Seminar

Modulare Quantoren

Lucas Unterberger

1325438

11. Jänner 2020

Betreuer
Associate Prof. Dipl.-Ing. Dr.techn. Stefan Hetzl

Inhaltsverzeichnis

1 Einleitung und Definitionen

Diese Arbeit basiert auf [1]. Es wird definiert wie Wörter Formeln erfüllen können und es werden Klassifikationen gewisser Logiken gegeben und deren Zusammenhang zu Sprachen untersucht. Dabei werden Eigenschaften von Sprachen zu Eigenschaften des zugehörigen syntaktischen Monoids übersetzt. Dies führt auf natürliche Weise zu algebraischen Überlegungen und Klassifikationen. Es wird daher ein Grundwissen der Algebra und Mengentheorie vorausgesetzt. Im Vordergrund stehen die in [1] Kapitel VII eingeführten 'modularen Quantoren' der Art $\exists^{(q,r)}$. Diese sollen für 'es existieren r modulo q viele Stellen...' stehen. Eine genaue Definition und eine Klassifikation der entstehenden Formeln werden in dieser Arbeit gegeben.

Sei A ein Alphabet, also eine Menge von Elementen, die wir *Buchstaben* nennen. Dann ist ein $Wort$ w über A definiert als eine endliche Folge von Buchstaben, die konkateniert geschrieben wird:

$$w = a_1 a_2 ... a_k \text{ mit } a_i \in A$$

Die *Länge* eines Wortes w, geschrieben als $|w|$, ist die Anzahl der Buchstaben aus denen das Wort besteht. Das *leere Wort*, also das eindeutige Wort, das aus keinen Buchstaben besteht nennen wir ϵ. Zwei Wörter w, v können konkateniert werden und bilden ein neues Wort wv. Statt ww wird auch w^2 geschrieben. Nun definieren wir A^* als die Menge aller Wörter über dem Alphabet A; A^+ soll als $A^* \setminus \epsilon$ definiert sein. Sei $L \subseteq A^*$, dann nennen wir L eine *Sprache* über A. Wenn der Kontext klar ist sagen wir einfach L ist eine Sprache. Es folgen nun die nötigen Definitionen um Formeln die von Wörtern erfüllt werden zu definieren. Wir definieren Formeln induktiv über deren Formelaufbau. Eine $Variable$ (erster Stufe) ist ein Symbol der Art

$$x, x_1, x_2, ..., y, y_1, y_2, ...$$

Ein *numerisches Prädikat* ist ein Symbol der Art R_i^j mit $i > 0, j \geq 0$. Es gibt zwei Arten von $Atomformeln$.

- Falls x eine Variable und $a \in A$ ist, dann ist $Q_a x$ eine Atomformel.
- Falls $x_1, ..., x_j$ Variablen sind und $i > 0$, dann ist $R_i^j(x_1, ..., x_j)$ eine Atomformel.

Definition 1.1. *Man definiert eine Formel induktiv.*

- *Jede Atomformel ist eine Formel.*
- *Sind ϕ und ψ Formeln, dann sind $\phi \wedge \psi$, $\neg\phi$ und $\exists x\phi$ Formeln.*

- *Ist* $q \in \mathbb{Z}^+$ *und* $0 \leq r < q$ *und* ϕ *eine Formel, dann ist* $\exists^{(q,r)} x\phi$ *eine Formel.*

Ein Vorkommen einer Variable in einer Formel heißt *frei*, falls es keine Quantoren in der Formel gibt, die genau vor dieser Variable stehen. Falls es so einen gibt, dann heißt die Variable *gebunden*.

Definition 1.2. *Eine* $\mathcal{V}-$*Struktur über einem Alphabet* A *ist ein Wort der Art* $(a_1, U_1)...(a_n, U_n)$ *über dem Alphabet* $A \times \mathcal{P}(\mathcal{V})$*, sodass*

- U_i *sind paarweise disjunkt*
- *die Vereinigung der* U_i *ist* $\mathcal{V}$*.*

Sei w eine $\mathcal{V}$-Struktur, sodass für eine Gleichung ϕ gilt, dass falls x frei in ϕ ist, dann ist $x \in \mathcal{V}$ und falls x gebunden ist, dann ist $x \notin \mathcal{V}$. Außerdem darf keine Variable mehr als einmal gebunden werden.

Definition 1.3. *Wir definieren* $w \models_I \phi$*, d.h. eine* $\mathcal{V}$*-Struktur* w *erfüllt eine Gleichung* ϕ*, induktiv über den Formelaufbau von* ϕ*.*

- $w \models_I Q_a x :\Leftrightarrow w$ *enthält einen Buchstaben* (a, S)*, mit* $x \in S$*.*
- $w \models_I R_i^k(x_1, ..., x_k) :\Leftrightarrow$ *die durch* I *zu* R_i^k *assoziierte* k*-stellige Relation ist erfüllt wobei die Variablen für Positionen in* w*, an den Stellen* $w_1, ..., w_k$*, stehen.*
- $w \models_I \phi \wedge \psi :\Leftrightarrow w \models_I \phi$ *und* $w \models_I \psi$
- $w \models_I \neg\phi :\Leftrightarrow w$ *ist kein Modell von* ϕ *in* I*.*
- $w \models_I \exists x\phi :\Leftrightarrow$ *es existiert eine Position* i*, sodass* $(a_1, S_1)...(a_i, S_i \cup \{x\})...(a_r, S_r) \models_I \phi$*.*
- $w \models_I \exists^{(q,r)} x\phi :\Leftrightarrow$ *es existieren* r *modulo* q *Positionen, sodass die um* x *an diesen Positionen erweiterte Struktur* $w' \models_I \phi$*.*

Falls ϕ ein Satz ist, also keine freien Variablen enthält, dann definieren wir $L_\phi := \{w \in A^* : w \models_I \phi\}$, da $\emptyset$-Strukturen solche Formeln erfüllen können. Falls der Kontext klar ist wird I nicht erwähnt beziehungsweise L statt L_ϕ geschrieben.

