RAIRO. INFORMATIQUE THÉORIQUE

GÜNTER HOTZ

Verschränkte homomorphismen formaler sprachen

RAIRO. Informatique théorique, tome 14, nº 2 (1980), p. 193-208
<http://www.numdam.org/item?id=ITA_1980__14_2_193_0>

© AFCET, 1980, tous droits réservés.

L'accès aux archives de la revue « RAIRO. Informatique théorique » implique l'accord avec les conditions générales d'utilisation (http://www.numdam.org/conditions). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
http://www.numdam.org/

R.A.I.R.O. Informatique théorique/Theoretical Computer Science
(vol. 14, n° 2, 1980, p. 193 à 208)

VERSCHRÄNKTE HOMOMORPHISMEN FORMALER SPRACHEN (*)

von Günter HOTZ ([1])
Communiqué par J. BERSTEL

Résumé. — *Nous donnons des conditions nécessaires calculables pour décider des problèmes de mots et des problèmes d'équivalence de langages formels. Ces conditions se formulent en termes d'algèbre commutative et sont indépendantes de celles qui découlent du théorème de Parikh.*

Zusammenfassung. — *Wir entwickeln notwendige berechenbare Kriterien zur Entscheidung von Wortproblemen und Aquivalenzproblemen formaler Sprachen. Diese Kriterien sind Kriterien der kommutativen Algebra. Sie sind unabhängig von den Kriterien, die sich aus dem Satz von Parikh ergeben.*

Abstract. — *We develop necessary computable conditions for deciding word problems and equivalence problems of formal languages. This conditions are formulated as theorems of commutative algebra. They are independent from conditions which follow from the theorems of Parikh.*

EINLEITUNG :

Das Ziel dieser Arbeit besteht in der Entwicklung notwendiger berechenbarer Kriterien zur Entscheidung des Wortproblems und des Äquivalenzproblemes formaler Sprachen. Insofern schließt diese Arbeit an die Arbeit [7] an, in der Parikh durch die Abbildung k.f.

Sprachen auf semilineare Mengen ein solches Kriterium angegeben hat. Für k.f. Sprachen wurde in [3] ein davon unabhängiges Kriterium angegeben. Dieses Kriterium bildet für kontextfreie Grammatiken $G=(X, T, P, S)$, die Freie Gruppe $F(X)$ und die Faktorgruppe $\mathcal{G}(G)=F(X)/P$, worin P als Relationensystem aufgefaßt wird. $\mathcal{G}(G)$ hängt für Grammatiken, die keine überflüssigen Variablen enthalten, nur von $L(G)$ ab. Damit stehen zur Entscheidung des Äquivalenzproblemes von k.f. Sprachen alle Methoden zur Verfügung, die zur Entscheidung der Isomorphie von Gruppen entwickelt wurden. Insbesondere wurde auf ein Kriterium von Fox [2] hingewiesen. In diesem Kriterium spielt der »free differential calculus« die entscheidende Rolle.

(*) Reçu avril 1979, et dans sa forme définitive octobre 1979.
([1]) Universität des Saarlandes, Saarbrücken.

© AFCET-Bordas-Dunod

Der free differential calculus wird in [6] als »crossed homomorphism« und in deutschsprachiger Literatur als »verschränkter Homomorphismus« bezeichnet.

Wir betrachten diesen Homomorphismus in der allgemeineren Form $d(u.v)=d(u).e(v)+c(v).d(u)$, worin c und e auf X^* Monoidhomomorphismen in das freie multiplikative kommutative Monoid $[X]$ sind.

Wir charakterisieren zunächst Thue-Systeme durch endlich erzeugte zweiseitige Ideale in $\mathbb{Z}(X^*)$. Danach befreien wir uns von der Symmetrie der Produktionssysteme und zeigen, daß Wort- und Äquivalenzproblem formaler Sprachen auf die entsprechenden Probleme für endlich erzeugte zweiseitige Ideale von $\mathbb{Z}(X^*)$ zurückgeführt werden kann. Damit erhalten wir das Resultat, daß Wort- und Äquivalenzproblem für endlich erzeugte zweiseitige Ideale nicht generell entscheidbar sind.

Um berechenbare notwendige Kriterien für diese Probleme zu erhalten, bilden wir $\mathbb{Z}[X]/(a(P))$. Hierin ist $a(P)=e(P)\cup c(P)$, und $(a(P))$ ist das durch $a(P)$ erzeugte Ideal in $\mathbb{Z}[X]$. d verlängern wir zu einem verschränkten Homomorphismus d_a von $\mathbb{Z}(X^*)$ in die direkte Summe

$$\mathscr{M}/(a)=\bigotimes_x \mathbb{Z}[X]/(a(P))\,dx.$$

Das Semi-Thue-System P wird hierdurch in einen $\mathbb{Z}(X^*)$-*Untermodul* $(d_a(P))$ von $\mathscr{M}/(a)$ abgebildet.

Leider ist das genaue Bild von formalen Sprachen unter d_a, wie es scheint, im allgemeinen nicht leicht bestimmbar, so daß man durch diese Konstruktion nicht unmittelbar notwendige Bedingungen für das Äquivalenzproblem erhält. Wir können jedoch zeigen, daß der Restklassenmodul von $\mathscr{M}/(a)$ nach $(d_a(P))$ unter gewissen Grammatiktransformationen invariant ist. Für kontextfreie Sprachen erhält man hieraus für verschiedene Homomorphismen c, e notwendige und berechenbare Kriterien für die Äquivalenz formaler Sprachen.

1. NOTATIONEN UND GRUNDLEGENDE DEFINITIONEN

Sei X eine endliche Menge, $\mathbb{Z}$ die Menge der ganzrationalen Zahlen und $\mathbb{Z}(X^*)$ der Monoidring der nicht kommutativen Polynome mit Unbestimmten aus X und Koeffizienten aus $\mathbb{Z}$. X^* ist das freie Monoid über X und $[X]$ das freie abelsche Monoid über X. $\mathbb{Z}[X]$ ist der Polynomring mit den Elementen von X als Unbestimmte. com : $\mathbb{Z}(X^*)\to\mathbb{Z}[X]$ ist der Ringhomomorphismus der $\mathbb{Z}(X^*)$ kommutativ macht. Zum Beispiel gilt also

$$\text{com}\,(a^n b^n c^n+2\,c^n b^n a^n+acba)=3\,a^n b^n c^n+a^2 bc.$$

$\mathbb{Z}(X^*)$ und $\mathbb{Z}[X]$ können wir auch als $\mathbb{Z}(X^*)$-Modul auffassen.

