

Instructions

2-3 people group projects. You may choose to do a *literature review* project or (more exciting) *original research*. For literature review, you'd read a few papers around a topic, understand the connection of this topic to the general field of quantum computing as well as the of various works under this topic. The final outcome would be a *survey* paper including interesting open problems. For research project, identify clearly a problem (e.g., designing/improving an algorithm for a specific task) and let your *creativity* guide you while maintaining reasonable *precision*! You are not required to completely solve a problem (big congrats if you do!).

Specs

- **Proposal:** 1-2 pages consisting of 1) the topic, background, context, motivation; 2) brief summary of the relevant works and core papers to be studied; and 3) a goal you intend to achieve and a plan.
- **Mid-term report:** ~5 pages. After more reading and group discussion, your mid-term report should have a polished and expanded version of your proposal. You also need to demonstrate the progress you've made since the proposal.
- **Oral presentation:** Each group will have about 20mins to present your project, demonstrating both *breath* and *depth*: you should aim for a clear introduction of your topic with sufficient background and motivation that would **interest** the audience; and then you may choose to explain 1-2 technical ideas in a little detail. Every group member needs to participate, and your group will be graded by other fellow students. You may give your the presentaion on board or with slides.
- **Final report:** ~10 pages. This should resemble a real research paper: a short abstract; 2) an introduction that motivates the topic/problem and gives an overview of the entire paper; 3) details including proper preliminary materials (e.g., notations & defintions), explaining some main technical results; and finally 4) further discussion and open questions.
- **Report Format:** follow the 2017 [ACM Article Template](#) {:target="_blank"} "ACM Small" format. Here is a sample [TeX](#) {:target="_blank"} and its [PDF](#) {:target="_blank"}. MS Word templates and samples are available on [ACM's website](#) {:target="_blank"}.

Timeline

- **Week 1 & 2:** forming groups.
 - **Week 3 & 4:** meeting and discussing project ideas.
 - **April 27:** proposal due.
 - **May 18:** mid-term report due.
 - **Week 10:** in-class presentations.
 - **June 15:** final report due.
-

Suggested Topics

Feel free to pursue a project not on this list. Good venues to look for inspirations: [QIP](#), [Qcrypt](#) and more general TCS conferences (e.g., [STOC](#), [FOCS](#), [Crypto](#)).

Quantum Algorithms

- **General survey** [[CvD10](#)] *Quantum algorithms for algebraic problems* by Andrew M. Childs, Wim van Dam.
- **Non-abelian Hidden subgroup problem** A tough case for HSP, but connected with many interesting problems, e.g., graph isomorphism, and (unique) shortest vector problem critical in lattice-based crypto.

- [EK04] *The quantum query complexity of the hidden subgroup problem is polynomial* by M. Ettinger, P. Høyer, E. Knill.
- [K03] *A subexponential-time quantum algorithm for the dihedral hidden subgroup problem* by G. Kuperberg.
- **(Generalized) hidden shift problem**
 - [vDHI02] *Quantum Algorithms for some Hidden Shift Problems* by W. van Dam, S. Hallgren, and L. Ip. A. Childs and W. van Dam, “Quantum algorithm for a generalized hidden shift problem”.
 - [CvD05] *Quantum algorithm for a generalized hidden shift problem* by A. Childs and W. van Dam.
- **High dimensional continuous abelian HSP.** nice generalization and new formalization of HSP on continuous groups with applications in solving basic number theoretic problems and breaking some lattice crypto.
 - [EHKS14] *A Quantum Algorithm for Computing the Unit Group of an Arbitrary Degree Number Field* by Kirsten Eisenträger, Sean Hallgren, Alexei Kitaev and Fang Song.
 - [BS16] *Efficient quantum algorithms for computing class groups and solving the principal ideal problem in arbitrary degree number fields* by J. Blass and F. Song.
- **Quantum random walk.** An extension of classical random walk to the quantum setting. It has become a framework for quantum algorithm design that usually achieves polynomial speedup.
 - Survey papers
 - * [K03] *Quantum random walks – an introductory overview* by J. Kempe.
 - * [A04] *Quantum walks and their algorithmic applications* by A. Ambainis.
 - * [MNR06] *Search via Quantum Walk* by F. Magniez, A. Nayak, J. Roland, and M. Santha.
 - [HK16] *Efficient quantum walk on the grid with multiple marked elements* by Peter Hoyer, Mojtaba Komeili.
 - **Continuous-time** quantum walk. [C08] *Universal computation by quantum walk* by A. M. Childs.

Quantum simulation related algorithms

Original motivation of quantum computers. They are already meaningful and possible on a “small” quantum computer with say 50 clean qubits. These algorithms have wide applications such as machine learning.

