Komplexität boolescher Funktionen bei Verwendung von Multiplexern wachsender Größe

Complexity of Boolean Functions regarding the Usage of Multiplexers of Increasing Size
Bachelor-Thesis von Tobias Reinhard aus Aschaffenburg
Tag der Einreichung:

1. Gutachten: Dr. rer. nat. Ulrike Brandt
2. Gutachten: Prof. Dr. Martin Ziegler

TECHNISCHE UNIVERSITÄT DARMSTADT

Fachbereich Informatik

Komplexität boolescher Funktionen bei Verwendung von Multiplexern wachsender Größe
Complexity of Boolean Functions regarding the Usage of Multiplexers of Increasing Size

Vorgelegte Bachelor-Thesis von Tobias Reinhard aus Aschaffenburg

1. Gutachten: Dr. rer. nat. Ulrike Brandt
2. Gutachten: Prof. Dr. Martin Ziegler

Tag der Einreichung:

Erklärung zur Bachelor-Thesis

Hiermit versichere ich, die vorliegende Bachelor-Thesis ohne Hilfe Dritter nur mit den angegebenen Quellen und Hilfsmitteln angefertigt zu haben. Alle Stellen, die aus Quellen entnommen wurden, sind als solche kenntlich gemacht. Diese Arbeit hat in gleicher oder ähnlicher Form noch keiner Prüfungsbehörde vorgelegen.
In der abgegebenen Thesis stimmen die schriftliche und elektronische Fassung überein.

Darmstadt, den 19. April 2015

(Tobias Reinhard)

Zusammenfassung

Üblicherweise wird die Komplexität boolescher Funktionen bezüglich einer festen Menge an Basisfunktionen (Basismenge) gemessen. Im Gegensatz dazu soll im Rahmen dieser Arbeit der Ansatz verfolgt werden, an Stelle einer festen Basismenge Ω eine Folge von Basismengen $\Omega_0, \Omega_1, \ldots$ zu betrachten und die Komplexität n-stelliger boolescher Funktionen bezüglich Ω_n zu bestimmen.

Konkret sollen für eine monoton wachsende und unbeschränkte Funktion $d : \mathbb{N} \to \mathbb{N}^*$ mit $d(n) < n$ und die Basismengen $\Omega_0 = \{0, 1\}$ und $\Omega_i = \{mux_{d(i)}, 0, 1\}$ für alle $i \in \mathbb{N}^*$ eine obere und eine untere Schranke (im Sinne von Shannons unterer Schranke) hergeleitet werden, wobei $mux_{d(i)}$ einen Multiplexer mit $d(i)$ Steuer- und $2^{d(i)}$ Dateneingängen bezeichnet.

Zusätzlich soll gezeigt werden, dass die zum Beweis der oberen Schranke verwendete Konstruktion und Wahl der Basismengen $\Omega_0, \Omega_1, \ldots$ asymptotisch betrachtet im Wesentlichen optimal bis auf den Faktor 2 ist.

Inhaltsverzeichnis

1 Einleitung 4

2 Grundlagen 6

3 Verallgemeinerung von Shannons unterer Schranke 9

4 Eine obere Schranke durch Multiplexer 13

5 Vergleich der unteren und oberen Schranke 23

6 Weiterführende Fragestellungen 27

1 Einleitung

Ein wichtiges Teilgebiet der Schaltkreiskomplexität ist die Suche nach oberen und unteren Schranken für die Komplexität von Funktionen aus bestimmten Funktionsklassen. So konnte Shannon beispielsweise zeigen, dass die Anzahl der n-stelligen booleschen Funktionen, deren Realisierung mehr als $\frac{2^n}{n}$ Gatter erfordert, für $n \to \infty$ gegen die Gesamtanzahl aller n-stelligen booleschen Funktionen 2^{2^n} konvergiert (untere Schranke) [9, S.64]. Mit anderen Worten: Für wachsende n strebt die Wahrscheinlichkeit, dass die Realisierung einer zufällig gewählten n-stelligen booleschen Funktion mehr als $\frac{2^n}{n}$ Gatter erfordert, gegen 1. Andererseits zeigte Lupanov, dass sich jede n-stellige boolesche Funktion durch maximal $\left(1 + O\left(\frac{\log n}{n}\right)\right) \cdot \frac{2^n}{n}$ Gatter realisieren lässt (obere Schranke) [6, S.23]. Deutlich bessere Resultate ergeben sich hingegen für die Funktionen einiger Teilklassen der booleschen Funktionen. So ist beispielsweise die Komplexität der n-stelligen symmetrischen Funktionen durch $2.5n - 5$ nach unten [11] und durch $4.5n + o(n)$ nach oben [2] beschränkt.

All diese Schranken hängen von der Arität der zu realisierenden Funktionen ab und meist wird – wie in den genannten Fällen – davon ausgegangen, dass Gatter für alle maximal zweistelligen Funktionen zum Aufbau eines Schaltkreises zur Verfügung stehen. Die Wahl eines anderen konstanten und vollständigen Satzes an Basisfunktionen würde die berechneten Schranken ohnehin nur um einen konstanten Faktor beeinflussen.

Anders verhält es sich hingegen, wenn man dazu übergeht die Basisfunktionen nach der Arität der untersuchten Funktionsklasse auszuwählen. In diesem Fall stellt sich jedoch allgemein die Frage, nach welchen Kriterien Basisfunktionen auszuwählen sind. Da die Menge der Basisfunktionen in diesem Szenario zwar abhängig von der Arität einer bestimmten Funktionsklasse, nicht jedoch abhängig von einer konkreten Funktion gewählt wird, muss es möglich sein, alle Funktionen der betrachteten Klasse durch Kombination der gewählten Basisfunktionen zu realisieren.

Ein möglicher Ansatz ist, an Stelle einer festen Menge Ω an Basisfunktionen – im Folgenden Basismenge genannt – eine Folge von Basismengen $\Omega_0, \Omega_1, \ldots$ zu wählen und die Komplexität der n-stelligen booleschen Funktionen bezüglich der Basismenge Ω_n zu bestimmen. Dabei stellt sich jedoch die Frage wie $\Omega_0, \Omega_1, \ldots$ zu wählen sind. Um die Wahl einer Folge von Basismengen an Stelle einer einzelnen Basismenge zu rechtfertigen, sollten sich für wachsende i zunehmend bessere obere Schranken bezüglich Ω_i ergeben.
Ebenso kann, um konstruktive Beweise oberer Schranken nicht unnötig zu verkomplizieren, darauf geachtet werden, dass sich die für diese Beweise genutzten Eigenschaften der Menge Ω auf jedes Element der Folge $\Omega_0, \Omega_1, \ldots$ übertragen. Weiterhin sollte, um die Herleitung nicht-trivialer Schranken zu ermöglichen, darauf geachtet werden, die Arität der Basisfunktionen aus Ω_n asymptotisch vernachlässigbar gegenüber n zu wählen oder sie als variabel zu betrachten.

Dieses Vorgehen soll nun exemplarisch an zwei Beispielen erläutert werden. Dazu seien $n \in \mathbb{N}$ die Arität der Funktionen der untersuchten Funktionsklasse und $d \in o(n)$ eine gegenüber n asymptotisch vernachlässigbare Funktion.

Angenommen es sei $\Omega = \mathbb{B}^{\mathbb{B}^2} \cup \{0, 1\}$ die Menge der zweistelligen booleschen Funktionen sowie der Konstanten 0 und 1 und die relevante Eigenschaft der Menge Ω_n bezüglich der zu führenden Beweise sei, dass alle booleschen Funktionen der Arität $d(n)$ sowie die booleschen Konstanten in Ω_n zur Verfügung stehen. Dann kann diese Wahl leicht auf $\Omega_n = \mathbb{B}^{\mathbb{B}^{d(n)}} \cup \{0,1\}$ verallgemeinert werden.

Angenommen Ω entspräche hingegen der Basismenge mit den Konstanten 0 und 1 sowie einem Multiplexer mit einem Steuereingang (und folglich zwei Dateneingängen) und angenommen für die zu führenden Beweise sei relevant, dass die Konstanten 0 und 1 sowie ein Multiplexer mit einer bestimmten Anzahl an Steuereingängen als Basisfunktionen zur Verfügung stehen. Dann kann Ω_n als die Menge mit den Konstanten 0 und 1 sowie einem Multiplexer mit $d(n)$ Steuereingängen (und somit $2^{d(n)}$ Dateneingängen) gewählt werden.

Aufbau und Ergebnisse

Im Rahmen dieser Arbeit soll die Komplexität beliebiger n-stelliger Funktionen bezüglich des Aufbaus aus Multiplexern mit $d(n)$ Steuer- und $2^{d(n)}$ Dateneingängen untersucht werden, wobei $d : \mathbb{N} \to$ [redacted]* eine monotone und unbeschränkte Funktion mit $d(n) < n$ sei. Konkret soll die Komplexität durch eine untere sowie eine obere Schranke abgeschätzt werden. Beide Schranken ergeben sich aus der Verallgemeinerung existierender Beweise, die von zweistelligen Basisfunktionen ausgehen.

Zur Einführung werden in Abschnitt 2 grundlegende Notationen und Begrifflichkeiten erläutert, die im weiteren Verlauf der Arbeit vorausgesetzt werden.

Abschnitt 3 liefert durch die Verallgemeinerung von Shannons Abzählargument [9, S.64] eine untere Schranke im Sinne von Shannon für die Komplexität n-stelliger Funktionen, bei der Arität und Anzahl der verwendeten Basisfunktionen als variabel betrachtet werden.

Abschnitt 4 beschäftigt sich hingegen mit der Konstruktion einer oberen Schranke für besagte Komplexität. Das Vorgehen basiert dabei auf einem [redacted], der auf der Konstruktion eines $(2^n + n)$-stelligen Multiplexers (also eines Multiplexers mit n Steuer- und 2^n Dateneingängen) auf Basis zweistelliger Funktionen beruht. Dabei wurde die Verwendung zweistelliger Funktionen durch die von $(2^d + d)$-stelligen Multiplexern ersetzt, um so einen iterativen Aufbau eines (2^n+n)-stelligen Multiplexers zu ermöglichen, der für die Realisierung einer n-stelligen Funktion genutzt werden kann. Folglich bezieht sich die resultierende obere Schranke auf die Verwendung $(2^d + d)$-stelliger Multiplexer.

In Abschnitt 5 werden schließlich aus diesen beiden in den Abschnitten 3 und 4 vorgestellten Schranken eine untere sowie eine obere Schranke abgeleitet, die sich auf die Verwendung d-stelliger Multiplexer beziehen. Anschließend erfolgt ein Vergleich beider Schranken für eine monoton wachsende und unbeschränkte Funktion $d : \mathbb{N} \to \mathbb{N}^*$ mit $d(n) < n$. Dieser zeigt, dass die zum Beweis der oberen Schranke verwendete Konstruktion sowie Wahl der Basismengenfolge $\Omega_0 = \{0,1\}$, $\Omega_i = \{mux_{d(i)}, 0, 1\}$ für alle $i \in \mathbb{N}^*$ asymptotisch betrachtet im Wesentlichen optimal bis auf den Faktor 2 ist, wobei $mux_{d(n)}$ einen Multiplexer mit $d(n)$ Steuer- und $2^{d(n)}$ Dateneingängen bezeichnet.

Zum Abschluss werden in Abschnitt 6 einige weiterführende Fragestellungen ausgeführt.

2 Grundlagen

In diesem Abschnitt sollen grundlegende Notationen und Begriffe definiert werden, die im weiteren Verlauf der Arbeit Verwendung finden.

Definition 2.1. Es seien $\mathbb{N}$ und $\mathbb{N}^*$ definiert als

$$\begin{aligned} \mathbb{N} \; &:= \{0,1,2,\dots\}, \\ \mathbb{N}^* &:= \mathbb{N} \setminus \{0\}. \end{aligned}$$

[1]

Definition 2.2. Es sei $\mathbb{R}_0^+$ definiert als

$$\mathbb{R}_0^+ \;:=\; [0,\infty).$$

Definition 2.3. Für $n \in \mathbb{N}$ seien $\mathbb{B}$, B_n und B definiert als

$$\begin{aligned} \mathbb{B} \; &:= \{0,1\}, \\ B_n &:= \begin{cases} \mathbb{B}, & \text{falls } \; n = 0 \\ B_{n-1} \cup \mathbb{B}^{\mathbb{B}^n}, & \text{sonst,} \end{cases} \\ B \; &:= \bigcup_{m \in \mathbb{N}} B_m. \end{aligned}$$

Definition 2.4. Es sei $arity : B \to \mathbb{N}$ definiert als

$$arity(f) \;:=\; \min\{n \in \mathbb{N} \;:\; f \in B_n\}\,.$$

Definition 2.5. Eine Menge $\Omega \subseteq B$ ist *vollständig bezüglich* einer Menge $\Gamma \subseteq B$, wenn sich alle Funktionen aus Γ mittels Komposition und Substitution aus Funktionen aus Ω erzeugen lassen.
Weiterhin ist Ω *vollständig*, wenn Ω vollständig bezüglich B ist.
[9, S.4]

Eine bezüglich Γ vollständige Menge Ω wird auch als Γ-*vollständig* bezeichnet.

