Acta Informatica 1, 320—335 (1972)

Berechnung und Programm. I

V. Strassen

Eingegangen am 15. Dezember 1971

Summary. Let A be an algebraic structure and assign to each operation of A a nonnegative real number as the performance time of the operation on a given computer. The notion of a computation (or straight line program) in A yields two functions from finite subsets of A to nonnegative real numbers, namely the computational length (or complexity), and the computational depth. We characterize these functions in a quasiaxiomatic way and prove a number of general results, which will be applied to concrete problems elsewhere (see [12]—[15]).

1. Einleitung

Sei A eine partielle Algebra, d.h. eine algebraische Struktur, deren Operationen nur partiell definiert zu sein brauchen. Jeder Operation von A sei eine nichtnegative reelle Zahl zugeordnet als die zur Ausführung der Operation in einem Computer benötigte Zeit. Für endliche Teilmengen $E, F \subset A$ seien $L(F \bmod E)$ bzw. $T(F \bmod E)$ die zur Berechnung aller Elemente von F ausgehend von den Elementen von E bei optimalem Vorgehen benötigten Zeiten, wobei der Computer seriell bzw. parallel arbeitet.

In dieser Abhandlung werden die Funktionen L und T „axiomatisch" charakterisiert und es werden einige einfache, technische Sätze über L und T bewiesen. Die Charakterisierungen von L und T erweisen sich schon beim Beweis dieser Sätze als nützlich. Ihre eigentliche Bedeutung liegt aber darin, daß sie eine allgemeine Methode liefern, um untere Schranken für L und T zu gewinnen (diese Methode wurde implizit schon oft verwandt).

Die formale Definition von L und T fußt auf dem Berechnungsbegriff, für den wir zwei äquivalente Definitionen geben. Die eine ist eine naheliegende Verallgemeinerung der in Ostrowskis Pionierarbeit [10] auftretenden Begriffsbildungen. Man findet im wesentlichen die gleiche Definition bei Winograd [16] (s. auch Belaga [1]). Die andere ist algebraischer Natur, weniger intuitiv und dafür in vielen Fällen handlicher.

Für die Berechnung von Funktionen scheint der Berechnungsbegriff zu speziell. da er die Möglichkeit von Verzweigungen nicht berücksichtigt. Wir zeigen im 2. Teil dieser Arbeit, daß für eine große Klasse von numerischen Problemen (z.B. Berechnung von Polynomfunktionen oder von rationalen Funktionen bei unendlichem Konstantenkörper) die Verwendung von Verzweigungen keine Erhöhung der Rechengeschwindigkeit zur Folge hat, wenn man von einer „dünnen" Menge von Inputs absieht.

In § 2 erinnern wir an die wichtigsten mit dem Begriff der Palgebra (= partiellen Algebra) zusammenhängenden Definitionen.

In § 3 werden Berechnungen und die daraus sich ergebenden Funktionen L (Länge) und T (Tiefe) eingeführt.

In § 4 werden L und T auf einfache Weise charakterisiert und einige Sätze wie der Transitivitätssatz und der Simulationssatz bewiesen.

In § 6 wird ein äquivalenter Berechnungsbegriff (Ω-Menge) eingeführt und zur gleichzeitigen Behandlung von Länge und Tiefe z.B. logischer Netze verwandt (hier ist Länge = Kosten, Tiefe = Reaktionszeit). Dabei tritt auch der axiomatische Charakter der Charakterisierung von L und T in § 4 deutlich hervor.

In § 7 werden Klassen von Palgebren in algebraisch geometrischer Terminologie studiert. Die Anwendung von Begriffsbildungen der algebraischen Geometrie scheint mir fruchtbar. Wir bringen allerdings nur so viel, wie im folgenden Paragraphen gebraucht wird. Meine Kenntnisse über Palgebren stammen aus Kerkhoff [5].

In § 8 erläutern wir den Zusammenhang von Berechnung und Programm.

Der vorliegende erste Teil der Arbeit besteht aus den §§ 1–4. Seine Lektüre erfordert mit Ausnahme der Beispiele keine besonderen Vorkenntnisse (Satz-Def. 8 von § 2 wird in diesem Teil nicht gebraucht).

Wir bezeichnen die Menge der natürlichen Zahlen einschließlich 0 mit $\mathbb{N}$, ausschließlich 0 mit $\mathbb{N}'$, die Menge der reellen Zahlen mit $\mathbb{R}$, die der nichtnegativen reellen Zahlen einschließlich ∞ mit $[0, \infty]$. $f\colon A \rightarrowtail B$ bedeutet, daß f eine partielle Abbildung von A nach B ist, d.h. eine Abbildung eines Teils Def (f) von A nach B. Imf bezeichnet die Menge der Bildpunkte von f. Ist $\mathfrak{a} = \langle a_1, \ldots, a_s \rangle$ eine endliche Folge, so ist also $\mathrm{Im}\,\mathfrak{a} = \{a_1, \ldots, a_s\}$. Ist $f\colon A \to B$, so bezeichnet f^n die von f induzierte Produktabbildung $A^n \to B^n$ (analog für partielles f). $\#F$ ist die Mächtigkeit von F. $X \sqcup Y$ bezeichnet die disjunkte Vereinigung von X und Y. Wir tun immer so, als ob X und Y Teilmengen von $X \sqcup Y$ wären. Ist A eine Menge, so bezeichnet $\mathfrak{E}(A)$ die Menge der endlichen Teilmengen von A. Runde oder geschweifte Klammern lassen wir häufig weg.

Herrn Arnold Schönhage bin ich für seine kritische Lektüre der Arbeit sehr dankbar.

2. Palgebren

1. Def. Sei Ω eine Menge, $s\colon \Omega \to \mathbb{N}$. Dann heißt Ω (genauer $\langle \Omega, s \rangle$) ein Typ. Die Elemente von Ω heißen Operationssymbole, $s(\omega)$ heißt die Stellenzahl von ω.

2. Def. Eine partielle Abbildung $\theta\colon A^n \rightarrowtail A$ heißt n-stellige partielle Operation in A. 0-stellige partielle Operationen sind dann entweder leer oder total. Totale 0-stellige Operationen sind bis auf triviale Identifikation Elemente von A und heißen Konstante.

3. Def. Sei Ω ein Typ, A eine Menge, α eine Abbildung, die jedem $\omega \in \Omega$ eine $s(\omega)$-stellige partielle Operation in A zuordnet. Dann heißt A (genauer $\langle A, \alpha \rangle$) eine Ω-Palgebra. Die Menge A heißt der Träger und Ω der Typ der Palgebra A. A heißt total oder Ω-Algebra, wenn jedes $\alpha(\omega)$ total ist. Statt $\alpha(\omega)$ schreiben wir auch ω_A oder einfach ω.

