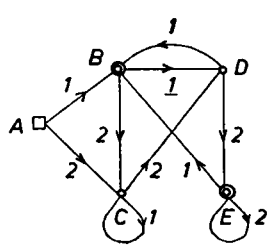
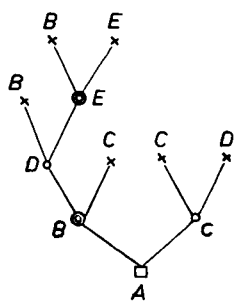
Mathematische Theorie des Verhaltens endlicher Automaten*)

Von J. Richard Büchi**)

Der Begriff des endlichen Automaten entstand als mathematische Abstraktion der deterministischen-diskreten-sequentiellen Systeme, wie es z. B. die modernen Rechenanlagen sind. Das Charakteristische am Funktionieren solcher Systeme liegt in der Rückkoppelung oder Selbst-Steuerung. Die Theorie der reinen Schaltungen (Boolesche Algebra) genügt nicht zur Erfassung dieses Phänomens und muß erweitert werden zur Theorie der endlichen Automaten (Kleenesche Algebra), die geradezu als Theorie der Schaltung durch Rückkoppelung bezeichnet werden kann. Es ist zu hoffen, daß eine streng mathematische Entwicklung von Begriffen und Sätzen über endliche Automaten auch dem Praktiker einen Einblick in das Verhalten und die Möglichkeiten digitaler Systeme gewährt, der sich dem nur empirischen Probieren auf dem Gebiete der Konstruktion und des Gebrauches von Schaltwerken komplementär zur Seite stellt. Allerdings ist es fraglich, ob die schon vorliegende Theorie im mehr naiven direkten Sinn praktisch anwendbar sei. Andererseits aber werden leistungsfähigere und vor allem neuartige Systeme schon in nächster Zukunft nur entstehen können auf Grund tiefgreifender Einsichten von allgemeiner Natur, wie sie nur bei der konsequenten Entwicklung mathematischer Theorien entstehen. Es wäre daher wünschenswert, daß sich ein weiter Kreis mathematisch denkender Forscher der verschiedensten Richtungen mit endlichen Automaten, Turing-Maschinen und ähnlichen Strukturen beschäftigte, und daß in Zukunft diese Dinge nicht nur einigen Logikern und vielen Dilettanten überlassen blieben. Seit einiger Zeit ist ein großes Gewimmel von Schlagwörtern (wie etwa Selbstreproduzierende, Selbstorganisierende, Lernende Systeme, Operations Research, Communication Science usw.) charakteristisch für einen ganzen Komplex von Aktivitäten, der sich um die modernen Rechenanlagen entwickelt hat. Ob es dabei immer bei großen Worten und anregenden Spekulationen bleiben soll? Daß das nicht so zu sein braucht, zeigt das Beispiel des Wörtchens „Verhalten". Im Folgenden werden wir sehen, daß sich diesem, wenigstens mit Bezug auf eine ganz einfache Sorte von Systemen, eine exakte Bedeutung zulegen läßt, die dann auch Anlaß gibt zu einer fruchtbaren Theorie.

	A	B	C	D	E
1	B	D	C	B	B
2	C	C	D	E	E
W	F	T	F	F	T





(a) Transit-Tafel von $\mathfrak{A}_0$ (b) Transit-Graph von $\mathfrak{A}_0$ (c) Transit-Baum von $\mathfrak{A}_0$

Bild 1

Ein Automat mit k Eingabezuständen ist ein algebraisches System $\mathfrak{A} = \langle \underline{S}, f_i, \ldots, f_k, \underline{W} \rangle$ bestehend aus einer Menge $\underline{S}$, deren Elemente die Zustände von $\mathfrak{A}$ heißen, einem Element A von $\underline{S}$ genannt Anfangszustand, Abbildungen f_i von $\underline{S}$ in $\underline{S}$ genannt Transit-Operatoren und einer Teilmenge $\underline{W}$ von $\underline{S}$, genannt die Ausgabe von $\mathfrak{A}$. Die Eingabezustände werden durch die Symbole $1, 2, \ldots, k$ bezeichnet, jeder von ihnen entspricht einem Transit-Operator von $\mathfrak{A}$. Der Automat heißt endlich, wenn die Menge $\underline{S}$ seiner Zustände endlich ist.

Ein Beispiel eines endlichen Automaten $\mathfrak{A}_0$ mit zwei Eingabezuständen ist durch Bild 1(a) gegeben. Seine Zustände sind A, B, C, D und E. Die Tafel ist so zu verstehen, daß z. B. $f_1 B = D$, $f_2 B = C$, $B \in \underline{W}$ da $\underline{W}(B) = T$, $C \notin \underline{W}$ da $\underline{W}(C) = F$. In selbstsprechender Weise ist derselbe Automat $\mathfrak{A}_0$ auch durch die Bilder 1(b) oder 1(c) bestimmt. Diese graphischen Darstellungen eines endlichen Automaten sind natürlich für die Theorie überflüssig, erweisen sich aber beide als nützliche Stützen der Anschauung. Auf Eingabe etwa des Signals 1121 reagiert der Automat $\mathfrak{A}_0$ indem er vom Anfangszustand A ausgehend sukzessiv die Zustände $f_1 A = B$, $f_1 B = D$, $f_2 D = E$, $f_1 E = B$ durchläuft. Der schlußendliche Zustand B heißt die interne Reaktion von $\mathfrak{A}_0$ auf das Eingabesignal 1121 und sei mit $\mathfrak{A}_0(1121)$ bezeichnet. Das Signal 1121 erregt die Ausgabe

*) Auf Einladung der Tagungsleitung gehaltener Hauptvortrag.

**) University of Michigan, Ann Arbor und Gutenberg-Universität, Mainz.

von $\mathfrak{A}_0$, weil $\mathfrak{A}_0(1121) \in \underline{W}$. Hingegen gilt z. B. $\mathfrak{A}_0(212) \notin W$, also erregt das Signal 212 die Ausgabe von $\mathfrak{A}_0$ nicht. Genauer wird die Arbeitsweise eines Automaten $\mathfrak{A}$ mit k Eingabezuständen so definiert:

Die Wörter über dem Alphabet $1, \ldots, k$ heißen die Eingabesignale von $\mathfrak{A}$. Sie bilden die Menge N_k, zu der auch das leere Wort o gerechnet wird. Die interne Reaktion $\mathfrak{A}(x)$ ist die für jedes $x \in N_k$ durch folgende einfache Rekursion definierte Funktion;

$$\mathfrak{A}(o) = A$$
$$\mathfrak{A}(x\,i) = f_i\,\mathfrak{A}(x) \quad \text{für} \quad i = 1, \ldots, k\,.$$

Für jedes Eingabesignal x bestehen nun folgende zwei Alternativen

$\mathfrak{A}(x) \in \underline{W}$: x erregt die Ausgabe von $\mathfrak{A}$

$\mathfrak{A}(x) \notin \underline{W}$: x erregt die Ausgabe von $\mathfrak{A}$ nicht.

