# Komplexitätstheorie

## Kapitel 7: Orakel

# Einleitung

Ein Gedankenexperiment:

- Nimm an, Programm $A$ rufe Unterprogramme $B_1,...,B_n$ auf
- Wir haben ein Orakel, das wir nach den $B_i$ befragen können
- Orakelantwort kommt nach 1 Schritt zurück (ohne extra Speicherbedarf)

Ermöglicht Analyse der Kosten für $A$ relativ zu den Kosten der $B_i$

Orakel erlauben feinere Komplexitätsanalyse mancher Probleme:

- Struktur der Standard-Komplexitätsklassen wird verfeinert
- Einige Orakelklassen haben natürliche vollständige Probleme

Orakel haben wie Nichtdeterminismus theoretischen Charakter

# Kapitel 7

## Die Polynomielle Hierarchie (PH)

# PH

(N)LogSpace, NC, AC, etc: reiche Struktur innerhalb von P

Die polynomielle Hierarchie liefert Struktur zwischen P und PSpace

Wichtiges Problem für Schaltkreisentwurf:

**Definition Minimal Circuit (MC)**

Schaltkreis $C$ ist minimal wenn $|C'| \geq |C|$ für alle $C'$, die *äquivalent* zu $C$ sind, also gleiche Anzahl $n$ von Eingabebits und

$$C(w) = C'(w) \text{ für alle } w \in \{0,1\}^n$$

MC ist Menge aller minimalen Schaltkreise.

Was ist die ”richtige” Komplexitätsklasse (Vollständigkeit!) für dieses Problem?

# PH

Offensichtliches “Teilproblem” ist CEQ $:= \{(C, C') \mid C$ äquivalent zu $C'\}$

**Lemma**

CEQ ist co-NP-vollständig.

Betrachte wieder $\overline{\text{MC}}$:

- Ist in NP wenn wir einen CEQ-Algorithmus als Unterprozedur ohne Zeitverbrauch verwenden
- Wir können beide Algorithmen nicht zu einem NP-Algorithmus vereinigen, weil der NP-Algorithmus einen co-NP-Algorithmus aufruft ($\exists\forall$-Charakteristik)

Derartige Probleme sind offensichtlich in PSpace. Man kann deren Komplexität aber noch exakter bestimmen

# Orakel

Orakel: Unterprogramm, dessen Zeitverbrauch ausgeblendet wird, dargestellt als formale Sprache

**Definition Orakel-TM**

Eine *Orakel-TM (OTM)* $M^O$ ist eine (deterministische oder nicht-deterministische) TM $M$ ausgestattet mit einem Orakel $O \subseteq \Sigma^*$. OTM hat

- ein zusätzliches *Orakelband*
- drei spezielle Zustände $q_?, q_+, q_-$.

Für $q_+$ und $q_-$ sind normale Transitionen definiert. Der Folgezustand von $q_?$ ist $q_+$ wenn das momentane Wort auf dem Orakelband in $O$ ist und $q_-$ sonst. Kopfposition und Bandinhalte bleiben dabei unverändert.

Also schon gesehen: $\overline{\text{MC}}$ wird von Polyzeit-beschränkter ONTM akzeptiert wenn O=CEQ

# Orakel

Orakel-TM ist ebensowenig realistisches Berechnungsmodell wie nicht-deterministische TMs

Dennoch können mittels Orakel-TMs natürliche Komplexitätsklassen definiert werden (natürlich = erfassen viele natürliche Probleme)

Orakel-TMs können auch verwendet werden, um komplexitäts-theoretische Annahmen zu formalisieren, z.B.:

- wenn SAT in konstanter Zeit lösbar wäre, welche anderen Probleme wären dann effizient lösbar (in Polyzeit mit SAT-Orakel)?
- wenn das Halteproblem für Turingmaschinen H entscheidbar wäre, welche anderen Probleme wären dann entscheidbar (von TM mit H-Orakel)

# Orakel

## Definition Orakel-Komplexitätsklassen

Sei $O \subseteq \Sigma^*$ ein Orakel. Dann:

- $\mathsf{P}^O := \{L \mid L$ wird von ODTM $M^O$ in poly-Zeit entschieden $\}$
- $\mathsf{NP}^O := \{L \mid L$ wird von ONTM $M^O$ in poly-Zeit entschieden $\}$

Sei $\mathcal{C}$ Komplexitätsklasse. Dann:

$$\mathsf{P}^{\mathcal{C}} := \bigcup_{O \in \mathcal{C}} \mathsf{P}^O \qquad \mathsf{NP}^{\mathcal{C}} := \bigcup_{O \in \mathcal{C}} \mathsf{NP}^O$$

Schon gezeigt: $\overline{\mathsf{MC}} \in \mathsf{NP}^{\mathsf{CEQ}}$, also in $\overline{\mathsf{MC}} \in \mathsf{NP}^{\text{co-NP}}$

Leicht zu sehen: $\mathsf{NP}^{\text{co-NP}} = \mathsf{NP}^{\mathsf{NP}}$

# PH

Einige Beispiele:

- $\mathrm{P}^{\mathrm{P}} = \mathrm{P}$, $\mathrm{NP}^{\mathrm{P}} = \mathrm{NP}$;

  (Integriere Orakel in OTM)

- $\mathrm{NP}^{\mathrm{NP}} = \mathrm{NP}$ ist hingegen nicht klar, denn $\text{co-NP} \subseteq \mathrm{P}^{\text{co-NP}} = \mathrm{P}^{\mathrm{NP}} \subseteq \mathrm{NP}^{\mathrm{NP}}$

- $\mathrm{P}^{\mathrm{NP}} = \mathrm{P}^{\mathrm{SAT}}$ und ebenso für jedes andere NP-vollständige Problem

  (Genügt zu zeigen: $\mathrm{P}^{O} \subseteq \mathrm{P}^{\mathrm{SAT}}$ mit $O \in \mathrm{NP}$
  integriere dazu Reduktion $O \leq_p \mathrm{SAT}$ in OTM)

$\text{co-NP}^{\mathcal{C}}$ verwenden wir für $\overline{\mathrm{NP}^{\mathcal{C}}}$

