Seminararbeit

zum Thema

Schaltkreiskomplexität

basierend auf dem Buch „Finite Automata, Formal Logic, and Circuit Complexity“ von Howard Straubing

Wintersemester 2019

Alexandra Bergmayr

Matrikelnummer: 1225525

Betreuung: Assoc. Prof. Dipl.-Ing. Dr.techn. Stefan Hetzl

Technische Universität Wien

Institut für Diskrete Mathematik und Geometrie

Inhaltsverzeichnis

1 Einführung **2**

2 Definition von Schaltkreisen **2**

3 Klassen von Schaltkreisen, Sprachen und Funktionen **5**

4 Hauptresultat **7**

Literatur **14**

1 Einführung

Die vorliegende Arbeit behandelt Kapitel VIII, „Circuit Complexity“, des Buches [1] „Finite Automata, Formal Logic, and Circuit Complexity“ von Howard Straubing, das eine Einführung in die Komplexität von Schaltkreisen darstellt und wichtige Ergebnisse aus diesem Bereich vorstellt und beweist. Insbesondere liegt im Folgenden der Schwerpunkt auf dem Beweis einer Erkenntnis über die Komplexität der Berechnung der Modulo-Funktion.

2 Definition von Schaltkreisen

Definition 2.1. Ein sogenannter ***Schaltkreis*** mit n Inputs ist definiert als ein gerichteter azyklischer Graph mit $2n$ Quellknoten. Die Quellknoten werden mit $x_1, \neg x_1, \ldots, x_n, \neg x_n$ bezeichnet.
Jeder Knoten, der kein Quellknoten ist, wird als eine Funktion

$$f : \{0,1\}^r \to \{0,1\}$$

dargestellt, wobei r die Anzahl an Kanten ist, die in den Knoten eingehen.
Ist f keine symmetrische Funktion, so wird zusätzlich eine Ordnung auf den eingehenden Kanten festgelegt.
Die ***Größe*** des Schaltkreises ist die Anzahl der Kanten. Die ***Tiefe*** des Schaltkreises ist die Länge des längsten Pfades, welche als die Anzahl jener Gatter entlang des Pfades, die weder Input- noch Outputgatter sind, definiert ist.

Darüber hinaus werden im Zusammenhang mit Schaltkreisen einige Begriffe der Graphentheorie durch fachspezifische Begriffe ersetzt.

Definition 2.2. Knoten werden ***Gatter*** genannt, wobei Senkknoten als ***Outputgatter*** und Quellknoten als ***Inputgatter*** bezeichnet werden.
Die Anzahl der Kanten, die in ein Gatter eingehen, heißt ***fan-in***, die Anzahl der Kanten, die ein Gatter verlassen, heißt ***fan-out***. Eine Kante wird ***Leitung*** genannt.

Jedes Gatter wird mit der Berechnung, die es durchführt, assoziiert.

Definition 2.3. Mit jedem Gatter g eines Schaltkreises $\mathcal{C}$ mit n Inputgattern wird eine Funktion $F_g : \{0,1\}^n \to \{0,1\}$ assoziiert, die wie folgt durch Induktion auf der Länge

des längsten Pfades von einem Inputgatter zu g definiert wird:

$$F_g(a_1,\ldots,a_n) := \begin{cases} a_i, & \text{falls } g \text{ ein mit } x_i \text{ bezeichnetes Inputgatter ist,} \\ 1-a_i, & \text{falls } g \text{ ein mit } \neg x_i \text{ bezeichnetes Inputgatter ist,} \\ f_g(F_{g_1}(a_1,\ldots,a_n),\ldots,F_{g_r}(a_1,\ldots,a_n)), & \text{sonst,} \end{cases}$$

wobei im dritten Fall r Leitungen in das Gatter g eingehen, f_g die Funktion, die das Gatter g kennzeichnet, und g_i der Ursprung der i-ten Leitung, die in Gatter g eingeht, ist.

Ein Beispiel für einen recht einfachen Schaltkreis ist ein solcher, der - abgesehen von den Inputgattern - nur aus Gattern besteht, von denen jedes entweder die UND-Funktion oder die $ODER$-Funktion berechnet, wobei

$$UND(a_1,\ldots,a_n) := \begin{cases} 0, & \text{wenn } a_i = 0 \text{ für mindestens ein } i \in \{1,\ldots,n\}, \\ 1, & \text{sonst,} \end{cases}$$

$$ODER(a_1,\ldots,a_n) := \begin{cases} 1, & \text{wenn } a_i = 1 \text{ für mindestens ein } i \in \{1,\ldots,n\}, \\ 0, & \text{sonst.} \end{cases}$$

Ein solcher Schaltkreis kann unter Anwendung der De Morganschen Gesetze auch leicht aus einem Schaltkreis, der neben UND- und $ODER$-Gattern auch $NICHT$-Gatter verwendet, erhalten werden, wie Abbildung 1 zeigt.

