Publ. I.R.M.A. Strasbourg, 1987, 340/S-15
Actes 15^{e} Séminaire Lotharingien, p. 67–75

Untermonoide freier Monoide

und eine Verallgemeinerung des Euklidischen Algorithmus

R. König, Erlangen

I. EINLEITUNG - Es sei A eine endliche Menge (von Buchstaben) und A^* das freie Monoid über A. Spricht man von einem Untermonoid M von A^*, so kann man dies konkret nur, wenn man ein Erzeugendensystem X, besser noch ein minimales Erzeugendensystem für M kennt. Da jedes Untermonoid von A^* ein eindeutig bestimmtes minimales Erzeugendensystem besitzt, bezeichnet man dieses als seine Basis B.

Im folgenden wird gezeigt, wie man für eine rationale Teilmenge X testen kann, ob sie eine Basis ist. Zu diesem Zweck definieren wir ein Produkt von Automaten, das wir im weiteren zu einem Test verwenden können, ob das gegebene X sogar ein Code ist. Als Nebenprodukt erhalten wir einen weiteren Beweis fur TILSONs Theorem [2], dass der Durchschnitt über eine Familie freier Untermonoide von A^* wieder ein freies Untermonoid von A^* ergibt. Aus dem Test entwickeln wir Verfahren zur Konstruktion der Basis bzw. der Basis der freien Hülle für gegebenes rationales X.

Sei also X eine Teilmenge von A^* und X^* das von X erzeugte Untermonoid. Mit X^+ bezeichnen wir die Menge $X^* - 1$ ($= X^* - \{1\}$), die von X erzeugte Unterhalbgruppe. Die Klasse Rat(A) ist die von der leeren Menge und den Buchstaben von A mit den folgenden Abschlussoperationen erzeugte Unterklasse von 2^{A^*}:

Wenn X und Y zu Rat(A) gehören, dann auch

-- $X + Y$ (= Vereinigung)
-- $X \cdot Y$
-- X^*

Unter einem A - Automaten verstehen wir ein Tripel $\mathcal{A} = (S, s_o, F)$, wobei

-- S eine Menge
-- $s_o \in S$ der Anfangszustand
-- $F \subseteq S$ die Menge der Endzustände

und $E \subseteq (S \times A \times S)$ eine Menge von Übergängen ist, die wir folgendermassen schreiben:

$$s_1 \xrightarrow{a} s_2$$

Ein Pfad ist eine Folge

$$s_1 \xrightarrow{a} s_2 \xrightarrow{b} s_3 \ldots\ldots s_n \xrightarrow{c} s_{n+1}$$

von aneinanderpassenden Übergängen. Er heisst erfolgreich, wenn

$$s_1 = s_o \text{ und } s_{n+1} \in F,$$

seine Beschriftung ist das Wort $ab\ldots c \in A^*$. Mit $|\mathcal{A}|$ bezeichnen wir die Menge aller Beschriftungen erfolgreicher Pfade in $\mathcal{A}$. Diese Bezeichnungen orientieren sich an EILENBERG [3], wo man auch Beispiele findet. Wir kennzeichnen Zustände durch $\bullet$, Anfangszustände durch $\dashrightarrow\bullet$ und Endzustände durch $\square$.

Rationale Mengen und endliche Automaten hängen eng zusammen durch das THEOREM von KLEENE:

$$\mathrm{Rat}(A) = \{\, |\mathcal{A}| \mid \mathcal{A} \text{ ist ein endlicher } A\text{ - Automat} \,\}.$$

Daraus folgt, dass Rat(A) eine Boolesche Algebra ist.