Ein Automat $\mathfrak{A}$ ist also die mathematische Abstraktion eines konkreten Systems, dessen Zweck es ist, die Eingabesignale in zwei komplementäre Mengen aufzulösen. Allerdings spielen in dieser Hinsicht nur endliche Automaten eine Rolle, und auf solche werden wir uns daher im folgenden konzentrieren. Dabei handelt es sich aber nicht darum, über diese und jene endliche Automaten Aussagen adhoc zu machen. Vielmehr soll eine allgemeine mathematische Theorie, bestehend aus Definitionen, Beweisen und Sätzen, entwickelt werden, mit dem Zweck, das Verhalten endlicher Automaten verstehen zu lernen. Dazu tut es vor allem not, geeignete Konzepte durch präzise Definitionen hervorzuheben. Wir beginnen mit der von KLEENE [10] stammenden Definition des fundamentalen Begriffs des Verhaltens.

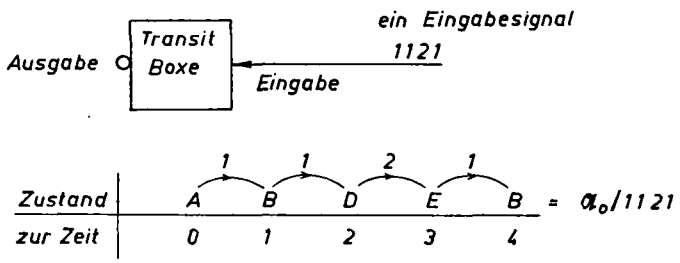


Bild 2

Seien $\mathfrak{A} = \langle \underline{S}, A, f_1, \ldots, f_k, \underline{W} \rangle$ und $\mathfrak{B} = \langle \underline{T}, B, g_1, \ldots, g_k, \underline{V} \rangle$ zwei Automaten. Man wird sagen „$\mathfrak{A}$ verhält sich gleich wie $\mathfrak{B}$", wenn die beiden Automaten auf gleiche Eingabesignale mit gleicher Ausgabe reagieren, d. h., wenn für jedes x aus N_k gilt, $\mathfrak{A}(x) \in \underline{W}$ genau dann, wenn $\mathfrak{B}(x) \in \underline{V}$. Diesen Sachverhalt kann man aber auch so ausdrücken:

$$\{x \,|\mathfrak{A}(x) \in \underline{W}\} = \{x|\ \mathfrak{B}(x) \in \underline{V}\}\,.$$

Es ist daher zweckmäßig, die Menge $\{x \,|\mathfrak{A}(x) \in \underline{W}\}$ das Verhalten von $\mathfrak{A}$ zu nennen und mit $v\,r\,h(\mathfrak{A})$ zu bezeichnen. Damit kann nun der Zweck unserer Theorie schon ziemlich scharf formuliert werden.

Hauptaufgabe: Sei Π_k die Menge aller Verhalten endlicher Automaten mit k Eingabezuständen. Es ist die Art derjenigen Teilmengen $\beta \subseteq N_k$ zu erforschen, die zu Π_k gehören. Auch sind Eigenschaften von Π_k zu untersuchen. Insbesondere gilt es Kriterien zu finden, die für irgendwelches $\beta \subseteq N_k$ aussagen, ob β zu Π_k gehört oder nicht gehört.

Zunächst ist zu bemerken, daß nur abzählbar viele der Teilmengen von N_k durch endliche Automaten realisierbar sind. Fernerhin sind diese Mengen rekursiv; ein endlicher Automat $\mathfrak{A}$ präsentiert ja geradezu ein effektives Verfahren, das darüber entscheidet, ob ein vorgelegtes $x \in N_k$ zu $v\,r\,h(\mathfrak{A})$ gehört. Es gibt aber andererseits ganz einfache rekursive Teilmengen von N_k, die nicht das Verhalten eines endlichen Automaten sind. Z. B. zeigt man leicht, daß die Menge $\{yy|y \in N_2\}$, bestehend aus allen Wörtern aus N_2, die aus zwei gleichen Stücken zusammengesetzt sind, nicht zu Π_2 gehört.

Gegenüber den in der Literatur vorkommenden Varianten hat unsere Definition der Automaten den Vorteil, daß so fundamentale Begriffe wie Homomorphie, direktes Produkt und Kongruenz gleich aus der abstrakten Algebra übernommen werden können. Damit ist dann erstens eine systematische Strukturtheorie der Automaten eröffnet und zweitens ein Beitrag zum Hauptproblem gewonnen. Auch die Resultate von MOORE [13] über minimale Automaten ergeben sich sozusagen als Beiprodukt. Diese Dinge können in Kürze wie folgt angedeutet werden. Dabei wollen wir uns auf solche Automaten beschränken, in welchen die Menge $\underline{S}$ aller Zustände vom Anfangszustand A durch die Transit-Operatoren erzeugt wird. Von A aus nicht „erreichbare" Zustände haben ja keinen Einfluß auf das Verhalten von $\mathfrak{A}$.

