Reguläre Sprachen und Schaltkreiskomplexität

Seminararbeit von Charlotte Jergitsch
unter der Aufsicht von
Associate Prof. Dipl.-Ing. Dr.techn. Stefan Hetzl

Februar 2020

Inhaltsverzeichnis

1 Einleitung

Diese Arbeit entstand im Rahmen eines Seminars, welches das Buch *Finite Automata, Formal Logic and Circuit Complexity* von Howard Straubing (siehe [Straubing]) behandelt. Im vorliegenden Text wird das Kapitel IX, *Regular Languages and Circuit Complexity*, dieses Buches ausgearbeitet. Darin werden die algebraischen und automatentheoretischen Themen des ersten Teils des Buches mit den Fragen aus der Schaltkreiskomplexität in Kapitel VIII, *Circuit Complexity*, verbunden.

Dementsprechend setzen wir als Vorkenntnisse für das Lesen dieser Arbeit Grundkenntnisse in Logik, Algebra und theoretischer Informatik voraus. Außerdem erwarten wir, dass der Inhalt der Kapitel I-VIII von Straubings Buch bekannt sind, insbesondere grundlegende Definitionen und Notationen. Nach Bedarf werden wir diese sowie Sätze aus den vorherigen Kapiteln im Text wiederholen. Einige Sprachen und Klassen solcher, wie sie in Kapitel VIII vorgestellt werden, wiederholen wir gleich hier in der Einleitung.

Definition 1.1. Wir bezeichnen mit AC^0 die Klasse der Sprachen, welche von Familien $\{C_n\}_{n\geq 1}$ von Schaltkreisen mit nur einem Outputgatter und folgenden Eigenschaften erkannt werden:

1. C_n hat n Inputgatter,
2. konstante Tiefe,
3. polynomiell beschränkte Größe.

Definition 1.2. Wir bezeichnen mit NC^1 die Klasse der Sprachen, welche von Familien $\{C_n\}_{n\geq 1}$ von Schaltkreisen mit nur einem Outputgatter und folgenden Eigenschaften erkannt werden:

1. C_n hat n Inputgatter,
2. Jedes UND- und $ODER$-Gatter hat fan-in 2,
3. Es gibt ein $k > 0$, so dass für alle n die Tiefe von C_n kleiner als $k \cdot \log_2 n$ ist,
4. polynomiell beschränkte Größe.

Definition 1.3. Seien $L, L' \in \{0,1\}^*$. Wir bezeichnen L als **AC^0-reduzibel** zu L' und schreiben $L \leq_{AC^0} L'$, wenn L von einer Familie von Schaltkreisen $\{C_n\}_{n\geq 1}$ mit folgenden Eigenschaften erkannt werden:

1. konstante Tiefe,
2. polynomiell beschränkte Größe,
3. bestehend aus $NICHT$-Gattern, sowie $ODER$-, UND- und L'-Gattern von unbeschränktem fan-in.

Wir bezeichnen L als **stark reduzibel** zu L' und schreiben $L \leq_{strong} L'$, wenn L von einer Familie von Schaltkreisen $\{C_n\}_{n\geq 1}$ mit folgenden Eigenschaften erkannt werden:

1. konstante Tiefe,
2. polynomiell beschränkte Größe,
3. bestehend aus $NICHT$-Gattern, sowie $ODER$- und UND-Gatter mit fan-in 2, sowie L'-Gattern.

Definition 1.4. Wir definieren folgende Sprache:

$$MOD_q := \{a_1 \cdots a_n : \sum_{i=1}^{n} a_i \equiv 0 \pmod{q}\},$$

Wir definieren folgende Klassen von Sprachen:

$$ACC(q) := \{L \subseteq \{0,1\}^* : L \leq_{AC^0} MOD_q\},$$
$$CC(q) := \{L \subseteq \{0,1\}^* : L \leq_{strong} MOD_q\}.$$

2 Formeln mit beliebigen numerischen Prädikaten

In den Kapiteln VI und VII wurden die regulären Sprachen, welche durch Sätze aus regulären numerischen Prädikaten und Quantoren erster Stufe verschiedener Art beschrieben werden können, untersucht. Das Resultat dieser Kapitel ist, dass diese Sprachen durch ihre syntaktischen Monoide und Morphismen charakterisiert werden können. In diesem Abschnitt wird ergründet, welche Sprachen wir durch logische Sätze beschreiben können, wenn wir nicht nur reguläre, sondern beliebige numerische Prädikate zulassen. Es zeigt sich, dass wir die so definierten Sprachen durch die Art der Schaltkreisfamilien charakterisieren können, welche die Sprachen erkennen. Somit wird ein Zusammenhang zwischen Schaltkreiskomplexität und Logik hergestellt, so wie im ersten Teil des Buches eine Verbindung zwischen Automatentheorie und Logik gezeigt wurde.

