Seminar Interaktives Beweisen

Prof. Johannes Köbler Sebastian Kuhnert

Sommersemester 2009

Normalerweise versteht man unter einem Beweis etwas statisches: Man kann ihn einmal aufschreiben und er bleibt in dieser Form unverändert gültig. In diesem Seminar betrachten wir eine Erweiterung dieses Prinzips: Zwei Akteure, der *Beweiser* und der *Überprüfer*, tauschen Nachrichten aus. Dabei möchte der Beweiser den Überprüfer von der Gültigkeit einer Aussage überzeugen, und der Überprüfer möchte nur Beweise für wahre Aussagen akzeptieren. In der Komplexitätstheorie sind in letzter Zeit zahlreiche Aussagen bewiesen worden, in denen interaktive Beweissysteme eine zentrale Rolle spielen.

Ein interessanter Spezialfall von interaktiven Beweisen sind die *zero knowledge proofs*, bei denen der Überprüfer durch die Interaktion mit dem Beweiser keine zusätzliche Information über die zu beweisende Aussage bekommt, sondern nur ihre Gültigkeit. Dies ermöglicht interessante Anwendungen in der Kryptographie.

Themen für Referate

1. **Interaktive Beweissysteme**

   Inhalt: Wie können interaktive Beweissysteme formal definiert werden?
   Worin liegt ihre Stärke?
   Warum gilt $\mathsf{IP} = \mathsf{PSPACE}$?

   Literatur: [Gol08, Kapitel 9.1]; ergänzend: [DK00, Kapitel 10.5]

2. **Arthur Merlin Games** *(2 Teile)*

   Inhalt: Was sind Arthur-Merlin-Spiele?
   Warum gilt $\mathsf{IP} = \mathsf{AM}[\mathrm{poly}]$?
   Warum gilt $\mathsf{IP}[\mathrm{const}] = \mathsf{AM}[\mathrm{const}] = \mathsf{AM}[2]$?

   Literatur: [Gol08, Kapitel 9.1.4, Anhang F.2]; ergänzend: [DK00, Kapitel 10.4]

3. **Multi-Prover Beweissysteme**

   Inhalt: Wie verändert sich die Mächtigkeit von interaktiven Beweissystemen, wenn mehrere Beweiser zugelassen werden?
   Warum gilt $\mathsf{MIP} = \mathsf{NEXP}$?

   Literatur: [HO02, Kapitel 6.4], [FRS94]

4. **Zero Knowledge Proofs** *(2 Teile)*

   Inhalt: Wie lässt sich die Zero-Knowledge-Eigenschaft formalisieren?
   Warum gilt 3-Coloring $\in \mathsf{ZK}$?
   Warum gilt $\mathsf{NP} \subseteq \mathsf{ZK}$?

   Literatur: [Gol08, Kapitel 9.2], [Gol01, Kapitel 4.4]

5. **Probabilistically Checkable Proofs**

   Inhalt: Wie können PCP definiert werden?
   Warum gilt $\mathsf{NP} = \mathsf{PCP}(\log n, 1)$?
   Welche Resultate lassen sich für Approximationsprobleme ableiten?

   Literatur: [Gol08, Kapitel 9.3], [AB07, Kapitel 11], [DK00, Kapitel 11]

