Karlsruhe Institute of Technology

KARLSRUHE INSTITUTE OF TECHNOLOGY
Institute of Theoretical Informatics
Lehrstuhl Prof. Dr. J. Müller-Quade
Seminar *Quantum Information Theory*

Preliminary Seminar Program

(subject to change)

Quantum Information Theory

Proseminar

Topic 1: Deutsch-Josza Algorithm

The Deutsch-Josza algorithm from 1992 (early version by Deutsch alone in 1985) was one of the very first quantum algorithms that outperforms classical algorithms. It solves the following problem: Decide if a black box function $f : \{0,1\}^n \to \{0,1\}$ is constant or balanced, i.e. if either all values are mapped to the same value or if half of the inputs are mapped to 0 and half to 1.
Whereas a classical computer requires worst case $2^{n-1}+1$ queries, an updated version of [4] only needs one and thus demonstrates exponential speedup.
Although this decision problem is of little relevance in practice, this algorithm is conceptually very interesting. In particular, it is well-suited to show how quantum gates are used to implement algorithms for a quantum computer.
The student should explain the algorithm's setup, go through the steps as matrix-vector multiplications and try to convey an intuition why the Deutsch-Josza algorithm works in one step.

[4] D. Deutsch and R. Jozsa. "Rapid solution of problems by quantum computation". In: *Proceedings of the Royal Society of London. Series A: Mathematical and Physical Sciences* 439 (1992), pp. 553–558

Topic 2: Simon's Algorithm

Simon's algorithm [13] is a quantum algorithm that solves a problem exponentially faster than its classical counterpart. While the original problem may be of little importance, the algorithm now has many applications in the area of (symmetric) cryptanalysis in a model comprising quantum access to a decryption oracle. Moreover, Simon's problem yields an oracle separation between the quantum complexity class BQP and its classical relative BPP, suggesting that quantum computers can indeed outperform classical computation.

The student is expected to explain Simon's problem, comprehensively present the working of Simon's algorithm and discuss its complexity as well as its implications regarding the difference between classical and qantum computation. The presentation should show a rigorous formal treatment as well as be easily understandable and tailored to the prior knowledge and capabilities of the audience.

[13] Daniel R. Simon. "On the Power of Quantum Computation". In: *SIAM J. Comput.* 26.5 (Oct. 1997), pp. 1474–1483. ISSN: 0097-5397. DOI: 10.1137/S0097539796298637. URL: https://doi.org/10.1137/S0097539796298637

Topic 3: Pebbling Games: Quantum Memory Management

In a nutshell, Landauer's principle states that any irreversible manipulation of information dissipates heat and thus increases the entropy of the system. In quantum information theory, one is only concerned with an idealized model, i.e. a complex vector space, that is perfectly isolated. As a result, any (*valid*) transformation on the state space representing qubits and their evolution must be reversible.

However, many classical operations are inherently reversible, for example a simple *AND* and gate that takes as input 2 states and outputs a single state. This topic is concerned with the problem of transforming non-reversible operations into reversible ones, in particular, with the resulting trade-off in time and space [2].

The student is expected to explain the concept of pebbling games and how they related to reversible computation. The topic may be expanded towards researching the impact of translating classical algorithm into the quantum setting.

[2] Charles H. Bennett. "Time/Space Trade-Offs for Reversible Computation". In: *SIAM J. Comput.* 18.4 (1989), pp. 766–776. DOI: 10.1137/0218053. URL: https://doi.org/10.1137/0218053

[7] Balagopal Komarath, Jayalal Sarma, and Saurabh Sawlani. "Pebbling meets coloring: Reversible pebble game on trees". In: *J. Comput. Syst. Sci.* 91 (2018), pp. 33–41. DOI: 10.1016/j.jcss.2017.07.009. URL: https://doi.org/10.1016/j.jcss.2017.07.009

Seminar

Topic 4: Grover's Algorithm

The algorithm of Grover [5] allows—among other applications—to find a date in an unstructured database with a quadratic speedup compared to classical algorithms. Despite being comparatively simple and easy to implement, Grover's algorithm has a large impact on cryptography, in particular regarding the key lengths of symmetric cryptography.

The student is expected to explain the problem and algorithm in detail. Furthermore the student is asked to demonstrate a simple attack on a cryptosystem using Grover's algorithm. The presentation should show a rigorous formal treatment as well as be easily understandable and tailored to the prior knowledge and capabilities of the audience.

[5] Lov K. Grover. “A fast quantum mechanical algorithm for database search”. In: *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing - STOC ’96* (1996). DOI: 10.1145/237814.237866. URL: http://dx.doi.org/10.1145/237814.237866

Topic 5: Superposition Attacks (Simon + Grover)

While Simon’s algorithm allows to solve Simon’s problem in polynomial time—which is thought to require exponential effort in the classical setting—Grover’s algorithm provides at least a quadratic speedup compared to classical algorithms. In settings with quantum oracle access both algorithms have been used to construct a number of superposition attacks against symmetric cryptographic primitives. For example (see [8]) to show that whitening keys do not add additional security in the setting of quantum computers.

