

Seminar Kommunikationskomplexität

Nichtdeterministische Kommunikationsprotokolle I

D. Sieling, RWTH-Aachen

Detlef.Sieling@udo.edu

4. August 2003, Alexander Lay

alex@nwadmin.de

Quelle:

Kushilevitz, E., Nisan, N. (1997). Communication Complexity. Cambridge University Press;
Kapitel 2 bis Seite 21

1. Covers and Nondeterminism

-> Motivation und Einführung von Nichtdeterminismus

2. Communication Complexity Versus Cover Protocol

-> Komplexitätsschranken bei Protokollen mit entarteten Bäumen

3. Determinism Versus Nondeterminism

-> Vergleich von det. und nichtdet. Kommunikationskomplexität

4. Zusammenfassung

1. Motivation und Einführung von Nichtdeterminismus

- Alle Protokolle erzeugen eine Partition von f -monochromatischen Rechtecken auf $X \times Y$

	y	y'	y''
x	1	0	0
x'	1	1	1
x''	0	0	1

- Nicht alle Partitionen stellen Protokolle dar, obere Partition stellt kein Protokoll dar

- Da f nicht konstant ist tauschen A und B Nachrichten aus:
 1. Fall: A sendet die erste, nicht konstante Nachricht im Protokoll:
 - Die Nachrichten auf den Eingaben x , x' und x'' sind nicht alle gleich:
 - i. Falls $x \neq x'$
 $\Rightarrow \{x, x'\} \times \{y\}$ ist kein durch ein Protokoll erzeugtes Rechteck
 - ii. Falls $x' \neq x''$
 $\Rightarrow \{x', x''\} \times \{y''\}$ ist kein durch ein Protokoll erzeugtes Rechteck
 2. Fall: B sendet die erste, nicht konstante Nachricht im Protokoll:
 Analog zu 1. mit $\{x\} \times \{y', y''\}$ und $\{x''\} \times \{y, y'\}$ \Rightarrow *Widerspruch*

\Rightarrow Neben der Bildung von Partitionen aus monochromatischen Rechtecken existieren weitere Beschränkungen, diese wurden bisher nicht berücksichtigt

\Rightarrow Betrachtung von Überdeckungen statt Partionen

	y	y'	y''
x	1	0	0
x'	1	1	1
x''	0	0	1

- Überdeckungen

- bestehen aus Rechtecken, die sich überlappen können
- Überdeckungen benötigen z.T. weniger Rechtecke als Partitionen
 - (x', y') gehört zu zwei Rechtecken, die Überdeckung enthält 4 Rechtecke, eine Partition würde mindestens 5 Rechtecke enthalten

	y	y'	y''
x	1	1	0
x'	1	1	1
x''	0	1	1

- „fooling set“-Methode gibt die selbe untere Schranke an, wenn die Rechtecke eine Überdeckung statt eine Partition bilden.
Nach Definition werden nur Eingabewerte und Ergebnis betrachtet.
⇒ Wie „gut“ sind Partitionen im Vergleich zu Überdeckungen?

Definition 2.1: Sei $f: X \times Y \rightarrow [0,1]$ eine Funktion:

1. Die „protocol partition number of f “ $C^P(f)$:
min. Anzahl von Blättern in einem Protokollbaum von f
2. Die „partition number of f “ $C^D(f)$:
min. Anzahl von monochromatischen Rechtecken in einer Partition von $X \times Y$
3. Die „cover number of f “ $C(f)$:
min. benötigte Anzahl von monochromatischen Rechtecken, um eine Überdeckung auf $X \times Y$ zu bilden
4. $C^z(f)$:
Anzahl der benötigten monochromatischen Rechtecken, um eine Überdeckung der z -inputs von f zu bilden, $z \in \{0,1\}$, $f(x,y) = z$

Proposition 2.2: $\forall f: X \times Y \rightarrow [0,1]$:

1. $C(f) \leq C^D(f) \leq C^P(f) \leq 2^{D(f)}$

2. $C(f) = C^0(f) + C^1(f)$

• $C(f) \leq C^D(f)$:

Anzahl der Rechtecke in einer Überdeckung \leq Anzahl der Rechtecke in einer disjunkten Überdeckung (einer Partition),

da bei einer Partition keine Überlappungen möglich sind

• $C^D(f) \leq C^P(f)$:

Anzahl der Rechtecke einer Partition = min. Anzahl der Bätter des Protokollbaums,

aus Kapitel 1 bekannt

• $C^P(f) \leq 2^{D(f)}$:

Aus Kapitel 1: $\log_2 t \leq D(f)$ mit $t = C^P(f)$

Definition 2.3: Die nichtdeterministische Kommunikationskomplexität einer booleschen Funktion $f: X \times Y \rightarrow \{0,1\}$ ist $N^1(f) = \log_2 C^1(f)$.

Die co-nichtdeterministische Kommunikationskomplexität von f ist $N^0(f) = \log_2 C^0(f)$ und es gilt $N(f) = \log_2 C(f)$

- A und B berechnen die Matrix komplett für alle Eingaben für sich selbst, danach kann z.B. A raten, ob das Ergebnis in einem 1-Rechteck liegt und B mitteilen, welches 1-Rechteck dies ist.

\Rightarrow *Kommunikationskomplexität:* Anzahl der 1-Rechtecke

$$\Rightarrow N^1(f) = \log_2 C^1(f)$$

- Da im Modell die Nummer eines 1-Rechtecks übertragen wird, wird die benötigte Komplexität zur Übermittlung der Nummer eines 0-Rechtecks als co-nichtdeterministische Kommunikationskomplexität bezeichnet.

\Rightarrow *Kommunikationskomplexität:* Anzahl der 0-Rechtecke

$$\Rightarrow N^0(f) = \log_2 C^0(f)$$

Alternatives Modell für nichtdeterministische Kommunikation mit

$$\underline{N^z(f) = \log_2 C^z(f):}$$

Prover P kennt x und y versucht A und B zu überzeugen, dass $f(x,y) = z$.

- Falls $f(x,y) \neq z$ müssen A und B erkennen, dass P etwas falsches angibt.
- Falls $f(x,y) = z$ muss P A und B überzeugen, dass dies richtig ist.

Beispiel: $f(x,y) = EQ(x,y)$, $|x| = |y| = n$

- Falls $f(x,y) = 0$ reicht es, wenn P einen Index i angibt mit $x_i \neq y_i$

Kommunikationskomplexität: **$\log_2 n$**

- Falls $f(x,y) = 1$ ist dies nicht so einfach zu beweisen.

Behauptung:

Im effizientesten Beweissystem beträgt die benötigte Kommunikationskomplexität $N^z(f) = \log_2 C^z(f)$

Beweis:

1. $N^z(f) \leq \log_2 C^z(f)$:

Alle Überdeckungen von z-inputs bilden ein Beweissystem.

Ein Beweis ist der Name eines Rechtecks $S \times T$ indem (x,y) liegt.

A prüft ob $x \in S$ und teilt das Ergebnis B mit, B prüft ob $y \in T$.

Außerdem muss P A und B mitteilen, ob $f(x,y) = 0$ oder 1 [$O(1)$ Bits].

\Rightarrow Es werden maximal $\log_2 C^z(f) + O(1)$ Bits benötigt.

$\Rightarrow N^z(f) \leq \log_2 C^z(f) + O(1)$

2. $N^z(f) \geq \log_2 C^z(f)$

Angenommen es existiert ein Beweissystem, welches höchstens b Bits benötigt ($N^z(f) = b$):

- Sei c die Kommunikation die A und B von $f(x,y) = z$ überzeugt.
- Alle Eingaben (x,y) mit denen A und B von $f(x,y) = z$ überzeugt werden bilden ein z -Rechteck.
- Es existieren maximal 2^b dieser Rechtecke, da es nicht mehr verschiedene Kommunikation geben kann.

