0 Algebraische Algorithmentheorie

H. Kaphengst

H. Reichel

Robotronbericht 1971

1. Multialgebren

1.1 Signaturen

Wir brauchen einen Vorrat von Dingen, auf die wir die Mengen und Operationen der Multialgebren beziehen können, und solche, die Rechenprozesse mit bzw. Bedingungen für Elemente von Multialgebren ausdrücken. Einen solchen Vorrat könnten wir in Form einer passenden Menge von Zeitreihen konstruieren, wollen aber lieber eine axiomatische Charakterisierung dieses Vorrats geben, weil damit von vornherein verhindert wird, daß unwesentliche Eigenschaften der zu konstruierenden Dinge betrachtet werden können.

Beim ersten Lesen genügt eine oberflächliche Kenntnisnahme der formalen Begriffe dieses Punktes, sie werden im nächsten Punkt durch inhaltliche Begriffe verständlich.

Ein Signaturvorrat besteht aus verschiedenen Dingen, die wir Sorten, Produkte, Operatoren, Terme, Gleichungen und Implikationen nennen. Dabei gilt:

(1) Es gibt unendlich viele Sorten.

(2) Jedes Produkt hat eine Länge, das ist eine natürliche Zahl und für jede natürliche Zahl i, kleiner als die Länge, ein i-tes Glied, das ist eine Sorte. Ist eine natürliche Zahl gegeben und für jede kleinere natürlichere Zahl eine Sorte, so gibt es genau ein Produkt, dessen Länge die gegebene Zahl ist und dessen i-te Glieder die zu den jeweiligen i gegebenen Sorten sind. Ein Produkt der Länge 1 ist eine Sorte, es stimmt mit seinen 0-ten Glied überein.

(3) Jeder Operator hat eine Definitionsbedingung, das ist eine Gleichung, und einen Ausgang, das ist eine Sorte. Der Eingang der Gleichung heißt auch Eingang des Operators. Zu jeder Gleichung und jeder Sorte gibt es unendlich viele Operatoren, dessen Definitionsbedingung diese Gleichung und dessen Ausgang diese Sorte ist.

(4) Jeder Term hat einen Eingang und einen Ausgang, das sind Produkte. Ein Grundterm ist ein Term, dessen Ausgang eine Sorte ist. Ein Term hat für jede natürliche Zahl i, kleiner als die Länge des Ausgangs, ein i-tes Glied, das ist ein Grundterm, dessen Eingang der Eingang des Terms und dessen Ausgang das i-te Glied des Ausgangs des Terms ist. Ist ein Produkt und eine natürliche Zahl gegeben und für jede kleinere natürliche Zahl ein Grundterm, dessen Eingang das gegebene Produkt ist, so gibt es genau einen Term mit dem gegebenen Produkt als Eingang, dessen i-te Glieder die zu den jeweiligen i gegebenen Grundterme sind, sein Ausgang hat die gegebene natürliche Zahl als Länge und als i-te Glieder die Ausgänge der entsprechenden Grundterme. Jeder Grundterm hat entweder einen Index (er heißt dann Projektor), das ist eine natürliche Zahl, die kleiner als die Länge eines Eingangs ist, oder aber er hat einen Hauptoperator, das ist ein Operator, dessen Ausgang mit dem Ausgang des Grundterms übereinstimmt, sowie einen Rest, das ist ein Term, dessen Eingang mit dem Eingang des Grundterms und dessen Ausgang mit dem Eingang des Hauptoperators übereinstimmt. Ist ein Produkt gegeben und eine natürliche Zahl i, kleiner als dessen Länge, so gibt es genau einen Grundterm, dessen Eingang das Produkt und dessen Index i ist; sein Ausgang ist dann das i-te Glied des Produkts. Ist ein Operator und ein Term, dessen Ausgang mit dem Eingang des Operators übereinstimmt, gegeben, so gibt es genau einen Grundterm, der diesen Operator als Hauptoperator und diesen Term als Rest hat.

(5) Jede Gleichung hat eine linke und eine rechte Seite, das sind Terme mit übereinstimmenden Eingängen und Ausgängen. Zu je zwei Termen mit übereinstimmenden Eingängen und Ausgängen gibt es genau eine Gleichung, dessen Seiten diese Terme sind. Der Eingang einer Gleichung ist der Eingang einer Seite. Eine Grundgleichung ist eine Gleichung, deren Seiten Grundterme sind.

(6) Jede Implikation hat eine linke und eine rechte Seite, das sind Gleichungen mit übereinstimmendem Eingang; dieser ist dann auch Eingang der Implikation mit diesen Gleichungen als linke bzw. rechte Seite.

(7) Jede Menge von Grundtermen, die alle Projektoren enthält und die einen beliebigen Grundterm mit Hauptoperator bereits dann enthält, falls sie die Glieder seines Restes und der linken und rechten Seite der Definitionsbedingung seines Hauptoperators enthält, ist die Menge aller Grundterme.