The student is asked to present an overview of known superposition attacks derived from Simon’s and Grover’s algorithm as well as to explain selected instructive attacks in more detail. The inner workings of the algorithms of Simon and Grover are covered ealier and may therefore be used black-box in this topic. The presentation should show a rigorous formal treatment as well as be easily understandable and tailored to the prior knowledge and capabilities of the audience.

- [8] Gregor Leander and Alexander May. “Grover Meets Simon – Quantumly Attacking the FX-construction”. In: Nov. 2017, pp. 161–178. ISBN: 978-3-319-70696-2. DOI: 10.1007/978-3-319-70697-9_6
- [11] Thomas Santoli and Christian Schaffner. *Using Simon’s Algorithm to Attack Symmetric-Key Cryptographic Primitives*. 2016. arXiv: 1603.07856 [quant-ph]

Topic 6: Shor’s Algorithm

The famous algorithm of Shor [12] allows to factor integers and find discrete logarithms in quantum polynomial time. The algorithm is based on Simon’s algorithm, however, extends the work to the domain of integers.

The student is expected to explain the algorithm for integer factorization in an easily understandable fashion. Moreover, the implications for cryptography and potential “countermeasures” (e.g. post-quantum RSA) should be reviewed.

[12] P. W. Shor. “Algorithms for Quantum Computation: Discrete Logarithms and Factoring”. In: *Proceedings of the 35th Annual Symposium on Foundations of Computer Science*. SFCS ’94. USA: IEEE Computer Society, 1994, pp. 124–134. ISBN: 0818665807. DOI: 10.1109/SFCS.1994.365700. URL: https://doi.org/10.1109/SFCS.1994.365700

Topic 7: Quantum Error Correction

Error correcting codes are a key enabler for modern computer hardware to mitigate bit flips occurring in the transistors of memory and cpu alike. These codes are usually embedded

into the hardware and as such not a concern for that software developers and users. More importantly, modern error correcting codes are sophisticated enough such that the process in question does have a significant impact on the complexity of a program.

In quantum computing the situation is similar: The idealized quantum circuit model assumes that fault-tolerant arbitrary gates can be applied and qubits can be used. However, when considering the actual cost of a quantum computation the error correction step is a lot more expensive.

In this topic the student is expected to introduce quantum error correcting codes [6, Section IV] [10] and explain and visualize the inner working of some in more detail.

[6] N. Cody Jones et al. “Layered Architecture for Quantum Computing”. In: *Physical Review X* 2.3 (July 2012). ISSN: 2160-3308. DOI: 10.1103/physrevx.2.031007. URL: http://dx.doi.org/10.1103/PhysRevX.2.031007

[10] Michael A. Nielsen and Isaac L. Chuang. “Quantum error-correction”. In: *Quantum Computation and Quantum Information: 10th Anniversary Edition*. Cambridge University Press, 2010, pp. 425–499. DOI: 10.1017/CBO9780511976667.014

Topic 8: Fault-tolerant Quantum Computing

Fault-tolerant quantum aims to formalize the obstacles of applying quantum gates in a fault-tolerant way and to keep qubits coherent using hardware and error correcting measures. In [6], the authors introduce a layered architecture for quantum computers, comprising five levels: The physical and virtual layers implementing and providing hardware interfaces. The third layer is the quantum error correction providing fault-tolerant qubits and *some* quantum gates, the logical layer providing a universal gate set and the application layer.

The student is expected to introduce the layers in more detail. The focus of the work should be on the quantum error correction and the logical layer, in particular magic state distillation to provide a universal gate set.l.

[6] N. Cody Jones et al. “Layered Architecture for Quantum Computing”. In: *Physical Review X* 2.3 (July 2012). ISSN: 2160-3308. DOI: 10.1103/physrevx.2.031007. URL: http://dx.doi.org/10.1103/PhysRevX.2.031007

Topic 9: Quantum Walks

Quantum Walks are the quantum equivalent of random walks, hence a discrete time quantization of Markov chains. However, quantum walks generally behave different than classical random walks, allowing them to speed up search procedures.

The student should introduce the basic model of discrete quantum walks and survey potential applications, for example to review the Grover algorithm on a graph structure [1]. For the graph structures, the student should compare quantum to classical results and present respective properties of (quantum) stochastic processes.