Seien $\phi, \psi : S \to T_1, T_2$ zwei Homomorphismen. Wir sagen ψ faktorisiert durch ϕ genau dann, wenn $\forall(s_1, s_2) \in S : (\phi(s_1) = \phi(s_2) \Rightarrow \psi(s_1) = \psi(s_2))$. Dann gilt $\exists$ Homomorphismus $v : \phi(S) \to T_2$ mit $v \circ \phi = \psi$.

Zu einer Sprache L definiert man eine Kongruenzrelation auf A^* durch $w_1 \equiv_L w_2 :\Leftrightarrow (\forall u, v \in A^* : uw_1v \in L \Leftrightarrow uw_2v \in L)$. Wir nennen $A^*/_{\equiv_L} =: M(L)$ das syntaktische Monoid von L und den zugehörigen Homomorphismus $\eta_L : A^* \to A^*/_{\equiv_L}$ den syntaktischen Morphismus. Diese Definitionen wollen wir von Wörtern auf $\mathcal{V}$-Strukturen erweitern. Dazu definiert man L als eine Familie von $\mathcal{V}$-Strukturen und passt obige Definitionen auf natürliche Weise an. Mit θ_ϕ bezeichnet man nun die Einschränkung von η_ϕ auf A^* und man schreibt $N(\phi)$ als das Bild von θ_ϕ. Ein Satz ϕ ist eine $\emptyset$-Struktur und die zugehörige Familie L wird mit der Sprache L identifiziert. Wenn der Kontext klar ist unterscheiden wir nicht zwischen den Schreibweisen η_L und η_ϕ, falls L die von ϕ erzeugte Familie von $\mathcal{V}$-Strukturen ist.

Ein Monoid N *teilt* ein Monoid M genau dann, wenn $\exists M' \leq M$ und es existiert ein surjektiver Homomorphismus $\phi : M' \to N$. Dies schreibt man als $N \prec M$. Das bedeutet, dass N homomorphes Bild eines Untermonoids von M ist. Wir sagen ein Monoid M *erkennt* eine Sprache $L \subseteq A^*$ genau dann, wenn $\exists T \subseteq M$ und $\exists \phi : A^* \to M$, sodass $L = \phi^{-1}(T)$. Dann sagen wir ϕ erkennt L.

Satz 1.1. *Sei $L \subseteq A^*$, M ein Monoid und $\gamma : A^* \to M$ ein Homomorphismus. Dann wird L von γ erkannt genau dann, wenn η_L durch γ faktorisiert. Ein Monoid M erkennt L genau dann, wenn $M(L) \prec M$.*

Definition 1.4 (bilaterale Semidirekte Produkt)**.** *Seien $(S, +, 0)$ und $(T, \cdot, 1)$ zwei Monoide, sodass eine Linksaktion: $T \times S \to S$ und eine duale Rechtsaktion existieren. Falls diese Aktionen monoidisch und kompatibel sind, dann definiert man das bilaterale Semidirekte Produkt $S * *T := (S \times T, \cdot)$ durch $(s_1, t_1) \cdot (s_2, t_2) := (s_1t_2 + t_1s_2, t_1 \cdot t_2)$.*

Man beachte, dass Terme der Art s_1t_2 die Rechtsaktion von t_2 auf s_1 darstellen und nach S abbilden, nicht zu verwechseln mit einer Multiplikation, diese macht keinen Sinn für Elemente aus zwei verschiedenen Monoiden.

Definition 1.5 (Blockprodukt)**.** *Seien $(M, \cdot, 1)$ und $(N, \cdot, 1)$ Monoide, mit geeigneten Links- und Rechtsaktionen, dann definieren wir das Blockprodukt $M \,\square\, N := M^{N\times N} * *N$. Außerdem schreiben wir $(M^{N\times N}, +, 0)$ für das Monoid mit komponentenweiser Multiplikation, um konsistent mit der obigen Schreibweise zu bleiben.*

Mehr zu diesen Konstruktionen und, dass es sich dabei wieder um Algebren handelt findet man in [1] Kapitel V.

Definition 1.6 (Pseudovarietäten)**.** *Eine Familie $\boldsymbol{V}$ von endlichen Halbgruppen heißt Pseudovarietät, falls*

- *Falls $S, T \in \boldsymbol{V}$, dann ist auch $S \times T \in \boldsymbol{V}$.*
- *Falls $T \in \boldsymbol{V}$ und $S \prec T$, dann ist auch $S \in \boldsymbol{V}$.*

Es folgt noch ein wichtiger Satz, der zu einem Monoid die Existenz eines Blockprodukts sichert, sodass dieses Monoid das Blockprodukt teilt.

Satz 1.2 (Krohn-Rhodes)**.** *Sei M ein endliches Monoid. Dann existiert eine Folge $M_0, ..., M_k$ endlicher Monoide, sodass $M_0 = \{1\}$ und $M \prec M_k$ und*

$$\forall i = 1, ..., k : M_i = N \,\square\, M_i$$

wobei N entweder eine einfache Gruppe ist, die M teilt, oder $N = U_1 = (\{0,1\}, \cdot, 1)$. Falls M eine Gruppe ist muss kein Faktor $N = U_1$ auftreten.

