann Lösungsvektor des betrachteten Gleichungssystems, falls in den betrachteten Matrizen an der Komponente i der selbe Eintrag steht.

Betrachten wir noch einmal unser Beispiel, für das wir dann erhalten:

Beispiel 6.2.37 (Fortsetzung von Beispiel 6.2.26)
Die Matrizen lauten (vgl. Beispiel 6.2.26)

1. für das erste Beispiel

$$\begin{aligned} m_{\tilde{s}_1} &:= (h_2, h_2, h_2, h_2, h_2, h_2, h_2, h_0, h_0) \\ m_{\tilde{t}_1} &:= (h_1, h_0, h_0, h_0, h_0, h_0, h_0, h_0, h_0) \end{aligned}$$

   Nur an den Komponenten 8 und 9 sind gleiche Einträge, so daß sich $\tilde{\sigma}\mu_1$ ergibt zu:

$$\begin{aligned} y_i &\mapsto \underline{0} \quad i \in \{1, \ldots, 7\} \\ y_8 &\mapsto y_1 \\ y_9 &\mapsto y_2 \end{aligned}$$

2. für das zweite Beispiel

$$\begin{aligned} m_{\tilde{s}_2} &:= (h_1, h_0, h_0, h_0, h_0, h_0, h_0, h_0, h_0) \\ m_{\tilde{t}_2} &:= (h_0, h_1, h_2, h_2, h_2, h_2, h_2, h_2, h_2) \end{aligned}$$

   Das heißt, die Komponenten sind paarweise verschieden, so daß sich $\tilde{\sigma}\mu_1$ ergibt als die Abbildung, die jeder Variablen 0 zuweist und mit Satz 6.2.35 folgt somit, daß kein Unifikator existiert.

Man kann sich also im wesentlichen auf einen Vergleich der entsprechenden Koeffizienten zweier Terme in Post-Normalform beschränken, da sich hierdurch der Unifikator (evtl. unter Verwendung der Variablen-Expansion) sehr leicht ermitteln läßt. Somit ist die Komplexität des Verfahrens im wesentlichen durch das NP-vollständige Entscheidungsproblem, welche zwei Atome in der Post-Normalform dieselben Koeffizienten haben, gegeben.

Kapitel 7

Zusammenfassung

In dieser Arbeit wurden die Zusammenhänge zwischen der Unifikation in primalen Algebren und der Unifikation in monoidal-kommutativen Theorien untersucht.

Dazu war es zunächst notwendig, den Begriff der Unifikation in einer Algebra geeignet zu definieren. Insbesondere mußte eine Analogie zu der Definition der Unifikation in Gleichungstheorien erreicht werden, um überhaupt Unifikationsverfahren für Gleichungstheorien mit denen für primale Algebren vergleichen zu können.

Die Definition erfolgte in Kapitel 3.3 und es wurde gezeigt, daß auch im Fall der $\mathcal{A}$-Unifikation – wie bei der Unifikation in Gleichungstheorien – in einer freien Algebra gerechnet werden kann, falls *Gültigkeit* von Gleichungen untersucht wird.

Auf die Besonderheiten dieser Definition des $\mathcal{A}$-Unifikators im Hinblick auf die Untersuchung der *Lösbarkeit* eines Gleichungssystems in einer Algebra wurde in Kapitel 4 eingegangen. Insbesondere wurde gezeigt, daß die Lösbarkeit eines Gleichungssystems in einer Algebra mittels $\mathcal{A}$-Unifikation entschieden werden kann, falls alle Elemente von $\mathcal{A}$ erreichbar sind.

Um die Unifikation in monoidal-kommutativen Theorien mit der in primalen Algebren vergleichen zu können, wurde als nächstes untersucht, unter welchen Voraussetzungen man zwei Gleichungstheorien oder zwei Algebren bzgl. der Unifikation identifizieren kann. Dazu wurde mittels des Begriffs der Signaturtransformation eine Äquivalenzrelation auf Gleichungstheorien und auf Algebren eingeführt und genauer analysiert (vgl. Kapitel 3.6).

Es wurde gezeigt, daß für zwei äquivalente Theorien/Algebren $\mathcal{A}$ und $\mathcal{B}$ eine minimal vollständige Menge von Unifikatoren (insbesondere also allgemeinste Unifikatoren) für ein Unifikationsproblem über $\mathcal{A}$ durch die zugehörigen Signaturtransformationen auf eine minimal vollständige Menge von Unifikatoren für das entsprechende Unifikationsproblem über $\mathcal{B}$ abgebildet werden und umgekehrt. Hat man daher die Signaturtransformationen explizit gegeben, so erhält man aus einem Unifikationsverfahren für $\mathcal{A}$ ein Verfahren für $\mathcal{B}$, indem man ein Unifikationsproblem über $\mathcal{B}$ in eines über $\mathcal{A}$ transformiert, hier die Unifikatoren berechnet und diese in Unifikatoren für das ursprüngliche Problem zurückübersetzt.

