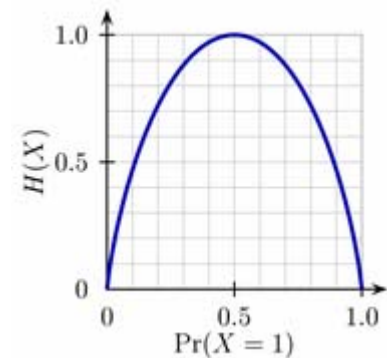


Information und Kommunikation

Hartmut Klauck
Universität Frankfurt
SS 07
22.6.



Eine untere Schranke

- Equality: $EQ(x,y)=1$ wenn $x=y$
- Eine Folge von Nachrichten/Berechnung des Protokolls ergibt ein Rechteck $R=U \times V$ in der Kommunikationsmatrix, wobei $U \subseteq X$ und $V \subseteq Y$:
 - Alice schränkt durch ihre Nachrichten Zeilen ein
 - Bob schränkt Spalten ein
- Alle Eingaben in R haben denselben Funktionswert, ansonsten macht das Protokoll Fehler
- Das Protokoll partitioniert $\{0,1\}^n \times \{0,1\}^n$ in Rechtecke, die keinen Fehler haben
- Es muss also mindestens 2^n 1-Rechtecke geben und mindestens ein 0-Rechteck
- Daher ist die Kommunikation mindestens $\lceil \log(2^n + 1) \rceil = n+1$
- Das triviale Protokoll ist somit optimal

Rechtecke

- Für jeden Knoten v im Protokollbaum sei R_v die Menge der Eingaben x,y , die v erreichen, d.h. für die v auf dem Berechnungspfad zu x,y liegt
- R_v ist immer ein Rechteck, d.h. es gibt $S \subseteq X$ und $T \subseteq Y$ mit $R_v = S \times T$
 - Beweis durch Induktion
- Die Menge der Rechtecke R_v die zu Blättern gehören bildet eine Partition der Eingabe, d.h. der Menge $X \times Y$ (jede Eingabe landet in einem Blatt)
- Alle Eingaben x,y in R_v zu einem Blatt v haben denselben Funktionswert
- Ein 1-Rechteck besteht aus Eingaben, die $f(x,y)=1$ erfüllen, ein 0-Rechteck $f(x,y)=0$
- Allgemeiner heißt ein Rechteck monochromatisch, wenn alle seine Elemente denselben Funktionswert haben

Rechtecke

- **Theorem 19.1**
 - Wenn jede Partition der Kommunikationsmatrix in monochromatische Rechtecke mindestens t Rechtecke enthält, dann gilt $D(f) \geq \log t$
- Beweis: Jedes Protokoll mit Kommunikation c für f entspricht einem Baum mit höchstens 2^c Blättern. Die Rechtecke bilden eine Partition der Eingaben in monochromatische Rechtecke

Rechtecke

- Wie zeigen wir, dass wir viele Rechtecke benötigen?
- Wir können wieder argumentieren, dass alle Rechtecke klein sind
- Dazu legen wir eine Verteilung μ auf die Eingaben
- $b(f, \mu, a)$ sei die Größe des größten Rechtecks unter μ , welches nur x, y mit $f(x, y) = a$ enthält
- Wenn alle a -chromatischen Rechtecke Größe $\leq b(f, \mu, a)$ haben, muss die Partition der Eingaben durch ein Protokoll mindestens $\mu(f^{-1}(a)) / b(f, \mu, a)$ Rechtecke enthalten
- Wir erhalten
- **Theorem 19.2**
 - Für $f: X \times Y \rightarrow Z$ gilt:
 - $D(f) \geq \max_{a \in Z} \max_{\mu} -\log b(f, \mu, a)$
- Hinweis: μ läuft über Verteilungen auf den Eingaben mit $f(x, y) = a$. Dabei müssen Rechtecke immer noch monochromatisch sein, d.h. keine x, y mit $f(x, y) \neq a$ enthalten

Beispiel

- Greater Than: Die Matrix ist eine obere Dreiecksmatrix
- Wenn wir μ uniform auf allen 1-Eingaben wählen, gibt es ein 1-chromatisches Rechteck mit Größe $1/4$
- Stattdessen wählen wir μ uniform auf den Einträgen der Diagonale
- Keine zwei dieser Einträge liegen im selben Rechteck, daher ist $b(GT, \mu, 1) = 1/2^n$
- $D(GT) \geq n$

