Perlen der theoretischen Informatik

Theorem von Khrapchenko

Lars Quentin und Lukas Niegsch

Georg-August-Universität Göttingen

Irgendwann 2020?

Problemstellung

- Komplexität von De-Morgan-Schaltkreisen

Problemstellung

- Komplexität von De-Morgan-Schaltkreisen
- Standartmaß: Blätteranzahl $L(f)$

Problemstellung

- Komplexität von De-Morgan-Schaltkreisen
- Standartmaß: Blätteranzahl $L(f)$
- Abschätzung durch einfachere Maße

Themenvorstellung

- Analyse boolscher Funktionen über das Konzept der Rechtecke
- Untere Schranke für die Blattgröße DeMorgan'scher Formeln
- Generalisierte Komplexitätsmaße:
  - konvexe Maße
  - submodulare Maße

Wiederholung

Definition [DeMorgan-Schaltkreis]

- $\Phi := \{\wedge, \vee, \neg\}$ boolsche Basis
- $\neg$ -Gatter nur bei Inputvariablen

Definition [Formel, Blattgröße]

- boolsche Funktion f
- Fan-Out 1 Schaltkreis
- $L(f)$ ist die Anzahl der Eingabegatter

Definition [kombinatorisches Rechteck]

- $R = A \times B$, $A, B \subset \{0,1\}^n$ disjunkt
- $S \subset R$ Unterrechteck, falls S ebenfalls ein Rechteck ist

Bemerkung

- R ist bipartiter Graph.
- $(a, b) \in R$ sind Paare von Ecken.

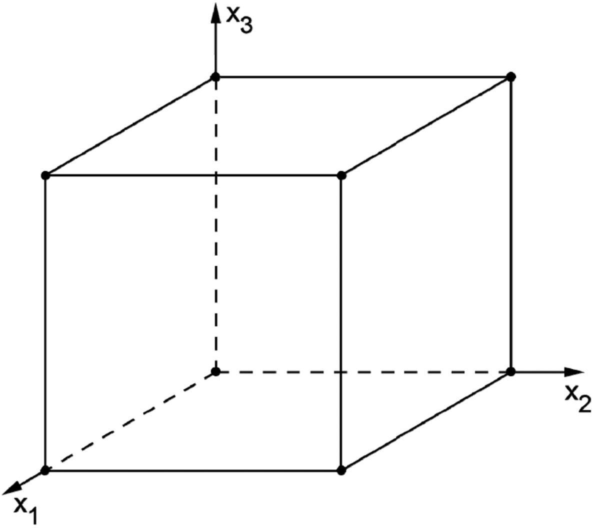

Figure: Beispiel

Definition

Sei f eine boolsche Funktion und $R = A \times B$ ein Rechteck. f separiert R, falls $f(A) = 1, f(B) = 0$.

Dabei ist

$$f(A) = 1 \Leftrightarrow \forall a \in A : f(a) = 1$$

$$f(B) = 0 \Leftrightarrow \forall b \in B : f(b) = 0$$

Definition

Ein Rechteck $R = A \times B$ heißt monochrom, wenn ein Index i existiert, so dass

$$a_i \neq b_i \text{ für alle Kanten } (a, b) \in R$$

Analog ist R positiv monochrom, wenn

$$a_i = 1,\ b_i = 0 \text{ für alle Kanten } (a, b) \in R$$

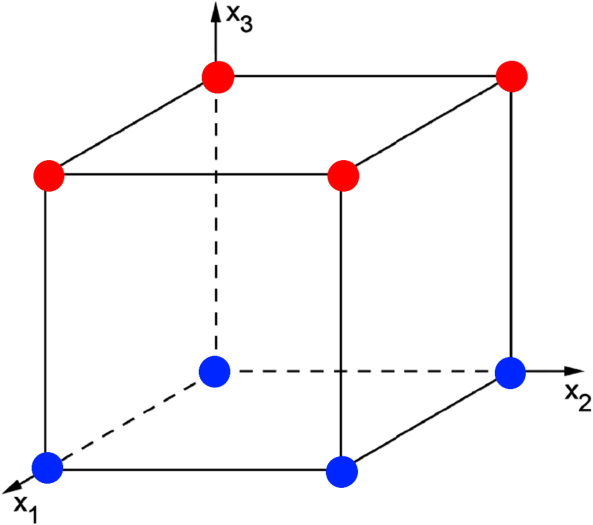

Figure: (positiv) monochromes Rechteck

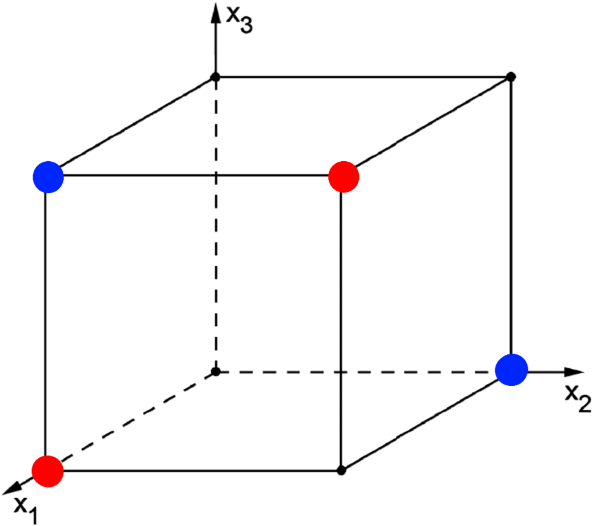

Figure: nichtmonochromes Rechteck

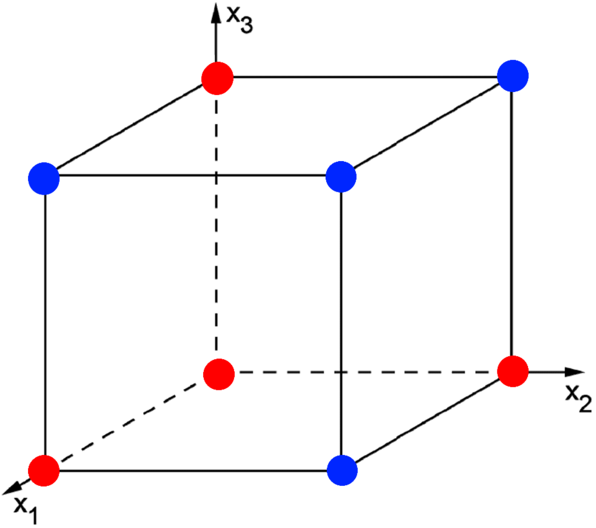

Figure: nichtmonochromes Rechteck

Lars Quentin und Lukas Niegsch

Definition [Partitionszahl]