Für einen Beweise siehe [1] Appendix A.

2 Charakterisierung von $(FO + MOD(P))[<]$

In diesem Kapitel definieren wir wann eine Formel aus $(FO + MOD(P))[<]$ ist und es wird eine Charakterisierung für solche Formeln gegeben. Genauer gesagt werden Bedingungen an das syntaktische Monoid der zugehörigen Sprache dieser Formeln gegeben, die genau dann erfüllt sind, wenn die besagte Formel in $(FO + MOD(P))[<]$ ist. Im vorherigen Kapitel wurde schon erläutert, dass die Struktur eines zu einer Sprache gehörigen syntaktischen Monoids wesentlich ist um Eigenschaften der Sprache herzuleiten.

Wir schreiben $FO[C]$ für die Familie von Sprachen, die durch Sätze erster Stufe über einer Klasse von numerischen Prädikaten C definiert sind. Analog schreiben wir $MOD(P)[C]$ für die Familie von Sprachen, deren Sätze durch numerische Prädikate aus C und modulare Quantoren $\exists^{(q,r)}$ mit $0 \leq r < q \in P$ und $P \subseteq \mathbb{N}$ definiert werden. Wir schreiben $(FO + MOD(P))[C]$ für die Familie von Sprachen, deren Sätze sowohl aus Sätzen erster Stufe, numerischen Prädikaten aus C und modularen Quantoren mit Modul $p \in P$ definiert sind.

Ein Beispiel einer Sprache die mit modulare Quantoren definiert wird ist

$$\exists^{(2,0)} x(x = x).$$

Dieser Satz definiert Wörter mit gerader Länge, da eine gerade Anzahl an Positionen existieren muss, sodass $x = x$ erfüllt ist. Da $True$ immer erfüllt ist müssen Wörter, die diese Formel erfüllen, eine gerade Anzahl an Stellen besitzen. Ein weiteres Beispiel ist

$$\exists^{(2,1)} x \exists y \exists z((y = x + 1) \wedge (z = y + 1) \wedge Q_a x \wedge Q_a y \wedge Q_a z).$$

Wörter die diese Formel erfüllen haben Teilwörtern der Art aaa an ungerade vielen Stellen.

Eine wichtige Anmerkung ist, dass modulare Quantoren immer reguläre Sprachen definieren. Die Formel $\exists^{(q,r)} x\phi$ ist äquivalent zu folgender monadischen Formel zweiter Stufe

$$\exists X(\forall x(\phi(x) \leftrightarrow X(x)) \wedge (|X| \equiv r \pmod{q})).$$

Da $|X| \equiv r \pmod{q}$ durch monadische Logik zweiter Stufe ausgedrückt werden kann, ist die gesamte Formel äquivalent zu einer monadischen Formel zweiter Stufe. Die zugehörigen Sprachen sind regulär.

Sei G eine endliche Gruppe. G hat eine *Subnormalreihe*, wenn eine echt absteigende Kette von Normalteilern von G existiert, sodass $G = G_0 \triangleright G_1 \triangleright ... \triangleright G_n = \{1\}$. G heißt *auflösbar* genau dann, wenn G eine Subnormalreihe mit abelschen Faktoren hat, also G_i/G_{i+1} ist abelsch für alle i. Ein endliches Monoid M heißt *auflösbar* genau dann, wenn jede Gruppe die in M enthalten ist auflösbar ist. $\mathbf{G}_P$ nennen wir die Pseudovarietät der endlichen Gruppen deren Mächtigkeit ein Produkt von Elementen aus P teilt, diese ist tatsächlich eine Pseudovarietät. Dann definieren wir $\mathbf{M}_P$ als die Pseudovarietät der endlichen Monoide in denen jede enthaltene Gruppe in $\mathbf{G}_P$ ist.

Das Hauptziel dieses Kapitels ist der folgende Satz.

Satz 2.1. *Sei $P \subseteq \mathbb{Z}^+$ und $L \subseteq A^*$.*

a) Sei $P \neq \emptyset$, dann gilt $L \in MOD(P)[<] \Leftrightarrow M(L) \in \boldsymbol{G}_P$.

b) $L \in (FO + MOD(P))[<] \Leftrightarrow M(L) \in \boldsymbol{M}_P$.

Dieser Satz liefert eine Klassifikation von Sprachen aus $MOD(P)[<]$ und $(FO + MOD(P))[<]$.

Um diesen Satz zu beweisen benötigen wir einige Hilfssätze. Im Folgenden steht $M(\phi)$ und η_ϕ für das syntaktische Monoid und den syntaktischen Morphismus von ϕ und $N(\phi)$ beziehungsweise θ_ϕ für die Einschränkung dieser auf A^*.

Lemma 2.1. *sei $0 \leq r < q$ und $\psi \in (FO + MOD)[<]$, dann gilt:*

a) Sei $\phi = \exists^{(q,r)} x\psi \Rightarrow \exists \zeta : A^* \to \mathbb{Z}_q \,\square\, M(\psi)$, sodass $\pi_{M(\psi)} \circ \zeta = \theta_\psi$ und θ_ϕ faktorisiert durch ζ.

b) Sei $\phi = \exists x\psi \Rightarrow \exists \zeta : A^* \to U_1 \,\square\, M(\psi)$, sodass $\pi_{M(\psi)} \circ \zeta = \theta_\psi$ und θ_ϕ faktorisiert durch ζ.

Beweis. Wir starten mit b).