II. DER VERBAND ALLER BASEN - Die Abbildung $X \longmapsto X^*$ ist ein Hüll-operator auf 2^{A^*}, dessen abgeschlossene Mengen gerade die Untermonoide von A^* sind. Die Menge $\mathfrak{S}(A)$ der abgeschlossenen Teilmengen ist daher ein vollständiger algebraischer Verband mit den Operationen

$$X^* \wedge Y^* = X^* \cap Y^*$$
$$X^* \vee Y^* = (X \cup Y)^*.$$

Jedes Untermonoid M von A^* hat ein eindeutig bestimmtes minimales Erzeugendensystem $B(M) = M^+ - M.M^+$, die Basis von M. Für $X \subseteq A^*$ definieren wir B(X) als die Basis von X^*. Die Menge $\{\, B(X) \mid X \in 2^{A^*} \,\}$ ist mit den Operationen

$$X \wedge Y := B(X^* \cap Y^*)$$
$$X \vee Y := B(X \cup Y)$$

und

$$X \leq Y \iff X^* \subseteq Y^*$$

ein zu $\mathfrak{L}(A)$ isomorpher Verband. Da $B(X) = X^+ - X.X^+$, erhält man für rationales X auch ein rationales B(X). Wir werden im weiteren Verlauf sehen, dass diese Operationen für rationales X sogar effektiv sind.

Es sei X durch einen A - Automaten $\mathcal{A}$ gegeben. Da keine Basis das neutrale Element 1 enthält, nehmen wir an, 1 gehört nicht zu X, d. h. $X \subseteq A^+$. Weiter modifizieren wir den Automaten $\mathcal{A}$ so, dass gilt

(*) für alle $w \in A^+$: $s_o \xrightarrow{w} t \implies t \neq s_o$

d.h. der Anfangszustand ist durch nichtleere Wörter unerreichbar (dies nennen wir einen adjungierten Anfangszustand). Wenn (*) in $\mathcal{A}$ noch nicht erfüllt ist, dann nehmen wir zu S einen neuen Anfangszustand q hinzu und führen für jeden Übergang $s_o \xrightarrow{a} t$ in $\mathcal{A}$ einen zusätzlichen Übergang $q \xrightarrow{a} t$ ein. Auf diese Weise entsteht ein A - Automat $\mathcal{A}_X$ mit adjungiertem Anfangszustand und $|\mathcal{A}_X| = X$.

Nun definieren wir das Produkt einer Familie $(\mathcal{A}_i)_{i \in I}$ von A - Automaten $\mathcal{A}_i = (S_i, s_{o,i}, F_i)$, $(i \in I)$ durch

$$\boxtimes_{i \in I} \mathcal{A}_i = \left(\prod_{i \in I} S_i, (s_{o,i})_{i \in I}, \prod_{i \in I} F_i \right)$$

mit Übergängen

$$(s_i)_{i \in I} \xrightarrow{a} (t_i)_{i \in I}$$

genau dann, wenn

für alle $i \in I$ gilt $s_i \xrightarrow{a} t_i$ in $\mathcal{A}_i$

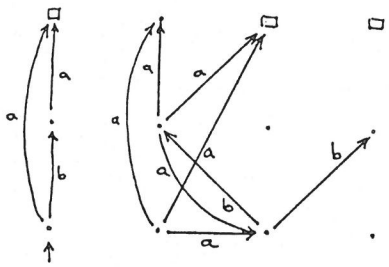
oder es gibt eine echte Teilmenge J von I mit

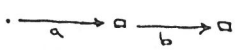
für alle $j \in J$ gilt $s_j \xrightarrow{a} f \in F_j$ und $t_j = s_{o,j}$

und für alle $i \in I - J$ gilt $s_i \xrightarrow{a} t_i$ in $\mathcal{A}_i$.

BEISPIEL: Sei X = a + ab, Y = a + ba

$\mathcal{A}_X \boxtimes \mathcal{A}_Y$





Wir bemerken, dass das Produkt von A - Automaten mit adjungierten Anfangszuständen wieder einen adjungierten Anfangszustand hat. Ebenso sieht man leicht, dass für beliebige $X_i \subseteq A^+$ $(i \in I)$ gilt:

(1) $$\left| \boxtimes_{i \in I} \mathcal{A}_{X_i} \right|^* = \bigcap_{i \in I} X_i^* \ .$$

Nun betrachten wir einen Pfad p in $\mathcal{A} \boxtimes \mathcal{A}$. p heisst

-- reflexiv, falls jeder Punkt auf p von der Form (s,s) ist mit $s \in S$,
-- linksseitig, falls kein Punkt auf p von der Form (s,s_0) und mindestens einer von der Form (s_0,s) ist,
-- rechtsseitig, wenn sein zugehöriger symmetrischer Pfad linksseitig ist,
-- einseitig, wenn p links- oder rechtsseitig ist,
-- zweiseitig, sonst.