Sei nun $\mathcal{Q}$ eine beliebige Klasse von Quantoren. Dann bezeichnen wir mit $\mathcal{Q}[\mathcal{N}]$ die Familie von Sprachen in A^*, welche durch geschlossene Formeln mit Quantoren aus $\mathcal{Q}$ definiert werden, wobei die numerischen Prädikate keiner Beschränkung unterliegen. Dann gilt folgender Zusammenhang zwischen logischen Formeln und Schaltkreisen:

Satz 2.1. *Sei $A = \{0,1\}$ und $q > 1$. Dann gilt:*

$$FO[\mathcal{N}] = AC^0,$$
$$MOD(q)[\mathcal{N}] = CC(q),$$

und

$$(FO + MOD(q))[\mathcal{N}] = ACC(q).$$

Beweis. Wir zeigen zuerst die Inklusion von links nach rechts:
Sei nun $L \in \mathrm{FO}[\mathcal{N}]$. Wir wollen den Satz, der L beschreibt, für jedes $n > 0$ in einen Schaltkreis $C_n \in AC^0$ umwandeln. Wir beginnen mit den äußersten Quantoren und ersetzen:

$$\exists x\phi(x) \text{ durch } \bigvee_{i=1}^{n} \phi(i),$$
$$\forall x\phi(x) \text{ durch } \bigwedge_{i=1}^{n} \phi(i),$$
$$\text{und } \exists^{(q,r)} x\phi(x) \text{ durch } |\{i \in \{1,\ldots,n\} : \phi(i)\}| \equiv r \pmod{q}.$$

Den letzten Ausdruck können wir mit Hilfe eines MOD_q-Gatters evaluieren, indem wir $q - r$ zusätzliche Leitungen mit konstantem Wert 1 hinzufügen. Somit gibt das Gatter genau dann 1 aus, wenn zusätzlich r verschiedene $\phi(i)$ gleich 1 sind.
Schließlich erhalten wir Atomformeln der Form $Q_0 i$, $Q_1 i$ oder $R(i_1, \ldots, i_n)$. Wir erinnern daran, dass für einen Buchstaben $a \in \{0, 1\}$ der Ausdruck $Q_a i$ von einem Wort genau dann erfüllt wird, wenn an seiner i-ter Stelle der Buchstabe a steht. Der Ausdruck R ist ein numerisches Prädikatensymbol. Die Formel $Q_1 i$ ersetzen wir durch ein Inputgatter der Form x_i, und $Q_0 i$ durch $\neg x_i$. Die Formel $R(i_1, \ldots, i_k)$ wird durch die Bool'sche Konstante 1 oder 0 ersetzt, je nach dem, ob die durch R definierte Relation auf $\{1, \ldots, n\}^k$ an der Stelle $(i_1, \ldots, i_k)$ gültig ist. Wir erhalten also einen Schaltkreis mit Gattern der jeweils gewünschten Art. Die Tiefe d des Schaltkreises ist von der Länge n des Inputs unabhängig, da sie alleine vom Grad der Verschachtelung der Quantoren im ursprünglichen Satz abhängt. Die Größe des Schaltkreises ist in Abhängigkeit von seiner Tiefe und der Länge des Inputs gleich $O(n^d)$. Das heißt, der Schaltkreis hat konstante Tiefe und polynomielle Größe, sodass abhängig von der Art der Quantoren im ursprünglichen Satz $L \in AC^0, ACC(q)$, oder $CC(q)$ folgt.

Nun beweisen wir die Inklusion von rechts nach links: Dabei zeigen wir die Inklusionen aller drei Teile des Satzes gleichzeitig. Sei $L \in AC^0, CC(q)$ oder in $ACC(q)$. Folglich wird L von einer Schaltkreisfamilie $\{C_n\}_{n \geq 0}$ mit polynomiell beschränkter Größe, konstanter Tiefe und entsprechenden weiteren Eigenschaften erkannt. Wir werden eine geschlossene Formel mit den vorgesehenen Quantoren konstruieren, die L bis auf Strings der Länge < 2 beschreibt. Die Formel kann aber leicht auf solche Strings ausgeweitet werden.