Definition 2.6 (Schaltkreis)**.**
Sei $\Omega \subseteq B$ eine nicht leere Menge boolescher Funktionen, dann ist ein Ω-Schaltkreis S gegeben durch:

1. Endliche, disjunkte Mengen G, E und A, wobei die Elemente aus G als Gatter, die Elemente aus E als Eingabevariablen und die Elemente aus A als Ausgabevariablen bezeichnet werden.

2. Einen azyklischen, gerichteten Graphen (V,R) mit $V = G \cup E \cup A$.

3. Eine Abbildung $g_S : G \to \Omega$.

4. Eine Abbildung $indeg_S : V \to \mathbb{N}$ mit

$$indeg_S(v) := \begin{cases} arity(g_S(v)), & \text{falls } v \in G \\ 0, & \text{falls } v \in E \\ 1, & \text{falls } v \in A. \end{cases}$$

5. Eine Abbildung $input_S : \Big\{(v,i) \mid v \in V,\ i \in \{1,\dots,indeg_S(v)\}\Big\} \to V$ mit $(input_S(v,i),\ v) \in R$ für alle $i \in \{1,\dots,indeg_S(v)\}$.

[4]

Die Funktionen aus Ω werden als *Basisfunktionen* und Ω als *Basismenge* bezeichnet. Weiterhin bezeichnet der Begriff *Schaltkreis* einen B-Schaltkreis.

Nach dieser Definition gilt für alle Mengen $\Omega \subseteq B$, dass ein Ω-Schaltkreis ein B-Schaltkreis und damit auch ein Schaltkreis ist. Außerdem ist zu beachten, dass ein Schaltkreis nicht notwendigerweise über Ausgabevariablen verfügen muss. Daher wird im weiteren Verlauf dieser Arbeit in allen vorgestellten Schaltkreisen auf Ausgabevariablen verzichtet, sofern dies nicht explizit angegeben ist.

Definition 2.7. Für $i,n \in \mathbb{N}^*$ mit $i \leq n$ sei $p_{i,n} : \mathbb{B}^n \to \mathbb{B}$ definiert als

$$p_{i,n}(x_1,\dots,x_n) := x_i.$$

[4]

Definition 2.8. Für einen Schaltkreis S mit Gattern $g_1,\dots,g_k$, Eingabevariablen $x_1,\dots,x_n$, Ausgabevariablen $y_1,\dots,y_r$ und Knotenmenge $V = \{g_1,\dots,g_k\} \cup \{x_1,\dots,x_n\} \cup \{y_1,\dots,y_r\}$ sei $comp_S : V \to \mathbb{B}^{\mathbb{B}^n}$ definiert als

$$comp_S(v) := \begin{cases} p_{i,n}, & \text{falls } i \in \{1,\dots,n\} \text{ existiert mit } v = x_i \\ g_S(v)(comp_S(input_S(v,1)),\ \dots,\ comp_S(input_S(v,indeg_S(v)))), & \\ & \text{falls } v \in \{g_1,\dots,g_k\} \\ comp_S(input_S(v,1)), & \text{falls } v \in \{y_1,\dots,y_r\}. \end{cases}$$

[4]

Definition 2.9 (Berechnete Funktion eines Schaltkreises)**.**
Sei S ein Schaltkreis mit Knotenmenge V. Dann *berechnet* S die Funktion $f \in B$ genau dann wenn eine der folgenden Bedingungen erfüllt ist:

1. S verfügt über Ausgabevariablen $y_1,\dots,y_r$ mit $r \in \mathbb{N}^*$ und es existiert ein $i \in \{1,\dots,r\}$ mit $f = comp_S(y_i)$.

2. S verfügt über keine Ausgabevariablen und es existiert ein $v \in V$ mit $f = comp_S(v)$.

[4]

Weiterhin *realisiert* der Schaltkreis S die Funktion f, wenn er diese berechnet.

Definition 2.10. Ein Schaltkreis S realisiert eine Funktionsmenge $\Gamma \subseteq B$, wenn er jede Funktion $f \in \Gamma$ realisiert.

Definition 2.11. Ein Ω-Schaltkreis S ist die Ω-*Realisierung* einer Funktion $f \in B$ bzw. einer Funktionsmenge $\Gamma \subseteq B$, wenn er f bzw. Γ realisiert.

In diesem Fall wird S auch als *Realisierung* von f bzw. Γ bezeichnet.

Definition 2.12. Für einen Schaltkreis S mit Gattern $g_1, ..., g_k$ sei $C(S)$ definiert als

$$C(S) := k.$$

$C(S)$ wird als die *Komplexität* des Schaltkreises S bezeichnet.
[12, S.9]

Definition 2.13. Für $n \in \mathbb{N}$, eine $\mathbb{B}^{\mathbb{B}^n}$-vollständige Menge $\Omega \subseteq B$ und eine boolesche Funktion $f \in \mathbb{B}^{\mathbb{B}^n}$ sei $C_\Omega(f)$ definiert als

$$C_\Omega := \min\{C(S) \mid S \text{ ist } \Omega\text{-Schaltkreis und realisiert } f\}.$$

$C_\Omega(f)$ wird als die *Komplexität* der Funktion f bezüglich Ω bezeichnet.
[12, S.9]

Definition 2.14. Seien $\Omega, \Gamma \subseteq B$ und Ω vollständig bezüglich Γ. Dann ist $f \in \Gamma$ eine *komplexeste Funktion aus* Γ bezüglich Ω, wenn für alle $g \in \Gamma$ gilt, dass $C_\Omega(g) \leq C_\Omega(f)$.

Definition 2.15. Seien $A \subseteq \mathbb{R}$ eine Menge und $f : A \to \mathbb{R}$, dann sind die Mengen $O(f)$ und $o(f)$ definiert als

$$O(f) := \left\{ g : D \to \mathbb{R} \mid D \subseteq \mathbb{R},\ k \in \mathbb{R},\ \lim_{n\to\infty} \left|\frac{g}{f}\right| \leq k \right\},$$
$$o(f) := \left\{ g : D \to \mathbb{R} \mid D \subseteq \mathbb{R},\ \lim_{n\to\infty} \left|\frac{g}{f}\right| = 0 \right\}.$$

[12, S.17]

3 Verallgemeinerung von Shannons unterer Schranke

Shannons untere Schranke besagt, dass die Anzahl der n-stelligen booleschen Funktionen, deren Realisierung als Schaltkreis mehr als $\frac{2^n}{n}$ Gatter erfordert, für n gegen unendlich und $\left(\mathbb{B}^{\mathbb{B}^2} \cup \{0,1\}\right)$ als Menge der Basisfunktionen gegen die Anzahl aller n-stelligen Funktionen $\left|\mathbb{B}^{\mathbb{B}^n}\right| = 2^{2^n}$ konvergiert. In anderen Worten: Für wachsende n strebt die Wahrscheinlichkeit, dass eine zufällig gewählte n-stellige Funktion eine Komplexität bezüglich $\left(\mathbb{B}^{\mathbb{B}^2} \cup \{0,1\}\right)$ größer $\frac{2^n}{n}$ hat, gegen 1. Eine formalere Fassung findet sich in dem nachfolgenden Theorem.

Theorem 3.1 (Shannons untere Schranke).
Für $\Omega = \mathbb{B}^{\mathbb{B}^2} \cup \{0,1\}$ *gilt*

$$\lim_{n\to\infty} \frac{\left|\left\{f \in \mathbb{B}^{\mathbb{B}^n} : C_\Omega(f) \leq \frac{2^n}{n}\right\}\right|}{|\mathbb{B}^{\mathbb{B}^n}|} = 0.$$

[9, S.64]

Im weiteren Verlauf dieses Abschnittes soll Shannons untere Schranke dahingehend verallgemeinert werden, dass sich eine untere Schranke (im Sinne von Shannon) für die Komplexität boolescher Funktionen ergibt, die sich auf beliebige Folgen jeweils B_n-vollständiger Basismengen $(\Omega_n)_{n\in\mathbb{N}}$ bezieht, wobei jeweils $C_{\Omega_n}(f)$ das Maß der Komplexität einer n-stelligen Funktion $f \in B_n$ ist. Hierfür wird Shannons Abzählargument in der Variante aus Clotes und Kranakis Buch *Boolean Functions and Computation Models* [9] entsprechend verallgemeinert, indem Arität und Anzahl der gewählten Basisfunktionen als variabel betrachtet werden.

Definition 3.2. Es sei $F : (\mathbb{N} \times \mathbb{R} \times \mathbb{N} \times \mathbb{N}) \to \mathbb{N}$ definiert als

$$F(n,t,d,m) := \max\Big(\Big\{ |\{f \in B_n \ : \ C_\Gamma(f) \leq t\}| \ : \ \Gamma \subseteq B_d,\ |\Gamma| = m, \\ \Gamma \text{ vollständig bezüglich } B_n\Big\} \cup \{0\}\Big).$$

$F(n,t,d,m)$ beschreibt die Anzahl der Funktionen, die sich für die optimale Wahl einer B_n-vollständigen Menge mit genau m maximal d-stelligen Basisfunktionen aus B_n, als Schaltkreis mit maximal t Gattern realisieren lassen. Im Folgenden soll diese Funktion zur Verallgemeinerung von Shannons unterer Schranke genutzt werden. Die nachfolgenden Beobachtungen liefern einige Eigenschaften dieser Funktion, die für die Beweise in diesem Abschnitt sowie in Abschnitt 5 relevant sind.

Beobachtung 3.3. *Seien* $n,d,m \in \mathbb{N}$ *und* $t_1, t_2 \in \mathbb{R}$ *mit* $t_1 \leq t_2$, *dann gilt*

$$F(n,t_1,d,m) \ \leq \ F(n,t_2,d,m).$$

Beobachtung 3.4. *Seien* $n,d,m \in \mathbb{N}$ *und* $t \in \mathbb{R}$, *dann gilt*

$$F(n,t,d,m) \ = \ F(n,\lfloor t \rfloor,d,m).$$

Beobachtung 3.5. *Seien $n, m, d_1, d_2 \in \mathbb{N}$, und $t \in \mathbb{R}$ mit $d_1 \leq d_2$, dann gilt*

$$F(n, t, d_1, m) \;\leq\; F(n, t, d_2, m).$$

Beobachtung 3.6. *Seien $n, d, m_1, m_2 \in \mathbb{N}$ und $t \in \mathbb{R}$ mit $m_1 \leq m_2$, dann gilt*

$$F(n, t, d, m_1) \;\leq\; F(n, t, d, m_2).$$

Beobachtung 3.7. *Seien $d, m : \mathbb{N} \to \mathbb{N}$ und $t : \mathbb{N} \to \mathbb{R}$ monotone Funktionen. Dann existiert der Grenzwert $\lim_{n\to\infty} F(n, t(n), d(n), m(n))$ oder es gilt*

$$\lim_{n\to\infty} F(n, t(n), d(n), m(n)) \;=\; \infty.$$

Teil der Verallgemeinerung von Shannons unterer Schranke ist die Entwicklung einer oberen Schranke für den Grenzwert $\lim_{n\to\infty} F(n, t(n), d(n), m(n))$. Zur besseren Lesbarkeit dieser oberen Schranke sei im Folgenden die Funktion $\bar{F}$ definiert.