Beispiele. Es empfiehlt sich, auftretende Typen Ω zu standardisieren. Wir wählen paarweise verschiedene Objekte $0, 1, +, -, *, {}^{-1}, /, \backslash$. Treten solche

Objekte in einem Typ auf, so wird in der Regel angenommen, daß $s(0)=s(1)=0$, $s(+)=s(-)=s(*)=s(/)=s(\backslash)=2$, $s(^{-1})=1$. Für die zugeordneten (partiellen) Operationen verwenden wir die übliche Schreibweise (dabei wird $\alpha(*)$ als Multiplikation geschrieben). Als Typ für Gruppen kann man $\{1, *, ^{-1}\}$ oder $\{1, *, /, \backslash\}$ nehmen (mit $a/b=ab^{-1}$, $a\backslash b=a^{-1}b$). Gruppen vom ersten Typ nennen wir Gruppen$_1$, Gruppen vom zweiten Typ Gruppen$_2$. Für die meisten algebraischen Untersuchungen sind die beiden Gruppenkonzepte gleichwertig. Vom Standpunkt der Berechnungsgeschwindigkeit ist dies jedoch keineswegs der Fall. Ringe haben den Typ $\{0, 1, +, -, *\}$, Körper den Typ $\{0, 1, +, -, *, /\}$. Gruppen und Ringe sind Algebren, Körper sind keine Algebren (wegen Def $(/)=A\times(A-\{0\})\neq A^2$). k-Vektorräume haben den Typ $k\sqcup\{0, +, -\}$, mit $s(\lambda)=1$ für $\lambda\in k$ (die λ zugeordnete Operation ist die Multiplikation mit λ; man unterscheide die nullstellige und die einstellige 0). Dieses Beispiel zeigt, daß man sich nicht auf endliche Ω beschränken kann. Ein k-Ring (üblicherweise k-Algebra genannt; wir wollen das Wort „Algebra" nur im Sinne von „algebraische Struktur" verwenden) ist ein k-Vektorraum zusammen mit einer bilinearen, assoziativen Multiplikation mit Eins, also eine Algebra vom Typ $k\sqcup\{0, 1, +, -, *\}$. Ein kommutativer k-Ring mit Division durch Einheiten ist ein kommutativer k-Ring, in dem die Division durch Einheiten als neue partielle Operation hinzugenommen wird. Ist jedes von 0 verschiedene Element Einheit, so sprechen wir von einem k-Körper (übliche Bezeichnung: kommutative k-Divisionsalgebra). Ein k-Körper ist also ebenso wie ein kommutativer k-Ring mit Division durch Einheiten eine Palgebra vom Typ $k\sqcup\{0, 1, +, -, *, /\}$.

4. Def. Seien A, B Ω-Palgebren. $F: A\to B$ heißt Homomorphismus von A nach B, wenn für jedes $\omega\in\Omega$ im Diagramm

$$\begin{array}{ccc} A^{s(\omega)} & \xrightarrow{f^{s(\omega)}} & B^{s(\omega)} \\ {\scriptstyle\omega}\downarrow & & \downarrow{\scriptstyle\omega} \\ A & \xrightarrow{f} & B \end{array}$$

der obere Weg eine Erweiterung des unteren ist: $f\circ\omega\subset\omega\circ f^{s(\omega)}$. f heißt strenger Homomorphismus, wenn das Diagramm kommutiert.

Für Algebren A, B ist jeder Homomorphismus streng. Die Ω-Palgebren zusammen mit den Homomorphismen bilden eine Kategorie. Unter einem Isomorphismus von Ω-Palgebren versteht man einen Isomorphismus in dieser Kategorie. Isomorphismen sind dasselbe wie strenge bijektive Homomorphismen. Homomorphismen von kommutativen k-Ringen mit Division durch Einheiten sind dasselbe wie Homomorphismen der unterliegenden k-Ringe.

5. Def. Seien $A\subset B$ Ω-Palgebren. A heißt (strenge) Unterpalgebra von B, wenn die Einbettung von A in B (strenger) Homomorphismus ist. Auch Träger von strengen Unterpalgebren nennt man häufig strenge Unterpalgebren.

Bemerkungen. Eine Unteralgebra ist immer streng. Ist $f: A\to B$ strenger Homomorphismus, so ist $\mathrm{Im}f$ strenge Unterpalgebra von B. Die Menge der

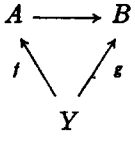
strengen Unterpalgebren einer Palgebra A ist durchschnittsabgeschlossen. Ihr Durchschnitt $\mathrm{Prim}A$, aufgefaßt wieder als Palgebra, heißt Primpalgebra von A. Es ist $\mathrm{Prim}A = \emptyset$ genau, wenn A keine totalen nullstelligen Operationen besitzt. A heißt prim, wenn $A = \mathrm{Prim}A$. Sind A prim und B Ω-Palgebren, so gibt es höchstens einen Homomorphismus $A \to B$ (denn die Menge, wo zwei Homomorphismen $A \to B$ übereinstimmen, ist eine strenge Unterpalgebra von A). Ist $E \subset A$, so heißt der Durchschnitt der E enthaltenden strengen Unterpalgebren von A die von E erzeugte Unterpalgebra von A. Ist A eine Ω-Palgebra, so sei $\tilde{A} := A \cup \{\infty\}$ mit $\infty \notin A$ (also z.B. $\infty = A$) und

$$\omega_{\tilde{A}}(\tilde{a}_1, \ldots, \tilde{a}_{s(\omega)}) := \begin{cases} \omega_A(\tilde{a}_1, \ldots, \tilde{a}_{s(\omega)}) & \text{falls definiert} \\ \infty & \text{sonst.} \end{cases}$$

$\tilde{A}$ ist eine Ω-Algebra und heißt Einpunkttotalisierung von A. A ist Unterpalgebra von A, streng genau, wenn A total ist.

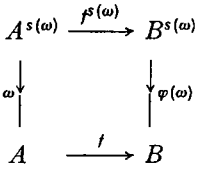
6. Def. Ist $\langle A, \alpha \rangle$ eine Ω-Palgebra, $\Omega' \subset \Omega$ und $\alpha' = \alpha | \Omega'$, so heißt $\langle A, \alpha' \rangle$ die von A induzierte Ω'-Palgebra. Umgekehrt heißt $\langle A, \alpha \rangle$ eine Ω-Expansion von $\langle A, \alpha' \rangle$.

Bemerkungen. Ist Ω ein Typ und Y eine Menge, so wird $\Omega \cup Y$ durch $s(y) = 0$ für alle $y \in Y$ zu einem Typ. Statt $\Omega \cup Y$-Palgebra sagen wir auch Ω-Palgebra über Y. Eine Ω-Palgebra über Y ist dann einfach ein Paar $\langle A, f \rangle$, wo A eine Ω-Palgebra und $f\colon Y \to A$ ist. Ein Homomorphismus $\langle A, f \rangle \to \langle B, g \rangle$ ist ein Homomorphismus $A \to B$ mit kommutativem



Die Primpalgebra von $\langle A, f \rangle$ ist das Paar $\langle B, f \rangle$, wo B die von $f(Y)$ erzeugte Unterpalgebra von A ist. Statt $\Omega \cup Y$-Expansion sagen wir auch einfach Y-Expansion. Ist $E \subset A$, so ist die kanonische E-Expansion von A durch $e_A := e$ für alle $e \in E$ definiert. Wenn wir sagen, daß wir A als Ω-Palgebra über E auffassen ($E \subset A$), so meinen wir stets die kanonische E-Expansion von A. Einen Polynomring $k[x_1, \ldots, x_n]$ können wir z.B. als k-Ring über $\{x_1, \ldots, x_n\}$ ansehen. Das bedeutet, es gibt außer den Ringoperationen noch Multiplikationen mit Elementen von k als einstellige Operationen und die x_i als nullstellige Operationen.

7. Def. Seien A eine Ω-Palgebra, B eine Ω'-Palgebra, $\varphi\colon \Omega \to \Omega'$ stellenzahlerhaltend, $f\colon A \to B$. f heißt φ-Homomorphismus von A nach B, wenn für jedes $\omega \in \Omega$ im Diagramm



der obere Weg eine Erweiterung des unteren ist.

