S E M I N A R A R B E I T

Charakterisierungen der Sprachen in $FO[<]$, $FO[+1]$ und $FO[Reg]$ mittels syntaktischem Monoid und Homomorphismus

verfasst von
Leo Brauner

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

im Rahmen des Seminars aus theoretischer Informatik WS 2019
Technische Universität Wien

Wien, am 11. Dezember 2019

Inhaltsverzeichnis

1 Einleitung

Diese Arbeit wurde im Rahmen des Seminars aus theoretischer Informatik WS 2019 verfasst, dessen Zweck in der Auseinandersetzung mit dem Inhalt des Buches *Finite Automata, Formal Logic and Curcuit Complexity* von Howard Straubing bestand. In diesem Buch wird eine Art und Weise präsentiert, formale Sprachen durch logische Formeln zu beschreiben, indem man die Variablen in den Formeln als Positionen in Wörtern interpretiert. Zu jeder geschlossenen Formel bilden dann die Wörter, die diese (in einem gewissen Sinne) erfüllen, eine Sprache. Im Rahmen besagten Seminars entstanden sieben Seminararbeiten, welche sich jeweils einem Kapitel dieses Buches widmen.

In dieser Seminararbeit widmen wir uns Kapitel VI: *First-Order Logic*. Wir betrachten drei bestimmte Klassen von geschlossenen Formeln, nämlich $FO[<]$, $FO[+1]$ und $FO[Reg]$, die alle dadurch definiert sind, dass man nur Formeln erster Ordnung und in ihnen nur bestimmte numerische Prädikate zulässt. In $FO[<]$ lassen wir nur $x < y$ zu, in $FO[+1]$ lassen wir nur $x = y$ und $x = y + 1$ zu und in $FO[Reg]$ lassen wir nur reguläre numerische Prädikate zu. Man sieht schnell, dass $FO[+1] \subseteq FO[<] \subseteq F[Reg]$. Wir sind daran interessiert, welche Sprachen sich durch Formeln dieser jeweiligen Klassen beschreiben lassen. Für jede dieser drei Klassen wird es uns gelingen, eine Charakterisierung ihrer Sprachen durch eine algebraische Eigenschaft der jeweiligen syntaktischen Monoide oder syntaktischen Homomorphismen zu finden. Aus diesen Charakterisierungen werden wir insbesondere Resultate zur Entscheidbarkeit dieser Klassen erhalten. Weiters gehen wir darauf ein, dass man zur Beschreibung von Sprachen in $FO[<]$ Formeln mit beliebig vielen Alternationen von Existenz- und Allquantoren benötigt. Der Fokus dieser Arbeit liegt aber ausdrücklich auf den folgenden beiden Charakterisierungen:

- Eine Sprache $L \subseteq A^*$ ist genau dann in $FO[<]$, wenn ihr syntaktisches Monoid aperiodisch ist.
- Eine reguläre Sprache $L \subseteq A^*$ ist genau dann in $FO[Reg]$, wenn ihr syntaktischer Homomorphismus quasi-aperiodisch ist.

Um diese Aussagen zu zeigen, werden wir vor allem Resultate aus [S, Kapitel III und V], verwenden, wo schon gewisse derartige Charakterisierungen getroffen werden bzw. algebraische Theorie zu Halbgruppen und Monoiden entwickelt wird. Wir setzen für diese Seminararbeit Grundkenntnisse in der Logik, theoretischen Informatik, sowie den Inhalt von [S, Kapitel I bis IV] voraus. Ausgewählte, für diese Arbeit besonders wichtige Definitionen und Notationen werden unter anderem im zweiten Abschnitt kurz wiederholt.

2 Blockprodukt und Aperiodizität

Diese Seminararbeit beruht im Wesentlichen auf [S, Kapitel VI] und lehnt daher ihre Notation auch an [S] an. Üblicherweise werden wir mit einem fixen nichtleeren Alphabet A arbeiten. Wir betrachten Formeln ϕ, die aus Atomformeln der Form $Q_a x$ und $R_i^k(x_1, \ldots, x_k)$ (mit Variablen $x, x_1, \ldots, x_k$) zusammengesetzt sind. In dieser Arbeit werden wir ausschließlich Formeln ϕ erster Ordnung behandeln, also solche ϕ, in denen nur mit Variablen erster Ordnung $x, y, x_1, y_1, x_2, y_2, \ldots$ quantifiziert wird, welche wir als Positionen in einem Wort auffassen. In [S] werden auch Variablen zweiter Ordnung eingeführt, welche als Menge von Positionen in einem Wort aufgefasst werden. Formeln, in welchen mit solchen Variablen quantifiziert wird, heißen Formeln zweiter Ordnung und wir werden Resultate über solche Formeln zwar erwähnen und verwenden, uns aber nicht explizit mit diesen auseinandersetzen. Kommen wir nun dazu, was wir mit „als Position in einem Wort auffassen“ meinen. Wir betrachten dazu sogenannte V-Strukturen, das sind Wörter $w = (a_1, S_1) \cdots (a_r, S_r) \in (A \times 2^V)^*$, wobei V eine Menge von Variablen ist, sodass $V = \biguplus_{i=1}^r S_i$.

Wir interpretieren jedes numerische Prädikat R_i^k als eine k-stellige numerische Relation; das ist eine Abbildung, die jedem $n \in \mathbb{N}_0$ eine k-stellige Relation auf $\{1, \ldots, n\}$ zuweist. Für eine Formel erster Ordnung ϕ mit freien Variablen in V und eine V-Struktur $w = (a_1, S_1) \cdots (a_r, S_r)$ definieren wir die *Erfüllungsrelation* $\models$ rekursiv:

$w \models Q_a x$,	falls w einen Buchstaben (a, S) mit $x \in S$ enthält
$w \models R_i^k(x_1, \dots x_k)$,	falls $P(j_1, \dots, j_k)$, wobei P die k-stellige Relation auf $\{1, \dots, r\}$ ist, als die wir R_i^k interpretieren und $j_1, \dots, j_k$ die Positionen von $x_1, \dots, x_k$ in w sind
$w \models \phi \wedge \psi$,	falls $w \models \phi$ und $w \models \psi$
$w \models \neg\phi$,	falls $w \not\models \phi$, und
$w \models \exists x\phi$,	falls es ein $i \in \{1, \dots, r\}$ gibt, sodass $(a_1, S_1) \cdots (a_i, S_i \cup \{x\}) \cdots (a_r, S_r) \models \phi$.

Die Menge der V-Strukturen w, die ϕ erfüllen, notieren wir mit L_ϕ.

In [S, Kapitel V] wird die Definition des halbdirekten Produkts und Blockprodukts zweier Monoide gegeben, welche wir an dieser Stelle wiederholen. Seien $(F, +, 0)$ und $(M, \cdot, 1)$ Monoide (beide nicht notwendigerweise kommutativ). $F \times M \to F : (f, m) \mapsto fm$ heißt monoidische Rechtsaktion von M auf F, falls $(f + f')m = fm + f'm$, $(fm)m' = f(mm')$, $0m = 0$ und $f1 = f$. Gibt es eine monoidale Rechts- und Linksaktion (dual definiert) von M auf F, sodass $(mf)m' = m(fm')$ erfüllt ist, dann ist das halbdirekte Produkt $F{*}{*}M := F \times M$ mit

$$\begin{pmatrix} f \\ m \end{pmatrix} \begin{pmatrix} f' \\ m' \end{pmatrix} = \begin{pmatrix} fm' + mf' \\ mm' \end{pmatrix}$$

wieder ein Monoid. Mit $\pi_F : F \times M \to F$, $\pi_M : F \times M \to M$ werden wir die Projektionen auf die erste bzw. zweite Koordinate bezeichnen. Induktiv lässt sich zeigen:

$$\begin{pmatrix} f_1 \\ m_1 \end{pmatrix} \cdots \begin{pmatrix} f_n \\ m_n \end{pmatrix} = \begin{pmatrix} \sum_{j=1}^{n} m_1 \cdots m_{j-1} f_j m_{j+1} \cdots m_n \\ m_1 \cdots m_n \end{pmatrix}.$$

Wie man der ersten Komponente des obigen Paars (f, m) möglicherweise ansieht, eignet sich das halbdirekte Produkt gut dazu, die Existenz gewisser Zerlegungen eines Wortes auf eine algebraische Weise auszudrücken. Insbesondere werden wir eine gewisse Verträglichkeit des Blockproduktes mit der Existenz-Quantifizierung von Formeln erster Ordnung zeigen.

