Beiträge zur Algebra und Geometrie
5 (1976), 33 – 40

Spezielle Gleichungen in freien Halbgruppen und eine Anwendung auf Normalformen regulärer Ereignisse

JÜRGEN DASSOW und WALTER HARNAU

Ausgehend vom Begriff der Ableitung, der für Wortmengen vor ungefähr zehn Jahren eingeführt wurde, gelangt man zu speziellen Gleichungen in freien Halbgruppen, die wir in Analogie zur Analysis *Differentialgleichungen* nennen. Die Untersuchung dieser Gleichungen führt auf einen Integralbegriff, den wir im ersten Teil der Arbeit studieren. Der zweite Teil beschäftigt sich mit der Lösung linearer Differentialgleichungen mit konstanten Koeffizienten.
Seit längerem werden Untersuchungen angestellt, um spezielle Wortmengen durch gewisse Gleichungen bzw. Normalformen zu beschreiben. Durch Anwendung der Resultate des zweiten Abschnitts erhalten wir eine Normalform für eine Klasse von Wortmengen, die die regulären Ereignisse umfaßt, und verallgemeinern dadurch eine Normalform von A. SALOMAA.

1. Der Integralbegriff

Es sei X ein Alphabet und $W(X)$ die freie Halbgruppe mit dem Einselement e über X. Dann ist die Ableitung von $R \subseteqq W(X)$ nach $Q \subseteqq W(X)$ durch

$$d_Q(R) = \{p : \exists\, q(q \in Q \wedge qp \in R)$$

definiert.
Wir führen nun die folgenden Mengen ein:

$$I_Q(R) = \{S : S \subseteqq W(X) \wedge d_Q(S) = R\}.$$

Jedes Element aus $I_Q(R)$ heißt *Integral* von R nach Q.
In [1] führten die Autoren unabhängige Ereignisse ein. $S \subseteqq W(X)$ heißt *unabhängig*, wenn aus $p \in S$ und $pq \in S$ die Beziehung $q = e$ folgt.

Lemma 1. *Ist Q unabhängig, so ist $I_Q(R)$ für alle R eine nichtleere Menge.*

Beweis. Da Q unabhängig ist, gilt $q_iR \cap q_jR = \emptyset$ für $i \neq j$ und $q_i, q_j \in Q$. Damit ist

$$d_{q_j}(q_iR) = \begin{cases} R & \text{für} \quad i = j, \\ \emptyset & \text{für} \quad i \neq j \end{cases}$$

und daher

$$d_Q(QR) = \bigcup_{q_i \in Q} d_{q_i}(QR) = \bigcup_{q_i \in Q} d_{q_i}\Big(\bigcup_{q_j \in Q} q_j R\Big) = \bigcup_{q_i \in Q} R = R.$$

Somit ist QR also ein Integral von R nach Q.
Ist Q nicht unabhängig, so ist QR nicht unbedingt ein Integral, wie das folgende Beispiel zeigt. Es sei $X = \{x, y\}$, $R = \{x\}$, $Q = \{y, y^2\}$. Dann ist $d_Q(QR) = \{x, xy\} \neq R$. Wie man leicht nachprüfen kann, ist es möglich, Q und R derart anzugeben, daß $I_Q(R) = \emptyset$ ist. Wir geben dafür zwei Beispiele. Für $Q = \{x, x^2\}$, $R_1 = \{x\}$ und $R_2 = (x^2)^*$ ist $I_Q(R_i) = \emptyset$ für $i = 1, 2$. (Mit R^* bezeichnen wir die von R erzeugte freie Halbgruppe mit Einselement, also $R^* = \{e\} \cup R \cup R^2 \cup R^3 \cup \cdots$.) Deshalb beschränken wir uns in dieser Arbeit stets auf unabhängige Ereignisse Q.

Lemma 2. *Es sei Q unabhängig. Dann ist $|I_Q(R)| = 1$ genau dann, wenn $Q = \{e\}$ ist.*

Beweis. Für ein unabhängiges Q gilt $Q = \{e\}$ oder $e \notin Q$. Ist $Q = \{e\}$, so ist wegen $d_e(S) = S$ sicher $I_Q(R) = R$. Es sei nun $e \notin Q$ und S ein Integral von R nach Q. Ist $e \notin S$, so haben wir wegen $d_Q(S \cup \{e\}) = d_Q(S) = R$ in $S \cup \{e\}$ ein weiteres Integral gefunden, und ist $e \in S$, so weist man $S \setminus \{e\}$ leicht auch als Integral nach.
Eine Menge $S \subseteq W(X)$ heißt Q-Konstante, wenn $d_Q(S) = \emptyset$ ist.

