Seminararbeit

Tomáš Nagy

Endliche Halbgruppen

Ausgeführt unter der Anleitung von:
Associate Prof. Dipl.-Ing. Dr.techn. Stefan Hetzl

Wien, am 20. November 2019

Inhaltsverzeichnis

1. Syntaktisches Monoid

Wir führen hier eine Methode ein, die uns ermöglicht, jeder regulären Sprache ein endliches Monoid zuzuordnen. Diese Methode ermöglicht uns, viele Eigenschaften der Klassen regulärer Sprachen zu beschreiben.

Sei also A ein endliches Alphabet und $L \subseteq A$. Wir definieren auf A^* eine Äquivalenzrelation durch $a \equiv_L b$ genau dann, wenn $\{(u,v) \in A^* \times A^* \mid uxv \in L\} = \{(u,v) \in A^* \times A^* \mid uyv \in L\}$.

Diese Äquivalenzrelation ist sogar eine Kongruenz: Seien nämlich $x \equiv_L y$ und $a \equiv_L b$, dann ist $\{(u,v) \in A^* \times A^* | uxav \in L\} = \{(u,v) \in A^* \times A^* | uyav \in L\} = \{(u,v) \in A^* \times A^* | uybv \in L\}$, also $xa \equiv_L yb$.

Definition 1 (Syntaktisches Monoid)**.** *Sei A eine endliche Alphabet und $L \subseteq A$. Das* syntaktische Monoid *ist definiert durch $M(L) = A^*/\equiv_L$. Die Projektion $\eta_L : A^* \longrightarrow M(L)$ wird auch* syntaktischer Morphismus *genannt.*

Um ein einfaches Beispiel zu nennen, betrachten wir als L die Menge der Wörter gerader Länge im Alphabet $\{0,1\}$. Dann, $x \equiv_L y$ genau dann, wenn $|x| \equiv |y| mod 2$. $M(L)$ hat dann zwei Elemente - die Klasse der Wörter gerader Länge und die Klasse der Wörter ungerader Länge.

1.1 Reguläre Sprachen

Der folgende Satz erklärt uns die Bedeutung des syntaktischen Monoides:

Satz 1. *Sei A ein endliches Alphabet und $L \subseteq A^*$. Dann, L ist regulär genau dann, wenn $M(L)$ endlich ist.*

Beweis. Sei zuerst L regulär und $\mathcal{A} = (Q, i, F, \lambda)$ ein deterministischer endlicher Automat, der L erkennt.

Wir definieren eine Äquivalenzrelation $\sim$ auf A^* so dass $x \sim y$ genau dann, wenn für alle Zustände $q \in Q$ gilt, dass $q \cdot x = q \cdot y$.

Zuerst zeigen wir, dass diese Äquivalenzrelation die Relation $\equiv_L$ verfeinert: Seien also $x \sim y$ und $uxv \in L$. Dann gilt: $i \cdot (uyv) = ((i \cdot u) \cdot y) \cdot v = ((i \cdot u) \cdot x) \cdot v = i \cdot (uxv)$. Da $i \cdot (uxv) \in F$ nach Voraussetzung, $uxv \in L$. Wir können auch ganz ähnlich sehen, dass $uyv \in L$ auch $uxv \in L$ impliziert. Deshalb gilt, dass $x \equiv_L y$.

Da die Anzahl der $\sim$-Klassen höchstens $|Q|^{|Q|}$ ist (für festgewähltes $x \in A^*$ ist die Äquivalenzklasse $[x]_\sim$ eindeutig durch das $|Q|$-Tupel $(q \cdot x)_{q \in Q}$ beschrieben, es existieren aber höchstens $|Q|^{|Q|}$ solche Tupeln), gilt es auch, dass $|M(L)| \leq |Q|^{|Q|}$. Insbesonders ist $M(L)$ endlich.

Sei jetzt $M(L)$ endlich. Wir möchten einen deterministischen endlichen Automaten $\mathcal{A} = (Q, i, F, \lambda)$ konstruieren, der L erkennt:

Definiere $Q = M(L)$, $i = 1$, $F = \{[w]_L | w \in L\}$. Die Übergangsfunktion λ wird dann durch $[w]_L \cdot a = [wa]_L$ definiert.