Insbesondere berechnet ein Schaltkreis $\mathcal{C}$ mit n Inputgattern und k Outputgattern, die in einer bestimmten Weise angeordnet sind, eine Funktion $F_{\mathcal{C}} : \{0,1\}^n \to \{0,1\}^k$. In diesem Zusammenhang werden für den Spezialfall $k = 1$, also für den Fall eines einzigen Outputgatters, folgende Begriffe gebraucht.

Definition 2.4. Man sagt, dass ein Schaltkreis jeden Bitstring $a_1,\ldots,a_n$, für den $F_{\mathcal{C}}(a_1,\ldots,a_n) = 1$ ist, ***akzeptiert***, und, dass er die Menge der Strings, die er akzeptiert, ***erkennt***.

Im Folgenden sind vor allem Familien von Schaltkreisen von Interesse, wobei je zwei verschiedene Schaltkreise einer Familie immer unterschiedlich viele Inputs haben. Wenn jeder Schaltkreis der Familie nur genau ein Outputgatter hat, erkennt die Familie

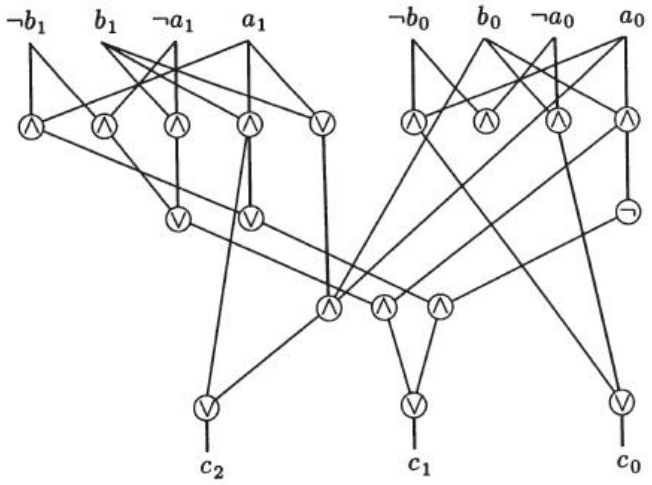

Abbildung 1: Zu sehen ist ein Schaltkreis, dessen Outputbits die Summe $(c_2\, c_1\, c_0)_2$ der Inputs $(a_1\, a_0)_2$ und $(b_1\, b_0)_2$ in Binärdarstellung ergeben. Er hat Tiefe 4, Größe 39, 8 Inputgatter, und seine UND- und $ODER$-Gatter haben jeweils fan-in 2. Auf die Verwendung des $NICHT$-Gatters kann verzichtet werden, indem man es zusammen mit dem vorangehenden UND-Gatter gemäß der Regel $\neg(b_0 \wedge a_0) = \neg b_0 \vee \neg a_0$ durch ein $ODER$-Gatter mit von $\neg b_0$ und $\neg a_0$ aus eingehenden Leitungen ersetzt. Bildquelle: [1]

eine Sprache $L \subseteq \{0,1\}^*$, wobei $L \cap \{0,1\}^n$ die Menge der Strings ist, die von dem Schaltkreis aus der Familie, der n Inputs hat, erkannt wird.
Gibt es mehr als ein Outputgatter, so berechnet die Familie von Schaltkreisen eine Funktion $f : \{0,1\}^* \to \{0,1\}^+$, mit der Eigenschaft, dass, wenn die Inputs $u, v \in \{0,1\}^*$ gleiche Länge haben, dann auch die Strings $f(u)$ und $f(v)$ gleiche Länge haben.

Da sich zeigen lässt, dass jede beliebige Funktion

$$f : \{0,1\}^k \to \{0,1\},\ k \in \mathbb{N}$$

mit einem aus nur einem einzigen $ODER$-Gatter und nicht mehr als 2^k UND-Gattern bestehenden Schaltkreis der Tiefe 2 berechnet werden kann, wenn man unbeschränkten fan-in erlaubt, sind Familien von Schaltkreisen beschränkter Tiefe mit UND- und $ODER$-Gattern uninteressant, wenn man keine weiteren Forderungen an sie stellt.
Darum werden im Folgenden Familien $\{\mathcal{C}_n\}_{n\geq 1}$ von Schaltkreisen betrachtet, in denen die Tiefe durch eine Konstante beschränkt ist und die Größe von $\mathcal{C}_n$ durch ein Polynom

in n.
Dies führt zu den im nächsten Abschnitt definierten Klassen.