Außerdem wurde gezeigt, daß die sehr „technische" Definition der Signaturtransformation für über abzählbar unendlicher Variablenmenge äquivalente Algebren/Theorien einen Isomorphismus der entsprechenden kanonischen Kategorien definiert und somit „recht anschaulich" charakterisiert werden kann.

In Kapitel 6 wurde gezeigt, daß primale Algebren und monoidal-kommutative Theorien *nicht* äquivalent sind. Man kann also einen Unifikationsalgorithmus für monoidal-kommutative Theorien nicht *direkt* zur Unifikation in primalen Algebren verwenden.

Da monoidal-kommutative Theorien genau die Theorien sind, bei denen ein allgemeinster Unifikator durch ein endliches Erzeugendensystem der Lösungsmenge eines linearen Gleichungssystems über einem Halbring gegeben ist, folgt, daß dies für die Unifikation in primalen Algebren nicht gilt. Das heißt, übersetzt man ein Unifikationsproblem Γ über einer primalen Algebra in ein Gleichungssystem über einem Halbring, so ist ein allgemeinster Unifikator im allgemeinen nicht durch ein Erzeugendensystem des Lösungsraums gegeben.

Allerdings zeigt das Vorgehen in Kapitel 6.2, daß die Einheitsvektoren, die in einem endlichen Erzeugendensystem des Lösungsraums liegen, verwendet werden können, um einen allgemeinsten Unifikator für Γ zu erhalten. Das heißt, ein allgemeinster Unifikator, sofern existent, kann durch ein endliches Erzeugendensystem eines geeigneten Teilraums des Lösungsraums des Gleichungssystems ermittelt werden. Ist der von den Einheitsvektoren im Lösungsraum des Gleichungssystems erzeugte Teilraum der Nullraum, so existiert kein allgemeinster Unifikator für Γ.

Daß die durch das Erzeugendensystem des Teilraums gegebene Abbildung noch einer Variablenexpansion bedarf, um allgemeinster Unifikator für Γ zu sein, ist eher als „technische Nebensache" zu verstehen.

Wenn auch für praktische Belange das hier vorgestellte Verfahren nicht zweckmäßig erscheint und mühelos durch die Bemerkungen in Kapitel 6.2.5 wesentlich verbessert werden kann, so macht dieses Ergebnis doch deutlich, daß die Unifikation in primalen Algebren zwar nicht äquivalent zu der in monoidal-kommutativen Theorien ist, aber große Gemeinsamkeiten zwischen beiden Ansätzen bestehen.

Symbolverzeichnis

Symbol	Bemerkung	Seite
$\lesssim$	Quasiordnung (auf Unifikatoren)	6, 32
$\leq$	Halbordnung	7
$\mathcal{A} \leq \mathcal{B}$	$\mathcal{A}$ Unteralgebra von $\mathcal{B}$	10
$\mathbb{N}$	natürliche Zahlen, $\mathbb{N} = \{0, 1, \ldots\}$	8
Σ	Signatur	8
st	Stelligkeitsfunktion	8
$\Sigma^{(n)}$	Menge der n-stelligen Symbole	9
$T(\Sigma, X)$	Menge der Σ-Terme über X	9
$Var(t)$	Menge der Variablen von t	9
Σ^A	Familie der zu jedem $f \in \Sigma$ gehörigen Operationen	10
$Sub\,\mathcal{A}$	Menge der Unteralgebren von $\mathcal{A}$	10
$Hom(\mathcal{A}, \mathcal{B})$	Menge der Homomorphismen von $\mathcal{A}$ nach $\mathcal{B}$	11
$End\,\mathcal{A}$	Menge der Endomorphismen von $\mathcal{A}$	11
$\mathcal{A} \cong \mathcal{B}$	$\mathcal{A}$ isomorph zu $\mathcal{B}$	11
$[t](\theta)$	Äquivalenz- bzw. Kongruenzklasse von t bzgl. θ	11, 20
$Con\,\mathcal{A}$	Menge aller Kongruenzrelationen von $\mathcal{A}$	11
$\mathcal{T}(\Sigma, X)$	Σ-Termalgebra über X	12
$Subs(\mathcal{T}(\Sigma, X), \mathcal{T}(\Sigma, Y))$	Menge der Substitutionen von $\mathcal{T}(\Sigma, X) \to \mathcal{T}(\Sigma, Y)$	12
$T(\mathcal{A})$	Menge der Polynomfunktionen von $\mathcal{A}$	13
$P_A(\Sigma, X)$	Menge der Polynome über X	15
$P(\mathcal{A})$	Menge der Termfunktionen von $\mathcal{A}$	15
$\mathcal{A} \models s = t$	$\mathcal{A}$ ist Modell für $s = t$	16
$(\mathcal{A}, \alpha) \models s = t$	$(\mathcal{A}, \alpha)$ ist Modell für $s = t$	16
$\mathfrak{K} \models s = t$	$\mathfrak{K}$ ist Modell für $s = t$	17
$M(E)$	Klasse der Modelle von E	17
$G_X(\mathfrak{K})$	Menge der in $\mathfrak{K}$ gültigen Gleichungen	17
$S(\mathfrak{K}), H(\mathfrak{K}), P(\mathfrak{K}), I(\mathfrak{K})$	Operatoren auf $\mathfrak{K}$	17