Für zwei Monoide U und M definieren wir auf $F := U^{M \times M}$ die binäre Operation $f = f_1 + f_2$ durch $f(m_1, m_2) := f_1(m_1, m_2) \cdot f_2(m_1, m_2)$ und von M auf F die Rechts- und Linksaktion

$F \times M \to F : (fm)(m_1, m_2) := f(m_1, mm_2)$ sowie

$M \times F \to F : (mf)(m_1, m_2) := f(m_1 m, m_2)$.

Diese erfüllen die Voraussetzungen, um $U \square M := U^{M \times M} {*}{*} M = F {*}{*} M$ zu bilden. $U \square M$ nennen wir das Blockprodukt von U mit M.

Wir fixieren im Folgenden ein Alphabet A.

Außerdem werden wir für eine Sprache $L \subseteq (A \times 2^V)^*$ syntaktische Kongruenz, Monoid und Homomorphismus mit $\equiv_L$, $M(L)$ bzw. η_L notieren sowie $\theta_L := \eta_L|_{A^*}$ und $N(L) := \theta_L(A^*) = \eta_L(A^*)$ definieren. Im Falle $L = L_\phi$ verwenden wir die Abkürzungen $\equiv_\phi$, $M(\phi)$, η_ϕ, θ_ϕ und $N(\phi)$.

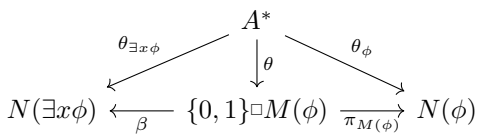
Wir sagen, dass ein Monoid M bzw. ein Monoidhomomorphismus $\eta : A^* \to M$ eine Sprache $L \subseteq A^*$ erkennt, wenn es $T \subseteq M$ gibt, sodass $L = \eta^{-1}(T)$. Für Halbgruppen H_1, H_2 schreiben wir $H_1 \leq H_2$, falls H_1 eine Unterhalbgruppe von H_2 ist und wir schreiben $H_1 \preccurlyeq H_2$, falls H_1 ein Teiler von H_2, also das homomorphe Bild einer Unterhalbgruppe von H_2 ist. Für das direkte Produkt von H_1 und H_2 schreiben wir einfach $H_1 \times H_2$.

Ein Monoid M erkennt eine Sprache genau dann, wenn $M(L) \preccurlyeq M$ ist und L ist genau dann regulär, wenn sie von einem endlichen Monoid erkannt wird. Überhaupt werden wir in dieser Arbeit ausschließlich mit regulären Sprachen arbeiten.

Im Folgenden bezeichne $\{0, 1\}$ stets das Monoid mit Trägermenge $\{0, 1\}$, neutralem Element 1 und $0 \cdot 0 = 0$.

Proposition 2.1. *Sei ϕ eine Formel erster Ordnung mit freien Variablen in $V \cup \{x\}$, $x \notin V$. Dann gibt es einen Monoidhomomorphismus $\eta : (A \times 2^V)^* \to \{0, 1\} \square M(\phi)$, der $L_{\exists x\phi}$ erkennt.*

Insbesondere gibt es einen surjektiven Monoidhomomorphismus $\beta : \{0, 1\} \square M(\phi) \to N(\exists x\phi)$, sodass folgendes Diagramm mit $\theta := \eta|_{A^*}$ kommutiert:



Beweis. Sei V die Menge der freien Variablen in $\exists x\phi$, dann geht $\eta_\phi : (A \times 2^{V\cup\{x\}})^* \to M(\phi)$ und es gibt $T_\phi \subseteq M(\phi)$, sodass $L_\phi = \eta_\phi^{-1}(T_\phi)$. Es ist $\{0,1\}\Box M(\phi) = F * *M(\phi)$ mit $F := \{0,1\}^{M\times M}$. Wir definieren nun den Monoidhomomorphismus

$$\eta : (A \times 2^V)^* \to \{0,1\}\Box M(\phi) = F * *M(\phi) : \qquad \text{durch} \qquad (a,S) \mapsto \begin{pmatrix} f_{(a,S)} \\ \eta_\phi(a,S) \end{pmatrix},$$

wobei

$$f_{(a,S)}(m_1,m_2) := \begin{cases} 0, & \text{falls } m_1 \cdot \eta_\phi(a, S\cup\{x\}) \cdot m_2 \in T_\phi, \\ 1, & \text{sonst.} \end{cases}$$

Seien $\pi_F, \pi_{M(\phi)}$ die Projektionen von $F{*}{*}M(\phi)$ auf die erste bzw. zweite Koordinate. Für $w = (a_1,S_1)\cdots(a_r,S_r) \in (A\times 2^V)^*$ berechnen wir nun:

$$f := (\pi_F \circ \eta)(w) = \sum_{j=1}^{r} \eta_\phi((a_1,S_1)\cdots(a_{j-1},S_{j-1}))f_{(a_j,S_j)}\eta_\phi((a_{j+1},S_{j+1})\cdots(a_r,S_r))$$

Mit $w_{<j} := (a_1,S_1)\cdots(a_{j-1},S_{j-1})$ und $w_{>j} := (a_{j+1},S_{j+1})\cdots(a_r,S_r)$ gilt:

$$\begin{aligned} 0 = f(1,1) &= \prod_{j=1}^{r} f_{(a_j,S_j)}(\eta_\phi(w_{<j}),\eta_\phi(w_{>j})) \\ &\iff \exists j \in \{1,\dots,r\} : \eta_\phi(w_{<j})\eta_\phi(a_j, S_j\cup\{x\})\eta_\phi(w_{>j}) \in T_\phi \\ &\iff \exists j \in \{1,\dots,r\} : w_{<j}(a_j,S_j\cup\{x\})w_{>j} \in L_\phi \\ &\iff w \models \exists x\phi. \end{aligned}$$

Daher ist $L_{\exists x\phi} = \eta^{-1}(T_{\exists x\phi})$ mit $T_{\exists x\phi} := \{(f,m) \in \{0,1\}\Box M(\phi) : f(1,1) = 0\}$, also wird $L_{\exists x\phi}$ von η erkannt. Nach Konstruktion ist $\pi_{M(\phi)} \circ \eta = \eta_\phi$.

Da η die Sprache $L_{\exists x\phi}$ erkennt, gibt es einen surjektiven Monoidhomomorphismus $\beta : \{0,1\}\Box M(\phi) \to N(\exists x\phi)$ mit $\eta_{\exists x\phi} = \beta \circ \eta$. Mit $\theta := \eta|_{A^*}$ erhalten wir:

$$\theta_{\exists x\phi} = \eta_{\exists x\phi}\big|_{A^*} = \beta \circ \eta\big|_{A^*} = \beta \circ \theta \qquad \text{und} \qquad \theta_\phi = \eta_\phi\big|_{A^*} = \pi_{M(\phi)} \circ \eta\big|_{A^*} = \pi_{M(\phi)} \circ \theta;$$

damit ist das angegebene Diagramm tatsächlich kommutativ. ∎

Definition 2.2. Eine Halbgruppe H heißt aperiodisch, wenn jede Untergruppe $G \leq H$ trivial ist.