Wir wollen zuerst einen Homomorphismus τ mit den gewünschten Eigenschaften auf einer größeren Definitionsmenge konstruieren und erhalten dann ζ durch eine geschickte Einschränkung von τ.

Sei $\mathcal{V}$ die Menge der freien Variablen von $\phi = \exists x\psi$. Man beachte dass x frei in ψ aber gebunden in ϕ ist. Sei $\eta_\psi : (A \times \mathcal{P}(\mathcal{V} \cup \{x\}))^* \to M(\psi)$ der syntaktische Morphismus zu ψ und $T \subseteq M(\psi)$ so, dass $L_\psi = \eta_\psi^{-1}(T)$ ist. Wir definieren nun einen Homomorphismus

$$\tau : (A \times \mathcal{P}(\mathcal{V} \cup \{x\}))^* \to U_1 \wr M(\psi)$$

indem wir das Bild eines Buchstabens setzen als $\tau(a, S) \mapsto (F, \eta_\psi(a, S))$. $F \in U_1^{M(\psi)\times M(\psi)}$ definieren wir als

$$F(n_1, n_2) := \begin{cases} 0 & \text{falls } \; n_1 \cdot \eta_\psi(a, S \cup \{x\}) \cdot n_2 \in T \\ 1 & \text{sonst.} \end{cases}$$

Nun erzwingen wir, dass τ ein Homomorphismus ist indem wir für ein Wort $w = (a_1, S_1)...(a_n, S_n)$ das Bild unter Tau definieren als

$$\tau(w) = \tau(a_1, S_1) \cdot ... \cdot \tau(a_n, S_n).$$

Also folgt

$$\tau(w) = (F_1, \eta_\psi(a_1, S_1)) \cdot ... \cdot (F_n, \eta_\psi(a_n, S_n)).$$

Man beachte, dass wir $U_1 = (\{0, 1\}, \cdot, 1)$ multiplikativ schreiben im Gegensatz zu $(U_1^{M(\psi)\times M(\psi)}, +, 0)$. Dann folgt nach n-maligem Ausmultiplizieren

$$\tau(w) = \left(\sum_{i=1}^{n} \eta_\psi(a_1, S_1) \; ... \; F_i \; ... \; \eta_\psi(a_n, S_n), \eta_\psi((a_1, S_1)...(a_n, S_n)) \right).$$

Der rechte Eintrag ergibt sich, da η_ψ ein Homomorphismus ist und der Linke durch die Definition der Multiplikation im Blockprodukt. Wir erinnern kurz, dass die Summe zweier solcher Funktionen als komponentenweises Produkt definiert war, also $(F_1 + F_2)(n_1, n_2) := F_1(n_1, n_2) \cdot F_2(n_1, n_2) \in U_1$. Hier wirkt $\eta_\psi(.,.)$ dabei von links beziehungsweise rechts auf F_i.

Wir betrachten nun nur den linken Eintrag, nennen ihn G und werten ihn an (n_1, n_2) aus.

$$G(n_1, n_2) = \prod_{i=1}^{n} (\eta_\psi(a_1, S_1) \; ... \; F_i \; ... \; \eta_\psi(a_n, S_n))(n_1, n_2)$$

Dies ist weiter gleich

$$\prod_{i=1}^{n} F_i(n_1 \cdot \eta_\psi(a_1, S_1) \cdot ... \cdot \eta_\psi(a_{i-1}, S_{i-1}), \eta_\psi(a_{i+1}, S_{i+1}) \cdot ... \cdot \eta_\psi(a_n, S_n) \cdot n_2).$$

Wenn wir nun $G(1,1)$ betrachten erhalten wir

$$G(1,1) = \prod_{i=1}^{n} F_i(\eta_\psi((a_1, S_1)...(a_{i-1}, S_{i-1})), \eta_\psi((a_{i+1}, S_{i+1})...(a_n, S_n))).$$

Nun betrachten wir alle Wörter für die $G(1,1) = 0$ gilt. $G(1,1) = 0$ gilt genau dann, wenn zumindest ein Faktor des oberen Produkts gleich $0 \in U_1$ ist. Das ist genau dann der Fall wenn $\eta_\psi((a_1, S_1)...(a_i, S_i \cup \{x\})...(a_n, S_n)) \in T$. Dies gilt genau dann, wenn $((a_1, S_1)...(a_i, S_i \cup \{x\})...(a_n, S_n)) \in \eta_\psi^{-1}(T) = L_\psi$. Also sind die Menge dieser Wörter genau die Wörter, sodass eine Zerlegung $w = w_1(a, S)w_2$ existiert und $w_1(a, S \cup \{x\})w_2 \in L_\psi$. Das sind genau jene Wörter für die $w \models \exists x\psi$ gilt.

Nun definieren wir $K := \{(G, m) \in U_1 \square M(\psi) : G(1,1) = 0\}$. Dann gilt $\tau^{-1}(K) = L_{\exists x\psi}$. Nach Satz 1.1 faktorisiert nun $\eta_{\exists x\psi}$ durch τ und $\pi_{M(\psi)} \circ \tau$ ist die Einschränkung von η_ψ auf $(A \times \mathcal{P}(\mathcal{V}))^*$. Das gewünschte Resultat erhält man nun durch Setzen von ζ als Einschränkung von τ auf A^*.