Für $\mathbb{Z}[X]$ tun wir dies mittels der Definition

$$a.f = \mathrm{com}\,(a).f \qquad \text{für} \quad a \in \mathbb{Z}(X^*), \quad f \in \mathbb{Z}[X].$$

Sind M_1 und M_2 Monoide und sind $\mathbb{Z}(M_1)$ und $\mathbb{Z}(M_2)$ die Monoidringe über M_1 bzw. M_2 mit Koeffizienten aus $\mathbb{Z}$ und sind $e, c : \mathbb{Z}(M_1) \to \mathbb{Z}(M_2)$ Ringhomomorphismen, dann definieren wir :

Eine Abbildung

$$d: \quad \mathbb{Z}(M_1) \to \mathbb{Z}(M_2),$$

heißt *verschränkter Homomorphismus* von $\mathbb{Z}(M_1)$ in $\mathbb{Z}(M_2)$ falls (1) und (2) gilt :

(1) $d(f+g) = d(f) + d(g)$;

(2) $d(f.g) = d(f).e(g) + c(f).d(g)$;

für $f, g \in \mathbb{Z}(M_1)$.

Für $M_1 = X^*$ und $M_2 = [X]$, $e(x) = 1$ für $x \in X$ und $c = \mathrm{com}$ erhält man den freien Differentialkalkül von Fox [2]. Setzt man $e(x) = c(x) = 1$, dann bildet dX^* in das additive freie abelsche Monoid homomorph ab.

Die Menge der verschränkten Homomorphismen von $\mathbb{Z}(X^*)$ in $\mathbb{Z}[X]$ bildet bei festem e, c selbst einen freien $Z(X^*)$-Modul, der durch die mit $\partial/\partial x$ bezeichneten und durch

$$\frac{\partial}{\partial x}(y) = \begin{cases} 1 & \text{für} \quad x = y \\ 0 & \text{für} \quad x \neq y \end{cases} \qquad \text{für} \quad x \in X, \quad y \in X,$$

definierten Elemente erzeugt wird.

Wir schöpfen also alle Möglichkeiten der verschränkten Homomorphismen aus, wenn wir diese erzeugenden Abbildungen simultan betrachten. Hierzu bilden wir die direkte Summe

$$\mathcal{M} = \bigoplus_{x \in X} \mathbb{Z}[X]\,dx,$$

worin dx eine freie Variable ist. $\mathcal{M}$ ist ein $Z(X^*)$-Modul und wir definieren

$$d: \quad \mathbb{Z}(X^*) \to \mathcal{M},$$

indem wir für $f \in \mathbb{Z}(X^*)$ setzen

$$d(f) = \sum_{x \in X} \frac{\partial f}{\partial x}\,dx,$$

d bezeichnen wir wieder als verschränkten Homomorphismus, da d (1) und (2) erfüllt.

Es ist in dieser Arbeit stets $T \subset X$ eine nicht leere Menge und $S \in X - T$, $P \subset X^* \times X^*$. $G = (X, T, P, S)$ heißt Grammatik, X das Alphabet von G, T das

Terminalalphabet, P das Produktionensystem und S das Axiom von G. P definiert ein Semi-Thue-System auf X^*. Die zugehörige Relation wird gewöhnlich durch $\rightarrow$ oder genauer $\underset{P}{\rightarrow}$ bezeichnet :

$$L(G)=\{w \in T^* \mid S \underset{P}{\rightarrow} w\},$$

ist die durch G erzeugte formale Sprache. P heißt symmetrisch, wenn aus $(u, v) \in P$ folgt $(v, u) \in P$. In diesem Fall definiert P ein Thue-System. Wir nennen in diesem Falle G auch symmetrisch.

Ist P irgendein Produktionensystem, so setzen wir

$$\overline{P}=P \cup \{(u, v) \mid (v, u) \in P\}.$$

$\overline{P}$ ist also das kleinste symmetrische Produktionssystem, das P erhält.

Das Ziel dieser Arbeit besteht in der Untersuchung des Verhaltens formaler Sprachen unter verschränkten Homomorphismen. Wir werden zeigen, daß verschränkte Homomorphismen die Hauptprobleme der Theorie der formalen Sprachen, nämlich das Wortproblem $w \in L(G)$? und das Äquivalenzproblem $L(G_1)=L(G_2)$? in Probleme der kommutativen Algebra übertragen.

2. EINIGE EINFACHE EIGENSCHAFTEN VON d

Wir interessieren uns dafür, wie weit d das Wort und Äquivalenzproblem erhält. Dies ist dann vollständig der Fall, wenn d eine bijektive Abbildung ist. Für $x_1, \ldots, x_n \in X$ erhalten wir

$$d(x_1 \cdot \ldots \cdot x_n)=\sum c(x_1 \ldots x_{i-1}) e(x_{i+1} \ldots x_n)\, dx_i.$$

Wenn für alle $w \in X^*$ $c(w) \neq 0$, $e(w) \neq 0$ gilt, bestimmt die Anzahl der Summanden des Ausdruckes n eindeutig. Bestimmt $c(x_1 \ldots x_{i-1}) e(x_{i+1} \ldots x_n)$ den Index i eindeutig, dann ist also d auf X^* injektiv. Dies ist der Fall für die Fälle

$$\left.\begin{array}{ll} c(x)=x, & e(x)=1 \\ c(x)=1, & e(x)=x \end{array}\right\} \quad \text{für} \quad x \in X. \tag{1}$$

Es genügt aber auch schon

$$\left.\begin{array}{ll} c(x)=x_1, & e(x)=1 \\ c(x)=1, & e(x)=x_1 \\ c(x)=x_1, & e(x)=x_2 \end{array}\right\} \quad \text{für} \quad x \in X \tag{2}$$

und feste $x_1, x_2 \in X$ und $x_1 \neq x_2$.

