Candidate Course Project Topics (CMSC/PHYS 457)

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.
    - Summoning Information in Spacetime, or Where and When Can a Qubit Be? by Patrick Hayden, Alex May. QIP 2013. arXiv:1210.0913.
    - Quantum causality by Caslav Brukner, Nature Physics 10, 259–263 (2014).
2. Superdense coding of quantum states.
    - A.Abeyesinghe, P.Hayden, G.Smith, and A.Winter. Optimal superdense coding of entangled states. IEEE Transactions on Information Theory 52(8): 3635–3641, 2006.
    - A. Harrow, P. Hayden, and D. Leung. Superdense coding of quantum states. Physical Review Letters 92(18): 187901, 2004.
3. Local hidden-variable theories for some entangled states.
    - R. Werner. Quantum states with Einstein-Podolsky-Rosen correlations admitting a hidden-variable model. Physical Review A 40(8): 4277, 1989.
    - J. Barrett. Non-sequential positive-operator-valued measurements on entangled mixed states do not always violate a Bell inequality. Physical Review A 65(4): 042302, 2002.
4. Remote preparation of quantum states.
    - C.Bennett, P.Hayden, D.Leung, P.Shor, and A.Winter. Remote preparation of quantum states. IEEE Transactions on Information Theory 51(1): 56?74, 2005.
5. Quantum data hiding.
    - P. Hayden, D. Leung, and G. Smith. Multiparty data hiding of quantum information. Physical Review A 71(6): 062339, 2005.
6. Unitary t-designs and random Clifford operations.
    - D. P. DiVincenzo, D. W. Leung, and B. M. Terhal. Quantum data hiding. IEEE Transactions on Information Theory 48(3):580?598, 2002.
    - C. Dankert, R. Cleve, J. Emerson, and E. Livine. Exact and approximate unitary 2-designs and their application to fidelity estimation. Physical Review A 80: 12304, 2009.
    - D. Gross, K. Audenaert, and J. Eisert. Evenly distributed unitaries: on the structure of unitary designs. Journal of Mathematical Physics 48(5): 052104, 2007.
    - R. Cleve, D. Leung, L. Liu, C. Wang, Near-linear constructions of exact unitary 2-designs, arXiv:1501.04592.
    - Zak Webb. The Clifford group forms a unitary 3-design, Quantum Information and Computation 16, 1379-1400 (2016), arXiv: 1510.02769; Huangjun Zhu. Multiqubit Clifford groups are unitary 3-designs, Phys. Rev. A 96, 062336 (2017), arXiv: 1510.02619.
7. Approximating random states and unitary designs by circuits.

- R. Oliveira, O. Dahlsten, and M. Plenio. Generic entanglement can be generated efficiently. Physical Review Letters 98(13): 130502, 2007.
- A. Harrow and R. Low. Random quantum circuits are approximate 2-designs. Communications in Mathematical Physics 291(1): 257?302, 2009.
- A. Harrow and R. Low. Efficient quantum tensor product expanders and k-designs. Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques, pages 548–561, 2009.
- F. Brandão, A. Harrow, and M. Horodecki. Local random quantum circuits are approximate polynomial-designs. arXiv:1208.0692, 2012.

8. Super-activation of quantum nonlocality.
   - C. Palazuelos. Super-activation of quantum non-locality. Physical Review Letters 109: 190401, 2012.
9. Separability and Quantum de Finetti bounds
   - F. Brandão, M. Christandl, and J. Yard. Faithful squashed entanglement. Communications in Mathematical Physics 306 (3): 805?830, 2011. (The latest arXiv version (arXiv:1010.1750) corrects an error in the published version.).
   - F. Brandão and A. Harrow. Quantum de Finetti theorems under local measurements with applications. In Proceedings of the 45th Annual ACM Symposium on Theory of Computing, pages 861?870, 2013.
   - Aram Harrow, Anand Natarajan, Xiaodi Wu. An improved semidefinite programming hierarchy for testing entanglement. Communications in Mathematical Physics, Volume 352, Issue 3, pp 881–904.
   - Aram Harrow, Anand Natarajan, Xiaodi Wu. Limitations of semidefinite programs for separable states and entangled games. QIP 2017. arXiv: 1612.09306.
10. An uncertainty relation when a particle is entangled with a quantum memory.
    - The uncertainty principle in the presence of quantum memory. M. Berta, M. Christandl, R. Colbeck, J. Renes, and R. Renner. Nature Physics 6 (9): 659–662, 2010.
11. The quantum substate theorem.
    - R.Jain, J.Radhakrishnan, and P.Sen. A new information-theoretic property about quantum states with an application to privacy in quantum communication. Journal of the ACM 56(6): article 33, 2009.
    - R. Jain and A. Nayak. Short proofs of the quantum substate theorem. IEEE Transactions on Information Theory 58 (6): 3664?3669, 2012.