3 Klassen von Schaltkreisen, Sprachen und Funktionen

Definition 3.1. $\mathbf{FAC^0}$ bezeichnet die Klasse von Funktionen, die von Familien $\{\mathcal{C}_n\}_{n\geq 1}$ von Schaltkreisen, deren Tiefe durch eine Konstante und deren Größe durch ein Polynom in n beschränkt ist, berechnet werden. Die Klasse der Sprachen, die von solchen Familien, in denen zudem jeder Schaltkreis nur genau ein Outputgatter hat, erkannt werden, wird mit $\mathbf{AC^0}$ bezeichnet.

Definition 3.2. Die Klasse von Funktionen, die von Familien $\{\mathcal{C}_n\}_{n\geq 1}$ von Schaltkreisen mit UND- und $ODER$-Gattern, die nachfolgend angeführte Bedingungen erfüllen, berechnet werden, wird mit $\mathbf{FNC^1}$ bezeichnet. Analog zu AC^0 wird die Klasse der Sprachen, die von Familien von Schaltkreisen, die nachfolgende Bedingungen erfüllen, und von denen jeder Schaltkreis ein einziges Outputgatter hat, erkannt werden, $\mathbf{NC^1}$ genannt.

1. $\mathcal{C}_n$ hat n Inputs.
2. Für alle n hat jedes UND- und $ODER$-Gatter fan-in 2.
3. Es gibt ein $k > 0$, sodass für alle n die Tiefe von $\mathcal{C}_n$ kleiner ist als $k \cdot \log_2 n$.
4. Es gibt ein Polynom p, sodass die Größe von $\mathcal{C}_n$ kleiner ist als $p(n)$.

Ein Beispiel für eine in FAC^0 liegende Funktion ist die Addition, das heißt, die Funktion $SUMME : \{0,1\}^* \to \{0,1\}^*$, definiert durch:

$$SUMME(w) := \begin{cases} 0, & \text{wenn } |w| \text{ ungerade ist,} \\ c_n \cdots c_0 \text{ für } (c_n \ldots c_0)_2 = (a_{n-1} \cdots a_0)_2 + (b_{n-1} \cdots b_0)_2, & \\ & \text{wenn } w = a_{n-1} \cdots a_0 b_{n-1} \cdots b_0. \end{cases}$$

Definition 3.3. Sind $L, L' \subseteq \{0,1\}^*$, so bezeichnen wir L als $\mathbf{AC^0}$***-reduzibel*** zu L' und schreiben $L \leq_{\mathbf{AC^0}} L'$, wenn L von einer Familie von Schaltkreisen, deren Tiefen durch Konstanten und deren Größen durch Polynome beschränkt sind, und die nur aus

$NICHT$-Gattern sowie $ODER$-, UND- und L'-Gattern von jeweils unbeschränktem fan-in aufgebaut sind, erkannt wird. Bei jedem L'-Gatter mit r Inputs sind die Inputbits $b_1, \ldots, b_r$ geordnet und das Gatter gibt genau dann Eins aus, wenn der String $b_1 \cdots b_r$ in L' liegt.

Aus der Definition der Reduzibilität folgt direkt der nachfolgende Zusammenhang.

Proposition 3.1. Seien $L, L' \subseteq \{0,1\}^*$, und sei $L \leq_{AC^0} L'$.
Ist $L' \in NC^1$, dann ist auch $L \in NC^1$.
Ist $L' \in AC^0$, dann ist auch $L \in AC^0$.

Beweis. Trivial. □

Zwei wichtige Sprachen, von denen erstgenannte im Folgenden eine zentrale Rolle spielt, sind MOD_q, $q \in \mathbb{N}$ und $MAJORITY$.

Definition 3.4. $\mathbf{MOD_q} := \{a_1 \cdots a_n : \sum_{i=1}^{n} a_i \equiv 0 \,(mod\, q)\}$,
$\mathbf{MAJORITY} := \{a_1 \cdots a_n : \sum_{i=1}^{n} a_i \geq \frac{n}{2}\}$

Zu zeigen, dass MOD_q nicht in der nachfolgend definierten Klasse $ACC(p^k)$ liegt, wenn p prim ist, $k \in \mathbb{N}^+$ und $q > 1$ einen von p verschiedenen Primfaktor hat, stellt das Hauptresultat dieser Arbeit dar.

Definition 3.5. $\mathbf{ACC(q)} := \{L \subseteq \{0,1\}^* : L \leq_{AC^0} MOD_q\}$,
$\mathbf{ACC} := \bigcup_{q>1} ACC(q)$
$\mathbf{TC^0} := \{L \subseteq \{0,1\}^* : L \leq_{AC^0} MAJORITY\}$

Man sagt, eine Familie von Schaltkreisen ist eine **Familie des Typs ACC(q)**, wenn sie konstante Tiefe hat, jeder Schaltkreis der Familie aus $NICHT$-Gattern, UND- sowie $ODER$-Gattern mit unbeschränktem fan-in und MOD_q-Gattern aufgebaut ist, und sie polynomiell beschränkte Größe hat.