Für $c(x)=e(x)$, d.h. im Falle der gewöhnlichen Leibnizformel ist d nicht injektiv. Als Abbildung auf $\mathbb{Z}(X^*)$ ist d in keinem der aufgezählten Fälle injektiv. Hieraus ergibt sich der

SATZ 1 : *In den Fällen* (1) *und* (2) *gilt für* $w \in T^*$:

$$w \in L(G) \Leftrightarrow d(w) \in d(L(G))$$

und

$$L(G_1)=L(G_2) \Leftrightarrow d(L(G_1))=d(L(G_2)).$$

Dieser Satz zeigt, daß sich in den Fällen (1) une (2) die Bilder $d(L)$ der formalen Sprachen L nicht einfach mit den Mitteln der kommutativen Algebra ausdrücken lassen. Denn ließe sich $d(L)$ etwa als Restklasse nach einem freien endlich erzeugten $\mathbb{Z}(X^*)$-Modul darstellen, dann wären aufgrund von Satz 1 das Wort- und Âquivalenzproblem generell entscheidbar.

Weniger wichtig ist die Surjektivität von d. Man erkennt, daß $d : \mathbb{Z}(X^*) \to \mathscr{M}$ im Falle (1) surjektiv ist. Hierzu betrachte man $d(wx-w)$ für $w \in X^*$.

3. SEMI-THUE-SYSTEME ALS IDEALE IN $\mathbb{Z}(X^*)$

Wir beschreiben den Ableitungsbegriff bezüglich des Produktionensystems P von G etwas algebraischer, als es allgemein üblich ist. Hierzu definieren wir auf $X^* \times X^*$ zwei Operationen $\times$ und $\circ$.

DEFINITION : Für (w, v) und $(w', v') \in X^* \times X^*$ gilt

$$(w, v) \times (w', v')=(ww', vv').$$

Ist $v=w'$, dann ist

$$(w, v) \circ (w', v')=(w, v').$$

Offensichtlich bilden $X^* \times X^*$ bezüglich $\times$ ein Monoid und bezüglich $\circ$ eine Kategorie. Darüber hinaus sogar eine monoidale oder x-Kategorie. Wir bezeichnen die durch P und die Objekte X^* erzeugte Unter-x-Kategorie mit $C(P)$.

Es ist $w \in T^*$ genau dann in $L(G)$, falls es ein $f \in C(P)$ gibt mit $f=(S, w)$. Jedes $f \in C(P)$ läßt sich wie folgt zerlegen

$$f=(1_{u_1} \times p_1 \times 1_{v_1}) \circ \ldots \circ (1_{u_k} \times p_k \times 1_{v_k}),$$

mit $p_i \in P$ und $u_i, v_i \in X^*$, $1_u=(u, u)$.

Wir gehen nun zu $\mathbb{Z}(X^* \times X^*)$ über und führen den Randoperator $\rho : \mathbb{Z}(X^* \times X^*) \to \mathbb{Z}(X^*)$ ein, indem wir für h_1, $h_2 \in \mathbb{Z}(X^* \times X^*)$ und $(w, v) \in X^* \times X^*$ definieren :

(1) $\rho(h_1 + h_2) = \rho(h_1) + \rho(h_2)$,

(2) $\rho(w, v) = v - w$.

Offensichtlich gilt

$$\rho(1_u \times p \times 1_v) = u . \rho(p) . v,$$

und für f, $g \in X^* \times X^*$, für die $f \circ g$ definiert ist

$$\rho(f \circ g) = \rho(f) + \rho(g).$$

Wenden wir ρ auf die obige Darstellung von f an, so erhalten wir also

$$\rho(f) = u_1 \rho(p_1) v_1 + u_2 \rho(p_2) v_2 + \ldots + u_k \rho(p_k) v_k.$$

Bezeichnen wir mit (P) das zweiseitige Ideal, das durch $\{\rho(p) \mid p \in P\}$ erzeugt wird, dann haben wir also das (*).

Lemma 1 : *Ist $f = (u, v) \in C(P)$, dann ist $v - u \in (P)$, v und u liegen also in der gleichen Restklasse von $\mathbb{Z}(X^*)$ nach (P).*

Lemma 2 : *Ist P symmetrisch und gilt $v - u \in (P)$ mit u, $v \in X^*$ dann ist $(u, v) \in C(P)$, d.h. es gilt $u \underset{P}{\to} v$.*

Beweis : Ist $v - u \in (P)$, dann gibt es eine Darstellung

$$v - u = \sum_{i=1}^{k} u_i \bar{p}_i v_i \quad \text{mit} \quad u_i v_i \in X^* \quad \text{und} \quad \bar{p}_i \in \rho(P).$$

Aufgrund der Symmetrie von P können wir annehmen, daß alle Koeffizienten in der Summe positiv sind. Wir führen den Beweis durch Induktion nach k. Für $k = 0$ und $k = 1$ ist der Satz offensichtlich richtig. Sei nun $k > 1$.

Es gibt dann ein i, $1 \leqslant i \leqslant k$, mit $u_i \bar{p}_i v_i = w - u$. Wir dürfen annehmen, daß $i = 1$ ist. Es gibt, wie bereits festgestellt wurde, dann ein $f_1 \in C(P)$ mit $f_1 : u \to w$.

Nun ist

$$v - w = (v - u) - (w - u) = \sum_{i=2}^{k} u_i \bar{p}_i v_i.$$

Nach Induktionsannahme gibt es ein $f_2 : w \to v$ in $C(P)$. Wegen $f = f_1 \circ f_2 \in C(P)$ gibt es auch $f \in C(P)$ mit $f : u \to v$, was zu zeigen war.

(*) Lemma 1 und Lemma 2 verallgemeinern zwei Lemmata in [1], die für kommutative Semi-Thue-Systeme eine analoge Aussage machen.