Beweis von a). Dieser Teil folgt nun sehr analog zu Punkt b). Wir definieren diesmal

$$\tau : (A \times \mathcal{P}(\mathcal{V} \cup \{x\}))^* \to \mathbb{Z}_q \square M(\psi)$$

und setzen das Bild eines Buchstabens unter τ als $\tau(a, S) \mapsto (F, \eta_\psi(a, S))$. Mit $F \in \mathbb{Z}_q^{M(\psi) \times M(\psi)}$ definiert als

$$F(n_1, n_2) := \begin{cases} 1 & \text{falls } \; n_1 \cdot \eta_\psi(a, S \cup \{x\}) \cdot n_2 \in T \\ 0 & \text{sonst.} \end{cases}$$

Dann folgt nach Multiplikation im Blockprodukt und gleicher Definition von G

$$G(1,1) = \sum_{i=1}^{n} F_i(\eta_\psi((a_1, S_1)...(a_{i-1}, S_{i-1})), \eta_\psi((a_{i+1}, S_{i+1})...(a_n, S_n))) \in \mathbb{Z}_q.$$

Man beachte, dass $(\mathbb{Z}_q, +, 0)$ additiv geschrieben ist. Nun ist $G(1,1) = r$ genau dann wenn r modulo q viele Summanden gleich 1 sind. Mit denselben Überlegungen wie vorher erhalten wir, dass das genau dann der Fall ist, wenn

$$w \models_I \exists^{(q,r)} x\psi.$$

Damit erkennt das Blockprodukt $L_{\exists^{(q,r)} x\psi}$ und wir erhalten das gewünschte Resultat durch Einschränken von τ zu A^*. $\square$

Im Folgenden brauchen wir die zu einer Formel $\phi \in (FO + MOD)[<]$ oder $MOD[<]$ 'relativierte Formel' $\phi[< x]$. Sei dazu $x \notin \mathcal{V}$ und w eine $\mathcal{V} \cup \{x\}$-Struktur, sodass alle Variablen in $\mathcal{V}$ links von der Variable x stehen. Außerdem sei w' das Wort bestehend aus allen Buchstaben von w, die links von x stehen. Dann ist w' eine $\mathcal{V}$-Struktur und es gilt: zu ϕ $\exists$ Formel $\phi[< x]$ mit freien Variablen in $\mathcal{V} \cup \{x\}$, sodass $w \models \phi[< x] \Leftrightarrow w' \models \phi$. Wir nennen $\phi[< x]$ die zu ϕ relativierte Formel.

Lemma 2.2. *Sei $q \in P$.*

a) Sei M ein endliches Monoid, sodass jede Sprache die von M erkannt wird in $(FO+MOD(P))[<]$ ist. Dann ist jede Sprache die von $U_1 \square M$ oder $\mathbb{Z}_q \square M$ erkannt wird auch in $(FO + MOD(P))[<]$.

b) Sei M ein endliches Monoid, sodass jede Sprache die von M erkannt wird in $MOD(P)[<]$ ist. Dann ist jede Sprache die von $\mathbb{Z}_q \square M$ erkannt wird auch in $MOD(P)[<]$.

Beweis. Wir betrachten zuerst den Fall für U_1 und vollenden später die Argumentation für $\mathbb{Z}_q$.

Sei M so wie oben definiert. Nun setzen wir $V := U_1^{M \times M}$. Dann ist $U_1 \square M = V * *M$ und V ist idempotent und kommutativ. Sei $L \subseteq A^*$ eine Sprache, die von einem Homomorphismus $\gamma : A^* \to V * *M$ erkannt wird. Dann existiert ein $T \subseteq V * *M$, sodass $L = \gamma^{-1}(T)$. Wir wollen nun zeigen, dass L in $(FO + MOD(P))[<]$ ist.

Es reicht dazu zu zeigen, dass $\forall (v, m) \in V * *M$ gilt, dass $\gamma^{-1}(v, m)$ definiert wird durch eine Formel $\phi_{(v,m)} \in (FO + MOD(P))[<]$. Wenn wir das gezeigt haben, nehmen wir für alle $(v, m) \in T$ die Disjunktion all dieser Formeln und können so L darstellen. Sei nun $w = a_1 ... a_n \in A^*$, dann ist $\gamma(w) = (v, m)$ genau dann wenn

1. $\pi_M \circ \gamma(w) = m$
2. $\pi_V \circ \gamma(w) = v$.

Wobei die zweite Bedingung bedeutet, dass

$$v = \sum_{i=1}^{n} \pi_V \circ \gamma(a_1) \cdot ... \cdot \pi_V \circ \gamma(a_{i-1}) \cdot \pi_M \circ \gamma(a_i) \cdot \pi_V \circ \gamma(a_{i+1}) \cdot ... \cdot \pi_V \circ \gamma(a_n).$$

Dies ist äquivalent zu

$$v = \sum_{w = w_1 a w_2} \pi_M \circ \gamma(w_1) \cdot \pi_M \circ \gamma(a) \cdot \pi_M \circ \gamma(w_2).$$

Nun ist $\pi_M \circ \gamma(w) = \pi_M \circ \eta_L(w) = m$ genau dann, wenn $w \models \alpha_m$ und $\alpha_m \in (FO + MOD(P))[<]$. Da V idempotent und kommutativ ist hängt die obige Bedingung nur von den Summanden ab und nicht von der Reihenfolge in der summiert wird. Deshalb erfüllt w diese Bedingung genau dann, wenn es eine boolsche Kombination von Bedingungen der Art

$$w = w_1 a w_2 \text{ und } \pi_M \circ \gamma(w_1) = m_1 \in M \text{ und } \pi_M \circ \gamma(w_2) = m_2 \in M.$$

Diese kann man nun mit Formeln beschreiben. Nämlich durch

$$\exists x(Q_a x \wedge \alpha_{m_1}[< x] \wedge \alpha_{m_2}[> x]).$$

Hier sind $\alpha_{m_1}[< x]$ und $\alpha_{m_2}[> x]$ Relativierungen der obigen Formel. Nun kann L als Konjunktion der α_m und einer boolschen Kombination aus Sätzen der obigen Form definiert werden.