Beispiele. Homomorphismen von Ω-Palgebren sind das gleiche wie id_Ω-Homomorphismen. Die identische Abbildung einer Ω'-Palgebra in eine Ω-Expansion ist ein φ-Homomorphismus, wenn φ die Einbettung von Ω' in Ω bezeichnet. Die Einbettung eines Integritätsbereichs in seinen Quotientenkörper ist ein φ-Homomorphismus, wo φ die Einbettung $\{0, 1, +, -, *\} \to \{0, 1, +, -, *, /\}$ ist. Entsprechendes gilt für die Einbettung einer Gruppe in ihren Gruppenring (bezüglich eines Körpers k), für die Einbettung eines Vektorraumes in seinen Tensorring, usw.

8. Satz-Def. (s. auch Cohn [2]). Es gibt eine prime Ω-Algebra $W = W(\Omega)$, die sich in jede Ω-Algebra A homomorph abbilden läßt. Ein solches W heißt Ω-Wortalgebra. Den (eindeutig bestimmten) Homomorphismus $W \to A$ bezeichnen wir mit f_A. Es ist $\mathrm{Im} f_A = \mathrm{Prim} A$. Statt $f_A(w)$ schreiben wir auch w_A. Zwei Ω-Wortalgebren sind isomorph mit einem eindeutig bestimmten Isomorphismus. Die Operationen ω_W sind injektiv und ihre Bilder $\mathrm{Im}\omega_W$ bilden eine Partition von W.

Beweis. (i) Konstruktion von W: Sei $\hat{W}$ die Menge der nichtleeren endlichen Folgen aus Ω. Für $w_1, w_2 \in \hat{W}$ sei $w_1 w_2$ ihre Konkatenation. $\hat{W}$ wird zu einer Ω-Algebra durch

$$\omega(w_1, \ldots, w_{s(\omega)}) := \omega w_1 \ldots w_{s(\omega)}.$$

$W :=$ Primalgebra von $\hat{W}$.

(ii) Eindeutige Entzifferbarkeit in W:

$$\forall w \in W \, \exists_1 \omega \, \exists_1 \langle w_1, \ldots, w_{s(\omega)} \rangle \in W^{s(\omega)} \quad w = \omega(w_1, \ldots, w_{s(\omega)}),$$

m.a.W., die Operationen ω sind injektiv und ihre Bildmengen liefern eine Partition von W (dazu nenne man w, w' vergleichbar, wenn eins Anfangsstück des andern ist. Man zeige, daß

$$\{w \in W : \exists \omega \, \exists \langle w_1, \ldots, w_{s(\omega)} \rangle [w = \omega(w_1, \ldots, w_{s(\omega)}) \,\&\, \forall \omega' \forall \langle v_1, \ldots, v_{s(\omega')} \rangle$$
$$(\omega'(v_1, \ldots, v_{s(\omega')}) \text{ vergleichbar mit } w \Rightarrow \omega = \omega' \,\&\, \langle w_1, \ldots, w_{s(\omega)} \rangle = \langle v_1, \ldots, v_{s(\omega')} \rangle)]\}$$

Unteralgebra von W ist).

(iii) Gegeben A, definiere f_A durch Induktion nach der Länge von $w \in W$ vermöge

$$f_A(\omega(w_1, \ldots, w_{s(\omega)})) = \omega(f_A(w_1), \ldots, f_A(w_{s(\omega)})).$$

Dann ist f_A Homomorphismus. Der Rest ist einfach.

3. Berechnungen

1. Def. Sei Ω ein Typ. Eine Ω-Berechnung β ist eine Folge

$$\beta = \langle \beta_1, \ldots, \beta_l \rangle$$

von Rechenschritten

$$\beta_i = \langle \omega_i, j_{i1}, \ldots, j_{is(\omega_i)} \rangle$$

mit $\omega_i \in \Omega$ und $j_{i\sigma} < i$ für alle i, σ. Zwei Ω-Berechnungen β und β' heißen isomorph ($\beta \approx \beta'$), wenn $l = l'$ und wenn es eine Permutation π mit

$$\forall i \quad \beta'_{\pi(i)} = \langle \omega_i, \pi j_{i1}, \ldots, \pi j_{is(\omega_i)} \rangle$$

gibt. $\approx$ ist eine Äquivalenzrelation.

2. Def. Sei β eine Ω-Berechnung, A eine Ω-Algebra. Die eindeutig bestimmte Folge $\langle a_1, \ldots, a_l \rangle \in A^l$ mit

$$\forall i \quad a_i = \omega_i(a_{j_{i1}}, \ldots, a_{j_{is(\omega_i)}})$$

heißt Ergebnisfolge von β in A. Ist A eine Ω-Palgebra, so verstehen wir unter der Ergebnisfolge von β in A die Ergebnisfolge von β in der Einpunkttotalisierung $\tilde{A}$ von A. a_i heißt Ergebnis von β_i und von β in A. β_i heißt ausführbar in A, wenn $a_i \neq \infty$. β heißt ausführbar in A, wenn $a_i \neq \infty$ für alle i. Sei $F \subset A$. β berechnet F in A, wenn F aus lauter Ergebnissen von β in A besteht.

Def. 1 hat syntaktischen, Def. 2 semantischen Charakter. Eine Berechnung ist über einem Typ definiert. Sie berechnet aber erst etwas, wenn eine partielle Algebra zu diesem Typ gegeben ist. Dem allgemeinen Gebrauch folgend sprechen wir zuweilen von einer Berechnung in A, wenn wir eine Berechnung über dem Typ von A meinen.

Der Berechnungsbegriff ist sehr allgemein. Die Ergebnisfolge einer ausführbaren Berechnung in einer Sprache erster Stufe mit den logischen Axiomen und den Axiomen einer Theorie T als nullstelligen Operationen und den logischen Schlußregeln als mehrstelligen partiellen Operationen ist dasselbe wie ein formaler Beweis in der Theorie T. Die Ergebnisfolge einer Berechnung in der Algebra der natürlichen Zahlen mit 1 als nullstelliger und $+$ als zweistelliger Operation ist dasselbe wie eine Additionskette im Sinne von Scholz [11] (s. auch Knuth [6], S. 398ff.). Eine Berechnung im Booleschen Verband der Wahrheitsfunktionen von n Variablen (mit den Koordinatenprojektionen als nullstelligen Operationen) ist im wesentlichen dasselbe wie ein rückkoppelungsfreies logisches Netz mit n Inputs (genauer: die Isomorphieklassen von Berechnungen im Booleschen Verband entsprechen den Isomorphieklassen von logischen Netzen; für die Definitionen s. Lupanov [7]). Auch geometrische Konstruktionen kann man als Berechnungen auffassen. Für die Numerik besonders wichtig sind Berechnungen in Polynomringen und rationalen Funktionenkörpern (Ostrowski [10]).

Wir messen die Güte einer Berechnung durch ihren Zeitaufwand. Um diesen festzulegen, ordnen wir zunächst jeder Operation ω ihren Zeitaufwand $z(\omega)$ zu. Zugriffszeiten sind mit zu berücksichtigen. Um spätere Schwierigkeiten (beim Beweis der Induktionsprinzipien) zu vermeiden, machen wir über den Wertebereich von z eine Voraussetzung, die in allen praktisch interessanten Fällen (z.B. wenn Ω endlich, oder z ganzzahlig) erfüllt ist.

3. Def. Eine Abbildung $z\colon \Omega \to [0, \infty)$ heißt Operationszeit, wenn Imz mit der von $[0, \infty)$ induzierten Ordnung wohlgeordnet ist. z heißt eigentlich, wenn

$z(\omega)=0$ für 0-stellige ω. Ist β eine Ω-Berechnung, so heißt

$$L(z|\beta):=\sum_{i=1}^{l} z(\omega_i)$$

die Länge von β (bez. z). Die Tiefe $T(z|\beta)$ von β wird induktiv durch

$$t_i=z(\omega_i)+\max_{1\leqq\sigma\leqq s(\omega_i)} t_{j_{i\sigma}},$$

$$T(z|\beta)=\max_{1\leqq i\leqq l} t_i$$

definiert. Statt $L(z|\beta)$ und $T(z|\beta)$ schreiben wir auch $L(\beta)$ und $T(\beta)$.

