Candidate Course Project Topics (CMSC 657)

Xiaodi Wu*

Abstract

This document is meant to provide some useful guideline and references for finding projects in the field of quantum information and computation. The selection is not comprehensive and subject to the author’s personal knowledge on the topics (mistakes are possible). Each topic comes with a brief description and a few representative references.

It is totally fine to pursue project topics beyond this document. However, please do identify your topic and relevant references in your proposal. Please feel free to contact me if you have difficulty identifying a project topic.

Contents

1 Quantum Information & Foundation 2
2 Physics and Quantum Information 3
3 Quantum Algorithms 4
4 Quantum Complexity 6
5 Quantum Cryptography 8
6 Quantum Programming Languages 8
7 Fault-tolerant Quantum Computation 9
8 Near-term Quantum Devices 9
9 Explorative topics 10

*Department of Computer Science, Institute for Advanced Computer Studies, and Joint Center for Quantum Information and Computer Science, University of Maryland, College Park, MD.
1 Quantum Information & Foundation

1. Understanding of quantum time-space and casual structure.

2. Superdense coding of quantum states.

3. Local hidden-variable theories for some entangled states.


5. Quantum data hiding.

6. Unitary t-designs and random Clifford operations.

7. Approximating random states and unitary designs by circuits.


9. Separability and Quantum de Finetti bounds


10. An uncertainty relation when a particle is entangled with a quantum memory.


11. The quantum substate theorem.


2 Physics and Quantum Information

1. Use ideas from quantum information to help improve the experiment design.


2. Quantum information, blackholes, and high energy physics.


3 Quantum Algorithms

1. Quantum random walks.


• A. Ambainis, Quantum walks and their algorithmic applications. arXiv: quant-ph/0403120


2. Quantum algorithm for linear systems and related topics.


• Quantum linear systems algorithm with exponentially improved dependence on precision by Andrew M. Childs, Robin Kothari, Rolando D. Somma, QIP 2016. arXiv:1511.02306


3. Quantum algorithm for data analysis, machine learning and so on.


4. Quantum algorithms for algebraic problems, and relations to cryptography.
• A quantum algorithm for computing the unit group of an arbitrary degree number field by Kirsten Eisentrger, Sean Hallgren, Alexei Kitaev, Fang Song, STOC 2014.
• Efficient quantum algorithms for computing class groups and solving the principal ideal problem in arbitrary degree number fields by Jean-François Biasse, Fang Song, SODA 2016.

5. Span programs and learning graphs.

• Aleksandrs Belovs. Span Programs for Functions with Constant-Sized l-certificates. arXiv:1105.4024

6. Quantum property testing.


7. Quantum algorithms for optimization.


8. A Quantum Approximate Optimization Algorithm

• Edward Farhi, Jeffrey Goldstone, Sam Gutmann. A Quantum Approximate Optimization Algorithm. arXiv:1411.4028
• Edward Farhi, Aram W Harrow. Quantum Supremacy through the Quantum Approximate Optimization Algorithm. arXiv:1602.07674
4 Quantum Complexity

1. The complexity of quantum computing with post-selection.

2. Equivalence of quantum circuits and quantum Turing machines.


4. Quantum interactive proof systems.
   • Succinct quantum proofs for properties of finite groups by J. Watrous. arXiv: cs.CC/0009002
   • PSPACE has 2-round quantum interactive proof systems by J. Watrous. arXiv:cs.CC/9901015


6. QMA(2)
• H. Blier and A. Tapp. All languages in NP have very short quantum proofs. arXiv:0709.0738.

7. Quantum proofs and advices.

8. Quantum computational learning theory.
• Scott Aaronson. Shadow Tomography of Quantum States. arXiv:1711.01053


10. Using the mathematics of quantum information to prove theorems.
• S. Aaronson. ”A Linear-Optical Proof that the Permanent is #P-Hard”. arXiv:1109.1674.
5 Quantum Cryptography

1. Device-independent quantum cryptography.
   - B.W. Reichardt, F. Unger, U. Vazirani, "Classical command of quantum systems via rigidity of CHSH games". arXiv.:1209.0449

2. Self-testing of quantum states.
   - Andrea Coladangelo, Koon Tong Goh, Valerio Scarani. All pure bipartite entangled states can be self-tested. Nature Communications 8, Article number: 15485 (2017).
   - AW Coladangelo. Parallel self-testing of (tilted) EPR pairs via copies of (tilted) CHSH and the magic square game. Quantum Information and Computation 17 (9&10).

3. Post-quantum Cryptography in the Quantum Random-Oracle Model

4. Quantum attacks on symmetric key classical cryptographic systems.

6 Quantum Programming Languages

1. Foundations of Quantum Programming Languages.
• Applying quantitative semantics to higher-order quantum computing by Michele Pagani, Peter Selinger, Benoît Valiron. POPL 2014, 647–658.
• Floyd–hoare logic for quantum programs by Mingsheng Ying. ACM Transactions on Programming Languages and Systems (TOPLAS), Vol 33, Issue 6, pages 16.

2. Simulation, verification, and so on of quantum programs.

• Bisimulation for quantum processes by Yuan Feng, Runyao Duan, and Mingsheng Ying. POPL 2011.
• Invariants of quantum programs: characterisations and generation by Mingsheng Ying, Shenggang Ying, Xiaodi Wu. POPL 2017.

7 Fault-tolerant Quantum Computation

1. Fault-tolerant Quantum Computation.


8 Near-term Quantum Devices

1. Establishing quantum supremacy, in theory or close-to-practical scenarios.

2. Architecture of quantum hardware.


3. Better classical algorithms to simulate quantum applications.


9 Explorative topics

Topics in this section have almost no research result yet. (Please do correct me if I am wrong.)

1. Implement a quantum algorithm with the publicly accessible quantum machines (or simulators), e.g., IBM Q Experience, Microsoft Q#, and so on. Design some measures to compare them.

2. Survey the hardware specifications of publicly accessible quantum machines. Think of any practical method to verify the real quantum machines against their claimed specifications.

3. Please tell me if you have any idea along this line.