Lemma 3. *Ist $S \in I_Q(R)$ und S' eine Q-Konstante, so ist auch $S \cup S' \in I_Q(R)$.*

Wir wollen nun noch den Fall etwas genauer untersuchen, in dem Q nur aus einem einzigen Wort q besteht.

Satz 4. *Es sei $R \subseteq W(X)$ und $q \in W(X)$. Dann gilt $S \in I_q(R)$ genau dann, wenn $S = qR \cup S'$ ist, wobei S' eine q-Konstante ist.*

Beweis. Wegen $d_q(S_1 \cap S_2) = d_q(S_1) \cap d_q(S_2)$ ist mit $S_1, S_2 \in I_q(R)$ auch $S_1 \cap S_2 \in I_q(R)$. Folglich gibt es genau ein kleinstes Integral S'' (bezüglich der Enthaltenseinsrelation). Ist also $S \in I_q(R)$, so gilt $S = S'' \cup S'$ mit $S'' \cap S' = \emptyset$. Damit aber gilt

$$d_q(S') = d_q(S \setminus S'') = d_q(S) \setminus d_q(S'') = R \setminus R = \emptyset.$$

Die Aussage ist daher bewiesen, wenn $S'' = qR$ bewiesen ist. Es sei $p \in R$. Wegen $d_q(S'') = R$, ist $qp \in S''$ und folglich $S'' \supseteq qR$. Lemma 1 und die Definition von S'' liefern aber $S'' \subseteq qR$.

Folgerung 5. *Es sei $|X| \geq 2$ und $R \subseteq W(X)$. Dann enthält $I_q(R)$ für $q \neq e$ unendlich viele Elemente.*

Beweis. Es sei q' ein Wort mit $l(q) = l(q')$ und $q \neq q'$. ($l(q)$ bezeichne die Länge des Wortes q.) Dann ist mit einer beliebigen Menge $S \subseteq W(X)$ nach Satz 4 auch $qR \cup q'S \in I_q(R)$.

2. Lineare Differentialgleichungen mit konstanten Koeffizienten

Zuerst wollen wir hier einige Begriffe einführen. Unter einer *linearen Differentialgleichung mit konstanten Koeffizienten* verstehen wir eine Gleichung folgender Art:

$$\bigcup_{i=1}^{r} S_i d_{x_i}(R) = R \cup T, \tag{0}$$

wobei $x \in X$ ist, die Koeffizienten S_i seien x-Konstanten für $i = 1, \ldots, r$ und $S_r \neq \emptyset$. Wir nennen die Gleichung (0) *homogen*, wenn das Absolutglied $T = \emptyset$ ist. Andernfalls nennen wir sie *inhomogen*.

Eine Menge $Q \subseteq W(X)$ heißt Polynom in $x \in X$ vom Grade k, falls

$$Q = x^k Q_k \cup x^{k-1} Q_{k-1} \cup \cdots \cup x Q_1 \cup Q_0$$

ist, wobei die Q_i, $i = 0, \ldots, k$, x-Konstanten sind und $Q_k \neq \emptyset$ ist. Offenbar ist Q genau dann ein Polynom vom Grade $l \leqq k$ in x, wenn Q eine x^{k+1}-Konstante ist.
Außerdem bemerken wir noch, daß sich jede Wortmenge R offensichtlich in der Form

$$R = \bigcup_{i=0}^{\infty} x^i R_i \tag{1}$$

darstellen läßt, wobei die R_i x-Konstanten sind. Die R_i sind dabei eindeutig bestimmt.