Beispiel

- Die Inner Product Funktion
- $IP:\{0,1\}^n \times \{0,1\}^n \rightarrow \{0,1\}$
- $IP(x,y) = \sum x_i y_i \pmod{2}$
- **Theorem 19.3**
 - $D(IP) \geq \Omega(n)$
- **Beweis:**
 - Wir betrachten 0-chromatische Rechtecke
 - Wir zeigen, dass jedes 0-chromatische Rechteck nur höchstens 2^n Eingaben x,y enthalten kann
 - Damit muss es mindestens $(2^{2n}/2)/2^n$ Rechtecke geben
 - „Schwierige“ Verteilung ist dabei die Gleichverteilung

Beweis 19.3

- Wir wollen also zeigen, dass unter der Gleichverteilung auf den 0-Eingaben $\mu(R) \leq 2^{-(n-1)}$ für alle Rechtecke ohne 1Eingaben
- Damit folgt dann $D(IP) \geq n-1$
- Sei $R=A \times B$
- A ist eine Menge von Vektoren in \mathbb{Z}_2^n (Eingaben x)
- A' sei der von A aufgespannte Unterraum
- Analog B'

Beweis 19.3

- $R' = A' \times B'$ ist ein Rechteck
- R' ist 0-chromatisch:
 - $\langle x+x', y+y' \rangle = \langle x, y \rangle + \langle x', y \rangle + \langle x, y' \rangle + \langle x', y' \rangle = 0$
- R' ist größer als R
- A' und B' sind zueinander orthogonale Unterräume
- Daher gilt $\dim(A') + \dim(B') \leq n$
- $|R'| = |A'| \cdot |B'| \leq 2^{\dim(A')} \cdot 2^{\dim(B')} \leq 2^n$

Die Rang Schranke

- Wir betrachten jetzt eine andere untere Schranke
- Zu $f: X \times Y \rightarrow \{0,1\}$ ist M_f die Kommunikationsmatrix
- $\text{rang}(M)$ bezeichne den Rang einer Matrix über den reellen Zahlen
- **Theorem 19.4**
 - $D(f) \geq \log \text{rang}(M_f)$

Beweis 19.4

- P sei ein Protokoll für f
- L_1 sei die Menge der akzeptierenden Blätter
- Für jedes Blatt $l \in L_1$ sei R_l das Rechteck der Eingaben, die l erreichen
- M_l sei die Matrix die für $x, y \in R_l$ den Eintrag 1 hat, für alle anderen Eingaben den Eintrag 0
- $M_f = \sum_{l \in L_1} M_l$

Beweis 19.4

- Es gilt somit:
- $\text{rang}(M_f) \leq \sum_{I \in L_1} \text{rang}(M_I)$
- $\text{rang}(M_I) = 1$
- Damit ist $\text{rang}(M_f) \leq |L_1|$
- D.h. P muss mindestens $\text{rang}(M_f)$ viele Blätter haben, daher ist die Tiefe des Protokollbaums mindestens $\log \text{rang}(M_f)$

Rang Schranke

- Einige Beispiele:
- $f=EQ$: $\text{rang}(M_f)=2^n$
- $f=GT$: $\text{rang}(M_f)=2^n$
- $f=IP$: $\text{rang}(M_f) \geq 2^n$:
 - Wir betrachten M_f^2
 - Eintrag x,y ist dann $\sum_z \langle x,z \rangle \cdot \langle z,y \rangle$
 - Das ist die Anzahl der z mit $\langle x,z \rangle = \langle z,y \rangle = 1$
 - Auf der Diagonalen steht damit 2^{n-1} , die restlichen Einträge sind 2^{n-2} , außer Zeile/Spalte 1
 - Also $\text{rang}(M_f) \geq \text{rang}(M_f^2) \geq 2^{n-1}$
- Warnung: der Rang von M_{IP} über Z_2 ist nur n

Rang Schranke

- $\text{rang}(M) = \min\{k: M = \sum_{i=1 \dots k} M_i, \text{ und } \text{rang}(M_i) = 1\}$
- Für $D(f)$ partitionieren wir in monochromatische Rechtecke, für $\text{rang}(M)$ in Rang 1 Matrizen
- „Rang Vermutung“:
 - $\log \text{rang}(M_f) \leq D(f) \leq \text{poly}(\log \text{rang}(M_f))$
 - Bisher bekannt:
 - $D(f) \leq \text{rang}(M_f)$
 - Es gibt ein f , für das $\log \text{rang}(M_f)$ polynomiell kleiner ist als $D(f)$

Überdeckungen

- Ein Rechteck ist eine Menge $A \times B$ für $A \subseteq X$ und $B \subseteq Y$
- Ein Rechteck R ist a -chromatisch, wenn für alle $x, y \in R$ gilt, dass $f(x, y) = a$
- Rechtecke, die a -chromatisch sind für ein a sind monochromatisch
- Eine Überdeckung der a -Eingaben in einer Kommunikationsmatrix M_f ist eine Menge von a -chromatischen Rechtecken, so dass jedes x, y mit $f(x, y) = a$ in mind. einem der Rechtecke liegt
- Eine Überdeckung der Eingaben in einer Kommunikationsmatrix ist eine Menge von monochromatischen Rechtecken, so dass jedes x, y in mindestens einem der Rechtecke liegt
- Eine Überdeckung ist disjunkt, bzw. eine Partition, wenn alle Rechtecke paarweise disjunkt sind.