Ein Wort $w \in A^*$ ist also genau dann akzeptiert, wenn $1 \cdot w = [w]_L$ ist gleich $[u]_L$ für ein Wort $u \in L$. Falls aber $[w]_L = [u]_L$ und $u \in L$, ist auch $1 \cdot w \cdot 1 = w \in L$. Falls umgekehrt $w \in L$, ist natürlich auch $[w]_L \in F$. Das heißt, dass $\mathcal{A}$ die Sprache L erkennt und da $M(L)$ endlich ist, heißt das, dass L regulär ist. □

Jetzt besteht die Frage, wie wir im allgemeinen Fall das syntaktische Monoid $M(L)$ berechnen können, falls wir den endlichen deterministischen Automat kennen, der L erkennt. Dazu wird der Begriff des Übergangsmonoid nützlich sein.

1.2 Übergangsmonoid

Definition 2 (Übergangsmonoid)**.** *Sei $\mathcal{A} = (Q, i, F, \lambda)$ ein deterministischer endlicher Automat. Definiere für jedes $w \in A^*$ eine Abbildung $f_w : Q \longrightarrow Q$ durch $f_w(q) = q \cdot w$. Wir definieren jetzt eine Monoid-Operation $\cdot$ auf der Menge aller Abbildungen f_w durch $f_x \cdot f_y = f_{xy}$. Das Monoid $M(\mathcal{A}) = (\{f_w, w \in A^*\}; \cdot)$ wird* Übergangsmonoid *von $\mathcal{A}$; genannt.*

Wir merken uns, dass wir schon im Beweis von Satz 1 gezeigt haben, dass für zwei Wörter $v, w \in A^*$ mit $f_v = f_w$ gilt, dass $v \equiv_L w$ (da $f_v = f_w$ genau dann, wenn $v \sim w$ in der Notation von Satz 1).

Falls wir aber annehmen, dass $\mathcal{A} = (Q, i, F, \lambda)$ ein minimaler Automat von L ist, können wir auch zeigen, dass $v \equiv_L w$ impliziert, dass $f_v = f_w$: Seien also $v \equiv_L w$ und $q \in Q$ und sei $u \in A^*$ so dass $q = i \cdot u$.

Definiere $q_1 = f_v(q) = i \cdot uv$ und $q_2 = f_w(q) = i \cdot uw$. Aus $v \equiv_L w$ folgt, dass für jedes $x \in A^*$, $uvx \in L$ genau dann, wenn $uwx \in L$. Also $q_1 \cdot x = i \cdot uvx \in F$ genau dann, wenn $q_2 \cdot x = i \cdot uwx \in F$. Da $\mathcal{A}$ minimal ist, gilt aber $f_v = f_w$.

Wir haben folgenden Satz bewiesen:

Satz 2. *Sei $\mathcal{A}$ ein minimaler Automat von L. Dann sind die Monoide $M(\mathcal{A})$ und $M(L)$ isomorph.*

Beweis. Definiere ein Isomorphismus $\phi : M(L) \longrightarrow M(\mathcal{A})$ durch $[v]_L \mapsto f_v$. □

Zum Ende möchten wir noch dem Zusammenhang zwischen allgemeine (auch unendliche) Monoide und syntaktischem Monoid verstehen. Dazu müssen wir zuerst zwei wichtige Begriffe definieren:

Definition 3. *Seien M_1 und M_2 zwei Monoide. Wir sagen, dass M_1* teilt *M_2, falls ein Untermonoid M von M_2 und ein surjektiver Homomorphismus $\phi : M \longrightarrow M_1$ existiert. Wir schreiben $M_1 \prec M_2$.*

Ein Monoid M erkennt *eine Sprache $L \subseteq A^*$, falls es existiert eine Menge $X \subseteq M$ und ein Homomorphismus $\phi : A^* \longrightarrow M$ so dass $L = \phi^{-1}(X)$. In diesem Fall sagen wir auch, dass ϕ die Sprache L erkennt.*