- [HHL09] *Quantum algorithm for solving linear systems of equations* by Aram W. Harrow, Avinandan Hassidim, Seth Lloyd.
- [CKS16] *Quantum linear systems algorithm with exponentially improved dependence on precision* by Andrew M. Childs, Robin Kothari, and Rolando D. Somma.
- [BCK15] *Hamiltonian simulation with nearly optimal dependence on all parameters* by Dominic W. Berry, Andrew M. Childs, and Robin Kothari.
- Application in quantum **machine learning**. ML, of course... but be critical about what you see.
 - A survey. [AW17] *A Survey of Quantum Learning Theory* by S. Arunachalam, R. de Wolf.
 - [KP16] *Quantum Recommendation Systems* by I. Kerenidis, A. Prakash.
- **Quantum supremacy.** Recent advances in physical implementation has brought up the hot topic on demonstrating: on a *small* (special-purpose) quantum device, is there a clear quantum speedup for some task, motivated by the goal of overturning the Extended Church-Turing Thesis as confidently as possible.
 - [AC16] *Complexity-Theoretic Foundations of Quantum Supremacy Experiments* by S. Aaronson and L. Chen.

Quantum Information Theory

- Broad survey on **Quantum entanglement** [HHHH08] *Quantum entanglement* by R. Horodecki, P. Horodecki, M. Horodecki, K. Horodecki.
- **Quantum error correcting.** We only scratch the surface of QECC in class. **Project idea:** a summary of the general error correcting theory and the stabilizer formalism, and discussing a particular

code (e.g. surface code).

- A survey. [B15] *Quantum Error Correction for Quantum Memories* by Barbara M. Terhal.
- [FMMC12] *Surface codes: Towards practical large-scale quantum computation* by Austin G. Fowler, Matteo Mariantoni, John M. Martinis, Andrew N. Cleland.
- **Theory of quantum fault-tolerant computing.** Fault-tolerance is critical for physical implementation of a quantum computer. **Project idea:** a general overview and explaining some of the key components in detail would be suitable for a course project.
 - [ABO99] *Fault-Tolerant Quantum Computation with Constant Error Rate* by D. Aharonov and M. Ben-Or.
 - [G13] *Fault-Tolerant Quantum Computation with Constant Overhead* by Daniel Gottesman.
- **Quantum Shannon theory.** It deals with communicating information via noisy channel. Many surprising and distinct features in the quantum generalization.
 - [BDH+09] *Quantum Reverse Shannon Theorem* by C.H. Bennett et al.
 - [HOW05] *Quantum information can be negative* by M. Horodecki, J. Oppenheim, A. Winter.
 - [SY08] *Quantum Communication With Zero-Capacity Channels* by G. Smith, J. Yard.
- **Quantum information and black holes.**
 - Lecture notes. [A16] *From quantum money to black holes* by S. Aaronson.
 - [HP07] *Black holes as mirrors: quantum information in random subsystems* by Patrick Hayden, John Preskill.
 - [HP13] *Quantum computation vs. firewalls* by D. Harlow and P. Hayden.

Quantum Computational Complexity

There is a large body of research that explores abstractly the power and the limits of quantum computing.

- **General survey** [W09] *Quantum Computational Complexity* by J. Watrous.
- **Quantum interactive proofs**
 - Survey. [VW16] *Quantum Proofs* by Thomas Vidick, John Watrous.
 - [JJUW09] *QIP = PSPACE* by Rahul Jain, Zhengfeng Ji, Sarvagya Upadhyay, John Watrous
 - Verifying a quantum computer classically? [ABOE08] *Interactive Proofs For Quantum Computations* by Dorit Aharonov, Michael Ben-Or, Elad Eban.
- **Non-local games.** Introduced for the purpose of testing quantum theory, it turns out to be far more influential and connects to many areas such as interactive proofs, operator theory, cryptography, etc.
 - [V13] *Three-player entangled XOR games are NP-hard to approximate* by Thomas Vidick.
 - Recent **breakthrough** [S16] *Tsirelson's problem and an embedding theorem for groups arising from non-local games* by William Slofstra.
- **Hamiltonian Complexity** How difficult is it to determine the ground energy of a physical system?
 - [AN02] *Quantum NP - A Survey* by Dorit Aharonov, Tomer Naveh.
 - [GN13] *Quantum 3-SAT is QMA1-complete* by David Gosset, Daniel Nagaj.
 - [LVV13] *A polynomial-time algorithm for the ground state of 1D gapped local Hamiltonians* by Zeph Landau, Umesh Vazirani, Thomas Vidick.

Quantum Query & Communication Complexity

- [MW13] *A Survey of Quantum Property Testing* by Ashley Montanaro, Ronald de Wolf.
- [G01] *Quantum Communication Complexity (A Survey)* by Gilles Brassard.
- **Separations of classical/quantum complexity**
 - [ABDK16] *Separations in query complexity using cheat sheets* by Scott Aaronson, Shalev Ben-David, and Robin Kothari.
 - [ABBD+16] *Separations in communication complexity using cheat sheets and information complexity* by Anurag Anshu et al.
- [ATYY16] *Exponential Separation of Quantum Communication and Classical Information* by Anurag Anshu, Dave Touchette, Penghui Yao, Nengkun Yu.

