Komplexitätstheorie

Kapitel 6: Schaltkreise

Motivation

Wir betrachten Schaltkreise als alternatives Berechnungsmodell

Damit lassen sich weitere Komplexitätsklassen definieren

Dies ist von Bedeutung, denn es

- schafft mehr Struktur innerhalb von P und erfasst wichtige, natürliche Probleme
- liefert Modell für massiv parallele Berechnungen (mehrere Millionen Prozessoren)
- führt auf natürliche Weise nicht-Uniformität als wichtigen theoretischen Aspekt ein

Schaltkreise

Definition (Boolescher) Schaltkreis

Boolescher Schaltkreis C ist Tupel $(V, E, \omega, x_1, \ldots, x_n, o)$ wobei

- (V, E) gerichteter azyklischer Graph,
- $x_1, \ldots, x_n \in V$ *Eingabeknoten* mit Eingangsgrad 0
- $o \in V$ *Ausgabeknoten* mit Ausgangsgrad 0
- $\omega : V \setminus \{x_1, \ldots, x_n\} \to \{\neg, \wedge, \vee, 0, 1\}$ Knotenbeschriftung so dass
  - $\omega(v) = \neg$ impliziert Eingangsgrad$(v) = 1$
  - $\omega(v) \in \{\wedge, \vee\}$ impliziert Eingangsgrad$(v) = 2$
  - $\omega(v) \in \{0, 1\}$ impliziert Eingangsgrad$(v) = 0$

Bei *Eingabe* $w \in \{0, 1\}^n$ ist der *Wert* jedes Knoten (induktiv) in der offensichtlichen Weise definiert. Die *Ausgabe* $C(w)$ von C ist der Wert des Ausgabeknoten

Schaltkreise

Schaltkreis-Terminologie:

- die Nicht-Eingabeknoten eines Schaltkreises werden *Gates* genannt
- der Eingangsgrad von Gates wird *Fan-In* genannt

Größe $|C|$ von Schaltkreis C ist die Anzahl seiner Gates

Definition Boolesche Funktion

Sei $n \in \mathbb{N}$.

n*-äre Boolesche Funktion* ist Funktion $f : \{0,1\}^n \to \{0,1\}$.

Schaltkreis C mit n Eingabeknoten:
berechnet n-äre Boolesche Funktion f_C mit $f_C(w) = C(w)$ für alle $w \in \{0,1\}^n$

Schaltkreise und Boolesche Funktionen

Definition Schaltkreiskomplexität

Schaltkreiskomplexität einer Booleschen Funktion f ist $|C|$ für kleinsten Schaltkreis C mit $f_C = f$

Durch direktes Implementieren der Wertetabelle:

Jede n-äre Boolesche Funktion hat Schaltkreiskomplexität $2^{\mathcal{O}(n)}$

Es ist nicht immer möglich, polynomiell große Schaltkreise zu finden:

Theorem (Shannon 1949)

Für alle $n > 1$ gibt es Boolesche Funktion $f : \{0,1\}^n \to \{0,1\}$ mit Schaltkreiskomplexität $> \frac{2^n}{10n}$.

Interessanterweise kennt man keine "natürliche" Boolesche Funktion, die mehr als linear viele Gates benötigt!

Kapitel 6

Schaltkreise und Sprachen

Schaltkreise und Sprachen

Erkennen von Sprache:

- Wir beschränken uns o.B.d.A. auf Sprachen $L \subseteq \{0,1\}^*$
  (Sprachen über anderen Alphabeten können “umkodiert” werden)
- Jeder Schaltkreis erkennt nur Eingaben fester Länge, darum verwenden wir *Familie* von Schaltkreisen $(C_n)_{n\in\mathbb{N}} = (C_1, C_2, \dots)$
  (ein Schaltkreis für jede Eingabelänge)

Definition Schaltkreise und Sprachen

Familie $(C_n)_{n\in\mathbb{N}}$ von Schaltkreisen *definiert* L wenn jedes C_n die Einschränkung von L auf Wörter der Länge n definiert:

$$C_n(w) = 1 \text{ gdw. } w \in L \quad \text{für alle } w \in \{0,1\}^n$$

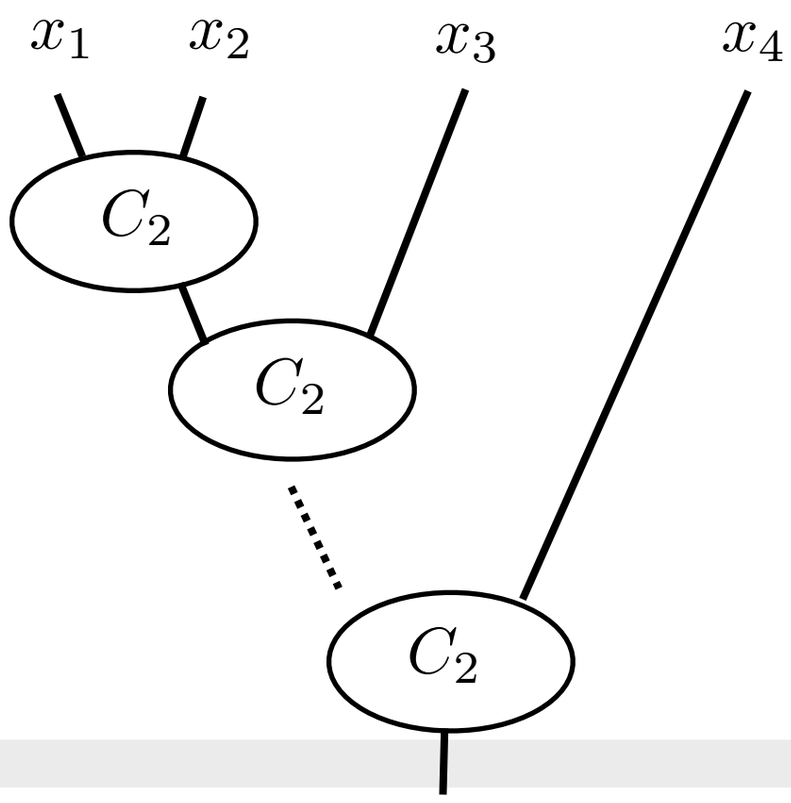
Schaltkreise und Sprachen

Paritäts-Beispiel leicht zu generalisieren zu Schaltkreisfamilie für

$$\text{PARITY} := \{w \in \{0,1\}^* \mid w \text{ hat Parität } 1\}$$

Im Detail:

- C_0: Konstantes 0-Gate liefert Ausgabe
- C_1: Ausgabe = (einziges) Eingabebit
- C_2: Schon gesehen
- $C > 2$: Zusammenschalten mehrerer Kopien von C_2:



Schaltkreise und Sprachen

Boolesche Funktion:

Ein einziger Schaltkreis, Schaltkreiskomplexität ist Zahl

Sprache:

Familie von Schaltkreisen, Schaltkreiskomplexität ist Funktion von Eingabelänge auf Schaltkreisgröße
(Analog zu Zeit- und Platzkomplexität von TMs)

Definition Schaltkreiskomplexität von Sprachen

Sei $s : \mathbb{N} \to \mathbb{N}$ monoton wachsende Funktion.

Schaltkreisfamilie $(C_n)_{n\in\mathbb{N}}$ ist *s-größenbeschränkt* wenn $|C_n| \leq s(n)$ für alle $n \in \mathbb{N}$.

Definiere Komplexitätsklasse

$\text{Size}(s) := \{L \subseteq \Sigma^* \mid \exists \mathcal{O}(s)$-größenbeschränkte Familie $(C_n)_{n\in\mathbb{N}}$ von Schaltkreisen, die L definiert $\}$

Kapitel 6

Polynomielle Schaltkreiskomplexität und Uniformität

Polynomielle Schaltkreiskomplexität

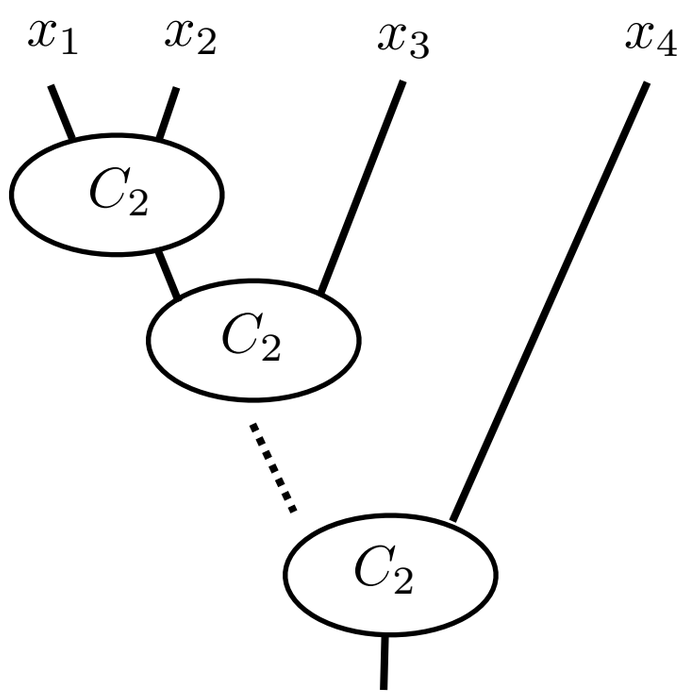
Jedes Gate eines Schaltkreises trägt “einen Schritt” zur Berechnung bei

In Analogie zu P ist es also natürlich, sich für polynomielle Schaltkreis-komplexität zu interessieren

Definition

$\mathsf{P}_{/\mathsf{poly}} = \bigcup_{i \geq 1} \mathsf{Size}(n^i)$

Schon gesehen: PARITY $\in \mathsf{P}_{/\mathsf{poly}}$



Polynomielle Schaltkreiskomplexität

Essentieller Unterschied zwischen P und $\mathsf{P}_{/\mathsf{poly}}$:

- Jeder Sprache in P liegt eine TM zugrunde, die für Eingaben jeder Länge verwendet wird (uniformes Berechnungsmodell)
- Schaltkreise aus Familie $(C_n)_{n\in\mathbb{N}}$ sind unabhängig, C_i kann ganz anders sein als C_{i+1} (nicht-uniformes Berechnungsmodell)

Insbesondere: Schaltkreisfamilie kein effektives Berechnungsmodell:

- bei Eingabe w mit $|w| = n$ müßte erstmal C_n berechnet werden
- unsere Definition garantiert diese Berechenbarkeit aber nicht.

Theorem

$\mathsf{P}_{/\mathsf{poly}}$ enthält unentscheidbare Probleme.

Also trivialerweise $\mathsf{P}_{/\mathsf{poly}} \neq \mathsf{P}$.

Uniformität

Definition Polyzeit-Uniformität

Familie $(C_n)_{n\in\mathbb{N}}$ ist *polyzeit-uniform*, wenn es polyzeit-beschränkte DTM gibt, die bei Eingabe 1^n den Schaltkreis C_n ausgibt.

Uniform $\mathsf{P}_{/\mathsf{poly}}$ ist definiert wie $\mathsf{P}_{/\mathsf{poly}}$, aber mit polyzeit-uniformen Familien

Intuitiv ist uniform $\mathsf{P}_{/\mathsf{poly}}$ sehr ähnlich zu P:

deterministische Modelle mit polynomiellen Ressourcen (Zeit und Platz)

In der Tat gilt:

Theorem

P = uniform $\mathsf{P}_{/\mathsf{poly}}$

Schaltkreise liefern uns also eine alternative Charakterisierung von P.