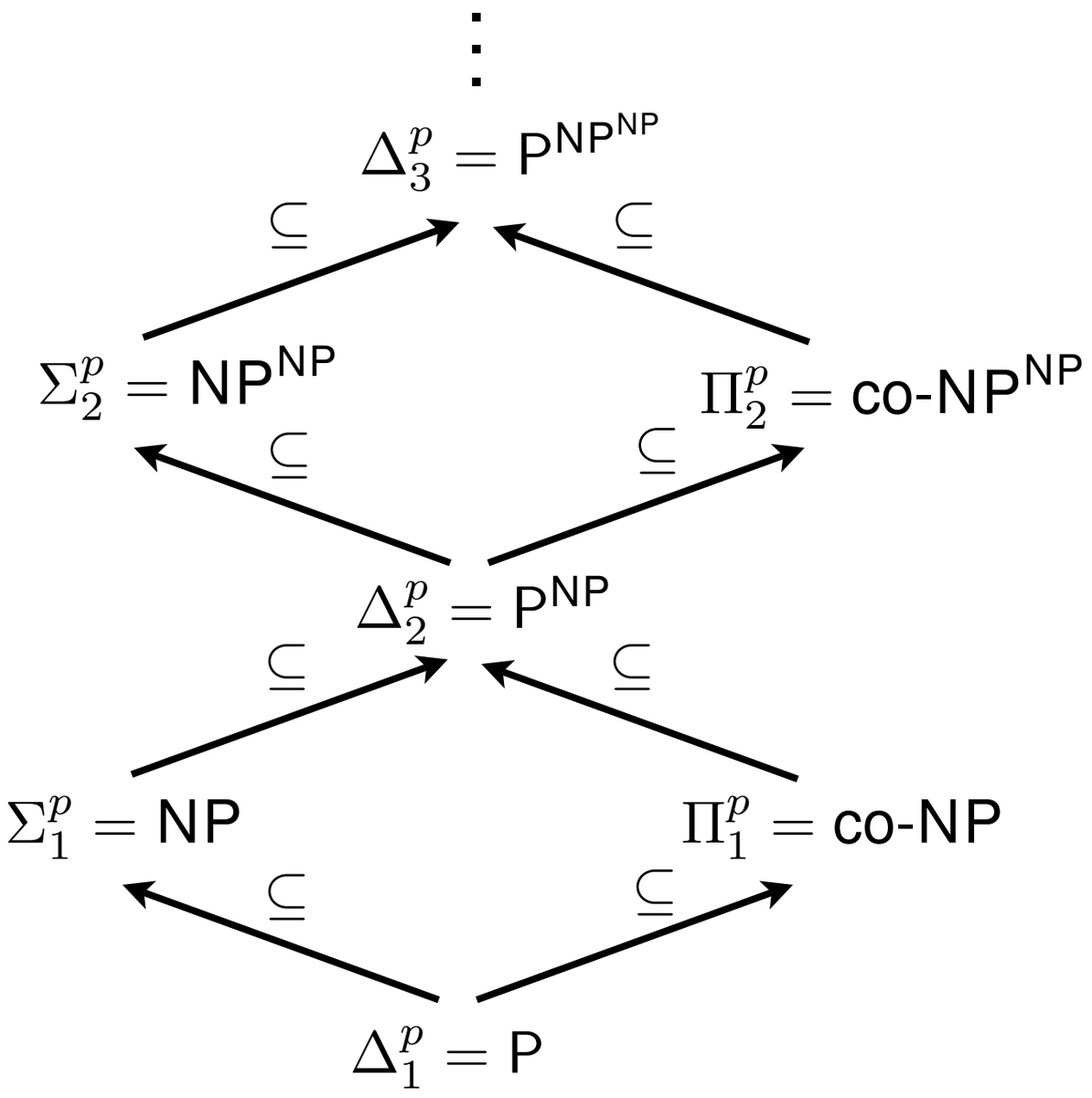
# PH: Definition

Die polynomielle Hierarchie entsteht nun durch iteriertes Orakel-anwenden

**Definition Polynomielle Hierarchie**

- $\Delta_1^p = \mathsf{P}$, $\Sigma_1^p = \mathsf{NP}$, $\Pi_1^p =$ co-NP,
- Für $k \geq 1$ sei
  - $\Delta_{k+1}^p = \mathsf{P}^{\Sigma_k^p}$
  - $\Sigma_{k+1}^p = \mathsf{NP}^{\Sigma_k^p}$
  - $\Pi_{k+1}^p = \text{co-}\Sigma_{k+1}^p$

# PH: Bild und einfache Eigenschaften




Echtheit der Inklusionen ist unbekannt.

**Lemma**

Für alle $k \geq 1$ gilt: $\Delta_k^p \subseteq \Sigma_k^p \subseteq \Delta_{k+1}^p$ und $\Delta_k^p \subseteq \Pi_k^p \subseteq \Delta_{k+1}^p$

# Die Klasse PH

Es gibt auch eine Klasse für die gesamte polynomielle Hierarchie:

**Definition Polynomielle Hierarchie**

$$\mathsf{PH} = \bigcup_{k \geq 1} \Sigma_k^p$$

Die polynomielle Hierarchie liegt zwischen P und PSpace:

**Theorem**

$$\mathsf{PH} \subseteq \mathsf{PSPACE}$$

# Kollaps der PH

Viele Resultate in der Komplexitätstheorie beziehen sich auf die Echtheit der Inklusionen in der polynomiellen Hierarchie

Die polynomielle Hierarchie kollabiert wenn PH $= \Sigma_k^p$ für ein $k \geq 1$

**Lemma**

Wenn $\Sigma_k^p = \Sigma_{k+1}^p$, dann PH $= \Sigma_k^p$.

