Seminar Komplexität und Kryptologie

Hürden zum Lösen des P-NP-Problems

Johannes Köbler Sebastian Kuhnert

Sommersemester 2008

Termin: Mittwoch 13:00 - 15:00, 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.

Themen für Referate

Grundlegende Themen:

- Weder $\mathsf{P} = \mathsf{NP}$ noch $\mathsf{P} \neq \mathsf{NP}$ kann mit relativierenden Techniken bewiesen werden
  Quellen: [Pap95, Kapitel 14.3]
- $\mathsf{IP} = \mathsf{PSPACE}$: Ein nicht-relativierender Beweis
  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
  Quellen: [AW08, insbes. Abschnitte 1, 2, 5.1]
- $\mathsf{IP} = \mathsf{PSPACE}$ algebriert – wie viele andere Beweise
  Quellen: [AW08, Abschnitte 1–3]

Weiterführende Themen:

- Arthur-Merlin Games: Varianten von interaktiven Beweissystemen
  Quellen: [DK00, Kapitel 10]
- Weder $\mathsf{P} = \mathsf{NP}$ noch $\mathsf{P} \neq \mathsf{NP}$ kann mit natürlichen Beweisen gezeigt werden
  Quellen: [RR97]
- Zero Knowledge Proofs: Ein Kandidat für nicht-algebrierende Techniken?
  Quellen: [AB07, Kapitel 10], [Gol01, Kapitel 4], [AW08, Abschnitt 8]

Literatur

[AB07] Arora, Sanjeev, und Boaz Barak. *Complexity Theory: A Modern Approach*. Web draft. Princeton University, 2007. URL: `http://www.cs.princeton.edu/theory/complexity/` (besucht am 29. 02. 2008).

[AW08] Aaronson, Scott, und Avi Wigderson. »Algebrization: A New Barrier in Complexity Theory«. In: *Electronic Colloquium on Computational Complexity* (5 2008). ISSN 1433-8092. URL: `http://eccc.hpi-web.de/eccc-reports/2008/TR08-005/`.

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

[FS88] Fortnow, Lance, und Michael Sipser. »Are There Interactive Protocols for co-NP Languages?«. In: *Information Processing Letters* 28.5 (Okt. 1988). 249–251. ISSN 0020-0190. URL: `http://people.cs.uchicago.edu/~fortnow/papers/conpipl.ps` (besucht am 29. 02. 2008).

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

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

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

[She92] Shen, Alexander. »IP = PSPACE: Simplified Proof«. In: *Journal of the ACM* 39.4 (Okt. 1992). 878–880. ISSN 0004-5411. DOI: `10.1145/146585.146613`.

[Zoo] *Complexity Zoo*. URL: `http://www.complexityzoo.com/` (besucht am 29. 02. 2008).