Lemma 2 Gilt ohne die Voraussetzung »P symmetrisch« nicht allgemein, sondern nur unter der Einschränkung, daß es für $v-u$ eine Darstellung mit positiven Koeffizienten gibt. Wir fassen diese Resultate in dem folgenden Satz zusammen.

SATZ 2 : *Ist G eine symmetrische Grammatik mit dem Axiom S und dem Produktionensystem P, dann gilt*

$$w \in L(G) \quad \Leftrightarrow \quad w \in S+(P) \qquad \text{und} \qquad w \in T^*.$$

Damit haben wir eine rein algebraische Definition der formalen Sprachen gewonnen. Das hilft uns zunächst natürlich nicht weiter. Wir sehen nur, daß die Frage, ob ein Polynom in der Restklasse eines zweiseitigen endlich erzeugten Ideals eines Ringes R liegt, schon für $R=\mathbb{Z}(T^*)$, nicht generell entscheidbar ist. Ebenso erkennen wir, daß das Problem, ob für zwei endlich erzeugte zweiseitige Ideale $\mathscr{A}_1$, $\mathscr{A}_2$ gilt $\mathscr{A}_1 \cap (T^*)=\mathscr{A}_2 \cap (T^*)$, nicht generell entscheidbar ist.

Was wir gewonnen haben, ist aber der Anschluß an eine Theorie, in der es zahlreiche Verfahren gibt, notwendige Kriterien zur Entscheidung unserer Probleme zu bestimmen. Wir sind insbesondere an effektiv berechenbaren Kriterien dieser Art interessiert. Ein solches Kriterium geben wir im übernächsten Abschnitt an. Zunächst befreien wir uns von der Voraussetzung, daß G symmetrisch sein muß.

4. SYMMETRISCHE GRAMMATIKEN

Wir zeigen in diesem Abschnitt, daß es zu jeder Grammatik G eine dazu symmetrische Grammatik G' gibt mit $L(G)=L(G')$. Darüber hinaus läßt sich eine solche Grammatik effektiv angeben.

Wir verwenden die Konstruktion von Post [8] in dem Beweis zur Nichtentscheidbarkeit des Wortproblemes für Thue-Systeme. In diesem Beweis beschreibt Post die Berechnung von Turingmaschinen durch Semi-Thue-Systeme P. Die Determiniertheit der Turingmaschine äußert sich darin, daß stets nur eine Produktion auf ein Wort anwendbar ist, das sich auf das Axiom reduzieren läßt. Hieraus ergibt sich, daß das durch den Übergang von P zu seiner symmetrischen Hülle erhaltene Produktionensystem $\overline{P}$ die gleiche Sprache definiert.

Nun bemerken wir noch, daß man zu jeder Grammatik G effektiv eine Turingmaschine T_G angeben kann, die $L(G)$ aufzählt. Damiterhalten wir zu G eine symmetrische Grammatik G', indem wir auf T_G die Post'sche Konstruktion anwenden. Also gilt in der Tat der

SATZ 3 : *Zu jeder Grammatik G läßt sich effektiv eine symmetrische Grammatik* G' *angeben mit* $L(G)=L(G')$.

Aus Satz 2 und Satz 3 folgt nun der

SATZ 4 : *Zu jeder Grammatik G läßt sich effektiv ein endlich erzeugtes zweiseitiges Ideal* $\mathscr{A}$ *in* $\mathbb{Z}(X^*)$ *angeben, so daß gilt :*

$$L(G)=(S+\mathscr{A})\cap(T^*).$$

Damit ist also gezeigt, daß sich zwei der Hauptprobleme der Theorie der formalen Sprachen vollständig in die Theorie der nicht kommutativen Algebra einbetten lassen. Allerdings muß man hierbei bemerken, daß wir dabei die hierarchische Gliederung der Grammatiken verloren haben. Dies ist insofern nicht gut, als entscheidbare Klassen von Problemen mit den nichtentscheidbaren in einen Topf gewandert sind.

5. VERSCHRÄNKTE HOMOMORPHISMEN FORMALER SPRACHEN

Sei $a=a(P,c,e)=c(P)\cup e(P)$ und (a) das durch a in $\mathbb{Z}[X]$ erzeugte zweiseitige Ideal.

Wir setzen

$$\mathscr{M}/(a)=\bigoplus_{x\in X}\mathbb{Z}[X]/(a)\,dx,$$

und bilden die freie Differentiation

$$d_a:\quad \mathbb{Z}(X^*)\rightarrow\mathscr{M}/(a).$$

Hierin sind e und c auf kanonische Weise verlängert zu Homomorphismen in $\mathbb{Z}[X]/(a)$.

LEMMA 3 : $d_a(P)$ *ist ein* $\mathbb{Z}(X^*)$*-Untermodul von* $\mathscr{M}/(a)$. *Hierbei ist für* $h\in\mathbb{Z}(X^*)$ *und* $f\in\mathscr{M}/(a)$ $h.f:=c(h).f$.

Beweis : Zu $f\in d_a((P))$ finden wir ein $f'\in(P)$ mit $d_a(f')=f$. Für beliebiges $g\in\mathbb{Z}(X^*)$ ist dann $g.f'\in(P)$. Wir betrachten

$$d_a(g.f')=d_a(g).e(f')+c(g).d_a(f').$$

Wegen $e(f')=0$ folgt nun

$$d_a(g.f')=c(g).f \qquad \text{und} \qquad g.f\in d_a((P)).$$

Also ist $d_a((P))$ ein $\mathbb{Z}(X^*)$ Unter-Modul von $\mathscr{M}/(a)$.

LEMMA 4 : *Der* $\mathbb{Z}(X^*)$*-Modul* $d_a((P))$ *wird durch* $d_a(P)$ *erzeugt, falls gilt* $e(\mathbb{Z}(X^*))\subset c(\mathbb{Z}(X^*))$.