Also: $\Sigma_{k-1}^p \neq \Sigma_k^p$ schwächere Annahme als $\Sigma_k^p \neq \Sigma_{k+1}^p$

und P $\neq$ NP schwächste aller dieser Annahmen

Anders formuliert: PH kollabiert am ehesten weit oben!

**Theorem**

Wenn PH $=$ PSPACE, dann kollabiert PH.

# Eine nützliche Eigenschaft

Eine Aussage über eingeschränkte Interaktion mit dem Orakel

**Lemma**

Sei $M^O$ eine Polyzeit-ONTM mit Orakel $O \in \Sigma_k^p$ mit $q_+ = q_{\text{acc}}$
(d. h.: $M^O$ akzeptiert, sobald eine Orakelfrage positiv beantwortet wird).

Dann gilt: $L(M^O) \in \Sigma_k^p$.

Idee:

- rate Orakelantworten im Voraus
- integriere $O$-Berechnung – verwirf bei abweichenden Antworten sofort

Analoge Aussage per Komplementierung:

**Lemma**

Sei $M^O$ eine Polyzeit-ONTM mit Orakel $O \in \Pi_k^p$ mit $q_- = q_{\text{rej}}$.

Dann gilt: $L(M^O) \in \Pi_k^p$.

# Kapitel 7

## Logische Charakterisierung der Polynomiellen Hierarchie

# Charakterisierung PH

Zur Erinnerung: $L \in$ NP gdw.
es gibt Polynom $q$ und $L' \in$ P mit $L = \{w \mid \underline{\exists} u \in \{0,1\}^{q(|w|)} : (w,u) \in L'\}$.

Folgende Charakterisierung generalisiert Definition von NP

**Theorem**

$L \in \Sigma_k^p$ gdw. es Polynom $q$ und $L' \in$ P gibt, so dass

$$L = \{w \mid \underline{\exists} u_1 \in A \,.\, \underline{\forall} u_2 \in A \,.\, \underline{\exists} u_3 \in A \;\ldots\; \underline{Q} u_k \in A : (w, u_1, \ldots, u_k) \in L'\},$$

wobei $A = \{0,1\}^{q(|w|)}$ und $Q$ der sich durch Alternierung ergebende Quantor.

Die Klassen der polynomiellen Hierarchie werden also mittels logischer Ausdrückbarkeit beschrieben

Frage nach Echtheit der Inklusionen in PH: liefern zusätzliche Quantoren-alternierungen zusätzliche Ausdrucksstärke?

# Charakterisierung PH

**Lemma**

Für $L \subseteq \Sigma^*$ gilt $L \in \Sigma_k^p$ gdw. es gibt Polynom $p$ und Relation $R \subseteq \Sigma^* \times \Gamma^*$ so dass

- $(w, b) \in R$ impliziert $|b| \leq p(|w|)$
- $R \in \Pi_{k-1}^p$ (wobei $\Pi_0^p :=$ P)
- $L = \{w \mid \exists b : (w, b) \in R\}$

Idee:

- Induktion über $k$
- Der Fall $k = 1$ folgt direkt aus Definition NP
- In "$\Rightarrow$" ist der Beweis $b$ eine Berechnung der NTM zusammen mit Beweisen für die "ja"-Antworten des Orakels (induktiv)

# Charakterisierung PH

## Korollar

Für $L \subseteq \Sigma^*$ gilt $L \in \Pi_k^p$ gdw. es gibt Polynom $p$ und Relation $R \subseteq \Sigma^* \times \Gamma^*$ so dass

- $(w, b) \in R$ impliziert $|b| \leq p(|w|)$
- $R \in \Sigma_{k-1}^p$ (wobei $\Sigma_0^p :=$ P)
- $L = \{w \mid \forall b \in \Gamma^*$ mit $|b| \leq p(|w|) : (w, b) \in R\}$