Eine Abbildung h von $\underline{S}$ auf $\underline{T}$ heißt Homomorphie des Automaten $\mathfrak{A} = \langle \underline{S}, A, f_1, \ldots, f_k, \underline{W} \rangle$ auf $\mathfrak{B} = \langle \underline{T}, B, g_1, \ldots, g_k, \underline{V} \rangle$ wenn $h\,A = B$, $h(f_i\,X) = g_i(h\,X)$ und $(X \in \underline{W}) \leftrightarrow (h\,X \in \underline{V})$. Bedeutet $\mathfrak{B} \leqq \mathfrak{A}$, daß $\mathfrak{B}$ homomorphes Bild von $\mathfrak{A}$ ist, dann gilt

$$\mathfrak{B} \leqq \mathfrak{A} \rightarrow v\,r\,h(\mathfrak{A}) = v\,r\,h(\mathfrak{B})$$

$$(\exists\, \mathfrak{C})\,(\mathfrak{A} \leqq \mathfrak{C} \wedge \mathfrak{B} \leqq \mathfrak{C}) \leftarrow v\,r\,h\,(\mathfrak{A}) = v\,r\,h\,(\mathfrak{B})$$

Für jedes $\beta \subseteq N_k$ ist die Menge V_β aller Automaten vom Verhalten β ein vollständiger Verband bezüglich der Ordnungsrelation $\leqq$. Dieser Strukturverband $(V_\beta, \leqq)$ hat als gröbstes Element den freien Automaten $\langle N_k, o, \varphi_1, \ldots, \varphi_k, \beta \rangle = \mathfrak{F}_\beta$, wobei $\varphi_1\,x = x\,1, \ldots, \varphi_k\,x = x\,k$. Sein kleinstes Element ist der minimale Automat $\mathfrak{M}_\beta$ des Verhaltens β. Gibt es endliche Automaten vom Verhalten β, so liegen sie unten im Strukturverband; $\mathfrak{M}_\beta$ ist dann auch der minimale in der Zahl von Zuständen unter allen Automaten vom Verhalten β.

Bild 3 zeigt den Strukturverband bestehend aus allen homomorphen Bildern von $\mathfrak{A}_1$. Wie man dem Beispiel entnimmt, brauchen solche Verbände nicht distributiv zu sein. Es brauchen auch keine Kettensätze zu gelten, und die irreduziblen Elemente können sehr unregelmäßig angeordnet sein. Die Strukturtheorie endlicher Automaten scheint daher eine fast hoffnungslos schwierige Angelegenheit zu sein.

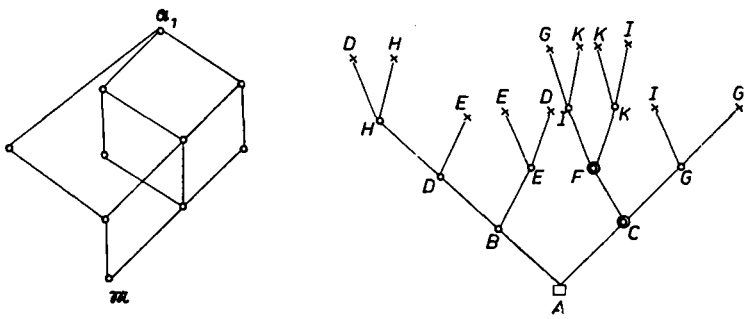


Bild 3

Eine Äquivalenzrelation $\backsim$ über der Menge $\underline{S}$ aller Zustände wird man dann eine Kongruenz des Automaten $\mathfrak{A}$ nennen, wenn gilt $(X \backsim Y) \rightarrow (f_i\,X \backsim f_i\,Y)$ und $(X \backsim Y \wedge X \in \underline{W}) \rightarrow (Y \in \underline{W})$. In bekannter Weise bildet man den Quotienten $\mathfrak{A}/\backsim$ von $\mathfrak{A}$ bezüglich einer Kongruenz. Wie man das von der Algebra her weiß, besteht nun der Strukturverband von $\mathfrak{A}$ aus allen Quotienten von $\mathfrak{A}$ und ist isomorph zum Verband der Kongruenzen von $\mathfrak{A}$. Insbesondere liefert die gröbste (das Supremum) $\simeq$ aller Kongruenzen von $\mathfrak{A}$ den minimalen Automaten des Verhaltens $v\,r\,h(\mathfrak{A})$. Daraus ergeben sich leicht effektive Methoden zur Minimierung; es handelt sich ja einfach um das Auffinden der gröbsten Kongruenz eines vorgelegten endlichen Automaten.

Bis auf Isomorphie sind also die Automaten vom Verhalten β genau die Quotienten $\mathfrak{F}_\beta/\backsim$ des freien Automaten $\mathfrak{F}_\beta$. Insbesondere erhalten wir daher die folgenden Kriterien für die Realisierbarkeit von $\beta \subseteq N_k$ als Verhalten eines endlichen Automaten:

1. Die Menge $\beta \subseteq N_k$ gehört zu Π_k genau dann, wenn der freie Automat $\mathfrak{F}_\beta$ eine Kongruenz von endlichem Index (Zahl der Kongruenzklassen) zuläßt.

2. Die Menge $\beta \subseteq N_k$ gehört zu Π_k genau dann, wenn die gröbste Kongruenz von $\mathfrak{F}_\beta$ endlichen Index hat.

Zwecks prägnanter Formulierung lohnt es sich, folgende Definitionen anzubringen. Eine Kongruenz der rechts-Nachfolgerfunktionen $\varphi_1, \ldots, \varphi_k$ nennen wir rechts-Kongruenz von N_k. Die gröbste Kongruenz von $\mathfrak{F}_\beta$ bezeichnen wir mit $\simeq(\beta)$ und nennen sie die von β induzierte rechts-Kongruenz. Der Index von $\simeq(\beta)$ heißt auch rechts-Rang von β. Obige Kriterien lassen sich nun auch so formulieren:

1′. Die Menge $\beta \subseteq N_k$ gehört zu Π_k genau dann, wenn sie Vereinigung von Kongruenzklassen einer rechts-Kongruenz von N_k von endlichem Index ist.

(II) Die Menge $\beta \subseteq N_k$ gehört zu Π_k genau dann, wenn der rechts-Rang von β endlich ist, d. h., wenn die von β induzierte rechts-Kongruenz $\simeq(\beta)$ nur endlich viele Klassen besitzt.