L und T sind konstant auf jeder $\approx$ Klasse. Das folgende einfache Lemma werden wir häufig stillschweigend benutzen (zum erstenmal bei der Verwendung von min statt inf in Def. 5).

4. Lemma. Ist $X\subset[0,\infty]$ wohlgeordnet, so ist auch

$$Y:=\bigcup_{n\geqq 1}\left\{\sum_{i=1}^{n} x_i : x\in X^n\right\}$$

wohlgeordnet.

Beweis indirekt: O.B.d.A. $0\notin X$. Sei (y_j) eine echt absteigende unendliche Folge aus Y, $y_j=\sum_{i=1}^{n_j} x_i^{(j)}$. Dann ist (n_j) beschränkt, also können wir $n_j=n$ annehmen (Übergang zu einer Teilfolge). Bei festem i ist $(x_i^{(j)})$ beschränkt, besitzt also einen Häufungspunkt und damit entweder eine streng monoton fallende oder eine schwach monoton wachsende unendliche Teilfolge. Das erste ist nicht der Fall, da X wohlgeordnet ist. Durch Übergang zu einer Teilfolge können wir also $x_i^{(j)}\leqq x_i^{(j+1)}$ erreichen, und zwar für alle i, j. Das steht aber im Widerspruch zur Wahl von (y_j).

5. Def. Sei A eine Ω-Palgebra. Für $F\in\mathfrak{P}(A)$ setzen wir

$$L(z|F)=\min\{L(z|\beta):\beta \text{ berechnet } F\}$$

$$T(z|F)=\min\{T(z|\beta):\beta \text{ berechnet } F\}$$

(bei leerer Konkurrenzmenge seien die Minima ∞). $L(z|F)$ heißt Länge oder Komplexität von F (in A und bez. z), $T(z|F)$ Tiefe von F. Eine optimale Berechnung von F (in A und bez. z) ist eine Ω-Berechnung β, die F in A berechnet und für die $L(z|\beta)=L(z|F)$ gilt. Sei $E\subset A$. Wir sagen, β berechne $F \bmod E$ in A, wenn β eine $E\sqcup\Omega$-Berechnung ist, die F in der kanonischen E-Expansion von A berechnet. $L(z|F \bmod E)$ und $T(z|F \bmod E)$ werden dann analog $L(z|F)$ und $T(z|F)$ definiert, wobei $z(e)=0$ für alle $e\in E$ angenommen wird.

Wir benutzen zahlreiche Varianten der obigen Bezeichnungen, z.B. $L(F)$, $L_A(F)$ für $L(z|F)$, oder $L(A|F)$ für $L(1_A|F)$ mit $A\subset\Omega$.

$L(F \bmod E)$ ist für endliche F und beliebige E definiert. Im folgenden werden wir aber einfachheitshalber die in einem Argument von L auftretenden Mengen stets als endlich voraussetzen.

Wir bemerken, daß $L(\cdot \bmod \cdot)$ eine informativere Funktion ist als $L(\cdot)$: Sei $A = \mathbb{N}$ mit 0 und Nachfolger als Operationen, $B = \mathbb{N}$ mit 0, Nachfolger und Vorgänger als Operationen. Dann ist $L_A(\cdot) = L_B(\cdot)$, aber $L_A(\cdot \bmod \cdot) \neq L_B(\cdot \bmod \cdot)$.

6. Satz. (i) $L(z|F \bmod E)$ und $T(z|F \bmod E)$ sind isoton in F, antiton in E, isoton und positiv homogen in z. Ferner gilt

$$L(E \bmod E) = T(E \bmod E) = 0.$$

(ii) $$T \leqq L$$

(iii) $$T(F \bmod E) = \max_{a \in F} T(a \bmod E).$$

Beweis. (iii) O.B.d.A. $E = \emptyset$. Es genügt dann,

$$T(F \cup F') \leqq \max\{T(F), T(F')\}$$

zu zeigen. $\beta = \langle \beta_1, \ldots, \beta_l \rangle$ berechne F mit $T(\beta) = T(F)$, $\beta' = \langle \beta'_1, \ldots, \beta'_{l'} \rangle$ berechne F' mit $T(\beta') = T(F')$. Sei β'' durch

$$\beta''_i = \beta_i \qquad \text{für} \quad i \leqq l,$$

$$\beta''_{l+i} = \langle \omega'_i, j'_{i1} + l, \ldots, j'_{is(\omega'_i)} + l \rangle \qquad \text{für} \quad 1 \leqq i \leqq l'$$

definiert. β'' berechnet dann $F \cup F'$ und es ist

$$T(\beta'') = \max\{T(\beta), T(\beta')\} = \max\{T(F), T(F')\}.$$

7. Kor. Sei $F \in \mathscr{E}(\operatorname{Prim} A)$. Dann gibt es ein β, welches F berechnet (die Umkehrung ist klar).

Beweis. Sei $z = 1$. $B := \{a \in A : T(a) < \infty\}$ ist eine strenge Unterpalgebra von A, denn ist $\langle b_1, \ldots, b_s \rangle \in B^s \cap \operatorname{Def}\omega$, so folgt aus Satz 6, (iii) $T(b_1, \ldots, b_s) < \infty$. Also gibt es eine Berechnung $\beta = \langle \beta_1, \ldots, \beta_l \rangle$, die $\{b_1, \ldots, b_s\}$ berechnet. Sei b_σ Ergebnis des Rechenschritts β_{i_σ} in A. Dann ist $\langle \beta_1, \ldots, \beta_{l+1} \rangle$ mit $\beta_{l+1} = \langle \omega, i_1, \ldots, i_s \rangle$ eine Berechnung, die $\omega(b_1, \ldots, b_s)$ in A berechnet. Also ist $T(\omega(b_1, \ldots, b_s)) < \infty$. Es folgt $\operatorname{Prim} A \subset B$, d.h.

$$\forall a \in \operatorname{Prim} A, \quad T(a) < \infty,$$

also nach Satz 6

$$\forall F \in \mathscr{E}(\operatorname{Prim} A), \quad T(F) < \infty,$$

und daraus die Behauptung.

Nach Kor. 7 gilt $L(F) = \infty$ für $F \notin \mathscr{E}(\operatorname{Prim} A)$. Andererseits ist $L(F) = L_{\operatorname{Prim} A}(F)$ für $F \in \mathscr{E}(\operatorname{Prim} A)$, denn eine Ω-Berechnung hat in A die gleiche Ergebnisfolge wie in $\operatorname{Prim} A$. Das bedeutet, daß man sich bei vielen Betrachtungen auf den Fall primer A beschränken kann. Ebenso kann man häufig annehmen, daß A total ist, denn aus den Definitionen folgt $L_A(F) = L_{\tilde{A}}(F)$ für $F \in \mathscr{E}(\operatorname{Prim} A)$. Schließlich kann man die Beweise von Aussagen über $L(F \bmod E)$ auf den Fall $E = \emptyset$ zurückführen, indem man zur kanonischen E-Expansion von A übergeht. Diese Reduktion ist gegebenenfalls vor der Reduktion auf prime Algebren durchzuführen. Analoge Bemerkungen gelten für T.

4. Charakterisierung von L und T

Sei Ω ein Typ, A eine Ω-Palgebra und z eine Operationszeit.