Eine Halbgruppe H ohne neutralem Element enthält keine Untergruppen und ist daher trivialerweise aperiodisch. Eine endliche Halbgruppe H ist genau dann aperiodisch, wenn es ein $k \in \mathbb{N}_0$ gibt, sodass für alle $h \in H$ gilt: $h^k = h^{k+1}$.

Proposition 2.3. *Die endlichen, aperiodischen Halbgruppen sind abgeschlossen unter $\leq$, $\preccurlyeq$, $\times$ und $**$ und bilden insbesondere eine Pseudovarietät.*

Dasselbe gilt für endliche, aperiodische Monoide.

Beweis. Der Erhalt der Endlichkeit unter diesen Operationen ist klar.

- $\leq$ Sei H eine aperiodische Halbgruppe und $H' \leq H$ eine Unterhalbgruppe, dann ist jede Untergruppe G von H' auch eine Untergruppe H und damit trivial, also ist H' aperiodisch.
- $\preccurlyeq$ Sei nun H' ein Quotient von H und $\pi : H \to H'$ die Quotientenabbildung. Für eine Untergruppe $G \leq H'$ von H' ist $\pi^{-1}(G)$ eine Untergruppe von H und damit trivial. Wegen der Surjektivität von π ist dann $G = \pi(\pi^{-1}(G)) = \pi(\{1\}) = \{1\}$, also G trivial. Zusammen mit der Abgeschlossenheit unter $\leq$ folgt dann die Abgeschlossenheit unter $\preccurlyeq$.
- $\times$ Seien H_1, H_2 zwei aperiodische Halbgruppen, $H := H_1 \times H_2$ ihr direktes Produkt, $\pi_i : H \to H_i$ die Projektion auf die i-te Koordinate und dann $G \leq H$ eine Untergruppe. Die Einschränkung eines Halbgruppenhomomorphismus auf eine Untergruppe ist ein Gruppenhomomorphismus, also sind $G_i := \pi_i(G) \leq H_i$ jeweils Untergruppen. Nach Voraussetzung sind G_1, G_2 trivial und damit auch $G \leq G_1 \times G_2$.

$**$ Sei nun $H := H_1 * *H_2$ und $G \leq H$ eine Untergruppe von H. Dann gibt es nach [S, V.4.2] jeweils Untergruppen $G_i \leq H_i$ von H_i, sodass $G \cong G_1 \times G_2$. Nach Voraussetzung sind G_1, G_2 trivial und damit auch G.

Für Monoide analog. ■

3 Eine Charakterisierung von $FO[<]$

Wir fixieren im Folgenden ein Alphabet A und interpretieren das zweistellige Prädikat $<$ als die gewöhnliche $<$-Relation auf $\mathbb{N}_0$.

Definition 3.1. Wir definieren $FO[<]$ als die Menge der Formeln erster Ordnung, in denen nur Atomformeln von der Form $Q_a x$ und $x < y$ vorkommen. Gleichzeitig werden wir mit $FO[<]$ die Familie der durch solche Formeln definierten Sprachen bezeichnen.

Wir beweisen nun folgendes praktisches Hilfslemma, welches es uns erlaubt, eine $FO[<]$-Eigenschaft eines Präfixes von w als eine $FO[<]$-Eigenschaft von w selbst zu betrachten.

Lemma 3.2. *Sei $\phi \in FO[<]$ mit freien Variablen in V, $x \notin V$. Dann gibt es eine Formel $\phi[< x] \in FO[<]$ mit freien Variablen in $V \cup \{x\}$, sodass für jede $(V \cup \{x\} \cup V')$-Struktur $w = w_{<x} \cdot (a, S) \cdot w_{>x}$ mit einer V-Struktur $w_{<x}$ und $x \in S$ gilt:*

$$w \models \phi[< x] \qquad \Longleftrightarrow \qquad w_{<x} \models \phi.$$

Beweis. Wir beweisen die Aussage mit Induktion über die Formelstruktur. Wir definieren induktiv:

$(y < z)[< x] \quad := (y < z) \wedge (z < x)$,
$(Q_a y)[< x] \quad := Q_a y \wedge (y < x)$,
$(\phi \wedge \psi)[< x] \quad := \phi[< x] \wedge \psi[< x]$,
$(\neg\phi)[< x] \quad := \neg(\phi[< x])$ und
$(\exists y \phi)[< x] \quad := \exists y(\phi[< x] \wedge (y < x))$.

Für die Atomformeln leistet unsere Definition offensichtlich das Gewünschte. Für Konjugation und Negation folgt dies unmittelbar aus unserer Definition der Semantik. Die Existenzquantifikation betrachten wir genauer.

Da y in $\exists y\phi$ gebunden ist, können wir o.B.d.A. $y \notin V \cup \{x\} \cup V'$ fordern. Seien $w = (a_1, S_1) \cdots (a_r, S_r)$ und j_0 die Position der Variable x im Wort w, also $x \in S_{j_0}$, und $w' = (a_1, S_1) \cdots (a_j, S_j \cup \{y\}) \cdots (a_r, S_r)$. Mit unserer Induktionshypothese angewandt auf $\phi[< x]$ (denn ϕ, w', $w'_{<x}$ erfüllen mit $V \mapsto V \cup \{y\}$ die Voraussetzungen des Lemmas) gilt:

$$\begin{aligned} w \models (\exists y\phi)[< x] := \exists y(\phi[< x] \wedge (y < x)) &\Longleftrightarrow \exists j \in \{1, \ldots, r\} : w' \models \phi[< x] \wedge y < x \\ &\Longleftrightarrow \exists j \in \{1, \ldots, j_0 - 1\} : w' \models \phi[< x] \\ &\Longleftrightarrow \exists j \in \{1, \ldots, j_0 - 1\} : w'_{<x} \models \phi \\ &\Longleftrightarrow w_{<x} \models \exists y\phi. \end{aligned}$$

Damit hat $(\exists y\phi)[< x]$ die gewünschte Eigenschaft und es folgt die Behauptung. ■

Die Formel $\phi[< x]$ heißt auch Relativierung von ϕ und analog kann man auch Relativierungen $\phi[\leq x]$, $\phi[> x]$ und $\phi[\geq x]$ definieren.

Definition 3.3. Eine Sprache $L \subseteq A^*$ heißt sternfrei, wenn es einen regulären Ausdruck ohne Kleene-Stern gibt, welcher L beschreibt.

Beispiel 3.4. Die Sprache $A^* = \emptyset^c$ ist sternfrei. Für $a, b \in A$ ist die Sprache $\{ab\}^*$ sternfrei, denn:

$$(ab)^* = 1 \cup (aA^*b \cap (A^*a^2A^*)^c \cap (A^*b^2A^*)^c) = 1 \cup (a\emptyset^c b \cap (\emptyset^c a^2 \emptyset^c)^c \cap (\emptyset^c b^2 \emptyset^c)^c).$$

Wir zeigen nun das Hauptresultat dieses Abschnitts:

Satz 3.5. *Für eine Sprache $L \subseteq A^*$ sind äquivalent:*
(a) $L \in FO[<]$.
(b) $M(L)$ *ist endlich und aperiodisch.*
(c) L *wird von einem endlichen, aperiodischen Monoid erkannt.*
(d) L *ist sternfrei.*

Beweis.