- R Rechteck, f boolsche Funktion
- $\chi(R)$ Partitionszahl
- Größe der kleinsten Partition in **disjunkte** monochrome Rechtecke
- $\chi_+(R)$ analog für positiv monochrome Rechtecke
- $\chi(f) := \chi(f^{-1}(1) \times f^{-1}(0))$

Definition [kanonische monochrome Rechtecke]

- R Rechteck
- $M_{i,b} := \{(x, y) \in R | x_i = b, y_i = 1 - b\}$
- $i = 0, \ldots, n;\ b = 0, 1$

Definition [kanonische monochrome Rechtecke]

- R Rechteck
- $M_{i,b} := \{(x,y) \in R | x_i = b, y_i = 1 - b\}$
- $i = 0, \ldots, n;\ b = 0, 1$

Bemerkung

- $M_{i,b}$ sind monochrom.
- $M_{i,b}$ überdecken R.
- $\chi(R)$ wird nichttrivial durch die Disjunktheit der Partition

Lemma [Rychkov 1985]

Für jede boolsche Funktion f und jede monotone boolsche Funktion g gilt:

$$L(f) \geq \chi(f), L_+(g) \geq \chi_+(g)$$

Hierbei ist $L(f)$ die kleinste Anzahl der Blätter einer DeMorgan Formel.

Beweis: Induktion über $t = L(f)$

Induktionsanfang:

Beweis: Induktion über $t = L(f)$

Induktionsanfang:

- $f(x) = x_i$ oder $f(x) = \neg x_i$.

Beweis: Induktion über $t = L(f)$

Induktionsanfang:

- $f(x) = x_i$ oder $f(x) = \neg x_i$.
- $R = f^{-1}(1) \times f^{-1}(0)$ monochrom

Beweis: Induktion über $t = L(f)$

Induktionsanfang:

- $f(x) = x_i$ oder $f(x) = \neg x_i$.
- $R = f^{-1}(1) \times f^{-1}(0)$ monochrom
- $L(f) = 1 \geq 1 = \chi(f)$

Beweis:

Induktionsschritt:

Beweis:

Induktionsschritt:

- Sei f eine minimale Formel.

Beweis:

Induktionsschritt:

- Sei f eine minimale Formel.
- $f = f_0 \wedge f_1$ oder $f = f_0 \vee f_1$

Beweis:

Induktionsschritt:

- Sei f eine minimale Formel.
- $f = f_0 \wedge f_1$ oder $f = f_0 \vee f_1$
- f_0, f_1 sind minimal.

Beweis:

Induktionsschritt:

- Sei f eine minimale Formel.
- $f = f_0 \wedge f_1$ oder $f = f_0 \vee f_1$
- f_0, f_1 sind minimal.
- $B_0 := \{b \in B | f_0(b) = 0\}$.

Beweis:

Induktionsschritt:

- Sei f eine minimale Formel.
- $f = f_0 \wedge f_1$ oder $f = f_0 \vee f_1$
- f_0, f_1 sind minimal.
- $B_0 := \{b \in B | f_0(b) = 0\}$.
- f_0 separiert $A \times B_0$

Beweis:

Induktionsschritt:

- Sei f eine minimale Formel.
- $f = f_0 \wedge f_1$ oder $f = f_0 \vee f_1$
- f_0, f_1 sind minimal.
- $B_0 := \{b \in B | f_0(b) = 0\}$.
- f_0 separiert $A \times B_0$
- f_1 separiert $A \times (B \setminus B_0)$.

Beweis:

Induktionsschritt:

- Sei f eine minimale Formel.
- $f = f_0 \wedge f_1$ oder $f = f_0 \vee f_1$
- f_0, f_1 sind minimal.
- $B_0 := \{b \in B | f_0(b) = 0\}$.
- f_0 separiert $A \times B_0$
- f_1 separiert $A \times (B \setminus B_0)$.
- $A \times B = A \times B_0 \cup A \times (B \setminus B_0)$.

Beweis:

Induktionsschritt:

- Sei f eine minimale Formel.
- $f = f_0 \wedge f_1$ oder $f = f_0 \vee f_1$
- f_0, f_1 sind minimal.
- $B_0 := \{b \in B | f_0(b) = 0\}$.
- f_0 separiert $A \times B_0$
- f_1 separiert $A \times (B \setminus B_0)$.
- $A \times B = A \times B_0 \cup A \times (B \setminus B_0)$.

Somit

$$\chi(R) \leq \chi(A \times B_0) + \chi(A \times (B \setminus B_0)) \leq L(f_0) + L(f_1) = L(f)$$

Beweis:

Induktionsschritt:

- Sei f eine minimale Formel.
- $f = f_0 \wedge f_1$ oder $f = f_0 \vee f_1$
- f_0, f_1 sind minimal.
- $B_0 := \{b \in B | f_0(b) = 0\}$.
- f_0 separiert $A \times B_0$
- f_1 separiert $A \times (B \setminus B_0)$.
- $A \times B = A \times B_0 \cup A \times (B \setminus B_0)$.

Somit

$$\chi(R) \leq \chi(A \times B_0) + \chi(A \times (B \setminus B_0)) \leq L(f_0) + L(f_1) = L(f)$$

Die anderen Fälle folgen analog. $\square$

Definition

Sei R ein Rechteck.

$$A \otimes B := \{(a, b) \in R | a \sim b\}$$

Wobei $a \sim b$, falls a und b sich in genau einem Bit unterscheiden.