Beweis : Jedes $f \in (P)$ läßt sich darstellen in der Form

$$f = \sum_i h_i p_i h'_i \quad \text{mit} \quad h_i, h'_i \in \mathbb{Z}(X^*) \quad \text{und} \quad p_i \in P.$$

Wir bilden

$$d_a(f) = \sum_i [d_a(h_i)\, e(p_i)\, e(h'_i) + c(h_i)\, d_a(p_i)\, e(h'_i)$$
$$+ c(h_i)\, c(p_i)\, d_a(h'_i)] = \sum c(h_i) . e(h'_i)\, d_a(p_i). \quad \binom{\star}{\star}$$

Es liegt also $d_a(f)$ in dem von $d_a(P)$ erzeugten $\mathbb{Z}(X^*)$-Modul.

Wir haben damit die Möglichkeit gewonnen in Abhängigkeit von e und c effektiv entscheidbare notwendige Kriterien für das Wortproblem formaler Sprachen anzugeben. Dies ist der Inhalt des folgenden Satzes.

SATZ 6 : *Zu jeder Grammatik G und jedem Paar c, e von Homomorphismen läßt sich effektiv ein $\mathbb{Z}(X^*)$-Modul $\mathcal{M}/(a)$ angeben und ein $\mathbb{Z}(X^*)$-Unter-Modul $(d_a(P))$, so daß $w \in L(G)$ nur dann gilt, wenn $d_a(w - S) \in (d_a(P))$ ist.*

Hieraus gewinnt man auch ein notwendiges Kriterium für die Frage $L(G_1) \cap L(G_2) = \emptyset$.

Seien $G_i = (X_i, T, P_i, S)_{i=1,2}$ zwei Grammatiken.

Wir dürfen annehmen, daß $(X_1 - T) \cap (X_2 - T) = \{S\}$ ist. Setzen wir $G'_i = (X_1 \cup X_2, T, P_i, S)_{i=1,2}$, dann ist $L(G_i) = L(G'_i)$.

Wir betrachten nun

$$d_{a_i} : \quad \mathbb{Z}((X_1 \cup X_2)^*) \to \mathcal{M}/(a_i) \qquad \text{für} \quad i = 1, 2.$$

Es seien

$$\varkappa_1 : \quad \mathcal{M}/(a_i) \to \mathcal{M}/(a_1 \cup a_2),$$
$$\varkappa_2 : \quad \mathcal{M}/(a_2) \to \mathcal{M}/(a_1 \cup a_2),$$

die zu diesen Faktorisierungen gehörigen kanonischen Abbildungen.

Setzen wir

$$d_2 = \varkappa_2 \circ d_{a_2} \qquad \text{und} \qquad d_1 = \varkappa_1 \circ d_{a_1},$$

dann ist $d_1 = d_2$. Also gilt

SATZ 7 : *Ist $L(G_1) \cap L(G_2) \neq \emptyset$, dann ist*

$$(d_1(S) + d_1((P_1))) \cap (d_1(S) + d_1((P_2))) \cap d_1(T^*) \neq \emptyset.$$

Es wäre natürlich schön, wenn

$$d_a(L(G)) = [d_a(S) + d_a((P_1))] \cap d_a(T^*),$$

gelten würde. Daß dies aber nicht der Fall ist, ergibt sich aus dem folgenden

Beispiel : $X=\{s, x, y, t\}$, $T=\{tr\}$, $G=(X, T, P, S)$.
P sei gegeben durch

$$S \to xy, \qquad xyx \to yxx, \qquad yx \to tr.$$

G ist eine kontext-sensitive Grammatik.
Offensichtlich ist $L(G)=\emptyset$.
Wir bilden

$$\begin{aligned} d(xy-S)+d(yxx-xyx)+d(tr-yx) \\ &= dxy-dS+dyx.e(x)+c(yx)dx \\ &\qquad -dxye(x)-c(xy)dx+dtr-dyx. \end{aligned}$$

Mit $e(x)=1$ erhalten wir hieraus aufgrund der Kommutativität von $\mathbb{Z}[X]$:

$$-dS+dtr.$$

Also gilt $dS+(d(P))\neq\emptyset$ im Gegensatz zu $L(G)=\emptyset$.

Es stellt sich damit die Frage nach dem Bild von $L(G)$ unter den Abbildungen d_a.

Betrachten wir den Sonderfall $e(x)=c(x)=1$, dann brauchen wir nicht nach (a) zu faktorisieren, da wegen $c(P)=e(P)=0$ die entsprechenden Summanden in $d(f)$ von selbst wegfallen.

Wir haben dann

$$d(u.v)=d(u)+d(v).$$

Also d macht hier T^* einfach kommutativ. Dieser Fall wurde von Parikh behandelt. Bekanntlich konnte er das Bild $d(L)$ für kontextfreie Sprachen L charakterisieren unter Heranziehung der Terminologie von Semi-Modulen. $d(L)$ erwies sich als Vereinigung endlich vieler Restklassen von endlich vielen Unter-Semi-Modulen des durch T erzeugten freien Semi-Moduls. Diese Mengen werden im allgemeinen als semilineare Mengen bezeichnet.

Dieser Satz von Parikh stellt ein starkes Kriterium für die Aquivalenz k.f. Sprachen dar. Allerdings besitzt es eine recht große Komplexität. In [5] wird gezeigt, daß dies Problem log.-vollständig ist in der 2. Klasse der Polynomzeithierarchie.

Aus diesem Grund muß man auch an eventuell schwächeren, aber leichter entscheidbaren Kriterien interessiert sein. Solche Kriterien entwickeln wir im nächsten Abschnitt für k.f. Sprachen. Hierzu bilden wir den Quotienten von $\mathscr{M}/(a)$ nach dem $\mathbb{Z}(X^*)$-Untermodul $(d_a(P))$. Wir setzen

$$\mathscr{M}(P, e, c)=(\mathscr{M}/(a))/(d_a(P)).$$

Wir verlängern d_a in kanonischer Weise zu einem verschränkten Homomorphismus

$$\tilde{d} : \ \mathbb{Z}(X^*) \to \mathscr{M}(P, e, c),$$

und haben wegen $\binom{\star}{\star}$ im Beweis zu Lemma 4 das

LEMMA 5 : *Für* $f \in (P)$ *gilt* $\tilde{d}(f) = 0$.

Wir wenden uns der Frage zu, gegenüber welchen Grammatiktransformationen $\mathscr{M}(P, e, c)$ invariant ist.