Bei max. b Bits Kommunikation beträgt die Höhe des Protokollbaums b , im Baum existieren also max. 2^b Blätter
 \Rightarrow es existiert eine Überdeckung mit max. 2^b Rechtecken

$$\Rightarrow C^z(f) \leq 2^b \text{ mit } b = N^z(f) \Rightarrow \log_2 C^z(f) \leq N^z(f)$$

$$\Rightarrow \log_2 C^z(f) \leq N^z(f) \leq \log_2 C^z(f) + O(1) \Rightarrow [\text{ohne } O(1)] N^z(f) = \log_2 C^z(f)$$

Wird die Kommunikationskomplexität der Beweise
unabhängig davon betrachtet,
ob $f(x,y) = 0$ oder $f(x,y) = 1$ bewiesen wird, so folgt:

$$\mathbf{N(f)} = \mathbf{\log_2 C(f)}$$

Die folgende untere Schranke aus Kapitel 1 bleibt bei nichtdeterministischer Kommunikation erhalten:

Lemma 2.4: Für $f: X \times Y \rightarrow [0,1]$:

Sei μ eine Wahrscheinlichkeitsverteilung

der z -inputs von f für $z \in \{0,1\}$, $f(x,y) = z$:

wenn \forall z -monochromatischen Rechtecke $\mu(R) \leq \delta \Rightarrow C^z(f) \geq 1/\delta$.

Beweis:

- $\mu(\{R \mid R \text{ ist } z\text{-monochromatisches Rechteck mit } z \in \{0,1\}\}) = 1$

Wahrscheinlichkeit in einem der 0 oder 1-Rechtecke zu sein ist 1.

- Die Wahrscheinlichkeit für jedes Rechteck ist $\leq \delta$

\Rightarrow Anzahl der z -monochromatischen Rechtecke

$$C^z(f) = 1/\delta, \text{ da } 1/\delta \times \delta = 1$$

- „fooling set“-Methode gibt eine untere Schranke der Rechtecke einer Partition an.

Da max. ein Element pro Rechteck im fooling set enthalten ist, ist dies auch eine untere Schranke der Überdeckungen. Es gilt schließlich $C(f) \leq C^D(f)$.

⇒ Methode liefert auch bei nichtdeterministischer Kommunikation eine Schranke

- Die Rangmethode läßt sich nicht direkt wie in Kapitel 1 beschrieben übertragen.

Bei $f(x,y) = \text{NEQ}(x,y)$ befinden sich in der Kommunikationsmatrix M auf der Diagonalen nur Nullen und sonst Einsen

⇒ $\text{Rang}(M) = 2^n$, $|x| = |y| = n$

⇒ *Widerspruch*, zur Angabe eines Index i mit $x_i \neq y_i$ werden nur **$\log_2 n$** Bits Kommunikation benötigt.

(Durch die Definition des Rang über dem Ring $(\{0,1\}, \text{AND}, \text{OR})$ lässt sich die Methode übertragen.)

Beispiel 2.5:

Ein Beispiel aus Kapitel 1 zeigt, dass $D(\text{EQ}) = n+1$:

○ (α, β) , $\alpha = \beta$, deterministischer und nichtdeterministischer Fall:

$$S = \{(\alpha, \beta) \mid \alpha = \beta \text{ und } \alpha, \beta \in \{0, 1\}^n\}$$

S ist fooling set mit $|S| = 2^n$ (es gibt 2^n Möglichkeiten $\alpha = \beta$ zu wählen), alle 1-Rechtecke befinden sich auf der Diagonalen und haben die Größe 1

$$\Rightarrow \mathbf{D(\text{EQ})} \geq \log_2(2^n) = \mathbf{n}$$

d.h. mit $N^1(f) = \log_2 C^1(f)$ gilt

$$\mathbf{N^1(\text{EQ})} \geq \mathbf{n}.$$

- (α, β) , $\alpha \neq \beta$, deterministischer Fall:

Durch das Hinzunehmen min. eines 0-Rechtecks ergibt sich

$$D(EQ) \geq n+1 \text{ und mit } D(f) \leq n+1$$

$$\Rightarrow \mathbf{D(EQ) = n+1.}$$

- (α, β) , $\alpha \neq \beta$, nichtdeterministischer Fall:

Um $NEQ(\alpha, \beta) = 1$ (also $\alpha \neq \beta$) zu zeigen wird ein Index i mit $\alpha_i \neq \beta_i$ angegeben, dazu werden $\log_2 n$ Bits benötigt, da $\alpha, \beta \in \{0, 1\}^n$ und $i = 0, \dots, n-1$.

