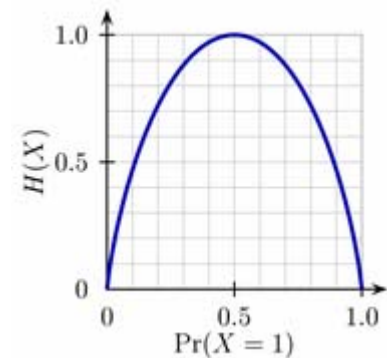


Information und Kommunikation

Hartmut Klauck
Universität Frankfurt
SS 07
15.6.



Public Coin

- **Theorem 17.1 [Newman]**
 1. Ein public coin Protokoll braucht nicht mehr als $\log n + O(1)$ Zufallsbits, d.h. zu einem gegebenen public coin Protokoll für $f: \{0,1\}^n \times \{0,1\}^n \rightarrow \{0,1\}$ mit Kommunikation c und Fehler $1/3$ existiert ein Protokoll mit Kommunikation $O(c)$, Fehler $1/3$ und $\log n + O(1)$ Zufallsbits
 2. $R^1(f) \leq O(R^{1,\text{pub}}(f)) + \log n$
- Der zweite Teil folgt unmittelbar aus dem ersten, denn Alice kann die Zufallsbits privat erzeugen und mit ihrer Nachricht an Bob senden
- Wir wissen aber noch nicht, ob $R^1(\text{EQ}) = \Omega(\log n)$ ist, vielleicht war unser Protokoll nicht optimal?

Randomisierung vs. Determinismus

- Wir wissen bereits, dass $D^1(\text{EQ})=n$ und $R^1(f)=O(\log n)$, d.h. Randomisierung gibt uns eine exponentielle Ersparnis
- **Theorem 17.2**
 - $R^1(f) \geq \Omega(\log D^1(f))$
- D.h. die Ersparnis ist maximal exponentiell

Beweis 17.2

- Idee: Simulation des rand. Protokolls
 - Alice sendet für jede mögliche Nachricht deren Wahrscheinlichkeit (als Zahl)
 - Dann kann Bob einfach bestimmen ob x,y mit hoher Wahrscheinlichkeit ($>2/3$) akzeptiert oder verworfen wird, und somit fehlerfrei $f(x,y)$ entscheiden
 - Problem: Wahrscheinlichkeiten sind reelle Zahlen
- Wir müssen aber nur mit beschränkter Genauigkeit rechnen
- Für alle $2^{R^1(f)}$ möglichen Nachrichten wird die Wahrscheinlichkeit der Nachricht mit jeweils $2R^1(f)$ Bits Genauigkeit kommuniziert
- Bob akzeptiert, wenn das rand. Protokoll mit Wahrsch. $>1/2$ akzeptieren würde
- Die Kommunikation ist damit $O(2^{R^1(f)}R^1(f))$
- Die Summe der tatsächlichen Akzeptierungsws. sei z.B. $p \geq 2/3$
- Der Fehler durch die beschränkte Genauigkeit in der Darstellung der Ws. ist durch $2^{R^1(f)} \cdot 2^{-2R^1(f)}$ beschränkt.
- Damit berechnet Bob eine Ws. von mind $2/3 - 2^{-R^1(f)} > 1/2$ und akzeptiert.

Beweis 17.1

- Gegeben sei ein public coin Protokoll mit Kommunikation c für eine Funktion f , der Fehler sei $1/3$
- OBdA gibt es keine privaten Zufallsbits
- Wenn wir den Wert der öffentlichen Zufallsbits fixieren erhalten wir ein deterministisches Protokoll
- Damit ist ein public coin Protokoll nichts anderes als eine Wahrscheinlichkeitsverteilung auf deterministischen Protokollen