Definition 3.8. Es sei $\bar{F} : \left(\mathbb{N} \times \mathbb{R}_0^+ \times \mathbb{N} \times \mathbb{N}\right) \to \mathbb{R}_0^+$ definiert als

$$\bar{F}(n, t, d, m) \;:=\; m^t \cdot 2^{dt} \cdot t^{(d-1)\cdot t - \frac{1}{2}} \cdot e^t.$$

Beobachtung 3.9. *Seien $d, m : \mathbb{N} \to \mathbb{N}$ und $t : \mathbb{N} \to \mathbb{R}_0^+$ monotone Funktionen. Dann existiert der Grenzwert $\lim_{n\to\infty} \bar{F}(n, t(n), d(n), m(n))$ oder es gilt*

$$\lim_{n\to\infty} \bar{F}(n, t(n), d(n), m(n)) \;=\; \infty.$$

[redacted]

[redacted]

Beweis. Seien $n, t, d, m \in \mathbb{N}$ und Ω eine B_n-vollständige Menge mit $\Omega \subseteq B_d$ und $|\Omega| = m$. Die Anzahl der Funktionen $f \in B_n$, die sich durch einen Ω-Schaltkreis mit maximal t Gattern realisieren lassen, soll im Folgenden über die kombinatorischen Eigenschaften des Aufbaus eines solchen Schaltkreises abgeschätzt werden. Jeder Schaltkreis mit einer Ausgabevariablen, die die realisierte Funktion bestimmt, und weniger als t Gattern lässt sich durch das Hinzufügen von Gattern in einen Schaltkreis mit exakt t Gattern überführen, ohne dass sich die realisierte Funktion ändert. Daher genügt es für den Rest des Beweises Ω-Schaltkreise mit exakt t Gattern zu betrachten.
Jedes Gatter eines solchen Schaltkreises realisiert eine von m verschiedenen Funktionen aus Ω. Da $\Omega \subseteq B_d$, besitzt jedes dieser Gatter maximal d Eingänge. Für die Belegung jedes Einganges gibt es $t + 1 + n$ Möglichkeiten, namentlich: die $t - 1$ übrigen Gatter, die beiden Konstanten 0 und 1 sowie die n Eingabevariablen. Gleichzeitig gibt es $t!$ Möglichkeiten die Gatter durchzunummerieren, ohne dass sich die durch den Schaltkreis realisierte Funktion

ändert. Lediglich die Ausgabevariable muss angepasst werden.
Somit ergibt sich

$$F(n,t,d,m) \;\leq\; \frac{[m\cdot[t+1+n]^d]^t}{t!} \;=\; \frac{m^t\cdot[t+1+n]^{dt}}{t!}.$$

Seien nun $n_0 \in \mathbb{N}$ sowie $t,d,m:\mathbb{N}\to\mathbb{N}$ monotone Funktionen mit $d(n_0)\geq 2$ und $t(n)\geq n+1$ für alle $n\in\mathbb{N}$. Der Übersichtlichkeit halber seien weiterhin $t=t(n)$, $d=d(n)$ und $m=m(n)$. Dann folgt

$$F(n,t,d,m) \;\leq\; \frac{m^t\cdot[t+1+n]^{dt}}{t!} \;\leq\; \frac{m^t\cdot[2t]^{dt}}{t!} \;=\; \frac{m^t\cdot 2^{dt}\cdot t^{dt}}{t!}.$$

Die Anwendung der Stirlingformel $\lim\limits_{t\to\infty}\dfrac{t!}{\sqrt{2\pi}\left(\frac{t}{e}\right)^t\cdot\sqrt{t}} = 1$ [3] sowie der Beobachtungen 3.7 und 3.9 liefert somit

$$\begin{aligned}\lim_{n\to\infty} F(n,t,d,m) \;&\leq\; \lim_{n\to\infty}\frac{m^t\cdot 2^{dt}\cdot t^{dt}}{t!} \;\leq\; \lim_{n\to\infty}\frac{m^t\cdot 2^{dt}\cdot t^{dt}}{\left(\frac{t}{e}\right)^t\cdot\sqrt{t}}\\ &=\; \lim_{n\to\infty} m^t\cdot 2^{dt}\cdot t^{(d-1)\cdot t-\frac{1}{2}}\cdot e^t.\end{aligned}$$

Sei $\hat{t}:\mathbb{N}\to\mathbb{R}_0^+$ eine monotone, reellwertige Funktion mit $\hat{t}(n)\geq n$ für alle $n\in\mathbb{N}$ und sei der Übersichtlichkeit halber $\hat{t}=\hat{t}(n)$. Da $d:\mathbb{N}\to\mathbb{N}$ monoton ist und da $d(n_0)\geq 2$, gilt auch für alle $n\in\mathbb{N}$ mit $n\geq n_0$, dass $d(n)\geq 2$. Mit Beobachtung 3.4 folgt daraus

$$\begin{aligned}\lim_{n\to\infty} F(n,\hat{t},d,m) \;&=\; \lim_{n\to\infty} F(n,\lfloor\hat{t}\rfloor,d,m) \;\leq\; \lim_{n\to\infty} m^{\lfloor\hat{t}\rfloor}\cdot 2^{d\lfloor\hat{t}\rfloor}\cdot\lfloor\hat{t}\rfloor^{(d-1)\cdot\lfloor\hat{t}\rfloor-\frac{1}{2}}\cdot e^{\lfloor\hat{t}\rfloor}\\ &\leq\; \lim_{n\to\infty} m^{\hat{t}}\cdot 2^{d\hat{t}}\cdot\hat{t}^{(d-1)\cdot\hat{t}-\frac{1}{2}}\cdot e^{\hat{t}} \;=\; \lim_{n\to\infty}\bar{F}(n,\hat{t},d,m).\end{aligned}$$

Damit ist die Behauptung des Lemmas für den Fall $\hat{t}(n)\geq n+1$ gezeigt. Für den Fall, dass $n\in\mathbb{N}$ mit $\hat{t}(n)<n+1$ existiert, folgt die Behauptung aus Beobachtung 3.3.
[9, S.64] □

Seien $d,m:\mathbb{N}\to\mathbb{N}$ und $t:\mathbb{N}\to\mathbb{R}_0^+$ monotone Funktionen, so dass $n_0\in\mathbb{N}$ mit $d(n_0)\geq 2$ existiert und sei $(\Omega_i)_{i\in\mathbb{N}}$ eine Folge jeweils B_i-vollständiger Mengen mit $\Omega_i\subseteq B_{d(i)}$ und $|\Omega_i| = m(i)$ für alle $i\in\mathbb{N}$. Dann ist die Anzahl der n-stelligen Funktionen, die sich als Ω_n-Schaltkreis mit maximal $t(n)$ Gattern realisieren lassen, für n gegen unendlich gemäß obigem Lemma durch

$$\lim_{n\to\infty}\bar{F}(n,t(n),d(n),m(n))$$

beschränkt. Damit lässt sich eine Größe $t(n)$ abschätzen, mit der gilt, dass die Wahrscheinlichkeit, dass jede Ω_n-Realisierung einer zufällig gewählten Funktion $f\in B_n$ mehr als $t(n)$ Gatter benötigt, für wachsende n gegen 1 konvergiert. Das nachfolgende Theorem liefert die entsprechend verallgemeinerte Fassung von Shannons unterer Schranke.

[redacted]

$$\underset{n\to\infty}{\text{[redacted]}} \frac{\text{[redacted]}}{|B_n|} \text{[redacted]}$$

Beweis. Seien $x, d, m : \mathbb{N} \to \mathbb{N}^*$ monotone Funktionen, für die ein $n_0 \in \mathbb{N}$ mit $d(n_0) \geq 2$ existiert. Der Übersichtlichkeit halber seien im Folgenden $x = x(n)$, $d = d(n)$, $m = m(n)$ und $t = \frac{2^n}{x}$. Gemäß Lemma 3.10 gilt

$$\begin{aligned}
\lim_{n\to\infty} \ln \frac{F(n, \frac{2^n}{x}, d, m)}{|B_n|} &= \lim_{n\to\infty} \ln \frac{F(n,t,d,m)}{|B_n|} \leq \lim_{n\to\infty} \ln \frac{\bar{F}(n,t,d,m)}{|B_n|} \\
&= \lim_{n\to\infty} \ln \frac{m^t \cdot 2^{dt} \cdot t^{(d-1)\cdot t - \frac{1}{2}} \cdot e^t}{2^{2^n}} \\
&= \lim_{n\to\infty} t \cdot \ln(m) + dt \cdot \ln(2) + \left((d-1)\cdot t - \frac{1}{2}\right) \cdot \ln(t) + t - 2^n \cdot \ln(2) \\
&\leq \lim_{n\to\infty} t \cdot \ln(m) + dt \cdot \ln(2) + (d-1)\cdot t \cdot \ln(t) + t - 2^n \cdot \ln(2) \\
&= \lim_{n\to\infty} t \cdot \Big[\ln(m) + d \cdot \ln(2) + (d-1)\cdot \ln(t) + 1\Big] - 2^n \cdot \ln(2) \\
&= \lim_{n\to\infty} \frac{2^n}{x} \cdot \left[\ln(m) + d \cdot \ln(2) + (d-1)\cdot \ln\left(\frac{2^n}{x}\right) + 1\right] - 2^n \cdot \ln(2) \\
&= \lim_{n\to\infty} 2^n \cdot \left[\frac{\ln(m) + d\cdot\ln(2) + (d-1)\cdot(n\cdot\ln(2) - \ln(x)) + 1}{x} - \ln(2)\right].
\end{aligned}$$

Für eine positive Konstante $C \in \mathbb{R}$ mit $0 < C < \ln(2)$ und $x = \dfrac{\ln(2)\cdot d\cdot n + \ln(m)}{C}$ folgt daraus

$$\begin{aligned}
\lim_{n\to\infty} \ln \frac{F\left(n, \frac{2^n}{x}, d, m\right)}{|B_n|} &= \lim_{n\to\infty} \ln \frac{F\left(n, C\cdot \frac{2^n}{\ln(2)\cdot d\cdot n + \ln(m)}, d, m\right)}{|B_n|} \\
&\leq \lim_{n\to\infty} 2^n \cdot \left[C \cdot \frac{\ln(m) + d\cdot\ln(2) + (d-1)\cdot(n\cdot\ln(2) - \ln(x)) + 1}{\ln(2)\cdot d\cdot n + \ln(m)} - \ln(2)\right] \\
&\leq \lim_{n\to\infty} 2^n \cdot \left[C \cdot \frac{\ln(m) + d\cdot n\cdot\ln(2)}{\ln(2)\cdot d\cdot n + \ln(m)} - \ln(2)\right] \\
&= \lim_{n\to\infty} 2^n \cdot [C - \ln(2)] \\
&= -\infty.
\end{aligned}$$

Somit gilt auch

$$\lim_{n\to\infty} \frac{F\left(n, C\cdot \frac{2^n}{\ln(2)\cdot d\cdot n + \ln(m)}, d, m\right)}{|B_n|} = 0$$

und die Behauptung des Theorems ist für den Fall $C > 0$ und die oben gewählte Funktion d bewiesen. Für den Fall $C = 0$ und obiges d folgt die Behauptung aus Beobachtung 3.3. Für den Fall $C \in \mathbb{R}$ mit $0 \leq C < \ln(2)$ und eine monotone Funktion $d : \mathbb{N} \to \mathbb{N}^*$, für die kein $n_0 \in \mathbb{N}$ mit $d(n_0) \geq 2$ existiert, folgt die Behauptung aus Beobachtung 3.5.
[9, S.64] □

4 Eine obere Schranke durch Multiplexer

In diesem Abschnitt soll der [redacted] großer Multiplexer auf die Komplexität boolescher Funktionen untersucht werden. Konkret soll gezeigt werden, dass die Nutzung von Multiplexern mit $d(n)$ Steuereingängen, für eine monoton wachsende und unbeschränkte Funktion $d : \mathbb{N}^* \to \mathbb{N}^*$ mit $d(n) < n$, die Realisierung jeder beliebigen maximal n-stelligen Funktion in Form eines Schaltkreises mit

$$(1 + o(1)) \cdot \frac{2^{n+1}}{2^{d(n)} \cdot (n - d(n))}$$

Gattern erlaubt. Die Vorgehensweise folgt dabei dem Beweis eines Satzes aus dem Skript *Boolean Circuit Complexity* von [redacted] [10]. Dieser Satz besagt, dass sich jede n-stellige boolesche Funktion als $\left(\mathbb{B}^{\mathbb{B}^2} \cup \{0,1\}\right)$-Schaltkreis mit $O\left(\frac{2^n}{n}\right)$ Gattern darstellen lässt. Um dies zu zeigen, wählt [redacted] $\left(\mathbb{B}^{\mathbb{B}^2} \cup \{0,1\}\right)$ als Basismenge und schätzt zum einen die maximale Größe für den Schaltkreis einer $(n-k)$-stelligen Funktion ab und zum anderen die Größe eines Schaltkreises für die Menge aller k-stelligen booleschen Funktionen. Weiterhin zeigt [redacted] wie sich durch geschickte Wahl des Parameters k daraus ein Schaltkreis mit $O\left(\frac{2^n}{n}\right)$ Gattern konstruieren lässt [10, S.3].
In Anlehnung an diese Beweisidee gliedert sich dieser Abschnitt in drei Teile. Zunächst soll jeweils die Anzahl an Multiplexern mit d Steuereingängen (d-Multiplexer) ermittelt werden, die notwendig ist, um einen n-Multiplexer beziehungsweise einen Schaltkreis für die Menge aller n-stelligen Funktionen zu konstruieren. Aufbauend auf den Ergebnissen dieser beider Teilabschnitte soll anschließend, dem Beweis von Pe'er folgend, ein Schaltkreis für eine beliebige n-stellige Funktion konstruiert und ein Parameter k ermittelt werden, mit dem sich für diesen Schaltkreis eine Größe von

$$(1 + o(1)) \cdot \frac{2^{n+1}}{2^{d(n)} \cdot (n - d(n))}$$

Gattern ergibt.

