C&O 781 / QIC 823 / CS 867 Quantum Algorithms

University of Waterloo, Winter 2017

Instructor: Ashwin Nayak

Project Suggestions

The following is an incomplete list of possible topics for a project. Please feel free to suggest other papers, for example, from recent conferences such as QIP, STOC, and FOCS.

Quantum walk.

- An exponential speed-up using quantum walk [14].
- An algorithm for balanced NAND trees [20].
- Universal quantum computation by quantum walk [13, 15].
- Applications of quantum walk search [16, 22].
- A search algorithm inspired by adiabatic quantum computation [28].

Query complexity

- Learning graphs for k-Distinctness [8].
- Multiplicative quantum adversary method [36].
- Lower bound for state generation [4].
- Quantum versus classical query complexity [1, 5, 2]

Hidden Subgroup Problem.

- Reduction from the Unique Shortest Vector problem to Dihedral HSP [35].
- An algorithm for the Hidden Shift Problem [37].
- Hidden Translation and Orbit Coset problems [21].
- Limitations of coset states for the symmetric group [31, 24].

Simulating continuous-time dynamics.

- Simulating Hamiltonians [9, 10, 11, 29].
- Simulating open quantum systems [17, 18].

Computational complexity.

- Error-reduction for QMA, containment in PP [30].
- Quantum interactive proof systems [27].
- The Quantum PCP conjecture [3].

Learning, property testing and related topics.

- Spectrum testing [32].
- Group and junta testing [6].
- Quantum tomography [33, 23, 34].
- Sequential measurements and property testing [25].
- Quantum learning theory [7].

Other.

- Sampling Gibbs states [26].
- An algorithm for Semi-Definite Programming [12].
- Connections to lattices [19].

References

[1] Scott Aaronson and Andris Ambainis. Forrelation: A problem that optimally separates quantum from classical computing. In *Proceedings of the Forty-seventh Annual ACM Symposium on Theory of Computing*, STOC '15, pages 307–316, New York, NY, USA, 2015. ACM.

[2] Scott Aaronson, Shalev Ben-David, and Robin Kothari. Separations in query complexity using cheat sheets. In *Proceedings of the Forty-eighth Annual ACM Symposium on Theory of Computing*, STOC '16, pages 863–876, New York, NY, USA, 2016. ACM.

[3] Dorit Aharonov, Itai Arad, and Thomas Vidick. Guest column: The quantum PCP conjecture. *SIGACT News*, 44(2):47–79, June 2013.

[4] Ambainis Ambainis, Loïck Magnin, Martin Roetteler, and Jérémie Roland. Symmetry-assisted adversaries for quantum state generation. In *Proceedings of the 26th Annual IEEE Conference on Computational Complexity*, pages 167–177, June 2011.

[5] Andris Ambainis, Kaspars Balodis, Aleksandrs Belovs, Troy Lee, Miklos Santha, and Juris Smotrovs. Separations in query complexity based on pointer functions. In *Proceedings of the Forty-eighth Annual ACM Symposium on Theory of Computing*, STOC '16, pages 800–813, New York, NY, USA, 2016. ACM.

[6] Andris Ambainis, Aleksandrs Belovs, Oded Regev, and Ronald de Wolf. Efficient quantum algorithms for (gapped) group testing and junta testing. In *Proceedings of the Twenty-seventh Annual ACM-SIAM Symposium on Discrete Algorithms*, SODA '16, pages 903–922, Philadelphia, PA, USA, 2016. Society for Industrial and Applied Mathematics.

[7] Srinivasan Arunachalam and Ronald de Wolf. A survey of quantum learning theory. Technical Report arXiv:1701.06806 [quant-ph], ArXiv.org Preprint Archive, `http://www.arxiv.org/`, January 2017.

[8] Aleksandrs Belovs. Learning-graph-based quantum algorithm for k-Distinctness. In *Proceedings of the 2012 53rd Annual IEEE Symposium on Foundations of Computer Science*, pages 207–216, Oct 2012.

[9] Dominic W. Berry, Graeme Ahokas, Richard Cleve, and Barry C. Sanders. Efficient quantum algorithms for simulating sparse Hamiltonians. *Communications in Mathematical Physics*, 270(2):359–371, 2007.

[10] Dominic W. Berry, Andrew M. Childs, Richard Cleve, Robin Kothari, and Rolando D. Somma. Simulating Hamiltonian dynamics with a truncated Taylor series. Technical Report arXiv:1412.4687 [quant-ph], arXiv.org, 2014.

[11] Dominic W. Berry, Andrew M. Childs, and Robin Kothari. Hamiltonian simulation with nearly optimal dependence on all parameters. Technical Report arXiv:1501.01715 [quant-ph], arXiv.org, 2015.

[12] Fernando G. S. L. Brandão and Krysta Svore. Quantum speed-ups for semidefinite programming. Technical Report arXiv: arXiv:1609.05537 [quant-ph], ArXiv.org Preprint Archive, `http://www.arxiv.org/`, September 2016.

[13] Andrew M. Childs. Universal computation by quantum walk. *Physical Review Letters*, 102:180501, May 2009. Full version available as arXiv:0806.1972 [quant-ph].

[14] Andrew M. Childs, Richard Cleve, Enrico Deotto, Edward Farhi, Sam Gutmann, and Daniel A. Spielman. Exponential algorithmic speedup by a quantum walk. In *Proceedings of the Thirty-fifth Annual ACM Symposium on Theory of Computing*, STOC '03, pages 59–68, New York, NY, USA, 2003. ACM.