1. Def.

$$\lambda\colon \mathscr{E}(A)\to[0,\infty]$$

heißt L-Schranke, wenn

$$\lambda(\emptyset)=0$$

und

$$\lambda(F\cup\{\omega\boldsymbol{a}\})\leqq\lambda(F\cup\operatorname{Im}\boldsymbol{a})+z(\omega)$$

für beliebige $F\in\mathscr{E}(A)$, $\omega\in\Omega$ und $\boldsymbol{a}\in\operatorname{Def}\omega$.

2. Satz. L ist die größte L-Schranke.

Beweis. O.B.d.A. A prim.

(i) L ist L-Schranke: $\beta=\langle\beta_1,\dots,\beta_l\rangle$ berechne $F\cup\operatorname{Im}\boldsymbol{a}$ mit $L(\beta)=L(F\cup\operatorname{Im}\boldsymbol{a})$. Sei $\boldsymbol{a}=\langle a_1,\dots,a_s\rangle$ und seien $a_1,\dots,a_s$ die Ergebnisse von $\beta_{i_1},\dots,\beta_{i_s}$. Setze

$$\beta_{l+1}=\langle\omega,i_1,\dots,i_s\rangle.$$

$\beta'=\langle\beta_1,\dots,\beta_{l+1}\rangle$ berechnet dann $F\cup\{\omega\boldsymbol{a}\}$ und es ist

$$L(\beta')=L(\beta)+z(\omega),$$

also

$$\begin{aligned}L(F\cup\{\omega\boldsymbol{a}\})&\leqq L(\beta')\\&=L(\beta)+z(\omega)\\&=L(F\cup\operatorname{Im}\boldsymbol{a})+z(\omega).\end{aligned}$$

(ii) λ L-Schranke $\Rightarrow\lambda\leqq L$: Es genügt zu zeigen

$$\forall F\,\forall\beta\ \ (\beta\text{ berechnet }F\Rightarrow\lambda(F)\leqq L(\beta)).$$

Wir beweisen die Aussage

$$\forall F\ \ (\beta\text{ berechnet }F\Rightarrow\lambda(F)\leqq L(\beta))$$

durch Induktion nach der Schrittzahl l von β. Der Induktionsanfang ist klar. Sei nun $\beta=\langle\beta_1,\dots,\beta_l\rangle$ gegeben. Wir können annehmen, daß F nicht schon durch $\langle\beta_1,\dots,\beta_{l-1}\rangle$ berechnet wird. Dann ist β_l ausführbar. Wir bezeichnen die Ergebnisse der Schritte $\beta_l,\beta_{\eta_{l_1}},\dots,\beta_{\eta_{l_s}}$ mit $a,a_1,\dots,a_s$ (wobei $s=s(\omega_l)$). Dann ist

$$\begin{aligned}\lambda(F)&=\lambda\big((F-\{a\})\cup\{\omega_l(a_1,\dots,a_s)\}\big)\\&\leqq\lambda\big((F-\{a\})\cup\{a_1,\dots,a_s\}\big)+z(\omega_l)\end{aligned}$$

(weil λ L-Schranke ist)

$$\leqq L(\langle\beta_1,\dots,\beta_{l-1}\rangle)+z(\omega_l)$$

(nach Induktionsvoraussetzung)

$$=L(\beta).$$

3. Def. Eine Abbildung

$$\tau\colon A\to[0,\infty]$$

heißt T-Schranke, wenn stets

$$\tau(\omega(a_1, \ldots, a_s)) \leqq \max_\sigma \tau(a_\sigma) + z(\omega)$$

für $\omega \in \Omega$, $\langle a_1, \ldots, a_s \rangle \in \mathrm{Def}\omega$ (bei leerer Konkurrenzmenge ist das maximum 0 zu setzen).

4. Satz. T ist die größte T-Schranke.

Beweis. O.B.d.A. A prim.

(i) T ist T-Schranke: Wie oben für L unter Verwendung von $T(\{a_1, \ldots, a_s\}) = \max_\sigma T(a_\sigma)$.

(ii) τ T-Schranke $\Rightarrow \tau \leqq T$: Sei $a \in A$ beliebig. β berechne a mit $T(\beta) = T(a)$. Sei $\langle a_1, \ldots, a_l \rangle$ die Ergebnisfolge von β, $\tau(a_i) = 0$ für $a_i \notin A$. Wir zeigen $\tau(a_i) \leqq t_i$ durch Induktion nach i (dann folgt $\tau(a) \leqq \max_i t_i = T(\beta) = T(a)$): Für $a_i \notin A$ ist $\tau(a_i) = 0 \leqq t_i$, für $a_i \in A$ ist

$$\begin{aligned} \tau(a_i) &= \tau(\omega_i(a_{j_{i_1}}, \ldots, a_{j_{i_s}})) \\ &\leqq \max_\sigma \tau(a_{j_{i_\sigma}}) + z(\omega_i) \\ &\leqq \max_\sigma t_{j_{i_\sigma}} + z(\omega_i) \\ &= t_i. \end{aligned}$$

Wir bringen zwei einfache Anwendungen.

5. Satz. Bei der Definition von L und T kann man sich auf ausführbare β beschränken.

Beweis. Die bisherigen Überlegungen sind ebenso bei Beschränkung auf ausführbare β gültig, insbesondere die Sätze 2 und 4.

6. Transitivitätssatz.

$$L(F \cup E \bmod D) \leqq L(F \bmod E \cup D) + L(E \bmod D)$$
$$T(a \bmod D) \leqq T(a \bmod E \cup D) + T(E \bmod D).$$

Beweis. O.B.d.A. $D = \emptyset$. Ferner können wir $E \subset \mathrm{Prim}A$ annehmen. Zu zeigen ist dann

$$L(F \cup E) - L(E) \leqq L(F \bmod E),$$
$$T(a) - T(E) \leqq T(a \bmod E).$$

Die linken Seiten sind aber bei festem E L- bzw. T-Schranken für die kanonische E-Expansion von A.

Aus dem Transititätssatz folgt durch Induktion leicht

$$L(F \bmod E) \leqq \sum_{i \leqq r} L(F_i \bmod E_i)$$
$$T(F \bmod E) \leqq \sum_{i \leqq r} T(F_i \bmod E_i),$$

falls $E_i \subset E \cup \bigcup_{j<i} (F_i \cup E_j)$, $F \subset \bigcup_{j \leqq r} (F_j \cup E_j)$.

Wir wollen nun $L(F \bmod E)$ und $T(F \bmod E)$ auch als Funktionen zweier Variablen charakterisieren.

7. Def. Eine Abbildung

$$\lambda(\cdot \bmod \cdot)\colon \mathscr{E}(A)^2 \to [0, \infty]$$

heißt relative L-Schranke, wenn die folgenden Bedingungen erfüllt sind:

(i) (Monotonie). $\lambda(F \bmod E)$ ist isoton in F, antiton in E, ferner $\lambda(E \bmod E) = 0$.

(ii) (Transitivität). $\lambda(F \cup E \bmod D) \leqq \lambda(F \bmod E \cup D) + \lambda(E \bmod D)$.

(iii) (Normierung). $\forall \omega\ \forall \boldsymbol{a} \in \mathrm{Def}\,\omega\ \lambda(\omega \boldsymbol{a} \bmod \mathrm{Im}\,\boldsymbol{a}) \leqq z(\omega)$.

Gilt außerdem

(iv) (Parallelität). $\lambda(F \bmod E) = \max\limits_{a \in F} \lambda(a \bmod E)$,

so heißt λ relative T-Schranke.

8. Satz. $L(\cdot \bmod \cdot)$ ist die größte relative L-Schranke. $T(\cdot \bmod \cdot)$ ist die größte relative T-Schranke.

