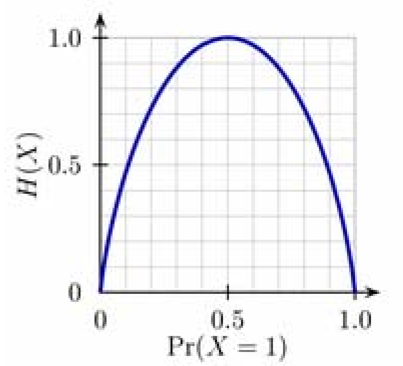
Information und Kommunikation

Hartmut Klauck
Universität Frankfurt

SS 07

6.7.



Schaltkreise und Kommunikation

- Bevor wir das Disjunktheitsproblem untersuchen betrachten wir eine Anwendung der unteren Schranke für R(DISJ)
- Wir analysieren die Tiefe monotoner Schaltkreise

Schaltkreise und Kommunikation

- Ein Schaltkreis ist gegeben durch
  - einen gerichteten azyklischen Graphen
  - jeder innere Knoten hat Eingangsgrad 2
  - jeder Knoten ist markiert mit der Funktion UND, oder ODER, oder einer (negierten) Eingabe
  - Es gibt n Eingaben, die Quellen im Graphen sind
  - Es gibt eine Senke
  - Ein Schaltkreis rechnet, indem (möglicherweise negierte) Variablen an die Eingaben angelegt werden und dann die Gatter/inneren Knoten in topologischer Reihenfolge ausgewertet werden
  - Die Ausgabe wird an der Senke abgelesen
  - Die Größe eines Schaltkreises ist die Anzahl Knoten im Graphen
  - Die Tiefe ist die Länge des längsten Weges von einer Quelle zur Senke
  - Ein Schaltkreis ist monoton, wenn nur unnegierte Eingaben vorkommen

Monotone Funktionen

- x,y seien aus $\{0,1\}^n$
- $x \geq y$, wenn $x_i \geq y_i$ für alle i
- Eine Funktion f heißt monoton, wenn $x \geq y \Rightarrow f(x) \geq f(y)$
- Es gilt: monotone Schaltkreise berechnen monotone Funktionen
- Jede monotone Boolesche Funktion kann von einem monotonen Schaltkreis berechnet werden
- Hinweis: Es gibt monotone Funktionen, für die nichtmonotone Schaltkreise effizienter sind als monotone Schaltkreise

Karchmer Wigderson Spiele

- f sei eine Boolesche Funktion
- Wir definieren ein Kommunikationsspiel wie folgt:
  - Im Spiel G_f
  - erhält Alice eine Eingabe $x \in \{0,1\}^n$ mit $f(x)=1$
  - Bob eine Eingabe $y \in \{0,1\}^n$ mit $f(y)=0$
  - Ihr Ziel ist es, ein i zu finden mit $x_i \neq y_i$
- Hinweis: für konstante Funktionen wie $f(x)=1$ $\forall x$ sind solche Spiele nicht definiert

Karchmer Wigderson Spiele

- In einem Spiel G_f gibt es normalerweise mehrere korrekte Ausgaben zu einer Eingabe
- D.h. Wir betrachten die Kommunikationskomplexität von Relationen
- $R \subseteq X \times Y \times Z$
- In einem Protokoll für R wird zu gegebenem x,y ein z gesucht mit $x,y,z \in R$

Kommunikation und Relationen

- Die Kommunikationskomplexität von Relationen ist völlig analog wie für Funktionen definiert.
- Ein deterministisches Protokoll für eine Relation R berechnet eine Funktion f, und ist korrekt, wenn $(x,y,f(x,y))\in R$ für alle x,y
- Die Kommunikationsmatrix von R enthält an der Stelle x,y die Menge der korrekten Ausgaben a, d.h. mit $(x,y,a)\in R$
- Ein Rechteck W ist monochromatisch, wenn es ein a gibt so dass für alle $x,y\in W$: $(x,y,a)\in R$
- Ein deterministisches Protokoll ergibt eine Partition der Kommunikationsmatrix in monochromatische Rechtecke
- Die Parameter $C(R)$, $C^P(R)$, $C^D(R)$ sind definiert wie zuvor

Karchmer Wigderson Spiele

- Tiefe(f) bezeichne die minimale Tiefe eines Schaltkreises, der f berechnet
- MTiefe(f) bezeichnet die minimale Tiefe eines monotonen Schaltkreises, der f berechnet (für monotone f).
- **Theorem 23.1**

  $D(G_f)$=Tiefe(f)

Beweis 23.1

- Wir zeigen, dass $D(G_f) \leq$ Tiefe(f)
- Gegeben sei ein Schaltkreis für f
- Wir konstruieren ein Protokoll für G_f
- Induktiv
- Tiefe=0:
  - D.h.die Ausgabe ist z_i oder $\neg z_i$ für ein i
  - Somit ist klar, dass $x_i \neq y_i$
  - $D(G_f)=0$
  - Bemerkung: konstante Funktionen sind nicht erlaubt