- (b) $\Longrightarrow$ (c): $M(L)$ erkennt M.
- (c) $\Longrightarrow$ (b): Sei M ein endliches, aperiodisches Monoid, welches L erkennt. Dann ist $M(L) \preccurlyeq M$ nach Prop. 2.3 wieder endlich und aperiodisch.
- (a) $\Longrightarrow$ (b) Wir behaupten, dass für jede Formel $\phi \in FO[<]$ das Monoid $N(\phi)$ endlich und aperiodisch ist und zeigen diese Behauptung mit Induktion nach Formelaufbau. Da wir am Ende nur an der Aussage für $\emptyset$-Strukturen bzw. geschlossene Formeln ϕ interessiert sind und für diese $M(\phi) = N(\phi)$ gilt, ist dies hinreichend.

  Q_a Für eine $\{x\}$-Struktur $u'wu''$ mit $w \in A^*$ gilt:

  $$u'wu'' \models Q_a x \quad \Longleftrightarrow \quad u'u'' \models Q_a x \quad \Longleftrightarrow \quad u'1u'' \models Q_a x,$$

  daher ist $w \equiv_{Q_a x} 1$ und $N(Q_a x) = \theta_{Q_a x}(\{1\}) = \{1\}$ ist endlich und aperiodisch.

  $<$ Analog wie für $Q_a x$.

  $\wedge$ Nach [S, V.6.1] ist $N(\phi \wedge \psi) \preccurlyeq N(\phi) \times N(\psi)$. Für $N(\phi)$, $N(\psi)$ endlich und aperiodisch ist nach Prop. 2.3 dann auch $N(\phi \wedge \psi)$ endlich und aperiodisch.

  $\neg$ Wegen $N(\neg\phi) = N(\phi)$ ist dieser Schritt trivial.

  $\exists$ Mit der Aussage und Notation von Prop. 2.1 ist $N(\exists x\phi) = \theta_{\exists x\phi}(A^*) = \beta(\theta(A^*))$, also ist $N(\exists x\phi) \preccurlyeq \theta(A^*)$. Mit $F := \{0,1\}^{M(\phi)\times M(\phi)}$ ist $\theta(A^*) \leq \{0,1\}\square M(\phi) = F * *M(\phi)$ und damit sicherlich auch $\theta(A^*) \leq F * *\pi_{M(\phi)}(\theta(A^*))$. Es folgt:

  $$N(\exists x\phi) \preccurlyeq \theta(A^*) \leq F * *\pi_{M(\phi)}(\theta(A^*)) = F * *\theta_\phi(A^*) = F * *N(\phi).$$

  Da jedes Element f des Monoids F idempotent ist, ist F endlich und aperiodisch, und nach Induktionsvoraussetzung ist $N(\phi)$ endlich und aperiodisch. Mit Prop. 2.3 ist dann $N(\exists x\phi)$ endlich und aperiodisch.

- (b) $\Longrightarrow$ (a) Sei nun $M(L)$ endlich und aperiodisch. Dann gilt nach [S, V.4.4]:

  $$M(L) \preccurlyeq \{0,1\}\square(\{0,1\}\square\cdots(\{0,1\}\square\{1\})\cdots),$$

  also wird L von obigem endlich iterierten Blockprodukt erkannt. Wir zeigen nun induktiv nach dem Aufbau dieses Blockprodukts, dass es nur Sprachen in $FO[<]$ erkennt. Das triviale Monoid $\{1\}$ erkennt nur die Sprachen $\emptyset = L_\perp$, $A^* = L_\top \in FO[<]$. Sei nun M ein endliches Monoid, welches nur Sprachen in $FO[<]$ erkennt. Dann bleibt nur noch zu zeigen, dass auch $\{0,1\}\square M$ nur Sprachen in $FO[<]$ erkennt und die Behauptung für L folgt dann induktiv. Sei also L' eine Sprache, die von $\{0,1\}\square M$ erkannt wird. Dann gibt es einen Monoidhomomorphismus $\eta : A^* \to \{0,1\}\square M$ und $T' \subseteq \{0,1\}\square M$ mit $L' = \eta^{-1}(T') = \bigcup_{(f,m)\in T'} \eta^{-1}(\{(f,m)\})$. Weil T' endlich ist, reicht es daher, für festes $(f,m) \in \{0,1\}\square M$ eine Formel $\phi \in FO[<]$ für $\eta^{-1}(\{(f,m)\}) = L_\phi$ zu finden.

  Es ist $\{0,1\}\square M = F * *M$ mit $F = \{0,1\}^{M\times M}$. Seien π_F, π_M die Projektionen von $F * *M$ auf die erste bzw. zweite Koordinate. Dann gilt für $w \in A^*$:

  $$\eta(w) = (f,m) \qquad \Longleftrightarrow \qquad (\pi_M \circ \eta)(w) = m \quad \wedge \quad (\pi_F \circ \eta)(w) = f$$

Nach Voraussetzung erkennt M nur $FO[<]$-Sprachen; daher gibt es zu jedem $m \in M$ eine Formel $\psi_m \in FO[<]$ mit $(\pi_M \circ \eta)^{-1}(\{m\}) = L_{\psi_m}$. Es bleibt daher eine $FO[<]$-Formel σ_f für $(\pi_F \circ \eta)^{-1}(\{f\})$ zu finden. Das Monoid $\{0,1\}$ ist kommutativ und idempotent, und damit auch $F = \{0,1\}^{M\times M}$, wo wir die binäre Operation punktweise erklärt haben; mit $w = a_1 \cdots a_r$ und $f_a := (\pi_F \circ \eta)(a)$ können wir nun berechnen:

$$\begin{aligned}(\pi_F \circ \eta)(w) &= \sum_{j=1}^{r} (\pi_M \circ \eta)(a_1 \cdots a_{j-1}) \cdot (\pi_F \circ \eta)(a_j) \cdot (\pi_M \circ \eta)(a_{j+1} \cdots a_r) \\ &= \sum_{w=w'aw''} (\pi_M \circ \eta)(w') \cdot f_a \cdot (\pi_M \circ \eta)(w'') = \sum_{w \models \sigma_{(m',a,m'')}} m' \cdot f_a \cdot m'',\end{aligned}$$

wobei $\sigma_{(m',a,m'')} := \exists x(Q_a x \wedge \psi_{m'}[< x] \wedge \psi_{m''}[> x]) \in FO[<]$. Wegen F kommutativ und idempotent hängt der Wert obiger Summe in F weder von der Reihenfolge noch von der jeweiligen Anzahl der Vorkommen eines Summanden ab – also nur von der Menge der vorkommenden Summanden. Das heißt, $\mathcal{I}_f := \{I \subseteq M \times A \times M : \sum_{(m',a,m'')\in I} m' \cdot f_a \cdot m'' = f\}$ ist ein wohldefiniertes Mengensystem und es gilt:

$$(\pi_F \circ \eta)(w) = f \qquad \Longleftrightarrow \qquad w \models \bigvee_{I\in\mathcal{I}_f} \left(\bigwedge_{(m',a,m'')\in I} \sigma_{(m',a,m'')} \wedge \bigwedge_{(m',a,m'')\in I^c} \neg\sigma_{(m',a,m'')} \right) =: \sigma_f.$$

Weil $\mathcal{I}_f$ und jedes $I \in \mathcal{I}_f$ endlich ist, sind wir fertig.

- (d) $\Longrightarrow$ (a): Wir zeigen die Aussage mit Induktion nach der Struktur der sternfreien regulären Ausdrücke.

$\emptyset$	$= L_\bot$
$\{1\}$	$= L_{\neg\exists x \top}$
$\{a\}$	$= L_{\exists x(Q_a x \wedge \neg\exists y(y<x) \wedge \neg\exists y(x<y))}$
$L_{\phi\wedge\psi}$	$= L_\phi \cap L_\psi$
$L_{\neg\phi}$	$= L_\phi^c$
$L_\phi \cdot L_\psi$	$= L_{\exists x(\phi[<x] \wedge \psi[\geq x]) \vee \exists x(\phi[\leq x] \wedge \psi[>x]) \vee ((\neg\exists x \top) \wedge \phi \wedge \psi)}$

  Man überzeugt sich leicht davon, davon dass dies das Gewünschte liefert.