Betrachten wir schlussendlich noch den Fall $V := \mathbb{Z}_q^{M \times M}$. Da V eine abelsche Gruppe mit Exponent q ist, ist Gleichheit in obiger Summe nur von der Anzahl der Summanden modulo q und nicht deren Reihenfolge abhängig. Es ergeben sich dadurch die Bedingungen

$$\begin{gathered} w \text{ hat } r \text{ modulo } q \text{ viele Aufspaltungen der Form } w_1 a w_2 \text{ und} \\ \pi_M \circ \gamma(w_1) = m_1 \in M \text{ und } \pi_M \circ \gamma(w_2) = m_2 \in M. \end{gathered}$$

Dies kann nun durch die Formeln

$$\exists^{(q,r)} x(Q_a x \wedge \alpha_{m_1}[< x] \wedge \alpha_{m_2}[> x]).$$

ausgedrückt werden. Dadurch kann jede Sprache die vom Blockprodukt erkannt wird durch eine boolsche Kombination solcher Sätze ausgedrückt werden. □

Nun können wir den Klassifikationssatz 2.1. beweisen.

Satz 2.1. *Sei $P \subseteq \mathbb{Z}^+$ und $L \subseteq A^*$.*

a) Sei $P \neq \emptyset$, dann gilt $L \in MOD(P)[<] \Leftrightarrow M(L) \in \boldsymbol{G}_P$.

b) $L \in (FO + MOD(P))[<] \Leftrightarrow M(L) \in \boldsymbol{M}_P$.

Beweis. '$\Leftarrow$': Sei $M(L) \in \mathbf{M}_P$, dann sind die einfachen Gruppen, die $M(L)$ teilen genau die zyklischen Gruppen $\mathbb{Z}_p$ und p ist ein primer Teiler eines Elements von P. Nach Satz 1.2 (Krohn-Rhodes) teilt dann $M(L)$ ein Blockprodukt der Art

$$M(L) \prec M_r \,\square\, (M_{r-1} \,\square\, ...(M_1 \,\square\, \{1\})...).$$

Wobei jedes M_i entweder gleich U_1 oder $\mathbb{Z}_p$ ist, p wie oben. Das triviale Monoid $\{1\}$ erkennt genau die Sprachen $\emptyset$ und A^*, da die Sätze $\alpha \wedge \neg\alpha$ und $\alpha \vee \neg\alpha$ diese Sprachen definieren. Also ist jede Sprache die von $\{1\}$ erkannt wird in $(FO + MOD(Q))[<]$, für alle $Q \subseteq \mathbb{Z}^+$. Nach Lemma 2.2 folgt, dass jede Sprache die vom iterierten Blockprodukt erkannt wird auch in $(FO+MOD(P'))[<]$ ist, mit P' gleich der Menge der primen Teiler von P. Wenn $p|q$ dann kann man jeden modularen Quantor mit Modul p auch mit einer Kombination aus modularen Quantoren mit Modul q schreiben. Dazu betrachtet man zu einer Formel $\psi_1 = \exists^{(p,r)}x\phi$ eine Formel $\psi_2 = \exists^{(q,r)}x\phi \vee \exists^{(q,r+p)}x\phi \vee \exists^{(q,r+2p)}x\phi \vee \exists^{(q,r+3p)}x\phi \vee ...$ mit Modul q, die zu ψ_1 äquivalent ist. Daraus folgt, dass $L \in (FO + MOD(P))[<]$. Falls $M(L) \in \mathbf{G}_P$, dann kommen nach Krohn-Rhodes keine Faktoren U_1 im iterierten Blockprodukt vor und mit Lemma 2.2 b) ist $L \in MOD(P)[<]$.

'$\Rightarrow$' Sei $L_\phi \in (FO + MOD(P))[<]$. Wir beweisen mit Induktion über den Formelaufbau von ϕ, dass $\eta_\phi(A^*) \in \mathbf{M}_P$. Falls nur modulare Quantoren auftreten, dann zeigen wir $\eta_\phi(A^*) \in \mathbf{G}_P$. Sei nun ϕ eine Atomformel, der Art $Q_a x$ oder $x < y$, dann ist das zu der Sprache gehörige syntaktische Monoid trivial. Dies sieht man, da für $w \in A^*$ und $L \subseteq A^*$ gilt, dass w einer $\emptyset$-Struktur entspricht und damit $w \equiv_\phi \epsilon$. Das triviale Monoid $\{1\}$ ist eine auflösbare Gruppe. Da $\mathbf{G}_P$ und $\mathbf{M}_P$ Pseudovarietäten sind, sind sie unter boolsche Operationen von Formeln abgeschlossen, siehe dazu [1] Kapitel V. Nun betrachten wir noch die existenziellen Quantoren.