Zuerst bringen wir die Schaltkreise C_n in eine Normalform, so dass jeder Pfad von einem Inputgatter zum Outputgatter dieselbe Länge hat. Das erreichen wir dadurch, dass wir als erstes die C_n in Bäume umwandeln, indem wir die Gatter replizieren, von denen mehr als eine Ausgabeleitung wegführt. Da die C_n konstante Tiefe haben, bleibt durch diesen Vorgang ihre Größe polynomiell beschränkt. Als nächsten Schritt erweitern wir Pfade, die eine kürzere Pfadlänge als der maximale Pfad von einem Inputgatter zum Outputgatter haben, auf diese maximale Länge. Hierfür führen wir $ODER$-Gatter mit nur einem Input ein, bis die Pfade die maximale Länge erreicht haben. Auch nach diesem Schritt haben die Schaltkreise C_n noch polynomiell beschränkte Größe. Es gibt daher ein $k > 0$, sodass die Anzahl der Gatter in C_n für $n \geq 2$ durch n^k nach oben beschränkt ist. Wir können daher jedes Gatter durch ein k-Tupel in $\{1, \ldots, n\}^k$ kodieren.

Wir erinnern uns daran, dass eine m-äre numerische Relation jeder Zahl $n \geq 0$ eine m-äre Relation auf $\{1, \ldots, n\}$ zuordnet, also die Menge an m-Tupeln in $\{1, \ldots, n\}^m$, für welche die Relation gilt. Definieren wir nun unter Verwendung der eben eingeführten Kodierung der Gatter die Interpretationen der numerischen Prädikate in unserer Formel.

$$INPUT1(r, r_1, \ldots, r_k)$$

mit $r, r_i \in \{1, \ldots, n\}$ ist genau dann erfüllt, wenn das Tupel $(r_1, \ldots, r_k)$ ein Inputgatter in C_n mit dem Label x_r kodiert.

$$INPUT0(r, r_1, \ldots, r_k)$$

gilt in analoger Weise genau dann, wenn $(r_1, \ldots, r_k)$ ein Inputgatter in C_n mit dem Label $\neg x_r$ kodiert.

$$OUTPUT(r_1, \ldots, r_k)$$

gilt genau dann, wenn $(r_1, \ldots, r_k)$ das Outputgatter von C_n kodiert.

$$A(r_1, \ldots, r_k)$$

gilt genau dann, wenn $(r_1, \ldots, r_k)$ ein UND-Gatter in C_n kodiert. Analog werden auch die numerischen Relationen O und M_q für $ODER$- und MOD_q-Gatter definiert. Außerdem gilt

$$PRED(r_1, \ldots, r_k, s_1, \ldots, s_k)$$

genau dann, wenn das Gatter mit dem Code $(r_1, \ldots, r_k)$ ein Vorgänger vom Gatter $(s_1, \ldots, s_k)$ in C_n ist.
Für Schaltkreisfamilien in $CC(q)$ gilt im Gegensatz zu Familien in AC^0 oder $ACC(q)$, dass sie keine UND- und $ODER$-Gatter von beliebigem fan-in haben. Sie besitzen nur UND- und $ODER$-Gatter von fan-in 2, sowie $NICHT$- und $ODER$-Gatter von fan-in 1, wobei letztere von der Umwandlung von C_n in die Normalform stammen. Daher führen wir für den Fall $L \in CC(q)$ noch folgende Relationen ein:

$$\begin{aligned} &A2(r_1, \ldots, r_k, s_1, \ldots, s_k, t_1, \ldots, t_k), \\ &O2(r_1, \ldots, r_k, s_1, \ldots, s_k, t_1, \ldots, t_k), \\ &O1(r_1, \ldots, r_k, s_1, \ldots, s_k), \\ \text{und } &N(r_1, \ldots, r_k, s_1, \ldots, s_k). \end{aligned}$$

Die erste dieser Relationen ist genau dann gültig, wenn $(r_1, \ldots, r_k)$ in C_n ein UND-Gatter von fan-in 2 kodiert, dessen Vorgänger durch $(s_1, \ldots, s_k)$ und $(t_1, \ldots, t_k)$ angegeben werden, wobei wir hier implizit eine Ordnung auf den Vorgängern annehmen. Die anderen drei Relationen werden in analoger Weise für $ODER$-Gatter von fan-in 2, $ODER$-Gatter von fan-in 1 und $NICHT$-Gatter von fan-in 1 definiert.

Sei nun g ein Gatter von C_n mit Kodierung $(r_1, \ldots, r_k)$, sodass jeder Pfad von einem Inputgatter zu g die Länge d hat. So ein g existiert aufgrund der Normalform von C_n. Es sei $C_{n,g}$ der Teilschaltkreis, welcher aus allen Gattern besteht, von denen ein Pfad zu g führt. Sei weiters w eine $\{y_1, \ldots, y_k\}$-Struktur der Länge n mit der Eigenschaft, dass y_i im r_i-ten Buchstaben von w vorkommt. Wir zeigen nun durch Induktion, dass für jedes $d \geq 0$ eine Formel $\psi_d(y_1, \ldots, y_k)$ existiert, welche folgende Eigenschaft hat:

$$w \models \psi_d(y_1, \ldots, y_k)$$

genau dann, wenn $C_{n,g}$ das Wort $\bar{w} \in \{0,1\}^n$ akzeptiert, welches entsteht, wenn man die Variablen y_i von w entfernt.