Auf einfache Weise lässt sich zeigen, dass $MAJORITY \in NC^1$ und dass $MOD_q \leq_{AC^0} MAJORITY$. Mit Proposition 3.1 folgt aus Ersterem, dass $TC^0 \subseteq NC^1$ und mit genannter AC^0-Reduzibilität, dass $ACC \subseteq TC^0$.
Das im nächsten Abschnitt vorgestellte Hauptresultat dieser Arbeit impliziert für die Teilmenge $ACC(t) \subseteq ACC$ im Falle, dass t Primpotenz ist, die strikte Inklusion $ACC(t) \subsetneq TC^0$.

4 Hauptresultat

Den Knackpunkt im Beweis von Satz 4.3 stellt die Übersetzung des Schaltkreisproblems in eine algebraische Sprache dar, wobei Schaltkreise mit Polynomen assoziiert werden.
Sei dazu R ein kommutativer Ring mit Eins und $\mathcal{F}_{R,n}$ die Menge der Funktionen von $\{0,1\}^n$ nach R. $\mathcal{F}_{R,n}$ ist selbst wieder ein kommutativer Ring unter punktweiser Addition und Multiplikation der Funktionen. Insbesondere enthält $\mathcal{F}_{R,n}$ die Menge aller Booleschen Funktionen $f : \{0,1\}^n \to \{0,1\}$.
Ein Polynom $P(x_1, \ldots, x_n)$ mit Koeffizienten in R repräsentiert die durch $(a_1, \ldots, a_n) \mapsto P(a_1, \ldots, a_n)$ gegebene Funktion aus $\mathcal{F}_{R,n}$.
Ist $a = (a_1, \ldots, a_n) \in \{0,1\}^n$, dann wird die Funktion $\chi_a : \{0,1\}^n \to \{0,1\}$, welche als

$$\chi_a(b) := \begin{cases} 1, & \text{wenn } a = b \\ 0, & \text{sonst} \end{cases}$$

definiert ist, durch das Polynom

$$\left(\prod_{\{i:a_i=1\}} x_i \right) \cdot \left(\prod_{\{i:a_i \neq 1\}} (1 - x_i) \right)$$

repräsentiert.
Daher gilt für jede Funktion $f \in \mathcal{F}_{R,n}$, dass

$$f = \sum_{a \in \{0,1\}^n} f(a) \cdot \chi_a,$$

was zeigt, dass jede Funktion in $\mathcal{F}_{R,n}$ als ein Polynom dargestellt werden kann.
Da zudem x_i und x_i^2 das gleiche Element von $\mathcal{F}_{R,n}$ repräsentieren, kann jede Funktion als eine R-lineare Kombination von Monomen $X_I := \prod_{i \in I} x_i$, mit $I \subseteq \{1, \ldots, n\}$ und $X_\emptyset := 1$, dargestellt werden, die im Folgenden als „reduziertes Polynom“ bezeichnet wird, und die für jedes $f \in \mathcal{F}_{R,n}$ eindeutig ist, wie man mit einem kurzen Widerspruchsbeweis sieht.
Ist R ein Körper, dann hat $\mathcal{F}_{R,n}$ die Struktur eines Vektorraumes über R und ist eine

R-Algebra der Dimension 2^n. In diesem Fall bildet die Menge der Monome der Form X_I eine Vektorraumbasis. Insbesondere ist für $D \subsetneq \{0,1\}^n$ die Menge der Funktionen $f : D \to R$ eine R-Algebra der Dimension $|D|$ und jedes Element dieser Algebra wird (auf nicht eindeutige Weise) durch ein reduziertes Polynom repräsentiert.
Das reduzierte Polynom, das ein UND-Gatter mit fan-in n repräsentiert, ist $\prod_{i=1}^{n} x_i$ und das, welches ein $ODER$-Gatter mit fan-in n repräsentiert, ist $1 - \prod_{i=1}^{n}(1 - x_i)$. Daher wird zur Repräsentation eines Schaltkreises mit n Inputgattern im Allgemeinen ein Polynom vom Grad n benötigt. Allerdings gibt es auch die Möglichkeit, eine näherungsweise Repräsentation durch ein Polynom niedrigen Grades zu erhalten, wobei unter „näherungsweise“ verstanden wird, dass das Polynom das Verhalten des Schaltkreises auf einer großen Teilmenge von $\{0,1\}^n$ repräsentiert, und „niedrigen“ Grades bedeutet, dass der Grad viel kleiner ist als der ursprüngliche Grad n.
Diese Tatsache wird in folgendem Lemma spezifiziert.

Lemma 4.1. Sei F ein Körper der Charakteristik p, p prim. Seien $f_1, \ldots, f_r : \{0,1\}^n \to \{0,1\}$ durch Polynome vom Grad d repräsentiert. Sei $1 \leq l \leq n$.
Dann können $UND(f_1, \ldots, f_r)$ und $ODER(f_1, \ldots, f_r)$ jeweils durch ein Polynom vom Grad kleiner oder gleich $(|F| - 1)ld$ auf einer Menge $D \subseteq \{0,1\}^n$ der Kardinalität größer oder gleich $2^n - 2^{n-l}$ repräsentiert werden.