Beweis. Daß $L(\cdot \bmod \cdot)$ relative L-Schranke ist, ist nach dem bisher bewiesenen klar. Sei nun λ relative L-Schranke und sei $E \in \mathscr{E}(A)$. Wir zeigen: $\lambda(\cdot \bmod E)$ ist L-Schranke für die kanonische E-Expansion von A. Es gilt

$$\lambda(\emptyset \bmod E) \leqq \lambda(E \bmod E) = 0.$$

Ist $e \in E$, so gilt

$$\begin{aligned} \lambda(F \cup \{e\} \bmod E) &\leqq \lambda(F \cup \{e\} \bmod F \cup E) + \lambda(F \bmod E) \\ &\leqq \lambda(F \cup E \bmod F \cup E) + \lambda(F \bmod E) \\ &\leqq \lambda(F \bmod E). \end{aligned}$$

Ist $\omega \in \Omega$, so gilt

$$\begin{aligned} \lambda(F \cup \{\omega \boldsymbol{a}\} \bmod E) &\leqq \lambda(\{\omega \boldsymbol{a}\} \cup F \cup \mathrm{Im}\,\boldsymbol{a} \bmod E) \\ &\leqq \lambda(\omega \boldsymbol{a} \bmod F \cup \mathrm{Im}\,\boldsymbol{a} \cup E) + \lambda(F \cup \mathrm{Im}\,\boldsymbol{a} \bmod E) \\ &\leqq z(\omega) + \lambda(F \cup \mathrm{Im}\,\boldsymbol{a} \bmod E). \end{aligned}$$

Die zweite Aussage des Satzes beweist man analog, unter Benutzung der Parallelität.

Die definierenden Eigenschaften von relativen L- und T-Schranken sind mit Ausnahme der Normierung unabhängig von z und von der algebraischen Struktur von A.

9. Def. Sei A irgendeine Menge.

$$\lambda(\cdot \bmod \cdot)\colon \mathscr{E}(A)^2 \to [0, \infty]$$

heißt L-artig, wenn Definition 7 (i) und (ii) erfüllt sind. Gilt außerdem (iv), so heißt λ T-artig.

10. Satz. (i) Sei J eine Hüllenoperation in einer Menge M. Dann ist

$$\lambda(F \bmod E) := \min\{\#U : F \subset J(E \cup U)\}$$

eine L-artige Funktion $\mathscr{E}(M)^2 \to [0, \infty]$.

(ii) ist $f\colon \mathscr{E}(M)\to\mathscr{E}(N)$ vereinigungstreu und $\lambda\colon \mathscr{E}(N)^2\to[0,\infty]$ L-artig (T-artig), so ist auch $\lambda(f(\cdot)\bmod f(\cdot))$ L-artig (T-artig).

Den einfachen Beweis überlassen wir dem Leser. Es ist übrigens nicht schwer zu zeigen, daß man durch Ausüben aller vereinigungstreuen Mengenabbildungen auf die Funktionen $L(\cdot \bmod \cdot)$ für alle möglichen Ω, A, z genau die Klasse der L-artigen Funktionen bekommt (entsprechend für T-artige Funktionen). Wir geben eine Anwendung der vorangehenden beiden Sätze:

11. Simulationssatz. Seien A eine Ω-Palgebra, B eine Ω'-Palgebra, z bzw. z' Operationszeiten für Ω bzw. Ω', $f\colon \mathscr{E}(A)\to\mathscr{E}(B)$ vereinigungstreu, $c\geqq o$. Aus

$$\forall\omega\ \forall \boldsymbol{a}\in\mathrm{Def}\omega,\quad L_B\big(f\{\omega\boldsymbol{a}\}\bmod f(\mathrm{Im}\,\boldsymbol{a})\big)\leqq c\,z(\omega)$$

folgt

$$L_B\big(f(F)\bmod f(E)\big)\leqq c\,L_A(F\bmod E)$$

für alle E, F. Aus

$$\forall\omega,\boldsymbol{a}\quad T_B\big(f\{\omega\boldsymbol{a}\}\bmod f(\mathrm{Im}\,\boldsymbol{a})\big)\leqq c\,z(\omega)$$

folgt

$$T_B\big(f(F)\bmod f(E)\big)\leqq c\,T_A(F\bmod E).$$

Beweis. O.B.d.A. $c=1$. $L_B(f(\cdot)\bmod f(\cdot))$ ist L-artig, also eine L-Schranke. $T_B(f(\cdot)\bmod f(\cdot))$ ist T-artig, also eine T-Schranke.

12. Kor. Seien A eine Ω-Palgebra, B eine Ω'-Palgebra, $\varphi\colon\Omega\to\Omega'$ stellenzahlerhaltend, $f\colon A\to B$ ein φ-Homomorphismus, z' Operationszeit für Ω'. Dann gilt für $E, F\in\mathscr{E}(A)$

$$L\big(z'|f(F)\bmod f(E)\big)\leqq L(z'\circ\varphi|F\bmod E)$$

$$T\big(z'|f(F)\bmod f(E)\big)\leqq T(z'\circ\varphi|F\bmod E).$$

Insbesondere sind L und T invariant unter Automorphismen.

Dieses Korollar läßt sich auch sehr leicht direkt beweisen.

13. Def. Gilt mit den Bezeichnungen von Kor. 12

$$L\big(z'|f(F)\bmod f(E)\big)=L(z'\circ\varphi|F\bmod E),$$

so heißt f L-autark für $F\bmod E$ (bez. z'). Ist speziell $E=\emptyset$, so heißt f L-autark für F. f heißt L-biautark, wenn

$$\forall E,F\quad f\ L\text{-autark für } F\bmod E.$$

f heißt L-autark, wenn

$$\forall F\quad f\ L\text{-autark für } F.$$

Analog für T.

Beispiele. 1. Sei R ein kommutativer k-Ring, x eine Unbestimmte über R. Wir fassen den Polynomring $R[x]$ als k-Ring über $\{x\}$ auf. Dann ist also $\Omega=\{0,1,+,-,*\}\sqcup k$ der Typ von R, $\Omega'=\Omega\cup\{x\}$ der Typ von $R[x]$. φ sei die Einbettung $\Omega\to\Omega'$, f die Einbettung $R\to R[x]$. Offenbar ist f ein φ-Homomorphismus. f ist L-biautark bezüglich jeder eigentlichen Operationszeit. Seien nämlich $\psi\colon\Omega'\to\Omega$ Linksinverse von φ mit $x\mapsto 0$, $g\colon R[x]\to R$ Linksinverse von

f mit $x \mapsto 0$. Anwendung von Kor. 12 auf den ψ-Homomorphismus g liefert für $F, E \in \mathscr{E}(R)$ die gewünschte Ungleichung.

2. Seien $k \subset K$ unendliche Körper. Wir fassen K als Körper über k auf (Typ: $\Omega = \{+, -, *, /\} \sqcup k$). Sei $K(x)$ eine einfach transzendente Erweiterung von K, aufgefaßt als Körper über $k \cup \{x\}$ (Typ: $\Omega' = \Omega \cup \{x\}$). Dann ist die Einbettung $K \to K(x)$ L-biautark bezüglich jeder eigentlichen Operationszeit. Denn seien $F, E \in \mathscr{E}(K)$ und β eine optimale ausführbare Berechnung von $F \bmod E$ in $K(x)$. Da k unendlich ist, gibt es ein $\lambda \in k$ so, daß alle von 0 verschiedenen Ergebnisse von β an der Stelle λ nichtverschwindende (gekürzte) Zähler und Nenner haben, also Einheiten im lokalen Ring $\mathcal{O}_\lambda$ des Punktes λ sind. Fassen wir $\mathcal{O}_\lambda$ als kommutativen Ring über $k \cup \{x\}$ mit Division durch Einheiten auf, so berechnet β $F \bmod E$ auch in $\mathcal{O}_\lambda$, also

$$L_{\mathcal{O}_\lambda}(F \bmod E) \leqq L_{K(x)}(F \bmod E).$$

$\psi\colon \Omega' \to \Omega$ wirke identisch auf Ω und bilde x in λ ab. Dann ist der kanonische ψ-Homomorphismus $\mathcal{O}_\lambda \to K$ eine Linksinverse zur Einbettung $K \to \mathcal{O}_\lambda$. Kor. 12 liefert

$$L_K(F \bmod E) \leqq L_{\mathcal{O}_\lambda}(F \bmod E).$$

Ein analoges Ergebnis erhält man, wenn man K als k-Körper auffaßt und etwa $z' = 1_{\{*,/\}}$ annimmt.