Ablauf

- In der ersten Woche stellen wir euch die Referatsthemen vor und ihr wählt euer Thema aus. Außerdem geben wir euch Hinweise zur Gestaltung von Referaten und Ausarbeitungen.
- Im Lauf des Semesters haltet ihr **Referate**
  - Die Referate haben das Ziel, dass ihr (a) euch ein Thema erarbeitet, (b) euer Thema den anderen vermittelt, (c) von den Referaten der anderen lernt und (d) Vortragspraxis sammelt.
  - Einerseits sollen eure Referate *anschaulich* sein: Ihr führt die anderen in euer Thema ein. Bitte setzt dabei nicht mehr voraus, als sie schon wissen. Mit Beispielen und Bildern könnt ihr euren Zuhörern das Verstehen erleichtern. Eine gute Richtschnur für gute Erklärungen ist die Frage »Was hat mir selbst geholfen, das zu verstehen?«
  - Andererseits sollen eure Referate auch *präzise* sein: Klare Definitionen und die Details von Konstruktionen und Algorithmen gehören auch dazu.
  - Für euer Referat stehen euch ca. 90 Minuten zur Verfügung. Bitte plant Zeit für Rückfragen ein!
- **Vorbereitung** des eigenen Referats:
  - Ihr arbeitet euch in das Thema ein, indem ihr die angegebene (und ggf. weitere) Literatur lest. Literatur, die es nicht in der Bibliothek oder im Netz gibt, kann bei uns kopiert werden.
  - Vor der Vorbereitung des Vortrags lest ihr am Besten [Tan07, Abschnitt 5] – das lohnt sich auch dann, wenn ihr nicht LaTeX verwendet.
  - Eine Woche vor dem Referat kommt ihr in unsere Sprechstunde, um letzte Verständnisfragen zu stellen und den Ablauf des Referats durchzusprechen.
- Es ist ein zentrales Element eines Seminars, auch von den Referaten der anderen zu lernen. Deshalb solltet ihr möglichst immer **anwesend sein**. Wenn ihr mehr als einmal fehlt, zeigt uns bitte unaufgefordert ein Attest.
- Nach dem Referat fertigt ihr noch eine schriftliche **Ausarbeitung** zu eurem Thema an.
  - Die Ausarbeitungen haben das Ziel, (a) das im Seminar gesammelte Wissen zusammenzufassen, (b) Interessierten einen Einstieg in euer Thema zu ermöglichen und (c) euch die Gelegenheit zu geben, wissenschaftliches Schreiben zu üben (Vorbereitung auf Studien- und Diplomarbeit).
  - Wir werden eure Ausarbeitungen auf der Webseite des Seminars veröffentlichen, wenn ihr damit einverstanden seid.
  - Eure Ausarbeitung sollte ungefähr 10-20 Seiten umfassen.
  - Hinweise zum wissenschaftlichen Schreiben findet ihr unter [Böt06] und [Mit07].

Literatur

[AB07] Sanjeev Arora and Boaz Barak. *Complexity Theory: A Modern Approach*. Web draft. Princeton University, 2007. URL: http://www.cs.princeton.edu/theory/index.php/Compbook/Draft (visited on Mar. 31, 2009).

[Böt06] Martin Böttcher. *Einführung in das wissenschaftliche Arbeiten*. Universität Leipzig. 2006. URL: http://bis.informatik.uni-leipzig.de/de/Lehre/0506/SS/SemASKE/files?get=einfuehrung_in_das_wiss_arbeiten.pdf (besucht am 30. März 2009).

[DK00] Ding-Zhu Du and Ker-I Ko. *Theory of Computational Complexity*. New York: Wiley, 2000. ISBN: 0-471-34506-7.

[FRS94] Lance Fortnow, John Rompel, and Michael Sipser. 'On the power of multi-prover interactive protocols'. In: *Theoretical Computer Science* 134.2 (Nov. 1994), pp. 545–557. ISSN: 0304-3975. DOI: 10.1016/0304-3975(94)90251-8.

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

[Gol07] Oded Goldreich. *Computational Complexity. A Conceptual Perspective*. Draft of [Gol08]. Rehovot, Israel: Weizmann Institute, 2007. URL: http://www.wisdom.weizmann.ac.il/~oded/cc-drafts.html (visited on Apr. 2, 2009).

[Gol08] Oded Goldreich. *Computational Complexity. A Conceptual Perspective*. Draft available online as [Gol07]. New York: Cambridge University Press, 2008. ISBN: 978-0-521-88473-0.

[HO02] Lane A. Hemaspaandra and Mitsunori Ogihara. *The Complexity Theory Companion*. Texts in Theoretical Computer Science. An EACTS Series. Berlin et al.: Springer, 2002. ISBN: 3-540-67419-5.

[Mit07] Roland Mittermair. *Hinweise für korrektes Zitieren*. Institut für Informatik-Systeme, Universität Klagenfurt. 2007. URL: http://www.uni-klu.ac.at/tewi/downloads/Zitierhinweise.pdf (besucht am 30. März 2009).

[Tan07] Till Tantau. *The* BEAMER *class*. Version 3.07. 2007. URL: http://mirror.ctan.org/macros/latex/contrib/beamer/doc/beameruserguide.pdf (visited on Mar. 30, 2009).