Überdeckungen

- Ein deterministisches Protokoll induziert eine Partition der Kommunikationsmatrix in monochromatische Rechtecke
- Nicht jede solche Partition entspricht einem Protokoll
- Wie weit kann $D(f)$ von dem \log der Anzahl Rechtecke entfernt sein?

Überdeckungen

- Definition 19.5
 - $f: X \times Y \rightarrow \{0,1\}$ sei eine Funktion
 - $C^P(f)$ sei die kleinste Anzahl Blätter in einem Protokollbaum für f
 - $C^D(f)$ sei die kleinste Anzahl monochromatischer Rechtecke in einer Partition von M_f (einer Überdeckung mit disjunkten Rechtecken)
 - $C(f)$ sei die kleinste Anzahl monochromatischer Rechtecke in einer Überdeckung von M_f
 - $C^z(f)$ sei die kleinste Anzahl z -chromatischer Rechtecke in einer Überdeckung von M_f

Überdeckungen

- Wir erhalten unmittelbar
- **Theorem 19.6**
 - $C(f) \leq C^D(f) \leq C^P(f) \leq 2^{D(f)}$
 - $C(f) = C^0(f) + C^1(f)$

Nichtdeterminismus

- **Definition 19.7**

- In einem nichtdeterministischen Protokoll für $f: X \times Y \rightarrow \{0,1\}$ erhalten Alice und Bob Eingaben x, y
- Sie können nichtdeterministisch Strings z_A, z_B raten (dieser Vorgang kostet keine Kommunikation, der geratene String ist aber privat)
- Dann wird beliebig kommuniziert
- Eine Eingabe x, y wird akzeptiert, wenn es ein $z = z_A, z_B$ gibt, so dass x, y, z_A, z_B akzeptiert wird
- Alle anderen Eingaben gelten als verworfen
- $N(f)$ bezeichne die minimale Kommunikation in einem nichtdeterministischen Protokoll, das genau die Eingaben in $f^{-1}(1)$ akzeptiert
- Die Ausgabe wird von Bob gegeben, d.h. Bob akzeptiert oder nicht

Nichtdeterminismus

- Beispiel:
 - $\neg\text{EQ}(x,y)=1$ gdw $x \neq y$
 - Alice rät i aus $1, \dots, n$, sendet $x_{i,i}$
 - Bob akzeptiert, wenn $x_i \neq y_i$
 - $N(\neg\text{EQ}) \leq \log n + 1$
- Beispiel:
 - $N(\neg\text{DISJ}(x,y)) \leq \log(n+1)$
 - Alice rät $i=1, \dots, n$. Wenn $x_i=1$ sendet sie i , ansonsten $n+1$
 - Bob akzeptiert wenn $x_i=y_i=1$ und $i \leq n$

Nichtdeterminismus

- Theorem 19.8
 - Wenn $N(f)=k$, dann gibt es ein nichtdeterministisches Einweg Protokoll für f mit Kommunikation k
 - D.h. $N(f)=N^1(f)$
- Beweis:
 - P sei ein nichtdeterministisches Protokoll für f
 - Auf Eingabe x rät Alice einen kompletten Dialog zwischen Alice und Bob, der in P erlaubt ist
 - Alice sendet den Dialog
 - Bob akzeptiert, wenn der Dialog mit y konsistent ist, und zum akzeptieren führen würde (in P)

Nichtdeterminismus

- Eine Bemerkung:
 - Wir haben untere Schranken für Formellänge mit der Neciporuk Methode gezeigt
 - Dabei wurden Einweg Spiele betrachtet
 - Die Eingaben waren extrem asymmetrisch verteilt (siehe Index Funktion)
 - Sowohl deterministisch als auch randomisiert
 - Solche Schranken versagen für nichtdeterministische Kommunikation (denn z.B. $N^1(\text{Index}) = O(\log n)$)
 - Das ist kein Zufall, denn die Größe einer nichtdeterministischen Formel für ein f ist \approx gleich der Größe eines nichtdeterministischen Schaltkreises
 - D.h. superlineare untere Schranken für nichtdeterministische Formeln sind extrem schwierig zu beweisen