Für den Induktionsanfang $d = 0$ besteht der Teilschaltkreis $C_{n,g}$ nur aus einem einzigen Inputgatter,

nämlich x_r oder $\neg x_r$. In diesem Fall können wir für $L \in AC^0$ oder $ACC(q)$ die Formel ψ_0 als

$$\exists z \bigvee_{i=0}^{1} (INPUTi(z, y_1, \ldots, y_k) \wedge Q_i z)$$

definieren. Für $L \in CC(q)$ setzen wir ψ_0 gleich

$$\exists^{(q,1)} z \bigvee_{i=0}^{1} (INPUTi(z, y_1, \ldots, y_k) \wedge Q_i z).$$

Diese Formel erfüllt die Anforderungen, denn falls es ein $r \geq 0$ gibt, sodass ein Inputgatter mit Label x_r oder $\neg x_r$ durch $(r_1, \ldots, r_k)$ kodiert ist, dann gibt es genau ein solches.

Nun folgt der Induktionsschritt: Sei $d > 0$. Für den Fall $L \in ACC(q)$ definieren wir die Formel ψ_d als

$$\begin{aligned}
&[A(y_1, \ldots, y_k) \wedge \forall z_1 \cdots \forall z_k (PRED(z_1, \ldots, z_k, y_1, \ldots, y_k) \rightarrow \psi_{d-1}(z_1, \ldots, z_k))] \\
&\vee [O(y_1, \ldots, y_k) \wedge \exists z_1 \cdots \exists z_k (PRED(z_1, \ldots, z_k, y_1, \ldots, y_k) \wedge \psi_{d-1}(z_1, \ldots, z_k))] \\
&\vee [M_q(y_1, \ldots, y_k) \wedge \exists^{(q,0)} (z_1, \ldots, z_k)(PRED(z_1, \ldots, z_k, y_1, \ldots, y_k) \wedge \psi_{d-1}(z_1, \ldots, z_k))].
\end{aligned}$$

Hier bedeutet der Ausdruck

$$\exists^{(q,0)} (z_1, \ldots, z_k)\phi,$$

dass „0 mod q k-Tupel an Positionen $(z_1, \ldots, z_k)$ existieren, für die ϕ gilt “. Dieser Ausdruck ist äquivalent zur folgenden Formel und somit in $MOD(q)[\mathcal{N}]$ induktiv definiert:

$$\bigvee_{f \in F} \bigwedge_{j=0}^{q-1} \exists^{(q,j)} (z_1, \ldots, z_{k-1}) \exists^{(q,f(j))} z_k \phi,$$

wobei $F = \{f : \mathbb{Z}_q \rightarrow \mathbb{Z}_q \ : \ \sum_{j=0}^{q-1} j \cdot f(j) = 0\}$. Daher können wir nach endlich vielen Iterationen den ursprünglichen Ausdruck durch die üblichen modularen Quantoren ausdrücken. Wir erklären kurz diese Äquivalenz: Ist die Formel $\exists^{(q,j)} (z_1, \ldots, z_{k-1}) \exists^{(q,f(j))} z_k \phi$ erfüllt, dann gibt es $j \mod q$ $(k-1)$-Tupel an Positionen $(z_1, \ldots, z_{k-1})$, für die wiederum $f(j) \mod q$ Positionen z_k existieren, so dass ϕ gilt - ϕ gilt also für $j \cdot f(j)$ k-Tupel an Positionen. Gilt dies für alle $j \in \{0, \ldots, q-1\}$, so ist ϕ für insgesamt $\sum_{j=0}^{q-1} j \cdot f(j)$ k-Tupel an Positionen erfüllt. Somit folgt die Äquivalenz aus der Eigenschaft $\sum_{j=0}^{q-1} j \cdot f(j) = 0$ von f.