- (b) $\Longrightarrow$ (d): Mit derselben Argumentation wie in „(c) $\Longrightarrow$ (a)“ und der Tatsache, dass die von $\{1\}$ erkannten Sprachen $\emptyset$ und $A^* = \emptyset^c$ sternfrei sind, reicht es wieder zu zeigen, dass für ein endliches Monoid M, welches nur sternfreie Sprachen erkennt, auch $\{0,1\}\Box M$ wieder nur sternfreie Sprachen erkennt. Sei also M ein solches Monoid und L' eine von $\{0,1\}\Box M$ erkannte Sprache, dann gibt einen Monoidhomomorphismus $\eta : A^* \to \{0,1\}\Box M$ und $T' \subseteq M$ mit $L' = \eta^{-1}(T')$. Aus der in „(c) $\Longrightarrow$ (a)“ gewonnenen $FO[<]$-Formel, die L' beschreibt, erhalten wir effektiv die Darstellung

  $$L' = \bigcup_{(f,m)\in T'} \left((\pi_M \circ \eta)^{-1}(\{m\}) \cap (\pi_F \circ \eta)^{-1}(\{f\}) \right),$$

  mit

  $$(\pi_F \circ \eta)^{-1}(\{f\}) = \bigcup_{I\in\mathcal{I}_f} \left(\bigcup_{(m',a,m'')\in I} (\pi_M \circ \eta)^{-1}(\{m'\}) \cdot \{a\} \cdot (\pi_M \circ \eta)^{-1}(\{m''\}) \right).$$

  Da $\pi_M \circ \eta$ ein Monoidhomomorphismus von A^* nach M ist, wird die Sprache $(\pi_M \circ \eta)^{-1}(\{m\})$ für $m \in M$ von M erkannt und ist daher nach Voraussetzung sternfrei. Da $T' \subseteq M$, $\mathcal{I}_f$ und jedes $I \in \mathcal{I}_f$ endlich sind, ist dann auch L' sternfrei, also erkennt $\{0,1\}\Box M$ nur sternfreie Sprachen und wir sind fertig.

■

Die Äquivalenz der Aussagen (b), (c) und (d) ist auch als der Satz von Schützenberger bekannt.

Beispiel 3.6. Sei $L := \{w \in A^* : |w| \equiv_p 0\} = (A^p)^*$ für $p > 1$. Dann ist (bis auf Isomorphie) $M(L) = \mathbb{Z}_p$ und $\eta_L : A^* \to \mathbb{Z}_p : w \mapsto |w| + p \cdot \mathbb{Z}$. Wegen $\mathbb{Z}_p$ endlich ist L regulär, aber weil $\mathbb{Z}_p$ eine nichttriviale Gruppe ist, ist L nach Satz 3.5 nicht durch eine $FO[<]$-Formel und auch nicht durch einen sternfreien regulären Ausdruck beschreibbar.

Charakterisierungen von Klassen von Sprachen wie Satz 3.5 erlauben eine Aussage über deren Entscheidbarkeit. Unter Entscheidbarkeit verstehen wir die Turing-Berechenbarkeit der charakteristischen Funktion. In der Formulierung solcher Resultate ist die Phrase „eine gegebene reguläre Sprache“ immer so zu verstehen, dass wir einen deterministischen oder nichtdeterministischen endlichen Automaten kennen, der diese Sprache erkennt, oder einen regulären Ausdruck, der diese Sprache beschreibt. Unter dem Gesichtspunkt der Entscheidbarkeit sind diese beiden Voraussetzungen effektiv äquivalent, da sich das eine mit einer Turing-Maschine aus dem anderen berechnen lässt, und umgekehrt.

Korollar 3.7. *Ob eine gegebene reguläre Sprache $L \subseteq A^*$ in $FO[<]$ ist, ist entscheidbar.*

Beweis. Mithilfe eines regulären Ausdrucks für L können wir den (bis auf Isomorphie eindeutigen) minimalen Automaten berechnen und dann die Verknüpfungstabelle dessen Übergangsmonoids, welches (bis auf Isomorphie) genau jene des syntaktischen Monoids $M(L)$ der Sprache L ist. Nun können wir berechnen, ob $M(L)$ eine nichttriviale Gruppe enthält. Nach Satz 3.5 ist dies äquivalent zu $L \notin FO[<]$. ■

4 Eine Hierarchie in $FO[<]$

Ähnlich zur arithmetischen Hierarchie können wir auch in unserer Signatur Klassen von Formeln definieren, die in einer Formel erster Ordnung ϕ die Alternationen von Existenz- und All-Quantifikation „zählen“.

Definition 4.1. Wir definieren induktiv

$FO[<]_0$	als die Menge $\{(Q_a x), (x < y) : x, y \text{ Variablen}\}$ der Atomformeln in $FO[<]$,
$FO[<]_k$	als die Menge der Booleschen Kombinationen aus Formeln der Gestalt $\exists x_1 \cdots \exists x_r \phi$ mit $\phi \in FO[<]_{k-1}$, $k > 0$.

Wir nehmen nun $|A| \geq 2$ an und definieren für $a, b \in A$, $a \neq b$, induktiv Folgen von Wörtern $(v_{n,k})_{k \geq 0}$, $(w_{n,k})_{k \geq 0}$ wie folgt:

$$\begin{aligned} v_{n,0} &:= 1, \\ v_{n,k+1} &:= (v_{n,k} a v_{n,k} b v_{n,k})^n, \\ w_{n,k} &:= v_{n,k} b v_{n,k}. \end{aligned}$$

Lemma 4.2. *Sei $\phi \in FO[<]_k$. Dann gilt:*

$$\exists n_0 \geq 1 \ \forall n \geq n_0 : \qquad \theta_\phi(v_{n,k}) = \theta_\phi(w_{n,k}).$$

Wir lassen den technisch aufwendigen Beweis dieses Lemmas aus und verweisen dafür auf [S, VI.2.2].
Ein Wort u heißt Präfix eines Wortes w, in Zeichen $u \leq w$, falls es ein Wort v mit $u \cdot v = w$ gibt.
Wir definieren nun eine Folge von Sprachen $(L_k)_{k>0}$ wie folgt:

$$L_k := \{w \in \{a, b\}^* : \forall u \leq w : 0 \leq |u|_a - |u|_b \leq k\}.$$

Mithilfe der hier definierten Familie von Wörtern und Sprachen und Lemma 4.2 können wir nun recht einfach zeigen, dass man zur Beschreibung der Sprachen in $FO[<]$ Formeln mit beliebig hoher Anzahl k an Alternationen von Existenz- und Allquantifikation benötigt.