Unser Ziel besteht nun darin, die Differentialgleichung (0) zu lösen.
Dazu betrachten wir zuerst die Differentialgleichung

$$\bigcup_{i=1}^{r} d_{x^{n_i}}(R) = R. \tag{2}$$

Mit d bezeichnen wir den größten gemeinsamen Teiler der positiven Zahlen $n_1, \ldots, n_r$. Aus den Darstellungen (1) und (2) gewinnen wir die Beziehungen

$$R_l = \bigcup_{i=1}^{r} R_{l+n_i} \quad \text{für} \quad l = 0, 1, 2, \ldots, \tag{3}$$

und diese Bedingungen sind offenbar notwendig und hinreichend dafür, daß R eine Lösung von (2) ist. Aus (3) erhalten wir durch Induktion

$$R_l \supseteq R_{l + \sum_{i=1}^{r} \alpha_i n_i} \quad \text{für beliebige} \quad \alpha_i \in Na,\ l \in Na.$$

Ohne große Schwierigkeiten beweist man das

Lemma 6. *Sind $n_1, \ldots, n_r$ von Null verschiedene natürliche Zahlen und ist d ihr größter gemeinsamer Teiler, dann gibt es eine natürliche Zahl N derart, daß für alle natürliche Zahlen $n \geqq N$ natürliche Zahlen α_i existieren, so daß*

$$nd = \sum_{i=1}^{r} \alpha_i n_i$$

gilt.

Hiervon ausgehend erhält man für alle $l \in Na$ und $n \geqq N$

$$R_l \supseteq R_{l+nd}.$$

Beachten wir noch (3), so erhalten wir

$$R_l = \bigcup_{n=N+1}^{\infty} R_{l+nd} \quad \text{und} \quad R_{l+d} = \bigcup_{n=N}^{\infty} R_{l+d+nd} = \bigcup_{n=N+1}^{\infty} R_{l+nd},$$

womit wir

$$R_l = R_{l+d}$$

erhalten. Hieraus folgt nun sofort der

Satz 7. *R ist genau dann eine Lösung der Differentialgleichung* (2), *wenn*

$$R = (x^d)^* S$$

ist, wobei S ein Polynom des Grades $k \leqq d - 1$ *in x und*

$$d = \text{g. g. T.}\,(n_1, \ldots, n_r)$$

ist.

Bemerkung. Es sind also die d Koeffizienten des Polynoms S frei wählbare Größen, im Gegensatz zur Analysis, wo die Lösung der entsprechenden Differentialgleichung

$$y^{(n_r)} + \cdots + y^{(n_1)} = y$$

n_r frei wählbare Konstanten enthält. Um zu einer eindeutigen Lösung zu kommen, gibt man in der Analysis zu der eigentlichen Differentialgleichung noch Anfangswerte vor. Da die Darstellung (1) einer Taylorentwicklung entspricht, ist die Forderung $R_i = Q_i$, $i = 0, 1, \ldots, d - 1$, mit vorgegebenem Q_i ein Analogon zu den Anfangswerten, und es gibt dann nur eine einzige Lösung, die dieser Zusatzbedingung auch genügt.

Wir wenden uns nun der homogenen linearen Differentialgleichung mit konstanten Koeffizienten

$$\bigcup_{i=1}^{r} S_i d_{x^i}(R) = R \tag{4}$$

zu. Wegen $d_x(S_i) = \emptyset$ erhalten wir durch Ableiten

$$\bigcup_{j \in D} d_{x^{j+1}}(R) = d_x(R),$$

wobei D die Menge der i mit $e \in S_i$ ist. Ist $D = \emptyset$, so erhält man hieraus und aus (4) sofort, daß $R = \emptyset$ sein muß. Es sei nun also $D \neq \emptyset$. Dann erhalten wir

$$\bigcup_{j \in D} d_{x^j}(d_x(R)) = d_x(R).$$

Die Lösung dieser Differentialgleichung für $d_x(R)$ ist aus Satz 7 bekannt, und durch Integration erhalten wir

$$R = x(x^d)^* \,(x^{d-1}Q_{d-1} \cup \cdots \cup xQ_1 \cup Q_0) \cup S,$$

wobei S und die Q_i x-Konstanten sind und $d = \text{g. g. T.}\,\{j : j \in D\}$ ist. Dabei sind nicht alle Größen frei wählbar. Sind die Q_i gegeben, so bestimmt sich S wie folgt. Wir setzen