Für den Fall $L \in AC^0$ lassen wir einfach den letzten Teil der Formel ψ_d weg, welcher modulare Quantoren enthält. Analog lassen wir für $L \in CC(q)$ die ersten beiden Teile weg und fügen stattdessen Formeln für die Bool'schen Gates mit beschränktem fan-in 1 oder 2 ein. Die Formel für ein UND-Gatter mit fan-in 2 würde zum Beispiel folgendermaßen aussehen:

$$\exists^{(q,1)} (z_1, \ldots, z_{2k})(A2(z_1, \ldots, z_{2k}, y_1, \ldots, y_k) \wedge \psi_{d-1}(z_1, \ldots, z_k) \wedge \psi_{d-1}(z_{k+1}, \ldots, z_{2k})).$$

Die anderen Formeln können wir analog definieren.

Nun können wir die Formeln ψ_d verwenden, um die Sprache L zu definieren. Sei D die Tiefe von C_n.

Dann ist $L \in ACC(q)$ oder AC^0 definiert durch die Formel

$$\forall y_1 \cdots \forall y_k (OUTPUT(y_1, \ldots, y_k) \rightarrow \psi_D(y_1, \ldots, y_k)).$$

Die Sprache $L \in CC(q)$ wird definiert durch

$$\exists^{(q,1)}(y_1, \ldots, y_k)(OUTPUT(y_1, \ldots, y_k) \wedge \psi_D(y_1, \ldots, y_k)).$$

Somit gilt $L \in FO[\mathcal{N}], MOD(q)[\mathcal{N}]$ bzw. $(FO + MOD(q))[\mathcal{N}]$.

□

3 Reguläre Sprachen und nichtreguläre numerische Prädikate

Im Abschnitt III.2 in [Straubing] werden numerische Prädikate, welche mit Relationen assoziiert werden, die durch endliche Automaten beschrieben werden können, als *reguläre Prädikate* bezeichnet. Es kann allerdings auch vorkommen, dass ein Satz, der nichtreguläre Prädikate enthält, dennoch eine reguläre Sprache beschreibt. Betrachten wir zum Beispiel

$$\forall x \exists y (y|x \wedge Q_a y),$$

wobei $y|x$ wie üblich „y teilt x“ bedeutet. Dieses ist zwar kein reguläres Prädikat, der Satz beschreibt dennoch die reguläre Sprache aA^*: Die Formel $\exists y(y|x \wedge Q_a y)$ muss auch für die erste Position erfüllt sein, und somit muss a an der ersten Position vorkommen. Diese Sprache könnten wir allerdings auch durch reguläre Prädikate definieren:

$$\forall x \exists y (y \leq x \wedge Q_a y).$$

Dies scheint ein allgemeines Phänomen zu sein und führt uns zu der zentralen Vermutung dieses Texts:

Vermutung 3.1. *Sei $\mathcal{Q}$ eine beliebige Klasse von Quantoren aus der Menge*

$$\{\exists\} \cup \{\exists^{(q,r)} : 0 \leq r \leq q\}.$$

Dann gilt

$$\mathcal{Q}[\mathcal{N}] \cap Reg(A) = \mathcal{Q}[Reg].$$

Diese Vermutung besagt, dass wir nur numerische Prädikate benötigen, welche selbst von einem endlichen Automaten erkannt werden, um eine reguläre Sprache durch eine geschlossene Formel zu beschreiben. Wir werden später noch ausführen, dass diese Vermutung zu einigen anderen Behauptungen in der Schaltkreistheorie äquivalent ist (siehe Satz 3.6). Somit würde ihr Beweis auch diese Probleme lösen. Grundsätzlich folgt aus dem Beweis dieser Vermutung, dass die Komplexitätstheorie von Schaltkreisen mit kleiner Tiefe eine Verallgemeinerung im Unendlichen der algebraisch-logischen Theorie endlicher Automaten ist, welche in den Kapiteln V-VII ausgearbeitet wurde. Dieser Übergang zum unendlichen Fall erhält einen großen Teil der Struktur der endlichen Theorie.

Sei $FO[Reg]$ die Familie der Sprachen in A^*, welche durch Sätze mit Quantoren erster Stufe mit regulären numerischen Prädikaten beschrieben werden. Es sei weiters $Reg(A)$ die Familie der regulären

Sprachen in A^*. Wir beweisen nun einen Spezialfall der zentralen Vermutung 3.1 für $\mathcal{Q} = FO$:

Satz 3.2. $FO[\mathcal{N}] \cap Reg(A) = FO[Reg]$.

Für den Beweis dieses Satzes wollen wir uns noch die Aussage von Satz VIII.2.3 in Erinnerung rufen:

Lemma 3.3. *Sei p eine Primzahl und $q > 1$ eine Zahl, welche einen Primfaktor ungleich p hat. Dann gilt $MOD_q \notin ACC(p^k)$ für alle $k > 0$.*

Beweis von Satz 3.2. Die Inklusion von rechts nach links ist trivial. Die andere Richtung beweisen wir, indem wir einige der bisherigen Resultate über Schaltkreise verwenden. Diese können allerdings nur Eingaben in binärer Schreibweise annehmen.