1 bit wird benötigt um anzugeben, ob $\alpha_i = 0$ und $\beta_i = 1$ oder umgekehrt.

$$\Rightarrow \mathbf{N^1(NEQ) \leq \log_2(n+1) \Rightarrow 2^{N^1(NEQ)} \leq n+1 = D(EQ) = D(NEQ)}$$

\Rightarrow exponentieller Unterschied zwischen Determinismus und Nichtdeterminismus

2. Komplexitätsschranken bei Protokollen mit entarteten Bäumen

- Bei einigen Protokollen kann der Protokollbaum sehr tief sein und wenige Blätter ($C^P(f)$ ist klein) haben.

⇒ Die Kommunikationspartner müssen viele Bits austauschen.

⇒ $D(f)$ ist groß

Es ist daher interessant, Schranken aufgrund der Anzahl der Blätter des Protokollbaums zu kennen.

Lemma 2.8: $D(f) = \theta(\log_2 C^P(f))$, genauer: $\log_2 C^P(f) \leq D(f) \leq 2 \log_{3/2} C^P(f)$

Beweisidee:

1. „Rebalancieren“ des Protokollbaums in einem Preprocessingschritt durch Entfernung eines Unterbaums mit zu vielen Blättern.
Dieser wird separat betrachtet.
2. Prüfung durch A und B in einem neuen Protokoll, ob der entfernte Unterbaum im Protokoll mit den Eingaben x und y erreicht wird oder nicht.
Davon hängt ab, ob der entfernte Unterbaum oder der bisherige Baum ohne den entfernten Unterbaum weiter betrachtet wird.
3. Rekursives wiederholen der Schritte auf aktuellem Baum, so lange dies möglich ist. So wird immer besser balanciert, der Baum ist immer weniger entartet.

Beweis:

1. $\log_2 C^P(f) \leq D(f)$ folgt direkt aus $C^P(f) \leq 2^{D(f)}$

2. $D(f) \leq 2 \log_{3/2} C^P(f)$: A, B sind die Kommunikationspartner

a. Es existiert ein Protokollbaum für f mit t Blättern.

t_v := Anzahl der Blätter im Unterbaum von v

R_v := Rechtecke der Inputs, die v erreichen

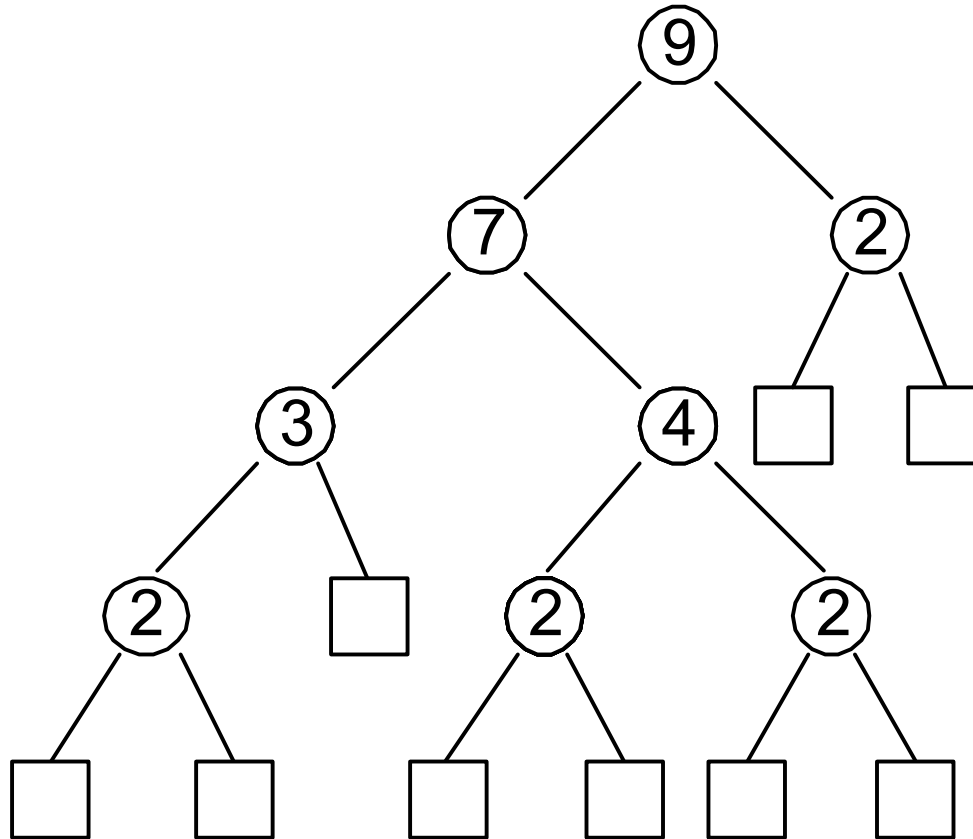
Suche Knoten v mit $t/3 < t_v \leq 2 t/3$ folgendermaßen:

i. Starte an der Wurzel w

ii. Gehe zum Kind u mit $t_u > 2 t/3$,
existiert ein solches nicht, weiter bei iii.,
sonst wiederhole ii.

iii. Prüfe Kinder r und s von u auf $t/3 < t_{r/s} \leq 2 t/3$
falls r erfüllt, $v := r$,
falls s erfüllt, $v := s$

Beispiel mit $t = 9 \Rightarrow 3 < t_v \leq 6$



- i. Wurzel mit $t = 9$
- ii. Knoten u mit $t_u = 7$, Kind mit $3 < t_u \leq 6$ existiert nicht
- iii. Knoten v mit $t_v = 4$ wird ausgewählt

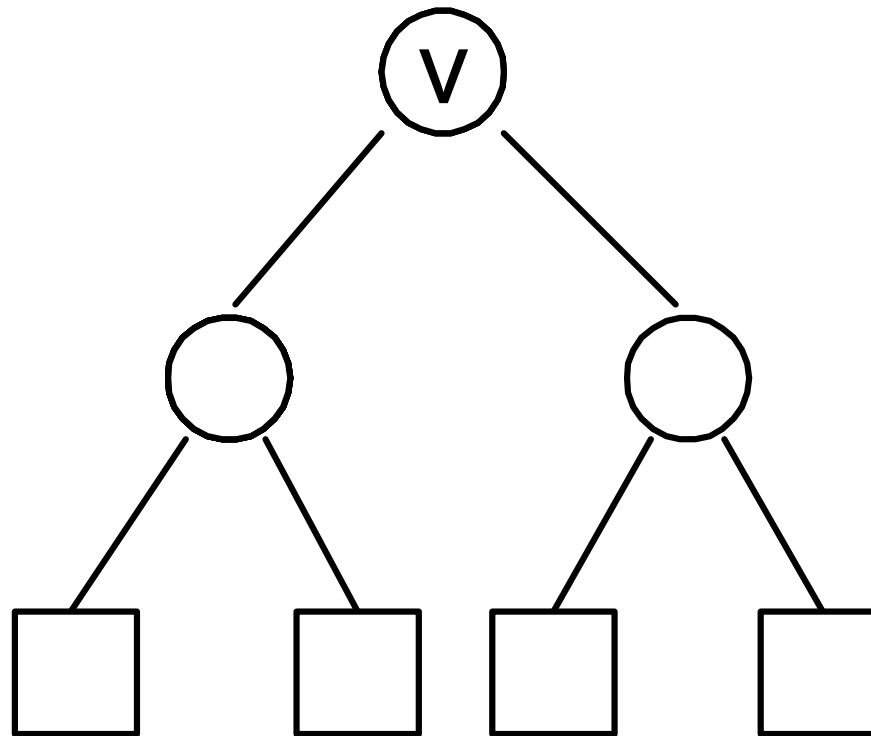
b. Prüfung, ob $(x,y) \in R_v$ durch A und B