Wir bezeichnen mit W(X) die Menge

{ w | w ist Beschriftung eines erfolgreichen einseitigen Pfades in $\mathcal{A}_X \boxtimes \mathcal{A}_X$ }

Dann gilt:

$$W(X) \subseteq X$$
$$B(X) = X - W(X)$$

Als Konsequenz ergibt sich: $X \in \mathfrak{L}(A) \iff W(X) = \emptyset$.

Für $X \in \mathrm{Rat}(A)$ ergibt sich damit ein Entscheidungsverfahren für die Frage

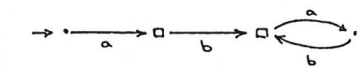
"Ist $X \in \mathfrak{L}(A)$?"

und ein Algorithmus zur Berechnung von B(X) aus X. Die Berechnung von $X \vee Y$ für rationale Basen X und Y ist ebenfalls effektiv:

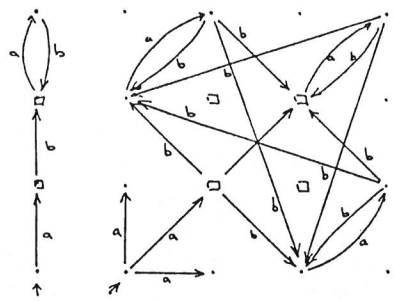
$$X \vee Y = B(X \cup Y)$$

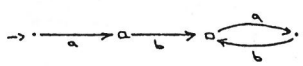
BEISPIEL: $Z = a + ab(ab)^*$

$\mathcal{A}_Z$:



$\mathcal{A}_Z \boxtimes \mathcal{A}_Z$:





$W(Z) = ab(ab)^*ab$

$B(Z) = Z - W(Z) = a + ab.$

THEOREM A:
Es sei $X_i \in \mathcal{L}(A)$ für $i \in I$. Dann ist $\bigwedge_{i \in I} X_i = \left| \boxtimes_{i \in I} \mathcal{A}_{X_i} \right|$.

Beweisidee: Da jedes X_i eine Basis ist, gibt es in $\mathcal{A}_{X_i} \boxtimes \mathcal{A}_{X_i}$ keinen erfolgreichen einseitigen Pfad für jedes $i \in I$. Aus einem erfolgreichen einseitigen Pfad in $\boxtimes_{i \in I} \mathcal{A}_{X_i} \boxtimes \boxtimes_{i \in I} \mathcal{A}_{X_i}$ lässt sich aber in wenigstens einer der Komponenten ein erfolgreicher einseitiger Pfad konstruieren. Zusammen mit (1) folgt dann die Behauptung. ∎

Als Spezialfall erhalten wir

$$X, Y \in \mathrm{Rat}(A) \Longrightarrow X \wedge Y \in \mathrm{Rat}(A)$$

Dies hat zur Folge:

> Der Verband aller rationalen Basen ist ein Unterverband des Verbands aller Basen.

BERECHNUNG von $X \wedge Y$ fur $X = a + ab$, $Y = a + ba$:
Wir betrachten wieder die Automaten aus dem ersten Beispiel und erhalten

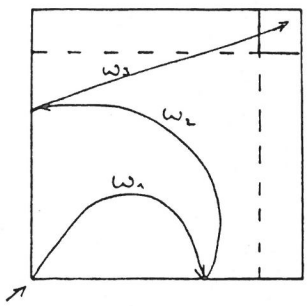
$$X \wedge Y = (ab)^* a.$$

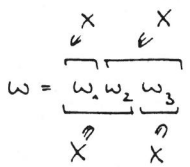
Dies zeigt (einmal mehr): Die Menge der endlichen Basen ist kein Unterverband des Verbands aller Basen. Aber es gilt: Sind X und Y endliche Basen, dann ist auch $X \vee Y$ eine endliche Basis, denn $X \vee Y \subseteq X \cup Y$.