Satz 4.3. *Sei $|A| \geq 2$. Dann ist $FO[<]_k \subsetneq FO[<]$ für alle $k \geq 0$.*

Beweis. Der minimale Automat von L_k ist gegeben durch $D_k = (Q_k, \delta_k, q_0, F_k)$ mit Zustandsmenge $Q_k = \{q_0, \ldots, q_k, q'\}$, Anfangszustand q_0, Endzuständen $F_k = Q \backslash \{q'\}$ und Übergangsfunktion

$$\delta_k : Q \times A \to Q : \delta_k(q, \alpha) := \begin{cases} q_{j+1} & \text{falls } q = q_j, j < k, \alpha = a, \\ q_{j-1} & \text{falls } q = q_j, j > 0, \alpha = b, \\ q' & \text{sonst.} \end{cases}$$

Damit ist L_k regulär, also $M(L_k)$ endlich. Falls $|w|_a \neq |w|_b$ ist, führen w^{k+1} und w^{k+2} alle Zustände q in q' über, insbesondere ist $w^{k+1} \equiv_{L_k} w^{k+2}$. Falls $|w|_a = |w|_b$, so sieht man leicht ein, dass w und w^2 dieselben Übergänge

in D_k erzeugen; es folgt wieder $w^{k+1} \equiv_{L_k} w^{k+2}$. Damit ist das Übergangsmonoid von D_k aperiodisch; dieses ist aber genau das syntaktische Monoid $M(L_k)$ von L_k. Nach Satz 3.5 ist damit $L_k \in FO[<]$.

Für jedes $n \in \mathbb{N}$ lässt sich jeweils mit einer einfachen Induktion nach $k \in \mathbb{N}$ zeigen:
$|v_{n,k}|_a = |v_{n,k}|_b$ und
$\forall u \leq v_{n,k} : 0 \leq |u|_a - |u|_b \leq k$.
Es folgt unmittelbar $v_{n,k} \in L_k$ und $w_{n,k} \notin L_k$ für jedes $n \in \mathbb{N}$. Aus Lemma 4.2 folgt dann $L_k \notin FO[<]_k$. Damit ist $L_k \in FO[<] \backslash FO[<]_k$. ■

5 Eine Charakterisierung von $FO[+1]$

Die Definition von $FO[+1]$ ist zu jener von $FO[<]$ ganz analog:

Definition 5.1. Wir definieren $FO[+1]$ als die Menge der Formeln erster Ordnung, in denen nur Atomformeln von der Form $Q_a x$, $x = y$ und $y = x + 1$ vorkommen. Gleichzeitig werden wir mit $FO[<]$ die Familie der durch solche Formeln definierten Sprachen bezeichnen.

Die Formel $x = y$ ist offensichtlich äquivalent zu $\neg(x < y) \wedge \neg(y < x)$ und die Formel $x = z+1$ ist offensichtlich äquivalent zu $x < z \wedge \neg\exists y(x < y \wedge y < z)$, daher ist $FO[+1] \subseteq FO[<]$ (es gilt insbes. $FO[+1] \subsetneq FO[<]$, vgl. [S, IV.3.4]). So wie für $FO[<]$ finden wir auch hier wieder eine Charakterisierung der Sprachen in $FO[+1]$ über eine algebraische Eigenschaft ihrer syntaktischen Monoide.

Satz 5.2. *Für $L \subseteq A^*$ sind äquivalent:*
(a) $L \in FO[+1]$
(b) *$M(L)$ ist endlich, aperiodisch und für alle $e, e', s, s', s'' \in \eta_L(A^+)$ mit e, e' idempotent gilt:*

$$ese's'es''e' = es''e's'ese'.$$

(c) *L ist lokal schwellenwert testbar.*

Die Äquivalenz von (a) und (c) wird in [S, IV.3.3] gezeigt. Die Implikation (a)$\Longrightarrow$ (*b*) wird in [S, VI.3.1] gezeigt, verwendet den Satz 3.5 und ist technisch sehr aufwendig. An selber Stelle wird auch (b)$\Longrightarrow$(c) gezeigt, mit Verwendung von [S, Abschnitt V.5] über Kategorien. Die umständlich wirkende Bedingung (b) ist nämlich dazu äquivalent, dass für alle $c_1, c_2 \in Obj(\mathcal{E}(\eta_L(A^+)))$ und für alle $s, u \in Arr(c_1, c_2)$, $t \in Arr(c_2, c_1)$ gilt: $stu = uts$.

Daraus folgt mit analoger Argumentation wie für Korollar 3.7 unmittelbar:

Korollar 5.3. *Ob eine gegebene reguläre Sprache $L \subseteq A^*$ in $FO[+1]$ ist, ist entscheidbar.*

6 Eine Charakterisierung von $FO[Reg]$

Ein reguläres numerisches Prädikat ist eine Formel ϕ über das Alphabet $\{a\}$, in der alle Variablen zweiter Ordnung gebunden sind und nur Variablen erster Ordnung frei vorkommen dürfen, und für die L_ϕ regulär ist – wir haben für diese Definitionen also die Sprache $\{a\}$ fixiert! Die Familie der regulären numerischen Prädikate nennen wir *Reg*. Da die Atomformel $Q_a x$ unter diesen Voraussetzungen keine Information enthält, kommt diese in ϕ o.B.d.A. nicht vor, womit es für die Definition von *Reg* auf die spezielle Wahl des Buchstaben a nicht ankommt.

Nach [S, III.1.1] entsprechen die regulären numerischen Prädikate genau die in $SOM_{\{a\}}[+1]$ definierbaren numerischen Relationen und nach [S, III.2.1] entsprechen diese wiederum genau den Formeln in $FO_{\{a\}}[<, \equiv]$, also ist $Reg = FO_{\{a\}}[<, \equiv]$.

Definition 6.1. Für ein Alphabet A definieren wir $FO_A[Reg]$ als die Menge der Formeln erster Ordnung ϕ über das Alphabet A, in der alle vorkommenden numerischen Prädikate regulär sind. Gleichzeitig werden wir mit $FO_A[Reg]$ die Familie der durch solche Sätze definierten Sprachen bezeichnen.

Indem wir o.B.d.A. $a \in A$ voraussetzen, gilt:

$$FO_A[Reg] = FO_A[FO_{\{a\}}[<, \equiv]] = FO_A[<, \equiv],$$

also ist $FO[Reg]$ genau die Menge jener Sprachen die sich durch Formeln erster Ordnung beschreiben lassen, in denen nur Atomformeln von der Form $Q_a x$, $x < y$ und $x \equiv_p 0$ mit $a \in A$, $p > 0$ vorkommen.

Definition 6.2. Sei M ein endliches Monoid. Ein Monoidhomomorphismus $\eta : A^* \to M$ heißt *quasi-aperiodisch*, wenn für jedes $t > 0$ jede Unterhalbgruppe $H \leq \eta(A^t)$ von $\eta(A^t)$ aperiodisch ist.

Lemma 6.3. *Sei M ein endliches Monoid und $\eta : A^* \to M$ ein Monoidhomomorphismus. Dann gibt es für jedes $t > 0$ ein $p > 0$, sodass $\eta(A^{pt}) = \eta((A^{pt})^+)$.*

Beweis. Sei $t > 0$ beliebig. Dann ist $(\eta(A^{kt}))_{k>0}$ eine Folge in 2^M. Wegen M endlich gibt es dann gewisse $k, s > 0$ mit $\eta(A^{kt}) = \eta(A^{(k+s)t})$. Für beliebige $p \geq k$, $\ell \geq 0$ gilt dann:

$$\eta(A^{(p+\ell s)t}) = \eta(A^{kt}A^{(p-k+\ell s)t}) = \eta(A^{kt})\eta(A^{(p-k+\ell s)t}) = \eta(A^{(k+s)t})\eta(A^{(p-k+\ell s)t}) = \eta(A^{(p+(\ell+1)s)t}).$$

Per Induktion über $\ell \in \mathbb{N}_0$ ist dann $\eta(A^{pt}) = \eta(A^{(p+\ell s)t})$ für alle $p \geq k, \ell \geq 0$. Für $r > 0$ hinreichend groß ist $p := rs \geq k$. Sei nun $n > 0$ beliebig, dann gilt mit $\ell = (n-1)r$:

$$\eta(A^{pt}) = \eta(A^{(p+\ell s)t}) = \eta(A^{(rs+(n-1)rs)t}) = \eta(A^{nrst}) = \eta((A^{pt})^n).$$

Damit ist

$$\eta(A^{pt}) = \bigcup_{n>0} \eta((A^{pt})^n) = \eta\left(\bigcup_{n>0} (A^{pt})^n\right) = \eta((A^{pt})^+).$$

■

Satz 6.4. *Für eine reguläre Sprache $L \subseteq A^*$ sind äquivalent:*
(a) *$L \in FO[Reg]$.*
(b) *$L \in FO[<, \equiv]$.*
(c) *η_L ist quasi-aperiodisch.*
(d) *L wird von einem quasi-aperiodischen Monoidhomomorphismus erkannt.*

Beweis.

