Seminar Komplexität und Kryptologie

Hürden zum Lösen des P-NP-Problems

Johannes Köbler Sebastian Kuhnert

Sommersemester 2008

Termin: Mittwoch 11:00 - 13:00, RUD 26, 1'303

Inhalt des Seminars

Das P-NP-Problem ist eine der größten offenen Fragen der Theoretischen Informatik: Über mehrere Jahrzehnte ist es nicht gelungen, einen Beweis für die Gleichheit oder die Ungleichheit dieser beiden Komplexitätsklassen zu finden.

In letzter Zeit konnten aber einige Hürden ausfindig gemacht werden, die solchen Beweisen entgegenstehen: Sie dürfen weder *natürlich* sein, noch *relativieren* oder *algebrieren*. In diesem Seminar werden wir uns mit den Konzepten beschäftigen, die sich hinter diesen Begriffen verbergen. Außerdem werden Techniken vorgestellt, mit denen zumindest manche dieser Hürden überwunden werden können.

Ablauf

- 16.4.: Vorstellung und Vergabe der Themen
- 23.4.: **Einführung** in die Konzepte der Komplexitätstheorie, mit denen wir in diesem Seminar arbeiten werden
  - Grundlagen, insbesondere für die, die noch nicht *Komplexitätstheorie* gehört haben
  - Kurze Wiederholung von Zeit- und Platzklassen
  - Reduktionen
  - Orakel-Turingmaschinen
  - Boolesche und arithmetische Schaltkreise
- Im Lauf des Semesters: Gegenseitiges Vorstellen von Themen in **Referaten**
  - Themen siehe unten
  - Einerseits anschaulich: Einführung und Einordnung des Themas
  - Andererseits präzise: Definitionen und Beweise
  - Ob mit Beamer oder mit Tafel ist egal
  - Zeitlicher Rahmen: Jeweils 90 Minuten, Zeit für Rückfragen einplanen
- **Anwesenheit**: Das eigene Referat ist nur ein Teil dessen, was gelernt wird
  - Nicht mehr als 2mal unentschuldigt fehlen
  - Ihr wollt euer Referat auch nicht vor einem leeren Raum halten
- Nach den Referaten: Schriftliche **Ausarbeitungen**
  - Ziel: Unser im Seminar gesammeltes Wissen zusammenfassen
  - Können auf der Website veröffentlicht werden
  - Umfang: ca. 10-20 Seiten

Themen für Referate

Grundlegende Themen:

- Weder $\mathsf{P} = \mathsf{NP}$ noch $\mathsf{P} \neq \mathsf{NP}$ kann mit relativierenden Techniken bewiesen werden
  - Was bedeutet Relativierung? Warum beschäftigen wir uns damit?
  - $\exists A \subseteq \Sigma^* : \mathsf{P}^A = \mathsf{NP}^A$
  - $\exists B \subseteq \Sigma^* : \mathsf{P}^B \neq \mathsf{NP}^B$
  - Quellen: [Pap95, Kapitel 14.3], [BGS75]
- $\mathsf{IP} = \mathsf{PSPACE}$: Ein nicht-relativierender Beweis
  - Was sind interaktive Beweise? Warum ist IP interessant?
  - $\mathsf{IP} \subseteq \mathsf{PSPACE}$, $\mathsf{PSPACE} \subseteq \mathsf{IP}$
  - Welche nicht-relativierenden Techniken werden verwendet?
  - Quellen: [She92], [DK00, Kapitel 10.1], [AB07, Kapitel 8.5], [FS88]
- Weder $\mathsf{P} = \mathsf{NP}$ noch $\mathsf{P} \neq \mathsf{NP}$ kann mit algebrierenden Techniken bewiesen werden
  - Wie kann man boolesche Schaltkreise zu arithmetischen erweitern?
  - Was bedeutet es, dass eine Inklusion oder nicht-Inklusion algebriert?
  - $\exists A \subseteq \Sigma^* : \exists \tilde{A} : \mathsf{NP}^{\tilde{A}} \subseteq \mathsf{P}^A$
  - $\exists B \subseteq \Sigma^* : \exists \tilde{B} : \mathsf{NP}^B \not\subseteq \mathsf{P}^{\tilde{B}}$
  - Quellen: [AW08, insbes. Abschnitte 1, 2, 5.1]
- $\mathsf{IP} = \mathsf{PSPACE}$ algebriert – wie viele andere Beweise
  - $\forall A \subseteq \Sigma^* : \forall \tilde{A} : \mathsf{PSPACE}^{A[\mathrm{poly}]} \subseteq \mathsf{IP}^{\tilde{A}}$
  - Quellen: [AW08, Abschnitte 1–3]