1 Kurzwiederholung: Klassische Algebren, Prädikatenkalkül ,Universelle Algebra, Kategorienbegriff

Algebra ist die Lehre vom Lösen von Gleichungen. Der Abstraktionsgrad der Algebra hat sich im Laufe der Geschichte der Mathematik wesentlich erhöht.
Rechnen mit natürlichen, gebrochenen, rationalen, reellen, komplexen Zahlen. (indische und arabische Mathematik)
Anfang des neunzehnten Jahrhunderts hat man versucht die wesentlichen Eigenschaften dieser Strukturen herauszukristallisieren.

1.1 Algebren mit einer Menge und einer Operation

Definitionen 1.1:
Eine **Gruppe** besteht aus einer Grundmenge G und einer binären Operation $\oplus$: G * G → G, für die die folgenden Axiome gelten
AXIOME
1. $x\oplus(y\oplus z) = (x\oplus y)\oplus z$ (Assoziativität)
2. $\exists n(n\oplus x = x\oplus n = x)$ (neutrales Element)
3. $\forall x\exists y(x\oplus y=y\oplus x=n)$ (negatives bzw. inverses Element)

Eine **abelsche (kommutative) Gruppe** ist eine Gruppe für die zusätzlich gilt:
4. $\forall x\forall y\ x\oplus y = y\oplus x$ (Kommutativität)

Ein **Monoid** ist eine **„G**ruppe" ohne Axiom 3
Eine Halbgruppe ist eine „Gruppe" ohne Axiom 2 und Axiom 3
(Struktur mit binärer Operation, die das Assoziativgesetz erfüllt)

Daraus folgt trivialerweise:
Jede abelsche Gruppe ist Gruppe.
Jede Gruppe ist Monoid.
Jedes Monoid ist Halbgruppe.
In jeder Gruppe ist das Element n aus Axiom 2 eindeutig bestimmt.
In jeder Gruppe ist das neutrale Element eindeutig bestimmt.

Beispiele:
1. Die ganzen Zahlen (Z,+) bilden eine abelsche Gruppe.
2. Die ganzen Zahlen (Z\{0},*) bilden ein Monoid.
3. Die rationalen Zahlen (Q,+) bilden eine abelsche Gruppe.
4. Die reellen Zahlen (R,+) bilden eine abelsche Gruppe.
5. Die rationalen Zahlen (Q\{0},*) bilden eine abelsche Gruppe.
6. M={1,2,3}mit

op	1	2	3
1	2	3	1
2	3	1	2
3	1	2	3

   ist eine abelsche Gruppe.
7. Menge aller Restklassen mod n bzgl. der Addition
   Def: $[i]_n + [j]_n = [i+j]_n$
8. Menge aller primen Restklassen mod p (p prim) bzgl. der Multiplikation
   z. B.: $\{[1]_6, [5]_6\}$, oder
   $\{[1]_5, [2]_5, [3]_5, [4]_5\}$
9. Menge aller Bijektionen über einer Menge M bilden eine Gruppe.

Falls M = {1, 2, 3, ..., n} endlich ist, spricht man von einer Permutationsgruppe.
Für eine endliche Bijektion sind zwei Repräsentationen üblich:
(1 2 3 4 5)
(2 1 4 3 5) entspricht (1 2) (3 4)

Definition 1.2:
Eine **Unterstruktur** (**Teilalgebra**) einer Algebra (M, $\oplus$) ist eine Teilmenge N von M mit der Einschränkung der Operation $\oplus$ auf N ($\oplus_N$), so dass (N,$\oplus_N$) wieder Struktur desselben Typs ist. Man sagt N ist abgeschlossen bzgl. der Operation $\oplus$.

Beispiele:
(Z, +) ist Untergruppe von (Q, +).
(Q, +) ist Untergruppe von (R, +)
Beispiel 6 ist keine Untergruppe von (Z, +), da in Beispiel 6 eine andere Operation op vorliegt. op(3,1) = 1 aber 3+1 = 4
Die durch 3 teilbaren Zahlen (3Z, +) bestimmen eine Untergruppe von (Z, +).