III. DER VERBAND ALLER CODES - Eine Basis X heisst ein Code, wenn das von X erzeugte Untermonoid frei (über X) ist, d. h. aus $x_1, \ldots, x_n, y_1, \ldots, y_m \in X$ und $x_1 \ldots x_n = y_1 \ldots y_m$ folgt $n = m$ und $x_i = y_i$ für alle $i = 1, \ldots, n$.

THEOREM B: Es sei $X \subseteq A^+$. X^* ist genau dann frei, wenn es keinen erfolgreichen zweiseitigen Pfad in $\mathcal{A}_X \boxtimes \mathcal{A}_X$ gibt.

Beweisidee: Zu jedem erfolgreichen zweiseitigen Pfad in $\mathcal{A}_X \boxtimes \mathcal{A}_X$ gibt es eine Doppelfaktorisierung seiner Beschriftung w:





∎

Nun definieren wir die Menge V(X) als die Menge aller Wörter w , für die es einen erfolgreichen zweiseitigen Pfad wie im obigen Beweis gibt.

THEOREM C: Es seien X_i $(i \in I)$ Codes in A^*. Dann ist $| \boxtimes_{i \in I} \mathcal{A}_{X_i} |$ ein Code.

Beweisidee: Aus jedem erfolgreichen zweiseitigen Pfad in $\boxtimes_{i \in I} \mathcal{A}_{X_i} \otimes \boxtimes_{i \in I} \mathcal{A}_{X_i}$ lässt sich ein erfolgreicher zweiseitiger Pfad in einer der Komponenten gewinnen. ■

Korollar (Theorem von TILSON) : Beliebige Durchschnitte freier Untermonoide von A^* sind wieder frei. ■

Für jede Teilmenge X von A^* existiert daher der Durchschnitt

$$M_f(X) = \bigcap \{ M \mid M \text{ ist freies Untermonoid von } A^*, \text{ das X enthält } \}.$$

Er heisst die freie Hülle von X. Seine Basis $B_f(X)$ heisst der von X erzeugte Code. Die Abbildung $X \longmapsto M_f(X)$ ist ein algebraischer Hülloperator auf 2^{A^*}; ihm entspricht auf $\mathfrak{L}(X)$ der Hülloperator $X \longmapsto B_f(X)$. Die Menge $\mathfrak{C}(A)$ aller Codes ist daher wieder ein vollständiger algebraischer Verband mit den Operationen

$$X \sqcap Y = X \wedge Y$$
$$X \sqcup Y = B_f(X \cup Y).$$

Nun stellt sich natürlich die Frage: Wie berechnet man $X \sqcup Y$?
Um diese beantworten zu können, definieren wir für beliebige Teilmengen X von A^*

$$T_0 := X$$
$$T_{n+1} := T_n + V(T_n)$$

THEOREM D: $$\left(\bigcup_{n \geq 0} T_n \right)^* = \bigcup_{n \geq 0} T_n^* = M_f(X)$$ ■

Wenn X rational ist, können wir effektiv eine natürliche Zahl k angeben, so dass $T_{k+j} = T_k$ für alle natürlichen Zahlen j. k ist dabei die Anzahl der Elemente des syntaktischen Monoids von X^*. Dann gilt offenbar $B_f(X) = B(T_k)$ und $B_f(X)$ ist rational. Also bilden die rationalen Codes einen Unterverband des Verbands aller Codes, aber die endlichen Codes nicht. Damit können wir einen Algorithmus zur Berechnung von $B_f(X)$ angeben:

ALGORITHMUS E:

```
input X
begin
    T := X; S := 0
        while  T = S  do  S := T;
                          T := T + V(T);
                      od
    B_f(X) := T - W(T)
end
```

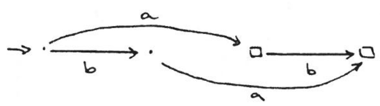
Über einem einelementigen Alphabet A ist $B_f(X)$ = ggT(X), wenn man jedes $w \in A^*$ mit seiner Länge identifiziert; daher reduziert sich in diesem Falle der Algorithmus E zum (langsamen) Euklidischen Algorithmus (auf den natürlichen Zahlen). Dann ist auch $\mathcal{L}$(A) nichts anderes als der Teilerverband über den natürlichen Zahlen.