Beweis: Für $\overline{L} \in \Sigma_k^p$ gibt es $R$ wie in vorigem Lemma, verwende für $L$:

$$\widehat{R} := \{(w, b) \in \Sigma^* \times \Gamma^* \mid (w, b) \notin R \text{ und } |b| \leq p(|w|)\}$$

Aus Lemma + Korollar folgt nun das ursprüngliche Theorem:
Ersetze wiederholt $\Sigma_i^p$ und $\Pi_i^p$ durch ihre Beweissysteme

# Kapitel 7

## Härte und Vollständigkeit in der polynomiellen Hierarchie

# Vollständigkeit

Um Probleme korrekt in die polynomielle Hierarchie "einzuordnen", brauchen wir Vollständigkeitsbegriff

**Definition**

Für $k \geq 1$ ist Problem $L$

- $\Sigma_k^p$-*hart* wenn $L' \leq_p L$ für alle $L' \in \Sigma_k^p$;
- $\Sigma_k^p$-*vollständig* wenn $L$ sowohl $\Sigma_k^p$-hart als auch in $\Sigma_k^p$.

Für $\Pi_k^p$, $\Delta_k^p$ und PH analog (außer für $\Delta_1^p = \mathrm{P}$)

Aber PH hat wahrscheinlich keine vollständigen Probleme:

**Lemma**

Wenn für PH vollständige Probleme existieren, kollabiert die Hierarchie

# Vollständigkeit

QBF liefert uniforme Familie von „typischen“ vollständigen Problemen

Für $\overline{V} = v_1, \ldots, v_n$ schreiben wir $\exists\overline{V}$ als Abkürzung für $\exists v_1 \cdots \exists v_n$

$\forall\overline{V}$ als Abkürzung für $\forall v_1 \cdots \forall v_n$

**Definition k-QBF**

QBF $Q_1\overline{V_1} \cdots Q_n\overline{V_n}\varphi$ heißt $k$-*QBF*, wenn

- $n = k$
- $Q_1 = \exists, \quad Q_2 = \forall, \quad Q_3 = \exists$ etc. (Quantoren alternieren)

$\text{QBF}_k$ ist die Menge aller gültigen $k$-QBFs.

Beispiel für 3-QBF: $\exists v_1 \exists v_2 \forall v_3 \exists v_4 \exists v_5 . \varphi$

# Vollständigkeit

**Theorem**

Für alle $k \geq 1$ ist QBF$_k$ $\Sigma_k^p$-vollständig.

Idee:

- “in $\Sigma_k^p$”: benutze logische Charakterisierung
- Härte: benutze logische Charakterisierung und Übersetzung von TM in AL-Formel analog zum Beweis von Cook’s Theorem

Beginnt man die Quantorenalternierung mit “$\forall$”, so ist $k$-QBF $\Pi_k^p$-vollständig.

# Vollständigkeit

In der Logik gibt es verschiedene natürliche Probleme, die vollständig für Klassen der polynomiellen Hierarchie sind.

**Definition MINSAT**

Für zwei WZen $\pi$ und $\pi'$ schreiben wir $\pi \leq \pi'$ gdw.

$$\pi'(v) = 1 \text{ impliziert } \pi(v) = 1 \text{ für alle Variablen } V$$

$\pi$ ist *minimales Modell* von AL-Formel $\varphi$ wenn

- $\pi$ erfüllt $\varphi$
- für alle $\pi'$, die $\varphi$ erfüllen, gilt $\pi \leq \pi'$

MINSAT ist die Menge aller Tripel $(\varphi, v)$ mit $\varphi$ AL-Formel und $v$ Variable so daß $\pi(v) = 0$ in allen minimalen Modellen von $\varphi$.

**Theorem**

MINSAT ist $\Pi_2^p$-vollständig.

# Vollständigkeit

Weiteres natürliches vollständiges Problem z.B.:

Äquivalenzproblem für kontextfreie Grammatiken über 1-elementigen (Terminal-)Alphabeten ist $\Pi_2^p$-vollständig.

