Komplexitätstheorie

SoSe 2018
Thomas Schneider

Kapitel 7: Orakel

Homepage der Vorlesung: `http://tinyurl.com/ss18-kt`

Einleitung

Ein Gedankenexperiment: Nimm an, …

- Programm A rufe Unterprogramme $B_1, \ldots, B_n$ auf;
- wir haben ein **Orakel,** das wir nach den B_i befragen können;
- Orakel liefere Antwort nach 1 Schritt (ohne extra Speicherbedarf).

Die 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

NEXT

PH

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

Die Polynomialzeithierarchie liefert Struktur zwischen P und PSpace.

Wichtiges Problem für Schaltkreisentwurf:

Definition 7.1 (Minimal Circuit, MC)

Zwei Schaltkreise C, C' sind *äquivalent,*
wenn sie dieselbe Anzahl n von Eingabebits haben und

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

Schaltkreis C ist *minimal,* wenn $|C'| \geq |C|$ für alle äquivalenten C'.

MC ist Menge aller minimalen Schaltkreise.

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

T7.1

PH

Offensichtliches „Teilproblem“:

$$\text{CEQ} := \{(C, C') \mid C \text{ äquivalent zu } C'\}$$

Lemma 7.2

CEQ ist coNP-vollständig.

T7.2

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

- Ist in NP, wenn wir einen CEQ-Algorithmus als Orakel (Unterprozedur ohne Zeitverbrauch) verwenden. T7.3
- Man kann beide Algorithmen nicht zu einem NP-Algorithmus vereinigen, weil der NP-Algorithmus einen coNP-Algorithmus aufruft ($\exists\forall$-Charakteristik). T7.4

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

Orakel

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

Definition 7.3 (Orakel-TM)

Eine *Orakel-TM (OTM)* M^O ist eine TM M (DTM oder NTM), ausgestattet mit einem *Orakel* $O \subseteq \Sigma^*$ sowie

- einem zusätzlichen *Orakelband* und
- drei speziellen Zuständen: $q_?$ q_+ q_-

Dabei ist/sind

- $q_?$ ein Zustand, in dem das Orakel befragt wird
  $\rightsquigarrow$ Folgezustand q_+ (q_-), wenn aktuelles Wort auf O-Band $\in O$ ($\notin O$); Kopfposition und Bandinhalte bleiben dabei unverändert;
- für die Folgezustände q_+, q_- normale Transitionen definiert.

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

Orakel

Orakel-TM ist ebensowenig realistisches Berechnungsmodell wie nichtdeterministische TMs.

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

Orakel-TMs können auch verwendet werden,
um komplexitätstheoretische 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 (mittels TM mit *H*-Orakel)?

Orakel

Definition 7.4 (Orakel-Komplexitätsklassen)

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

$$\text{P}^O := \{L \mid L \text{ wird von ODTM } M^O \text{ in Polyzeit entschieden}\}$$
$$\text{NP}^O := \{L \mid L \text{ wird von ONTM } M^O \text{ in Polyzeit entschieden}\}$$

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

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

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

Leicht zu sehen: $\text{NP}^{\text{coNP}} = \text{NP}^{\text{NP}}$

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 $\mathrm{coNP} \subseteq \mathrm{P}^{\mathrm{coNP}} = \mathrm{P}^{\mathrm{NP}} \subseteq \mathrm{NP}^{\mathrm{NP}}$)
- $\mathrm{P}^{\mathrm{NP}} = \mathrm{P}^{\mathrm{SAT}}$ 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)

$\mathrm{coNP}^{\mathcal{C}} = (\mathrm{coNP})^{\mathcal{C}} = \mathrm{co}(\mathrm{NP}^{\mathcal{C}})$

PH: Definition

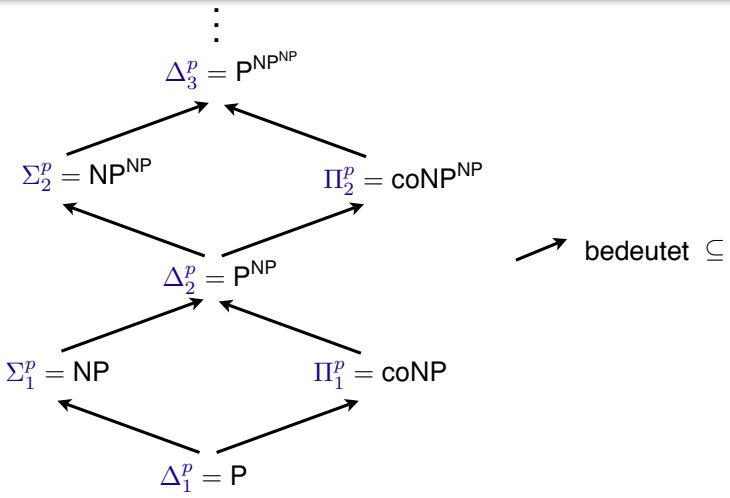
Die **Polynomialzeithierarchie** (**PH**, engl.: polynomial(-time) hierarchy) entsteht nun durch iterierte Orakelanwendung:

Definition 7.5 (Polynomialzeithierarchie)

- $\Delta_1^p = \mathrm{P}$ $\Sigma_1^p = \mathrm{NP}$ $\Pi_1^p = \mathrm{coNP}$
- Für $k \geq 1$ ist:

$$\Delta_{k+1}^p = \mathrm{P}^{\Sigma_k^p}$$
$$\Sigma_{k+1}^p = \mathrm{NP}^{\Sigma_k^p}$$
$$\Pi_{k+1}^p = \mathrm{co}\Sigma_{k+1}^p$$

PH: Bild und einfache Eigenschaften



Lemma 7.6

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

T7.5

Echtheit der Inklusionen ist unbekannt.

Die Klasse PH

Es gibt auch eine Klasse für die gesamte Polynomialzeithierarchie:

Definition 7.7 (Polynomialzeithierarchie)

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

Die Polynomialzeithierarchie liegt zwischen P und PSpace:

Theorem 7.8

$\mathrm{PH} \subseteq \mathrm{PSpace}$

T7.6

Kollaps der PH

Viele Resultate in der Komplexitätstheorie beziehen sich auf die Echtheit der Inklusionen in der Polynomialzeithierarchie.

Die Polynomialzeithierarchie *kollabiert,* wenn PH $= \Sigma_k^p$ für ein $k \geq 1$.

Lemma 7.9

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

T7.7

Also: $\Sigma_{k-1}^p \neq \Sigma_k^p$ ist 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 7.10

Wenn PH $=$ PSpace, dann kollabiert PH.

T7.8

Eine nützliche Eigenschaft

Eine Aussage über eingeschränkte Interaktion mit dem Orakel

Lemma 7.11

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

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

Idee:

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

T7.9

Analoge Aussage per Komplementierung:

Lemma 7.12

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

Charakterisierung PH

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

Folgende Charakterisierung generalisiert Definition von NP:

Theorem 7.13

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

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

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

Die Klassen der Polynomialzeithierarchie werden also mittels logischer Ausdrückbarkeit beschrieben.

Frage nach Echtheit der Inklusionen in PH:
liefern zusätzliche Quantorenalternierungen zusätzliche Ausdrucksstärke?

Charakterisierung PH

Lemma 7.14

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 $\Pi_0^p := \mathrm{P}$)
- $L = \{w \mid \exists b : (w, b) \in R\}$

Idee: T7.10

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

Charakterisierung PH

Korollar 7.15

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 $\Sigma_0^p := \mathrm{P}$)
- $L = \{w \mid \forall b \in \Gamma^* \text{ mit } |b| \leq p(|w|) : (w, b) \in R\}$

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

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

Theorem 7.14 folgt nun aus Lemma 7.15 und Korollar 7.16:
Ersetze wiederholt Σ_i^p und Π_i^p durch ihre Beweissysteme.

Kapitel 7

Vollständigkeit

Um Probleme korrekt in die Polynomialzeithierarchie „einzuordnen“, brauchen wir wieder einen passenden Vollständigkeitsbegriff.

Definition 7.16 (Härte und Vollständigkeit für PH)

Für $k \geq 1$ ist ein Problem L

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

Für Π_k^p, Δ_k^p und PH analog (außer für $\Delta_1^p = \mathrm{P}$).

Aber PH hat wahrscheinlich keine vollständigen Probleme:

Lemma 7.17

Wenn für PH vollständige Probleme existieren, kollabiert die Hierarchie.

T7.11

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 7.18 (k-QBF)

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

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

QBF_k ist die Menge aller gültigen k-QBFs.

Beispiel für 3-QBF: $\exists v_1 v_2\, \forall v_3\, \exists v_4 v_5\, \varphi(v_1, \ldots, v_5)$

Vollständigkeit

Theorem 7.19

Für alle $k \geq 1$ ist QBF_k Σ_k^p-vollständig.

Σ_k^p-Zugehörigkeit: benutze logische Charakterisierung

Σ_k^p-Härte: benutze logische Charakterisierung
sowie Übersetzung von TM in AL-Formel
analog zum Beweis des Satzes von Cook

T7.12

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

Vollständigkeit

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

Definition 7.20 (MINSAT)

Für zwei WZen π und π' schreiben wir $\pi \preceq \pi'$, wenn

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

π ist *minimales Modell* einer AL-Formel φ, wenn:

- π erfüllt φ
- für alle π', die φ erfüllen, gilt $\pi \preceq \pi'$

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

Theorem 7.21

MINSAT ist Π_2^p-vollständig.

Vollständigkeit

Weiteres natürliches vollständiges Problem z. B.:

Äquivalenzproblem für kontextfreie Grammatiken über
1-elementigen (Terminal-)Alphabeten ist Π_2^p-vollständig.