Um jedoch die Zusammensetzbarkeit von Multiplexern untersuchen zu können, muss der oben intuitiv benutzte Begriff des Multiplexers zunächst noch formaler gefasst werden.

Definition 4.1. Es sei $dec : \bigcup_{n \in \mathbb{N}^*} \mathbb{B}^n \to \mathbb{N}$ definiert als

$$dec(x_1, \ldots, x_n) := \sum_{j=1}^{n} x_j \cdot 2^{j-1}.$$

Definition 4.2. Für $n \in \mathbb{N}^*$ ist ein *n-Multiplexer* eine boolesche Funktion $f : \mathbb{B}^n \times \mathbb{B}^{2^n} \to \mathbb{B}$, für die gilt

$$f(s_1, \ldots, s_n, a_1, \ldots, a_{2^n}) = a_{dec(s_1, \ldots, s_n)+1}.$$

Weiterhin bezeichnet mux_n einen n-Multiplexer.

Bei einem n-Multiplexer $mux_n(s_1, ...s_n, a_1, ..., a_{2^n})$ handelt es sich folglich entsprechend der Intuition um eine $(2^n + n)$-stellige Funktion, die für Steuerwerte $s_1, ..., s_n \in \{0, 1\}$ und Datenwerte $a_1, ..., a_{2^n} \in \{0, 1\}$ den Datenwert $a_{dec(s_1,...,s_n)+1}$ annimmt, dessen Index durch den Vektor $(s_1, ..., s_n)$ kodiert wird. Folglich lässt sich jede n-stellige Funktion $f \in \mathbb{B}^{\mathbb{B}^n}$ durch einen n-Multiplexer realisieren, der für die Steuereingänge $s_1, ...s_n$ den Datenwert $f(s_1, ..., s_n)$ durchschaltet.

Beobachtung 4.3. *Sei $n \in \mathbb{N}^*$ und $f \in \mathbb{B}^{\mathbb{B}^n}$, dann lässt sich f wie folgt unter Verwendung eines n-Multiplexers sowie der Konstanten 0 und 1 darstellen*

$$f(x_1, ..., x_n) \;=\; mux_n(x_1, ..., x_n,\ f(0, ..., 0), ..., f(1, ..., 1)).$$

Folglich lässt sich auch jede maximal n-stellige Funktion $f \in B_n$ durch einen n-Multiplexer sowie die Konstanten 0 und 1 realisieren. Es reicht aus, in der Konstruktion aus Beobachtung 4.3 die nicht benötigten Steuer- und Dateneingänge des Multiplexers auf 0 zu setzen.

Beobachtung 4.4. *Seien $m, n \in \mathbb{N}^*$ mit $m \leq n$ und $f \in \mathbb{B}^{\mathbb{B}^m}$, dann lässt sich f wie folgt unter Verwendung eines n-Multiplexers sowie der Konstanten 0 und 1 darstellen*

$$f(x_1, ..., x_m) \;=\; mux_n(x_1, ..., x_m, \underbrace{0, ..., 0}_{n-m},\ f(0, ..., 0), ..., f(1, ..., 1), \underbrace{0, ..., 0}_{2^n-2^m}).$$

Diese Konstruktionen alleine erlaubt es jedoch lediglich mittels eines n-Multiplexers Funktionen der Stelligkeit kleiner gleich n zu konstruieren. Um mit Hilfe der Beobachtungen 4.3 und 4.4 Schaltkreise für Funktionen größerer Stelligkeit angeben zu können, ist es notwendig die Zusammensetzbarkeit größerer Multiplexer aus kleineren zu untersuchen.

Lemma 4.5. *Seien $n, m \in \mathbb{N}^*$. Dann handelt es sich bei der Funktion*

$$\begin{aligned} h(s_1, ..., s_{n+m}, a_1, ..., a_{2^{n+m}}) \;=\; mux_m(s_{n+1}, ..., s_{n+m},\ & mux_n(s_1, ..., s_n,\ a_1, ..., a_{2^n}),\ ..., \\ & mux_n(s_1, ..., s_n,\ a_{(2^m-1)\cdot 2^n+1}, ..., a_{2^{n+m}})) \end{aligned}$$

um einen $(n + m)$-Multiplexer.

Beweis. Seien $n, m \in \mathbb{N}^*$ und h wie im Lemma definiert. Seien weiterhin $s_1, ..., s_{m+n}$, $a_1, ..., a_{2^{m+n}} \in \{0, 1\}$. Gemäß Definition 4.2 handelt es sich bei h genau dann um einen $(m + n)$-Multiplexer, wenn gilt

$$h(s_1, ..., s_{m+n},\ a_1, ..., a_{2^{m+n}}) \;=\; a_{dec(s_1,...,s_{m+n})+1}.$$

Seien $S_n := (s_1, ..., s_n)$, $S_m := (s_{n+1}, ..., s_{n+m})$ sowie $A_j := (a_{(j-1)\cdot 2^n+1},\ ...,\ a_{j\cdot 2^n})$ für alle $j \in \{1, ..., 2^m\}$. Gemäß Definition 4.2 gilt damit

$$\begin{aligned} h(s_1, ..., s_{n+m},\ a_1, ..., a_{2^{n+m}}) &= h(S_n, S_m, A_1, ..., A_{2^m}) \\ &= mux_m(S_m,\ mux_n(S_n, A_1), ..., mux_n(S_n, A_{2^m})) \\ &= mux_n(S_n,\ A_{dec(S_m)+1}) \\ &= mux_n(S_n,\ a_{dec(S_m)\cdot 2^n+1}, ..., a_{dec(S_m)\cdot 2^n+2^n}) \\ &= a_{dec(S_m)\cdot 2^n+dec(S_n)+1} \\ &= a_{dec(S_n,S_m)+1} \\ &= a_{dec(s_1,...,s_{n+m})+1} \end{aligned}$$

Somit handelt es sich bei h um einen $(n + m)$-Multiplexer. □

Ein $(d+m)$-Multiplexer lässt sich also o.B.d.A. aus einem m-Multiplexer und 2^m d-Multiplexern aufbauen. Durch induktive Fortsetzung dieses Vorgehens und $d = m$ wird klar, dass sich aus einem d-Multiplexer jeder größere Multiplexer zusammensetzen lässt, dessen Anzahl an Steuereingängen einem Vielfachen von d entspricht. Die exakte Anzahl an d-Multiplexern, die für die Konstruktion eines $(q \cdot d)$-Multiplexers nötig ist, liefert das nachfolgende Lemma.

Lemma 4.6. *Für $q, d \in \mathbb{N}^*$ lässt sich ein $(q \cdot d)$-Multiplexer aus $\frac{2^{q \cdot d} - 1}{2^d - 1}$ d-Multiplexern zusammensetzen.*

Beweis. Der Beweis erfolgt per Induktion über q. Sei $d \in \mathbb{N}^*$.

<u>Induktionsanfang:</u> Für $q = 1$ gilt $\frac{2^{q \cdot d} - 1}{2^d - 1} = 1$.

<u>Induktionsannahme:</u> Es existiert ein $q \in \mathbb{N}^*$, für das sich ein $(q \cdot d)$-Multiplexer aus $\frac{2^{q \cdot d} - 1}{2^d - 1}$ d-Multiplexern zusammensetzen lässt.

<u>Induktionsschritt:</u> Es sei angenommen die Induktionsannahme gilt für $q \in \mathbb{N}^*$. Gemäß Lemma 4.5 lässt sich ein $((q+1) \cdot d)$-Multiplexer aus einem d-Multiplexer und 2^d $(q \cdot d)$-Multiplexern konstruieren. Somit lässt sich ein $((q+1) \cdot d)$-Multiplexer aus insgesamt

$$1 + 2^d \cdot \frac{2^{q \cdot d} - 1}{2^d - 1} = \frac{2^{(q+1) \cdot d} - 2^d + 2^d - 1}{2^d - 1} = \frac{2^{(q+1) \cdot d} - 1}{2^d - 1}$$

d-Multiplexern zusammensetzen.

Folglich lässt sich für alle $q, d \in \mathbb{N}^*$ ein $(q \cdot d)$-Multiplexer mittels $\frac{2^{(q+1) \cdot d} - 1}{2^d - 1}$ d-Multiplexern realisieren. □

Boolesche Funktionen der Stelligkeit $n = q \cdot d + r$ mit $0 < r < d$ lassen sich nach Lemma 4.5 durch einen r-Multiplexer und 2^r $(q \cdot d)$-Multiplexer realisieren. Lemma 4.6 gibt Aufschluss über die Anzahl an d-Multiplexern, die für die Konstruktion eines einzelnen $(q \cdot d)$-Multiplexers benötigt werden. Für die Konstruktion eines r-Multiplexers genügen hingegen ein einzelner d-Multiplexer sowie die Konstante 0, denn es reicht aus, die nicht benötigten Steuer- und Dateneingänge auf 0 zu setzen. Das nachfolgende Korollar 4.9 bietet eine formalere Abschätzung der Anzahl an d-Multiplexern, die für die Realisierung eines n-Multiplexers nötig ist. Zuvor soll jedoch eine Notation eingeführt werden, die die Darstellung der nachfolgenden Schranken vereinfacht.

Definition 4.7. Für $d \in \mathbb{N}^*$, sei $r_d : \mathbb{R}_0^+ \to \mathbb{N}$ definiert als

$$r_d(n) := \left\lceil n - \left\lfloor \frac{n}{d} \right\rfloor \cdot d \right\rceil.$$

Beobachtung 4.8. *Seien $n, q, r \in \mathbb{N}$ und $d \in \mathbb{N}^*$ mit $0 \leq r < d$ und $n = q \cdot d + r$. Dann gilt $r = r_d(n)$.*

Korollar 4.9. *Seien $n, d \in \mathbb{N}^*$ mit $n \geq d$, dann lässt sich ein n-Multiplexer als $\{mux_d, 0\}$-Schaltkreis mit maximal $\dfrac{2^n - 2^{r_d(n)}}{2^d - 1} + 2$ Gattern realisieren (darunter maximal $\frac{2^n - 2^{r_d(n)}}{2^d - 1} + 1$ mux_d-Gatter).*

Beweis. Seien $n, d \in \mathbb{N}^*$ mit $n \geq d$. Es gibt eindeutige $q, r \in \mathbb{N}$ mit $q \geq 1$ und $r < d$, für die $n = q \cdot d + r$ gilt. Zusätzlich gilt nach Beobachtung 4.8, dass $r = r_d(n)$. Falls $r = 0$ folgt die Behauptung aus Lemma 4.6. Daher sei für den weiteren Beweis $r > 0$ angenommen.