Mit Hilfe der Formel

(a) $$x \simeq y(\beta) \leftrightarrow (\forall\, u)\,(x\,u \in \beta \leftrightarrow y\,u \in \beta)$$

gelingt es oft, die induzierte rechts-Kongruenz genügend konkret zu ermitteln (oder doch ihren Index abzuschätzen), sodaß dann Kriterium (II) wirklich angewandt werden kann. Z. B. zeigt man so leicht, daß die induzierte rechts-Kongruenz der Menge $\{x\,x \mid x \in N_2\}$ die Gleichheitsrelation ist, und sie daher nicht durch einen endlichen Automaten realisiert werden kann. Zur Bedeutung von Kriterium (1′) ist folgendes zu sagen:

$N_1 = \{0, 1, 11, 111, \ldots\}$ ist doch einfach die Menge der natürlichen Zahlen. Die Nachfolgerfunktion ist $\varphi_1 x = x\,1 = (x + 1)$, ihre Kongruenzen sind, nebst der Gleichheit, die wohlbekannten elementaren Kongruenzen

$$x \equiv y(l, q) \leftrightarrow (x < l \wedge x = y) \vee (l \leqq x \wedge l \leqq y \wedge x \equiv y \,(\mathrm{mod}\, q)),$$

wobei $0 \leqq l$ und $1 \leqq q$. Sie sind alle von endlichen Index $(l + q)$, und Vereinigungen ihrer Kongruenzklassen pflegt man (schlußendlich-) periodische Mengen von Zahlen zu nennen. Es scheint daher angebracht, auch im Falle $k > 1$, die Vereinigungen von Kongruenzklassen modulo einer rechts-Kongruenz von endlichem Index, als rechts-periodische Teilmengen von N_k zu bezeichnen. Das Kriterium (1') kann dann auch so formuliert werden:

(I) Die Menge β gehört zu Π_k genau dann, wenn sie rechts-periodisch ist.

Übrigens kann N_k auch im Falle $k > 1$ als die Menge der natürlichen Zahlen interpretiert werden. Nur sind jetzt die Zahlen nicht mehr durch eine einzige, aber durch k freie Funktionen $\varphi_1 x = x\,1 = (k \cdot x + 1), \ldots, \varphi_k x = x\,k = (k \cdot x + k)$ aus 0 erzeugt (siehe Bild 4 für den Fall $k = 2$). Mit einer Variante dieses k-ären Nummernsystems $\langle N_k, 0, \varphi_1, \ldots, \varphi_k\rangle$ lernt man zwar schon auf der Schule zu manipulieren (Algorithmen für k-äre Addition und Multiplikation), und es wird doch gerade dieses Umgehen mit Wörtern von altersher Rechnen genannt. Warum aber sind eigentlich diese k-Kongruenzen (Kongruenzen des Funktionssystems $k \cdot x + 1, \ldots, k \cdot x + k$) von endlichem Index und die zugehörigen k-periodischen Mengen von Zahlen nicht schon früher systematisch behandelt worden? Die Theorie der endlichen Automaten kann geradezu als Beitrag zu diesem Teil der elementaren Zahlentheorie bezeichnet werden. — Einige Bemerkungen über k-periodische Mengen von Zahlen sind bei Büchi [2] zu finden. — Ein sehr anspruchsvolles Problem ist es, irgendwelche Übersicht über alle k-Kongruenzen (von endlichem Index) der Zahlen zu gewinnen. Daß die Verbandtheorie hier nicht weiter hilft, wurde schon angedeutet. — Im Kontrast zum Falle $k = 1$ gibt es unter den k-Kongruenzen von unendlichem Index sehr komplizierte (nämlich nicht rekursive) Relationen (Post und Markow, rekursive Unlösbarkeit des Wortproblems für Halbgruppen).

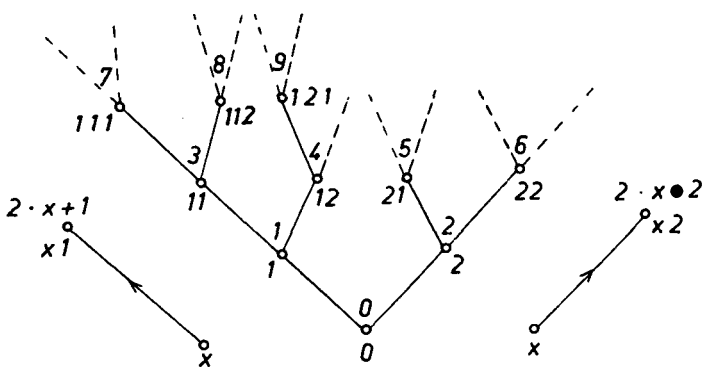


Bild 4

Über N_k gibt es auch die links-Nachfolgerfunktionen $\lambda_1 x = 1\,x, \ldots, \lambda_k x = k\,x$, und ihre Kongruenzen, die links-Kongruenzen von N_k. Eine Menge $\beta \leqq N_k$ heißt links-periodisch, wenn die von β induzierte links-Kongruenz $\approx(\beta)$ endlichen Index hat. Dieser heißt auch der links-Rang von β, und es gilt,

(b) $$x \approx y(\beta) \leftrightarrow (\forall\, u)\,(u\,x \in \beta \leftrightarrow u\,y \in \beta).$$

Schließlich nennen wir eine Relation, die links- und rechts-Kongruenz ist, einfach eine Kongruenz von N_k. Es sind dies die Kongruenzen der freien Halbgruppe $\langle N_k, \hat{}\,\rangle$. Eine Menge $\beta \leqq N_k$ heißt periodisch, wenn die induzierte Kongruenz $\approx(\beta)$ endlichen Index hat. Dieser Index heißt auch Rang von β, und es gilt

(c) $$x \approx y(\beta) \leftrightarrow (\forall\, u, v)\,(u\,x\,v \in \beta \leftrightarrow u\,y\,v \in \beta).$$

Unter Verwendung von (a), (b), (c) ist es nun möglich zu zeigen, daß die Ränge r_1, r_2, r einer Menge $\beta \leqq N_k$ den Abschätzungen $r_1 \leqq 2^{r_2}$, $r_2 \leqq 2^{r_1}$ und $r \leqq r_1^{r_2}, r_2^{r_1}$ genügen. Da trivialerweise $r_1, r_2, \leqq r$, folgt also aus der Endlichkeit einer der drei Ränge die Endlichkeit der beiden anderen, d. h., „rechts-periodisch", „links-periodisch" und „periodisch" haben alle denselben Sinn. Wegen (I) gilt also,

Satz 1: Die Verhaltensmengen endlicher Automaten sind genau die periodischen Mengen von Wörtern. Diese wiederum sind identisch mit den rechts-periodischen und auch den links-periodischen Mengen.