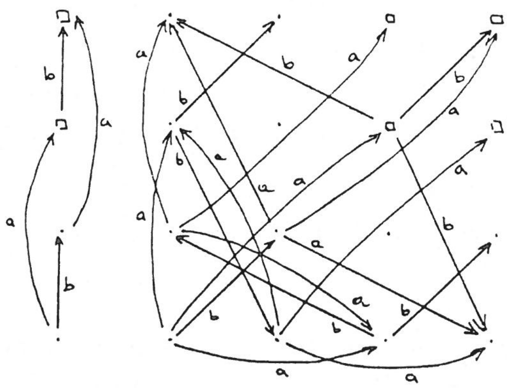
Berechnung von $X \sqcup Y$ für $X = a + ab$, $Y = a + ba$:

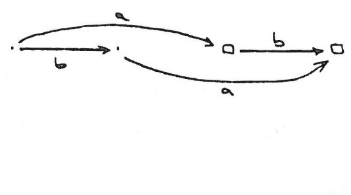
$Z = X + Y$ ist kein Code (aber eine Basis), denn $a.ba = ab.a$

Setze $T_o := Z$

$\mathfrak{A}_Z$:







$V(Z) = a + b$, also ist $T_1 = a + b + ab + ba$ und es folgt $T_2 = T_1$.
Daraus ergibt sich $X \sqcup Y = B_f(T_1) = a + b$.

IV. SCHLUSSBEMERKUNGEN - In der Literatur findet man mehrere Tests, ob eine gegebene Menge X ein Code ist:

(1) Sardinas - Patterson (1953)

(2) Spehner (1975)

(3) Blattner - Head (1977)

(4) Lallement (1979)

(5) Berstel - Perrin (1985)

(2) und (3) sind nur für endliche X effektiv, (4) ist eine geringfügige Modifikation von (2). (1) und (5) arbeiten zwar für rationale X, aber befriedigend nur dann, wenn X eine Basis ist; denn wenn X keine Basis, aber X^* frei ist, können sie darüber keine Auskunft geben.

In (2) findet man auch eine Konstruktion für $B_f(X)$, die aber wieder nur für endliche X effektiv ist. Berstel - Perrin - Perrot - Restivo (1979) geben eine Konstruktion für $M_f(X)$ mit Hilfe einer symmetrischen Version von (1).

Durch die Betrachtung des Automaten $\mathcal{A}_X \boxtimes \mathcal{A}_X$ kann man all diese Nachteile gleichzeitig vermeiden. Ausserdem kann man ihn benutzen, um weitere Klassen von Codes zu definieren (z. B. zirkuläre Codes, schwach zirkuläre Codes ...) und die entsprechenden Hülloperationen zu realisieren.

LITERATUR:

[1] Sardinas - Patterson :
A necessary and sufficient condition for the unique decomposition of coded messages
IRE Intern. Conv. Rec. 8 (1953), pp. 1o4 - 1o8

[2] Tilson, B.:
The intersection of free submonoids of a free monoid is free
Semigroup Forum 4 (1972), pp.345 - 35oL

[3] Eilenberg, S.:
Automata, Languages and Machines, vol. A
Academic Press (1974)

[4] Spehner, C.:
Quelques constructions et algorithmes relatifs aux sous-monoides d'un monoide libre
Semigroup Forum 9 (1975), pp. 334 - 353

[5] Blattner - Head:
Automata that recognize intersections of free submonoids
Inform. and Contr. 35 (1977), pp. 173 -176

[6] Lallement, G.:
Semigroups and Combinatorial Applications
Wiley (1979)

[7] Berstel - Perrin - Perrot - Restivo:
Sur le théorème du défaut
J. of Algebra 6o (1979), pp. 169 - 18o

[8] Berstel - Perrin:
Theory of Codes
American Press (1985)

Dr. Roman König
IMMD (Informatik) I
Universität Erlangen-Nürnberg
Martensstraße 3
D-8520 Erlangen

Electronic-mail: koenig@fauern.uucp