Uniform $\mathsf{P}_{/\mathsf{poly}}$

Uniform $\mathsf{P}_{/\mathsf{poly}} \subseteq \mathsf{P}$ ist offensichtlich: verwende Schaltkreisauswertung.

Definition CVP

Das *Schaltkreisauswertungsproblem (Circuit Value Problem, CVP)*:

$$\mathsf{CVP} := \{(C, w) \mid C \text{ } n\text{-ärer Schaltkreis}, w \in \{0,1\}^n, C(w) = 1\}$$

Leicht zu sehen: CVP ist in P (Azyklizität ausnutzen)

Theorem

Uniform $\mathsf{P}_{/\mathsf{poly}} \subseteq \mathsf{P}$.

Uniform $\mathsf{P}_{/\mathsf{poly}}$

Theorem

$\mathsf{P} \subseteq$ uniform $\mathsf{P}_{/\mathsf{poly}}$

Ideen:

- Sei $L \in \mathsf{P}$, M p-zeitbeschränkte DTM M mit $L(M) = L$
- Für jede Eingabelänge n, konstruiere in Polyzeit Schaltkreis C_n so dass: M akzeptiert $w = b_1 \cdots b_n \in \{0,1\}^n$ gdw. $C_n(w) = 1$
- Stelle Berechnung wieder als $(p(n)+2) \times (p(n)+1)$-Matrix dar:

$\triangleright$	q_0, b_1	b_2	$\cdots$	b_n	$\perp$	$\cdots$	$\perp$
$\triangleright$	a	q, b_2	$\cdots$	a_n	$\perp$	$\cdots$	$\perp$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$

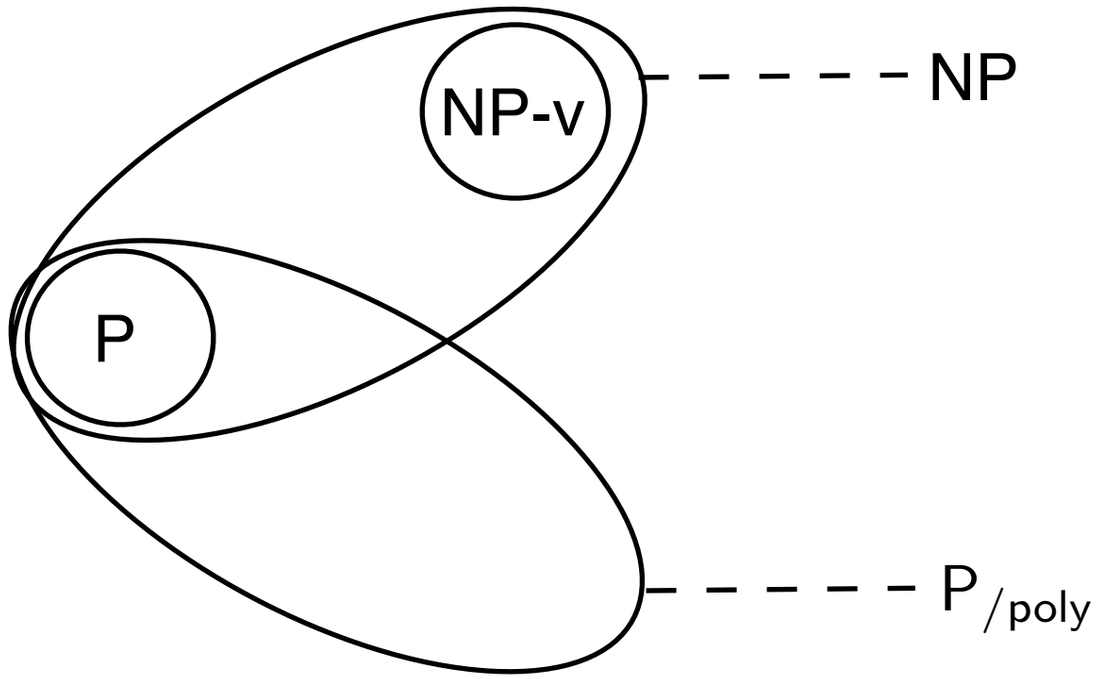
- Kodiere jeden möglichen Feldinhalt mittels $c = |\Gamma| + |Q|$ bits

Nicht-Uniformität

Wir haben gesehen:

(nicht-uniformes) $P_{/poly}$ enthält Probleme, die weder in P noch in NP sind

Interessanterweise ist unbekannt,
ob $NP \subseteq P_{/poly}$



Man vermutet, dass Uniformität ein irrelevanter Aspekt für P vs NP ist, nämlich dass $NP \subseteq P$ gdw. $NP \subseteq P_{/poly}$.

Es gibt konkrete technische Resultate, die dafür Indizien liefern

Kapitel 6

Die Klasse NC und massiv parallele Berechnungen

Massiv parallele Berechnungen

Massiv parallele Rechenmodelle:

- sehr viele (hunderttausende) sehr einfache Prozessoren
- Prozessoren arbeiten unabhängig, kommunizieren über direkte Links oder Bus

Schaltkreise

- erlauben Parallelität, denn Gates (= Prozessoren), die sich wechselseitig nicht erreichen können, arbeiten unabhängig
- taugen daher als abstraktes Modell für massiv parallele Berechnungen (massiv: die Anzahl der Gates/Prozessoren steigt mit Eingabelänge!)
- wenn man Rechenzeit jedes Prozessors mit 1 ansetzt, ist Rechenzeit des Schaltkreises C dessen Tiefe $d(C)$ (Länge des längsten Pfades)

Massiv parallele Berechnungen

Ziel von parallelen Berechnungen:

Rechenzeit signifikant verkürzen, inbesondere exponentieller Speedup von linearer Zeit auf logarithmische Zeit

Beachte:

- Eine TM kann in logarithmischer Zeit nicht mal die Eingabe lesen
- Ein Schaltkreis braucht die Eingabe gar nicht (sequentiell) zu lesen, bekommt sie parallel zur Verfügung gestellt

Man interessiert sich also für Schaltkreise mit logarithmischer Tiefe und polynomieller Größe (damit Anzahl Prozessoren nicht absurd wird)

NC

Definition LogSpace-Uniformität

Familie $(C_n)_{n\in\mathbb{N}}$ ist *LogSpace-uniform*, wenn es LogSpace-Transduktor gibt, der bei Eingabe 1^n den Schaltkreis C_n ausgibt.