Weiterführende Themen:

- Arthur-Merlin Games: Varianten von interaktiven Beweissystemen
  - Wie sind die Sprachklassen $\mathsf{AM}[k]$, $\mathsf{MA}[k]$ und AM definiert?
  - $\mathsf{AM} = \mathsf{AM}[2]$
  - $\mathsf{AM} = \mathsf{IP}$
  - Quellen: [DK00, Kapitel 10]
- $\mathsf{NP} \not\subseteq \mathsf{P}/\mathrm{poly}$ kann nicht mit natürlichen Beweisen gezeigt werden
  - Was sind untere Schranken für Schaltkreise? Warum sind sie interessant?
  - Wie ist *natürlicher Beweis* definiert?
  - Satz: Wenn 2^{n^ϵ}-harte Funktionen existieren, gibt es keinen natürlichen Beweis für $\mathsf{P}/\mathrm{poly} \not\subseteq \mathsf{NP}$
  - Quellen: [RR97], [AB07, Kapitel 22]
- Zero Knowledge Proofs: Ein Kandidat für nicht-algebrierende Techniken?
  - Was sind Zero Knowledge Proofs? Welche Bedeutung haben sie in der Kryptographie?
  - Mit welchen Einschränkungen können sie als algebrierend betrachtet werden?
  - Quellen: [AB07, Kapitel 10], [Gol01, Kapitel 4], [AW08, Abschnitt 8], [Gol07, Kapitel 9.2]

Literatur

[AB07] Sanjeev Arora and Boaz Barak. *Complexity Theory: A Modern Approach*. Web draft. Princeton University, 2007. URL: `http://www.cs.princeton.edu/theory/complexity/` (visited on Feb. 29, 2008).

[AW08] Scott Aaronson and Avi Wigderson. 'Algebrization: A New Barrier in Complexity Theory'. In: *Electronic Colloquium on Computational Complexity*, TR08-005 (Feb. 2008). ISSN: 1433-8092. URL: `http://eccc.hpi-web.de/eccc-reports/2008/TR08-005/`.

[BGS75] Theodore Baker, John Gill, and Robert Solovay. 'Relativizations of the $\mathsf{P} =? \mathsf{NP}$ Question'. In: *SIAM Journal on Computing* 4.4 (Dec. 1975). Pp. 431–442. ISSN: 0097-5397. DOI: `10.1137/0204037`.

[Coo06] Stephen Cook. 'The P versus NP Problem'. In: *The Millennium Prize Problems*. Clay Mathematics Institute and American Mathematical Society, 2006. Pp. 87–106. ISBN: 0-8218-3679-X. URL: `http://www.claymath.org/millennium/P_vs_NP/pvsnp.pdf` (visited on Apr. 9, 2008).

[DK00] Ding-Zhu Du und Ker-I Ko. *Theory of Computational Complexity*. New York, NY, USA: John Wiley & Sons, Inc., 2000.

[FS88] Lance Fortnow and Michael Sipser. 'Are There Interactive Protocols for co-NP Languages?'. In: *Information Processing Letters* 28.5 (Oct. 1988). Pp. 249–251. ISSN: 0020-0190. URL: `http://people.cs.uchicago.edu/~fortnow/papers/conpipl.ps` (visited on Feb. 29, 2008).

[Gol01] Obed E. Goldreich. *Foundations of Cryptography*. Vol. 1: Basic Tools. Cambridge University Press, 2001. ISBN: 0-521-79172-3.

[Gol07] Obed Goldreich. *Complexity Theory: A Conceptual Perspective*. Draft – to appear May 2008 at Cambridge University Press. Rehovot, Israel: Weizmann Institute, 2007. URL: `http://www.wisdom.weizmann.ac.il/~oded/cc-drafts.html` (visited on Mar. 6, 2008).

[Pap95] Christos H. Papadimitriou. *Computational Complexity*. Reading, Mass.: Addison-Wesley, 1995. ISBN: 0-201-53082-1.

[RR97] Alexander A. Razborov and Steven Rudich. 'Natural Proofs'. In: *Journal of Computer and System Sciences* 55 (1 1997). Pp. 24–35. ISSN: 0022-0000. DOI: `10.1006/jcss.1997.1494`.

[She92] Alexander Shen. '$\mathsf{IP} = \mathsf{PSPACE}$: Simplified Proof'. In: *Journal of the ACM* 39.4 (Oct. 1992). Pp. 878–880. ISSN: 0004-5411. DOI: `10.1145/146585.146613`.