Es wird vermutet, dass MC (Minimial Circuit) ebenfalls $\Pi_2^p$-vollständig ist, die Härte konnte aber bisher nicht bewiesen werden!

Für Klassen weit oben in der polynomiellen Hierarchie scheint es nur sehr wenig „natürliche“ vollständige Probleme zu geben

# Kapitel 7

## P versus NP und das Theorem von Baker, Gill und Solovay

# Baker, Gill und Solovay (BGS)

Warum ist P ≠ NP so schwer zu zeigen?

Theorem von BGS bietet eine Erklärung dafür:

**Theorem (Baker, Gill, Solovay 1975)**

Es gibt Orakel $A$ und $B$, so dass $\mathrm{P}^A = \mathrm{NP}^A$ und $\mathrm{P}^B \neq \mathrm{NP}^B$.

Das heißt: ein Beweis für P ≠ NP darf nicht relativierbar sein

Das schließt die meisten (elementaren) Beweistechniken aus

# BGS: der Fall $P^A = NP^A$

Der einfachere Teil:

**Lemma**

Es gibt ein Orakel $A$, so dass $P^A = NP^A$.

Idee:

- Wählen als $A$ ein beliebiges PSPACE-vollständiges Problem
- Zeigen: $PSPACE \overset{(1)}{\subseteq} P^A \subseteq NP^A \overset{(2)}{\subseteq} PSPACE$
  - (1) Für $L \in PSPACE$, berechne Reduktionsfunktion für $L \leq_p A$ und befrage Orakel
  - (2) Für $L \in NP^A$, integriere Orakelberechnung in Basis-ONTM $\rightsquigarrow$ NPSPACE-Maschine

# BGS: der Fall $P^B \neq NP^B$

Der anspruchsvollere Teil:

**Lemma**

Es gibt ein Orakel $B$, so dass $P^B \neq NP^B$.

Idee:

- Eingabealphabet für alle TM sei $\{0,1\}$ (o. B. d. A.)
- Ziel: konstruieren Orakel $B$ und Problem $L_B \in NP^B \setminus P^B$
- Wenn $B$ konstruiert ist, können wir $L_B$ setzen als

$$L_B = \{1^n \mid \exists w \in B : |w| = n\}$$

1. Leicht zu sehen: $L_B \in NP^B$, unabhängig von $B$
2. Müssen noch $B \subseteq \{0,1\}^*$ so konstruieren, dass $L_B \notin P^B$,
   d. h.: für *jede* Polyzeit-ODTM $M^?$ muss gelten: $L(M^B) \neq L_B$ $(*)$

# BGS

BGS' Ansatz hat zu zahlreichen ähnlichen Resultaten geführt, z.B.:

- Es gibt Orakel $A$ und $B$, so dass NP$^A$ = co-NP$^A$ und NP$^B \neq$ co-NP$^B$.
- Es gibt ein Orakel $A$, so dass NP$^A$ = co-NP$^A$ und P$^A \neq$ NP$^A$.
- Es gibt Orakel $A$ und $B$, so dass
  - für NP$^A \cap$ co-NP$^A$ vollständige Probleme existieren und
  - für NP$^B \cap$ co-NP$^B$ nicht

Probabilistische Analyse liefert zudem:

Für *fast alle* Orakel $A$ gilt P$^A \neq$ NP$^A$

# Über BGS hinaus

„Moderner Nachfahre“ von BGS für Schaltkreistheorie:

Theorem von Razborov und Rudich (1997) schließt natürliche Beweise für super-polynomielle Schaltkreiskomplexität aus

(EATCS-Gödelpreis 2007)