Hier ist eine entsprechende Komplexitätsklasse

Definition NC

Problem L ist in NC^i, $i \geq 1$, wenn es LogSpace-uniforme Familie $(C_n)_{n\in\mathbb{N}}$ gibt, die L erkennt und so dass:

- es gibt $k \in \mathbb{N}$ mit $|C_n| \in \mathcal{O}(n^k)$
- $d(C_n) \in \mathcal{O}(\log(n)^i)$

Nun ist $\mathsf{NC} := \bigcup_{i\geq 0} \mathsf{NC}^i$

NC steht für Nick's Class, nach Nicolas Pippenger

NC

Lemma

PARITY $\in$ NC^1 $\subseteq$ NC

Beachte: NC^1 $\subseteq$ NC^2 $\subseteq \cdots$ NC ist unendliche Hierarchie in NC (und in P!)

Echtheit der Inklusionen unbekannt!

Die gesamte unendliche NC-Hierarchie ist trivialerweise unterhalb von P:

Theorem

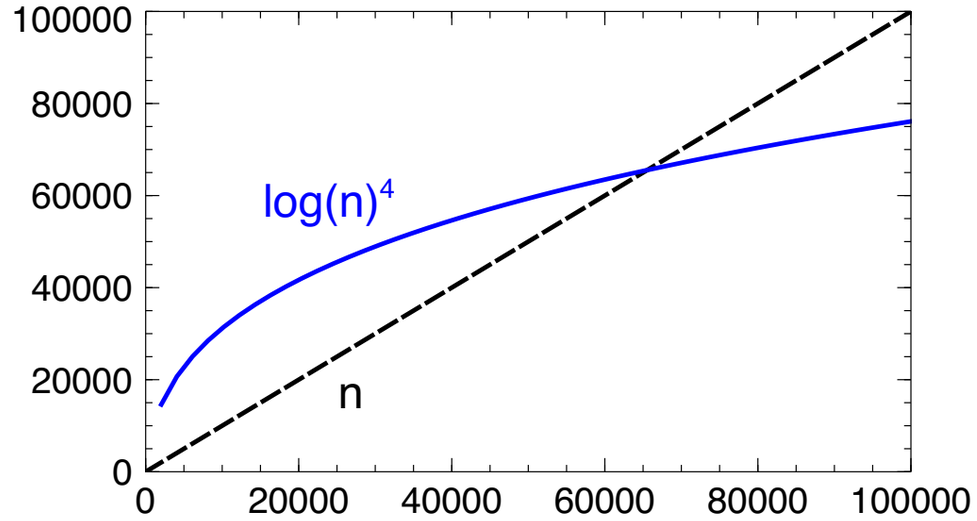
NC $\subseteq$ uniform P$_{/\text{poly}}$ = P

NC

$L \in$ NC with oft mit "L effizient parallelisierbar" gleichgesetzt.

Etwas Vorsicht ist aber geboten:

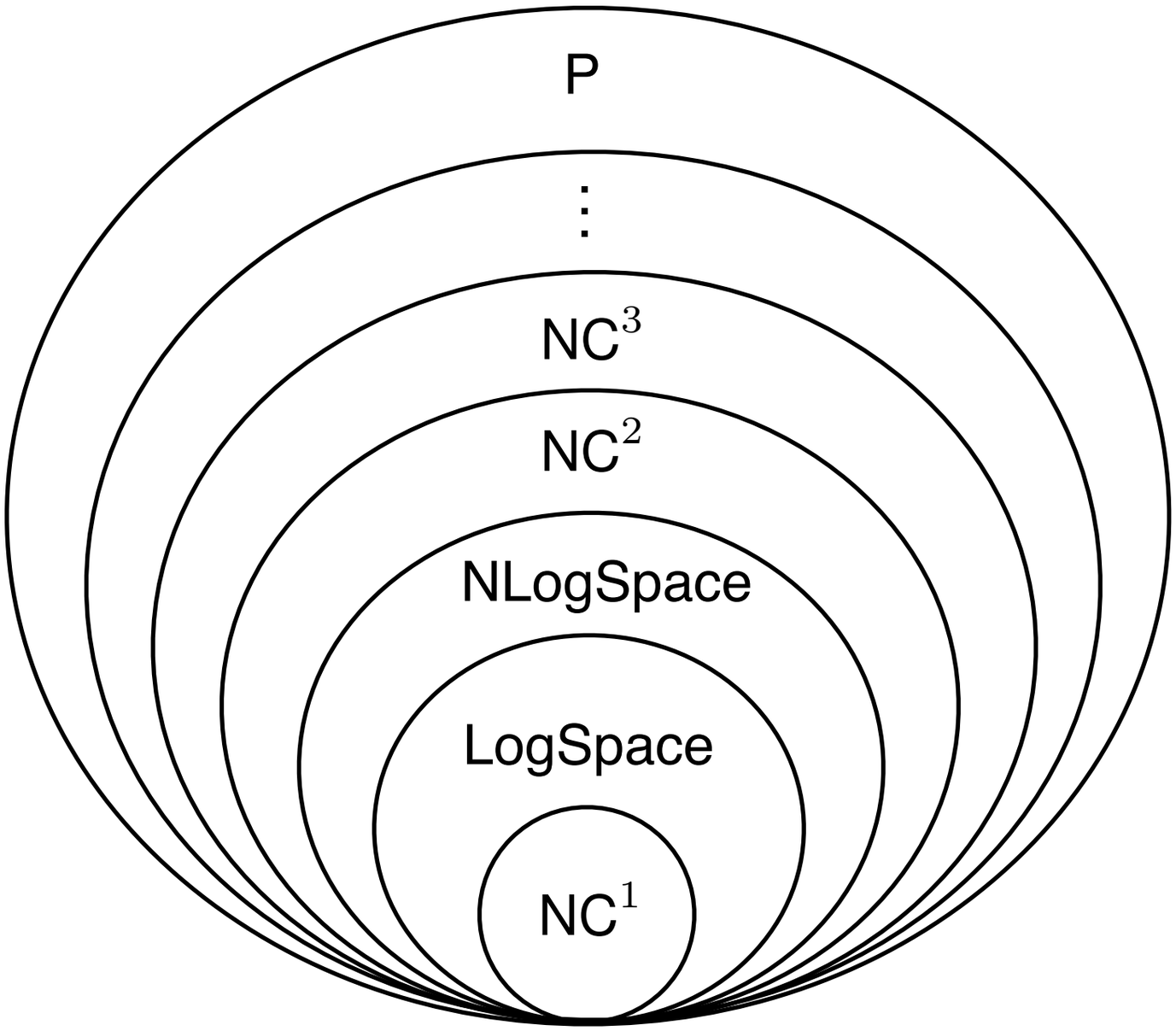
- Schon für recht kleine Werte von i (z.B. $i = 4$) wächst $\log(n)^i$ nur für sehr große Werte von n deutlich langsamer als n



