Seminar Komplexität und Kryptologie

Prof. Dr. Johannes Köbler Frank Fuhlbrück

Sommersemester 2020

Mi 13:15–14:45, RUD 26, 1'307

In diesem Seminar werden aktuelle Forschungsthemen der Gebiete Komplexitätstheorie und Kryptografie vorgestellt und diskutiert. Hierbei gehen wir auch gern auf Teilnehmerwünsche ein. Vorkenntnisse aus dem Bereich Komplexitätstheorie und Graphalgorithmen sind hilfreich, aber nicht notwendig. Das Seminar eignet sich gut zur Vorbereitung auf Abschlussarbeiten.

In diesem Semester liegt der Schwerpunkt auf *Kryptographie*.

Themen für Referate

Im Seminar sind Vorträge einführenden und vertiefenden Charakters zu folgenden Themenbereichen geplant:

1. **Quanten-DFAs, Quanten-PDAs, Quanten-Grammatiken:** 2 Vorträge

   Inhalt: Grundlegende Konzepte von (endlichen) Automaten mit Quantenzuständen.

   Literatur: https://arxiv.org/abs/quant-ph/9707031

2. **Quanten-TM und die Klasse BQP:** 1-2 Vorträge

   Inhalt:

   Literatur: z.B. https://arxiv.org/abs/quant-ph/0003035 und https://epubs.siam.org/doi/abs/10.1137/S0097539796300921

3. **Härte der Simulation von Quantensystemen:** 1 Vortrag

   Inhalt: Falls ein Orakel zur Wkt.vorhersage in einem bestimmten (s. Paper) Quantensystem existiert, kollabiert die PH.

   Literatur: z.B. https://eccc.weizmann.ac.il/report/2010/170/

4. **Beispiele für kein Speedup:** 1 Vortrag

   Inhalt: Umsetzung eines Quantenalgor. mit klassischen Rechenmodellen.

   Literatur: z.B. https://eccc.weizmann.ac.il/report/2018/128/

5. **Sicherheit von Postquantenkryptografie gegen Quantenzufallsorakel** 2-3 Vorträge

   Inhalt: Sicherheit von kryptografischen Algorithmen wird üblicherweise im Zufallsorakelmodell bewiesen, d.h. ist z.B. eine Hashfunktion Teil eines Systems wird diese im Beweis durch ein Zufallsorakel ersetzt. Um auch gegen die Berechnung dieses Hashfunktion durch Quantencomputer durch den Angreifer abzusichern, wird das normale Zufallsorakelmodell durch ein Modell mit speziellem Zugriff für den Angreifer, das sog. Quantenzufallsorakel ersetzt. Das erste Paper führt in dieses Konzept ein, das zweite zeigt, wie Sicherheit im klassische ZOM auf Sicherheit im QZOM erweitert werden kann, was zu einfacheren Beweisen für die Sicherheit von Postquantenkryptografie führt.

   Literatur: Grundlagen QZOM: https://arxiv.org/abs/1008.0931,
   Beweise mit ZOM statt QZOM: https://eprint.iacr.org/2020/129, Vorstellen der Algorithmen deren Sicherheit im 2. Paper gezeigt wird.

6. **Quantenkryptografie** 1-2 Vorträge

   Inhalt: Im Gegensatz zur Postquantenkryptografie hat nicht nur der Angreifer Zugriff auf Quantencomputer, sondern auch Sender und Empfänger.

   Literatur: Einführung: [NC10, Kapitel 12.6], Quantenmünzwurf: https://arxiv.org/abs/quant-ph/0206088

Quantenfreie Themen

7. **Parametrisierte Komplexität: Cliquen- und Rangweite** ≥ 1 Vortrag

   Inhalt: In der Parametrisierten Komplexitätstheorie misst man den Aufwand (Zeit oder Platz) nicht nur anhand der Eingabelänge sondern zusätzlich mittels eines strukturellen Parameters. Für Graphen sind z.B. der Maximalgrad oder die Baumweite sinnvolle Parameter. Für die Baumweite ist mittlerweile die parametrisierte Komplexität weitreichend erforscht, für viele bekannte Probleme existieren sog. FPT-Algorithmen. Graphen mit beschränkter Baumweite sind allerdings immer dünn (nur $O(n)$ Kanten), sodass Parameter wie die Cliquenweite (äquivalent dazu die Rangweite) betrachtet werden. Interessant sind auch Parameter die ebenfalls dichte Graphen ermöglichen, aber restriktiver sind.

Literatur: aktuell z.B. https://arxiv.org/abs/2001.08122

8. **Suchprobleme und P vs. BPP** ≥ 1 Vortrag

   Inhalt: BPP (mit Zufall) und P (ohne Zufall) sind übliche Formalisierungen der Theorie für »effizient« lösbare Entscheidungsprobleme. Für Suchprobleme (»Finde eine beliebige Clique der Größe k!«, statt »Gibt es eine?«) kann noch feinere Abstufungen hinsichtlich Determinismus machen. Während ein probabilistischer Entscheidungsalgorithmus nur korrekt, indifferent oder falsch antworten kann, kann ein Suchalgorithmus auch verschiedene korrekte Lösungen liefern. Hier werden Konzepte betrachtet, wo genau das eingeschränkt wird.

   Literatur: aktuell z.B. https://eccc.weizmann.ac.il/report/2019/012/

Ablauf

- In der ersten Vorlesungswoche stellen wir euch die Referatsthemen vor und ihr wählt euer Thema aus.
- 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!
  - Nach jedem Referat gibt es eine Feedbackrunde.
- **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 [**TWM13b**] – 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**.
- 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 Abschlussarbeiten).
  - Der Umfang eurer Ausarbeitung soll dem Umfang eures Referats entsprechen. Erfahrungsgemäß ergibt das 10–20 Seiten.
  - Hinweise zum wissenschaftlichen Schreiben findet ihr unter [**Boe06**] und [**Mit07**].
  - Der **Abgabeschluss** für Ausarbeitungen ist der erste Tag der Vorlesungszeit im folgenden Semester.

Literatur

[NC10] Michael A. Nielsen und Isaac L. Chuang. *Quantum Computation and Quantum Information: 10th Anniversary Edition.* Cambridge University Press, 2010.