Beweis. Die Behauptung wird für $ODER(f_1, \ldots, f_r)$ gezeigt. Für UND folgt sie daraus aufgrund der Beziehung $UND(f_1, \ldots, f_r) = 1 - ODER(1 - f_1, \ldots, 1 - f_r)$.
Betrachtet man die Menge der Polynome der Form

$$1 - \prod_{j=1}^{l} \left(1 - (\sum_{i=1}^{r} c_{ij} f_i)^{|F|-1} \right),$$

wobei $c_{ij} \in F$ für $1 \leq i \leq r$, $1 \leq j \leq l$, so sieht man, dass jedes darin enthaltene Polynom den Grad $(|F| - 1)ld$ hat und nur Werte in $\{0,1\}$ liefert.
Nun wählt man ein fixes $a \in \{0,1\}^n$ und zählt die Anzahl der Möglichkeiten, die c_{ij} so mit Elementen aus F zu belegen, dass das Polynom auf diesem a mit $ODER(f_1, \ldots, f_r)$ übereinstimmt.
Ist $f_i(a) = 0$ für $i = 1, \ldots, r$, so ergibt das Polynom unabhängig von der Belegung der c_{ij} Null, was dem Ergebnis von $ODER(f_1, \ldots, f_r)$ entspricht.

Andernfalls gibt es ein $m \in \{1, \ldots, r\}$, sodass $f_m(a) = 1$. Das hat zur Folge, dass es, egal, mit welchem Wert die $c_{k1}, \ldots, c_{kl}$ für $k \neq m$ belegt werden, für jedes $j \in \{1, \ldots, l\}$ immer genau eine Belegung von c_{mj} gibt, sodass $\sum_{i=1}^{r} c_{ij} f_i(a) = 0$.
Das bedeutet, unter allen $|F|^l$ Möglichkeiten, das $l-$Tupel $(c_{m1}, \ldots, c_{ml})$ zu belegen, gibt es genau eine, sodass das Polynom Null ergibt.
Somit ist der Anteil der Belegungen der c_{ij}, sodass das Polynom mit $ODER(f_1, \ldots, f_r)$ nicht übereinstimmt, für jedes fixe $a \in \{0,1\}^n$ höchstens $|F|^{-l}$. Da a aus einer Menge mit 2^n Elementen beliebig gewählt war, und F mindestens zwei Elemente enthält, gibt es folglich eine Belegung, für welche das resultierende Polynom mit $ODER(f_1, \ldots, f_r)$ auf höchstens $2^n \cdot |F|^{-l} \leq 2^{n-l}$ Elementen von $\{0,1\}^n$ nicht übereinstimmt. □

Lemma 4.2. Sei p prim und sei F ein Körper der Charakteristik p. Sei $\{\mathcal{C}_n\}_{n \geq 0}$ eine Familie des Typs $ACC(p)$ mit Schaltkreisen der Tiefe d und 2^r Gattern, wobei $r = o(n^{1/2d})$.
Dann gibt es eine Familie $\{P_n\}$ von Polynomen über F, sodass $deg(P_n) = o(\sqrt{n})$ und sodass P_n mit der von $\mathcal{C}_n$ berechneten Funktion auf einer Menge der Kardinalität $2^n - o(2^n)$ übereinstimmt.

Beweis. Für den Beweis wird wiederholt Lemma 4.1 mit $l = 2r$ angewandt. Bei den Inputgattern beginnend, wird jedes Gatter von $\mathcal{C}_n$ durch ein Polynom ersetzt, wobei die Inputgatter durch x_i und $1 - x_i$ ersetzt werden und jedes MOD_p-Gatter mit fan-in k durch $1 - (Q_1 + \ldots + Q_k)^{|F|-1}$, wobei $Q_1, \ldots Q_k$ die mit den Gattern der eingehenden Leitungen assoziierten Polynome sind. Die UND- und $ODER$-Gatter werden mit polynomiellen Funktionen der mit den Gattern der eingehenden Leitungen assoziierten Polynome ersetzt.
Da der Schaltkreis nach Voraussetzung Tiefe d hat, folgt mit Lemma 4.1, dass das mit dem Outputgatter assoziierte Polynom höchstens den Grad $((|F| - 1)l)^d = ((|F| - 1)2r)^d = (2(|F| - 1))^d \cdot r^d = o(\sqrt{n})$ hat und die von $\mathcal{C}_n$ berechnete Funktion auf allen bis auf $2^r \cdot 2^{n-l} = 2^{n-r} = o(2^n)$ Elementen von $\{0,1\}^n$ repräsentiert, wobei im Falle, dass r konstant ist, 2^{n-r} zwar nicht in $o(2^n)$ ist, aber dann l als eine Funktion in $o(n^{1/2d})$ gewählt werden kann. □

Mithilfe dieses Lemmas kann das folgende Hauptresultat bewiesen werden.