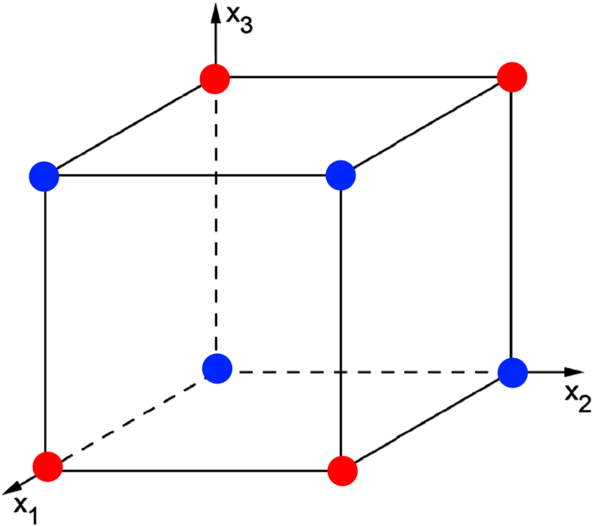

Figure: $A \otimes B$ Beispiel

Lemma

Ein monochromes Unterrechteck von $A \times B$ der Größe $s \times t$ kann maximal $\sqrt{st}$ Elemente von $A \otimes B$ überdecken.

Beweis:

Sei $S \times T \subset A \times B$ ein Unterrechteck, $S \times T$ monochrom, $|S| = s, |T| = t$.

Die Monochromie besagt, dass $\exists i : a_i \neq b_i \; \forall (a, b) \in S \times T$.

Falls $(a, b) \in A \otimes B$, dann unterscheiden sich a und b in genau einem Index.

Für die Überdeckung folgt also

$$\min\{|S|, |T|\} = \min\{s, t\} \leq \sqrt{st}$$

$\square$

Theorem [Khrapchenko 1971]

Sei f eine boolsche Funktion, die das Rechteck $A \times B$ separiert. Dann gilt:

$$L(f) \geq \frac{|A \otimes B|^2}{|A| \cdot |B|}$$

Beweis:
Sei $S_i \times T_i$ eine Zerlegung von $A \times B$ in r monochrome Rechtecke, $i = 1, \dots, r$ mit $|S_i| = s_i$ und $|T_i| = t_i$.
Sei c_i die Anzahl der Elemente aus $A \otimes B$ in $S_i \times T_i$.

Beweis:
Sei $S_i \times T_i$ eine Zerlegung von $A \times B$ in r monochrome Rechtecke, $i = 1, \ldots, r$ mit $|S_i| = s_i$ und $|T_i| = t_i$.
Sei c_i die Anzahl der Elemente aus $A \otimes B$ in $S_i \times T_i$.
Aus dem obigem Lemma folgt: $c_i^2 \leq s_i t_i$.
Da $S_i \times T_i$ eine paarweise disjunkte Zerlegung ist folgt

$$|A \otimes B| = \sum_{i=1}^{r} c_i, \qquad |A \times B| = \sum_{i=1}^{r} s_i t_i$$

Beweis:
Sei $S_i \times T_i$ eine Zerlegung von $A \times B$ in r monochrome Rechtecke, $i = 1, \ldots, r$ mit $|S_i| = s_i$ und $|T_i| = t_i$.
Sei c_i die Anzahl der Elemente aus $A \otimes B$ in $S_i \times T_i$.
Aus dem obigem Lemma folgt: $c_i^2 \leq s_i t_i$.
Da $S_i \times T_i$ eine paarweise disjunkte Zerlegung ist folgt

$$|A \otimes B| = \sum_{i=1}^{r} c_i, \qquad |A \times B| = \sum_{i=1}^{r} s_i t_i$$

Es folgt:

$$|A \otimes B|^2 = (\sum_{i=1}^{r} c_i)^2 \leq r(\sum_{i=1}^{r} c_i^2) \leq r(\sum_{i=1}^{r} s_i t_i) = r|A \times B|$$

Beweis:
Sei $S_i \times T_i$ eine Zerlegung von $A \times B$ in r monochrome Rechtecke, $i = 1, \dots, r$ mit $|S_i| = s_i$ und $|T_i| = t_i$.
Sei c_i die Anzahl der Elemente aus $A \otimes B$ in $S_i \times T_i$.
Aus dem obigem Lemma folgt: $c_i^2 \leq s_i t_i$.
Da $S_i \times T_i$ eine paarweise disjunkte Zerlegung ist folgt

$$|A \otimes B| = \sum_{i=1}^{r} c_i, \qquad |A \times B| = \sum_{i=1}^{r} s_i t_i$$

Es folgt:

$$|A \otimes B|^2 = (\sum_{i=1}^{r} c_i)^2 \leq r(\sum_{i=1}^{r} c_i^2) \leq r(\sum_{i=1}^{r} s_i t_i) = r|A \times B|$$

$$\Rightarrow L(f) \geq \chi(f) = r \geq \frac{|A \otimes B|^2}{|A \times B|} = \frac{|A \otimes B|^2}{|A| \cdot |B|}$$

Theorem

Sei

$$\bigoplus_n := x_1 \oplus \cdots \oplus x_n$$

Dann folgt aus Kharapchenko's Theorem, dass

$$L(\bigoplus_n) \geq n^2$$

Beweis:

A die Menge aller Vektoren mit ungerader Anzahl an Einsen.
Sei B die Menge aller Vektoren mit gerader Anzahl an Einsen.

Beweis:

A die Menge aller Vektoren mit ungerader Anzahl an Einsen.
Sei B die Menge aller Vektoren mit gerader Anzahl an Einsen.
Dann

$$|A| = 2^{n-1}, |B| = 2^{n-1}, |A \otimes B| = n2^{n-1}$$

Beweis:

A die Menge aller Vektoren mit ungerader Anzahl an Einsen.
Sei B die Menge aller Vektoren mit gerader Anzahl an Einsen.
Dann

$$|A| = 2^{n-1}, |B| = 2^{n-1}, |A \otimes B| = n2^{n-1}$$

Es folgt

$$L(\oplus_n) \geq \frac{n^2 2^{2(n-1)}}{2^{n-1}2^{n-1}} = n^2$$

□

Theorem [Yablonskii 1954]

Sei $n \in \mathbb{N}$ mit $n \geq 2$. Dann

$$L(\oplus_n) \leq 3np_n - 2p_n^2 \leq \frac{9}{8}n^2,$$

wobei $p_n = 2^{\lfloor log_2 n \rfloor}$.

Wenn n eine Zweierpotenz ist, dann gilt

$$L(\oplus_n) = n^2$$

Es wird vermutet, dass diese Schranke scharf ist.

Beweis:

Sei $\lambda(n) := L(\oplus_n)$.
Zudem sei $m := \lfloor \log_2 n \rfloor$, so dass $n = 2^m + k, 0 \leq k < 2^m$.