Ein r-Multiplexer lässt sich mit Hilfe eines mux_d-Gatters sowie der Konstante 0 realisieren, denn es gilt

$$mux_r(s_1, \ldots, s_r,\ a_1, \ldots, a_{2^r}) \;=\; mux_d(s_1, \ldots, s_r, \underbrace{0, \ldots, 0}_{d-r},\ a_1, \ldots, a_{2^r}, \underbrace{0, \ldots, 0}_{2^d - 2^r}).$$

Weiterhin lässt sich ein n-Multiplexer gemäß Lemma 4.5 aus einem r-Multiplexer und 2^r $(q \cdot d)$-Multiplexern zusammensetzen. Nach Lemma 4.6 benötigt die Realisierung eines $(q \cdot d)$-Multiplexers $\dfrac{2^{q \cdot d} - 1}{2^d - 1}$ mux_d-Gatter. Der resultierende Gesamtschaltkreis besteht folglich aus

$$1 + 2^r \cdot \frac{2^{q \cdot d} - 1}{2^d - 1} \;=\; 1 + \frac{2^{q \cdot d + r} - 2^r}{2^d - 1} \;=\; 1 + \frac{2^n - 2^{r_d(n)}}{2^d - 1}$$

mux_d-Gattern sowie aus der Konstante 0. □

Nachdem nun feststeht, dass $\dfrac{2^n - 2^{r_d(n)}}{2^d - 1} + 1$ d-Multiplexer genügen, um jede beliebige n-stellige Funktion zu konstruieren, stellt sich – wie zu Beginn dieses Abschnitts besprochen – die Frage wie viele d-Multiplexer nötig sind, um alle booleschen Funktionen der Stelligkeit n in Form eines einzelnen $\{mux_d, 0, 1\}$-Schaltkreises zu realisieren. Dabei soll zunächst die Konstruktion eines Schaltkreises für alle $(q \cdot d)$-stelligen Funktionen untersucht werden, bevor das Resultat auf die Menge der n-stelligen Funktionen verallgemeinert wird.

Lemma 4.10. *Für $q, d \in \mathbb{N}^*$ lässt sich $\mathbb{B}^{\mathbb{B}^{q \cdot d}}$ als ein $\{mux_d, 0, 1\}$ Schaltkreis mit maximal*

$$2^{2^{q \cdot d}} + \frac{2^{2^{q \cdot d}}}{2^{(q+1) \cdot d}} + 6$$

Gattern realisieren.

Beweis. Sei $d \in \mathbb{N}^*$. Der Beweis erfolgt per Induktion über q.

<u>Induktionsanfang:</u> Da der Induktionsschritt voraussetzt, dass die Behauptung für alle $q \in \mathbb{N}^*$ mit $q \leq 3$ gilt, sollen diese drei Fälle zunächst untersucht werden.
<u>1. Fall:</u> $q = 1$
Unter Verwendung der kanonischen Form aus Beobachtung 4.3 lässt sich $\mathbb{B}^{\mathbb{B}^d}$ als $\{mux_d, 0, 1\}$-Schaltkreis mit $2^{2^d} + 2$ Gattern realisieren und für $q = 1$ gilt

$$2^{2^d} + 2 \;<\; 2^{2^d}\left(1 + \frac{1}{2^{2d}}\right) + 6 \;=\; 2^{2^{qd}}\left(1 + \frac{1}{2^{(q+1)d}}\right) + 6 \;=\; 2^{2^{qd}} + \frac{2^{2^{qd}}}{2^{(q+1)d}} + 6.$$

2. Fall: $q = 2$

$\mathbb{B}^{\mathbb{B}^{2d}}$ lässt sich unter Verwendung des Schaltkreises für $\mathbb{B}^{\mathbb{B}^{d}}$ ebenfalls gemäß der Konstruktion aus Beobachtung 4.3 realisieren. Seien $f \in \mathbb{B}^{\mathbb{B}^{2d}}$ und $a_i(x_1, \ldots, x_d) = f(dec^{-1}(i-1), x_1, \ldots, x_d) \in \mathbb{B}^{\mathbb{B}^{d}}$ für $i \in \{1, \ldots, 2^d\}$. Dann gilt

$$f(x_1, \ldots, x_{2d}) \;=\; mux_d(x_1, \ldots, x_d,\; a_1(x_{d+1}, \ldots, x_{2d}), \ldots, a_{2^d}(x_{d+1}, \ldots, x_{2d}))$$

Folglich benötigt die Realisierung einer einzelnen $(2d)$-stelligen Funktion ein zusätzliches mux_d-Gatter. Demnach benötigt der resultierende $\{mux_d, 0, 1\}$-Schaltkreis zur Realisierung aller $(2d)$-stelligen Funktionen $2^{2^{2d}}$ zusätzliche mux_d-Gatter. Somit besteht er insgesamt aus maximal $\sum_{j=1}^{2} 2^{2^{j\cdot d}} + 2$ Gattern. Für $q = 2$ und $d = 1$ folgt damit

$$\sum_{j=1}^{2} 2^{2^{j\cdot d}} + 2 \;=\; 22 \;<\; 24 \;=\; 2^{2^{q\cdot d}} + \frac{2^{2^{q\cdot d}}}{2^{(q+1)\cdot d}} + 6$$

und für $d \geq 2$ folgt

$$\begin{aligned}\sum_{j=1}^{2} 2^{2^{j\cdot d}} + 2 \;&=\; 2^{2^{2d}} + 2^{2^{d}} + 2 \;\leq\; 2^{2^{2d}} + 2^{2^{d}+2^{d}+2-3d} + 2 \;<\; 2^{2^{2d}} + 2^{2^{2d}-3d} \\ &<\; 2^{2^{q\cdot d}} + \frac{2^{2^{q\cdot d}}}{2^{(q+1)\cdot d}} + 6.\end{aligned}$$

3. Fall: $q = 3$

Der Fall $q = 3$ verläuft weitgehend analog zum Fall $q = 2$. Für die Konstruktion von $\mathbb{B}^{\mathbb{B}^{3d}}$ lässt sich der Schaltkreis für $\mathbb{B}^{\mathbb{B}^{2d}}$ verwenden. Der resultierende Gesamtschaltkreis besteht folglich aus $\sum_{j=1}^{3} 2^{2^{j\cdot d}} + 2$ Gattern. Für $q = 3$ und $d = 1$ gilt

$$\sum_{j=1}^{3} 2^{2^{j\cdot d}} + 2 \;=\; 278 \;=\; 2^{2^{q\cdot d}} + \frac{2^{2^{q\cdot d}}}{2^{(q+1)\cdot d}} + 6$$

und für $d \geq 2$ gilt

$$\begin{aligned}\sum_{j=1}^{3} 2^{2^{j\cdot d}} + 2 \;&<\; 2^{2^{3d}} + 2^{2^{2d}+1} \;\leq\; 2^{2^{3d}} + 2^{2^{2d}+1+2^{d+1}-4d} \\ &<\; 2^{2^{3d}} + 2^{2^{3d}-4d} \;<\; 2^{2^{q\cdot d}} + \frac{2^{2^{q\cdot d}}}{2^{(q+1)\cdot d}} + 6.\end{aligned}$$

Induktionsannahme: Es existiert ein $q \in \mathbb{N}^*$ mit $q \geq 3$, für das sich $\mathbb{B}^{\mathbb{B}^{q\cdot d}}$ als $\{mux_d, 0, 1\}$-Schaltkreis mit $2^{2^{q\cdot d}} + \frac{2^{2^{q\cdot d}}}{2^{(q+1)\cdot d}} + 6$ Gattern realisieren lässt.

Induktionsschritt: Es sei angenommen die Induktionsannahme gilt für $q \in \mathbb{N}^*$ mit $q \geq 3$. $\mathbb{B}^{\mathbb{B}^{(q+1)\cdot d}}$ lässt sich unter Verwendung des Schaltkreises für $\mathbb{B}^{\mathbb{B}^{q\cdot d}}$ als $\{mux_d, 0, 1\}$-Schaltkreis mit $2^{2^{(q+1)\cdot d}}$ zusätzlichen mux_d-Gattern realisieren. Als Gesamtgatteranzahl ergibt sich folglich

$$\begin{aligned} 2^{2^{q\cdot d}} + \frac{2^{2^{q\cdot d}}}{2^{(q+1)\cdot d}} + 6 + 2^{2^{(q+1)\cdot d}} &< 2^{2^{q\cdot d}+1} + 2^{2^{(q+1)\cdot d}} = 2^{2^{q\cdot d}+1+(q+2)\cdot d-(q+2)\cdot d} + 2^{2^{(q+1)\cdot d}} \\ &< 2^{2^{(q+1)\cdot d}-(q+2)\cdot d} + 2^{2^{(q+1)\cdot d}} < 2^{2^{(q+1)\cdot d}} + \frac{2^{2^{(q+1)\cdot d}}}{2^{(q+2)\cdot d}} + 6. \end{aligned}$$

Somit gilt die Behauptung für alle $q, d \in \mathbb{N}^*$. □

Es genügen folglich $2^{2^{q\cdot d}} + \frac{2^{2^{q\cdot d}}}{2^{(q+1)\cdot d}} + 6$ mux_d-Gatter um die Menge aller $(q \cdot d)$-stelligen Funktionen in Form eines $\{mux_d, 0, 1\}$-Schaltkreises zu realisieren. Eine ähnliche obere Schranke lässt sich für die Menge der $(q \cdot d + r)$-stelligen Funktionen mit $0 < r < d$ angeben, deren Stelligkeit nicht durch d teilbar ist.

Lemma 4.11. *Für $q, d, r \in \mathbb{N}^*$ mit $0 < r < d$ lässt sich $\mathbb{B}^{\mathbb{B}^{q\cdot d+r}}$ als ein $\{mux_d, 0, 1\}$-Schaltkreis mit maximal*

$$2^{2^{q\cdot d+r}} + \frac{2^{2^{q\cdot d+r}}}{2^{q\cdot d+2r}} + 22$$

Gattern realisieren.

Beweis. Seien $q, d, r \in \mathbb{N}^*$ mit $0 < r < d$. Gemäß Lemma 4.10 lässt sich $\mathbb{B}^{\mathbb{B}^{q\cdot d}}$ als $\{mux_d, 0, 1\}$-Schaltkreis mit maximal $2^{2^{q\cdot d}} + \frac{2^{2^{q\cdot d}}}{2^{(q+1)\cdot d}} + 6$ Gattern realisieren. Durch die Konstruktion aus Beobachtung 4.4 und den Schaltkreis für $\mathbb{B}^{\mathbb{B}^{q\cdot d}}$ lässt sich folglich ein $\{mux_d, 0, 1\}$-Schaltkreis für $\mathbb{B}^{\mathbb{B}^{q\cdot d+r}}$ mit maximal

$$2^{2^{q\cdot d+r}} + 2^{2^{q\cdot d}} + \frac{2^{2^{q\cdot d}}}{2^{(q+1)\cdot d}} + 6 < 2^{2^{q\cdot d+r}} + 2^{2^{q\cdot d}+1} + 6$$

Gattern konstruieren. Es bleibt nun also noch $2^{2^{q\cdot d}+1} \leq \frac{2^{2^{q\cdot d+r}}}{2^{q\cdot d+2r}} + 16$ zu zeigen. Für $q = r = 1$ und $d = 2$ gilt

$$2^{2^{q\cdot d}+1} = 32 = \frac{2^{2^{q\cdot d+r}}}{2^{q\cdot d+2r}} + 16.$$

Weiterhin ist die Differenz der Exponenten der rechten und den linken Seite der Ungleichung streng monoton steigend, denn es gilt

$$
\begin{aligned}
\partial_q\left(2^{q\cdot d+r} - q\cdot d - 2r \;-\; 2^{q\cdot d} - 1\right) &= 2^{q\cdot d+r}\cdot\ln(2)\cdot d \;-\; d \;-\; 2^{q\cdot d}\cdot\ln(2)\cdot d \\
&= d\cdot\left(2^{q\cdot d}\cdot\ln(2)\cdot(2^r-1)-1\right) \\
&> 0, \\
\partial_d\left(2^{q\cdot d+r} - q\cdot d - 2r \;-\; 2^{q\cdot d} - 1\right) &= 2^{q\cdot d+r}\cdot\ln(2)\cdot q \;-\; q \;-\; 2^{q\cdot d}\cdot\ln(2)\cdot q \\
&= q\cdot\left(2^{q\cdot d}\cdot\ln(2)\cdot(2^r-1)-1\right) \\
&> 0, \\
\partial_r\left(2^{q\cdot d+r} - q\cdot d - 2r \;-\; 2^{q\cdot d} - 1\right) &= 2^{q\cdot d+r}\cdot\ln(2) \;-\; 2 \\
&> 0.
\end{aligned}
$$

Damit ist auch die Differenz $\frac{2^{2^{q\cdot d+r}}}{2^{q\cdot d+2r}} + 16 \;-\; 2^{2^{q\cdot d}+1}$ streng monoton steigend und es folgt für alle $q,d,r \in \mathbb{N}^*$ mit $0 < r < d$ die Ungleichung $2^{2^{q\cdot d}+1} \leq \frac{2^{2^{q\cdot d+r}}}{2^{q\cdot d+2r}} + 16$. Damit gilt auch

$$2^{2^{q\cdot d+r}} + 2^{2^{q\cdot d}} + \frac{2^{2^{q\cdot d}}}{2^{(q+1)\cdot d}} + 6 \quad<\quad 2^{2^{q\cdot d+r}} + 2^{2^{q\cdot d}+1} + 6 \quad\leq\quad \frac{2^{2^{q\cdot d+r}}}{2^{q\cdot d+2r}} + 22$$

und die Behauptung des Lemmas ist für alle $q,d,r \in \mathbb{N}^*$ mit $0 < r < d$ gezeigt. □

Soll ein $\{mux_d, 0, 1\}$-Schaltkreis für die Menge der n-stelligen booleschen Funktionen konstruiert werden und ist $n = q\cdot d$ ein Vielfaches der Anzahl an Steuereingängen d der zur Verfügung stehenden Multiplexer, so genügt folglich die Verwendung von $2^{2^n} + \frac{2^{2^n}}{2^{n+d}} + 6$ mux_d-Gattern. Gleichzeitig sind für eine Stelligkeit $n = q\cdot d + r$ mit $0 < r < d$, die nicht durch d teilbar ist, maximal $2^{2^n} + \frac{2^{2^n}}{2^{n+r_d(n)}} + 22$ mux_d-Gatter notwendig.