- (a) $\iff$ (b): Dies haben wir bereits am Anfang des Abschnitts argumentiert.
- (c) $\implies$ (d): η_L erkennt L.
- (d) $\implies$ (c): Sei M ein endliches Monoid und $\eta : A^* \to M$ ein quasi-aperiodischer Monoidhomomorphismus, welcher L erkennt. Seien dann $t > 0$ und $H' \leq \eta_L(A^t)$. Dann gibt es nach Prop. 6.3 ein $p > 0$, sodass $H := \eta_L(A^{pt}) = \eta_L((A^{pt})^+) \leq M(L)$ eine Unterhalbgruppe ist. Weil H' eine Halbgruppe ist, ist $H' \leq \eta_L(A^{pt}) = H$. Da M die Sprache L erkennt, ist $M(L) \preccurlyeq M$ und es gibt einen surjektiven Monoidhomomorphismus $\beta : M \to M(L)$, sodass $\eta_L = \beta \circ \eta$. Wegen $H = \eta_L(A^{pt}) = \beta(\eta(A^{pt}))$ ist dann $H' \leq H \preccurlyeq \eta(A^{pt})$. Nach Voraussetzung ist $\eta(A^{pt})$ aperiodisch, also ist mit Prop. 2.3 auch H' aperiodisch und damit η_L quasi-aperiodisch.
- (b) $\implies$ (c) Wir behaupten, dass für jede Formel $\phi \in FO[<, \equiv]$ der Monoidhomomorphismus θ_ϕ quasi-aperiodisch ist und zeigen diese Behauptung mit Induktion nach Formelaufbau. Da wir am Ende nur an der Aussage für $\emptyset$-Strukturen bzw. geschlossene Formeln ϕ interessiert sind und für diese $\eta_\phi = \theta_\phi$ gilt, ist dies hinreichend.

  Q_a Wir haben bereits im Beweis von Satz 3.5 gezeigt, dass $N(Q_a x) = \{1\}$ aperiodisch ist, insbesondere ist dann $\theta_{Q_a x}$ quasi-aperiodisch.

  $<$ Analog wie für $Q_a x$.

$\equiv$ Für $t > 0$, $p > 0$ und eine $\{x\}$-Struktur $u'wu''$ mit $w \in A^t$ gilt:

$$u'wu'' \models x \equiv_p 0 \quad \iff \quad u'a^tu'' \models x \equiv_p 0.$$

daher ist $w \equiv_{x\equiv_p 0} a^t$, also ist $\theta_{x\equiv_p 0}(A^t) = \{\theta_{x\equiv_p 0}(a^t)\}$ und damit $\theta_{x\equiv_p 0}$ aperiodisch.

$\wedge$ Seien nun $\phi, \psi \in FO[<, \equiv]$ mit θ_ϕ, θ_ψ quasi-aperiodisch. Seien dann $t > 0$ und $H' \leq \theta_{\phi\wedge\psi}(A^t)$ eine Unterhalbgruppe. Dann gibt es nach Lemma 6.3 ein $p > 0$, sodass $H := \theta_{\phi\wedge\psi}(A^{pt}) = \theta_{\phi\wedge\psi}((A^{pt})^+) \leq N(\phi \wedge \psi)$ eine Unterhalbgruppe ist. Weil H' eine Halbgruppe ist, ist $H' \leq \theta_{\phi\wedge\psi}(A^{pt}) = H$. Nach [S, V.6.1] ist $N(\phi \wedge \psi) \preccurlyeq N(\phi) \times N(\psi)$, daher gibt es einen surjektiven Monoidhomomorphismus $\beta : N(\phi) \times N(\psi) \to N(\phi \wedge \psi)$ mit $\theta_{\phi\wedge\psi} = \beta \circ (\theta_\phi, \theta_\psi)$. Folglich ist

$$H = \theta_{\phi\wedge\psi}(A^{pt}) = \beta((\theta_\phi, \theta_\psi)(A^{pt})) = \beta(\theta_\phi(A^{pt}) \times \theta_\psi(A^{pt})).$$

Daher ist $H' \leq H \preccurlyeq \theta_\phi(A^{pt}) \times \theta_\psi(A^{pt})$. Nach Induktionsvoraussetzung sind $\theta_\phi(A^{pt})$, $\theta_\psi(A^{pt})$ aperiodisch, also ist mit Prop. 2.3 auch H' aperiodisch und damit $\theta_{\phi\wedge\psi}$ quasi-aperiodisch.

$\neg$ Nach [S, V.6.1] ist $\theta_{\neg\phi} = \theta_\phi$, also also ist dieser Schritt trivial.

$\exists$ Sei nun $\phi \in FO[<, \equiv]$ mit θ_ϕ quasi-aperiodisch. Seien dann $t > 0$ und $H' \leq \theta_{\exists x\phi}(A^t)$ eine Unterhalbgruppe. Dann gibt es nach Lemma 6.3 ein $p > 0$, sodass $\theta(A^{pt}) = \theta((A^{pt})^+)$. Mit der Aussage und Notation von Prop. 2.1 ist

$$H := \theta_{\exists x\phi}(A^{pt}) = \beta(\theta(A^{pt})) = \beta(\theta((A^{pt})^+)) = \theta_{\exists x\phi}((A^{pt})^+) \leq N(\exists x\phi).$$

Weil H' eine Halbgruppe ist, ist $H' \leq \theta_{\exists x\phi}(A^{pt}) = H$.
Wegen $H = \beta(\theta(A^{pt}))$ ist zugleich $H \preccurlyeq \theta(A^{pt})$. Mit $F := \{0,1\}^{M(\phi)\times M(\phi)}$ ist $\theta(A^{pt}) \leq \{0,1\}^{\square M(\phi)} = F * *M(\phi)$ und damit sicherlich auch $\theta(A^{pt}) \leq F * *\pi_{M(\phi)}(\theta(A^{pt}))$. Es folgt:

$$H' \leq H \preccurlyeq \theta(A^{pt}) \leq F * *\pi_{M(\phi)}(\theta(A^{pt})) = F * *\theta_\phi(A^{pt}).$$

Da jedes Element f des Monoids F idempotent ist, ist F endlich und aperiodisch. Nach Induktionsvoraussetzung ist θ_ϕ quasi-aperiodisch und damit $\theta_\phi(A^{pt})$ endlich und aperiodisch. Mit Prop. 2.3 ist dann H' endlich und aperiodisch und damit $\theta_{\exists x\phi}$ quasi-aperiodisch.