Sei dazu $\phi = \exists^{(p,r)}x\psi$ und $M(\psi) \in \mathbf{M}_P$, zu zeigen ist $M(\phi) \in \mathbf{M}_P$. Nach Lemma 2.1 existiert ein Homomorphismus $\zeta : A^* \to \mathbb{Z}_q \,\square\, M(\psi)$, sodass θ_ϕ durch ζ faktorisiert. Das bedeutet es existiert ein Homomorphismus $v : \zeta(A^*) \to N(\phi)$. Sei G eine Gruppe, die in $\mathbb{Z}_q \,\square\, M(\psi)$ enthalten ist. Nach [1] Satz V.4.2 existiert ein Normalteiler H von G, sodass $G/H = \pi_{M(\psi)}(G)$ isomorph zu einer Gruppe in $M(\psi)$ ist und H isomorph zu einer Gruppe in $\mathbb{Z}_q^{M(\psi)\times M(\psi)}$ ist. Dann kann man G über die Projektion auf die beiden Koordinaten darstellen $G = \pi_{\mathbb{Z}_q^{M(\psi)\times M(\psi)}}(G) \times \pi_{M(\psi)}(G)$. Nun sind allerdings sowohl $\mathbb{Z}_q^{M(\psi)\times M(\psi)} \in \mathbf{M}_P$ als auch $M(\psi) \in \mathbf{M}_P$, da Pseudovarietäten abgeschlossen unter direkten Produkten sind. Also sind die Projektionen der Koordinaten von G auflösbar und damit ist G auflösbar. Damit ist das Blockprodukt $\mathbb{Z}_q \,\square\, M(\psi) \in \mathbf{M}_P$. Nach Lemma 2.1 teilt $N(\phi)$ das Blockprodukt $\mathbb{Z}_q \,\square\, M(\psi)$ und damit ist auch $M(\phi) \in \mathbf{M}_P$, da Pseudovarietäten abgeschlossen unter Teilern und Erweiterungen sind. Falls nur modulare Quantoren auftreten zeigt man mit Lemma 2.2 $\eta_\phi \in \mathbf{G}_P$. Den 'normalen' Existenzquantor behandelt man analog, nur nimmt man stattdessen das Blockprodukt $U_1 \,\square\, M(\psi)$ und verwendet Lemma 2.1 b). $\square$

3 Charakterisierung von $(FO + MOD(P))[Reg]$

Reguläre numerische Prädikate sind numerische Relationen, die durch endliche Automaten definiert werden können. Die Familie der regulären numerischen Prädikate nennen wir *Reg*. Nach [1] Satz III.2.1 sind alle regulären numerischen Prädikate in $FO_{\{a\}}[<, \equiv]$ darstellbar. Wir betrachten deshalb die Relationen $<$ und $\equiv$ in den folgenden Überlegungen.

Satz 3.1. *Sei $P \subseteq \mathbb{Z}^+$. Sei $L \subseteq A^*$ eine reguläre Sprache, dann sind äquivalent:*

a) $L \in (FO + MOD(P))[Reg]$

b) $\forall t > 0$*: jede Gruppe in* $\eta_L(A^t)$ *ist in* $\boldsymbol{G}_P$

Beweis. *a)* $\Rightarrow$ *b)*. Sei $\mathbf{S}_P$ die Familie der endlichen Halbgruppen, in der jede Gruppe in $\mathbf{G}_P$ ist. Dann ist $\mathbf{S}_P$ eine Pseudovarietät, siehe [1] Proposition V.6.4. Wir zeigen nun mit Induktion über den Formelaufbau von ϕ, dass für $L \in (FO + MOD(P))[Reg]$ folgt, dass $\forall t > 0$ jede Halbgruppe in $\eta_L(A^t)$ in $\mathbf{S}_P$ ist. Sei ϕ eine der Atomformeln $Q_a x$ oder $x < y$, dann ist, wie schon im Beweis von Satz 2.1 überlegt wurde, das zugehörige syntaktische Monoid das triviale Monoid $\{1\}$. Die Einschränkung von A^* auf A beziehungsweise A^t ergibt damit auch das triviale Monoid, das eine auflösbare Gruppe ist. Falls ϕ die Formel $x \equiv 0\ (m)$ ist, dann ist $\theta_\phi(A)$ einelementig, da $\epsilon \notin A$ und damit ist $\theta_\phi(A^t)$ auch das einelementige Monoid.

Wir betrachten nun $\psi \ \wedge \ \phi$, wobei ψ und ϕ in $(FO + MOD(P))[Reg]$ sind und jede Halbgruppe in $\eta_\phi(A^t)$ und $\eta_\psi(A^t)$ für alle $t < 0$ in $\mathbf{S}_P$ ist. Sei G eine Halbgruppe in $\theta_{\phi\wedge\psi}(A^t)$. Wie im Beweis von [1] Satz VI.4.1 gefolgert wird existiert für alle t ein p, sodass $\theta_{\phi\wedge\psi}(A^{pt}) = \theta_{\phi\wedge\psi}((A^{pt})^+)$ und damit insbesondere eine Unterhalbgruppe von $N(\phi \wedge \psi)$ ist. Dies beweist man leicht, indem man die Endlichkeit der betrachteten Monoide benutzt. Außerdem ist $G \leq \theta_{\phi\wedge\psi}(A^{pt})$. Nach [1] Satz V.6.1 ist $N(\phi \wedge \psi) \prec N(\phi) \times N(\psi)$, daher existiert ein surjektiver Homomorphismus $\beta : N(\phi) \times N(\psi) \to N(\phi \wedge \psi)$ mit $\theta_{\phi\wedge\psi} = \beta \circ (\theta_\phi, \theta_\psi)$. Schließlich erhalten wir, dass $G \leq \theta_{\phi\wedge\psi}(A^{pt}) = \beta \circ (\theta_\phi, \theta_\psi)(A^{pt}) = \beta(\theta_\phi(A^{pt}) \times \theta_\psi(A^{pt}))$. Also ist G eine Unteralgebra eines Teilers von $\theta_\phi(A^{pt}) \times \theta_\psi(A^{pt})$. Nach Induktionsvoraussetzung ist $\theta_\phi(A^{pt})$ und $\theta_\psi(A^{pt})$ in $\mathbf{S}_P$ und damit das kartesische Produkt und damit auch $G \in \mathbf{S}_P$. Nach [1] Satz V.6.1 ist $\theta_{\neg\phi} = \theta_\phi$ und mit der Induktionsvoraussetzung ist das Bild in $\mathbf{S}_P$. Sei nun $\phi = \exists^{(q,r)} x\psi$, $q \in P$ und $\forall t > 0$ ist jede Halbgruppe in $\eta_\psi(A^t)$ in $\mathbf{S}_P$. Nach Lemma 2.1 existiert ein $\zeta : A^* \to \mathbb{Z}_q \,\square\, M(\psi)$, sodass $\pi_{N(\psi)} \circ \zeta = \theta_\psi$ und es existiert ein Homomorphismus $v : \mathbb{Z}_q \,\square\, M(\psi) \to N(\phi)$, sodass $v \circ \zeta = \theta_\phi$. Sei nun G eine Halbgruppe in $\theta_\phi(A^t)$. Nach Satz (..)

