

Weder $P = NP$ noch $P \neq NP$ kann mit relativierenden Techniken bewiesen werden

Martin Stigge

7. März 2008



Einführung Relativierung

Relativierung von $P \stackrel{?}{=} NP$

Ein Orakel A für $P^A = NP^A$

Ein Orakel B für $P^B \neq NP^B$

Berechnungsmodell: Orakel-TM

Definition (OTM)

Sei $A \subseteq \Sigma^*$. Eine *Orakel-Turingmaschine* M^A ist eine TM, welche über ein spezielles Frageband Anfragen an die Zugehörigkeit von Wörtern $w \in \Sigma^*$ zum *Orakel* A stellen kann und *in einem Schritt* die Antwort bekommt.

- ▶ Details:
 - ▶ 3 zusätzliche Zustände: $q_?$, q_{yes} und q_{no}
 - ▶ Anfrage $w \in \Sigma^*$ wird auf das Frageband geschrieben, Wechsel nach $q_?$
 - ▶ Im nächsten Schritt ist die TM in q_{yes} falls $w \in A$, andernfalls q_{no}
- ▶ Bemerkung:
 - ▶ Meint man nur die OTM ohne ein spezielles Orakel, schreibt man auch $M^?$.

Relativierte Sprachklassen

Definition

Sei $A \subseteq \Sigma^*$ eine Sprache und \mathcal{C} eine Komplexitätsklasse.

$$\mathcal{C}^A := \{L \subseteq \Sigma^* \mid L \text{ wird von einer } \mathcal{C}\text{-TM mit Orakel } A \text{ erkannt}\}$$

Beispiel

P^A ist die Klasse der Sprachen, die von OTMs erkannt werden, die

1. deterministisch sind,
2. polynomiell beschränkte Laufzeit haben, und
3. A als Orakel benutzen.

Analog NP^A für nichtdeterministische OTMs.

Bedeutung von Relativierung

- ▶ Diese OTMs können als erweitertes Berechnungsmodell betrachtet werden:
 - ▶ Wie normale Turingmaschine,
 - ▶ nur mit zusätzlicher Fähigkeit (Orakel-Entscheidungen)
- ▶ Klassische Beweismethoden *relativieren*, d.h. sie gelten unverändert auch *relativ zu* beliebigen Orakeln.

Beispiel

- ▶ Das *spezielle Halteproblem* $K := \{x \mid M_x(x) \text{ hält}\}$ ist unentscheidbar (durch Turingmaschinen)
- ▶ Beweist man durch *Diagonalisierung*
- ▶ Dieser Beweis relativiert (d.h. funktioniert auch mit OTMs)
- ▶ Also ist $K_A := \{x \mid M_x^A(x) \text{ hält}\}$ auch für jedes A unentscheidbar (durch Orakel-Turingmaschinen mit Orakel A)

Bedeutung von Relativierung: Die Intuition dazu

- ▶ Damit gilt also umgekehrt:
 - ▶ Falls ein Problem in der „normalen Welt“ schwer ist, kann man es in der „relativierten Welt“ betrachten.
 - ▶ Gilt es dort, ist dies zunächst ein *Indiz*, dass es auch in der „normalen Welt“ gelten könnte
 - ▶ Gilt nämlich das Gegenteil in der „normalen Welt“, dürfte der Beweis dafür *nicht relativieren*
- ▶ Die $P \stackrel{?}{=} NP$ Frage ist so ein schweres Problem.

Relativierung von $P \stackrel{?}{=} NP$

- ▶ Werden nun zeigen: Es gibt Orakel $A \subseteq \Sigma^*$ und $B \subseteq \Sigma^*$ mit:
 - ▶ $P^A = NP^A$ und
 - ▶ $P^B \neq NP^B$.
- ▶ Geben also zwei „relativierte Welten“ an, in denen die $P \stackrel{?}{=} NP$ Frage *verschiedene Antworten* hat.
- ▶ Damit kann es weder für $P = NP$ noch für $P \neq NP$ einen relativierenden Beweis geben.

Ein Orakel A für $P^A = NP^A$

- ▶ Wir wählen A als beliebige $PSPACE$ -vollständige Sprache
- ▶ Z.B. das SPACE BOUNDED HALTING PROBLEM ($SBHP$),
oder QUANTIFIED SATISFIABILITY ($QSAT$ bzw. $TQBF$)
- ▶ Dann gilt:

$$PSPACE \subseteq P^A \subseteq NP^A \subseteq NPSPACE \subseteq PSPACE$$

Schritt für Schritt:

- ▶ $PSPACE \subseteq P^A$ (denn A ist $PSPACE$ -vollständig)
 - ▶ $P^A \subseteq NP^A$ (denn $P \subseteq NP$ relativiert)
 - ▶ $NP^A \subseteq NPSPACE$ (simuliere NP -TM und $PSPACE$ Orakel)
 - ▶ $NPSPACE \subseteq PSPACE$ (Savitch's Theorem)
- ▶ Also sind alle Mengen gleich, insbesondere $P^A = NP^A$.

Ein Orakel B für $P^B \neq NP^B$

- ▶ $P^B \subseteq NP^B$ gilt ohnehin, gelten soll also: $NP^B \setminus P^B \neq \emptyset$
- ▶ Es soll also ein $L \in NP^B$ geben mit $L \notin P^B$.
- ▶ Wir werden B derart konstruieren, dass L so aussieht:

$$L = \{0^n \mid \exists x \in B : |x| = n\}$$

- ▶ Offenbar ist $L \in NP^B$. (Rate passendes x und frage $x \stackrel{?}{\in} B$.)
- ▶ Offen: Konstruktion von B derart, dass $L \notin P^B$.
- ▶ Idee: Diagonalisierung (über alle P -OTM $M_i^?$, $i \in \mathbb{N}$)

Bemerkungen

- ▶ Wahl der Funktion $f : i \mapsto i^{\log i}$:
 - ▶ Steigt stärker als jedes Polynom: $f \in n^{\omega(1)}$
(Damit jede polynomielle Zeitschranke überschritten wird.)
 - ▶ Summe steigt schwächer als exponentiell: $\sum_{i=1}^n f(i) \in 2^{o(n)}$
(Damit die Ausnahmemenge X „klein“ bleibt.)
- ▶ Für „fast alle“ Sprachen B gilt $P^B \neq NP^B$:

$$\Pr_B[P^B \neq NP^B] = 1$$

- ▶ Dass $P \neq NP$ (also die allgemeine Vermutung?) nicht relativiert, wurde bereits durch den ersten Teil ($\exists A : P^A = NP^A$ gezeigt)

Zusammenfassung

- ▶ Relativierung
 - ▶ Definiert über Orakel-Turingmaschinen
 - ▶ „Mächtigeres“ Berechnungsmodell als anderer Blickwinkel
- ▶ Orakel A für $P^A = NP^A$
 - ▶ A als $PSPACE$ -vollständig wählen
 - ▶ (Kollabiert damit nicht nur NP auf P sondern sogar alle Klassen zwischen P und $PSPACE$.)
- ▶ Orakel B für $P^B \neq NP^B$
 - ▶ Via Diagonalisierung, sodass keine P -DOTM L entscheidet