Zuerst übersetzen wir daher die Buchstaben aus unserem beliebigen endlichen Alphabet A in Binärschreibweise. Dafür kodieren wir jeden Buchstaben $a \in A$ durch einen String $\alpha(a)$, der die Länge $m := \lceil \log_2 |A| \rceil$ hat. Diese Kodierung liefert uns einen injektiven Homomorphismus $\alpha : A^* \to \{0,1\}^*$. Folglich ist für jede reguläre Sprache L auch ihr Bild $\alpha(L)$ regulär. Ebenso kann eine geschlossene Formel aus $FO[\mathcal{N}]$, die L definiert, leicht in eine geschlossene Formel übersetzt werden, die $\alpha(L)$ beschreibt. Somit gilt für die kodierte Sprache $\alpha(L)$, dass aus $L \in FO[\mathcal{N}] \cap Reg(A)$ auch $\alpha(L) \in FO[\mathcal{N}] \cap Reg(\{0,1\})$ folgt. Da die Sprache $\alpha(L)$ aus dem Alphabet $\{0,1\}$ konstruiert ist, können wir Satz 2.1 darauf anwenden. Aus $\alpha(L) \in FO[\mathcal{N}]$ schließen wir daher, dass $\alpha(L)$ in AC^0 liegt.

Wir wollen nun zeigen, dass für eine Sprache $L \in FO[\mathcal{N}] \cap Reg(A)$ gilt, dass $L \in FO[Reg]$ ist. Dafür verwenden wir Satz VI.4.1. Dieses besagt, dass eine reguläre Sprache K genau dann in $FO[Reg]$ liegt, wenn ihr syntaktischer Morphismus η_K quasi-aperiodisch ist. Wir müssen daher zeigen, dass $\eta_L(A^r)$ für alle $r > 0$ nur triviale Gruppen enthält. Angenommen es existiert ein $r > 0$, sodass $\eta_L(A^r)$ eine nichttriviale Gruppe enthält. Diese enthält ein Element $g \neq 1$ und somit die nichttriviale zyklische Gruppe $\langle g \rangle =: G$ der Größe $q > 0$. Wir werden zeigen, dass die Existenz einer solchen Gruppe in $\eta_L(A^r)$ impliziert, dass $MOD_q \leq_{strong} \alpha(L)$ gilt. Allerdings folgt dann aus den obigen Ausführungen, dass $\alpha(L) \in AC^0$ und somit $MOD_q \in AC^0$. Somit ist auch $MOD_q \leq_{AC^0} MOD_{p^k}$ für p prim und $q \neq p^n$ für ein $n \in \mathbb{N}$ und daher $MOD_q \in ACC(p^k)$. Dies widerspricht jedoch Lemma 3.3, nach welchem $MOD_q \notin ACC(p^k)$, wenn q keine Potenz von p ist.

Wir betrachten den syntaktischen Morphismus η_L: Nach dessen Definition kennen wir für ein Wort $w \in A^*$ den Wert von $\eta_L(w)$ genau dann, wenn wir für alle Paare (u, v) von Worten in A^* wissen, ob uwv in L liegt. Die Sprache $u^{-1}Lv^{-1} = \{z \in A^* : uzv \in L\}$ wird durch eine Abwandlung des minimalen Automaten von L erkannt, bei der wir den Anfangszustand i durch $i \cdot u$ ersetzen, und die Menge F der Endzustände durch $\{q : q \cdot v \in F\}$. Die Sprache L ist regulär, somit ist der minimale Automat von L endlich. Das heißt, es gibt nur endlich viele Sprachen der Form $u^{-1}Lv^{-1}$ mit $u, v \in A^*$. Folglich können wir t Wortpaare $(u_1, v_1), \ldots, (u_t, v_t)$ auswählen, sodass der Wert von $\eta_L(w)$ durch die Antworten auf die t Fragen

$$u_i w v_i \in L?$$

für $i \in \{1, \ldots, t\}$ festgelegt wird.