- Für sehr große Eingaben ist aber die Annahme "Poly viele Prozessoren" unrealistisch
- Also wäre NC^1 oder NC^2 vielleicht realistischer (das ist aber sehr kleine Klasse)

NC

Wir setzen nun NC in Beziehung zu unseren bisherigen Klassen:



NC

Theorem

$\mathrm{NC}^1 \subseteq \mathrm{LogSpace}$

Vorbemerkung:

Wir repräsentieren Knoten in Schaltkreisen als binäre Zahlen;

o.B.d.A. ist Knoten 1 der Ausgabeknoten

Wenn M LogSpace-Transduktor ist, der Schaltkreisfamilie $(C_n)_{n\in\mathbb{N}}$ konstruiert, dann kann folgendes in LogSpace berechnet werden:

- gegeben (k, n) mit $n \geq 0$ und k Knoten in C_n, den Typ von k in C_n
- gegeben (k, j, n) mit $n \geq 0$, k Knoten in C_n und $j \in \{1, 2\}$, den j-ten Nachfolger von k in C_n (oder $\perp$, wenn er nicht existiert)

(NB: Die Umkehrung gilt ebenfalls!)

NC

Theorem

NLogSpace $\subseteq$ NC^2 $\subseteq$ NC

Idee für Konstruktion von Schaltkreis C_n:

- Wir repräsentieren Konfigurationen α durch uqv für Arbeitsband plus Kopfposition auf Eingabeband (aber nicht dessen Inhalt)
- Dann ist Konfigurationsmenge nur von n abhängig, nicht von genauer Eingabe (genauso wie C_n)
- Der Schaltkreis berechnet den transitiven Abschluss von "$\vdash_M$" auf dieser Konfigurationsmenge
  mittels "teile und herrsche" (ähnlich wie im Satz von Savitch)
- Nur Basisfall $\alpha \vdash_M \alpha'$ hängt von Eingabe ab

Kapitel 6

Die Klasse AC

AC

Es gibt eine weitere Hierarchie

$$\mathsf{AC}^0 \subseteq \mathsf{AC}^1 \subseteq \cdots \subseteq \mathsf{AC} \subseteq \mathsf{P}$$

die exakt wie NC definiert ist, außer dass bei $\wedge$- und $\vee$-Gates das Fan-in unbeschränkt ist.

Interessanterweise konnte folgendes negatives Resultat bewiesen werden (ohne Beweis):

Theorem (Furst, Saxe, Sipser 1981; Ajtai 1983)

$\mathsf{PARITY} \notin \mathsf{AC}^0$

Daraus folgt offensichtlich $\mathsf{AC}^0 \subsetneq \mathsf{NC}^1$, also auch $\mathsf{AC}^0 \subsetneq \mathsf{P}$.

NC / AC

Einige weitere Probleme in NC / AC:

- Erreichbarkeit in gerichteten Graphen ist in NC (denn in NLogSpace)
- Das Auswertungsproblem für AL-Formeln ist in NC1
- Multiplikation, Division, Potenzieren, ganzer Zahlen sind in NC1
- Erreichbarkeit in gitterförmigen Graphen ist in AC0:
- Die Beantwortung von jeder festen (Boolschen) SQL-Anfrage ist in AC0

Kapitel 6

P-Härte

P-Härte

Identifizierte Teilklassen von P werfen neue Fragen auf:

- Gilt P = NC, also: ist jedes Polyzeitproblem effizient parallelisierbar?
- Gilt sogar P = LogSpace?

Beides ist unbekannt, aber man vermutet, dass das nicht der Fall ist.