Siehe auch:

M. Schaefer and C. Umans.
Completeness in the polynomial-time hierarchy: a compendium.
`http://ovid.cs.depaul.edu/documents/phcom.pdf`

Es wird vermutet, dass MC (Minimial Circuit) ebenfalls Π_2^p-vollständig ist, die Härte konnte aber bisher nicht bewiesen werden!

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

Kapitel 7

Baker, Gill und Solovay (BGS)

Warum ist P $\neq$ NP so schwer zu zeigen?

Der Satz von Baker, Gill und Solovay (BGS) bietet eine Erklärung dafür:

Theorem 7.22 (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 $\neq$ NP darf nicht relativierbar sein.

Das schließt die meisten (elementaren) Beweistechniken aus.

(**Allerdings:** Weder löst BGS die Frage P $\neq$ NP, noch legt BGS einen konkreten Beweisansatz nahe.)

BGS: der Fall $\mathrm{P}^A = \mathrm{NP}^A$

Der einfachere Teil:

Lemma 7.23

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

Idee:

- Wählen als A ein beliebiges PSpace-vollständiges Problem.
- Zeigen: $\mathrm{PSpace} \overset{(1)}{\subseteq} \mathrm{P}^A \subseteq \mathrm{NP}^A \overset{(2)}{\subseteq} \mathrm{PSpace}$
  - (1) Für gegebenes $L \in \mathrm{PSpace}$ berechne Reduktionsfunktion für $L \leq_p A$ und befrage Orakel.
  - (2) Für gegebenes $L \in \mathrm{NP}^A$ integriere Orakelberechnung in Basis-ONTM $\rightsquigarrow$ NPSpace-TM.

T7.13

BGS: der Fall $\mathrm{P}^B \neq \mathrm{NP}^B$

Der anspruchsvollere Teil:

Lemma 7.24

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

Idee:

- Eingabealphabet für alle TM sei $\{0,1\}$ (o. B. d. A.)
- **Ziel:** konstruieren Orakel B und Problem $L_B \in \mathrm{NP}^B \setminus \mathrm{P}^B$.
- 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: $L_B \in \mathrm{NP}^B$, für jedes B
2. Müssen noch $B \subseteq \{0,1\}^*$ so konstruieren, dass $L_B \notin \mathrm{P}^B$, d. h.: für jede Polyzeit-ODTM $M^?$ muss gelten: $L(M^B) \neq L_B$ $(*)$

T7.14

BGS: über „P versus NP“ hinaus

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

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

Probabilistische Analyse liefert zudem:
Für fast alle Orakel A gilt: $\mathrm{P}^A \neq \mathrm{NP}^A$

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)

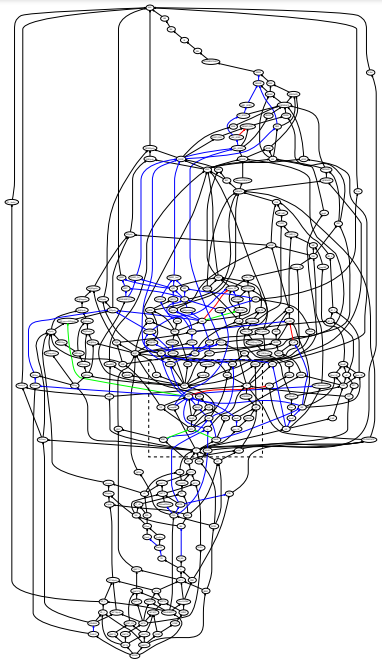
Siehe auch:
Seminar „P vs NP Survival Guide“, Do. 26.7., MZH 5210

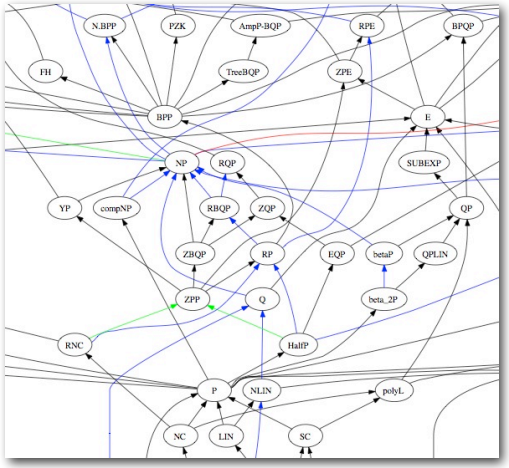
Abschließende Bemerkungen

Mehr Komplexitätsklassen

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/`

(mit interaktivem und statischem Inklusionsdiagramm
als XML bzw. PDF)

Das war's (fast)

Danke für's Teilnehmen! 🙂

Es folgt noch:

- Exkurs: PRIMES $\in$ P
- Nachbesprechung Evaluation
- Besprechung Übungsserie 6 (übermorgen)