CO 781 / QIC 823 / CS 867 Quantum Algorithms
University of Waterloo, Winter 2017

Instructor: Ashwin Nayak
Bibliography

Quantum walk. An optimal query algorithm for Element Distinctness was discovered by Ambainis [2], and it is based on quantum walk. Szegedy [22] designed a search algorithm for symmetric Markov chains, and established quadratic speed-up over classical hitting time. The search framework for reversible Markov chains is due to Magniez, Nayak, Roland, and Santha [15]. See the survey [16] for a more detailed history of discrete-time quantum walk.

Span programs and learning graphs. The use of span programs in the design of quantum algorithms arose from a sequence of works on algorithms for NAND formulae [9, 3]. The connection between span programs and query algorithms was discovered by Reichardt and Špalek [18]. Subsequently, Reichardt proved that an optimal *canonical* span program corresponds to an almost optimal query algorithm [17]. Remarkably, these algorithms were developed using continuous-time quantum walk. Lee, Mittal, Reichardt, Špalek, and Szegedy [14] present the most general version of the algorithm, along with a simplified analysis. We use the term "span program" to mean "canonical span program", which is readily seen to be equivalent to the dual of the SDP for the adversary bound.

Learning graphs were introduced by Belovs [4] and used to design more efficient quantum algorithms, such as that for Triangle Finding. The efficient algorithm derived from learning graphs is also due to him [5, 6].

The adversary bound. The quantum adversary method was developed by Ambainis [1], and refined by him and others. The strongest version of the bound is due to Høyer, Lee and Špalek [11], and the term "adversary bound" is now used for this version. See Ref. [11] for the historical development of the bound. The bound was shown to be optimal, with the discovery of span programs (see, e.g., Ref. [14]) for the details).

Fourier Sampling. The basics of representations of finite groups may be found in the book [19]. The discovery of the Simon and Shor algorithms [21, 20] led to the formulation of the Hidden Subgroup Problem. Phase Estimation was developed by Kitaev [12, 13], and used to design efficient algorithms for, among other things, the Fourier transform over $\mathbb{Z}_n$. More efficient phase estimation was discovered by Cleve, Ekert, Macchiavello, and Mosca [8]. This algorithm uses the Fourier transform over $\mathbb{Z}_{2^k}$, for which they presented an efficient exact quantum circuit. Hales and Hallgren [10] explain why we are able to solve HSP over $\mathbb{Z}$. The survey [7] describes further developments on the topic, including the representation theoretic analysis of the Fourier sampling algorithm.

Quantum Merlin Arthur games. The computational complexity class QMA was studied by Kitaev under the name BQNP [13], and the QMA-completeness of the 5-Local Hamiltonian Problem is due to him.

The QMA protocol for Group Non-Membership is due to Watrous [23]. The Local Hamiltonian Problem has been studied extensively since then.

References

[1] Andris Ambainis. Quantum lower bounds by quantum arguments. *Journal of Computer and System Sciences*, 64(4):749–898, 2002.

[2] Andris Ambainis. Quantum walk algorithm for Element Distinctness. *SIAM Journal on Computing*, 37(1):210–239, 2007.

[3] Andris Ambainis, Andrew M. Childs, Ben W. Reichardt, Robert Špalek, and Shengyu Zhang. Any AND-OR formula of size n can be evaluated in time $n^{1/2+o(1)}$ on a quantum computer. *SIAM Journal on Computing*, 39(6):2513–2530, 2010.

[4] Aleksandrs Belovs. Span programs for functions with constant-sized 1-certificates: Extended abstract. In *Proceedings of the Forty-fourth Annual ACM Symposium on Theory of Computing*, STOC '12, pages 77–84, New York, NY, USA, 2012. ACM. Complete version available as arXiv:1105.4024.

[5] Aleksandrs Belovs. Quantum walks and electric networks. Technical Report arXiv:1302.3143, arXiv.org, 2013.

[6] Aleksandrs Belovs, Andrew M. Childs, Stacey Jeffery, Robin Kothari, and Frédéric Magniez. Time-efficient quantum walks for 3-Distinctness. In Fedor V. Fomin, Rūsiņš Freivalds, Marta Kwiatkowska, and David Peleg, editors, *Automata, Languages, and Programming*, volume 7965 of *Lecture Notes in Computer Science*, pages 105–122. Springer Berlin Heidelberg, 2013.

[7] Andrew M. Childs and Wim van Dam. Quantum algorithms for algebraic problems. *Reviews of Modern Physics*, 82:1–52, Jan 2010.

[8] Richard Cleve, Artur Ekert, Chiara Macchiavello, and Michele Mosca. Quantum algorithms revisited. *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences*, 454(1969):339–354, 1998.

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

[10] Lisa Hales and Sean Hallgren. An improved quantum Fourier transform algorithm and applications. In *Proceedings of the 41st Annual IEEE Symposium on Foundations of Computer Science*, pages 515–525, 2000.

[11] Peter Høyer, Troy Lee, and Robert Špalek. Negative weights make adversaries stronger. In *Proceedings of the Thirty-Ninth Annual ACM Symposium on Theory of Computing*, STOC '07, pages 526–535, New York, NY, USA, 2007. ACM.

[12] Alexei Kitaev. Quantum measurements and the Abelian stabilizer problem. Technical Report arXiv:quant-ph/9511026, arXiv.org, 1995.

[13] Alexei Yu. Kitaev, Alexander H. Shen, and Mikhail N. Vyalyi. *Classical and Quantum Computation*, volume 47 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 2002.

[14] Troy Lee, Rajat Mittal, Ben W. Reichardt, Robert Spalek, and Mario Szegedy. Quantum query complexity of state conversion. In *Proceedings of the 52nd Annual IEEE Symposium on Foundations of Computer Science*, pages 344–353, October 2011.

[15] Frédéric Magniez, Ashwin Nayak, Jérémie Roland, and Miklos Santha. Search via quantum walk. *SIAM Journal on Computing*, 40:142–164, February 10, 2011.

[16] Ashwin Nayak, Peter C. Richter, and Mario Szegedy. Quantum analogues of Markov chains. In *Encyclopedia of Algorithms*. Springer Berlin Heidelberg, 2015.

[17] Ben W. Reichardt. Span programs are equivalent to quantum query algorithms. *SIAM Journal on Computing*, 43(3):1206–1219, 2014.

[18] Ben W. Reichardt and Robert Špalek. Span-program-based quantum algorithm for evaluating formulas. *Theory of Computing*, 8(13):291–319, 2012.

[19] Jean-Pierre Serre. *Linear Representations of Finite Groups*, volume 42 of *Graduate Texts in Mathematics*. Springer New York, 1977.

[20] Peter W. Shor. Polynomial-time algorithms for Prime Factorization and Discrete Logarithms on a quantum computer. *SIAM Journal on Computing*, 26(5):1484–1509, October 1997.

[21] Daniel R. Simon. On the power of quantum computation. *SIAM Journal on Computing*, 26(5):1474–1483, 1997.

[22] Mario Szegedy. Quantum speed-up of Markov chain based algorithms. In *Proceedings of the 45th Annual IEEE Symposium on Foundations of Computer Science*, pages 32–41, October 2004.

[23] John Watrous. Succinct quantum proofs for properties of finite groups. In *Proceedings of the 41st Annual IEEE Symposium on Foundations of Computer Science*, FOCS '00, pages 537–546, Washington, DC, USA, 2000. IEEE Computer Society.