- (c) $\implies$ (b): Sei nun $L \subseteq A^*$ regulär und η_L quasi-aperiodisch. Dann gibt es $T \subseteq M(L)$ mit $L = \eta_L^{-1}(T)$. Nach Lemma 6.3 (angewandt auf den Fall $t = 1$) gibt es ein $p > 0$, sodass $H := \eta_L(A^p) = \eta_L((A^p)^+)$ eine Halbgruppe und damit nach Voraussetzung aperiodisch ist. Wir können jedes Wort $w \in L$ als ein Produkt eines Wortes $u \in (A^p)^*$ mit einem Wort $v \in A^*$ mit $0 \leq |v| < p$ darstellen, d.h.:

$$L = \bigcup_{0\leq|v|<p} L_v \cdot v, \qquad \text{wobei} \qquad L_v := \{u \in (A^p)^* : u \cdot v \in L\}.$$

Wir möchten zeigen, dass wir L mit einer Formel in $FO_A[<, \equiv]$ beschreiben können. Da obige Vereinigung endlich ist, reicht es, für $v \in A^*$, $0 \leq |v| < p$ eine Formel $\phi \in FO_A[<, \equiv]$ für $L_v \cdot v$ zu finden. Angenommen, es gibt eine Formel $\psi \in FO_A[<, \equiv]$, welche L_v beschreibt. Dann erhalten wir mit derselben Technik wie in Lemma 3.2 eine Relativierung $\psi[\leq x] \in FO_A[<, \equiv]$ von ψ. Mit $v = a_1 \cdots a_r$ wird die Sprache $L_v \cdot v$ dann durch die Formel

$$\phi := \exists x \left(\psi[\leq x] \wedge \exists y_1 \cdots \exists y_r \left((y_1 = x + 1) \wedge \left(\bigwedge_{j=1}^{r-1} (y_{i+1} = y_i + 1) \right) \wedge \left(\bigwedge_{j=1}^{r} Q_{a_i} y_i \right) \right) \right) \vee \neg\exists y \top.$$

beschrieben. Weil $z = z'' + 1$ äquivalent ist zu $z < z'' \wedge \neg\exists z(z < z' \wedge z' < z'')$, ist $(z = z'' + 1) \in FO_A[<]$ und damit $\phi \in FO_A[<, \equiv]$. Es reicht daher nun, eine Formel $\psi \in FO_A[<, \equiv]$ für L_v zu finden.

Dazu setzen wir $B := A^p$ und behandeln nun B – anders als gewohnt – als ein weiteres Alphabet neben A. Wir können nun die Abbildung $\eta_0 : B \to H = \eta_L(A^p) : b \mapsto \eta_L(b)$ zu einem Monoidhomomorphismus

$\eta : B^* \to H^* = H \cup \{1\}$ fortsetzen. Man beachte, dass wegen H aperiodisch auch $H \cup \{1\}$ aperiodisch ist, denn 1 erfüllt trivialerweise auch $1^k = 1^{k+1}$. Für $u \in B^*$ gilt dann:

$$u \in L_v \quad \iff \quad u \cdot v \in L \quad \iff \quad \eta(u) \cdot \eta_L(v) \in T,$$

also ist $L_v = \eta^{-1}(T_v)$ mit $T_v := \{h \in H \cup \{1\} : h \cdot \eta_L(v) \in T\} \subseteq H \cup \{1\}$. Folglich wird L_v, aufgefasst als Sprache über B, von einem aperiodischen Monoid erkannt. Nach Satz 3.5 gibt es daher eine Formel $\sigma \in FO_B[<]$, welche L_v beschreibt. Wir behaupten nun, dass es zu jeder Formel $\sigma \in FO_B[<]$ eine Formel $\sigma' \in FO_A[<, \equiv]$ gibt, sodass gilt:

$$\forall w \in B^* : \quad w \models \sigma \quad \iff \quad w \models \sigma'.$$

Wir zeigen diese Behauptung mit Induktion nach dem Aufbau der Formel σ:

$$\begin{array}{ll}
(Q_{a_1 \cdots a_p} x)' & := \exists x \left(Q_{a_p} x \wedge \exists y_1 \cdots \exists y_r \left((y_1 = x) \cap \left(\bigwedge_{j=1}^{p-1} (y_{i+1} = y_i + 1) \right) \cap \left(\bigwedge_{j=1}^{p} Q_{a_i} y_i \right) \right) \right) \\
(x < y)' & := (x < y) \\
(\sigma_1 \wedge \sigma_2)' & := \sigma_1' \wedge \sigma_2' \\
(\neg \sigma)' & := \neg(\sigma') \\
(\exists x \sigma)' & := \exists x((x \equiv_p 0) \wedge \sigma')
\end{array}$$

Man überzeugt sich leicht davon, dass die so definierte Formel σ' das Gewünschte leistet. Wir beobachten:

$$\forall w \in A^* : \quad w \in B^* \quad \iff \quad w \models \forall y(\forall x(x \leq y) \to (y \equiv_p 0)) =: \tau_p.$$

Daher ist $\psi := \sigma' \wedge \tau_p$ eine Formel in $FO_A[<, \equiv]$, welche L_v (nun aufgefasst als Sprache über A) beschreibt und wir sind fertig.

■

Korollar 6.5. *Ob eine gegebene reguläre Sprache $L \subseteq A^*$ in $FO[Reg]$ ist, ist entscheidbar.*

Beweis. Mit analoger Argumentation wie für Korollar 3.7 können wir das syntaktische Monoid $M(L)$ und den syntaktischen Homomorphismus η_L berechnen. Für $k = 1, 2, \ldots$ können wir $\eta_L(A^k)$ berechnen, bis wir, weil L regulär ist, Indizes $0 \leq j < k$ finden mit $\eta_L(A^j) = \eta_L(A^k)$. Dann wissen wir, dass jede Menge $\eta_L(A^t)$, $t > 0$ mit einer Menge $\eta_L(A^j)$, $0 < j \leq k$, übereinstimmt. Nach Satz 6.4 ist L genau dann in $FO[Reg]$, wenn jede Unterhalbgruppe jeder Menge $\eta_L(A^j)$, $0 < j \leq k$, aperiodisch ist. Dies ist berechenbar. ■

Beispiel 6.6. In Bsp. 3.6 haben wir gesehen, dass $L := (A^p)^* = \{w \in A^* : |w| \equiv_p 0\} \notin FO[<]$ für $p > 1$. Die Formel τ_p im Beweis von Satz 6.4 beschreibt genau L, also ist $L \in FO[<, \equiv] = FO[Reg]$. Man sieht auch leicht, dass η_L quasi-aperiodisch ist, denn $\eta_L(A^t) = \{\eta_L(a^t)\}$.

Beispiel 6.7. Für $a, b \in A$, $a \neq b$, sei $L := \{w \in A^* : |w|_a \equiv_p 0\}$. Dann ist (bis auf Isomorphie) $M(L) = \mathbb{Z}_p$ und $\eta_L : A^* \to \mathbb{Z}_p : w \mapsto |w|_a$. Wegen $\mathbb{Z}_p$ endlich ist L regulär. Für $k + p \cdot \mathbb{Z} \in \mathbb{Z}_p$ ist $k + p \cdot \mathbb{Z} = \eta_L(a^k b^{p-k}) \in \eta_L(A^p)$, also ist $\eta_L(A^p) = \mathbb{Z}_p$, da $\mathbb{Z}_p$ eine nichttriviale Gruppe ist, nicht aperiodisch. Folglich ist η_L nicht quasi-aperiodisch und damit $L \notin FO[Reg]$

Korollar 6.8. *Sei $|A| \geq 2$. Dann ist $FO[+1] \subsetneqq FO[<] \subsetneqq FO[Reg] \subsetneqq SOM[+1]$.*

Beweis. Aus den Sätzen 3.5, 5.2 und 6.4 folgen die drei Inklusionen. Die Ungleichheit $FO[+1] \neq FO[<]$ wird in [S, IV.3.4] gezeigt. Die anderen beiden Ungleichheiten folgen nun aus den Beispielen 3.6, 6.6 und 6.7. ■

Literatur

[S] Howard Straubing *Finite Automata, Formal Logic and Curcuit Complexity* Springer Science+Business Media, LLC; New York 1994; ISBN 978-1-4612-6695-2