existiert ein p, sodass $\zeta(A^{pt}) = \zeta((A^{pt})^+)$. Damit ist dann $\theta_\phi(A^{pt}) = v \circ \zeta(A^{pt}) = v \circ \zeta((A^{pt})^+) \leq N(\phi)$. Die erste Gleichheit heißt nichts anderes als $\theta_\phi(A^{pt}) \prec \zeta(A^{pt})$. Also ist $G \leq \theta_\phi(A^t) \leq \theta_\phi(A^{pt}) \prec \zeta(A^{pt})$. Schließlich ist noch $\zeta(A^{pt}) \leq \mathbb{Z}_q \,\square\, \pi_{M(\psi)}(\zeta(A^{pt}))$ und das ist genau $\mathbb{Z}_q \,\square\, \theta_\psi(A^{pt})$. Wenn man diese Ergebnisse nun zusammensetzt erhält man, dass G ein Teiler einer Unteralgebra von $\mathbb{Z}_q \,\square\, \theta_\psi(A^{pt})$ ist. Nun ist $\mathbb{Z}_q \in \mathbf{S}_P$, da $\mathbb{Z}_q$ eine auflösbare Gruppe ist und $\theta_\psi(A^{pt}) \in \mathbf{S}_P$ aufgrund der Induktionshypothese und der Tatsache, dass Pseudovarietäten abgeschlossen unter Erweiterungen sind. Aus dem Beweis von Satz 2.1 sieht man, dass Pseudovarietäten unter Blockprodukten abgeschlossen sind und damit ist auch $G \in \mathbf{S}_P$, was zu zeigen war.

$a) \Leftarrow b)$. Der Beweis für dies Implikation verläuft im wesentlichen analog zu dem Beweis von [1] Satz VI.4.1, wobei man Lemma 2.1 statt [1] Satz VI.4.1 benutzt um die modularen Quantoren einzubeziehen. Man muss nur noch bei der Relativierung aufpassen, die benutzt wird um einen Satz, der $L_w w$ definiert, aus einem Satz, der L_w definiert, zu erhalten. Dazu benutzen wir jenen Satz, der L_w definiert und schreiben alle numerischen Prädikate mithilfe von Formeln der Art $x < y$ und $x \equiv 0(m)$. Die Atomformeln bleiben unverändert unter der Relativierung, allerdings nur solange wir 'von links' relativieren. Das bedeutet wir transformieren ψ nur zu $\psi[\leq z]$.

□

4 Zusammenfassung

In dieser Arbeit wurden zwei Klassen von Sprachen, die sich durch verschiedene numerische Prädikate unterscheiden, klassifiziert. Es folgt ein Überblick über mehrere Klassen von Sprachen und deren Zusammenhang zu ihren zugehörigen syntaktischen Monoiden. Für eine genauere Beschreibung siehe [1] Kapitel VII.5.

	$+1$	$<$	Reg
FO	$M(L)$ ist aperiodisch, $esfs'es''f = es''fs'esf$ und $e = e^2, f = f^2$, $s, s's'' \in \eta_L(A^+)$	M(L) ist aperiodisch	$\eta_L(A^t)$ ist aperiodisch
$FO + MOD(P)$	$M(L)$ erfüllt $x^{k+kgV(P)} = x^k$, $esfs'es''f = es''fs'esf$ und $e = e^2, f = f^2$, $s, s', s'' \in \eta_L(A^+)$	$M(L) \in \mathbf{M}_P$	$\eta_L(A^t) \in \mathbf{S}_P$
$MOD(P)$	$M(L)$ erfüllt $x^{k+kgV(P)} = x^k$, $e \cdot M(L) \cdot e$ ist abelsche Gruppe für $e = e^2 \in \eta_L(A^+)$	$M(L) \in \mathbf{G}_P$	$\eta_L(A^t) \in \mathbf{S}_P$ und U_1 ist nicht in $\eta_L(A^+)$
SOM	L ist regulär	L ist regulär	L ist regulär

Damit erhalten wir zu jeder der angeführten Klassen eine geeignete Charakterisierung. Es reicht nun das syntaktische Monoid einer Sprache zu bestimmen und die obigen Bedingungen zu überprüfen, ob die Sprache in einer dieser Klassen enthalten ist. Dies ist wesentlich effizienter als Gegenbeispiele oder Beweise zu finden um eine Sprache zuzuordnen.

Literaturverzeichnis

[1] Howard Straubing, Finite Automata, Formal Logic and Curcuit Complexity, Springer Science+ Buisness Media, LLC; New York (1994)