2 Physics and Quantum Information

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

- Longer-Baseline Telescopes Using Quantum Repeaters. by Daniel Gottesman, Thomas Jennewein, and Sarah Croke. Phys. Rev. Lett. 109, 070503. arXiv: 1107.2939.
- Enhanced Sensitivity of Photo-detection via Quantum Illumination. by Seth Lloyd, Science 12 Sep 2008: Vol. 321, Issue 5895, pp. 1463-1465. arXiv: 0803.2022.

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

- Black holes as mirrors: quantum information in random subsystems by Patrick Hayden and John Preskill, Journal of High Energy Physics 0709:120, arXiv:0708.4025.
- Quantum Computation vs. Firewalls by Daniel Harlow, Patrick Hayden, Journal of High Energy Physics June 2013, 2013:85, arXiv: 1301.4504.

3 Quantum Algorithms

1. Quantum random walks.

- J. Kempe, Quantum random walks – an introductory overview. arXiv: quant-ph/0303081
- A. Ambainis, Quantum walks and their algorithmic applications. arXiv: quant-ph/0403120
- F. Magniez, A. Nayak, J. Roland, and M. Santha, Search via Quantum Walk. arXiv: quant-ph/0608026
- A. M. Childs, Universal computation by quantum walk. arXiv:0806.1972

2. Quantum algorithm for linear systems and related topics.

- Quantum algorithm for solving linear systems of equations by Aram W. Harrow, Avinatan Hassidim, Seth Lloyd, Phys. Rev. Lett. vol. 15, no. 103, pp. 150502 (2009). arXiv:0811.3171.
- Quantum linear systems algorithm with exponentially improved dependence on precision by Andrew M. Childs, Robin Kothari, Rolando D. Somma, QIP 2016. arXiv:1511.02306
- Quantum Algorithms for Approximating the Effective Resistances in Electrical Networks by Guoming Wang. arXiv:1311.1851.

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

- Quantum support vector machine for big data classification by Patrick Rebentrost, Masoud Mohseni, Seth Lloyd, Phys. Rev. Lett. 113, 130503 (2014). arXiv:1307.0471.
- Quantum algorithms for topological and geometric analysis of data by Seth Lloyd, Silvano Garnerone, Paolo Zanardi, Nature Communications 7, Article number: 10138. arXiv:1408.3106
- Quantum principal component analysis by Seth Lloyd, Masoud Mohseni, Patrick Rebentrost, Nature Physics 10, 631 (2014). arXiv:1307.0401
- Quantum Data Fitting by Nathan Wiebe, Daniel Braun, Seth Lloyd, Phys. Rev. Lett. 109, 050505 (2012). arXiv:1204.5242.

4. Quantum algorithms for algebraic problems, and relations to cryptography.

- A subexponential-time quantum algorithm for the dihedral hidden subgroup problem by Greg Kuperberg, SIAM Journal on Computing, Volume 35 Issue 1, 2005, Pages 170-188. arXiv:quant-ph/0302112
- Another subexponential-time quantum algorithm for the dihedral hidden subgroup problem by Greg Kuperberg. arXiv:1112.3333.
- A Subexponential Time Algorithm for the Dihedral Hidden Subgroup Problem with Polynomial Space by Oded Regev. arXiv:quant-ph/0406151
- 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-Franois Biasse, Fang Song, SODA 2016.

5. Span programs and learning graphs.
    - Ben W. Reichardt. Span Programs and Quantum Query Complexity: The General Adversary Bound Is Nearly Tight for Every Boolean Function. FOCS 09.
    - Aleksandrs Belovs. Span Programs for Functions with Constant-Sized 1-certificates. arXiv:1105.4024
6. Quantum property testing.
    - Ashley Montanaro, Ronald de Wolf. A Survey of Quantum Property Testing. arXiv:1310.2035.
    - Andris Ambainis, Aleksandrs Belovs, Oded Regev, Ronald de Wolf. Efficient Quantum Algorithms for (Gapped) Group Testing and Junta Testing. arXiv:1507.03126.
    - Tongyang Li, Xiaodi Wu. Quantum query complexity of entropy estimation. arXiv:1710.06025.
7. Quantum algorithms for optimization.
    - J. V. Apeldoorn, A. Gilyen, S. Gribling, and R. de Wolf. Quantum SDP-solvers: Better upper and lower bounds. FOCS 2017. Arxiv: 1705.01843.
    - F. G. Brandao and K. Svore. Quantum speed-ups for semidefinite programming. FOCS 2017.
    - Fernando G. S. L. Brando, Amir Kalev, Tongyang Li, Cedric Yen-Yu Lin, Krysta M. Svore, Xiaodi Wu. Exponential Quantum Speed-ups for Semidefinite Programming with Applications to Quantum Learning. arXiv:1710.02581
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.