Satz 4.3. *Ist p prim und hat $t \in \mathbb{N}$, $t > 1$ einen von p verschiedenen Primfaktor, dann ist $MOD_t \notin ACC(p^k)$ für jedes $k > 0$.*

Beweis. Da $ACC(p^k) \subseteq ACC(p)$, genügt es, die stärkere Aussage für $ACC(p)$ anstatt $ACC(p^k)$ zu beweisen.
Ist $MOD_t \in ACC(p)$, dann ist auch jede der Sprachen

$$MOD_{t,s} := \{a_1 \cdots a_n \in \{0,1\}^* : \sum_{i=1}^{n} a_i \equiv s \,(mod\, t)\}, \text{ für } 0 \leq s < t$$

in $ACC(p)$, wie eine einfache Mfodifikation der Schaltkreise zeigt. Insbesondere gilt dann für jeden von p verschiedenen Primteiler q von t, dass $MOD_q \in ACC(p)$, weil sich MOD_q als $MOD_q = \bigcup_{c=0}^{\frac{t}{q}-1} MOD_{t,cq}$ schreiben lässt und die rechte Seite in $ACC(p)$ ist.

Die Gleichheit $MOD_q = \bigcup_{c=0}^{\frac{t}{q}-1} MOD_{t,cq}$ sieht man wie folgt:
MOD_q besteht aus (endlichen) Zeichenfolgen, in denen die Anzahl der auftretenden Einser ein Vielfaches von q ist.
„ $\supseteq$ “:
Ist nun t ein Vielfaches von q, das heißt, $t = mq$ für ein $m \in \mathbb{N}$, dann enthält jeder String, der in der Vereinigung auf der rechten Seite liegt, $cq + rt = cq + rmq$ Einser, wobei jeweils $r \in \mathbb{N}$ ist. Diese Anzahl ist ein Vielfaches von q, also ist jeder der Strings auch in MOD_q.
„ $\subseteq$ “:
Liegt andererseits ein String in MOD_q, so hat er uq Einser für ein $u \in \mathbb{N}$. Nun ist $u \equiv c \,(mod\, m)$ für ein $0 \leq c < m$, wobei m wieder jene natürliche Zahl sei, für die $t = mq$ gilt. Somit hat der String $cq + rmq = cq + rt$ Einser für ein $r \in \mathbb{N}$, womit er auch in $MOD_{t,cq}$ enthalten ist.

Daher wird im Folgenden gezeigt, dass $MOD_q \notin ACC(p)$ für eine von der Primzahl p verschiedene Primzahl q, womit mittels Kontraposition die zu beweisende Behauptung folgt.
Genauer, wird gezeigt, dass keine Familie des Typs $ACC(p)$ von Schaltkreisen der Tiefe d mit 2^r Gattern, wobei $r = o(n^{1/2d})$, MOD_q erkennen kann. Somit erweist sich MOD_q als nicht AC^0-reduzibel auf MOD_p und liegt daher nicht in $ACC(p)$.
Sei $F := GF(p^l)$ für ein $l \in \mathbb{N}^+$. F hat Charakteristik p, umfasst p^l Elemente und enthält $\mathbb{Z}_p$ als Unterkörper.
Da q eine Primzahl ist, enthält die Einheitengruppe modulo q - also die Gruppe aller