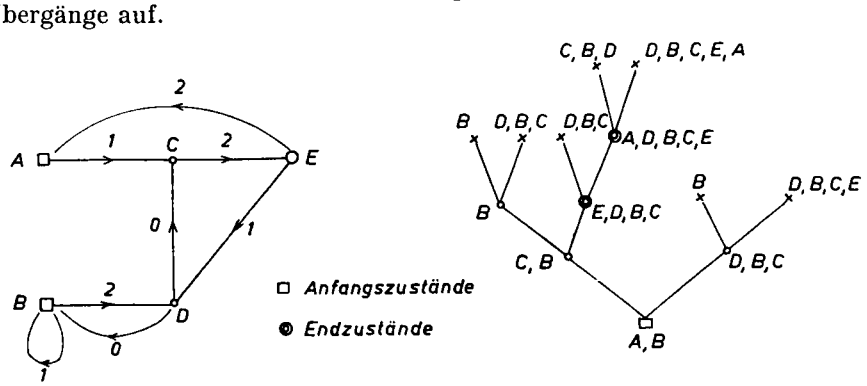
Trotzdem brauchen natürlich die drei Ränge einer Menge $\beta \in \Pi_k$ nicht identisch zu sein, sie genügen aber den oben zitierten Ungleichungen. Übrigens ist der rechts-Rang r_1 einer periodischen Menge β gerade die Minimalzahl von Zuständen die zur Realisierung von β durch einen

Automaten nötig sind; es ist ja $\mathfrak{F}_\beta / \simeq (\beta)$ der minimale Automat des Verhaltens β. Das links-rechts Vertauschte eines Wortes x heiße das Konverse zu x und sei mit $\overleftarrow{x}$ bezeichnet. Trivialerweise ist β periodisch genau dann, wenn es $\overleftarrow{\beta}$ ist, und der links-Rang von β ist gleich dem rechts-Rang von $\overleftarrow{\beta}$. Aus Satz 1 folgt also: Ist $\beta \leq N_k$ realisierbar durch einen endlichen Automaten, dann ist es auch $\overleftarrow{\beta}$. Mit anderen Worten, bei der Frage der Realisierbarkeit von β spielt es keine Rolle, ob man sich dazu entscheidet, die Signale immer von links nach rechts, oder immer von rechts nach links einzugeben. Apriori (ohne Satz 1) ist dies ein erstaunliches Resultat über endliche Automaten, und die Zahl der zur Realisierung von β nötigen Zustände kann auch für die eine Art des Eingebens viel größer sein als für die andere (rechts-Rang und links-Rang von β). Das Resultat kann übrigens auch so formuliert werden: Π_k ist abgeschlossen unter Konversion. Unter Verwendung der Formeln (a), (b) zur Abschätzung von Rängen ist es nicht schwer zu zeigen, daß Periodizität auch erhalten bleibt unter den Booleschen Operationen $\cup, \cap, \sim$ und den weiteren, sogenannten regulären Operationen $\alpha\hat{}\beta = \{xy \mid x \in \alpha \wedge y \in \beta\}$ und $\alpha^* = \{x_1 x_2 \ldots x_n \mid x_1, x_2, \ldots, x_n \in \alpha\} = \alpha \cup (\alpha\hat{}\alpha) \cup (\alpha\hat{}\alpha\hat{}\alpha) \cup \cdots$. Aus Satz 1 folgt dann

Satz 2: Die Menge Π_k der Verhalten endlicher Automaten ist abgeschlossen unter den Operationen $\cup, \cap, \sim, \leftarrow, \hat{}, *$.

Wir werden sehen, daß die abstrakte Algebra $\mathfrak{R}_k = \langle \Pi_k, \cup, \cap, \sim, \leftarrow, \hat{}, * \rangle$ das Einmaleins der Theorie der Schaltung durch Rückkoppelung ist. Fälschlich wird dies oft von der Booleschen Algebra behauptet, die aber nur das reine Schalten beherrscht[1]. Dies wurde zuerst von Kleene [10] erkannt, und wir schlagen deshalb vor, $\mathfrak{R}_k$ die Kleene'schen Algebren zu nennen. Über sie ist leider nicht viel bekannt; es bleibt die wichtige Aufgabe, ihre Theorie auf den Stand derjenigen der Booleschen Algebra zu bringen. Z. B. sind die Probleme der Axiomatisierung der Kleeneschen Algebra ungelöst.

Der oben angedeutete Beweis von Satz 2 ist nicht derjenige von Kleene [10]. Diese Arbeit enthält vieles von vielleicht sekundärer Bedeutung und ist daher schwer verdaulich. Eine bessere Darstellung der Hauptresultate ist bei Copi, Elgot und Wright [8] zu finden. Im folgenden werde ein eleganter und sehr aufschlußreicher Beweis von Myhill [12] des Satzes 2 wiedergegeben. Er beruht auf der folgenden Verallgemeinerung der Automaten, die auch aus ganz anderen Gründen beachtenswert sein dürfte. Ein Transit-System (auch Flußdiagramm und nicht deterministischer Automat genannt) $\mathfrak{C} = \langle \underline{S}, \underline{A}, F_1, \ldots, F_k, F, \underline{W} \rangle$ besteht aus einer Menge $\underline{S}$ von Zuständen, der Anfangsmenge $\underline{A} \leq \underline{S}$, den Transit-Relationen $F_1, \ldots, F_k$, $F \leq (\underline{S} \times \underline{S})$ und der Endmenge $W \leq S$. Die Relationen F_i entsprechen den Eingabezuständen $i = 1, \ldots, k$. F heißt auch Relation der spontanen Übergänge und entspricht dem leeren Signal o. In Bild 5 ist ein Transit-System $\mathfrak{C}_0$ mit den Zuständen A, B, C, D, E durch seinen Transit-Graphen gegeben. Man sieht gleich, daß $\mathfrak{C}_0$ kein Automat ist, denn erstens gibt es zwei Anfangszustände, zweitens sind die Relationen F_1 und F_2 nicht funktionell, und drittens treten spontane Übergänge auf.



(a) Das Transit - System $\mathfrak{L}_0$ (b) Teilmengenkonstruktion Tm ($\mathfrak{L}_0$)

Bild 5

Bemerkung zu Bild 5(a): E ist Endzustand

Unter der Kontaktmenge eines Transit-Systems $\mathfrak{C}$ verstehen wir die Menge $knt(\mathfrak{C})$, bestehend aus allen Signalen $x \in N_k$, die einen gerichteten Weg vom Anfang nach dem Ende markieren. Z. B. gehört also das Signal 121122 = 12o12o2 zu $knt(\mathfrak{C}_0)$, da in Bild 5 der gerichtete Weg $A \to C \to E \to D \to B \to B \to D \to C \to E$ in der Anfangsmenge $\underline{A} = \{A, B\}$

[1]) Eigentlich ist es nur die zweiwertige Schaltung, die der Booleschen Algebra entspricht. Die n-wertigen Schaltungen werden von den Postschen Algebren [14] beherrscht, die leider wenig Beachtung finden. Für eine kurze Darstellung siehe Rosenbloom [17].

beginnt, in der Endmenge $\underline{W} = \{E\}$ endet und seine Kanten durch 1, 2, 1, o, 1, 2, o, 2 markiert sind. Es ist leicht einzusehen, daß das Verhalten eines Automaten gerade die Kontaktmenge des zugehörigen Transit-Graphen ist. Umgekehrt gilt aber auch das

Lemma: Zu jedem endlichen Transit-System $\mathfrak{C}$ (mit n Zuständen) kann man einen endlichen Automaten $\mathfrak{A} = Tm(\mathfrak{C})$ (mit höchstens 2^n Zuständen) konstruieren, so daß $vrh(\mathfrak{A}) = knt(\mathfrak{C})$.