Satz 3. *Sei $L \subseteq A^*$ und sei $\phi : A^* \longrightarrow M$ ein Homomorphismus. ϕ erkennt L genau dann, wenn η_L durch ϕ faktorisiert (d. h. es existiert ein Homomorphismus ψ mit $\psi \circ \phi = \eta_L$). Ein Monoid M erkennt L genau dann, wenn $M(L) \prec M$.*

Beweis. Sei also zuerst L eine Sprache, die durch ϕ erkannt wird, d. h. es existiert $X \subseteq M$ so dass $L = \phi^{-1}(X)$. Seien $u, v \in A^*$ mit $\phi(u) = \phi(v)$. Falls zusätzlich $xuy \in L$, gilt es, dass $\phi(xuy) = \phi(xvy) \in X$, und deswegen $xvy \in L$. Ein duales Argument zeigt, dass $xvy \in L$ auch $xuy \in L$ impliziert. Das bedeutet aber, dass $u \equiv_L v$ und deshalb faktorisiert sich η_L durch ϕ und $M(L)$ ist ein homomorphes Bild von $\phi(A^*)$.

Sei jetzt $\psi : \phi(A^*) \longrightarrow M(L)$ ein Homomorphismus mit $\psi \circ \phi = \eta_L$. Falls $\phi(w) \in \phi(L)$, dann $\eta_L(w) = \psi \circ \phi(w) \in \eta_L(L)$, also $w \in L$. Damit haben wir

gezeigt, dass $w \in L$ genau dann, wenn $\phi(w) \in \phi(L)$ und deshalb wird L von ϕ erkannt.

Falls $M(L) \prec M$, dann existiert ein Untermonoid M_1 von M und ein surjektives Homomorphismus $\psi : M_1 \longrightarrow M(L)$. Wir können einen Homomorphismus $\phi : A^* \longrightarrow M$ auf folgender Art und Weise definieren: Wähle $\phi(a)$ für jedes $a \in A$ so dass $(\psi \circ \phi)(a) = \eta_L(a)$. Wir können dieses ϕ auf eine offensichtliche Weise auf den erwünschten Homomorphismus erweitern. Dann faktorisiert sich aber η_L offensichtlich durch ϕ und wie wir schon gezeigt haben, bedeutet das, dass ϕ L erkennt, d. h. dass M durch L erkannt wird. □

Die Methoden, die wir in dieser Kapitel vorgestellt haben, können angewendet werden, um viele Eigenschaften von reguläre Sprachen zu beweisen. Wir können damit z. B. elegant beweisen, dass die Menge der Wörter gerader Länge nicht in FO[<] liegt.

2. Pseudovarietäten

2.1 Pseudovarietäten und reguläre Sprachen

In diesem Kapitel führen wir den Begriff der Pseudovarietät ein. Wir zeigen lediglich ein paar wichtige Eigenschaften der Pseudovarietäten. Die Pseudovarietäten sind für uns wichtig, da verschiedene Pseudovarietäten von Monoide sind in Eins-zu-eins-Korrespondenz mit verschiedene Klassen von Sprachen. Ein Beispiel solcher Ergebnisse ist die Satz von Schützenberger [2, Theorem 2.7], die zeigt, dass die Klasse der aperiodische Monoide in eindeutiger Korrespondenz zu der Klasse der sternfreien Sprachen ist.

Definition 4 (Pseudovarietät)**.** *Sei V eine Familie algebraischer Strukturen derselber endlichen Signatur. Wir sagen, dass V eine* Pseudovarietät *ist, falls sie abgeschlossen unter endliche Produkten, Unteralgebren und homomorphische Bildern ist.*

Wir sehen, dass der einzige Unterschied zwischen Varietäten (wie sie in universeller Algebra eingeführt werden) und Pseudovarietäten die Abgeschlossenheit unter endlichen Produkten ist (die Varietäten sind unter belieblige Produkte abgeschlossen). Das heißt, dass der Begriff der Pseudovarietät eine Schwächung des Begriffes der Varietät darstellt. Wir werden aber in diesem Kapitel sehen, dass viele Eigenschaften der Varietäten auch für Pseudovarietäten gelten.