Beweis 17.1

- Es gibt also eine Verteilung Π auf den deterministischen Protokollen mit Kommunikation höchstens c die unser public coin Protokoll beschreibt
- Wir ziehen $t=100n$ Protokolle zufällig gemäß Π
- Diese Protokolle nennen wir P_1, \dots, P_t
- Unser neues Protokoll ist durch die uniforme Verteilung auf P_1, \dots, P_t gegeben
 - D.h. Der public coin ist uniform auf $1, \dots, t$ und die Spieler verwenden P_i wenn i gezogen wurde.
- Wir zeigen, dass es eine Wahl von P_1, \dots, P_t gibt, für die das so konstruierte Protokoll kleinen Fehler hat
- Damit erhalten wir ein gültiges Protokoll mit $\log n + O(1)$ Zufallsbits

Beweis 17.1

- Sei $Z(x,y,P_i)=1$ wenn das Protokoll P_i (mit Kommunikation c) auf x,y falsch rechnet
- $E_{\Pi}[Z(x,y,P)] \leq 1/3$ für alle x,y
- Wenn wir P_1, \dots, P_t zufällig gemäß Π ziehen, gilt
 - $E_{P_1, \dots, P_t} E_{i=1, \dots, t} [Z(x,y,P_i)] \leq 1/3$
- Wir sind nun interessiert an der Wahrscheinlichkeit (über die Wahl der P_i) einer großen Abweichung von diesem Erwartungswert

Chernoff Schranke

- Gegeben seien t unabhängige Indikatorzufallsvariablen Z_i mit Erwartungswert $\varepsilon \leq 1/2$
- $\text{Prob}(|\sum Z_i - \varepsilon t| \geq \delta t) \leq 2e^{-2\delta^2 t}$
für alle $0 < \delta \leq \varepsilon(1-\varepsilon)$
- D.h. die Wahrscheinlichkeit einer Abweichung sinkt exponentiell

Beweis 17.1

- $E_{P_1, \dots, P_t} E_{i=1, \dots, t} [Z(x, y, P_i)] \leq 1/3$
- $\text{Prob}_{P_1, \dots, P_t} (E_i Z(x, y, P_i) \geq 1/3 + 1/10) \leq 2e^{-2t/100} < 2^{-2n}/2$ für alle x, y
- Damit gilt:
 $\text{Prob}(\text{es gibt } x, y \text{ mit } E_i Z(x, y, P_i) \geq 0,44) \leq 2^{2n} 2^{-2n}/2 = 1/2$
- Folglich existieren P_1, \dots, P_t so dass für alle x, y der Fehler kleiner als 0,44 ist
- Durch Boosting kann der Fehler verringert werden
- Dies erhöht die Kommunikation um einen konstanten Faktor (und ebenfalls die Anzahl der Zufallsbits).
- Wir können stattdessen auch zuerst den Fehler auf 1/4 verringern (Kommunikation steigt auf $O(c)$), und dann den Fall $\delta = 1/3 - 1/4$ betrachten. Dabei ist $t = 125n$ ausreichend. Damit ist die Anzahl der Zufallsbits $\log(125t) = \log n + O(1)$

Untere Schranken

- Wir sind daran interessiert, untere Schranken für $R^1(f)$ zu zeigen
- Aus technischen Gründen werden wir meistens $R^{1,\text{pub}}(f)$ betrachten
- Der maximale Unterschied ist $O(\log n)$
- Wir in 17.1 bereits gesehen sind public coin Protokolle durch Verteilungen auf deterministischen Protokollen gegeben

Protokolle mit Fehler

- Wir betrachten deterministische Protokolle mit Fehler
- Dies macht nur Sinn, wenn der Fehler im Durchschnitt beschränkt ist
- Sei μ eine Verteilung auf den Eingaben, d.h. auf $\{0,1\}^n \times \{0,1\}^m$
- Ein deterministisches Einwegprotokoll P hat Fehler ε auf μ , wenn $E_{x,y \text{ gemäß } \mu} (P(x,y) \neq f(x,y)) \leq \varepsilon$
- **Definition 17.3**
 - Die deterministische Einwegkomplexität mit Fehler unter μ ist $D_{\varepsilon}^{1,\mu}(f)$, die Komplexität eines optimalen Protokolls das bzgl. μ Fehler ε hat