6. EIN INVARIANZKRITERIUM FÜR FORMALE SPRACHEN

Wir definieren zwei elementare Transformationstypen für Grammatiken.

DEFINITION : Seien G_1 und G_2 Grammatiken.

T 1 : Wir schreiben $G_1 \overset{(1)}{—} G_2$ genau dann, wenn gilt

$$S_1 = S_2, \quad X_2 = X_1 \cup \{x\}, \quad x \notin X_1, \quad T_1 = T_2,$$
$$P_2 = P_1 \cup \{p\}, \quad p = (u, v), \quad u = u' x u'', \quad u', u'', v \in X_1^*.$$

T 1 *c* : Wir schreiben $G_1 \overset{(1c)}{—} G_2$ genau dann, wenn gilt

$$S_1 = S_2, \quad X_2 = X_1 \cup \{x\}, \quad x \notin X_1, \quad T_1 = T_2,$$
$$P_2 = P_1 \cup \{p\}, \quad p = (x, v), \quad v \in X_1^*.$$

T 2 : Wir schreiben $G_1 \overset{(2)}{—} G_2$ genau dann, wenn (*a*) und (*b*) gelten :
(*a*) $S_1 = S_2$, $X_1 = X_2$, $T_1 = T_2$, $P_2 = P_1 \cup \{p\}$;
(*b*) es gibt zu $p = (u, v)$ Ableitungen

$$S \underset{G_1}{\longrightarrow} u_1 u u_2, \quad u_1 v u_2 \underset{G_1}{\longrightarrow} w_2, \quad S \underset{G_1}{\longrightarrow} w_2.$$

T 3 : G heißt elementarverwandt (*c*-elementarverwandt), in Zeichen $G \sim G'$ ($G \underset{c}{\sim} G'$), falls es eine Kette $G = G_1, G_2, \ldots, G_k = G'$ von Grammatiken G_i gibt mit $k \geqq 1$ und

$$G_i \overset{(1)}{—} G_{i+1} \quad \text{oder} \quad G_{i+1} \overset{(1)}{—} G_i \left(G_i \overset{(1c)}{—} G_{i+1} \text{ oder } G_{i+1} \overset{(1c)}{—} G_i \right)$$

oder

$$G_i \overset{(2)}{—} G_{i+1} \quad \text{oder} \quad G_{i+1} \overset{(2)}{—} G_i \quad \text{für } i = 1, \ldots, k-1.$$

SATZ 8 : *Sind* G *und* G' *reduzierte kontextfreie Grammatiken, dann gilt* $L(G) = L(G')$ *genau dann, wenn* $G \underset{c}{\sim} G'$ *gilt.*

Dieser Satz wird in [3] nicht explizit ausgesprochen. In dem Beweis der Invarianz der zu G gehörigen Gruppe wird aber gerade der Satz 8 bewiesen.

Wir wollen zeigen, daß $\mathcal{M}(P, e, c)$ für gewisse e und c unter (T 1 c) und (T 2) invariant sind.

LEMMA 6 : *Sind G und G' Grammatiken mit $G \overset{(1c)}{\text{——}} G'$, dann ist $\mathcal{M}(P', e, c)$ isomorph zu $\mathcal{M}(P, e, c)$ für $c(x) = \pm x$, $e(x) = 1$ oder $c(x) = 1$, $e(x) = \pm x$ oder $c(x) = e(x) = \pm x$. Für $c(x) = e(x) = 1$ gilt das analoge Resultat, wenn wir anstelle von $\mathcal{M}(P, e, c)$ den Modul $\bigoplus_{x \in X} \mathbb{Z}\, dx/(d_a(P))$ setzen.*

Beweis : Sei also $X \cup \{z\} = X'$, $z \notin X$, $p = (z, v)$ und $v \in X^*$.

Wir vergleichen zunächst $\mathbb{Z}[X]/(a(P))$ mit $\mathbb{Z}[X']/(a(P'))$, worin $a(P) = c(P) \cup e(P)$ gesetzt wurde.

c und e sind Homomorphismen, so daß in $\mathbb{Z}[X']/(a(P'))$ gilt

$$c(z) = c(v), \qquad e(z) = e(v).$$

Aufgrund unserer Voraussetzung geht entweder eine der beiden Relationen in eine Identität über, oder beide Relationen fallen zu einer zusammen. Also induziert die Abbildung $\varphi : X' \to X^*$ mit $\varphi(x) = x$ für $x \in X$ und $\varphi(z) = c(v)$ bzw. $\varphi(z) = e(v)$, je nachdem ob c oder e nicht trivial ist, einen Isomorphismus zwischen $\mathbb{Z}[X]/(a(P))$ und $\mathbb{Z}[X']/(a(P'))$. Sind c und e trivial, dam ist $a(P)$ das O-Ideal. In diesem Falle betrachten wir $\mathbb{Z}$ allein anstelle von $\mathbb{Z}[X]$ bzw. $\mathbb{Z}[X']$.

Wir betrachten nun die $\mathbb{Z}(X^*)$-Untermodule

$$\mathcal{M}(P, e, c) \qquad \text{und} \qquad \mathcal{M}(P', e, c).$$

Wir haben in $\mathcal{M}(P', e, c)$:

$$d_a(z - v) = d_a(z) - d_a(v) = 0,$$

und also

$$d_a(z) = d_a(v).$$

Also induziert

$$d_a(x) \mapsto d_a(x) \qquad \text{für} \quad x \in X,$$
$$d_a(z) \mapsto d_a(v),$$

einen Isomorphismus von $\mathcal{M}(P', e, c)$ auf $\mathcal{M}(P, e, c)$.

LEMMA 7 : *Sind G und G' Grammatiken und ist* $G \overset{(2)}{—} G'$, *dann sind* $\mathcal{M}(P, e, c)$ *und* $\mathcal{M}(P', e, c)$ *isomorph, falls* $(a(P))$ *prim ist und* $e(S) \neq 0$, $c(S) \neq 0$.