Uns werden nur Pseudovarietäten der endliche Monoide (bzw. Halbgruppen) interessieren, wir werden deshalb alle Eigenschaften nur für diese Pseudovarietäten zeigen. Die Verallgemeinerung einiger diesen Eigenschaften für allgemeine Pseudovarietäten ist aber nicht schwierig.

Falls wir die Notation, die wir im vorigen Kapitel eingeführt haben, benutzen, können wir den Begriff der Pseudovarietäten endlicher Monoide (bzw. Halbgruppen) auf folgender Weise umformulieren: Eine Familie endlicher Monoide (Halbgruppen) V ist Pseudovarietäat genau dann, wenn für alle $S, T \in V$ gilt, dass $S \times T \in V$ und für jedes $U \prec T$, $U \in V$.

Wir führen jetzt folgende Notation ein: Sei ϕ eine Formel erster Stufe so dass alle freie Variablen in ϕ in einer endliche Menge W liegen. In vorigen Vorträgen wurde die Notation L_ϕ für Menge aller W-Strukturen, die ϕ erfüllen eingeführt. Wir bezeichnen jetzt das syntaktische Monoid von L_ϕ durch $M(\phi)$, den dazugehörigen syntaktischer Morphismus durch η_ϕ und die Kongruenz von L_ϕ durch $\equiv_\phi$.

Wir verstehen A als eine Untermenge von $A \times 2^W$ durch die Einbettung $a \mapsto (a, \emptyset)$. Wir bezeichnen die Einschränkung von η_ϕ auf A^* durch θ_ϕ und das Bild von θ_ϕ durch $N(\phi)$.

Wir sagen, dass ein Monoid M *aperiodisch* ist, falls er keine nicht-triviale Gruppe enthält. Der folgende Satz fasst die Eigenschaften der Pseudovarietäten, die uns interessiern werden, zusammen:

Satz 4. *Seien ϕ und ψ Formeln, die reguläre Sprachen L_ϕ und L_ψ in $(A \times 2^V)^*$ definieren und sei V eine Varietät endlicher Monoide. Dann gilt:*

1. *Falls $N(\phi), N(\psi) \in V$, dann $N(\phi \wedge \psi), N(\neg\phi) \in V$.*

2. *Falls $M(\phi), M(\psi) \in V$, dann $M(\phi \wedge \psi)$. Falls zusätzlich V alle aperiodische kommutative Monoide enthält, dann auch $M(\neg\phi) \in V$.*

Beweis. Um den ersten Punkt zu beweisen, definiere zuerst den Homomorphismus $(\theta_\phi, \theta_\psi) : A^* \longrightarrow N(\phi) \times N(\psi)$. Seien $u, v \in A^*$ so dass $(\theta_\phi, \theta_\psi)(u) = (\theta_\phi, \theta_\psi)(v)$. Wir zeigen, dass $(\theta_{\phi\wedge\psi})(u) = (\theta_{\phi\wedge\psi})(v)$. Dann, selbstverständlich, $N(\phi \wedge \psi) \prec N(\phi) \times N(\psi)$, und deshalb $N(\phi \wedge \psi) \in V$.

Seien also $x, y \in (A \times 2^V)^*$ so dass $xuy \models \phi \wedge \psi$. Es folgt, dass $xuy \models \phi$ und $xuy \models \psi$, und deshalb $xvy \models \phi$ und $xvy \models \psi$. Das bedeutet aber, dass $xvy \models \phi \wedge \psi$. Der Beweis, dass $xvy \models \phi \wedge \psi$ impliziert $xuy \models \phi \wedge \psi$, ist dual.

Sei jetzt $\theta_\phi(u) = \theta_\phi(v)$ und sei $xuy \models \neg\phi$. Falls $xvy \models \phi$, dann folgt $xuy \models \phi$, was ein Widerspruch wäre. Deshalb gilt $xvy \models \neg\phi$. Die andere Implikation ist auf ähnliche Weise zu beweisen. Das heißt, dass $\theta_{\neg\phi}(u) = \theta_{\neg\phi}(v)$ und da $\neg\neg\phi$ zu ϕ äquivalent ist, folgt unmittelbar auch $\theta_\phi = \theta_{\neg\phi}$. Deshalb $N(\neg\phi) \in V$.