Die Teilmengen-Konstruktion $Tm(\mathfrak{C})$ wurde von MYHILL [12] erfunden und ist in Bild 5(b) im Beispiel $\mathfrak{C}_0$ durchgeführt. Die Zustände des Automaten $Tm(\mathfrak{C}_0)$ sind gewisse Teilmengen aller Zustände von $\mathfrak{C}_0$. Als Anfangszustand wählt man die Anfangsmenge $\underline{A} = \{A, B\}$. Sei die Menge $\underline{X}$ schon als Zustand von $Tm(\mathfrak{C}_0)$ gefunden. Dann schlägt man zum Nachfolger $f_1(\underline{X})$ zunächst alle 1-Nachfolger von $\mathfrak{C}_0$ von Elementen $X \in \underline{X}$ und schließt die so entstandene Menge ab, durch sukzessives Zufügen aller ihrer spontanen Nachfolger in $\mathfrak{C}_0$. Ähnlich konstruiert man $f_2(\underline{X})$. Schließlich wählt man als Elemente der Ausgabe von $Tm(\mathfrak{C}_0)$ alle diejenigen Mengen, die Zustände von $Tm(\mathfrak{C}_0)$ sind und sich mit der Endmenge $\underline{W} = \{E\}$ von $\mathfrak{C}_0$ überschneiden. Es ist nun ganz leicht einzusehen, daß das Verhalten des Automaten $Tm(\mathfrak{C}_0)$ gerade mit der Kontaktmenge $knt(\mathfrak{C}_0)$ übereinstimmt. Zunächst ergibt das Lemma von MYHILL ein weiteres Kriterium für das Verhalten endlicher Automaten:

(III) Eine Menge β gehört zu Π_k genau dann, wenn sie Kontaktmenge eines endlichen Transit-Systems ist.

Daraus folgt nun wieder ganz leicht die Abgeschlossenheit von Π_k unter $\leftarrow$, $\cup$, $\frown$, *; es braucht ja nur gezeigt zu werden, daß mit α und β auch $\overleftarrow{\alpha}$, $\alpha \cup \beta$, $\alpha \frown \beta$ und β^* Kontaktmengen sind. Aus einem Transit-System für α erhält man aber eines für $\overleftarrow{\alpha}$, indem man alle Transitionen umdreht und Anfang mit Ende vertauscht. Ferner ist in Bild 6 angedeutet, wie aus Transit-Systemen für α und β neue Transit-Systeme mit den Kontaktmengen $\alpha \cup \beta$, $\alpha \frown \beta$, β^* konstruiert werden können. Die Bilder erklären wohl diese Konstruktionen zur Genüge (die Doppelpfeile bedeuten jeweils ganze Kabel von spontanen Transitionen). Damit ist dann Satz 2 nach der Methode von MYHILL bewiesen (die Abgeschlossenheit von Π_k unter $\sim$ zeigt man ja leicht direkt; das Komplement der Ausgabe eines Automaten ergibt doch das komplementäre Verhalten). Übrigens zeigt die Konstruktion für β^* in Bild 6 ganz deutlich die fundamentale Bedeutung des Operators *. Er verdient geradezu als Rückkoppelungsoperator bezeichnet zu werden.

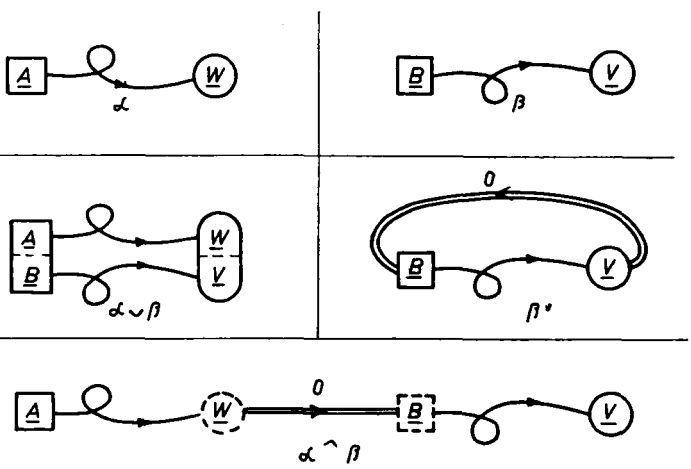


Bild 6

Leicht konstruiert man zu jeder endlichen Menge $\beta \subseteq N_k$ ein endliches Transit-System (Automaten), dessen Kontaktmenge (Verhalten) gleich β ist. Aus Satz 2 folgt daher:

(d) Jede aus endlichen Teilmengen von N_k durch die Operationen $\cup$, $\frown$, * aufgebaute Menge β ist das Verhalten eines endlichen Automaten.

Eine Formel, die aus den Symbolen $1, \ldots, k$ durch Anwendung der Operationssymbole $\cup$, $\frown$, * aufgebaut ist, wenn man einen regulären Ausdruck (dabei ist oft $(\mathfrak{E} \frown \mathfrak{F})$ durch $(\mathfrak{E}\mathfrak{F})$ abgekürzt). Jeder solchen Formel $\mathfrak{E}$ wird, in augenscheinlicher Weise, ein Wert $|\mathfrak{E}| \subseteq N_k$ zugeordnet. Z. B. bezeichnet der Ausdruck $(1 \cup 2)^* 2$ die Menge aller Wörter in N_2, die auf eine 2 enden. Es ist nun leicht einzusehen, daß (d) in folgender stärkerer Form gilt:

Synthesen-Satz: Es gibt ein effektives Verfahren, das zu jedem regulären Ausdruck $\mathfrak{E}$ einen endlichen Automaten $\mathfrak{A}$ vom Verhalten $|\mathfrak{E}|$ liefert.