   - 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.

2. Equivalence of quantum circuits and quantum Turing machines.

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

3. Equivalence of standard and adiabatic quantum computation.

   - 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.

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
   - 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.
   - C. Marriott and J. Watrous. Quantum Arthur-Merlin games. Computational Complexity, 14(2):122?152, 2005.
   - R. Jain, Z. Ji, S. Upadhyay, and J. Watrous. QIP = PSPACE. Journal of the ACM 58(6): article 30, 2011.
   - 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.
   - G. Gutoski and X. Wu. Parallel approximation of min-max problems. Computational Complexity 22(2):385–428, 2013.

5. Multi-prover quantum interactive proofs.

   - 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. Computational Complexity 18(2): 273?307, 2009.
   - J. Kempe, H. Kobayashi, K. Matsumoto, B. Toner, and T. Vidick. Entangled games are hard to approximate. SIAM Journal on Computing 40(3): 848-877, 2011.

- T. Vidick. Three-player entangled XOR games are NP-hard to approximate.Proceedings of the 54th Annual IEEE Symposium on Foundations of Computer Science, pages 766?775, 2013.
- A. Natarajan, T. Vidick. Two-player entangled games are NP-hard. arXiv:1710.03062

6. QMA(2)
   - H. Blier and A. Tapp. All languages in NP have very short quantum proofs. arXiv:0709.0738.
   - S. Aaronson, S. Beigi, A. Drucker, B. Fefferman, and P. Shor. The power of unentanglement. Theory of Computing 5: 1–42, 2009.
   - Aram W. Harrow, Ashley Montanaro. Testing product states, quantum Merlin-Arthur games and tensor optimisation. Journal of the ACM vol. 60 no. 1, 2013. arXiv:1001.0017.
7. Quantum proofs and advices.
   - S. Aaronson and A. Drucker. A full characterization of quantum advice. Proceedings of the 42nd ACM Symposium on Theory of Computing, 131–140, 2010.
   - S. Aaronson and G. Kuperberg. Quantum versus classical proofs and advice. Theory of Computing, 3:129–157, 2007.
8. Quantum computational learning theory.
   - Srinivasan Arunachalam and Ronald de Wolf. A Survey of Quantum Learning Theory. arXiv:1701.06806
   - Srinivasan Arunachalam and Ronald de Wolf. Optimal Quantum Sample Complexity of Learning Algorithms. arXiv:1607.00932
   - Scott Aaronson. Shadow Tomography of Quantum States. arXiv:1711.01053
   - Scott Aaronson. The Learnability of Quantum States. arXiv:quant-ph/0608142
9. Complexity of super-quantum computational model.
   - Quantum Computing, Postselection, and Probabilistic Polynomial-Time by Scott Aaronson, Proceedings of the Royal Society A, 461(2063):3473-3482, 2005. quant-ph/0412187
   - The Space "Just Above" BQP by S. Aaronson, A. Bouland, J. Fitzsimons, and M. Lee, ITCS 2016. arXiv:1412.6507.
10. Using the mathematics of quantum information to prove theorems.
    - A. Drucker, R. de Wolf. "Quantum Proofs for Classical Theorems". Theory of Computing Library Graduate Surveys 2. arXiv: 0910.3376.
    - S. Fiorini, S. Massar, S. Pokutta, H. R. Tiwary, R. de Wolf. "Linear vs. Semidefinite Extended Formulations: Exponential Separation and Strong Lower Bounds". STOC 2012. arXiv:1111.0837.
    - S. Aaronson. "A Linear-Optical Proof that the Permanent is #P-Hard". arXiv:1109.1674.

5 Quantum Cryptography

1. Device-independent quantum cryptography.

   - Robust protocols for securely expanding randomness and distributing keys using untrusted quantum devices by Carl Miller, Yaoyun Shi, STOC 2014. arXiv:1402.0489
   - Physical Randomness Extractors: Generating Random Numbers with Minimal Assumptions by Kai-Min Chung, Yaoyun Shi, Xiaodi Wu, QIP 2014. arXiv:1402.4797
   - U.V. Vazirani and T. Vidick, "Certifiable Quantum Dice - Or, testable exponential randomness expansion". STOC 2012. arXiv:1111.6054
   - U.V. Vazirani and T. Vidick, "Fully device independent quantum key distribution", QIP 2013. arXiv: 1210.1810.
   - 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).
   - Anand Natarajan, Thomas Vidick. Robust self-testing of many-qubit states. STOC 2017. arXiv:1610.03574.

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

   - Eike Kiltz and Vadim Lyubashevsky and Christian Schaffner. A Concrete Treatment of Fiat-Shamir Signatures in the Quantum Random-Oracle Model. ia.cr/2017/916.
   - D. Unruh. Non-interactive zero-knowledge proofs in the quantum random oracle model. In EUROCRYPT 2015, Part II (Apr. 2015), E. Oswald and M. Fischlin, Eds., vol. 9057 of LNCS, Springer, Heidelberg, pp. 755–784.
   - D. Unruh. Computationally binding quantum commitments. In EUROCRYPT (2016).