Somit lässt sich in beiden Fällen eine obere Schranke von $2^{2^n} + \frac{2^{2^n}}{2^{n+x}} + C$ angeben, wobei es sich bei C beides mal um eine asymptotisch zu vernachlässigende Konstante handelt. Asymptotisch relevant ist jedoch der Faktor x, der jeweils auf d beziehungsweise $r_d(n)$ zu setzen ist. Grund dafür ist, dass d – wie zu Beginn des Abschnitts besprochen – letztendlich durch eine monoton wachsende und unbeschränkte Funktion $d(n)$ ersetzt werden soll. Im Falle eines Vielfachen n von d als Stelligkeit teilt sich somit der zweite Summand $\frac{2^{2^n}}{2^n}$ durch 2^d, ansonsten lediglich durch $2^{r_d(n)}$. Um jedoch die Anzahl an Gattern abschätzen zu können, die für die Realisierung von $\mathbb{B}^{\mathbb{B}^n}$ mit beliebigem $n \in \mathbb{N}$ notwendig ist, muss für beide Fälle eine gemeinsame obere Schranke gefunden werden. Diese liefert das nachfolgende Korollar.

Korollar 4.12. *Für $n,d \in \mathbb{N}^*$ lässt sich $\mathbb{B}^{\mathbb{B}^n}$ als ein $\{mux_d, 0, 1\}$-Schaltkreis mit maximal*

$$2^{2^n} + \frac{2^{2^n}}{2^{n+r_d(n)+\left(2^{-r_d(n)\cdot d}-2^{-d}\right)\cdot d}} + 22$$

Gattern realisieren.

Beweis. Seien $n, d \in \mathbb{N}^*$, dann gibt es eindeutig bestimmte $q, r \in \mathbb{N}$ mit $r < d$ und $n = q \cdot d + r$. Für $r = 0$ lässt sich $\mathbb{B}^{\mathbb{B}^n}$ gemäß Lemma 4.10 als $\{mux_d, 0, 1\}$-Schaltkreis mit maximal $2^{2^{q\cdot d}} + \dfrac{2^{2^{q\cdot d}}}{2^{(q+1)\cdot d}} + 6$ Gattern realisieren und es gilt

$$
\begin{aligned}
2^{2^{q\cdot d}} + \frac{2^{2^{q\cdot d}}}{2^{(q+1)\cdot d}} + 6 \;&=\; 2^{2^n} + \frac{2^{2^n}}{2^{n+d}} + 6 \;=\; 2^{2^n} + \frac{2^{2^n}}{2^{n+r+2^{-r\cdot d}\cdot d}} + 6 \\
&< \; 2^{2^n} + \frac{2^{2^n}}{2^{n+r+2^{-r\cdot d}\cdot d - 2^{-d}\cdot d}} + 22 \;=\; 2^{2^n} + \frac{2^{2^n}}{2^{n+r+\left(2^{-r\cdot d}-2^{-d}\right)\cdot d}} + 22 \\
&= \; 2^{2^n} + \frac{2^{2^n}}{2^{n+r_d(n)+\left(2^{-r_d(n)\cdot d}-2^{-d}\right)\cdot d}} + 22.
\end{aligned}
$$

Für $r > 0$ lässt sich $\mathbb{B}^{\mathbb{B}^n}$ gemäß Lemma 4.11 als $\{mux_d, 0, 1\}$-Schaltkreis mit maximal $2^{2^{q\cdot d+r}} + \dfrac{2^{2^{q\cdot d+r}}}{2^{q\cdot d+2r}} + 22$ Gattern realisieren und es gilt

$$
\begin{aligned}
2^{2^{q\cdot d+r}} + \frac{2^{2^{q\cdot d+r}}}{2^{q\cdot d+2r}} + 22 \;&=\; 2^{2^n} + \frac{2^{2^n}}{2^{n+r}} + 22 \;\le\; 2^{2^n} + \frac{2^{2^n}}{2^{n+r+\left(2^{-r\cdot d}-2^{-d}\right)\cdot d}} + 22 \\
&= \; 2^{2^n} + \frac{2^{2^n}}{2^{n+r_d(n)+\left(2^{-r_d(n)\cdot d}-2^{-d}\right)\cdot d}} + 22.
\end{aligned}
$$

Folglich gilt die Behauptung des Korollars für alle $n, d \in \mathbb{N}^*$. □

Lemma 4.13. *Seien $n \in \mathbb{R}_0^+$ und $d \in \mathbb{N}^*$, dann gilt*

$$
r_d(n) + (2^{-r_d(n)\cdot d} - 2^{-d}) \cdot d \;\ge\; \frac{1}{2}.
$$

Beweis. Seien $n \in \mathbb{R}_0^+$ und $d \in \mathbb{N}^*$ sowie $r = r_d(n) \in \mathbb{N}$. Es gilt $\frac{d}{2^d} \le \frac{1}{2}$. Damit folgt für $r = 0$

$$
r + \left(2^{-r\cdot d} - 2^{-d}\right) \cdot d \;=\; \left(1 - 2^{-d}\right) \cdot d \;\ge\; \left(1 - \frac{1}{2}\right) \cdot d \;\ge\; \frac{1}{2}
$$

und für $r \ge 1$

$$
r + \left(2^{-r\cdot d} - 2^{-d}\right) \cdot d \;>\; r - \frac{d}{2^d} \;\ge\; r - \frac{1}{2} \;\ge\; \frac{1}{2}.
$$

□

[redacted]

Beweis. Seien $n, k, d \in \mathbb{N}^*$ mit $k, d < n$ und $f \in \mathbb{B}^{\mathbb{B}^n}$ eine n-stellige boolesche Funktion. Dann lässt sich f durch einen $(n-k)$-Multiplexer und 2^{n-k} k-stellige Funktionen $a_1, \dots, a_{2^{n-k}} \in \mathbb{B}^{\mathbb{B}^k}$ in der Form

$$f(x_1, \dots, x_n) \;=\; mux_{n-k}(x_1, \dots, x_{n-k},\; a_1(x_{n-k+1}, \dots, x_n), \dots, a_{2^{n-k}}(x_{n-k+1}, \dots, x_n))$$

darstellen, wobei für alle $j \in \{1, \dots, 2^{n-k}\}$ jeweils

$$a_j(x_{n-k+1}, \dots, x_n) \;=\; f(dec^{-1}(j-1), x_{n-k+1}, \dots, x_n)$$

gelte. Gemäß Korollar 4.9 lässt sich der $(n-k)$-Multiplexer als $\{mux_d, 0\}$-Schaltkreis bestehend aus maximal $\dfrac{2^{n-k} - 2^{r_d(n-k)}}{2^d - 1} + 1$ mux_d-Gattern sowie der Konstante 0 realisieren. Für die k-stelligen Funktionen $a_1, \dots, a_{2^{n-k}}$ lässt sich nach Korollar 4.12 ein gemeinsamer $\{mux_d, 0, 1\}$-Schaltkreis mit maximal

$$2^{2^k} + \frac{2^{2^k}}{2^{k + r_d(k) + \left(2^{-r_d(k)\cdot d} - 2^{-d}\right)\cdot d}} + 22$$

Gattern konstruieren. Somit ergibt sich ein $\{mux_d, 0, 1\}$-Schaltkreis für f mit insgesamt maximal

$$\frac{2^{n-k} - 2^{r_d(n-k)}}{2^d - 1} \;+\; 2^{2^k} \;+\; \frac{2^{2^k}}{2^{k + r_d(k) + \left(2^{-r_d(k)\cdot d} - 2^{-d}\right)\cdot d}} \;+\; 23$$

Gattern. Für $k = \log_2(n - d - \log_2(n-d))$ folgt weiter

$$\begin{aligned}
&\frac{2^{n-k} - 2^{r_d(n-k)}}{2^d - 1} \;+\; 2^{2^k} \;+\; \frac{2^{2^k}}{2^{k + r_d(k) + \left(2^{-r_d(k)\cdot d} - 2^{-d}\right)\cdot d}} \;+\; 23 \\
=\;& \frac{2^n}{(2^d - 1)\cdot(n - d - \log_2(n-d))} - \frac{2^{r_d(n-k)}}{2^d - 1} + \frac{2^n}{2^d \cdot (n-d)} \\
&+ \frac{2^n}{2^d \cdot (n-d) \cdot (n - d - \log_2(n-d)) \cdot 2^{r_d(k) + (2^{-r_d(k)\cdot d} - 2^{-d})\cdot d}} \;+\; 23 \\
<\;& \frac{2^{n+1}}{(2^d - 1)\cdot(n - d - \log_2(n-d))} - \frac{2^{r_d(n-k)}}{2^d - 1} \\
&+ \frac{2^n}{2^d \cdot (n-d)} \cdot \frac{1}{(n - d - \log_2(n-d)) \cdot 2^{r_d(k) + (2^{-r_d(k)\cdot d} - 2^{-d})\cdot d}} \;+\; 23 \\
:=\;& \Gamma(n, d).
\end{aligned}$$

Für eine monoton wachsende und unbeschränkte Funktion $d = d(n) < n$ folgt mit Lemma 4.13

$$\begin{aligned}
\lim_{n\to\infty} \Gamma(n, d(n)) &= \lim_{n\to\infty} \Gamma(n,d) \\
&= \lim_{n\to\infty} \left(\frac{2^{n+1}}{2^d \cdot (n-d-\log_2(n-d))} - \frac{2^{r_d(n-k)}}{2^d} \right. \\
&\qquad \left. + \frac{2^n}{2^d \cdot (n-d)} \cdot \frac{1}{(n-d-\log_2(n-d)) \cdot \underbrace{2^{r_d(k)+(2^{-r_d(k)\cdot d}-2^{-d})\cdot d}}_{>1}} \right) \\
&\leq \lim_{n\to\infty} \left(\frac{2^{n+1}}{2^d \cdot (n-d)} + \frac{2^n}{2^d \cdot (n-d)^2} \right).
\end{aligned}$$

Damit gilt für die Abschätzung der Gatteranzahl

$$\Gamma(n,d) \in \frac{2^{n+1}}{2^d \cdot (n-d)} + o\left(\frac{2^{n+1}}{2^d \cdot (n-d)} \right) = (1+o(1)) \cdot \frac{2^{n+1}}{2^d \cdot (n-d)}$$

und die Behauptung des Theorems ist für den Fall $f \in \mathbb{B}^{\mathbb{B}^n}$ gezeigt. Angenommen es sei $f \in \mathbb{B}^{\mathbb{B}^m}$ für ein $m \in \mathbb{N}$ mit $m < n$. Dann sei $f' \in \mathbb{B}^{\mathbb{B}^n}$ mit

$$f'(x_1, ..., x_m, x_{m+1}, ..., x_n) = f(x_1, ..., x_m).$$

Anwendung der obigen Konstruktion auf f' liefert die Behauptung des Theorems für den Fall $f \in \mathbb{B}^{\mathbb{B}^m}$. Folglich ist die Behauptung für alle $f \in B_n$ bewiesen. □

[10, S.3]

5 Vergleich der unteren und oberen Schranke

Abschnitt 3 und 4 liefern jeweils eine Schranke für die Komplexität n-stelliger boolescher Funktionen. Jedoch setzen beide Schranken unterschiedliche Eigenschaften der zur Verfügung stehenden Basisfunktionen voraus, was einen direkten Vergleich erschwert. Um dennoch einen direkten Vergleich zu erlauben, sollen im Folgenden beide Schranken derart umformuliert werden, dass sie die selben Voraussetzungen an die zur Verfügung stehenden Basisfunktionen stellen.