Protokolle mit Fehler

- Ein Beispiel:
- Equality unter uniformer Verteilung
 - kann mit Fehler $1/2^n$ ohne Kommunikation entschieden werden, indem Bob immer verwirft
- Equality unter der Verteilung:
 - x uniform. $y=x$ mit Ws. $1/2$, y Hamming Distanz 1 von x mit Ws. $1/2$
 - braucht konstante Kommunikation
- Disjunktheit: Alice erhält eine Teilmenge von $\{1, \dots, n\}$, ebenso Bob. Sind die Mengen disjunkt?
- Verteilung: Die Mengen haben Größe $n^{1/2}$
 - braucht Kommunikation $\Omega(n^{1/2})$ bei konstantem Fehler

Protokolle mit Fehler

- **Theorem 17.4 [Yao-Prinzip]**
 - $R^{1,\text{pub}}_\varepsilon(f) = \max_\mu D^{1,\mu}_\varepsilon(f)$, wobei μ über alle Verteilungen auf den Eingaben läuft
- In Worten: die randomisierte Komplexität mit (worst case) Fehler ε ist gleich der deterministischen Komplexität mit average case Fehler ε für die schwierigste Verteilung

Beweis 17.4

- $R^{\text{pub}}_{\varepsilon}(f) \geq \max_{\mu} D^{1,\mu}_{\varepsilon}(f)$:
 - Gegeben μ und ein randomisiertes Protokoll mit Kommunikation c und Fehler ε
 - r sei der public coin
 - Für alle x,y : E_r [Fehler auf x,y bei coin r] $\leq \varepsilon$
 - Daher: $E_{x,y \text{ gemäß } \mu} E_r$ [Fehler auf x,y bei coin r] $\leq \varepsilon$
 - $E_r E_{x,y \text{ gemäß } \mu}$ [Fehler auf x,y bei coin r] $\leq \varepsilon$
 - Es gibt r mit $E_{x,y \text{ gemäß } \mu}$ [Fehler auf x,y bei coin r] $\leq \varepsilon$
 - Fixiere r um ein deterministisches Protokoll zu erhalten

Beweis 17.4

- $R^{1,\text{pub}}_\varepsilon(f) \leq \max_\mu D^{1,\mu}_\varepsilon(f)$:
 - Wir betrachten ein zwei Personen Spiel:
 - Spieler 1 wählt Eingaben x,y
 - Spieler 2 wählt ein Protokoll
 - Spieler 1 gewinnt wenn das Protokoll sich irrt, d.h. nicht $f(x,y)$ ausgibt
 - Wir wissen: Es gibt eine randomisierte Strategie von Spieler 2, so dass für alle Wahlen von x,y Spieler 1 erwartet nur ε gewinnt
 - Das Minimax Prinzip der Spieltheorie besagt über solche Spiele (Nullsummen 2 Spieler Spiele):
 - Das Minimum über allen Strategien von 2 des Maximums über alle Strategien von 1 des erwarteten Gewinns von 1 ist gleich dem Maximum über alle Strategien von 1 des Minimum über alle Strategien von 2 des erwarteten Gewinns von 1
 - Dabei sind Strategien randomisiert

Beweis 17.4

- Für uns bedeutet dies:
 - Min aller Strategien von 2 Max aller Strategien von 1:
Spieler 2 wählt ein randomisiertes Protokoll
Spieler 1 wählt die Eingabe mit größtem erwartetem Fehler bezüglich des Protokolls
 - Max aller Strategien von 1 Min aller Strategien von 2:
Spieler 1 wählt eine Verteilung auf Eingaben
Spieler zwei wählt das beste passende Protokoll
Das Protokoll kann dabei deterministisch sein!
- D.h. unsere Aussage folgt aus dem Minimax Prinzip