4. Quantum attacks on symmetric key classical cryptographic systems.

   - A Note on Quantum Security for Post-Quantum Cryptography by Fang Song, PQCrypto2014. arXiv:1409.2187.
   - Using Simon's Algorithm to Attack Symmetric-Key Cryptographic Primitives by Thomas Santoli, Christian Schaffner. arXiv:1603.07856.

6 Quantum Programming Languages

1. Foundations of Quantum Programming Languages.

   - Quantum lambda calculus. Book chapter by Benoit Valiron and Peter Selinger. In Simon Gay and Ian Mackie, editors, Semantic Techniques in Quantum Computation, Cambridge University Press, pp. 135–172, 2009.

- Programming the quantum future by Benoit Valiron, Neil J. Ross, Peter Selinger, D. Scott Alexander, and Jonathan M. Smith. Communications of the ACM Vol. 58 No. 8, pages 52–61, 2015.
- Applying quantitative semantics to higher-order quantum computing by Michele Pagani, Peter Selinger, Benoit 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. POPL2011.
   - Symbolic bisimulation for quantum processes by Y. Feng, Y. X. Deng, M. S. Ying, ACM Transactions on Computational Logic, 15(2) (2014), 14:1-14:32.
   - Model-Checking Linear-Time Properties of Quantum Systems by M. S. Ying, Y. J. Li, N. K. Yu, and Y. Feng. ACM Transactions on Computational Logic, 15(3) (2014), 22:1-22:31.
   - Invariants of quantum programs: characterisations and generation by Mingsheng Ying, Shenggang Ying, Xiaodi Wu. POPL 2017.
   - QWIRE: A Core Language for Quantum Circuits by Jennifer Paykin, Robert Rand, Steve Zdancewic. POPL 2017.

7 Fault-tolerant Quantum Computation

1. Fault-tolerant Quantum Computation.

   - D. Aharonov and M. Ben-Or, Fault-Tolerant Quantum Computation with Constant Error Rate. arXiv: quant-ph/9906129
   - J. Preskill, Fault-tolerant quantum computation. arXiv: quant-ph/9712048
   - E. Knill, R. Laflamme, W. Zurek, Threshold Accuracy for Quantum Computation. arXiv: quant-ph/9610011
   - D. Gottesman, Fault-Tolerant Quantum Computation with Constant Overhead. arXiv: 1310.2984.
   - Earl T. Campbell, Barbara M. Terhal, and Christophe Vuillot. Roads towards fault-tolerant universal quantum computation. Nature 549, 172?179.
   - Barbara M. Terhal. Quantum Error Correction for Quantum Memories. Rev. Mod. Phys. 87, 307 (2015). arXiv:1302.3428.

8 Near-term Quantum Devices

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

   - The Computational Complexity of Linear Optics by S. Aaronson and A. Arkhipov, Theory of Computing 4:143-252, 2013. arXiv:1011.3245. (Known as BosonSampling)

- Average-case complexity versus approximate simulation of commuting quantum computations by Michael J. Bremner, Ashley Montanaro, Dan J. Shepherd. QIP 2016. arXiv:1504.07999.
- Complexity-Theoretic Foundations of Quantum Supremacy Experiments by Scott Aaronson, Lijie Chen, arXiv:1612.05903. (CCC 2017)
- Quantum computational supremacy by Aram W. Harrow, Ashley Montanaro. Nature 549, 203–209 (14 September 2017).

2. Architecture of quantum hardware.
   - An experimental microarchitecture for a superconducting quantum processor by X. Fu et al. Proceeding MICRO-50 '17 Proceedings of the 50th Annual IEEE/ACM International Symposium on Microarchitecture Pages 813-825. arXiv: 1708.07677.
   - Optimized surface code communication in superconducting quantum computers by A. Javadi-Abhari et al. Proceeding MICRO-50 '17 Proceedings of the 50th Annual IEEE/ACM International Symposium on Microarchitecture Pages 692-705. arXiv:1708.09283.
   - Taming the instruction bandwidth of quantum computers via hardware-managed error correction by S. Tannu. Proceeding MICRO-50 '17 Proceedings of the 50th Annual IEEE/ACM International Symposium on Microarchitecture Pages 679-691.
3. Better classical algorithms to simulate quantum applications.
   - Classical boson sampling algorithms with superior performance to near-term experiments by A. Neville et al. Nature Physics (2017) arXiv:1705.00686.
   - The Classical Complexity of Boson Sampling by Peter Clifford and Raphel Clifford. SODA 2018. arXiv:1706.01260.

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.