3. Seien $k_0 \subset k$ unendliche Körper und entweder k rein transzendent über k_0 oder k_0 algebraisch abgeschlossen. Seien $x_1, \ldots, x_n$ Unbestimmte über k. Wir fassen $k_0(x_1, \ldots, x_n)$ als k_0-Körper, $k(x_1, \ldots, x_n)$ als k-Körper auf (also $\Omega = \{0, 1, +, -, *, /\} \sqcup k_0$, $\Omega' = \{0, 1, +, -, *, /\} \sqcup k$ mit einstelligen $\lambda \in k_0$ bzw. $\in k$). Dann ist die Einbettung

$$k_0(x_1, \ldots, x_n) \to k(x_1, \ldots, x_n)$$

L-autark für jede Operationszeit zu Ω', die auf k konstant ist. Wir zeigen dies etwa, wenn k_0 algebraisch abgeschlossen ist (der Fall, daß k rein transzendent über k_0 ist, ist etwas einfacher). Sei β eine optimale ausführbare Berechnung von $F \bmod E$ in $k(\boldsymbol{x}) = k(x_1, \ldots, x_n)$, $F, E \subset k_0(\boldsymbol{x})$. Seien $a_1, \ldots, a_r$ die von 0 verschiedenen Ergebnisse von β, $a_i = u_i / v_i$, $u_i, v_i \in k[\boldsymbol{x}]$. Die nicht verschwindenden Koeffizienten der u_i, v_i und ihre Inversen erzeugen einen k_0-Ring R mit $k_0 \subset R \subset k$. Sei

$$S = R[x_1, \ldots, x_n]\left[\frac{1}{u_1}, \frac{1}{v_1}, \ldots, \frac{1}{u_r}, \frac{1}{v_r}\right] \subset k(\boldsymbol{x}).$$

Fassen wir S als kommutativen k_0-Ring mit Division durch Einheiten auf, so berechnet β $F \bmod E$ auch in S. Also

$$L_S(F \bmod E) \leqq L_{k(\boldsymbol{x})}(F \bmod E).$$

Da R ein endlich erzeugter k_0-Integritätsbereich ist, gibt es nach Hilbert's Nullstellensatz einen Homomorphismus von k_0-Ringen $R \to k_0$, der sich zu einem Homomorphismus $R[\boldsymbol{x}] \to k_0(\boldsymbol{x})$ fortsetzt. Nach Konstruktion von R gehen die u_i, v_i dabei in von 0 verschiedene Elemente von $k_0(\boldsymbol{x})$, also in Einheiten über. Da S Quotientenring von $R[\boldsymbol{x}]$ bezüglich der von den u_i, v_i erzeugten Halb-

gruppe ist, erhalten wir einen Homomorphismus $S \to k_0(\boldsymbol{x})$, der offenbar $k_0(\boldsymbol{x})$ identisch abbildet. Korr. 12 liefert dann

$$L_{k_0(\boldsymbol{x})}(F \bmod E) \leqq L_S(F \bmod E).$$

14. Kor. Sei A eine Ω-Palgebra. Hinzunahme einer neuen partiellen Operation ω' läßt $L(\cdot \bmod \cdot)$ genau dann unverändert, wenn die Operationszeit von ω' so festgesetzt wird, daß

$$\forall \boldsymbol{a} \in \mathrm{Def}\omega' \quad L_A(\omega' \boldsymbol{a} \bmod \mathrm{Im}\,\boldsymbol{a}) \leqq z(\omega')$$

gilt. Analog für T.

Die beiden L und T charakterisierenden Sätze sind Spezialfälle zweier Induktionsprinzipien, die wir jetzt angeben wollen.

Die Aussage „A ist prim" kann man so formulieren: Ist $P \subset A$ und gilt

$$\forall \omega \quad \forall \boldsymbol{a} \in \mathrm{Def}\omega \quad (\mathrm{Im}\boldsymbol{a} \subset P \Rightarrow \omega \boldsymbol{a} \in P),$$

so ist $P = A$. Verwendung dieser Tatsache nennt man algebraische Induktion. Statt Mengen P von Elementen von A kann man auch Mengen $\mathscr{P}$ von endlichen Teilmengen von A betrachten: ist A prim, $\emptyset \in \mathscr{P}$ und gilt

$$\forall F \quad \forall \omega \quad \forall \boldsymbol{a} \in \mathrm{Def}\omega \quad (F \cup \mathrm{Im}\boldsymbol{a} \in \mathscr{P} \Rightarrow F \cup \{\omega \boldsymbol{a}\} \in \mathscr{P}),$$

so ist $\mathscr{P} = \mathscr{E}(A)$. Die folgenden beiden Sätze verbessern diese Induktionsprinzipien, indem sie deren Voraussetzungen abschwächen.

15. Satz (L-Induktion). Sei $\mathscr{P} \subset \mathscr{E}(\mathrm{Prim}\,A)$. Es gelte $\emptyset \in \mathscr{P}$ und

$$\big(L(F \cup \{\omega \boldsymbol{a}\}) = L(F \cup \mathrm{Im}\boldsymbol{a}) + z(\omega)\ \&\ F \cup \mathrm{Im}\boldsymbol{a} \in \mathscr{P}\big) \Rightarrow F \cup \{\omega \boldsymbol{a}\} \in \mathscr{P}$$

für beliebige $F \in \mathscr{P}(\mathrm{Prim}\,A)$, $\omega \in \Omega$, $\boldsymbol{a} \in \mathrm{Def}\omega$. Dann ist $\mathscr{P} = \mathscr{E}(\mathrm{Prim}\,A)$.

Beweis. Indirekt: Ein Gegenbeispiel ist ein $F \in \mathscr{E}(\mathrm{Prim}\,A) - \mathscr{P}$. Unter allen Ω-Berechnungen, die ein Gegenbeispiel berechnen, sei für β das Zahlenpaar $\langle L(z|\beta), l\rangle$ lexikographisch minimal, wobei l die Schrittzahl von β ist. Dann ist $a_l \in F$ und $L(\beta) = L(F)$ und wir haben

$$\begin{aligned} L\big((F - \{a_l\}) \cup \{\omega_l(a_{j_{l_1}}, \ldots, a_{j_{l_s}})\}\big) &= L(F) \\ &= L(\beta) = z(\omega_l) + L(\langle \beta_1, \ldots, \beta_{l-1}\rangle) \\ &\geqq z(\omega_l) + L\big((F - \{a_l\}) \cup \{a_{j_{l_1}}, \ldots, a_{j_{l_s}}\}\big). \end{aligned}$$

Da L eine L-Schranke ist, gilt auch $\leqq$ und deshalb $=$. Nach Wahl von β ist $(F - \{a_l\}) \cup \{a_{j_{l_1}}, \ldots, a_{j_{l_s}}\} \in \mathscr{P}$, also nach der Voraussetzung des Satzes auch $F = (F - \{a_l\}) \cup \{\omega_l(a_{j_{l_1}}, \ldots, a_{j_{l_s}})\} \in \mathscr{P}$, Widerspruch.