Seien nun $w_0, w_1 \in A^r$, sodass $\eta_L(w_0) = 1_G$ und $\eta_L(w_1)$ ein erzeugendes Element von G ist. Wir konstruieren nun einen Schaltkreis, der bei Eingabe $b_1 \cdots b_n \in \{0,1\}^n$ die Repräsentation von $\alpha(w_{b_1}) \ldots \alpha(w_{b_n})$ ausgibt. Diese hat Länge nmr, wobei der Faktor n von der Größe der Eingabe, m von der Kodierung α, und r von der Länge der w_{b_i} kommt. Dieser Repräsentant wird mit den Elementen $\alpha(u_i)$ und $\alpha(v_i)$ verknüpft, sodass wir für $i = 1, \ldots, t$ Strings der Form $\alpha(u_i)\alpha(w_{b_1}) \cdots \alpha(w_{b_n})\alpha(v_i)$ der Länge $m(|u_i| + |v_i| + rn)$ erhalten. Diese t Elemente werden jeweils in ein $\alpha(L)$-Gatter eingespeist, sodass wir einen Vektor $s \in \{0,1\}^t$ mit folgender Eigenschaft erhalten: Für diesen gilt $s_i = 1$ genau dann, wenn $u_i w_{b_1} \cdots w_{b_n} v_i \in L$ - er gibt also die eindeutige Kodierung des Werts von $\eta_L(w_{b_1} \cdots w_{b_n})$ aus. Wir speisen die t Komponenten des Vektors s in einen Bool'schen Schaltkreis konstanter Größe, der genau dann 1 ausgibt, wenn $\eta_L(w_{b_1} \cdots w_{b_n})$ gleich der Identität von G ist. Die Gruppe G hat genau q Elemente, somit folgt $MOD_q \leq_{strong} \alpha(L)$ und wir erhalten den erwünschten Widerspruch. □

Dieses Argument kann auch auf Formeln mit modularen Quantoren ausgeweitet werden, solange wir den Modul auf Primpotenzen beschränken.

Satz 3.4. *Sei p prim und $k > 0$. Dann gilt*

$$(FO + MOD(p^k))[\mathcal{N}] \cap Reg(A) = (FO + MOD(p^k))[Reg],$$

und

$$MOD(p^k)[\mathcal{N}] \cap Reg(A) = MOD(p^k)[Reg].$$

Für den Beweis dieses Satzes verwenden wir folgendes Lemma, welches sich in [Straubing] als Satz IX.1.5 mitsamt Beweis auf S. 159f. befindet:

Lemma 3.5. *Sei K eine reguläre Sprache, sodass ihr syntaktisches Monoid $M(K)$ nicht auflösbar ist. Dann gilt für alle Sprachen $L \in NC^1$, dass $L \leq_{strong} K$.*

Nun beweisen wir den ersten Teil von Satz 3.4. Für den zweiten Teil, der auf ähnliche Art bewiesen wird, verweisen wir auf [Straubing] S. 168.

Beweis von Satz 3.4, 1. Teil. Die Inklusion von rechts nach links ist wieder trivial. Für die andere Richtung betrachten wir eine Sprache

$$L \in (FO + MOD(q))[\mathcal{N}] \cap Reg(A),$$

wobei $q = p^k$ eine Primpotenz sei. Wir verwenden wie im Beweis von Satz 3.2 eine Kodierung $\alpha : A^* \to \{0,1\}^*$ und folgern analog, dass

$$\alpha(L) \in (FO + MOD(q))[\mathcal{N}] \cap Reg(\{0,1\})$$

liegt.
Nach Satz 2.1 folgt daraus $\alpha(L) \in ACC(q)$. Wir verwenden nun Satz VII.4.1, welcher besagt, dass eine reguläre Sprache L dann in $(FO + MOD(p^k))[Reg]$ liegt, wenn für alle $r > 0$ alle Gruppen in $\eta_L(A^r)$ auflösbar sind und als Ordnung eine Potenz von p hat.
Ist $M(L)$ auflösbar, so auch all seine Untergruppen, und somit auch alle Gruppen in $\eta_L(A^r)$. Angenommen $M(L)$ ist nicht auflösbar. Aus Lemma 3.5 folgt, dass für alle Sprachen $K \in NC^1$, $K \leq_{strong} \alpha(L)$ gilt.

Daraus folgt, dass $NC^1 \subseteq ACC(q)$ und folglich $NC^1 = ACC(q)$ ist, was Lemma 3.3 widerspricht. Folglich sind für alle $r > 0$ alle Gruppen in $\eta_L(A^r)$ auflösbar.
Nehmen wir an, dass es ein $r > 0$ gibt, sodass $\eta_L(A^r)$ eine Gruppe enthält, deren Ordnung t nicht eine Potenz von p ist. Durch ein Argument ähnlich dem im Beweis von Satz 3.2 können wir dann zeigen, dass $MOD_t \leq \alpha(L)$ ist. Daraus folgern wir, dass $MOD_t \in ACC(q)$ liegt, was wiederum Lemma 3.3 widerspricht. □