Jetzt bleibt uns noch der zweite Punkt übrig. Um diese Aussage für Konjuktion zu beweisen, können wir dieselbe Argumente wie oben benutzen, falls wir θ_ϕ durch η_ϕ ersetzen. Um die Aussage für Negation zu zeigen, müssen wir zuerst beweisen, dass $\eta_{\neg\phi}$ durch (η_ϕ, η_L) faktorisiert (wo L die Menge aller W-Strukturen bezeichnet). Dann folgt die Aussage aus der Beobachtung, dass $M(L)$ kommutativ ist und keine nicht-triviale Gruppe enthält. □

2.2 Pseudovarietäten definiert durch Gleichungen

Wir möchten jetzt zeigen, dass die Pseudovarietäten durch Erfüllung von Identitäten definiert werden können. Zuerst müssen wir aber den intuitiv einfach verständlicher Begriff 'Erfüllung von Gleichungen' definieren.

Definition 5. *Sei U eine abzählbare Sprache und seien $w_1, w_2 \in U^*$. Ein Monoid erfüllt die Gleichung $w_1 = w_2$, falls für jeden Homomorphismus $\zeta : U^* \longrightarrow M$, $\zeta(w_1) = \zeta(w_2)$.*

Wir können denselben Begriff auch für Halbgruppen definieren, wir müssen aber U^+ statt U^* betrachten.

Satz 5. *Sei U ein abzählbares Alphabet und sei $\{(w_i, w_i' : i > 0\} \subseteq U^* \times U^*$. Die Familie der endlichen Monoide, die alle Gleichungen $w_i = w_i'$ erfüllen, ist eine Pseudovarietät. Die Familie der Monoide, die alle bis auf endlich viele Gleichungen erfüllen, ist eine Pseudovarietät.*

Falls wir U^* durch U^+ ersetzen, gilt diese Behauptung auch für Halbgruppen.

Beweis. Sei V_i die Familie der Monoide, die die Gleichung $w_i = w_i'$ erfüllen. Wir können ganz einfach zeigen, dass V_i eine Pseudovarietät ist.

Wir können auch ganz einfach beweisen, dass der Schnitt von Pseudovarietäten wieder eine Pseudovarietät ist. Es folgt, dass die Familie der Monoide, die alle Gleichungen $w_i = w_i'$ erfüllen, eine Pseudovarietät ist, da die gleich $\bigcap\{V_i : i > 0\}$ ist.

Wir können auch einfach beweisen, dass die Vereinigung der Pseudovarietäten $A_i : i > 0$, so dass $A_i \subseteq A_j, i > j$, eine Pseudovarietät ist, woraus die letzte Behauptung folgt (Für $A_i = \bigcap\{V_j : j \geq i\}$). □

Dieser Satz ermöglicht uns, viele Beispiele von Pseudovarietäten zu konstruieren:

Beispiel. Die Gleichung $u = u$ definiert die Pseudovarietät, die genau alle endliche Monoide (bzw. Halbgruppen) enthält.

Die Gleichung $u = v$ definiert die Pseudovarietät, die lediglich die triviale, einelementige Gruppe, enthält.

Um zwei interessantere Beispiele zu nennen, zeigen wir, dass die Familie endlicher aperiodischer Monoide und die Familie aller endlicher Gruppen auch Pseudovarietäten endlicher Monoide sind.

Beispiel. Falls wir die Menge der Gleichungen $m^k = m^{k+1}, k > 0$ betrachten, können wir die Pseudovarietät endlicher aperiodischer Monoide bekommen als die Familie aller Monoide, die alle bis auf endlich viele diese Gleichungen erfüllen. Wir können nämlich zeigen, dass ein endlicher Monoid M aperiodisch ist genau dann, wenn es ein $k > 0$ existiert, so dass $m^k = m^{k+1}$ für alle $m \in M$ gilt (das ist eine einfache Übung).