Beweis:

Sei $\lambda(n) := L(\oplus_n)$.
Zudem sei $m := \lfloor \log_2 n \rfloor$, so dass
$n = 2^m + k, 0 \leq k < 2^m$.

Zu zeigen: $\lambda(n) \leq 2^{2m} + 3k2^m = 3np_n - 2p_n^2$.

Beweis:

Sei $\lambda(n) := L(\oplus_n)$.
Zudem sei $m := \lfloor \log_2 n \rfloor$, so dass
$n = 2^m + k, 0 \leq k < 2^m$.

Zu zeigen: $\lambda(n) \leq 2^{2m} + 3k2^m = 3np_n - 2p_n^2$.

Beweis durch Induktion über $n = 2^m + k$.

Induktionsanfang: $n = 1 = 2^0 + 0$:

Beweis:

Sei $\lambda(n) := L(\oplus_n)$.
Zudem sei $m := \lfloor \log_2 n \rfloor$, so dass
$n = 2^m + k, 0 \leq k < 2^m$.

Zu zeigen: $\lambda(n) \leq 2^{2m} + 3k2^m = 3np_n - 2p_n^2$.

Beweis durch Induktion über $n = 2^m + k$.

Induktionsanfang: $n = 1 = 2^0 + 0$:

$$2^{2 \cdot 0} + 3 \cdot 0 \cdot 2^0 = 1 = \lambda(1)$$

und analog für 2.

Induktionsschritt:

Hierfür nutzen wir, dass für Funktionen g, h gilt, dass

$$f = g \oplus h \Leftrightarrow f = (g \wedge \neg h) \vee (\neg g \wedge h)$$

Somit muss gelten, dass

$$L(f) \leq 2L(g) + 2L(h)$$

Somit erhalten wir

$$\lambda(n) \leq 2(\lambda(\lfloor n/2 \rfloor) + \lambda(\lceil n/2 \rceil)) = 3np_n - 2p_n^2 \leq \frac{9}{8}n^2$$

$\square$

Resultat

Nach den beiden obigen Lemmas folgt:

$$n^2 \leq L(\oplus_n) \leq \frac{9}{8}n^2$$

Für $n = 2^k$ gilt:

$$n^2 = L(\oplus_n)$$

Theorem

$$L(Th_k^n) \geq k(n - k + 1)$$

Beweis:

A sei die Menge aller Vektoren mit genau k Einsen.

Beweis:

A sei die Menge aller Vektoren mit genau k Einsen.

B sei die Menge aller Vektoren mit genau $k-1$ Einsen.

Beweis:

A sei die Menge aller Vektoren mit genau k Einsen.

B sei die Menge aller Vektoren mit genau $k-1$ Einsen.

Es folgt:

$$|A \otimes B| = k|A| = (n-k+1)|B|$$

Beweis:

A sei die Menge aller Vektoren mit genau k Einsen.

B sei die Menge aller Vektoren mit genau $k-1$ Einsen.

Es folgt:

$$|A \otimes B| = k|A| = (n-k+1)|B|$$

Somit

$$L(Th_k^n) \geq \frac{(n-k+1)|A| \cdot k|B|}{|A| \cdot |B|} = k(n-k+1)$$

Ende Teil 1, Teil 2 nächste Woche

Definition [kombinatorisches Rechteck]

- $R = A \times B$, $A, B \subset \{0,1\}^n$ disjunkt
- $S \subset R$ Unterrechteck, falls S ebenfalls ein Rechteck ist

Definition [Monochrom]

Ein Rechteck $R = A \times B$ heißt monochrom, wenn ein Index i existiert, so dass

$$a_i \neq b_i \text{ für alle Kanten } (a, b) \in R$$

Analog ist R positiv monochrom, wenn

$$a_i = 1,\ b_i = 0 \text{ für alle Kanten } (a, b) \in R$$

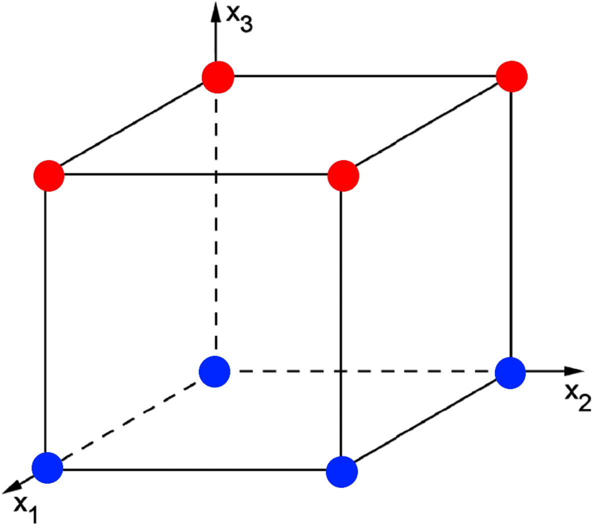

Figure: (positiv) monochromes Rechteck

Definition [Partitionszahl]

- R Rechteck, f boolsche Funktion
- $\chi(R)$ Partitionszahl
- Größe der kleinsten Partition in **disjunkte** monochrome Rechtecke
- $\chi_+(R)$ analog für positiv monochrome Rechtecke
- $\chi(f) := \chi(f^{-1}(1) \times f^{-1}(0))$

Definition [Tensoroperator]

Sei R ein Rechteck.

$$A \otimes B := \{(a, b) \in R | a \sim b\}$$

Wobei $a \sim b$, falls a und b sich in genau einem Bit unterscheiden.