Ob die Aussagen aus Satz 3.4 auch gelten, wenn wir einen beliebigen Modul zulassen, ist noch ungelöst. Diese offene Frage ist äquivalent zu den Vermutungen über $CC(q)$ und $ACC(q)$ in Kapitel VIII:

Satz 3.6. *Sei $q > 0$.*

1. *Folgende Aussagen sind äquivalent:*
   (a) ***Vermutung VIII.***2.6***:*** *Seien $p, q > 1$. Wenn q einen Primfaktor hat, der p nicht teilt, dann gilt $MOD_q \notin ACC(p)$.*
   (b) $(FO + MOD(q))[\mathcal{N}] \cap Reg(A) = (FO + MOD(q))[Reg]$
2. *Folgende Aussagen sind äquivalent:*
   (a) ***Vermutung VIII.***2.6 ***und Vermutung VIII.***2.11***:*** $1^* \notin CC$.
   (b) $MOD(q)[\mathcal{N}] \cap Reg(A) = MOD(q)[Reg]$

4 Weitere Spezialfälle der zentralen Vermutung

Die Hauptvermutung 3.1 wurde schon in einer Vielzahl an Spezialfällen bewiesen, wobei in der Beweismethode auf komplexitätstheoretische untere Schranken zurückgegriffen wurde, wie wir es im Satz 3.2 im vorhergehenden Abschnitt gesehen haben. Das wirft die Frage auf, ob diese Vermutung nicht über einen direkteren Weg bewiesen werden kann, der die Eigenschaften endlicher Automaten anstatt asymptotische untere Schranken für Schaltkreise verwendet. Tatsächlich ist es in einigen Spezialfällen der Vermutung gelungen, diese durch kombinatorisch-algebraische Methoden zu beweisen. Bei diesen Fällen ist entweder die Struktur der Quantoren oder die der numerischen Prädikate besonders einfach.

Ein solcher Spezialfall ist der jener Sprachen in A^*, welche durch geschlossene Formeln in $\Sigma_1[\mathcal{C}]$ beschrieben werden, wobei $\mathcal{C}$ eine beliebige Klasse numerischer Prädikate sei. Wir erinnern an dieser Stelle an die Definition von Σ_k-Formeln: eine Formel ϕ in Prädikatenlogik erster Stufe ist eine Σ_k-Formel, wenn in ihrer Präfixform zu Beginn k maximale homogene Blöcke von Quantoren stehen, und der Block links außen aus Existenzquantoren besteht.

Satz 4.1. $\Sigma_1[\mathcal{N}] \cap Reg(A) = \Sigma_1[Reg]$.

Für den Beweis dieses Satzes verweisen wir auf [Straubing] S. 170ff. Dieser Satz scheint nicht direkt aus Satz 3.2 oder der Hauptvermutung 3.1 zu folgen, da diese keine Aussage darüber treffen, wie sich die Komplexität der Quantoren verändert, wenn wir von beliebigen zu regulären numerischen Prädikaten übergehen. H. Straubing vermutet, dass für geschlossene Formeln erster Stufe die Komplexität bei diesem Übergang immer erhalten bleibt und stellt folgende Behauptung auf:

Vermutung 4.2. $\Sigma_k[\mathcal{N}] \cap Reg(A) = \Sigma_k[Reg]$ *für alle* $k > 0$.

Ein weiterer Spezialfall der zentralen Vermutung 3.1 kann bewiesen werden, indem man die zugelassenen numerischen Prädikate einschränkt. Sei $\mathcal{M}$ die Klasse der numerischen Prädikate, welche aus der Ordnung $<$ und beliebigen *monadischen* (also unären) Prädikaten besteht. Wir bezeichnen mit $FO[\mathcal{M}]$ die Klasse jener Sprachen, welche durch geschlossene Formeln erster Stufe mit numerischen Prädikaten aus $\mathcal{M}$ beschrieben werden. Analog definieren wir $(FO + MOD(q))[\mathcal{M}]$ und $MOD(q)[\mathcal{M}]$.

Satz 4.3. *Sei* $q > 0$. *Dann gilt Folgendes:*

1. $(FO + MOD(q))[\mathcal{M}] \cap Reg(A) = (FO + MOD(q))[Reg]$.
2. $MOD(q)[\mathcal{M}] \cap Reg(A) \subseteq MOD(q)[Reg]$.

Das bedeutet, dass die regulären Sprachen in $(FO+MOD(q))[\mathcal{M}]$ und $MOD(q)[\mathcal{M}]$ unter ausschließlicher Verwendung von regulären numerischen Prädikaten definiert werden können. Der Beweis erfordert einige zusätzliche algebraische Resultate und kann in [Straubing] S. 172-176 nachgelesen werden.

Literatur

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