Beweis : Aufgrund von T 2 gilt mit $\tilde{p} = v - u$;

$u_1 \tilde{p} u_2 = (S - u_1 u u_2) + (u_1 v u_2 - w_2) + (w_2 - S)$ und also $u_1 \tilde{p} u_2 \in (P)$. Hieraus folgt wegen $(a(P))$ prim und $e(u_1 u_2) \neq 0$, $c(u_1 . u_2) \neq 0$;

$e(\tilde{p}) = c(\tilde{p}) = 0$ in $\mathbb{Z}[X]/(a(P))$.

Also gilt weiter

$$0 = d_a(u_1 \tilde{p} u_2) = d_a(u_1)\, e(\tilde{p})\, e(u_2) + c(u_1)\, d_a(\tilde{p})\, e(u_2) + c(u_1)\, c(\tilde{p})\, d_a(u_2),$$

und schließlich

$$d_a(\tilde{p}) = 0 \quad \text{in } \mathcal{M}(P, e, c).$$

Daher ist $\mathcal{M}(P, e, c)$ isomorph zu $\mathcal{M}(P', e, c)$, wie behauptet wurde.

Aus Lemma 6 und Lemma 7 und Satz 8 folgt nun unmittelbar der

SATZ 9 : *Sind G und G' reduzierte kontextfreie Grammatiken, dann ist* $\mathcal{M}(P, e, c) \cong \mathcal{M}(P', e, c)$ *für* $e(S) \neq 0$, $c(S) \neq 0$, $(a(P))$ *prim und für* $c(x) = \pm x$, $e(x) = 1$ *oder* $c(x) = 1$, $e(x) = \pm x$ *oder* $c(x) = e(x) = \pm x$, $x \in X \cup X'$.

Für $c(x) = e(x) = 1$ gilt dieser Satz ohne Einschränkung für $\oplus \mathbb{Z} dx/(d_a(P))$.

Wir können Lemma 6 und Lemma 7 unter schwächeren Voraussetzungen auch für die Transformation T 1 zeigen, wenn wir anstelle des Monoidringes $\mathbb{Z}(X^*)$ den Gruppenring $\mathbb{Z}(F(X))$ setzen. $F(X)$ ist die durch X erzeugte freie Gruppe. Mit $A(X)$ bezeichnen wir die multiplikative freie abelsche Gruppe, die durch X erzeugt wird. Anstelle von $\mathbb{Z}[X]$ haben wir dann $\mathbb{Z}(A(X))$. Im übrigen übertragen sich nun alle Definitionen in selbstverständlicher Weise von den Monoidringen auf die Gruppenringe. Zur Unterscheidung versehen wir die so erhaltenen $\mathbb{Z}(F(X))$-Module mit dem Index $\mathcal{M}_\gamma$. Wir verwenden also $\mathcal{M}_\gamma(P)$ und $\mathcal{M}_\gamma(P, e, c)$. e und c sind nun Gruppenringhomomorphismen.

LEMMA 8 : *Seien G und G' Grammatiken mit* $G \overset{(1)}{—} G'$.
Für

$$c(x) = \pm x, \quad e(x) = 1 \qquad \textit{oder} \qquad c(x) = 1, \quad e(x) = \pm x$$

oder $c(x) = e(x) = \pm x$ *für* $x \in X'$

ist $\mathcal{M}_\gamma(P, e, c)$ *isomorph zu* $\mathcal{M}_\gamma(P', e, c)$.

Beweis : Sei also $X \cup \{z\} = X'$, $z \notin X$, $p = (u, v)$, $u = u_1 z u_2$ und $u_1 u_2 v \in X^*$. Wir vergleichen zunächst $\mathbb{Z}(A(X'))/(a(P'))$ mit $\mathbb{Z}(A(X))/(a(P))$, worin $a(P) = c(P) \cup e(P)$ gesetzt ist.

c und e sind Homomorphismen, so daß in $\mathbb{Z}(A(X'))/a(P')$ gilt

$$c(z) = c(u_1)^{-1}.c(v).c(u_2)^{-1}, \qquad e(z) = e(u_1)^{-1}.e(v).e(u_2)^{-1}.$$

Diese beiden Relationen liefern aufgrund der Voraussetzungen nur eine Bedingung für z, die dazu explizit ist. Also sind $\mathbb{Z}(A(X'))/(a(P'))$ und $\mathbb{Z}(A(X))/(a(P))$ isomorph.

Wir betrachten nun die $\mathbb{Z}(F(X))$-Unter-Module $(d_a(P))$ und $(d_a(P'))$ von $\mathscr{M}_{\gamma/P}$ bzw. $\mathscr{M}'_{\gamma/P'}$.

Wir haben

$$d_a(u_1 z u_2 - v) = d_a u_1 e(z) e(u_2) + c(u_1) d_a(z) e(u_2) + c(u_1) c(z) d_a(u_2) - d_a(v).$$

In $\mathscr{M}_\gamma(P', e, c)$ gilt

$$d_a(z) = -\frac{d_a(u_1) e(z) e(u_2) + c(u_1) c(z) d_a(u_2) - d_a v}{c(u_1).e(u_2)}.$$

Aufgrund des ersten Teiles des Beweises können wir auf der rechten Seite $e(z)$ und $c(z)$ durch Elemente aus $\mathbb{Z}(A(X))/(a(P))$ ersetzen. Also ist $\mathscr{M}_\gamma(P', e, c)$ isomorph zu $\mathscr{M}_\gamma(P, e, c)$, was zu zeigen war.