Seien hierfür zunächst $d, m : \mathbb{N} \to \mathbb{N}^*$ monotone Funktionen sowie $C \in \mathbb{R}_0^+$ eine Konstante mit $C < \ln(2)$. Dann gilt gemäß Theorem 3.11, dass

$$\lim_{n\to\infty} \frac{F\left(n, C \cdot \frac{2^n}{\ln(2)\cdot d(n)\cdot n + \ln(m(n))}, d(n), m(n)\right)}{|B_n|} = 0.$$

Sei nun $\Omega_n \subseteq B_{d(n)}$ für alle $n \in \mathbb{N}$ eine Menge von insgesamt $m(n)$ booleschen Funktionen mit Arität kleiner gleich $d(n)$. Dann bedeutet obiges Resultat, dass die Anzahl der n-stelligen booleschen Funktionen, die sich durch einen Ω_n-Schaltkreis mit maximal $C \cdot \frac{2^n}{\ln(2)\cdot d(n)\cdot n + \ln(m(n))}$ Gattern realisieren lassen, im Vergleich zu der Anzahl aller n-stelligen booleschen Funktionen asymptotisch zu vernachlässigen ist. Also konvergiert für wachsende n die Wahrscheinlichkeit, dass die Realisierung einer zufällig gewählten Funktion $f \in B_n$ durch einen Ω_n-Schaltkreis mehr als

$$C \cdot \frac{2^n}{\ln(2) \cdot d(n) \cdot n \; + \; \ln(m(n))}$$

Gatter benötigt, gegen 1.

Zur Betrachtung der oberen Schranke aus Abschnitt 4 seien nun $n \in \mathbb{N}^*$ und $d : \mathbb{N}^* \to \mathbb{N}^*$ eine monoton wachsende und unbeschränkte Funktion mit $d(n') \leq n'$ für alle $n' \in \mathbb{N}^*$. Dann lässt sich nach Theorem 4.14 jede maximal n-stellige boolesche Funktion $f \in B_n$ als $\{mux_{d(n)}, 0, 1\}$-Schaltkreis mit maximal

$$(1 + o(1)) \cdot \frac{2^{n+1}}{2^{d(n)} \cdot (n - d(n))}$$

Gattern realisieren.

Das Problem bei einem Vergleich dieser beider Schranken ist, dass ein $d(n)$-Multiplexer eine $\left(d(n) + 2^{d(n)}\right)$-stellige Funktion und damit $\{mux_{d(n)}, 0, 1\} \nsubseteq B_{d(n)}$ ist, während $\Omega_n \subseteq B_{d(n)}$ eine Menge maximal $d(n)$-stelliger Funktionen ist. Die Lösung liefern die nachfolgenden Korollare. Da für alle $n \in \mathbb{N}^*$ die Anzahl der zur Verfügung stehenden Basisfunktionen $|\{mux_{d(n)}, 0, 1\}| = 3$ in Theorem 4.14 konstant ist, wird diese Anzahl in besagten Korollaren wahlweise als konstant oder beschränkt betrachtet.

Korollar 5.1 (zu Theorem 3.11).
Seien $C \in \mathbb{R}_0^+$ mit $C < 1$ sowie $m \in \mathbb{N}$ und sei $d : \mathbb{N} \to \mathbb{N}^*$ monoton. Dann gilt

$$\lim_{n\to\infty} \frac{F\left(n,\; C \cdot \frac{2^n}{[2^{d(n)}+d(n)]\cdot n},\; 2^{d(n)} + d(n),\; m\right)}{|B_n|} = 0.$$

Bei dem nachfolgenden Beweis handelt es sich um eine Abwandlung des Beweises zu Theorem 3.11.

Beweis. Seien $m \in \mathbb{N}^*$ und $x, d : \mathbb{N} \to \mathbb{N}^*$ monotone Funktionen, für die ein $n_0 \in \mathbb{N}$ mit $d(n_0) \geq 2$ existiert. Der Übersichtlichkeit halber seien im Folgenden $x = x(n)$, $d = d(n)$ und $D = 2^d + d$. Gemäß des Beweises von Theorem 3.11 gilt

$$\lim_{n\to\infty} \ln \frac{F\left(n, \frac{2^n}{x}, 2^d + d, m\right)}{|B_n|} \;=\; \lim_{n\to\infty} \ln \frac{F(n, \frac{2^n}{x}, D, m)}{|B_n|}$$

$$\begin{aligned}
&\leq \lim_{n\to\infty} 2^n \cdot \left[\frac{\ln(m) + D \cdot \ln(2) + (D-1)\cdot(n\cdot\ln(2) - \ln(x)) + 1}{x} - \ln(2)\right] \\
&= \lim_{n\to\infty} 2^n \cdot \left[\frac{\ln(m) + (2^d + d)\cdot \ln(2) + (2^d + d - 1)\cdot(n\cdot\ln(2) - \ln(x)) + 1}{x} - \ln(2)\right] \\
&\leq \lim_{n\to\infty} 2^n \cdot \left[\frac{\ln(m) + (2^d + d)\cdot \ln(2) + (2^d + d)\cdot n\cdot\ln(2) + 1}{x} - \ln(2)\right].
\end{aligned}$$

Für ein $C \in \mathbb{R}$ mit $0 < C < 1$ und $x = \dfrac{(2^d + d)\cdot n}{C}$ folgt daraus

$$\lim_{n\to\infty} \ln \frac{F\left(n, \frac{2^n}{x}, 2^d + d, m\right)}{|B_n|} \;=\; \lim_{n\to\infty} \ln \frac{F\left(n,\ C\cdot\frac{2^n}{(2^d+d)\cdot n},\ 2^d + d,\ m\right)}{|B_n|}$$

$$\begin{aligned}
&\leq \lim_{n\to\infty} 2^n \cdot \left[C \cdot \frac{\ln(m) + (2^d + d)\cdot \ln(2) + (2^d + d)\cdot n\cdot\ln(2) + 1}{(2^d + d)\cdot n} - \ln(2)\right] \\
&\leq \lim_{n\to\infty} 2^n \cdot \left[C\cdot\ln(2) - \ln(2)\right] \\
&= -\infty.
\end{aligned}$$

Somit gilt auch $\lim\limits_{n\to\infty} \dfrac{F\left(n,\ C\cdot\frac{2^n}{(2^d+d)\cdot n},\ 2^d + d,\ m\right)}{|B_n|} = 0$ und die Behauptung des Korollars ist für den Fall $C > 0$, $m \geq 1$ und die oben gewählte Funktion d bewiesen. Für den Fall $C = 0$ und obiges d folgt die Behauptung aus Beobachtung 3.3. Für den Fall $C \in \mathbb{R}$ mit $0 \leq C < 1$ und eine monotone Funktion $d : \mathbb{N} \to \mathbb{N}^*$, für die kein $n_0 \in \mathbb{N}$ mit $d(n_0) \geq 2$ existiert, folgt die Behauptung aus Beobachtung 3.5. Weiterhin gilt für $m = 0$, dass $F(n, t, d, m) = 0$ für alle $n, t, d \in \mathbb{N}$. Somit folgt auch in diesem Fall die Behauptung des Korollars. ☐

Korollar 5.2. *Seien $C \in \mathbb{R}_0^+$ mit $C < 1$ sowie $m \in \mathbb{N}$ und sei $d : \mathbb{N} \to \mathbb{N}^*$ eine monoton wachsende und unbeschränkte Funktion. Dann gilt*

$$\lim_{n\to\infty} \frac{F\left(n,\ (1 + o(1))\cdot C\cdot\frac{2^n}{2^{d(n)}\cdot n},\ 2^{d(n)} + d(n),\ m\right)}{|B_n|} \;=\; 0.$$

Beweis. Seien $C \in \mathbb{R}_0^+$ mit $C < 1$ sowie $m \in \mathbb{N}$ und sei $d : \mathbb{N} \to \mathbb{N}^*$ eine monoton wachsende und unbeschränkte Funktion. Gemäß Korollar 5.1 gilt

$$\lim_{n\to\infty} \frac{F\left(n,\ C \cdot \frac{2^n}{[2^{d(n)}+d(n)]\cdot n},\ 2^{d(n)}+d(n),\ m\right)}{|B_n|} \ = \ 0.$$

Weiterhin gilt

$$\lim_{n\to\infty} C \cdot \frac{2^n}{2^{d(n)} \cdot n} \cdot \left[C \cdot \frac{2^n}{[2^{d(n)}+d(n)]\cdot n}\right]^{-1} \ = \ \lim_{n\to\infty} \frac{2^{d(n)}+d(n)}{2^{d(n)}} \ = \ 1.$$

Daraus folgt

$$C \cdot \frac{2^n}{[2^{d(n)}+d(n)]\cdot n} \ \in \ (1+o(1)) \cdot C \cdot \frac{2^n}{2^{d(n)}\cdot n}$$

und

$$\lim_{n\to\infty} \frac{F\left(n,\ (1+o(1)) \cdot C \cdot \frac{2^n}{2^{d(n)}\cdot n},\ 2^{d(n)}+d(n),\ m\right)}{|B_n|} \ = \ 0.$$

□

Korollar 5.3. *Seien $C \in \mathbb{R}, \bar{m} \in \mathbb{N}$ mit $0 \leq C < 1$ sowie $m : \mathbb{N} \to \mathbb{N}$ mit $m(n) \leq \bar{m}$ für alle $n \in \mathbb{N}$ und sei $d : \mathbb{N} \to \mathbb{N}^*$ eine monoton wachsende und unbeschränkte Funktion. Dann gilt*

$$\lim_{n\to\infty} \frac{F\left(n,\ (1+o(1)) \cdot C \cdot \frac{2^n}{2^{d(n)}\cdot n},\ 2^{d(n)}+d(n),\ m(n)\right)}{|B_n|} \ = \ 0.$$

Beweis. Die Aussage des Korollars folgt aus Korollar 5.2 und Beobachtung 3.6. □

Korollar 5.4 (zu Theorem 4.14)**.**
Seien $n \in \mathbb{N}^*$ und $d : \mathbb{N}^* \to \mathbb{N}^*$ eine monoton wachsende und unbeschränkte Funktion mit $d(n) \leq n$, dann lässt sich jede n-stellige boolesche Funktion $f \in B_n$ als $\{mux_{d(n)}, 0, 1\}$-Schaltkreis mit maximal

$$(1+o(1)) \cdot \frac{2^{n+1}}{2^{d(n)} \cdot n}$$

Gattern realisieren.