multiplikativ invertierbaren Elemente des Rings $\mathbb{Z}_q$ - alle Elemente bis auf das Nullelement, insbesondere also auch p, weil p nach Voraussetzung teilerfremd zu q ist. Da die Gruppe endlich ist, hat p endliche Ordnung in der Gruppe, das heißt, es gibt ein $m \in \mathbb{N}^+$, sodass $p^m \equiv 1 \pmod{q}$, woraus $q|(p^m - 1)$ folgt. Das l wird in der Definition von F als $l := m$ für dieses m gewählt und $GF(p^m)$ betrachtet.
Die multiplikative Gruppe von F besteht aus allen Elementen außer Null, hat also Ordnung $p^m - 1$ und ist zyklisch. Da generell jede zyklische Gruppe der Ordnung $k \in \mathbb{N}$ genau dann eine Untergruppe der Ordnung d hat, wenn $d|k$, und diese Untergruppe die einzige ihrer Ordnung ist, und weil $q|(p^m - 1)$, hat die multiplikative Gruppe von F genau eine Untergruppe der Ordnung q. Diese ist als Untergruppe einer zyklischen Gruppe ebenfalls zyklisch und wird daher von einer Primitivwurzel der Ordnung q erzeugt, das bedeutet, es gibt ein Element g, sodass $g^q = 1$ und $g^r \neq 1$ für $1 \leq r < q$.
Für $x_i = 0$ und $x_i = 1$ gilt jeweils $x_i = (g-1)^{-1}(g^{x_i} - 1)$.
Sei nun $y_i := g^{x_i}$. Dann ist $y_i^{-1} = g^{-x_i} = (g^{-1} - 1)(g-1)^{-1}(y_i - 1) + 1$, wie man durch Umformung auf $\frac{g^{x_i}-1}{g-1} = \frac{(g^{-1})^{x_i}-1}{g^{-1}-1}$ und Einsetzen von $x_i = 0$ bzw. $x_i = 1$ sieht.
Im Widerspruch zu dem zu Zeigenden sei nun angenommen, dass eine Familie von Schaltkreisen der Tiefe d und Größe 2^r des Typs $ACC(p)$ existiert, die MOD_q erkennt. Ist dies der Fall, so erhält man leicht eine solche Familie für jede der Sprachen $MOD_{q,s}$, $0 \leq s < q$.
Laut Lemma 4.2 gibt es eine Folge $\{P_{n,s}\}_{n \geq 0}$ von Polynomen über F, mit zugehörigen Teilmengen $E_{n,s}$ von $\{0,1\}^n$, sodass $deg(P_{n,s}) = o(\sqrt{n})$, $|E_{n,s}| = o(2^n)$, und

$$P_{n,s}(a) = \begin{cases} 1, \text{ wenn } a \in MOD_{q,s} \text{ ist,} \\ 0, \text{ andernfalls,} \end{cases} \qquad \text{für } a \notin E_{n,s}.$$

Sei $P_n := \sum_{s=0}^{q-1} g^s P_{n,s}$. Dann ist $deg(P_n) = o(\sqrt{n})$ und P_n stimmt mit der Funktion $g^{x_1+\ldots+x_n}$ außerhalb der Menge $E_n := \bigcup_{s=0}^{q-1} E_{n,s}$ überein.

Die Übereinstimmung sieht man folgendermaßen:
Nach Definition ist $P_{n,s}(a) = \begin{cases} 1, & \text{wenn } a \in MOD_{q,s} \\ 0, & \text{sonst.} \end{cases}$

Demnach ist $P_n(a) = \sum_{s=0}^{q-1} g^s P_{n,s}(a) = g^s$, wenn $a_1 + \ldots + a_n = qm + s$, für ein $m \in \mathbb{N}$, was - aufgrund der Definition von g als q-te Primitivwurzel - $g^{x_1+\ldots+x_n}(a)$ entspricht.

Für E_n gilt: $|E_n| \leq q \cdot o(2^n) = o(2^n)$.

Sei D_n die Menge, auf der P_n mit $g^{x_1+\ldots+x_n}$ übereinstimmt, das heißt, $D_n := \{0,1\}^n \backslash E_n$, und sei f eine Funktion von D_n nach F. Sei Q_n ein Polynom in n Variablen, das f auf D_n repräsentiert.

Ist Q_n vom Grad größer $\frac{n}{2}$, so wird jedes Vorkommen von x_i in Q_n durch $(g-1)^{-1}(y_i - 1)$ ersetzt, sodass man eine F-lineare Kombination der Funktionen $Y_I := \prod_{i \in I} y_i$, für $I \subseteq \{1, \ldots, n\}$, erhält.

Um ein Polynom niedrigen Grades zu bekommen, wird nun jedes Y_I, für das $|I| > \frac{n}{2}$, als $y_1 \cdots y_n \prod_{j \notin I} y_j^{-1}$ geschrieben und anschließend durch das damit auf D_n übereinstimmende Polynom

$$P_n \cdot \prod_{j \notin I} [(g^{-1} - 1)(g-1)^{-1}(y_j - 1) + 1]$$

ersetzt.

Nun folgt die Umkehrung des Austauschs der Variablen, das heißt, jedes y_i wird durch $(g-1)x_i + 1$ substituiert.

Das Resultat ist ein Polynom Q_n' vom Grad $o(\sqrt{n}) + \frac{n}{2}$, das f auf D_n repräsentiert.