$$R' = x(x^d)^* \,(x^{d-1}Q_{d-1} \cup \cdots \cup Q_0)$$

und erhalten

$$d_{x^d}(R') = Q_{d-1} \cup R'. \tag{5}$$

Da $R = R' \cup S$ gilt, ist nun

$$\bigcup_{i=1}^{r} S_i d_{x^i}(R' \cup S) = R' \cup S$$

und somit wegen (5)

$$\bigcup_{i=1}^{r} S_i d_{x^i}(R' \cup S) = \bigcup_{i=1}^{r} S_i d_{x^i}(R') = \bigcup_{i=1}^{r} (S_i \setminus \{e\})\, d_{x^i}(R') \bigcup_{j\in D} (R' \cup Q_{d-1}).$$

Damit haben wir den folgenden Satz erhalten.

Satz 8. *In der Differentialgleichung* (4) *seien die* S_i *für* $i = 1, 2, 3, \ldots, r$ *x-Konstanten, und es sei* $D = \{i : e \in S_i\}$. *Dann hat die Lösung* R *von* (4) *folgende Gestalt:*

a) *Ist* $D = \emptyset$, *so ist auch* $R = \emptyset$.

b) *Ist* $D \neq \emptyset$ *und* $d = \text{g. g. T.}\,\{i : i \in D\}$, *so ist*

$$R = x(x^d)^*\,(x^{d-1}Q_{d-1} \cup x^{d-2}Q_{d-2} \cup \cdots \cup xQ_1 \cup Q_0) \cup S.$$

Dabei sind die Q_i, $i = 0, \ldots, d-1$, *und* S *x-Konstanten, die nur die Bedingung*

$$S = \bigcup_{i=1}^{r} (S_i \setminus \{e\})\, d_{x^i}(x(x^d)^*\,(x^{d-1}Q_{d-1} \cup \cdots \cup Q_0) \cup Q_{d-1})$$

erfüllen müssen.

Damit ist unser Problem in homogenen Fall gelöst. Damit hat man auch einen kleinen Überblick über die Lösungen der zugehörigen inhomogenen Gleichung, denn es gilt

Lemma 9. *Ist* R *eine Lösung der inhomogenen Differentialgleichung* (0) *und* R' *eine Lösung der zugehörigen homogenen Gleichung, so ist auch* $R \cup R'$ *eine Lösung der inhomogenen Differentialgleichung* (0).

Mittels Beispielen kann man nun nachweisen, daß man R aber nicht so angeben kann, daß sich jede Lösung von (0) in der Gestalt $R \cup R'$ schreiben läßt, wobei R' (4) löst. In einem Spezialfall wollen wir nun aber alle Lösungen der inhomogenen Gleichung angeben.

Satz 10. *R ist genau dann eine Lösung der inhomogenen Differentialgleichung*

$$\bigcup_{i=1}^{r} d_{x^{n_i}}(R) = R \cup T,$$

wobei T *ein Polynom des Grades* $k < \min\limits_{1\le i\le r} n_r$ *in* x *mit den Koeffizienten* T_i *ist, wenn* R *die Gestalt*

$$R = x^{k+1}(x^d)^*\,(x^{d-1}Q_{d-1} \cup \cdots \cup Q_0) \cup x^k S_k \cup \cdots \cup xS_1 \cup S_0$$

hat, wobei $d = \text{g. g. T.}\,(n_1, \ldots, n_r)$ *ist und folgende Bedingung erfüllt sein muß:*

$$S_i \cup T_i = Q_{d'+i \bmod d} \quad \textit{für} \quad i = 0, 1, \ldots, k$$

mit $d' \equiv -k - 1 \bmod d$ *und* $d' \in \{0, 1, \ldots, d-1\}$.

Beweis. Durch $(k+1)$-maliges Ableiten erhalten wir die Differentialgleichung

$$\bigcup_{i=1}^{r} d_{x^{n_i}}(d_{x^{k+1}}(R)) = d_{x^{k+1}}(R)$$

für $d_{x^{k+1}}(R)$, deren Lösung aus Satz 7 bekannt ist. Nun erhalten wir durch $(k+1)$-malige Integration, daß R die behauptete Form haben muß.
Wegen $n_i \geqq k+1$ und $d' \equiv n_i - k - 1 \bmod d$ für alle $i = 1, \ldots, k$ ist

