CS395T Project

Handed out: Oct. 10, 2016

All students taking CS395T for credit are expected to complete a course project by the end of the semester. The project can be either a survey of some topic in the quantum complexity theory literature, or original research. Projects can be done either individually or in groups of two. Pick a project that interests you, that's at least somewhat related to the course, and that (crucially!) you'll actually be able to finish by the end of the semester. Here are a few good ways to pick a project:

- Something that combines your own research interests with quantum complexity theory
- Something mentioned in the course that you'd like to understand better
- Something *not* mentioned in the course that you wish had been
- scholar.google.com, arxiv.org/find/quant-ph
- The last twenty years' proceedings of ACM Symposium on Theory of Computing (STOC), IEEE Foundations of Computer Science (FOCS), and IEEE Conference on Computational Complexity (CCC), as well as the list of talks at the annual Quantum Information Processing (QIP) conference

To help get you started, there's a list of topic suggestions at the end of this handout. Scott will also be happy to help you with additional suggestions and pointers to the literature. Here is what's expected of you:

1. **Project Proposal.** Just a single paragraph describing your proposed project, together with a list of relevant papers. Please email this to aaronson@cs.utexas.edu by **Wednesday, October 19**. Please indicate if you are collaborating with anyone. Scott will then give you feedback and suggest additional relevant papers. Please don't hesitate to make an appointment to discuss your project in person.
2. **Ten-Minute Class Presentation.** Each project group must give an in-class presentation. We'll probably schedule these presentations during the class sessions of Monday, November 28 and Monday, December 5—more details later. The time allotted to each presentation will depend on how many projects there are and on other factors (such as whether we use one or two class sessions for presentations). You can use blackboard or PowerPoint.
3. **Written Report.** You must turn in a written project report by **Tuesday, December 6**. The report should be up to six pages long, together with optional appendices that can be as long as you like and will be read at Scott's discretion. (No, there are no rules about font size, margins, etc.; just be reasonable!)

Students will also *optionally* be invited to have their project reports featured in a "Project Showcase" on Scott's blog. For the past Project Showcases, see:

- http://www.scottaaronson.com/blog/?p=515
- http://www.scottaaronson.com/blog/?p=1181

- http://www.scottaaronson.com/blog/?p=2109

Actual Projects From Previous Iterations of This Course (some leading to new publishable results)

- A $\mathsf{QMA}(k)$ protocol for $3SAT$ requiring unentangled measurements only
- Quantum Hidden Markov Models
- Simple presentation of the Solovay-Kitaev Theorem
- Universality of measurement-based quantum computing
- Lower bounds on quantum communication complexity
- Stoquastic Hamiltonians (Terhal, Bravyi, et al.)
- Quantum finite automata
- Classical simulation of quantum circuits
- Query-limited reducibilities and quantum computing
- Quantum money relative to a classical oracle
- On the query complexity of counterfeiting quantum money
- Improving success probability for $\mathsf{QMA}(k)$ protocols
- Quantum correlated equilibria
- Superpolynomial quantum speedups for Boolean evaluation trees with hidden structure
- Witness-indistinguishability against quantum adversaries

(Extremely Incomplete) List of Possible Other Topics

- Quantum cellular automata; equivalence with quantum circuits and quantum Turing machines
- Parallel implementation of Shor's algorithm (Cleve and Watrous)
- Quantum Statistical Zero-Knowledge
- $\mathsf{QIP} = \mathsf{QIP}(3) = \mathsf{PSPACE}$
- Quantum query complexity of compositions of Boolean functions (Reichardt)
- Quantum query complexity of graph-theoretic problems
- Quantum walk algorithms (Ambainis, Childs-Goldstone...)
- Real vs. complex numbers in quantum complexity theory
- Valiant's matchgate theorem
- QMA-complete problems
- Complexity issues related to the quantum adiabatic algorithm

- Multi-prover quantum interactive proof systems: parallel repetition, etc.
- Continuous-time quantum query complexity
- Two-way quantum communication complexity (e.g., Razborov's lower bound for Disjointness)
- One-way quantum communication complexity
- Quantum streaming complexity (Le Gall)
- Quantum Lovasz Local Lemma
- Reichardt's span-program characterization of quantum query complexity
- Complexity of quantum field theories (Jordan-Lee-Preskill)
- Certifiable randomness expansion using Bell's inequality
- Quantum computing and the Jones polynomial (Freedman-Kitaev-Larsen-Wang, Aharonov-Jones-Landau)
- The QMA versus QMA_1 problem
- Area laws, and quantifying entanglement in local Hamiltonian solutions
- Quantum t-designs and their applications