16. Satz (T-Induktion). Sei $P \subset \mathrm{Prim}\,(A)$. Es gelte stets

$$\big(T(\omega \boldsymbol{a}) = \max_{\sigma} T(a_\sigma) + z(\omega)\ \&\ \mathrm{Im}\boldsymbol{a} \subset P\big) \Rightarrow \omega(\boldsymbol{a}) \in P.$$

Dann ist $P = \mathrm{Prim}\,(A)$.

Beweis. Indirekt: O.B.d.A. A total. Unter allen Berechnungen, die ein $a \notin P$ berechnen, sei für β das Zahlenpaar $\langle T(\beta), l\rangle$ lexikographisch minimal. Dann ist

$$T(a_l) = T(\beta) \geqq t_l = z(\omega_l) + \max_\sigma t_{j_{l\sigma}}.$$

Ferner gilt $t_i \geqq T(a_i)$ für alle i (dies folgt durch Induktion nach i unter Benutzung der Tatsache, daß T eine T-Schranke ist), also

$$T(a_l) \geqq z(\omega_l) + \max_\sigma T(a_{j_{l\sigma}}).$$

Da T eine T-Schranke ist, gilt auch $\leqq$, also $=$. Nach Wahl von β sind die $a_{j_{l\sigma}} \in P$, also nach der Voraussetzung des Satzes $a_l \in P$, im Widerspruch wiederum zur Wahl von β.

Bemerkungen. 1. Die Menge der T-Schranken auf A ist abgeschlossen gegenüber den Verbandsoperationen, die Menge der L-Schranken ist abgeschlossen gegenüber Verbandsoperationen und konvexen Kombinationen.

2. Für monotone λ kann man die zweite Ungleichung in Def. 1 von § 4 durch

$$\forall F \quad \forall \omega \quad \forall \boldsymbol{a} \in \mathrm{Def}\omega \cap F^{s(\omega)} \quad \lambda(F \cup \{\omega \boldsymbol{a}\}) \leqq \lambda(F) + z(\omega)$$

ersetzen. Eine L-Schranke braucht nicht monoton zu sein, aber L ist auch die größte monotone L-Schranke.

3. L- und T-Schranken ebenso wie L- und T-Induktion sind wichtige Hilfsmittel, um L und T nach unten abzuschätzen. Wir erläutern dies an einem einfachen Beispiel: Sei $A = 2^X$, $\Omega = \{\cup,$ einpunktige Mengen$\}$, $\cup$ zweistellig, einpunktige Mengen nullstellig. Dann ist

$$L(\cup|a) = \#(a) - 1.$$

$\leqq$ ist klar. Durch L-Induktion zeigt man leicht $L(F) \geqq \#(\cup F) - \#F$. Daraus folgt $L(a) \geqq \#(a) - 1$. $\#(\cup F) - \#F$ ist übrigens keine L-Schranke. Man kann diese Funktion aber zu einer L-Schranke vergrößern: Dazu machen wir F durch Verbinden der $a, b \in F$ mit $a \cap b \neq \emptyset$ zu einem Graphen. Sei $\mathrm{Komp}(F)$ die Menge der Zusammenhangskomponenten dieses Graphen. Dann ist $\lambda(F) := \#(\cup F) - \#\mathrm{Komp}F$ eine L-Schranke.

Ebenso haben wir

$$T(\cup|a) = \lceil \lg_2 \#(a) \rceil,$$

denn $\leqq$ ist klar und $\geqq$ gilt, weil $\lg_2 \#(a)$ eine T-Schranke ist.

4. Wir haben die in $L(F \bmod E)$ und $T(F \bmod E)$ auftretenden Mengen E, F bisher stets als endlich angenommen. Für manche Betrachtungen ist es zweckmäßig, auch unendliche E, F zuzulassen. Dazu erinnern wir uns daran, daß $L(F \bmod E)$ und $T(F \bmod E)$ ursprünglich für beliebige E definiert worden sind. Wir setzen nun

$$L(F \bmod E) := \sup\{L(F_0 \bmod E) : F_0 \text{ endlich} \subset F\}$$

$$T(F \bmod E) := \sup\{T(a \bmod E) : a \in F\}$$

für beliebige $F, E \subset A$. Man sieht leicht, daß Satz 6 von § 3 (mit sup anstelle von max) ebenso wie der Transitivitätssatz und die beiden Korollare des Simula-

tionssatzes für die so erweiterten Funktionen richtig bleiben. Als Beispiel skizzieren wir den Beweis der Transitivitätseigenschaft von L: O.B.d.A. $D=\emptyset$. Sei $r<L(F\cup E)$ beliebig und seien E_0 endlich $\subset E$, F_0 endlich $\subset F$ mit $r<L(F_0\cup E_0)$ und $L(F_0 \bmod E_0)=L(F_0 \bmod E)$. Dann ist

$$\begin{aligned} r &< L(F_0\cup E_0)\\ &\leqq L(F_0 \bmod E_0)+L(E_0)\\ &= L(F_0 \bmod E)+L(E_0)\\ &\leqq L(F \bmod E)+L(E). \end{aligned}$$

Weil r beliebig ist, folgt die Behauptung.

Literatur

1. Belaga, E. G.: Evaluation of polynomials of one variable with preliminary processing of the coefficients. Problemy Kibernetiki 5, 7—15 (1961).
2. Cohn, P. M.: Universal algebra. New York: Harper & Row 1965.
3. Engeler, E.: Formal languages. Chicago: Markham Publ. Co. 1968.
4. Engeler, E.: Introduction to the theory of computation. Part 2: Recursive functions. Lecture Notes 1970/71. Minneapolis: School of Mathematics, University of Minnesota.
5. Kerkhoff, R.: Gleichungsdefinierbare Klassen partieller Algebren. Math. Ann. **185**, 112—133 (1970).
6. Knuth, D. E.: The art of computer programming. Vol. II: Seminumerical algorithms. Addison-Wesley 1969.
7. Lupanov, O. B.: Ueber die Synthese einiger Klassen von Steuersystemen. Probleme der Kybernetik 7, 20—63. Berlin: Akademie-Verlag 1966.
8. Mumford, D.: Introduction to algebraic geometry. Harvard Lecture Notes.
9. Neumann, B. H.: Special topics in algebra: Universal algebra. Lectures delivered in the Fall Semester 1961/62. New York: Courant Inst. of Math. Sci. 1962.
10. Ostrowski, A. M.: On two problems in abstract algebra connected with Horner's rule. Studies in Mathematics and Mechanics, 40—48. New York: Academic Press 1954.
11. Scholz, A.: Jahresbericht der deutschen Mathematiker-Vereinigung, class II, **47**, 41—42 (1937).
12. Strassen, V.: Evaluation of rational functions. Complexity of Computer Computations, Plenum Press 1972.
13. Strassen, V.: Die Berechnungskomplexität von elementarsymmetrischen Funktionen und von Interpolationskoeffizienten. Numerische Mathematik, Frühjahr 1973 (?).
14. Strassen, V.: Vermeidung von Divisionen. Crelle Journal fur die reine und angew. Mathematik 1973 (?).
15. Strassen, V.: Berechnungen in partiellen Algebren endlichen Typs. Computing 1972/73 (?).
16. Winograd, S.: On the number of multiplications necessary to compute certain functions. Com. PA Math. XXIII/2, 165—179 (1970).

Prof. Dr. Volker Strassen
Seminar für angewandte Mathematik
Universität Zürich
Freie Straße 36
CH-8032 Zürich
Schweiz