- **Query lower bound**
 - Polynomial method. [BBCMW98] *Quantum Lower Bounds by Polynomials* by R. Beals et al.
 - Adversarial method. [A00] *Quantum lower bounds by quantum arguments* by Andris Ambainis.
 - [HLS07] *Negative weights make adversaries stronger* P. Hoyer T. Lee, R. Spalek.
 - [R09] *Span programs and quantum query complexity: The general adversary bound is nearly tight for every boolean function* by Ben W. Reichardt.

Quantum and crypto

- **Post-quantum crypto** cope with quantum codebreakers
 - [R04] *Quantum Computation and Lattice Problems* by Oded Regev.
 - [Z12] *How to Construct Quantum Random Functions* by Mark Zhandry.
 - [Z13] *Quantum-Secure Message Authentication Codes* by Dan Boneh and Mark Zhandry.
 - [S14] *A Note on Quantum Security for Post-Quantum Cryptography* by F. Song.
 - [HHS11] *Classical Cryptographic Protocols in a Quantum World* by Sean Hallgren, Adam Smith, Fang Song.
 - [BDF+11] *Random Oracles in a Quantum World*, by Dan Boneh et al.
 - [KLLNP16] *Breaking Symmetric Cryptosystems using Quantum Period Finding* by Marc Kaplan, Gaëtan Leurent, Anthony Leverrier, María Naya-Plasencia.
- **Quantum cryptograpy** equip codemakers with quantum information processing
 - **Survey.** [BS15] *Quantum Cryptography Beyond Quantum Key Distribution* by Anne Broadbent, Christian Schaffner.
 - **QKD** [R05] *Security of Quantum Key Distribution* by Renato Renner.
 - Quantum key exchange a la **Merkle** [BHK+11] *Merkle Puzzles in a Quantum World* by G. Brassard, P. Hoyer, K. Kalach, M. Kaplan, S. Laplante, L. Salvail.
 - [BCG+02] *Authentication of Quantum Messages* by Howard Barnum et al.
 - **Quantum Money** [AC12] *Quantum Money from Hidden Subspaces* by Scott Aaronson, Paul Christiano.
 - **Quantum homomorphic encryption** [DSS16] *Quantum homomorphic encryption for polynomial-sized circuits* by Yfke Dulek, Christian Schaffner, Florian Speelman.
 - [U13] *Revocable quantum timed-release encryption* by Dominique Unruh.
- **Device-independence, randomness amplification** What if your devices for cryptography cannot be trusted (recall what NSA did)? Quantum non-locality enables certified security and a lot many fascinating tasks.
 - [MS14] *Robust protocols for securely expanding randomness and distributing keys using untrusted quantum devices* by Carl A. Miller, Yaoyun Shi.
 - [CSW14] *Physical Randomness Extractors: Generating Random Numbers with Minimal Assumptions* by Kai-Min Chung, Yaoyun Shi, Xiaodi Wu.

Other models of quantum computation

- **Adiabatic quantum computation** [AvDK+04] *Adiabatic Quantum Computation is Equivalent to Standard Quantum Computation* by D. Aharonov et al.
- **Topological quantum computation** [K97] *Fault-tolerant quantum computation by anyons* by A. Yu. Kitaev.
- **Measurement-based** [RB01] *A One-Way Quantum Computer* by Robert Raussendorf and Hans J. Briegel.
- A non-universal model concerning **boson sampling**. [AA11] *The Computational Complexity of Linear Optics* by S. Aaronson and A. Arkhipov.
- Qubit is precious, be conservative. [KL98] *On the Power of One Bit of Quantum Information* by E. Knill, R. Laflamme.

Quantum software and logic

- Universal quantum gates. Quantum computer is digital!
 - Survey. [DN05] *The Solovay-Kitaev algorithm* by Christopher M. Dawson, Michael A. Nielsen.
 - [S03] *Both Toffoli and Controlled-NOT need little help to do universal quantum computation* by Y. Shi.
- [SHT16] *ProjectQ: An Open Source Software Framework for Quantum Computing* by Damian S. Steiger, Thomas Häner, Matthias Troyer. More info. on their project [website](#){:target=“_blank“}.
- [WS14] *LIQUi/>: A Software Design Architecture and Domain-Specific Language for Quantum Computing* by QuArC @ Microsoft Research. [Github](#).
- [GLRSV13] *Quipper: A Scalable Quantum Programming Language* by A. S. Green et al. [Project website](#).
- [PRZ17] *QWIRE: A Core Language for Quantum Circuits* by Jennifer Paykin Robert Rand Steve Zdancewic.
- [YYW17] *Invariants of Quantum Programs: Characterisations and Generation* by M. Ying, S. Ying and X. Wu.

Quantum-inspired proofs for classical theorems

The techniques and formalism in quantum information processing have inspired proofs for mathematical theorems that seem to have nothing to do with Quantum.

- [DW11] *Quantum Proofs for Classical Theorems* by Andrew Drucker, Ronald de Wolf.
- [FMP+11] *_Linear vs. “Semidefinite Extended Formulations: Exponential Separation and Strong Lower Bounds_* by S. Fiorini, S. Massar, S. Pokutta, H. R. Tiwary, R. de Wolf.
- [A11] *A Linear-Optical Proof that the Permanent is #P-Hard* by Scott Aaronson.