Um Kandidaten für "echte" P-Probleme zu finden, benötigen wir

Begriffe von Härte und Vollständigkeit für P

Polynomialzeit-Reduktionen sind hier nicht sinnvoll, da

für alle $L, L' \in$ P mit L' nicht-trivial: $L \leq_p L'$

(*nicht-trivial*: es gibt positive Instanzen und negative Instanzen)

P-Härte

Definition P-Härte, P-Vollständigkeit

Problem L ist

- *P-hart* wenn $L' \leq_{\log} L$ für alle $L' \in$ P;
- *P-vollständig* wenn L P-hart und in P.

Also: wenn Problem L P-vollständig, dann

1. L nicht in LogSpace, außer wenn LogSpace = P
2. L nicht in NC (= nicht effizient parallelisierbar), außer wenn NC = P

Für 2. brauchen wir allerdings noch (ohne Beweis):

Theorem

Wenn $L \in$ NC und $L' \leq_{\log} L$, dann $L' \in$ NC.

P-Härte

Das Circuit Value Problem ist das "protoytpische" P-vollständige Problem:

Theorem (Ladner)

CVP ist P-vollständig.

Weitere P-vollständige Probleme z.B.:

- das Leerheitsproblem für kontextfreie Grammatiken
- monotones CVP (Schaltkreise ohne Negation)
- Linear programming (= Integer Programming mit rationalen Lösungen)
- Erfüllbarkeit von AL-Formeln in Horn-Form

$$p_1 \wedge \cdots \wedge p_n \rightarrow p, \qquad p_1 \wedge \cdots \wedge p_n \rightarrow \bot, \qquad p$$

Kapitel 6

Untere Schranken

NP versus $P_{/poly}$: ein Zugang zu $P \neq NP$?

Vor ca. 30 Jahren hat man geglaubt, das Problem $P \stackrel{?}{=} NP$ lösen zu können

Ein Zugang über Schaltkreiskomplexität ...

- wurde lange erforscht
- lieferte viele interessante und anspruchsvolle Resultate
- aber hat bisher nicht zum Ziel geführt

Es folgt: ein kurzer Abriss dieses Forschungsprogramms

NP versus $P_{/poly}$: ein Zugang zu $P \neq NP$?

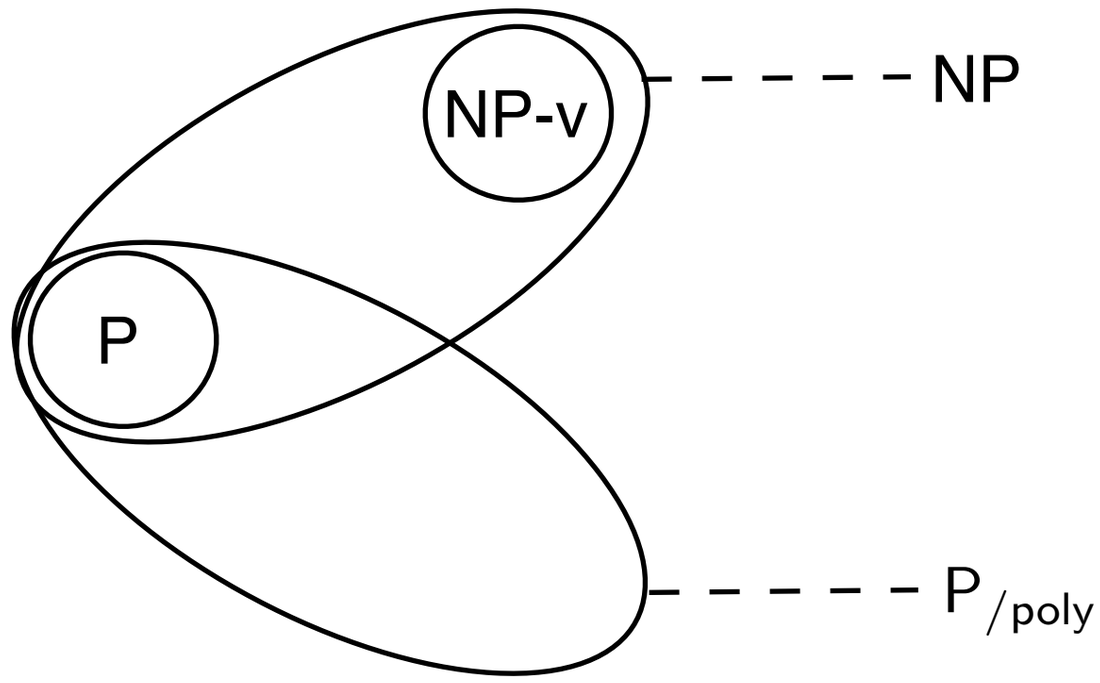
Zur Erinnerung:

$P = \text{uniform } P_{/poly} \subseteq P_{/poly}$

Also gilt:

wenn $NP \not\subseteq P_{/poly}$

dann $P \neq NP$



Man hat lange versucht, $NP \not\subseteq P_{/poly}$ zu zeigen

NP versus $\mathsf{P}_{/\mathrm{poly}}$ mittels schwerer Funktionen

Definition schwere Funktion

Boolesche Funktion $f : \{0,1\}^n \to \{0,1\}$ ist schwer,
wenn Schaltkreiskomplexität von f größer als poly(n) ist

Zur Erinnerung:

Theorem (Shannon 1949)

Für alle $n > 1$ gibt es Boolesche Funktion $f : \{0,1\}^n \to \{0,1\}$ mit Schaltkreiskomplexität $> \frac{2^n}{10n}$.

Folgerung:

Für jedes $n \geq 1$ gibt es schwere Funktionen $f : \{0,1\}^n \to \{0,1\}$.