Definition 1.3:
Ein **Homomorphismus** h: (M, op1) → (N, op2) ist eine Abbildung
h: M → N, die mit den Operationen verträglich ist. D.h., es ist egal, ob zuerst die Operation *op1* und dann die Abbildung *h* oder erst die Abbildung *h* und dann die entsprechende Operation *op2* angewandt wird: h(op1(x,y))=op2(h(x), h(y))

Beispiele:
1. h: Z → Z mit h(x)=3*x ist Homomorphismus von (Z,+) nach (Z,+), da
   h(+(x,y)) = 3*(x+y) = 3*x+3*y = +(3*x,3*y) = +(h(x),h(y))
2. h(Z, +) → Beispiel 6 mit h(x) = x mod 3 ist Homomorphismus, da
   h(x+y) = (x+y) mod 3 = op((x mod 3) (y mod 3)) = op(h(x), h(y))
3. h: Z → Z mit h(x) = 0 ist Homomorphismus von (Z,+) → (Z,+), da
   h(x+y) = 0 = 0 + 0 = h(x) + h(y)
4. h:Beispiel 6 → Beispiel 6 mit h(1)=1 h(2)=3 h(3)=2 ist <u>kein</u> Homomorphismus, da
   h(op(1,2)) = h(3) = 2 ≠1 = op(1,3) = op(h(1),h(2))

Definition 1.4:
Ein injektiver und surjektiver Homomorphismus heißt **Isomorphismus**. Ist h: G1 → G2 ein Isomorphismus, so betrachtet man die Algebren G1 und G2 als algebraisch gleich.

Definition 1.5:
Sind (G1, op1) und (G2, op2) algebraische Strukturen, so ist das **direkte Produkt** in folgender Weise definiert.
(G1×G2, op3), wobei ((g1,g2) op3 (g1',g2')) =((g1 op1 g1'), (g2 op2 g2'))

Definition 1.5b:
Ist (G, op) eine algebraische Struktur und R$\subseteq$G×G eine Äquivalenzrelation, so heißt R **Kongruenzrelation**, wenn R mit der Operation op kompatibel ist. D.h., wenn (a,b) $\in$R und (a',b') $\in$R dann ist auch ((a op a',b op b') $\in$R

Satz:
Jede Kongruenzrelation R einer Algebra (G,op) induziert durch elementweise Definition auf der Klasseneinteilung von R eine (Faktor-) Algebra (G/R,opR)

[a] opR [b] = [a op b]
Beweis:...

1.2 Algebren mit einer Grundmenge und zwei Operationen

Definition 1.6:
Ein **Ring** R = (R,+,*) ist eine algebraische Struktur, für die (R,+) eine kommutative Gruppe ist, (R,*) eine Halbgruppe (Assoziativität) ist und die Distributivgesetze gelten:
$\forall x \forall y \forall z \quad x*(y+z) = x*y+x*z$
$\forall x \ \forall y \ \forall z \quad (y + z) * x = y * x + z * x$

Beispiele:
1. Ring der ganzen Zahlen (Z,+,*)
2. Die natürlichen Zahlen (N,+,*) bilden keinen Ring, da kein Inverses bzgl. der Addition existiert.
3. Restklassenring (Z/(n), +, *) (Z/(n)={$[0]_n$, $[1]_n$, $[2]_n$, ..., $[n-1]_n$})

Definition 1.7:
Ein **Körper** ist eine algebraische Struktur (K,+,*), wenn (K,+,*) ein Ring ist und zusätzlich (K\{0},*) eine kommutative Gruppe ist.

Beispiele:
1. Körper der rationalen Zahlen (Q, +, *)
2. Körper der reellen Zahlen (R, +, *)
3. Körper der komplexen Zahlen (K, +, *)
4. Restklassenring (Z/(p), +, *) , wenn p eine Primzahl ist,
5. Ist p nichtprim, so liegt kein Körper vor (z.B. Z/(4)={$[0]_4$, $[1]_4$, $[2]_4$, $[3]_4$} $[2]_4$ hat kein Inverses bzgl. der Multiplikation, d.h. es gibt kein Element, so dass $[2]_4 * [x]_4=[1]_4$
6. Die Menge von Wahrheitswerten ({true, false}, and, or) ist kein Körper
7. Die Potenzmenge einer beliebigen Menge M (P(M), $\cap$, $\cup$) ist <u>kein</u> Körper. Die neutralen Elemente bzgl. $\cap$ und $\cup$ sind M bzw. $\varnothing$ ($X \cap M=X$, $X \cup \varnothing=X$). Es gibt aber nicht in jedem Fall ein negatives (inverses) Element (Für M={1,2} gibt es zu {1} kein Element X mit {1}$\cap$ X=M)

In einem Körper kann man alle normalen arithmetischen Operationen durchführen außer die Division durch "0".

Definition 1.8:
Ein **Verband** ist eine algebraische Struktur (V, op1, op2), wenn op1 und op2 kommutative und assoziative Operationen sind und zusätzlich die
Absorptions-
x op1 (x op2 y) = x und
x op2 (x op1 y) = x und die
Idempotenzgesetze
x op1 x = x und
x op2 x = x gelten.
Für jeden Verband kann man eine Halbordnung x <= y $\leftrightarrow$ x op1 y = x $\leftrightarrow$ x op2 y= y definieren. Bzgl. dieser Halbordnung existiert dann das Supremum und das Infimum zweier beliebiger Elemente des Verbandes.