\Rightarrow benötigt 2 Bits Kommunikation (A teilt B mit, ob mit x eine Zeile, in der das Rechteck R_v liegt, erreicht wird und umgekehrt)

I. Falls $(x,y) \in R_v$:

A und B berechnen f im Unterbaum von v (im Rechteck R_v)

\Rightarrow Protokollbaum hat t_v **Blätter**



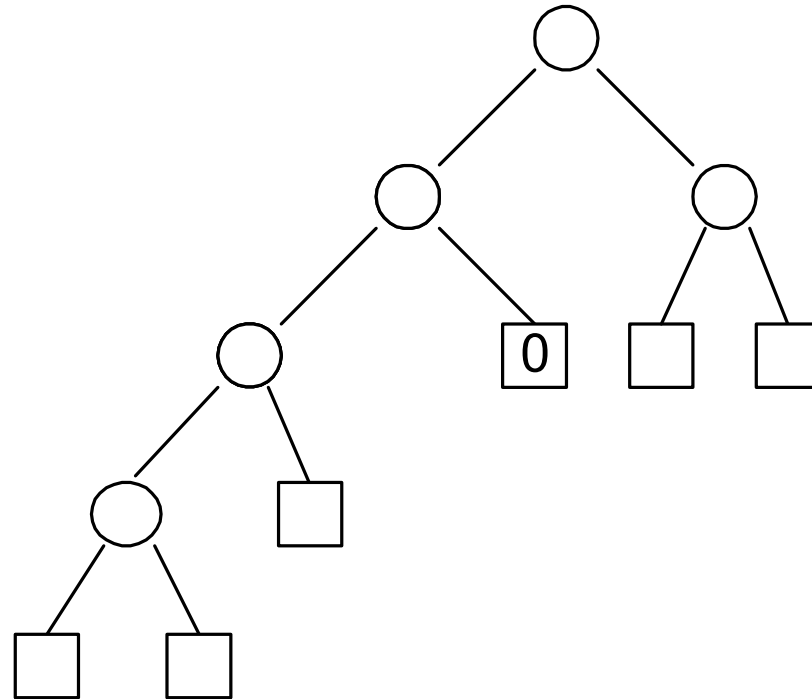
$(x,y) \in R_v, t_v = 4$ Blätter

II. Falls $(x,y) \notin R_v$:

A und B berechnen f' auf $X \times Y$,

$f' = f$ mit: Unterbaum t_v durch 0-Blatt ersetzt

\Rightarrow Protokollbaum hat $t-t_v+1$ **Blätter**



$(x,y) \notin R_v, t-t_v+1 = 9-4+1 = 6$ Blätter

Korrekt, da R_v nie erreicht wird

Fall I: Protokollbaum hat t_v **Blätter** mit $t/3 < t_v \leq 2 t/3$

\Rightarrow maximal $2 t/3$ Blätter

Fall II: Protokollbaum hat $t-t_v+1$ **Blätter** mit $t/3 < t_v \leq 2 t/3$

\Rightarrow maximal $t - (t/3 + 1) + 1 = 2 t/3$ Blätter

\Rightarrow In beiden Fällen (I. & II.) existiert ein Protokollbaum mit max. $2 t/3$ Blättern.

Dieses Verfahren wird so oft wiederholt, wie es möglich ist.

$\Rightarrow D(t) \leq 2 + D(2 t/3)$, mit $D(1) = 0$
durch rekursives Auflösen folgt

$D(t) \leq 2 \log_{3/2} t$ mit $t = C^P(f)$

$\Rightarrow \mathbf{D(f) \leq 2 \log_{3/2} C^P(f)}$

Die Kommunikationskomplexität unterscheidet sich max. exponentiell von der minimalen Anzahl der Blätter des Protokollbaums.