Beweis 23.1

- Induktionsschritt:
  - Das oberste Gatter von C sei UND, und $C=C_1 \wedge C_2$
  - $f=f_1 \wedge f_2$ für die von C_1 und C_2 berechneten Funktionen
  - $D(G_{f_1}) \leq$ Tiefe(C)-1 und $D(G_{f_2}) \leq$ Tiefe(C)-1
  - $f(x)=1$, $f(y)=0$
    - Daher gilt $f_1(x)=f_2(x)=1$ und $f_1(y)=0$ oder $f_2(y)=0$
  - Bob sendet 1 Bit b, das angibt, ob $f_1(y)=0$ oder $f_2(y)=0$
  - Dann kann per Induktion das Protokoll für f_b verwendet werden
  - Denn: $f_b(x)=1$ und $f_b(y)=0$
  - Also $D(G_f) \leq$ Tiefe(f)-1+1

Beweis 23.1

- Für Oder Gatter wird analog vorgegangen, Alice sendet ein Bit
- Damit ist $D(G_f) \leq$ Tiefe(f)

- Beweis der anderen Richtung $D(G_f) \geq$ Tiefe(f) überspringen wir

KW Spiele

- Tatsächlich kann man obige Simulation verstärken:
  - Angenommen der Eingangsgrad der Gatter ist k
  - Die Tiefe entspricht der Anzahl Runden im Protokoll
  - Pro Runde werden log k Bits kommuniziert
  - Die Gesamtkommunikation verhält sich wie der log der Größe einer Formel

KW Spiele

- Die beste bekannte untere Schranke für Tiefe ist 2log n
- Dies entspricht auch einer n^2 Schranke für die Formellänge (der Paritätsfunktion)
- Man erhält so z.B. die sog. Khrapchenko Methode für untere Schranken für Formellänge

Die Paritätsrelation

- Wir betrachten nun die Paritätsfunktion
- Alice erhält einen String x mit Parität 1
- Bob einen String y mit Parität 0
- Aufgabe ist es, ein i mit $x_i \neq y_i$ zu finden
- Wir nennen die zugrunde liegende Relation $R_{\oplus}$
- Wir zeigen zunächst: $D(R_{\oplus}) \leq 2\log n$

Die Paritätsrelation

- Alice und Bob verwenden binäre Suche für die Bestimmung von i
  - Zu Beginn sei $j=1$, $k=n$
  - Es gilt immer, dass $x_j,\dots,x_k$ und $y_j,\dots,y_k$ verschiedene Parität haben
  - In jeder Runde setze $l=(k-j)/2$
  - Alice sendet die Parität von $x_j,\dots,x_l$
  - Bob sendet die Parität von $y_j,\dots,y_l$
  - Wenn diese gleich sind, setze $j=l$
  - Wenn nicht, dann $k=l$
  - Iteriere, bis $j=k$, Ausgabe j
- Klar: das Protokoll ist korrekt und hat 2log n Bits Kommunikation

Die Paritätsrelation

- Wir zeigen nun, dass obiges Protokoll optimal ist
- **Theorem 23.2**
  $D(R_\oplus) \geq 2\log n$
- Damit muss jeder Schaltkreis für Parität mind. 2log n Tiefe haben (und jede Formel mind. $\Omega(n^2)$ Größe, wenn nur UND ODER NICHT Gatter erlaubt sind)

Beweis 23.2

- Wir zeigen folgendes Lemma:
- **Lemma 23.3** [Khrapchenko]
  - Seien X und Y disjunkte Teilmengen von $\{0,1\}^n$
  - Sei $C=\{(x,y):x\in X,\ y\in Y$, Hamming Distanz von $x,y=1\}$
  - R sei eine Relation definiert durch alle Tripel (x,y,i) mit $x\in X$, $y\in Y$, $x_i\neq y_i$
  - Dann gilt $C^D(R)\geq |C|^2/(|X|\ |Y|)$
- Damit gilt auch $D(R)\geq \log (|C|^2/(|X|\ |Y|))$
- Für die Relation zur Parität gilt $|X|=|Y|=2^n/2$ und $|C|=n2^n/2$
- Also Tiefe(Parität)$\geq$ 2log n

Beweis 23.3

- Ein det. Protokoll induziert eine Partition der Kommunikationsmatrix in monochromatische Rechtecke
- $W_1,\dots,W_t$ seien die Rechtecke
- Setze $m_i=|W_i \cap C|$
- Es gilt $|C|=\sum m_i$ und $\sum_{i=1,\dots,t} |W_i|=|X|\ |Y|$

Beweis 23.3

- j sei die Ausgabe auf Rechteck W_i
- In jeder Zeile x von W_i gibt es höchstens ein y, so dass $(x,y)\in C$
  - Denn für alle y gilt: $x_j \neq y_j$. Weiterhin ist die Hamming Distanz von x,y =1, also ist $x_i=y_i$ für alle $i\neq j$ wenn $x,y\in C$
- Analoges gilt für Spalten
- Daher hat W_i mind. m_i Zeilen und Spalten
- $|W_i|\geq m_i^2$

Beweis 23.3

- $|C|^2=(\sum_{i=1,\ldots,t} m_i)^2$
  $\leq t \cdot \sum_{i=1,\ldots,t} m_i^2$ mit Cauchy Schwartz
  $\leq t \cdot \sum_{i=1,\ldots,t} |W_i|$

  $=t\ |X|\ |Y|$
- Also gilt $t \geq |C|^2/(|X|\ |Y|)$