(Es gilt sogar: Die meisten Funktionen $\{0,1\}^n \to \{0,1\}$ sind schwer)

NP versus $\mathsf{P}_{/\mathsf{poly}}$ mittels schwerer Funktionen

Versuch, NP $\not\subseteq \mathsf{P}_{/\mathsf{poly}}$ zu zeigen:
Finde Familie $(f_n)_{n\in\mathbb{N}}$ schwerer Funktionen, die in NP berechenbar sind

Man begann, Funktionen zu finden,
die schwer bezüglich eingeschränkter Schaltkreisklassen sind:

- konstante Tiefe
- konstante Tiefe plus Zählgatter
- monotone Schaltkreise

Boolesche Fkt. $f : \{0,1\}^n \to \{0,1\}$ ist schwer für Schaltkreisklasse $\mathcal{C}$,
wenn $\mathcal{C}$-Schaltkreiskomplexität von f größer als poly(n) ist,
d. h. f kann nicht durch $\mathcal{C}$-Schaltkreise d. Größe poly(n) berechnet werden

Schaltkreise konstanter Tiefe

Zur Erinnerung:

Theorem (Furst, Saxe, Sipser 1981; Ajtai 1983)

PARITY $\notin$ AC^0

Das bedeutet: die Funktionenfamilie $(f_n)_{n\in\mathbb{N}}$ mit

$$f_n(x_1, \ldots, x_n) = \text{Parität von } x_1 \cdots x_n$$

ist schwer für Schaltkreise konstanter Tiefe

Nächster Schritt: Untere Schranken für allgemeinere Schaltkreisklassen?

Schaltkreise konstanter Tiefe mit Zählgattern

Erlauben zusätzlich MOD_m-Gatter:
berechnen die Funktion $\text{MOD}_m(x_1, \ldots, x_n) = \begin{cases} 0, \text{falls } \sum_{i=1}^{n} x_i \equiv 0 \bmod m \\ 1, \text{sonst} \end{cases}$
(Klar: PARITY $= \text{MOD}_2$)

Definition ACC^0

$\text{ACC}^0(m_1, \ldots, m_k) = \{L \mid L$ wird von einer Schaltkreisfamilie konstanter Tiefe und poly. Größe akzeptiert, die nur Gatter $\wedge, \vee, \neg, \text{MOD}_{m_1}, \ldots, \text{MOD}_{m_k}$ verwendet$\}$

$\text{ACC}^0 = \bigcup_{k \geq 0} \bigcup_{m_1 > 1} \cdots \bigcup_{m_k > 1} \text{ACC}^0(m_1, \ldots, m_k)$

MOD_p ist schwer für SKe konstanter Tiefe mit MOD_q-Gattern (o. Bew.):

Theorem (Razborov 1987; Smolensky 1987)

Für je zwei verschiedene Primzahlen p, q ist MOD_p nicht in $\text{ACC}^0(q)$.

monotone Schaltkreise

Betrachten Schaltkreisklassen ohne Größenbeschränkung

Definition Monotonie

Ein Schaltkreis heißt *monoton*, wenn er nur $\wedge$- und $\vee$-Gatter enthält.

Für alle n-Tupel $\overline{x}, \overline{y} \in \{0,1\}^n$ mit $\overline{x} = (x_1, \ldots, x_n)$ und $\overline{y} = (y_1, \ldots, y_n)$ gelte $\overline{x} \preceq \overline{y}$, wenn für alle $i \leq n$ gilt: $\quad x_i = 1 \;\Rightarrow\; y_i = 1$.

Eine Boolesche Funktion $f : \{0,1\}^n \to \{0,1\}$ heißt *monoton*, wenn für alle $\overline{x}, \overline{y} \in \{0,1\}^n$ gilt: $\quad \overline{x} \preceq \overline{y} \;\Rightarrow\; f(\overline{x}) \leq f(\overline{y})$

Relativ leicht zu sehen:

- Jeder monotone Schaltkreis berechnet eine monotone Funktion
- jede monotone Fkt. kann von einem (hinreichend großen) monotonen Schaltkreis berechnet werden

CLIQUE braucht große monotone Schaltkreise

Betrachten Boolesche Funktion $\text{CLIQUE}_{k,n} : \{0,1\}^{\binom{n}{2}} \to \{0,1\}$ mit

$\text{CLIQUE}_{k,n}(\overline{x}) = 1 \Leftrightarrow$
Der Graph mit n Knoten, dessen Adjazenzmatrix durch $\overline{x}$ gegeben ist, hat eine k-Clique

Es folgt sofort: $\text{CLIQUE}_{k,n}$ ist monoton

$\text{CLIQUE}_{k,n}$ ist schwer für monotone Schaltkreise (ohne Beweis):

Theorem (Razborov 1985; Andreev 1985; Alon und Boppana 1987)

$\exists \varepsilon > 0 \ \ \forall k \leq n^{\frac{1}{4}}$: es gibt keinen monotonen Schaltkreis der Größe $< 2^{\varepsilon\sqrt{k}}$, der $\text{CLIQUE}_{k,n}$ berechnet

Verallgemeinerung auf beliebige (nicht-monotone) Schaltkreisklassen offen

Zurück zu *uneingeschränkt* schweren Funktionen

Versuch, NP $\not\subseteq \mathsf{P}_{/\mathsf{poly}}$ zu zeigen:
Finde Familie $(f_n)_{n\in\mathbb{N}}$ schwerer Funktionen, die in NP berechenbar sind

Versuch blieb erfolglos –
beste bisher bekannte untere Schranke ist linear (ohne Beweis):

Theorem (Iwama, Morizumi 2002)

Es gibt eine Familie $(f_n)_{n\in\mathbb{N}}$ von polyzeit-konstruierbaren Funktionen $f_n : \{0,1\}^n \to \{0,1\}$,
deren Schaltkreiskomplexität mindestens $5n - o(n)$ beträgt.