3. Vergleich von det. und nichtdet. Kommunikationskomplexität

- Folgendes ist bekannt:
 - $D(f) = \theta(\log C^P(f))$
 - $D(f)$ kann exponentiell größer sein als $C^1(f)$
 - $D(f) \geq \log_2 C^D(f)$ – es ist nicht bekannt wie scharf die Schranke ist
- Unterschied zwischen $D(f)$ und
 - $C^D(f)$
 - $C(f)$fehlen noch.

Open Problem 2.10: $D(f) = O(\log C^D(f))$?

Theorem 2.11: \forall Funktionen $f: X \times Y \rightarrow [0,1]$:

$$D(f) = O(N^0(f)N^1(f)) \quad [N(f) = \log C(f)]$$

\Rightarrow Unterschied zwischen $D(f)$ und $N(f)$ existiert, ist aber quadratisch.

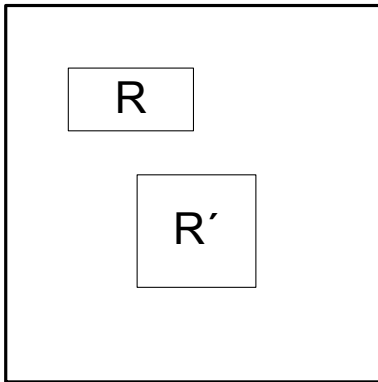
- Theorem impliziert: Unterschied zwischen $D(f)$ und $O(\log C^D(f))$ nicht sehr groß, da Unterschied zwischen $D(f)$ und $\log C(f)$ nicht groß und $\log C(f) \leq \log C^D(f) \leq D(f)$

Beweis (algorithmisch):

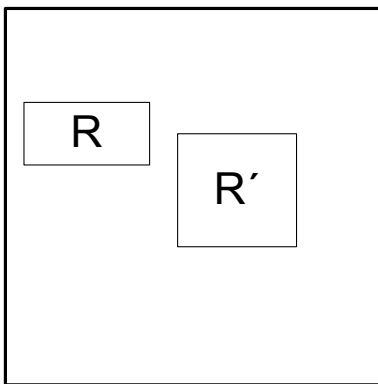
Sei $R = S \times T$ 0-monochromatisches Rechteck und

sei $R' = S' \times T'$ 1-monochromatisches Rechteck

\Rightarrow R und R' liegen nicht in einer Zeile ($S \cap S' = \emptyset$)



oder R und R' liegen nicht in einer Spalte ($T \cap T' = \emptyset$)



Angenommen es ex. (x,y) mit $x \in S \cap S'$ und $y \in T \cap T'$, dann gilt

$(x,y) \in R$, also $f(x,y) = 0$ und

$(x,y) \in R'$, also $f(x,y) = 1$

\Rightarrow *Widerspruch*

Beweisidee:

Protokoll für A und B:

A und B suchen ein 0-Rechteck aus einer Überdeckung,
dass (x,y) enthält, wird keins gefunden $\Rightarrow f(x,y) = 1$

- In jedem Schritt
 - werden $\log C^1(f) + O(1)$ Bits benötigt
 - reduziert sich die Anzahl der 0-Rechtecke durch Streichung min. um den Faktor 2,
Anfangs ist kein 0-Rechteck gestrichen
 - Es werden maximal $\log C^0(f)$ Schritte benötigt
- $\Rightarrow D(f) = O(\log C^0(f) \log C^1(f)) = O(N^0(f)N^1(f))$

Das Protokoll funktioniert folgendermaßen:

1. A betrachtet die nicht-gestrichenen 0-Rechtecke, existieren keine solchen \Rightarrow Ausgabe $f(x,y) = 1$, sonst sucht A nach einem 1-Rechteck Q,
 - durch das die Zeile x läuft und
 - das mit höchstens der Hälfte, der nicht-gestrichenen 0-Rechtecke in einer gleichen Zeile liegt

Findet A ein solches Q

- werden alle 0-Rechtecke, die nicht in einer Zeile mit Q liegen gestrichen
- wird (der Name von) Q an B gesendet,

sonst wird B mitgeteilt, das kein Q existiert (1 Bit)