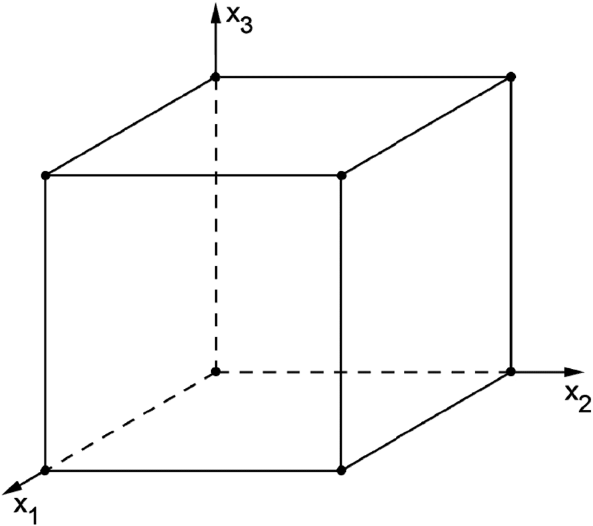

Figure: Beispiel Tensoroperator

Theorem [Khrapchenko 1971]

Sei f eine boolsche Funktion, die das Rechteck $A \times B$ separiert. Dann gilt:

$$L(f) \geq \frac{|A \otimes B|^2}{|A| \cdot |B|} \in O(n^2)$$

Forschung seit 1971

Elias Koutsoupias: Improvements on Khrapchenko's theorem (1993)

"[...] we know of no Boolean function where our method improves upon Kharapchenko's theorem by a factor *larger than two*, when A, B are chosen appropriately"

Somit $O(n^2)$!

Quelle: `cs.ox.ac.uk`

Weitere Forschung seit 1971

S. Laplante, T. Lee, M. Szegedy: The Quantum Adversary Method and Classical Formula Size Lower Bounds (2006)

Zu einem Optimierungsansatz von Karchmer (1995):

"They show that this bound is larger than the bound given by Kharapchenko's method, but cannot prove lower bounds larger than n^2"

Weitere Forschung seit 1971

S. Laplante, T. Lee, M. Szegedy: The Quantum Adversary Method and Classical Formula Size Lower Bounds (2006)

Zu einem Optimierungsansatz von Karchmer (1995):

“They show that this bound is larger than the bound given by Kharapchenko’s method, but cannot prove lower bounds larger than n^2”

Wieso ist die n^2 Schranke so schwierig zu brechen?

Definition Komplexitätsmaß

Sei $\mathcal{F}_n$ die Menge aller boolschen Funktionen der Form

$$f : \{0,1\}^n \rightarrow \{0,1\}$$

Eine Funktion $\nu : \mathcal{F}_n \rightarrow \mathbb{R}$ heisst *formles Komplexitätsmaß*, wenn

Definition Komplexitätsmaß

Sei $\mathcal{F}_n$ die Menge aller boolschen Funktionen der Form

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

Eine Funktion $\nu : \mathcal{F}_n \to \mathbb{R}$ heisst *formles Komplexitätsmaß*, wenn

(a) Das Maß jeden Literals ≤ 1 ist (Normalisierung)

Definition Komplexitätsmaß

Sei $\mathcal{F}_n$ die Menge aller boolschen Funktionen der Form

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

Eine Funktion $\nu : \mathcal{F}_n \to \mathbb{R}$ heisst *formles Komplexitätsmaß*, wenn

(a) Das Maß jeden Literals ≤ 1 ist (Normalisierung)

(b) Fuer alle $g, h \in \mathcal{F}_n$ gilt, dass

$$\nu(g \vee h) \leq \nu(g) + \nu(h)$$

(Subadditivität)

Subadditives Rechtecksmaß

$\mathcal{R}(S)$: Menge aller Unterrechtecke von S.

Subadditives Rechtecksmaß

$\mathcal{R}(S)$: Menge aller Unterrechtecke von S.

$\mu : \mathcal{R}(S) \to \mathbb{R}$ *(stark) subadditives Rechtecksmaß*, wenn

(i) (Normalisierung) $\mu(M) \leq 1$, M monochrom

(ii) (Subadditivität) Für disjunkte Partition $R = R_1 \cup \cdots \cup R_m$

$$\mu(R) \leq \sum_{i=1}^{m} \mu(R_i)$$

Subadditives Rechtecksmaß

$\mathcal{R}(S)$: Menge aller Unterrechtecke von S.

$\mu : \mathcal{R}(S) \to \mathbb{R}$ *(stark) subadditives Rechtecksmaß*, wenn

(i) (Normalisierung) $\mu(M) \leq 1$, M monochrom

(ii) (Subadditivität) Für disjunkte Partition $R = R_1 \cup \cdots \cup R_m$

$$\mu(R) \leq \sum_{i=1}^{m} \mu(R_i)$$

- **Subadditivität**: $m = 2$
- **Starke Subadditivität**: m beliebig

Gebrochene Partitionen

Seien

- R ein Rechteck
- $R_1, \ldots, R_m$ dessen Unterrechtecke mit
- Gewichten $r_1, \ldots, r_m \in [0, 1]$

Gebrochene Partitionen

Seien

- R ein Rechteck
- $R_1, \ldots, R_m$ dessen Unterrechtecke mit
- Gewichten $r_1, \ldots, r_m \in [0, 1]$

$R_1, \ldots, R_m$ bilden eine *gebrochene Partition*, wenn für alle Kanten e

$$\sum_{i:e \in R_i} r_i = 1$$

gilt.

Konvexität

Sei μ stark subadditives Rechtecksmaß.

Konvexität

Sei μ stark subadditives Rechtecksmaß.

μ ist *konvex*, wenn für beliebige gebrochene Partitionen $S = \sum_{i=1}^{m} r_i R_i$

$$\mu(S) \leq \sum_{i=1}^{m} r_i \mu(R_i)$$

gilt.

Überblick Maße

- Subadditiv:

$$\mu(R) \leq \mu(R_1) + \mu(R_2)$$

Überblick Maße

- Subadditiv:

$$\mu(R) \leq \mu(R_1) + \mu(R_2)$$

- Stark Subadditiv:

$$\mu(R) \leq \sum_{i=1}^{m} \mu(R_i)$$

Überblick Maße

- Subadditiv:

$$\mu(R) \leq \mu(R_1) + \mu(R_2)$$

- Stark Subadditiv:

$$\mu(R) \leq \sum_{i=1}^{m} \mu(R_i)$$

- Konvex:

$$\mu(R) \leq \sum_{i=1}^{m} r_i \mu(R_i)$$

Gebrochene Partitionsnummer

Die gebrochene Partitionsnummer ist das Minimum

$$\pi(S) := \min \sum_{i=1}^{t} r_i$$

über alle **monochromen** gebrochenen Partitionen $R_1, \ldots, R_t$ und Gewichte $r_1, \ldots, r_t$.