LEMMA 9 : *Sind G und G' Grammatiken und ist $G \overset{(2)}{—} G'$, dann ist $\mathscr{M}_\gamma(P, e, c)$ isomorph zu $\mathscr{M}_\gamma(P', e, c)$, falls $c(F(X)) \subset F(X) \cup -F(X)$ und $e(F(X)) \subset F(X) \cup -F(X)$ ist.*

Beweis : Aufgrund von T 2 gilt mit $\tilde{p} = v - u$:

$u_1 \tilde{p} u_2 = (S - u_1 u u_2) + (u_1 v u_2 - w_2) + (w_2 - S)$ und also $u_1 \tilde{p} u_2 \in (P)$. Da wir uns im Gruppenring befinden, gilt

$$\tilde{p} = u_1^{-1}(u_1 \tilde{p} u_2) u_2^{-1} \in (P).$$

Also haben wir

$$e(\tilde{p}) = c(\tilde{p}) = 0 \quad \text{in } \mathbb{Z}(A(X))/(a(P)).$$

Daher gilt weiter

$$0 = d_a(u_1 \tilde{p} u_2) = d_a(u_1) e(\tilde{p} u_2) + c(u_1) d_a(\tilde{p}) e(u_2) + c(u_1 \tilde{p}) d_a(u_2),$$

und schließlich

$$c(u_1).e(u_2) d_a(\tilde{p}) = 0.$$

Da wir uns im Gruppenring befinden folgt $d_a(\tilde{p})=0$ und daraus die behauptete Isomorphie.

Aus dem Lemmata 8 und 9 und dem Satz 8 folgt der

SATZ 10 : *Sind G und G' reduzierte kontextfreie Grammatiken, dann ist* $\mathcal{M}_\gamma(P, e, c)$ *isomorph zu* $\mathcal{M}_\gamma(P', e, c)$ *und zwar in den folgenden Fällen :*

$$c(x)=\pm x, \quad e(x)=1; \qquad c(x)=1, \quad e(x)=\pm x; \qquad c(x)=e(x)=\pm x.$$

Hierdurch wird das Kriterium in [3], das die Invarianz der Alexanderideale für kontextfreie Grammatiken feststellt, um weitere berechenbare notwendige Kriterien ergänzt. Ist $\mathbb{Z}[X]/(a(P))$ ein euklidscher Ring, dann läßt sich jenes Kriterium aus diesem für $c(x)=x$, $e(x)=1$ mittels des Hauptsatzes für abelsche Gruppen ableiten.

Ein Beispiel und Schlußbemerkung : Wir wenden unser Kriterium auf das Wortproblem für die Dycksprache an. Sei

$$X=\{S, a, a', b, b'\}, \qquad T=\{a, a', b, b'\},$$

und

$$P=\{S\to S^2, S\to 1, S\to aSa', S\to bSb'\}.$$

Ist $\overline{P}$ der symmetrische Abschluß von P, dann gilt offensichtlich $L(G)=L(\overline{G})$. Also ist unser Kriterium anwendbar.

Wir betrachten die Basis des Ideals $(\overline{P})$. Man hat

$$S-1=0, \qquad S-S^2=0, \qquad S-aSa'=0, \qquad S-bSb'=0.$$

Hieraus ergibt sich das äquivalente System

$$S=1, \qquad aa'=1, \qquad bb'=1.$$

Wir bilden $d\overline{P}$ mod $(\overline{P})$. Durch einfache Reduktionen erhält man die Basis dS, $da+ada'$, $db+bdb'$. $(\star)$

Wir fragen : $aba'b'\in L(G)$?

Wir bilden

$$d(S-aba'b')=dS-da-adb-abda'-aba'db'.$$

Ist $aba'b'\in L(G)$, dann läßt sich $d(S-aba'b')$ mittels $(\star)$ darstellen. Wir machen den entsprechenden Ansatz :

$$\lambda_1 dS+\lambda_2(da+ada')+\lambda_3(db+bdb')=d(S-aba'b')$$

und erhalten für λ_2 und λ_3 nicht erfüllbare Bedingungen. Also ist $aba'b'\notin L(G)$.

Unser Kriterium ist also unabhängig vom Satz von Parikh, der über $aba'b' \in L(G)$ keine Auskunft gibt.

Dieses Beispiel ist sehr einfach. Es stellt sich natürlich die Frage nach der Kraft des Kriteriums. Eine Erprobung des Kriteriums an einer Grammatik G, für die die Frage $t^2 \in L(G)$ mit der Frage »$\sqrt{2}$ rational« äquivalent ist, hat leider zu einer trivialen Bedingung geführt. Die Faktorisierung nach $\bar{p}$ machte in diesem Falle alles zu 0.

Grundsätzlich sollte dieses Kriterium aber mit zur Entscheidung von Problemen der Prädikatenlogik 1. Stufe beitragen können.

Die Komplexität des hier angegebenen Kriteriums ist noch offen. Das Wortproblem für endlich erzeugte Ideale in Polynomringen ist niedrig. Das Wortproblem für die hier betrachteten endlich erzeugten $\mathbb{Z}(X^*)$-Untermodule läßt sich auf die Lösung eines linearen ganzzahligen Gleichungsproblemes zurückführen.

Herrn Christoph Reutenauer danke ich für einige kritische Kommentare zu einer ersten Version dieser Arbeit; Herrn Bernd Becker für die Durchsicht der vorliegenden Fassung.

LITERATUR

1. E. Cardoza, R. Lipton und A. R. Meyer, *Exponential Space Complete Problems for Petri Nets and Commutative Semigroups*, 8th Annual A.C.M. Symp. on Theory of Computing, 1976, S. 50-54.
2. R. H. Fox »*Free Differential Calculus I*«. *Derivation in the free Grouping*. Ann. of Math., Bd 57, 1953, S. 547-560, R. H. Fox, »*Free Differential Calculus II*«. *The Isomorphism Problem*, Ann. of Math., Bd 59, 1954, S. 196-210.
3. G. Hotz, *Eine neue Invariante k. f. Sprachen*, Erscheint in Theoretical Computer Science, 1980.
4. G. Hotz, *Über die Darstellbarkeit des syntaktischen Monoides kontextfreier Sprachen*, R.A.I.R.O. Informatique théorique, Bd 13, 1979, S. 337-345.
5. T. Huynh, *Komplexität semilinearer Mengen*, Unveröffentlichtes Manuskript.
6. S. MacLane *Homology*, Springer-Verlag, Berlin, Heidelberg, Göttingen, 1963.
7. R. J. Parikh, *On Contextfree Languages*, J. Assoc. Comp. Mach., Bd 13, 1966, S. 570-581.
8. E. L. Post *Recursive Unsolvability of a Problem of Thue*, J. Symbolic Logic, Bd 12, 1947, S. 1-11.