$\Rightarrow \log C^1(f) + O(1)$ Bits

2. B betrachtet ein nicht-gestrichenes 1-Rechteck Q ,

○ durch das die Spalte y läuft und

○ das mit höchstens der Hälfte, der nicht-gestrichenen 0-Rechtecke in einer gleichen Spalte liegt

Findet B ein solches Q

○ werden alle 0-Rechtecke, die nicht in einer Spalte mit Q liegen gestrichen

○ wird (der Name von) Q an A gesendet,
sonst Ausgabe $f(x,y) = 0$

$\Rightarrow \log C^1(f) + O(1)$ Bits

- Jeder Schritt reduziert die Anzahl der 0-Rechtecke mindestens um den Faktor 2 mit $\log C^1(f) + O(1)$ Kommunikation

Beispiel (zur besseren Darstellung nur mit einer Überlappung):

1. A wählt 1-Rechteck Q und x läuft durch Q

		y				
	1	1	0	0	0	0
	1	1	0	0	1	0
	0	0	0	0	1	1
x	0	0	0	0	1	1
	0	0	1	1	0	1
	0	0	1	1	0	1

2. A streicht alle 0-Rechtecke, die nicht in einer Zeile mit Q liegen

		y				
	1	1	0	0		
	1	1	0	0	1	
	0	0	0	0	1	1
x	0	0	0	0	1	1
	0	0	1	1		1
	0	0	1	1		1

3.B wählt 1-Rechteck Q,

		y			
	1	1	0	0	
	1	1	0	0	1
x	0	0	0	0	1
	0	0	0	0	1
	0	0	1	1	
	0	0	1	1	
					1
					1

- durch das die Spalte y läuft und
- das mit höchstens der Hälfte, der nicht-gestrichenen 0-Rechtecke in einer gleichen Spalte liegt

4.B streicht alle 0-Rechtecke, die nicht in einer Spalte mit Q liegen

		y			
	1	1	0	0	
	1	1	0	0	1
x			0	0	1
			0	0	1
			1	1	
			1	1	
					1
					1

5.A findet kein 1-Rechteck Q ,

- durch das die Zeile x läuft und
- das mit höchstens der Hälfte, der nicht-gestrichenen 0-Rechtecke in einer gleichen Zeile liegt

Es existiert nur noch ein 0-Rechteck \Rightarrow kann nicht erfüllt werden

		y					
		1	1	0	0		
		1	1	0	0	1	
x				0	0	1	1
				0	0	1	1
				1	1		1
				1	1		1

6.A teilt B dies mit.

7.B findet kein 1-Rechteck Q , das

- durch das die Spalte y läuft und
- das mit höchstens der Hälfte, der nicht-gestrichenen 0-Rechtecke in einer gleichen Spalte liegt

Es existiert nur noch ein 0-Rechteck \Rightarrow kann nicht erfüllt werden

B gibt $f(x,y) = 0$ aus

		y			
		1	1	0	0
		1	1	0	0
x				1	1
				1	1
			1	1	
			1	1	

4. Zusammenfassung

1. Motivation und Einführung von Nichtdeterminismus

- Überdeckungen
- Definition der Grundlagen von Nichtdeterminismus
- Modelle für nichtdeterministische Kommunikation

2. Komplexitätsschranken bei Protokollen mit entarteten Bäumen

- Schranken der Kommunikation,
die auch bei entarteten Protokollbäumen gelten:
 $D(f) = \theta(\log_2 C^P(f))$

3. Vergleich von det. und nichtdet. Kommunikationskomplexität

- Obere Schranke der Kommunikation anhand der minimalen Anzahl der Rechtecke einer Partition:
 $D(f) = O(\log C^D(f))$ – offenes Problem
- Unterschied zwischen $D(f)$ und $N(f)$ existiert, ist aber quadratisch
 $D(f) = O(N^0(f)N^1(f))$

Bemerkungen:

- Folie 7 werde ich vor dem Vortrag an die Tafel schreiben.
- Folie 22 werde ich an die Tafel zeichnen und dabei Folie 21 aufgelegt lassen.