Gebrochene Partitionsnummer

Die gebrochene Partitionsnummer ist das Minimum

$$\pi(S) := \min \sum_{i=1}^{t} r_i$$

über alle **monochromen** gebrochenen Partitionen $R_1, \ldots, R_t$ und Gewichte $r_1, \ldots, r_t$.
Hierbei handelt es sich um die gewichtete Version von $\chi(S)$

Lemma subadditive Rechtecksmaße

$\chi(R)$ ist das größte stark subadditive Rechtecksmaß, d.h.

- $\chi(R)$ ist stark subadditiv
- $\mu(R) \leq \chi(R)$

für alle Rechtecke R und stark subadditiven Rechtecksmaßen μ.

Lemma subadditive Rechtecksmaße

$\chi(R)$ ist das größte stark subadditive Rechtecksmaß, d.h.

- $\chi(R)$ ist stark subadditiv
- $\mu(R) \leq \chi(R)$

für alle Rechtecke R und stark subadditiven Rechtecksmaßen μ.

Lemma konvexe Rechtecksmaße

$\pi(R)$ ist das größte konvexe Rechtecksmaß, d.h.

- $\pi(R)$ ist konvex
- $\mu(R) \leq \pi(R)$

für alle Rechtecke R und konvexe Rechtecksmaßen μ.

Beweis konvexe Rechtecksmaße

Zu zeigen: π ist konvex.

Beweis konvexe Rechtecksmaße

Zu zeigen: π ist konvex. Seien

- $S = \sum_j r_j \; \boxed{R_j}$ eine gebrochene Partition
- $\boxed{R_j = \sum_i s_{ij} M_{ij}}$ gebrochene Partitionen für alle j, so dass
  - M_{ij} monochrom
  - $\pi(R_j) = \sum_i s_{ij}$ (sprich minimal)

Beweis konvexe Rechtecksmaße

Zu zeigen: π ist konvex. Seien

- $S = \sum_j r_j R_j$ eine gebrochene Partition
- $R_j = \sum_i s_{ij} M_{ij}$ gebrochene Partitionen für alle j, so dass
  - M_{ij} monochrom
  - $\pi(R_j) = \sum_i s_{ij}$ (sprich minimal)

Dies kann man umformen zu

$$S = \sum_{ij} r_j s_{ij} M_{ij}$$

Beweis konvexe Rechtecksmaße

Zu zeigen: π ist konvex. Seien

- $S = \sum_j r_j R_j$ eine gebrochene Partition
- $R_j = \sum_i s_{ij} M_{ij}$ gebrochene Partitionen für alle j, so dass
  - M_{ij} monochrom
  - $\pi(R_j) = \sum_i s_{ij}$ (sprich minimal)

Dies kann man umformen zu

$$S = \sum_{ij} r_j s_{ij} M_{ij}$$

Da π das Minimum zurückgibt, gilt

$$\pi(S) \leq \sum_{ij} r_j s_{ij} = \sum_j r_j \pi(R_j)$$

Beweis konvexe Rechtecksmaße 2

Sei nun μ ein beliebiges Konvexitätsmaß. Dann gilt

$$\begin{aligned} \mu(S) &\leq \sum_i r_i \mu(M_i) && \text{Konvexität} \\ &\leq \sum_i r_i && \text{Normalität} \\ &= \pi(S) \end{aligned}$$

Konvexe Schranken

[Hrubes, Jukna, Kulikov, Pudlak 2010]

Sei μ ein Konvexitätsmaß, dann gilt

$$\mu(S) \leq \frac{9}{8}(n^2 + n)$$

für jedes n-dimensionales Rechteck S

Definition zyklische Gruppe

Sei $\mathbb{Z}_2 = (\{0, 1\}, +, \cdot)$ der zyklische Körper vom Grad 2.

- $+$ ist die Addition modulo 2
- $\cdot$ ist $\wedge$

Definition zyklische Gruppe

Sei $\mathbb{Z}_2 = (\{0, 1\}, +, \cdot)$ der zyklische Körper vom Grad 2.

- $+$ ist die Addition modulo 2
- $\cdot$ ist $\wedge$

Satz 1

Jeder Vektor $v \in \mathbb{Z}_2^n \backslash \{0\}$ ist genau zu der Hälfte aller Vektoren aus $\{0, 1\}^n$ orthogonal.

Beweis

Seien

- $v, w \in \{0,1\}^n$ beliebig
- s Anzahl der Nullen in v
- $r = n - s$ Anzahl der Einsen in v

Beweis

Seien

- $v, w \in \{0,1\}^n$ beliebig
- s Anzahl der Nullen in v
- $r = n - s$ Anzahl der Einsen in v

Orthogonalität ist definiert als

$$\langle v, w \rangle := \sum_{i=1}^{n} v_i w_i = 0$$

Beweis

Seien

- $v, w \in \{0,1\}^n$ beliebig
- s Anzahl der Nullen in v
- $r = n - s$ Anzahl der Einsen in v

Orthogonalität ist definiert als

$$\langle v, w \rangle := \sum_{i=1}^{n} v_i w_i = 0$$

Wir haben

- s Freiheitsgerade, da $0 \cdot w_i = 0$
- $r - 1$ Freiheitsgerade, da $\forall k : 2k \bmod 2 = 0$

Beweis

Seien

- $v, w \in \{0,1\}^n$ beliebig
- s Anzahl der Nullen in v
- $r = n - s$ Anzahl der Einsen in v

Orthogonalität ist definiert als

$$\langle v, w \rangle := \sum_{i=1}^{n} v_i w_i = 0$$

Wir haben

- s Freiheitsgerade, da $0 \cdot w_i = 0$
- $r - 1$ Freiheitsgerade, da $\forall k : 2k \bmod 2 = 0$

Somit

$$2^s \cdot 2^{r-1} = 2^{s+r-1} = 2^{n-1}$$

orthogonale Vektoren

Definition Paritätsrechtecke

Sei $I \subseteq [n] := \{1, \ldots, n\}$.
Dann sind die I-Paritätsrechtecke definiert als

$$S_I := \{x \in \{0,1\}^n : \bigoplus_{i \in I} x_i = 0\} \times \{y \in \{0,1\}^n : \bigoplus_{i \in I} y_i = 1\}$$

$$T_I = \{(y, x) : (x, y) \in S_I\}$$

Satz 2

Jede Kante $(x, y) \in \{0,1\}^n \times \{0,1\}^n$, $x \neq y$ gehört zu 2^{n-1} Paritätsrechtecken.