Beweis. Seien $n \in \mathbb{N}^*$ und $d : \mathbb{N}^* \to \mathbb{N}^*$ eine monoton wachsende und unbeschränkte Funktion mit $d(n) \leq n$, dann lässt sich nach Theorem 4.14 jede n-stellige boolesche Funktion $f \in B_n$ als $\{mux_{d(n)}, 0, 1\}$-Schaltkreis mit maximal

$$(1+o(1)) \cdot \frac{2^{n+1}}{2^{d(n)} \cdot (n - d(n))}$$

Gattern realisieren. Mit $C(n) \in (1+o(1))$ gilt weiterhin

$$\lim_{n\to\infty} C(n) \cdot \frac{2^{n+1}}{2^{d(n)} \cdot n} \cdot \left[C(n) \cdot \frac{2^{n+1}}{2^{d(n)} \cdot (n-d(n))} \right]^{-1} = \lim_{n\to\infty} \frac{2^{d(n)} \cdot (n-d(n))}{2^{d(n)} \cdot n}$$

$$= \lim_{n\to\infty} \frac{2^{d(n)} \cdot n \; - \; 2^{d(n)} \cdot d(n)}{2^{d(n)} \cdot n} = 1.$$

Damit folgt

$$(1+o(1)) \cdot \frac{2^{n+1}}{2^{d(n)} \cdot (n-d(n))} = (1+o(1)) \cdot \left(\frac{2^{n+1}}{2^{d(n)} \cdot n} + \frac{2^{n+1}}{2^{d(n)} \cdot (n-d(n))} - \frac{2^{n+1}}{2^{d(n)} \cdot n} \right)$$

$$= (1+o(1)) \cdot \left(\frac{2^{n+1}}{2^{d(n)} \cdot n} + o(1) \right) \subset (1+o(1)) \cdot (1+o(1)) \cdot \frac{2^{n+1}}{2^{d(n)} \cdot n}$$

$$= (1+2 \cdot o(1) + o(1)^2) \cdot \frac{2^{n+1}}{2^{d(n)} \cdot n} = (1+o(1)) \cdot \frac{2^{n+1}}{2^{d(n)} \cdot n}.$$

Somit lässt sich jede n-stellige boolesche Funktion $f \in B_n$ als $\{mux_{d(n)}, 0, 1\}$-Schaltkreis mit maximal

$$(1+o(1)) \cdot \frac{2^{n+1}}{2^{d(n)} \cdot n}$$

Gattern realisieren. □

Zum Vergleich beider Schranken seien nun $C \in \mathbb{R}_0^+, \bar{m} \in \mathbb{N}$ mit $C < 1$ und $m : \mathbb{N} \to \mathbb{N}$ eine durch $\bar{m}$ beschränkte Funktion sowie $d : \mathbb{N} \to \mathbb{N}^*$ eine monoton wachsende und unbeschränkte Funktion mit $d(n) \leq n$. Dann gilt nach Korollar 5.3

$$\lim_{n\to\infty} \frac{F\left(n,\ (1+o(1)) \cdot C \cdot \frac{2^n}{2^{d(n)} \cdot n},\ 2^{d(n)} + d(n),\ m(n)\right)}{|B_n|} = 0.$$

Sei nun $(\Omega_n)_{n\in\mathbb{N}}$ eine beliebige Folge jeweils B_n-vollständiger Funktionsmengen mit der für alle $n \in \mathbb{N}$ gilt, dass $\Omega_n \subseteq B_{2^{d(n)}+d(n)}$ und dass $|\Omega_n| \leq \bar{m}$. Dann bedeutet obiges Resultat, dass für n gegen unendlich die Wahrscheinlichkeit, dass eine zufällig gewählte Funktion $f \in B_n$ eine Komplexität $C_{\Omega_n}(f)$ mit

$$C_{\Omega_n}(f) > (1+o(1)) \cdot C \cdot \frac{2^n}{2^{d(n)} \cdot n}$$

hat, gegen 1 konvergiert. Dies gilt insbesondere für die Wahl $\Omega_0 = \{0, 1\}$ und $\Omega_n = \{mux_{d(n)}, 0, 1\}$ für alle $n \in \mathbb{N}^*$. Gleichzeitig lässt sich nach Korollar 5.4 jede maximal n-stellige boolesche Funktion durch einen $\{mux_{d(n)}, 0, 1\}$-Schaltkreis der Größe

$$(1+o(1)) \cdot \frac{2^{n+1}}{2^{d(n)} \cdot n}$$

realisieren. Für wachsende n konvergiert somit die Wahrscheinlichkeit, dass eine zufällig gewählte Funktion $f \in B_n$ eine Komplexität $C_{\Omega_n}(f)$ mit

$$(1+o(1)) \cdot C \cdot \frac{2^n}{2^{d(n)} \cdot n} < C_{\Omega_n}(f) \leq (1+o(1)) \cdot 2 \cdot \frac{2^n}{2^{d(n)} \cdot n}.$$

hat, gegen 1. Da $0 \leq C < 1$, sind folglich die Konstruktion aus Theorem 4.14 sowie die Wahl der Basismengen $\Omega_0 = \{0, 1\}$ und $\Omega_i = \{mux_{d(n)}, 0, 1\}$ für alle $i \in \mathbb{N}^*$ asymptotisch betrachtet im Wesentlichen optimal bis auf den Faktor 2. Das Gleiche gilt für die beiden Schranken aus den Theoremen 3.11 und 4.14.

6 Weiterführende Fragestellungen

Aus den in den vorangegangenen Abschnitten vorgestellten Ergebnissen ergeben sich weitere Fragestellungen, die sich als Gegenstand zukünftiger Arbeiten anbieten und darum im Folgenden aufgeführt werden sollen.

Die vorgestellten unteren und oberen Schranken für die Komplexität boolescher Funktionen verwenden als Komplexitätsmaß allesamt die Anzahl an Gattern, die eine minimale Schaltkreisrealisierung aufweisen würde. Es existieren jedoch auch andere Maße für die Komplexität einer booleschen Funktion, beispielsweise die Messung des längsten Pfades in einem realisierenden Schaltkreis [12, S.9], [6, S.159] oder die Messung der Anzahl an Kanten in dem entsprechenden Graphen. Eine jeweilige untere Schranke könnte über eine Abwandlung des Abzählarguments aus Theorem 3.11 berechnet werden und eine obere Schranke über eine Abschätzung der Tiefe beziehungsweise der Anzahl an Verbindungen in der Konstruktion aus Theorem 4.14.

Im Rahmen einer Untersuchung der Anzahl an Kanten würde es sich ebenfalls anbieten, die Anzahl an Kanten der Konstruktion aus Theorem 4.14 zu untersuchen, die sich in einer ebenen Darstellung schneiden. Für eine untere Schranke an die Anzahl der Kanten wäre zu prüfen, ob sich diese auch in Abhängigkeit der Anzahl an schneidenden Kanten formulieren ließe.

Zusätzlich ließen sich sämtliche bisher aufgeführte Fragestellungen auch für eine Teilklasse der booleschen Funktionen formulieren, beispielsweise für die Klasse der symmetrischen [6, S.4] oder der monotonen [6, S.8] Funktionen. Interessant wäre hierbei zu sehen, ob sich durch die Untersuchung einer Teilklasse der booleschen Funktionen die oben erwähnten Schranken aufgrund der zusätzlichen Eigenschaften verbessern ließen.

Ebenso ließen sich sämtliche Fragestellungen auch auf mehrwertige Logiken verallgemeinern. Hierfür würde es genügen statt booleschen Funktionen Funktionen der Form $f : \{0, \ldots, N-1\}^n \to \{0, \ldots, N-1\}$ für ein $N \in \mathbb{N}$ mit $N \geq 2$ zu betrachten. Dabei könnte N zum einen durch einen konkreten Wert ersetzt werden, was es beispielsweise im Falle von $N = 3$ erlauben würde, Eigenschaften der dreiwertigen Funktionen $f : \{0, 1, 2\}^n \to \{0, 1, 2\}$ ausnutzen. Zum anderen könnte auch ein beliebiges $N \in \mathbb{N}$ mit $N \geq 2$ gewählt werden um noch allgemeinere Resultate zu erzielen.

Als letzte und wohl interessanteste Fragestellung bliebe die empirische Prüfung der Optimalität der Konstruktion aus Theorem 4.14. Dafür würde es sich anbieten eine monoton wachsende und unbeschränkte Funktion $d : \mathbb{N}^* \to \mathbb{N}^*$ mit $d(n) < n$, eine endliche Menge von Aritäten $A \subset \mathbb{N}^*$ sowie für jedes $n \in A$ eine endliche Menge von Funktionen $F_n \subseteq \mathbb{B}^{\mathbb{B}^n}$ zu wählen und anschließend für jedes $n \in A$ und jedes $f \in F_n$ den kleinsten bekannten B_2-Schaltkreis für f mit dem $\{mux_{d(n)}, 0, 1\}$-Schaltkreis aus Theorem 4.14 für f hinsichtlich ihrer Größe zu vergleichen. Um möglichst gute Erkenntnisse über die Effizienz der Konstruktion aus Theorem 4.14 zu erhalten, wäre es hierbei wichtig die Funktionsmengen F_n so zu wählen, dass für alle $n \in A \setminus \{\max(A)\}$ die Menge F_{n+1} genau die $(n+1)$-stelligen Verallgemeinerungen der Funktionen aus F_n enthält. Falls F_n eine n-äre Konjunktion enthält, sollte F_{n+1} beispielsweise eine $(n+1)$-äre Konjunktion enthalten. Weiterhin sollten die Funktionsmengen F_n aus Funktionen bestehen, die zum einen hinreichende Anwendung in realen Schaltkreisen finden und zum anderen ausreichend untersucht sind, damit kleine B_2-Schaltkreise für ihre Realisierung bekannt sind. Daher wäre eine Möglichkeit für die Wahl von A, F_n und d

$$\begin{aligned} d(n) &= \log_2 n, \\ A &= \{2^2, 2^3, \ldots, 2^6\} = \{4, 8, \ldots, 64\}, \\ F_n &= \{Th^n_{d(n)},\ Th^n_{n-d(n)},\ Maj_n,\ Mod^n_{d(n)},\ PRIME_n,\ \oplus_n,\ \wedge_n,\ \vee_n\} \subseteq B_n \qquad \text{für } n \in A. \end{aligned}$$

Dabei bezeichnen Th^n_k die Schwellwertfunktion (engl. threshold function), Maj_n die Mehrheitsfunktion (engl. majority function), Mod^n_k die Modulofunkion, $PRIME_n$ die Primzahlfunktion, $\oplus_n$ die Paritätsfunktion sowie $\wedge_n$ und $\vee_n$ jeweils eine n-äre Konjunktion beziehungsweise Disjunktion [6, S.4].
Für die Konstruktion eines noch realistischeren Szenarios wäre es auch möglich die Funktionsmengen F_n aus einer realen Benchmark Suite für FPGAs oder integrierte Schaltkreise herzuleiten [8], [7], [5].

Es ergeben sich somit aus den Ergebnissen dieser Arbeit einige weitere Fragestellungen, die es Wert sind näher untersucht zu werden.

Literaturverzeichnis

[1] *DIN 5473:1992-07, Logik und Mengenlehre; Zeichen und Begriffe*.

[2] A. Kulikov G. Yaroslavtsev E. Demenkov, A. Kojevnikov. New upper bounds on the boolean circuit complexity of symmetric functions, 2010.
online verfuegbar auf `http://grigory.github.io/files/publications/2010_upper_bounds_symmetric_ipl.pdf`, Stand: 19.04.2015.

[3] William Feller. A direct proof of stirling's formula. *The American Mathematical Monthly*, 74(10):pp. 1223–1225, 1967.

[4] U. Brandt H. Walter. private Kommunikation.

[5] M.C. Hansen, H. Yalcin, and J.P. Hayes. Unveiling the iscas-85 benchmarks: a case study in reverse engineering. *Design Test of Computers, IEEE*, 16(3):72–80, 1999.

[6] S. Jukna. *Boolean Function Complexity: Advances and Frontiers*. Springer Verlag, 2012.

[7] Hakan Yalcin Mark Hansen and John Hayes. Iscas high-level models.
online verfügbar auf `http://web.eecs.umich.edu/~jhayes/iscas.restore/benchmark.html`, Stand: 15.01.2015
Als HTML-Version verfügbar auf
`http://web.eecs.umich.edu/~jhayes/iscas.restore/benchmark.html`, Stand: 15.01.2015.

[8] Raphael Njuguna. A survey of fpga benchmarks.
online verfügbar auf `http://www.cse.wustl.edu/~jain/cse567-08/ftp/fpga.pdf`, Stand: 19.04.2015
Als HTML-Version verfügbar auf
`http://www.cse.wustl.edu/~jain/cse567-08/ftp/fpga/`, Stand: 19.04.2015.

[9] E. Kranakis P. Clote. *Boolean Functions and Computation Models*. Springer Verlag, 2002.

[10] Izik Pe'er. Handout boolean circuit complexity, chapter 2, 1994/1995.
online verfügbar auf `http://www2.cs.uni-paderborn.de/cs/ag-madh/WWW/Teaching/2005WS/Schaltkreis/urizwick_v2.pdf`, Stand: 19.04.2015
Alle Kapitel des Skriptes sind online verfügbar auf
`http://www2.cs.uni-paderborn.de/cs/ag-madh/WWW/Teaching/2005WS/Schaltkreis/`, Stand: 19.04.2015
Es konnte keine alternative Literatur zu den zitierten Beweisen gefunden werden.

[11] LarryJ. Stockmeyer. On the combinational complexity of certain symmetric boolean functions. *Mathematical systems theory*, 10(1):323–336, 1976.

[12] I. Wegener. *The Complexity of Boolean Functions*. B.G. Teubner, John Wiley & Sons Ltd, 1987.