Betrachten wir die Menge der Gleichungen $u^{i!} = 1, i > 0$ und sei V die Pseudovarietät der endlichen Monoide, die alle bis auch endlich viele diese Gleichungen erfüllen. Es ist ganz einfach zu sehen, dass alle endliche Gruppen in diese Varietät enthalten sind. Gleichzeitig gilt aber, dass jedes $G \in V$ enthält ein Element 1, das die Gruppenaxiome für 1 erfüllt.

Am Ende des Kapitels zeigen wir noch eine interessante Möglichkeit, die Pseudovarietäten zu konstruieren:

2.3 Pseudovarietät $\bar{V}$

Sei V eine Pseudovarietät endlicher Gruppen. Dann ist $\bar{V}$ definiert als die Familie der endlichen Monoide M, so dass jede Gruppe, die in ein $M \in V$ enthalten ist, in V liegt.

Satz 6. *$\hat{V}$ ist eine Pseudovarietät endlicher Monoide.*

Beweis. $\hat{V}$ ist offensichtlich abgeschlossen unter Untermonoide.

Sei $M \in \hat{V}$ und $N = \phi(M)$ ein Quotient von M. Sei G eine Gruppe in N und H die kleinste Unterhalbgruppe in M, so dass $\phi(H) = G$. Dann, für alle $h \in H$, $\phi(hH) = \phi(h)G = G = g\phi(h) = \phi(hH)$. Da H die kleinste Unterhalbgruppe ist, folgt umittelbar, dass $Hh = H = hH$. H ist also eine Gruppe und da $H \in V$, folgt, dass $G \in V$ und deshalb auch $N \in \hat{V}$.

Jetzt müssen wir noch zeigen, dass $\hat{V}$ unter endlichen Produkte abgeschlossen ist. Seien dazu $M, N \in V$ und G eine Gruppe, die in $M \times N$ enthalten ist. Die Projektionen G_1 und G_2 von G auf M_1 und M_2 sind offensichtlich Gruppen und G ist eine Untergruppe von $G_1 \times G_2$. Da aber $G_1 \times G_2 \in V$, gilt auch $G \in V$ und deshalb auch $M_1 \times M_2 \in \hat{V}$. □

3. Blockprodukt

3.1 Semidirektes Produkt

In diesem Kapitel möchten wir einen anderen Begriff, der für die folgende Vorträge wichtig wird, vorstellen. Bevor wir aber das Blockprodukt definieren können, müsen wir zuerst den Begriff des semidirekten Produktes verstehen.

Im Folgenden seien S und T endliche Halbgruppen. Wir bezeichnen die Halbgruppenoperation in S durch $+$ (obwohl diese natürlich nicht kommutativ sein muss!), falls S ein Monoid ist, wird die Identität in S durch 0 bezeichnet. Falls S eine Gruppe ist, bezeichnen wir das inverse Element durch $-s$.

Definition 6 (Linksaktion)**.** *Eine* Linksaktion *von T auf S ist eine Abbildung $(T \times S \longrightarrow S, (t, s) \mapsto ts$, die folgende Eigenschaften für alle $t_1, t_2 \in T$, $s_1, s_2 \in S$ erfüllt:*

- $t_1(s_1 + s_2) = t_1s_1 + t_1s_2$,
- $(t_1t_2)s_1 = t_1(t_2s_1)$.

Seien S und T Monoide. Wir nennen die Linksaktion monoidisch*, falls sie zusätzlich für alle $s \in S$ und $t \in T$ folgende Eigenschaften erfüllt:*

- *1s=s,*
- *t0=0.*

Wir können die *Rechtsaktion* auf ähnlicher Weise definieren.

Definition 7 (kompatible Aktionen)**.** *Linke und rechte Aktion sind* kompatibel *genannt, falls für alle $t, t' \in T$ und $s \in S$, $(ts)t' = t(st')$.*

Im Falle einer kompatibler Aktion können wir den Ausdruck tst' ohne Klammern schreiben.

