Quantum Computation Seminar

Prof. Dr. Blömer & Prof. Dr. Gharibian

UNIVERSITÄT PADERBORN
Die Universität der Informationsgesellschaft

Preliminaries

In addition to a solid grasp of linear algebra you should have basic knowledge in at least two of the following areas

- data structures and algorithms
- complexity theory
- quantum computation
- probability theory and stochastics

Overview

- **All meetings are mandatory**
- **General kick-off meeting (today)**
- **Topic choice**
  - Send us your top 3 topics sevag.gharibian@upb.de (ranked order)
  - We distribute the topics
  - You can also swap your topic once with another willing person

- **Introductory Talk**
  - We will give a talk on the style of a scientific paper and how to work with literature.

Overview

- **Topic kick-off Meeting**
  - Meeting with your supervisor.
  - You should have read your assigned topic paper and understood main ideas
  - We discuss your tasks and questions you have

- **Q&A day**
  - We answer all of your questions in a personal meeting

- **Essay Draft**
  - You hand in a "feature complete“ draft of your essay
  - "feature complete", i.e. everything you plan to have in the final essay should be included in this version.
  - This is your chance to get comprehensive feedback on your work.

Overview

- **Talk Slides**
  - We ask you to turn in the slides of your talk (presentation). We will give feedback for this.

- **Talk**
  - You will present your topic for all seminar participants and the supervisors
  - Your talk should last 1h including discussion (plan to talk 40-45 minutes).

- **Essay Final Version**
  - The final version of the essay should incorporate the feedback given for the draft version and your talk.

Topics

UNIVERSITÄT PADERBORN
Die Universität der Informationsgesellschaft

Topics

Quantum cryptography

1. Random oracles in a quantum world (Boneh, Dagdelen, Fischlin, Lehmann, Schaffner, Zhandry)
2. Security of the Fiat-Shamir Transformation in the Quantum Random-Oracle Model (Don, Fehr, Majenz, Schaffner)
3. Non-interactive zero-knowledge proofs in the quantum random oracle model (Unruh)
4. Zero-knowledge against quantum attacks (Watrous)
5. Zero-knowledge for QMA from locally simulatable proofs (Broadbent, Grilo)

Topics

Quantum Algorithms

5. Quantum singular value transformation and beyond: exponential improvements for quantum matrix arithmetics (Gilyen, Su, Low, Wiebe)

6. Quadratic speedup for finding marked vertices by quantum walks (Ambainis, Gilyen, Jeffery, Kokainis)

Topics

Quantum complexity theory

7. On the limits of nonapproximability of lattice problems (Goldreich, Goldwasser)

8. Classical interaction cannot replace a quantum message (Gavinsky)

9. The complexity of stoquastic local Hamiltonian problems (Bravyi, DiVincenzo, Oliveira, Terhal)

10. Stoquastic PCP vs randomness (Aharonov, Grilo)

11.StoqMA vs MA: the power of error reduction (Aharonov, Grilo, Liu)

Topics

Quantum information

11. Certified randomness expansion (Vazirani, Vidick)

Dates

Time table

PADERBORN UNIVERSITY

Deadlines/Dates	What
12.11.2020	send top 3 topics and preferred slot
19.11.2020	assignment of topics
26.11.2020	exchange topic with willing students and inform us
Individual meetings with supervisor (latest 19.12.2020)	topic kick-off meeting (private meeting 1)
TBA	introductory talk (by instructors)
TBA	Q&A day (private meeting 2)
20.1.2021	first slot for talk
21.01.2021	second slot for talk
TBA	essay draft
TBA	deadline: essay final version

Other notes

Communication

- Likely to be entirely through PAUL
- Check your PAUL messages for BigBlueButton room link and access code

Websites for quantum papers etc

- Arxiv.org (go to quant-ph)
- Scirate (an arxiv overlay where people vote on papers)
- QIP websites (flagship annual theoretical quantum computation conference, eg QIP 2020)

Questions…

UNIVERSITÄT PADERBORN
Die Universität der Informationsgesellschaft