Literaturverzeichnis

[Baa86] **Baader, F.;**
The theory of idempotent semigroups is of unification type zero.
J. Automated Reasoning, 2(3):283-286, 1986

[Baa89] **Baader, F.;**
Unifikation und Reduktionssysteme für Halbgruppenvarietäten
Arbeitsberichte des Instituts für mathematische Maschinen und Datenverarbeitung (Informatik), Band 22, Nummer 8, Erlangen, 1986

[Baa89a] **Baader, F.;**
Characterization of unification type zero
Proceedings of the 3rd International Conference on Rewriting Techniques and Applications, RTA 89, Chapel Hill (USA), LNCS 355, S. 2 – 14, Springer 1989

[Baa91] **Baader, F.;**
Unification, weak unification, upper bound, lower bound, and generalization problems
Proceedings of the 4th International Conference on Rewriting Techniques and Applications, RTA 91, LNCS 488, S. 86 – 97, Springer 1991

[BaNu90] **Baader, F.; Nutt, W.;**
Adding Homomorphisms to Commutative/Monoidal Theories
DFKI Research Report RR-90-16 (German Research Center for Artificial Intelligence)

[BaaSi94] **Baader, F; Siekmann, J. H.;**
Unification Theory
In: Gammay, D. M.; Hogger C.J.; Robinson, J. A., (editors), Handbook of Logic in Artificial Intelligence and Logic Programming, Oxford University Press, Oxford, UK, 1994

[Bü90] **Büttner, W.; Estenfeld, K.; Schmid, R.; Schneider, H.-A.; Tidén, E.;**
Symbolic constraint handling through unification in finite algebras
AAECC, Applicable Algebra in Engineering, Communication and Computing, 1, S. 97 – 118, Springer-Verlag, 1990

[Grä79] **Grätzer, G.;**
Universal Algebra
Springer-Verlag New York, 2. Auflage, 1979

[HeSt79] **Herrlich, H.; Strecker, G. E.;**
Category Theory
Heldermann Verlag Berlin, 2. edition, 1979

[Ih93] **Ihringer, Th.;**
Allgemeine Algebra
B. G. Teubner Stuttgart, 2. Auflage, 1993

[KiRi94] **Kirchner, H.; Ringeissen, Ch.**
Combining symbolic constraint solvers on algebraic domains
Journal of Symbolic Computation, (1994), 11, 1-000

[La63] **Lawvere, F.W.;**
Functional Semantics of Algebraic Theories
Ph.D. Thesis, Columbia University, 1963

[Ni90] **Nipkow, T.;**
Unification in primal algebras, their powers and their varities
Journal of the Association for Computing Machinery, Vol. 38, No. 1, October 1990, pp. 742 – 776

[Nutt92] **Nutt, W.;**
Unification in Monoidal Theories is Solving Linear Equations over Semirings
DFKI Research Report RR-92-02 (German Research Center for Artificial Intelligence)

[Pl72] **Plotkin, G.;**
Building in equational theories
Machine Intelligence, 7:73-90, 1972

[Ro65] **Robinson, J. A.;**
A machine oriented logic based on the resolution principle
J. of the ACM, 12(1):23-41, 1965

[Si79] **Siekmann, J. H.;**
Unification of commutative terms
Proceedings of the International Symposium on Symbolic and Algebraic Manipulation, EUROSAM '79, volume 72 of Lecture Notes in Computer Science, pages 5331–545, Springer Verlag, 1979

[We92] **Wechler, W.;**
Universal Algebra for Computer Scientists
Springer-Verlag Berlin, 1992

Index