$$d_{x^{n_i}}(R) = x^{d'-1}(x^d)^*\,(x^{d-1}Q_{d-1} \cup \cdots \cup Q_0) \cup x^{d'-1}Q_{d-1} \cup \cdots \cup Q_{d'-1}$$

und folglich für $i = 0, 1, \ldots, k$

$$S_i \cup T_i = Q_{d'+i \bmod d}.$$

Alle bisher angestellten Betrachtungen lassen sich auch für andere Strukturen durchführen. Wir wollen hier nur ein einziges Beispiel anführen. Es sei G eine Gruppe. Dann ist $d_a(K) = a^{-1}K$ für $a \in G$ und einen Komplex K. Ein Komplex R ist genau dann Lösung der Differentialgleichung

$$K = a^{-1}K \cup \bigcup_{i=1}^{r} a^{-n_i}K,$$

wenn er Vereinigung von Nebenklassen der von a erzeugten Untergruppe ist. Dies entspricht genau unserem Resultat über freie Halbgruppen.

3. Eine Anwendung auf Normalformen

In diesem Abschnitt beschränken wir uns auf endliche Alphabete. Spezielle Wortmengen spielen in einigen Teilgebieten der Mathematik eine wesentliche Rolle. In der Automatentheorie sind es die regulären Mengen und in der mathematischen Linguistik die contextfreien Sprachen. (Für die genauen Definitionen vgl. [2].) Wir suchen nun eine Normalform für Wortmengen (oder mindestens einer Klasse von Wortmengen), die uns gestattet, auch zu erkennen, ob die Menge regulär oder contextfrei ist.
Zwar ist die Darstellung (1) schon eine Normalform, aber man kann an ihr nicht erkennen, ob die vorgelegte Menge regulär ist, denn R muß nicht regulär sein, obwohl alle R_i regulär sind, wie das Beispiel $R = \{x^n y^n : n \geqq 0\}$ über $X = \{x, y\}$ zeigt. Wir beschränken uns daher auf solche Wortmengen, die nur endlich viele verschiedene Ableitungen nach den Potenzen von $x \in X$ besitzen.

Satz 11. *Ist die Menge $M = \{d_{x^i}(R) : i \in Na\}$ für ein Ereignis $R \subseteqq W(X)$ endlich, so existieren natürliche Zahlen d und k und eindeutig bestimmte x-Konstanten Q_i, $i = 0, 1, \ldots, d-1$, und S_j, $j = 0, 1, \ldots, k-1$, mit*

$$R = x^k(x^d)^* (x^{d-1}Q_{d-1} \cup \cdots \cup xQ_1 \cup Q_0) \cup x^{k-1}S_{k-1} \cup \cdots \cup S_0. \tag{8}$$

Hat R umgekehrt diese Form, so ist M endlich.

Beweis. Da M endlich ist, gibt es natürliche Zahlen d und k mit

$$d_{x^{k+d}}(R) = d_{x^k}(R).$$

Fassen wir dies als Differentialgleichung für $d_{x^k}(R)$ auf, so erhalten wir aus Satz 7

$$d_{x^k}(R) = (x^d)^* (x^{d-1}Q_{d-1} \cup \cdots \cup Q_0),$$

und durch k-maliges Integrieren folgt die behauptete Form von R.
Wegen $R_i = S_i$ für $i = 0, \ldots, k-1$ und $R_{i+k} = Q_i$ für $i = 0, \ldots, d-1$ folgt die Eindeutigkeit der Q_i und S_j.
Die Umkehrung ist trivial.

Folgerung 12 (SALOMAA [3]). *Ist* $|X| = 1$, *so ist* R *genau dann regulär, wenn natürliche Zahlen* $k, d, d_1, \ldots, d_r, k_1, \ldots, k_s$ *mit*

$$0 \leqq d_r < d_{r-1} < \cdots < d_1 < d, \qquad 0 \leqq k_s < k_{s-1} < \cdots < k_1 < k$$

und

$$R = x^k(x^d)^* (x^{d_1} \cup x^{d_2} \cup \cdots \cup x^{d_r}) \cup x^{k_1} \cup x^{k_2} \cup \cdots \cup x^{k_s}$$

existieren.