Satz 2

Jede Kante $(x, y) \in \{0,1\}^n \times \{0,1\}^n$, $x \neq y$ gehört zu 2^{n-1} Paritätsrechtecken.

Beweisskizze

- Sei $I \subseteq [n]$, $v_I \in \{0,1\}^n$ charakteristischer Vektor

Satz 2

Jede Kante $(x, y) \in \{0,1\}^n \times \{0,1\}^n$, $x \neq y$ gehört zu 2^{n-1} Paritätsrechtecken.

Beweisskizze

- Sei $I \subseteq [n]$, $v_I \in \{0,1\}^n$ charakteristischer Vektor
- $x \oplus y$ nicht orthogonal zu 2^{n-1} Vektoren (Satz 1)

Satz 2

Jede Kante $(x, y) \in \{0,1\}^n \times \{0,1\}^n$, $x \neq y$ gehört zu 2^{n-1} Paritätsrechtecken.

Beweisskizze

- Sei $I \subseteq [n]$, $v_I \in \{0,1\}^n$ charakteristischer Vektor
- $x \oplus y$ nicht orthogonal zu 2^{n-1} Vektoren (Satz 1)
- Diese kann man als v_I interpretieren

Satz 2

Jede Kante $(x, y) \in \{0,1\}^n \times \{0,1\}^n$, $x \neq y$ gehört zu 2^{n-1} Paritätsrechtecken.

Beweisskizze

- Sei $I \subseteq [n]$, $v_I \in \{0,1\}^n$ charakteristischer Vektor
- $x \oplus y$ nicht orthogonal zu 2^{n-1} Vektoren (Satz 1)
- Diese kann man als v_I interpretieren
- (x, y) in 2^{n-1} Paritätsrechtecken

Satz 3

Sei μ ein Rechtecksmaß. Dann gilt für alle $I \subseteq [n]$

$$\mu(S_I) \leq \frac{9}{8}|I|^2$$

sowie

$$\mu(T_I) \leq \frac{9}{8}|I|^2$$

Satz 3

Sei μ ein Rechtecksmaß. Dann gilt für alle $I \subseteq [n]$

$$\mu(S_I) \leq \frac{9}{8}|I|^2$$

sowie

$$\mu(T_I) \leq \frac{9}{8}|I|^2$$

Folgerung aus

Theorem [Yablonskii 1954]

Sei $n \in \mathbb{N}$ mit $n \geq 2$. Dann

$$L(\oplus_n) \leq 3np_n - 2p_n^2 \leq \frac{9}{8}n^2,$$

wobei $p_n = 2^{\lfloor log_2 n \rfloor}$.

Zu Zeigen:

[Hrubes, Jukna, Kulikov, Pudlak 2010]

Sei μ ein Konvexitätsmaß, dann gilt

$$\mu(S) \leq \frac{9}{8}(n^2 + n)$$

für jedes n-dimensionales Rechteck S

Beweis

Seien

- S ein n-dimensionales Rechteck, $I \subseteq [n]$, $|I| = i$

Beweis

Seien

- S ein n-dimensionales Rechteck, $I \subseteq [n]$, $|I| = i$
- μ Konvexitätsmaß

Beweis

Seien

- S ein n-dimensionales Rechteck, $I \subseteq [n]$, $|I| = i$
- μ Konvexitätsmaß
- $\mathcal{R}(S)$ die Multimenge aller Paritätsrechtecke bzgl S und I, sprich
$$(S_I \cup T_I) \cap S$$

Beweis

Seien

- S ein n-dimensionales Rechteck, $I \subseteq [n]$, $|I| = i$
- μ Konvexitätsmaß
- $\mathcal{R}(S)$ die Multimenge aller Paritätsrechtecke bzgl S und I, sprich
$$(S_I \cup T_I) \cap S$$

Dann

- Jede Kante in S gehört zu 2^{n-1} Elementen in $\mathcal{R}(S)$

Beweis

Seien

- S ein n-dimensionales Rechteck, $I \subseteq [n]$, $|I| = i$
- μ Konvexitätsmaß
- $\mathcal{R}(S)$ die Multimenge aller Paritätsrechtecke bzgl S und I, sprich
$$(S_I \cup T_I) \cap S$$

Dann

- Jede Kante in S gehört zu 2^{n-1} Elementen in $\mathcal{R}(S)$

Satz 2

Jede Kante $(x, y) \in \{0,1\}^n \times \{0,1\}^n$, $x \neq y$ gehört zu 2^{n-1} Paritätsrechtecken.

- Somit ist $\mathcal{R}(S)$ eine gebrochene Partition mit Gewicht
$$r_R = \frac{1}{2^{n-1}}$$
für jedes Rechteck $R \in \mathcal{R}(S)$, da

- Somit ist $\mathcal{R}(S)$ eine gebrochene Partition mit Gewicht
$$r_R = \frac{1}{2^{n-1}}$$
für jedes Rechteck $R \in \mathcal{R}(S)$, da

Gebrochene Partitionen

$R_1, \ldots, R_m$ bilden eine *gebrochene Partition*, wenn für alle Kanten e
$$\sum_{i:e \in R_i} r_i = 1$$
gilt.

- Somit ist $\mathcal{R}(S)$ eine gebrochene Partition mit Gewicht

$$r_R = \frac{1}{2^{n-1}}$$

für jedes Rechteck $R \in \mathcal{R}(S)$, da

- Zudem wissen wir, dass

$$\mu(R) \leq \frac{9}{8} i^2$$

Somit folgt

$$\mu(S) \underbrace{\leq}_{\text{konvex}} \sum_{R \in \mathcal{R}(S)} r_R \mu(R) = \frac{1}{2^{n-1}} \sum_{R \in \mathcal{R}(S)} \mu(R)$$

Somit folgt

$$\mu(S) \leq \sum_{R \in \mathcal{R}(S)} r_R \mu(R) = \frac{1}{2^{n-1}} \sum_{R \in \mathcal{R}(S)} \mu(R)$$
$$= \frac{1}{2^{n-1}} \sum_{i=1}^{n} \sum_{\substack{R \in \mathcal{R}(S) \\ |R|=i}} \mu(R)$$

