

CS 898 Quantum Complexity Theory

Suggested Presentations

Each student registered in this course is required to give one or more lectures on some topic in quantum complexity theory. (People who attend the course but are not registered are also welcome to give a presentation.) Below is a list of suggested lecture topics, including a short description of the topic presentation and one or more references. For some of the topics listed below, it may not be immediately clear why the references listed have been suggested. Please feel free to ask me for clarifications, or if you have any other questions about the presentations. Also, keep in mind that these are just suggestions—you are free to deviate from the suggestions, or choose a different topic altogether.

1. *Oracle separations in quantum complexity.* Several oracle separations are known in quantum complexity theory. For example, there exist choices of sets $A, B \subseteq \Sigma^*$ such that $\text{NP}^A \not\subseteq \text{BQP}^A$ and $\text{BQP}^B \not\subseteq \text{MA}^B$. Consider doing a short survey of what you think are the most interesting oracle separations in quantum complexity, and discuss one of them in detail.

References:

- E. Bernstein and U. Vazirani. Quantum complexity theory. *SIAM Journal on Computing*, 26(5):1411–1473, 1997.
- C. Bennett, E. Bernstein, G. Brassard, and U. Vazirani. Strengths and weaknesses of quantum computing. *SIAM Journal on Computing*, 26(5):1510–1523, 1997.
- S. Aaronson and Y. Shi. Quantum lower bounds for the collision and the element distinctness problems. *Journal of the ACM*, 51(4):595–605, 2004.

2. *QMA-completeness of the local Hamiltonian problem.* There are several variants of the local Hamiltonian problem that are known to be QMA-complete, with the simplest probably being the 5-local Hamiltonian problem first considered by Kitaev. Consider explaining how this most basic variant is proved to be QMA-complete, and possibly discuss the complexity of one or more of the other variants of this problem.

References:

- J. Kempe, A. Kitaev, and O. Regev. The complexity of the local Hamiltonian problem. *SIAM Journal on Computing*, 35(5):1070–1097, 2006.
- A. Kitaev, A. Shen, and M. Vyalyi. *Classical and Quantum Computation*, volume 47 of *Graduate Studies in Mathematics*. American Mathematical Society, 2002.

3. *The complexity of quantum computing with post-selection.* Scott Aaronson defined a complexity class called PostBQP that represents the problems solvable by efficient quantum computations with post-selection. He proved that $\text{PostBQP} = \text{PP}$, and then used this fact to obtain a simple proof of a classic result of complexity theory, which is that PP is closed under intersection.

References:

- S. Aaronson. Quantum computing, post-selection, and probabilistic polynomial-time. *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Science* 461(2063): 3473, 2005.

4. *Honest-verifier quantum statistical zero-knowledge*. The notion of *zero-knowledge* refers to an interactive proof system in which the verifier cannot extract any knowledge from the prover beyond the validity of the assertion being proved. There are several variants of zero-knowledge, but one of the simplest is *honest verifier statistical zero-knowledge*. This notion has a natural quantum analogue, which gives rise to a complexity class QSZK. There are several known facts about honest-verifier quantum statistical zero-knowledge that parallel known facts about classical honest-verifier statistical zero-knowledge. Consider summarizing known facts about these notions and give details about one that you find interesting.

References:

- J. Watrous. Limits on the power of quantum statistical zero-knowledge. In *Proceedings of the 43rd Annual IEEE Symposium on Foundations of Computer Science*, pages 459–468, 2002.
- A. Sahai and S. Vadhan. A complete problem for statistical zero knowledge. *Journal of the ACM* 50(2): 196–249, 2003.

5. *General-verifier quantum statistical zero-knowledge*. Zero-knowledge is a cryptographically motivated concept, wherein the assumption that verifiers are honest is not well-motivated. In the quantum setting, the general notion of zero-knowledge is particularly sensitive, but it is possible to prove that some interactive proof systems are zero-knowledge against arbitrary quantum verifiers. A presentation on this topic should make clear the definitions used and include a discussion of the quantum techniques involved in proving interactive proofs to be zero-knowledge against quantum verifiers.

References:

- J. Watrous. Zero-knowledge against quantum attacks. *SIAM Journal on Computing* 39(1): 25–58, 2009.
- S. Hallgren, A. Kolla, P. Sen, and S. Zhang. Making Classical Honest Verifier Zero Knowledge Protocols Secure against Quantum Attacks. *Proceedings of the 35th International Colloquium on Automata, Languages and Programming*, volume 5126 of *Lecture Notes in Computer Science*, pages 592–603, 2008.

6. *Equivalence of standard and adiabatic quantum computation*. The so-called *adiabatic* model of quantum computation is known to be equivalent to the usual notion based on quantum circuits. The proof that adiabatic quantum computation can simulate ordinary quantum computation is based on Kitaev’s proof that the local Hamiltonian problem is QMA-complete, so this topic should only be chosen if someone else presents that topic.

References:

- D. Aharonov, W. van Dam, J. Kempe, Z. Landau, S. Lloyd, and O. Regev. Adiabatic quantum computation is equivalent to standard quantum computation. *SIAM Journal on Computing*, 37(1):166–194, 2007.
- W. van Dam, M. Mosca, and U. Vazirani. How powerful is adiabatic quantum computation? *Proceedings of the 42nd Annual IEEE Symposium on Foundations of Computer Science*, pages 279–287, 2001.

7. *Quantum advice*. A quantum advice state is a trusted state supplied to a quantum computation that can depend on the length of the input string to the computation, but is independent of the input aside from its length (so exponentially many input strings must share the same advice state). Some interesting facts are known about quantum advice and the complexity classes

defined by it. For a presentation, consider focusing on just BQP/qpoly and its containment in PP/poly.