Beweis. Für reguläre Mengen ist M endlich. Wegen Q_i, $S_j \in \{\emptyset, \{e\}\}$ folgt die Behauptung aus Satz 11, da Mengen der obigen Form sicher regulär sind. Wir haben damit für den Fall $|X| = 1$ auch gleichzeitig die Äquivalenz der Regularität von R und der Endlichkeit von M nachgewiesen.

Folgerung 13. a) *R ist genau dann regulär, wenn natürliche Zahlen k und d und reguläre x-Konstanten Q_i, S_j so existieren, daß R die Form* (8) *hat.*

b) *Für R sei die Menge M aus Satz* 11 *endlich. Dann ist R genau dann eine contextfreie Sprache, wenn R in der Form* (8) *darstellbar ist mit contextfreien x-Konstanten Q_i, S_j.*

Beweis. a) Hat R die Form (8) mit regulären S_i, Q_j, so ist R sicher regulär.
Es sei nun R regulär. Dann ist M endlich und R ist in der Form (8) darstellbar. Ferner sind dann alle Ableitungen von R wieder regulär. Insbesondere ist also $d_{x^i y}(R) = d_y(R_i)$ eine reguläre Menge. Wegen

$$R_i = yd_y(R_i) \cup zd_z(R_i) \cup \cdots \cup wd_w(R_i)$$

ist damit R_i regulär. (Dabei sei $X = \{x, y, z, \ldots, w\}$.) Wegen $R_{i+k} = Q_i$ und $R_i = S_i$ folgt damit die Regularität der Q_i, S_i.

b) beweist man analog.

Durch Minimalitätsforderungen kann man auch noch die natürlichen Zahlen d und k aus Satz 11 eindeutig festlegen.

Wir wollen nun noch eine weitere Normalform herleiten. Dafür benötigen wir einige Begriffe.
Es sei N das k-fache kartesische Produkt der Menge der natürlichen Zahlen. $L \subseteqq N$ heißt *linear*, wenn für gewisse $c, p_1, \ldots, p_n$ aus N

$$L = \{c + \alpha_1 p_1 + \cdots + \alpha_n p_n : \alpha_i \in Na\}$$

ist. $p_1, \ldots, p_n$ heißen *Perioden.*
$\varrho_i(w)$ gebe an, wie oft der Buchstabe x_i in $w \in W(X)$ vorkommt. Dann sei für eine Sprache $R \subseteqq W(X)$, $X = \{x_1, \ldots, x_k\}$,

$$L(R) = \{(\varrho_1(w), \ldots, \varrho_k(w)) : w \in R\}.$$

Eine Menge $R \subseteqq W(X)$ heißt *beschränkt*, wenn $R \subseteqq x_1^* x_2^* \cdots x_k^*$ ist.

Folgerung 14 (GINSBURG und SPANIER). *Es sei R eine beschränkte Menge. R ist genau dann regulär, wenn $L(R)$ die Vereinigung endlich vieler linearer Mengen ist, deren sämtliche Perioden genau eine von* 0 *verschiedene Koordinate besitzen.*

Beweis. Für $k = 1$ folgt die Behauptung aus Folgerung 12 sofort. Die geforderte Linearitätseigenschaft für eine reguläre beschränkte Menge R läßt sich nun wegen Satz 11 und Folgerung 13 leicht mittels vollständiger Induktion erbringen.

Umgekehrt ist jede Menge mit entsprechendem $L(R)$ die endliche Vereinigung und Verkettung gewisser $(x_i^j)^*$, und somit regulär.

LITERATUR

[1] MÜNTEFERING, P., und P. H. STARKE: Über reduzible Ereignisse. EIK *8* (1972), 187—196.
[2] GÉCSEG, F., and I. PEÁK: Algebraic Theory of Automata. Akadémiai Kiadó, Budapest 1972.
[3] SALOMAA, A.: Theorems on the representation of events in Moore automata. Ann. Univ. Turku. Ser. AI, *69* (1964), 3—14.
[4] GINSBURG, S., and E. H. SPANIER: Bounded regular sets. Proc. Amer. Math. Soc. *17* (1966), 1043—1049.

Manuskripteingang: 15. 10. 1974

VERFASSER:

JÜRGEN DASSOW und WALTER HARNAU, Sektion Mathematik
der Wilhelm-Pieck-Universität Rostock