[15] Andrew M. Childs, David Gosset, and Zak Webb. Universal computation by multiparticle quantum walk. *Science*, 339(6121):791–794, 2013.

[16] Andrew M. Childs and Robin Kothari. Quantum query complexity of minor-closed graph properties. *SIAM Journal on Computing*, 41(6):1426–1450, 2012.

[17] Andrew M. Childs and Tongyang Li. Efficient simulation of sparse Markovian quantum dynamics. Technical Report arXiv:1611.05543 [quant-ph], ArXiv.org Preprint Archive, `http://www.arxiv.org/`, November 2016.

[18] Richard Cleve and Chunhao Wang. Efficient quantum algorithms for simulating lindblad evolution. Technical Report arXiv:1612.09512 [quant-ph], ArXiv.org Preprint Archive, `http://www.arxiv.org/`, December 2016.

[19] Lior Eldar and Peter Shor. A discrete Fourier transform on lattices with quantum applications. Technical Report arXiv:1703.02515 [quant-ph], ArXiv.org Preprint Archive, `http://www.arxiv.org/`, March 2017.

[20] Edward Farhi, Jeffrey Goldstone, and Sam Gutmann. A quantum algorithm for the Hamiltonian NAND tree. *Theory of Computing*, 4(8):169–190, 2008.

[21] Katalin Friedl, Gábor Ivanyos, Frédéric Magniez, Miklos Santha, and Pranab Sen. Hidden translation and orbit coset in quantum computing. *SIAM Journal on Computing*, 43(1):1–24, 2014.

[22] François Le Gall. Improved quantum algorithm for triangle finding via combinatorial arguments. In *Proceedings of the 55th Annual IEEE Symposium on Foundations of Computer Science*, pages 216–225, Los Alamitos, CA, USA, October 18–21 2014. IEEE Computer Society Press.

[23] Jeongwan Haah, Aram W. Harrow, Zhengfeng Ji, Xiaodi Wu, and Nengkun Yu. Sample-optimal tomography of quantum states. In *Proceedings of the Forty-eighth Annual ACM Symposium on Theory of Computing*, STOC '16, pages 913–925, New York, NY, USA, 2016. ACM.

[24] Sean Hallgren, Cristopher Moore, Martin Rötteler, Alexander Russell, and Pranab Sen. Limitations of quantum coset states for Graph Isomorphism. In *Proceedings of the Thirty-eighth Annual ACM Symposium on Theory of Computing*, STOC '06, pages 604–617, New York, NY, USA, 2006. ACM.

[25] Aram W. Harrow, Cedric Yen-Yu Lin, and Ashley Montanaro. Sequential measurements, disturbance and property testing. In *Proceedings of the Twenty-Eighth Annual ACM-SIAM Symposium on Discrete Algorithms*, SODA '17, pages 1598–1611, Philadelphia, PA, USA, 2017. Society for Industrial and Applied Mathematics.

[26] Michael J. Kastoryano and Fernando G. S. L. Brandão. Quantum gibbs samplers: The commuting case. *Communications in Mathematical Physics*, 344(3):915–957, 2016.

[27] Alexei Kitaev and John Watrous. Parallelization, amplification, and exponential time simulation of quantum interactive proof systems. In *Proceedings of the Thirty-second Annual ACM Symposium on Theory of Computing*, STOC '00, pages 608–617, New York, NY, USA, 2000. ACM.

[28] Hari Krovi, Frédéric Magniez, Maris Ozols, and Jérémie Roland. Quantum walks can find a marked element on any graph. Technical Report arXiv:1002.2419v2, arXiv.org, 2014.

[29] Guang Hao Low and Isaac L. Chuang. Optimal hamiltonian simulation by quantum signal processing. *Physical Review Letters*, 118:010501, Jan 2017.

[30] Chris Marriott and John Watrous. Quantum Arthur-Merlin games. *Computational Complexity*, 14(2):122–152, June 2005.

[31] Cristopher Moore, Alexander Russell, and Leonard J. Schulman. The symmetric group defies strong Fourier sampling. In *Proceedings of the 46th Annual IEEE Symposium on Foundations of Computer Science*, pages 479–488, Oct 2005.

[32] Ryan O'Donnell and John Wright. Quantum spectrum testing. In *Proceedings of the Forty-seventh Annual ACM Symposium on Theory of Computing*, STOC '15, pages 529–538, New York, NY, USA, 2015. ACM.

[33] Ryan O'Donnell and John Wright. Efficient quantum tomography. In *Proceedings of the Forty-eighth Annual ACM Symposium on Theory of Computing*, STOC '16, pages 899–912, New York, NY, USA, 2016. ACM.

[34] Ryan O'Donnell and John Wright. Efficient quantum tomography II. Technical Report arXiv:1612.00034 [quant-ph], ArXiv.org Preprint Archive, `http://www.arxiv.org/`, November 2016.

[35] Oded Regev. Quantum computation and lattice problems. *SIAM Journal on Computing*, 33(3):738–760, 2004.

[36] Robert Špalek. The multiplicative quantum adversary. In *Proceedings of the 23rd Annual IEEE Conference on Computational Complexity*, pages 237–248, June 2008.

[37] Wim van Dam, Sean Hallgren, and Lawrence Ip. Quantum algorithms for some hidden shift problems. *SIAM Journal on Computing*, 36(3):763–778, 2006.