Somit folgt

$$\mu(S) \leq \sum_{R \in \mathcal{R}(S)} r_R \mu(R) = \frac{1}{2^{n-1}} \sum_{R \in \mathcal{R}(S)} \mu(R)$$

$$= \frac{1}{2^{n-1}} \sum_{i=1}^{n} \sum_{\substack{R \in \mathcal{R}(S) \\ |R|=i}} \mu(R)$$

$$\leq \frac{1}{2^{n-1}} \sum_{i=1}^{n} 2 \binom{n}{i} \frac{9}{8} i^2$$

wobei

- $|I| = i$
- $\mu(R) \leq \frac{9}{8} i^2$ (Satz 3)
- 2, da S_I und T_I

Somit folgt

$$\mu(S) \leq \sum_{R \in \mathcal{R}(S)} r_R \mu(R) = \frac{1}{2^{n-1}} \sum_{R \in \mathcal{R}(S)} \mu(R)$$

$$= \frac{1}{2^{n-1}} \sum_{i=1}^{n} \sum_{\substack{R \in \mathcal{R}(S) \\ |R|=i}} \mu(R)$$

$$\leq \frac{1}{2^{n-1}} \sum_{i=1}^{n} 2 \binom{n}{i} \frac{9}{8} i^2 = \frac{1}{2^{n-2}} \frac{9}{8} \sum_{i=1}^{n} \binom{n}{i} i^2$$

Somit folgt

$$
\begin{aligned}
\mu(S) &\leq \sum_{R \in \mathcal{R}(S)} r_R \mu(R) = \frac{1}{2^{n-1}} \sum_{R \in \mathcal{R}(S)} \mu(R) \\
&= \frac{1}{2^{n-1}} \sum_{i=1}^{n} \sum_{\substack{R \in \mathcal{R}(S) \\ |R| = i}} \mu(R) \\
&\leq \frac{1}{2^{n-1}} \sum_{i=1}^{n} 2 \binom{n}{i} \frac{9}{8} i^2 = \frac{1}{2^{n-2}} \frac{9}{8} \sum_{i=1}^{n} \binom{n}{i} i^2 \\
&= \ldots
\end{aligned}
$$

Somit folgt

$$
\begin{aligned}
\mu(S) &\leq \sum_{R \in \mathcal{R}(S)} r_R \mu(R) = \frac{1}{2^{n-1}} \sum_{R \in \mathcal{R}(S)} \mu(R) \\
&= \frac{1}{2^{n-1}} \sum_{i=1}^{n} \sum_{\substack{R \in \mathcal{R}(S) \\ |R|=i}} \mu(R) \\
&\leq \frac{1}{2^{n-1}} \sum_{i=1}^{n} 2 \binom{n}{i} \frac{9}{8} i^2 = \frac{1}{2^{n-2}} \frac{9}{8} \sum_{i=1}^{n} \binom{n}{i} i^2 \\
&= \ldots \\
&= \frac{1}{2^{n-2}} \frac{9}{8} (n^2 + n) 2^{n-2}
\end{aligned}
$$

Somit folgt

$$\begin{aligned}
\mu(S) &\leq \sum_{R\in\mathcal{R}(S)} r_R\mu(R) = \frac{1}{2^{n-1}} \sum_{R\in\mathcal{R}(S)} \mu(R) \\
&= \frac{1}{2^{n-1}} \sum_{i=1}^{n} \sum_{\substack{R\in\mathcal{R}(S)\\ |R|=i}} \mu(R) \\
&\leq \frac{1}{2^{n-1}} \sum_{i=1}^{n} 2\binom{n}{i}\frac{9}{8}i^2 = \frac{1}{2^{n-2}}\frac{9}{8}\sum_{i=1}^{n}\binom{n}{i}i^2 \\
&= \ldots \\
&= \frac{1}{2^{n-2}}\frac{9}{8}(n^2+n)2^{n-2} \\
&= \frac{9}{8}(n^2+n)
\end{aligned}$$

Zusammenfassend:

- Konvexe Maße können nicht die $O(n^2)$ Schranke brechen

Zusammenfassend:

- Konvexe Maße können nicht die $O(n^2)$ Schranke brechen

[Hrubes, Jukna, Kulikov, Pudlak 2010]

Sei μ ein Konvexitätsmaß, dann gilt

$$\mu(S) \leq \frac{9}{8}(n^2 + n)$$

für jedes n-dimensionales Rechteck S

Zusammenfassend:

- Konvexe Maße können nicht die $O(n^2)$ Schranke brechen

[Hrubes, Jukna, Kulikov, Pudlak 2010]

Sei μ ein Konvexitätsmaß, dann gilt

$$\mu(S) \leq \frac{9}{8}(n^2 + n)$$

für jedes n-dimensionales Rechteck S

- Danke für alle tollen Vorträge

Vielen Dank für eure Aufmerksamkeit

Quellen

- **Boolean Function Complexity - Advances and Frontiers**
  - Stasys Jukna 2012
    doi.org/10.1007/978-3-642-24508-4
- **On convex complexity measures**
  - Pavel Hrubeš, Stasys Jukna, Alexander Kulikov, Pavel Pudlák 2010
    doi.org/10.1016/j.tcs.2010.02.004
- **Bild zum 3D Würfel**
  - https://www.mathelike.de/images/stories/B2014BA_PT_B_G_2/B2014BA_PT_B_G_2_a_01.png

Quellen

- **Improvements on Khrapchenko's theorem**
  - Elias Koutsoupias
    Theoretical Computer Science. Vol. 116, 1993
- **The Quantum Adversary Method and Classical Formula Size Lower Bounds**
  - Sophie Laplante, Troy Lee, Mario Szegedy
    Computational Complexity 15, 2006

Satz 3

Sei μ ein Rechtecksmaß. Dann gilt für alle $I \subseteq [n]$

$$\mu(S_I) \leq \frac{9}{8}|I|^2 \text{ sowie } \mu(T_I) \leq \frac{9}{8}|I|^2$$

Theorem [Yablonskii 1954]

Sei $n \in \mathbb{N}$ mit $n \geq 2$. Dann

$$L(\oplus_n) \leq 3np_n - 2p_n^2 \leq \frac{9}{8}n^2,$$

wobei $p_n = 2^{\lfloor log_2 n \rfloor}$.

Lemma [Rychkov 1985]

Für jede boolsche Funktion f und jede monotone boolsche Funktion g gilt:

$$L(f) \geq \chi(f), L_+(g) \geq \chi_+(g)$$