Ein solches Verfahren kann doch etwa so beschrieben werden: 1. Durch Anwendung der Konstruktionen aus Fig. 6 stelle man ein Transit-System $\mathfrak{C}$ her, dessen Kontaktmenge gleich dem Wert des vorgelegten Ausdrucks $\mathfrak{E}$ ist. 2. Auf $\mathfrak{C}$ wende man die Teilmengenkonstruktion an; der so gewonnene Automat $\mathfrak{A}$ hat das gewünschte Verhalten $|\mathfrak{E}|$. In Bild 7 wurde diese Konstruktion im Beispiel des Ausdruckes $(12^*1 \cup 22)^*22$ durchgeführt.

Auch die Umkehrung zum Synthesen-Satz wurde von KLEENE [10] gefunden; für den Beweis verweisen wir auf diese Arbeit, sowie auf MYHILL [12], COPI, ELGOT und WRIGHT [8],

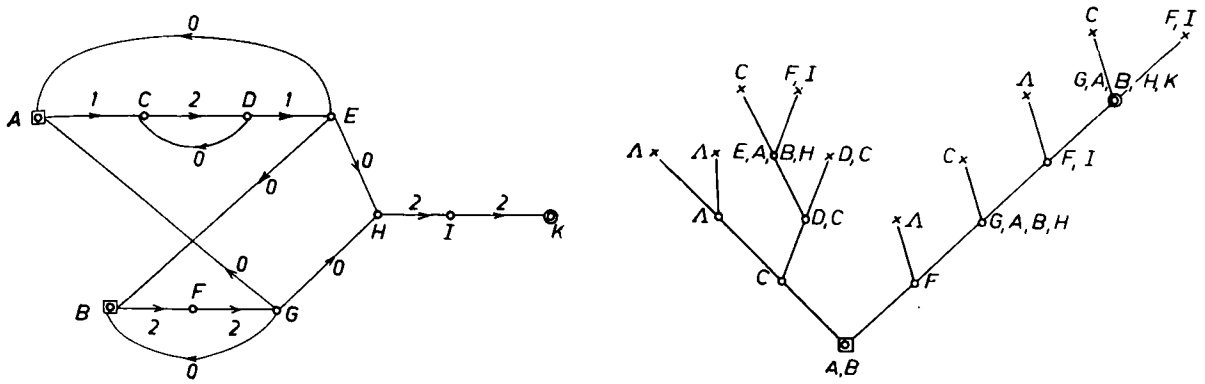


Bild 7

RABIN und SCOTT [16]. Zu den regulären Ausdrücken ist jetzt aber noch das Symbol Λ für die leere Menge, zu rechnen.

Analysen-Satz: Es gibt ein effektives Verfahren, das zu jedem endlichen Automaten $\mathfrak{A}$ einen regulären Ausdruck $\mathfrak{E}$ liefert, der das Verhalten von $\mathfrak{A}$ bezeichnet.

Die beiden Sätze zusammen zeigen, daß die regulären Ausdrücke genau das Verhalten endlicher Automaten beschreiben. Ihre Bedeutung für die Theorie der Schaltung durch Rückkoppelung entspricht also gerade der Bedeutung BOOLEscher Ausdrücke in der Theorie der reinen Schaltung. Endlich ergibt der Analysen-Satz die Umkehrung zu (d), so daß wir als weiteres Kriterium für das Verhalten endlicher Automaten erhalten:

(IV) Eine Menge $\beta \subseteq N_k$ gehört zu Π_k, genau dann, wenn sie der Wert eines regulären Ausdruckes ist, d. h., wenn sie durch die Operationen $\cup$, $\frown$, * aus endlichen Mengen aufgebaut werden kann.

Wegen Satz 2 können in (IV) auch die Operationen $\cap$, $\sim$, $\leftarrow$ zugefügt werden. Über reguläre Ausdrücke bleiben viele wichtige Fragen ungelöst, die mit den Problemen der Axiomatisierung der KLEENEschen Algebren verwandt sind. So folgt zwar aus dem Synthesensatz, daß das Zutreffen von Gleichungen $\mathfrak{E} = \mathfrak{F}$ zwischen regulären Ausdrücken algorithmisch entschieden werden kann. Man kennt aber keine endliche Menge von Identitäten, aus denen alle zutreffenden Gleichungen $\mathfrak{E} = \mathfrak{F}$ herleitbar sind. Sodann fehlt für reguläre Ausdrücke ein brauchbares Konzept der Normalform.

Wir haben damit die fundamentalen Resultate über das Verhalten endlicher Automaten besprochen. Tiefgreifendere Ergebnisse in dieser Richtung sind bei BÜCHI [3] zu finden. Es bleibt uns noch, vor allzu stur-einseitiger Beurteilung der Bedeutung dieser Dinge zu warnen. Es ist doch einfach undenkbar, daß Einsichten über so anschauliche konkrete Strukturen, wie es z. B. die endlichen Transit-Systeme sind, nicht auch in ganz anderen Zusammenhängen von praktischem Wert sein können. Zudem verdient die Arithmetik der Wörter (oder k-ären Zahlsysteme) im allgemeinen und der periodischen Mengen von Wörtern (k-äre Kongruenzen der Zahlen) im speziellen auch die Beachtung des reinen Mathematikers. Daß, auch von diesem Standpunkt aus gesehen, die Theorie des Verhaltens endlicher Automaten nicht inhaltsleer ist, zeigt vielleicht am schönsten ihre Anwendung, BÜCHI [1], auf ein Problem von TARSKI, das sich immerhin von anderer Seite her als unzugänglich erwiesen hat.

Eine ganz andere Fragestellung über endliche Automaten ist wohl am ausführlichsten bei CHURCH [7] formuliert; siehe auch BÜCHI, ELGOT und WRIGHT [4]. Es handelt sich hier um Probleme der Existenz von Algorithmen zur Konstruktion von endlichen Automaten, die vorgelegten Anforderungen genügen sollen. Solche Probleme sind natürlich erst dann fixiert, wenn man sich für eine genau umschriebene, also eine formalisierte Sprache S entschieden hat, in der die Anforderungen zu formulieren sind. Abhängig vom Reichtum der Sprache S existieren dann Konstruktions-Algorithmen oder sie existieren nicht. Ein sehr starker Algorithmus dieser Art findet sich bei BÜCHI [1]. Weiter sind zu diesem Thema folgende Arbeiten zu nennen: FRIEDMAN [9], BÜCHI [2], WANG [19].