References:

- S. Aaronson. Limitations of quantum advice and one-way communication. *Theory of Computing*, 1:1–28, 2005.
- S. Aaronson. QMA/qpoly is contained in PSPACE/poly: de-Merlinizing quantum protocols. In *Proceedings of the 21st Annual IEEE Conference on Computational Complexity*, pages 261–273, 2006.
- S. Aaronson and G. Kuperberg. Quantum versus classical proofs and advice. *Theory of Computing*, 3:129–157, 2007.

8. *Quantum interactive proofs and semidefinite programming*. It was known for about ten years that $\text{QIP} \subseteq \text{EXP}$, and this was recently improved to $\text{QIP} = \text{PSPACE}$. Both of the containments $\text{QIP} \subseteq \text{EXP}$ and $\text{QIP} \subseteq \text{PSPACE}$ make critical use of semidefinite programming. An introduction to semidefinite programming, followed by an explanation of how quantum interactive proof systems are described by semidefinite programs, is a possible presentation topic.

References:

- A. Kitaev and J. Watrous. Parallelization, amplification, and exponential time simulation of quantum interactive proof system. In *Proceedings of the 32nd ACM Symposium on Theory of Computing*, pages 608–617, 2000.
- G. Gutoski and J. Watrous. Toward a general theory of quantum games. *Proceedings of the 39th ACM Symposium on Theory of Computing*, pages 565–574, 2007.
- J. Watrous. Semidefinite programs for completely bounded norms. Manuscript, 2009. Available as arXiv.org e-Print 0901.4709.

9. *Hardness of distinguishing quantum circuits*. Quantum circuits, as we have defined them, implement quantum channels; and one computational problem that one can consider is to determine whether or not two given quantum circuits implement nearly the same channel. This problem is complete for the class QIP (and is therefore PSPACE-complete given that $\text{QIP} = \text{PSPACE}$). A presentation on this topic could summarize the notion of distance between channels based on the *diamond norm* (or *completely bounded trace norm*), and present the main parts of the proof of the above result.

References:

- B. Rosgen and J. Watrous. On the hardness of distinguishing mixed-state quantum computations. In *Proceedings of the 20th Annual Conference on Computational Complexity*, pages 344–354, 2005.

10. *Equivalence of quantum circuits and quantum Turing machines*. The equivalence of the quantum Turing machine model and quantum circuit model was proved by Yao in the paper below. There are, naturally, two main parts of this equivalence: simulating quantum Turing machines with quantum circuits and simulating quantum circuits with Turing machines. A presentation on this topic could cover both directions of the equivalence.

References:

- A. Yao. Quantum circuit complexity. *Proceedings of the 34th Annual IEEE Symposium on Foundations of Computer Science*, pages 352–352, 1993.

11. *Quantum Arthur–Merlin games.* Quantum Arthur–Merlin games, or public-coin quantum interactive proofs, are quantum interactive proofs where the prover (Merlin) can send quantum information to the verifier (Arthur) as normal, but where Arthur’s messages to Merlin can consist only of uniformly generated random bits. For three or more messages, quantum Arthur–Merlin games are equivalent in power to ordinary quantum interactive proof systems, although for two messages this may not be the case. A presentation of quantum Arthur–Merlin games could include a proof of this equivalence for three or more messages, which corresponds to the complexity class equality $QMAM = QIP$. This fact is a helpful first step to proving $QIP = PSPACE$.

References:

- C. Marriott and J. Watrous. Quantum Arthur-Merlin games. *Computational Complexity*, 14(2):122–152, 2005.

12. *Multi-prover quantum interactive proofs.* In complexity-theoretic terms, quantum variants of multi-prover interactive proof systems are poorly understood. This includes multi-prover interactive proofs where the verifier is classical and the provers share entanglement, as well as multi-prover interactive proofs where the verifier and provers are quantum. There are, however, many possible presentation ideas based on the results in the references that follow (as well as several others I have not listed).

References:

- H. Kobayashi and K. Matsumoto. Quantum multi-prover interactive proof systems with limited prior entanglement. *Journal of Computer and System Sciences*, 66(3), 2003.
- J. Kempe, H. Kobayashi, K. Matsumoto, and T. Vidick. Using entanglement in quantum multi-prover interactive proofs. *Proceedings of the 2008 IEEE 23rd Annual Conference on Computational Complexity*, pages 211–222, 2008.
- S. Wehner. Entanglement in interactive proof systems with binary answers. In *Proceedings of the 23rd Annual Symposium on Theoretical Aspects of Computer Science*, volume 3884 of *Lecture Notes in Computer Science*, pages 162–171. Springer, 2006.
- J. Kempe, H. Kobayashi, K. Matsumoto, B. Toner, and T. Vidick. Entangled games are hard to approximate. Available as arXiv.org e-Print 0704.2903, 2007.
- R. Cleve, P. Høyer, B. Toner, and J. Watrous. Consequences and limits of nonlocal strategies. In *Proceedings of the 19th Annual IEEE Conference on Computational Complexity*, pages 236–249, 2004.
- J. Kempe, O. Regev, and B. Toner. Unique Games with Entangled Provers are Easy. *Proceedings of the 49th Annual IEEE Symposium on Foundations of Computer Science*, pages 457–466, 2008.

Other presentation topics include bounded-depth quantum circuits, multiple-Merlin QMA, space-bounded quantum computation, quantum interactive proofs with competing provers, and surely several other topics I have not listed.