Beispiele:

1. Die Potenzmenge einer beliebigen Menge M (P(M), $\cap$, $\cup$) ist ein Verband.

2. Die Menge der natürlichen Zahlen mit den Operationen ggT und kgV ist ein Verband.

Definition 1.9:

Ein Verband ist **Boole'sche Algebra (Boole'scher Verband),** wenn zusätzlich beide Distributivitätsgesetze gelten, und eine Komplementoperation comp und zwei Konstante null und eins existieren, so dass gilt:

x op1 (comp x) = null und x op2 (comp x) = eins

In jedem Booleschen Verband gilt:

x op1 null = null und x op2 eins = eins

Beweis: x op1 null = x op1 (x op1 (comp x)) = (x op1 x) op1 (comp x) = x op1 comp x = null

x op2 eins = eins wird analog bewiesen.

q.e.d.

Beispiele

1. Potenzmenge

2. Wahrheitswerte mit or und and

3. n-stellige Binärvektoren (null=(0,...,0),eins=(1,...,1)) mit or-v und and-v

1.3 Prädikatenkalkül erster Ordnung (Kurzwiederholung)

Im Prädikatenkalkül hat man eine unendliche Menge von Variablen

x,y,z,x‘,y‘,...

n-näre Funktionssymbole ($n \geq 0$)und n-äre ($n \geq 1$) Prädikatensymbole und die Symbole $\neg$ (für Negation), $\wedge$ (Konjunktion), $\vee$ (Disjunktion), $\rightarrow$ (Implikation), $\leftrightarrow$ (Äquivalenz), $\exists$ (Existenzquantor),$\forall$ (Für alle Quantor).

Mit diesen Symbolen kann man Terme und prädikatenlogische Ausdrücke erster Stufe induktiv definieren:

Definition 1.10:

Terme:

1. Jede Variable ist ein Term
2. Jedes 0-äre Funktionssymbol ist ein Term
3. Wenn $u_1,..,u_n$ ($n \geq 1$) Terme sind und f ein n-äres Funktionssymbol ist , dann ist auch $f(u_1,...,u_n)$ ein Term
4. Terme entstehen nur auf Grund von (1), (2) und (3)

Atomare Ausdrücke:

Wenn $u_1,..,u_n$ Terme sind und p ein n-äres Prädikatensymbol ist , dann ist $p(u_1,...,u_n)$ ein atomarer Ausdruck.

Ein **Ausdruck** wird wieder induktiv definiert:

1. Jeder atomare Ausdruck ist ein Ausdruck.
2. Wenn u ein Ausdruck ist dann ist auch $\neg u$ ein Ausdruck.
3. Wenn u und v Ausdrücke sind, dann sind auch $(u \wedge v)$, $(u \rightarrow v)$, $(u \leftrightarrow v)$ und $(u \vee v)$ Ausdrücke.
4. Wenn u ein Ausdruck ist und x in u vollfrei vorkommt, dann sind auch $\forall x\, u$ und $\exists x\, u$ Ausdrücke.

Versuch der Modellierung (Spezifikation) der **natürlichen Zahlen**:

Funktionssymbole: null (0-stellig), succ (Nachfolger), +(Addition), *(Multiplikation) <(Kleinerrelation):

N1: $\neg(succ(x) = null)$

N2: $succ(x) = succ(y) \rightarrow x = y$

N3: $x + 0 = x$

N4: $x + (succ(y)) = succ(x + y)$

N5: $x * null = null$

N6: $x * (succ(y)) = (x * y) + x$

N7: $\neg(x < 0)$

N8: $x < succ(y) \rightarrow x < y \vee x = y$

N9: $x < y \vee x = y \rightarrow x < succ(y)$

N10: $x < y \vee x = y \vee y < x$

Dieses Axiomensystem besitzt kein endliches Modell (N1 und N2 sichern dies ab); es ist aber nicht eindeutig in dem Sinn, dass es nur die natürlichen Zahlen als Modell besitzt. Nach dem Satz von Beth gibt es zu jeden Axiomensystem, das ein unendliches Modell besitzt zu jeder größeren Kardinalzahl ein weiteres Modell. Man kann aufgrund dieses Satzes aber auch kein anderes Axiomensystem finden, das die natürlichen Zahlen bis auf Isomorphie spezifiziert. Man müsste Quantifizierungen von Prädikaten zulassen. Damit verlässt man aber den Boden des Prädikatenkalküls erster Stufe. Aufgrund des Gödelschen Unvollständigkeitssatzes ist es weiterhin nicht möglich ein Axiomensystem mit formalem Ableitbarkeitsbegriff zu finden, so

dass genau die wahren Aussagen der natürlichen Zahlen im Sinn der Entscheidbarkeit (Berechenbarkeit) hergeleitet werden können.