Für gewisse Zwecke ist es wohl nützlich, digitale Rechenanlagen als TURINGsche Maschinen zu interpretieren. Mit seiner universellen Maschine ist TURING ja der geniale Erfinder der heute so wichtigen Programmsteuerung geworden. Allerdings darf man nicht stur auf der praktischen Unbrauchbarkeit seiner linearen Bänder herumreiten; es kann ja leicht TURINGS Konzeption der Maschine in vielen Richtungen flexibler gestaltet werden. (Schließlich hatte TURINGS Arbeit den

mehr theoretischen Zweck der exakten Definition der Berechenbarkeit und Lösung des HILBERTschen Entscheidungsproblems.) Als sehr weitreichende Idealisierung verbleibt aber die Unbegrenztheit des Rechenbandes. Im Unterschied zur allgemeineren TURING-Maschine mit endlichem, aber unbegrenztem Gedächtnis ist das Gedächtnis des endlichen Automaten beschränkt durch die Zahl seiner Zustände. Es gibt nun eine Mannigfaltigkeit von Begriffen, die zwischen denjenigen des endlichen Automaten und der TURING-Maschine fallen. Siehe z. B. RABIN und SCOTT [16]. Eine wichtige Aufgabe bleibt es zu erforschen, ob einer dieser Begriffe sich besser eigne, als mathematische Abstraktion der programmgesteuerten Rechenmaschine zu dienen.

Zum Schluß sei noch ganz deutlich gesagt, daß hier nicht der Eindruck erweckt werden soll, als ob die Automatentheorie alle Aspekte der Konstruktion und des Programmierens von digitalen Rechenanlagen und Datenverarbeitungssystemen erfasse. Diese Theorie ist aber ein Zweig (und zwar ein ganz junger und bescheidener) einer hoch entwickelten mathematischen Disziplin, die als Ganzes für den Computerspezialisten sehr wohl sein könnte, was für den Physiker die Theorie der Differentialgleichungen und was für den Statistiker die Maßtheorie ist. Gemeint natürlich ist die formale Logik; allerdings nicht mit Akzent auf Grundlagenforschung, sondern als eine Art von Mathematik gewisser endlicher Strukturen. Der angehende Computermann sollte (vielleicht sogar auf Kosten der Analysis) lernen, was der Logiker über exakte Sprachen weiß und wie man mit solchen umgeht. Vor allem sollte er sich ein tiefes Verständnis aneignen des Begriffes der Berechenbarkeit, wie er in den 30er Jahren seine Klärung fand mit der Entwicklung der Theorie der rekursiven Funktionen, TURING-Maschinen und Algorithmen.

Literatur

[1] J. R. BÜCHI, A Decision Method for Sequential Calculus, Proceedings of the International Congress for Logic, Methodology, and the Philosophy of Science, Stanford University, 1960, S. 1—11.
[2] J. R. BÜCHI, Weak Second Order Arithmetic and Finite Automata, Zeitschrift für Mathematische Logik und Grundlagen der Mathematik **6** (1960), S. 66—92.
[3] J. R. BÜCHI, Regular Canonical Systems, University of Michigan Research Institute Technical Report 2794–7–T, 1959. To appear in Archiv für Mathematische Logik, 1962.
[4] BÜCHI, ELGOT and WRIGHT, The Non-existence of Certain Algorithms of Finite Automata Theory, Abstract, Notices of the American Mathematical Society **5** (1958), S. 98.
[5] A. W. BURKS and J. B. WRIGHT, Sequence Generators and Digital Computers, Proceedings, Symposium on Recursive Functions, Am. Math. Soc., New York 1961.
[6] A. W. BURKS and J. B, WRIGHT Theory of Logical Nets, Proc. IRE **41** (1953), S. 1357—1365.
[7] A. CHURCH, Application of Recursive Arithmetic to the Problem of Circuit Synthesis, Proceedings of the Cornell Logic Conference, Cornell University, 1957. Also see Application of Recursive Arithmetic in the Theory of Computing and Automata, Notes for a summer course, The University of Michigan, 1959.
[8] I. M. COPI, C. C. ELGOT and J. B. WRIGHT, Realization of Events by Logical Nets, Journal Ass. Comp. Mach, **5** (1958), S. 181—196.
[9] J. FRIEDMAN, Some Results in Church's Restricted Recursive Arithmetic, The Journal of Symbolic Logic **22** (1957), S. 337—342.
[10] S. C. KLEENE, Representation of Events in Nerve Nets and Finite Automata, Automata Studies, Princeton University Press, 1956, S. 3—41.
[11] I. T. MEDVEDEV, On a Class of Events Representable in a Finite Automaton, MIT Lincoln Laborators Group Report, S. 34—73, translated from the Russian by J. Schorr-Kon, 1958.
[12] J. MYHILL, Finite Automata and Representation of Events, WADC Report TR 57—624, Fundamental Concepts in the Theory of Systems, 1957, S. 112—137.
[13] E. F. MOORE, Gedanken-Experiments on Sequential Machines, Automata Studies, Princeton 1956, S. 129 bis 153.
[14] E. L. POST, Introduction to a General Theory of Elementary Propositions, Amer. Jour. Math. **43** (1921), S. 163—185.
[15] E. L. POST, Recursive Unsolvability of a Problem of Thue, Journal of Symbolic Logic **12** (1947), S. 1—11.
[16] M. RABIN and D. SCOTT, Finite Automata and Their Decision Problems, IBM Journal, April 1959, S. 114 bis 125.
[17] P. C. ROSENBLOOM, The Elements of Mathematical Logic, Dover 1950.
[18] A. THUE, Probleme über Veränderungen von Zeichenreihen nach gegebenen Regeln, Skrifter utgit av Videnskapsselskapet i Kristiania, I. Matematisk-naturvidens-kabelig klasse, No. 10 (1914), 34 S.
[19] HAO WANG, Circuit Synthesis by Solving Sequential Boolean Equations, Zeitsch. für Math. Logik und Grundl. der Math. **5** (1959), S. 291—322.

Anschrift: Prof. Dr. J. BÜCHI, Mainz, Mathematisches Institut der Universität

Theoretische Grundlagen der Numerischen Mathematik*)

Von L. COLLATZ

Eine Wiedergabe des Vortrages erscheint demnächst im „Jahresbericht der Deutschen Mathematiker-Vereinigung".

*) Auf Einladung der Tagungsleitung gehaltenen Hauptvortrag.