Also wird der Raum der Funktionen von D_n nach F von Monomen eines Grades kleiner oder gleich $\frac{n}{2} + o(\sqrt{n})$ aufgespannt. Folglich gilt für die Dimension des Raumes, dass

$$|D_n| \leq \sum_{i=0}^{\frac{n}{2}+o(\sqrt{n})} \binom{n}{i}.$$

Um die Summe zu approximieren, nutzt man die Ähnlichkeit ihrer Form zur Binomialverteilung:

Für eine $Binom(n, \frac{1}{2})$-verteilte Zufallsvariable X_n gilt

$$P\left(X \leq \frac{n}{2} + o(\sqrt{n})\right) = \sum_{i=0}^{\frac{n}{2}+o(\sqrt{n})} \binom{n}{i} \cdot \left(\frac{1}{2}\right)^i \cdot \left(\frac{1}{2}\right)^{n-i},$$

also entspricht obige Summe der 2^n-maligen Wahrscheinlichkeit, dass eine binomialverteilte Zufallsvariable in $\{0, \ldots, n\}$ kleiner oder gleich $\frac{n}{2} + o(\sqrt{n})$ ist. Mittels des Zentralen Grenzwertsatzes kann die Wahrscheinlichkeit nun folgendermaßen zu $\frac{1}{2} + o(1)$ abgeschätzt werden:
Da $X_n \sim Binom(n, \frac{1}{2})$ Erwartungswert $\frac{n}{2}$ und Standardabweichung $\frac{\sqrt{n}}{2}$ hat, gilt für festes $x \in \mathbb{R}$, dass $\lim\limits_{n\to\infty} P\left(\frac{X_n - \frac{n}{2}}{\frac{\sqrt{n}}{2}} \leq x\right) = \Phi(x)$. Zu zeigen ist nun

$$P\left(X_n \leq \frac{n}{2} + o(\sqrt{n})\right) = \frac{1}{2} + o(1).$$

Das ist nach Definition des Landau-Symbols äquivalent dazu, zu zeigen, dass für e_n mit $\lim\limits_{n\to\infty} e_n = 0$ gilt, dass

$$\lim_{n\to\infty} P\left(X_n \leq \frac{n}{2} + e_n\sqrt{n}\right) = \frac{1}{2}.$$

Sei also A_n das Ereignis $[X_n \leq \frac{n}{2} + e_n\sqrt{n}]$, und seien $B_n := [X_n \leq \frac{n}{2} - \epsilon\frac{\sqrt{n}}{2}]$ und $C_n := [X_n \leq \frac{n}{2} + \epsilon\frac{\sqrt{n}}{2}]$. Für jedes $\epsilon > 0$ gilt $|e_n\sqrt{n}| < \epsilon\frac{\sqrt{n}}{2}$, wenn n groß genug ist. Für solches n gelten die Inklusionen $B_n \subseteq A_n \subseteq C_n$.
Anwendung des Zentralen Grenzwertsatzes auf die linke und rechte Seite liefert $\Phi(-\epsilon) \leq \liminf\limits_{n\to\infty} P(A_n)$ und $\limsup\limits_{n\to\infty} P(A_n) \leq \Phi(\epsilon)$. Da $\epsilon > 0$ beliebig war, und Φ an der Stelle Null stetig ist, folgt daraus, dass $\lim\limits_{n\to\infty} P(A_n) = \Phi(0) = \frac{1}{2}$, was genau $P(A_n) = \frac{1}{2} + o(1)$ bedeutet.
Somit gilt $|D_n| \leq \sum\limits_{i=0}^{\frac{n}{2}+o(\sqrt{n})} \binom{n}{i} = 2^{n-1} + o(2^n)$, was im Widerspruch zu der vorangegangenen Feststellung, dass $|D_n| = 2^n - o(2^n)$ ist, steht. □

Dieser Satz zieht folgende Konsequenzen nach sich.

Satz 4.4. *Wenn r eine Primpotenz ist, das heißt, $r = p^k$ für p prim, $k \in \mathbb{N}^+$, dann ist $ACC(r) \subsetneq TC^0$.*

Beweis. Sei p prim und sei $q \in \mathbb{N}^+$ so, dass mindestens ein Primfaktor von q verschieden von p ist.
Falls $ACC(p^k) = TC^0$ für ein $k \geq 1$, dann gilt nach Definition von TC^0, dass $MAJORITY \in ACC(p^k)$. Da $MOD_q \leq_{AC^0} MAJORITY\, \forall q > 1$ ist, folgt $MOD_q \in ACC(p^k)$, im Widerspruch zu Satz 4.3. □

Es wird angenommen, dass in Satz 4.3 die Primalitätsbedingung nicht benötigt wird. Damit erhält man folgende Vermutung:

Satz 4.5 (Vermutung)**.** *Seien $p, q > 1$. Wenn q einen Primfaktor hat, der p nicht teilt, dann ist $MOD_q \notin ACC(p)$.*

Satz 4.6. *Wenn Vermutung 4.5 wahr ist, dann gilt, dass $ACC \subsetneq TC^0$.*

Beweis. Ist $ACC = TC^0$, dann ist $MAJORITY \in ACC$ und nach Definition von ACC somit $MAJORITY \in ACC(p)$ für ein $p > 1$. Da $MOD_q \leq_{AC^0} MAJORITY \; \forall q$, erhält man $MOD_q \in ACC(p) \; \forall q$, im Widerspruch zur Vermutung. □

Literatur

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