Jetzt sind wir in der Lage, das bilaterale semidirekte Produkt zu definieren:

Definition 8 (Bilaterales semidirektes Produkt)**.** *Wir haben zwei kompatible Links- und Rechtsaktionen von T auf S. Das* bilaterales semidirektes Produkt *ist die Struktur $S * *T = (S \times T, \cdot)$, wo die Multiplikation durch $(s_1, t_1) \cdot (s_2, t_2) = (s_1t_2 + t_1s_2, t_1t_2)$ definiert wird.*

Das bilaterales semidirektes Produkt bewahrt die Eigenschaften von S und T im folgenden Sinne:

Satz 7. *Das bilaterale semidirekte Produkt $S * *T$ von zwei Halbgruppen S, T ist eine Halbgruppe. Falls S und T Monoide sind und die Aktionen monoidisch sind, ist auch $S * *T$ ein Monoid.*

Beweis. Der Beweis ist ganz einfach, wir müssen nur die Assoziativität und eventuell Existenz des neutralen Elements überprüfen. □

Wir nennen zwei einfache Beispiele für das bilaterale semidirekte Produkt:

Beispiel.

- Wir definieren die Aktionen durch $ts = s = st$ für alle $s \in S, t \in T$. Das bilaterale semidirekte Produkt $S * *T$ ist dann isomorph zu $S * T$ mit üblichem direkten Produkt.

- Falls wir die Rechtsaktion durch $s = st$ definieren, ist sie mit alle Linksaktionen kompatibel. In dieser Weise bekommen wir den üblichen Begriff des direkten Produktes, den wir z. B. aus der Gruppentheorie kennen.

3.2 Blockprodukt

Jetzt sind wir endlich bereit, das Blockprodukt vorzustellen. Das Blockprodukt ermöglicht uns, ein bilaterales semidirektes Produkt von zwei belieblige Monoide zu konstruieren:

Definition 9 (Blockprodukt)**.** *Seien $(M, \cdot, 1)$ und $(N, \cdot, 1)$ zwei Monoide. Die Menge $M^{N \times N}$ (d. h. die Menge aller Abbildungen von $N \times N$ nach M) bildet ein Monoid $(M^{N \times N}, +, 0)$ wo $F_1 + F_2$ durch $(F_1 + F_2)(n_1, n_2) = F_1(n_1, n_2) \cdot F_2(n_1, n_2)$ definiert ist.*

Auf diese Weise ist $(M^{N \times N}, +, 0)$ isomorph zu $|N|^2$ Kopien von M und $0_{M^{N \times N}}$ ist durch $0_{M^{N \times N}}(n_1, n_2) = 1$ definiert.

Wir definieren die Links- und Rechtsaktion von N auf $M^{N \times N}$:

- $(Fn)(n_1, n_2) = F(n_1, nn_2)$,
- $(nF)(n_1, n_2) = F(n_1 n, n_2)$.

Diese Aktionen sind kompatibel, und deshalb liefern sie uns ein bilaterales semidirektes Produkt $N * *M^{N \times N}$, das durch $M \square N$ bezeichnt wird.

Der folgende Satz zeigt uns eine der wichtige Verwendungen des Blockproduktes:

Satz 8 (Satz von Krohn-Rhodes)**.** *Sei U_1 das Monoid auf $\{0, 1\}$ mit der üblichen Multiplikation und sei M ein endliches Monoid.*

Dann existiert eine Folge von endlichen Monoiden $M_0, \ldots, M_n$, so dass M_0 das triviale Monoid ist, $M \prec M_n$ und für alle $i \in \{0, \ldots, n-1\}$, $M_{i+1} = N \square M_i$, wobei N entweder eine einfache Gruppe, die M teilt, ist, oder $N = U_1$.

Falls, zusätzlich, M eine Gruppe ist, müssen wir keine $N = U_1$ benutzen.

Beweis. Siehe Anhang von [1, Theorem V.4.4]. □

Literatur

[1] Straubing, Howard. *Finite Automata, Formal Logic, and Circuit Complexity*. Springer Science+Business Media, New York, 1994. ISBN: 978-1-4612-6695-2.

[2] Hetzl, Stefan. *Automata and Formal Languages*. Vienna University of Technology, 2017.