Schaltkreiskomplexität: bekannte untere Schranken

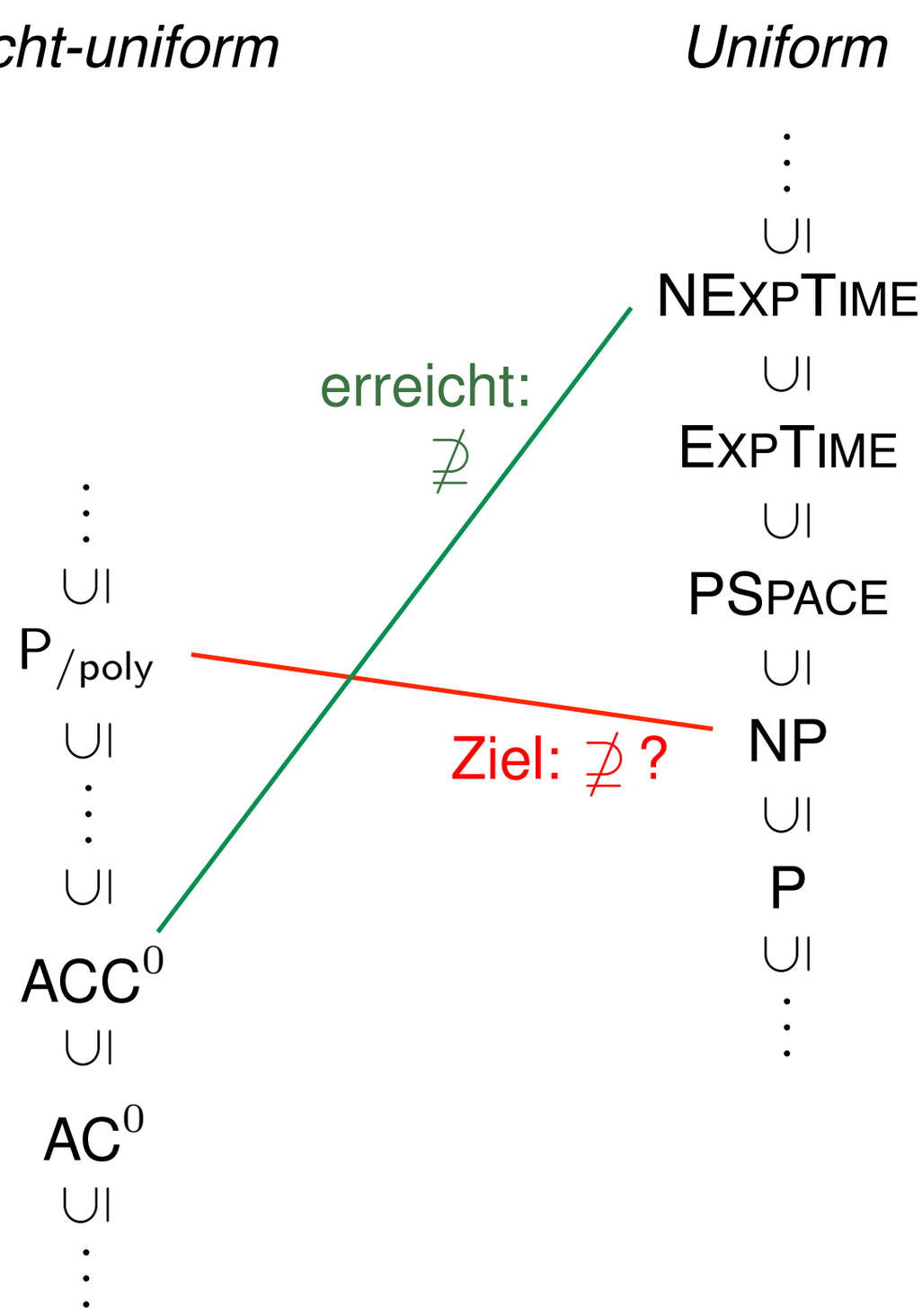
Ziel: Gilt NP $\not\subseteq P_{poly}$?

Bisher erreicht:

NExpTime $\not\subseteq ACC^0$

(Williams 2011)

You can't always get what you want ...



Offene Fragen für ACC^0

Bekannt: $PARITY \notin AC^0 \quad \Rightarrow \quad AC^0 \subsetneq NC^1$ und $AC^0 \subsetneq P$

Offene Fragen

- $ACC^0 \subsetneq NC^1$?
- $ACC^0 \subsetneq P$?
- $CLIQUE \notin ACC^0(6)$?

Schaltkreise nicht konstanter Tiefe

Beschränkung der Tiefe wird gelockert

Einfachste SK-Klasse mit nicht konstanter Tiefe: $O(\log n)$ Tiefe und $O(n)$ Größe

Offene Fragen

- Finde eine n-stellige Boolesche Funktion, die *nicht* durch SK der Tiefe $O(\log n)$ und Größe $O(n)$ berechnet werden kann
- Finde eine *nicht-Boolesche* Funktion mit dieser Eigenschaft

(Mittels eines Zählarguments kann man leicht beweisen, dass es eine solche Funktion geben muss)

Zusammenfassung untere Schranken

Forschungsprogramm war erfolgreich für einige
eingeschränkte Schaltkreisklassen:

- konstante Tiefe
- monotone Schaltkreise

Für diese sind nichttriviale untere Schranken bekannt

Die ursprüngliche Frage “NP $\not\subseteq \mathrm{P}_{/\mathrm{poly}}$?” bleibt offen:

Bisher kennt man für keine explizite Funktion f
eine *super-lineare* untere Schranke für die Schaltkreiskomplexität von f

Übersicht Vorlesung

- Kapitel 1: Einführung
- Kapitel 2: Turingmaschinen
- Kapitel 3: P vs. NP
- Kapitel 4: Mehr Ressourcen, mehr Möglichkeiten?
- Kapitel 5: Platzkomplexität
- Kapitel 6: Schaltkreise
- Kapitel 7: Orakel