[1] Andris Ambainis. “QUANTUM WALKS AND THEIR ALGORITHMIC APPLICATIONS”. in: *International Journal of Quantum Information* 1 (Apr. 2004). DOI: 10.1142/S0219749903000383. URL: https://arxiv.org/pdf/quant-ph/0403120.pdf

Topic 10: Quantum Random Oracle Model

The quantum random oracle model is modeled similar to the classical random oracle model, with the one exception that the adversary now has access to a quantum computer. This models the intuition that when replacing the random oracle with a hash function for a real instantiation, a quantum adversary can query the hash function in superposition, thus enabling new attacks that are not possible in the classical random oracle model.

This modeling implies that many of the proof techniques used classically do not work anymore. Thus, existing proofs in the random oracle model have to be adjusted to those shortcomings. The student should introduce the quantum random oracle model and show, to what extend classical tricks such as reprogramming and lazy sampling work against a quantum adversary.

[3] Dan Boneh et al. "Random Oracles in a Quantum World". In: *Advances in Cryptology - ASIACRYPT 2011 - 17th International Conference on the Theory and Application of Cryptology and Information Security, Seoul, South Korea, December 4-8, 2011. Proceedings*. 2011, pp. 41–69. DOI: 10.1007/978-3-642-25385-0_3. URL: https://doi.org/10.1007/978-3-642-25385-0%5C_3

[17] Mark Zhandry. "How to Record Quantum Queries, and Applications to Quantum Indifferentiability". In: *Advances in Cryptology - CRYPTO 2019 - 39th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 18-22, 2019, Proceedings, Part II*. ed. by Alexandra Boldyreva and Daniele Micciancio. Vol. 11693. Lecture Notes in Computer Science. Springer, 2019, pp. 239–268. DOI: 10.1007/978-3-030-26951-7_9. URL: https://doi.org/10.1007/978-3-030-26951-7%5C_9

Topic 11: Quantum rewinding

In many security proofs, especially for proving security of classical zero-knowledge proof systems, rewinding is a core technical tool. Roughly speaking, rewinding means to run an algorithm (namely the adversary), and in case of problems, e.g. a simulation failure, backtrack to an earlier saved state and try again. This technique of rewinding does not carry over to the quantum world: Taking snapshots of states would contradict the no-cloning theorem. Therefore, the question of the existence of zero-knowledge proofs (ZKP) against quantum adversaries is non-trivial.

Watrous [16] shows that rewinding (for zero-knowledge simulation) is possible, if certain properties are satisfied. Building on this, Watrous [16] shows that there are ZKPs against quantum adversaries, and that in fact the classical examples of graph isomorphism, graph 3-colouring and graph hamiltonicity are secure (assuming commitment schemes secure against quantum adversaries).

The student is expected to present the definition of zero-knowledge in the quantum setting, explain Watrous' rewinding, and apply it to an example. Moreover, the rewinding technique should be related to Grover search. The presentation should give rigorous definitions and a proof of the "exact case" of Watrous' rewinding. The general statement and its application to a zero-knowledge protocol for NP should be sketched.

Preparation and presentation of this topic should be coordinated with topic 12.

[16] John Watrous. "Zero-Knowledge against Quantum Attacks". In: *SIAM J. Comput.* 39.1 (2009), pp. 25–58. DOI: 10.1137/060670997. URL: https://doi.org/10.1137/060670997

[9] Keiji Matsumoto. “A simpler proof of zero-knowledge against quantum attacks using Grover’s amplitude amplification”. In: *arXiv e-prints* (2006), quant–ph/0602186. arXiv: quant-ph/0602186. URL: https://arxiv.org/abs/quant-ph/0602186

Topic 12: Zero-knowledge proofs of knowledge

Zero-knowledge proofs of knowledge are a very important type of proof system. In a proof of knowledge, a convincing prover must “know” an NP witness for the statement. Most classical proof system use rewinding to extract such a witness from a successful prover. However, rewinding seems, in general, to be impossible in the quantum setting. Moreover, Watrous’ rewinding is not applicable here, since roughly speaking, Watrous’ rewinding “forgets” everything that was learnt after the rewinding. Thus, it is useless for extracting knowledge. In [14, 15], Unruh describes a technique for constructing a (weak form of) proofs of knowledge in the quantum setting, which works for so-called Σ-protocols with additional properties.

The student is expected to explain the definitions and the algorithm in detail. Moreover, a suitably precise proof sketch and intuition should be given. The presentation should rigorously define the required properties and provide at least a proof sketch.

Preparation and presentation of this topic should be coordinated with topic 11.

[15] Dominique Unruh. “Quantum Proofs of Knowledge”. In: *Advances in Cryptology - EUROCRYPT 2012 - 31st Annual International Conference on the Theory and Applications of Cryptographic Techniques, Cambridge, UK, April 15-19, 2012. Proceedings*. Ed. by David Pointcheval and Thomas Johansson. Vol. 7237. Lecture Notes in Computer Science. Springer, 2012, pp. 135–152. DOI: 10.1007/978-3-642-29011-4_10. URL: https://doi.org/10.1007/978-3-642-29011-4%5C_10