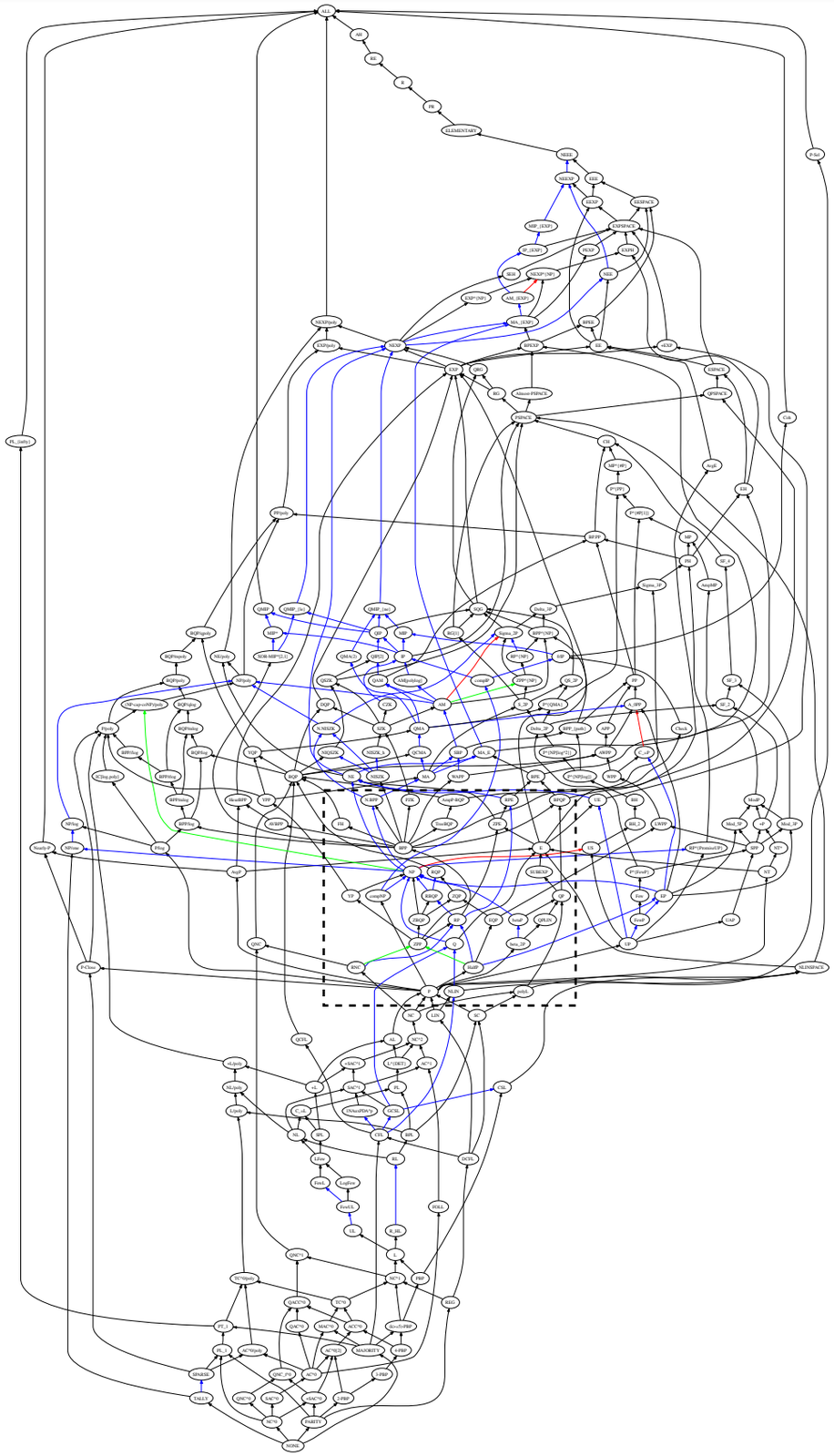
Es gibt neue Ansätze zum Beweis von P ≠ NP,
die weder von BGS noch RR ausgeschlossen werden:

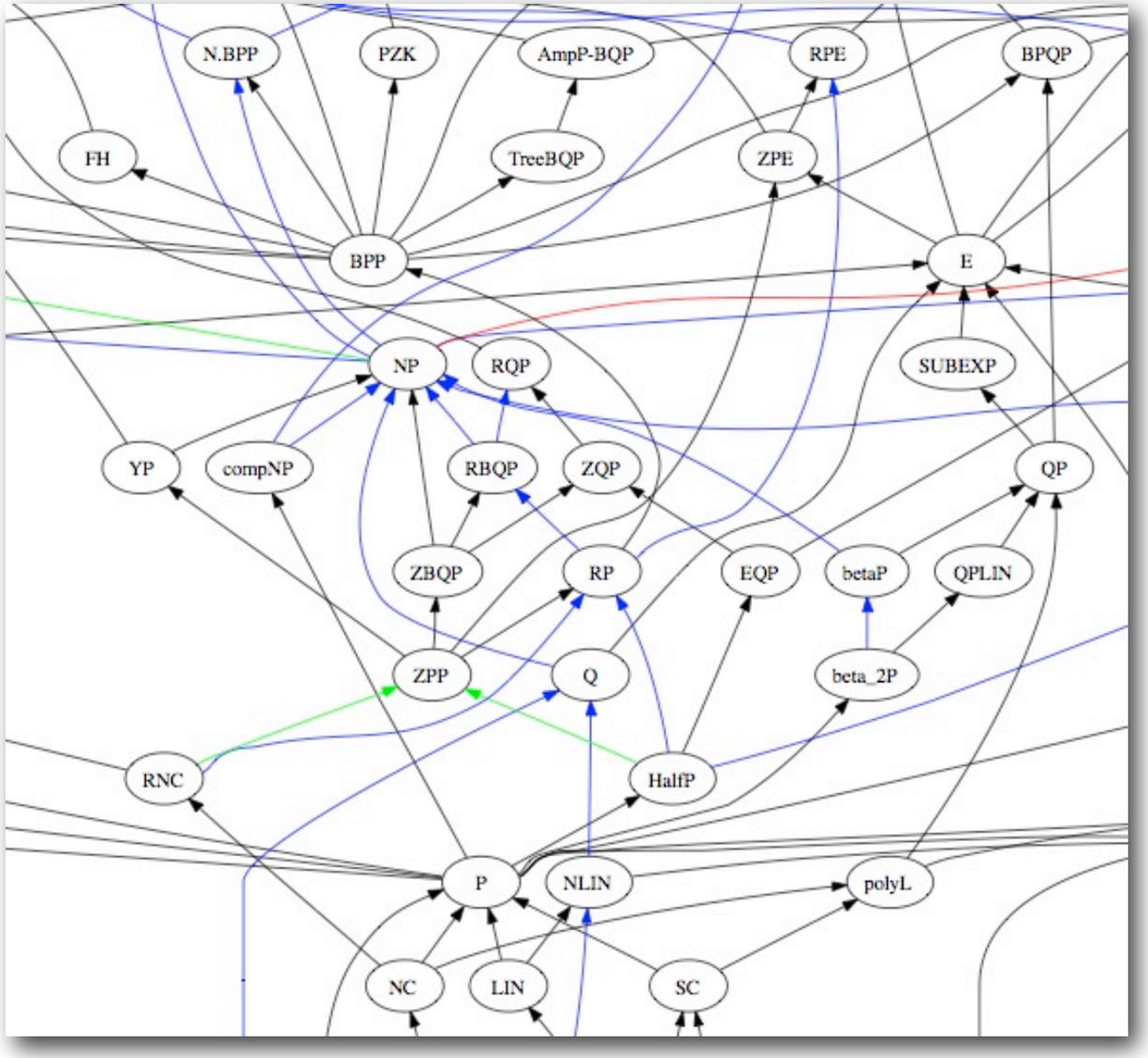
z.B. über algebraische Geometrie (Mulmuley 2012)

# Abschließende Bemerkung

Wie viele Komplexitätsklassen gibt es eigentlich?

# Hierarchie der Komplexitätsklassen (Ausschnitt)





# Mehr Komplexitätsklassen

Abgesehen von den angegebenen Büchern:

https://complexityzoo.uwaterloo.ca/Complexity_Zoo

http://www.math.ucdavis.edu/~greg/zoology/