More Quantum Algorithms have been found

George Watkins, CMPT409[1], Due 28/05/2020

Introduction The feeling in Shor's reference paper [20] is somewhat pessimistic. Few new quantum algorithms that yield exponential speedup were found after his eponymous algorithm had been discovered nearly a decade earlier. We will see that more quantum algorithms have been found since. In this paper, I examine some of the progress made since, in the field of quantum computing, with a focus on quantum algorithms. We will see how these relate to Aaronson's perspective in his reference paper [1].

The New Limits of Quantum A major question is whether a quantum computer can solve efficiently (in polynomial time with a fixed probability) any problem that a classical computer can verify in polynomial time [1]. That is the problem of finding an NP-Complete problem that is also in the complexity class BQP (Bounded Error Quantum Polynomial Time). A quantum algorithm, to solve an NP-Complete problem in polynomial time, would have to exploit the structure of the specific problem, as the improvement possible by black box search had already been shown to be limited to the known quadratic speedup given by Grover's algorithm [6].

An NP-Complete problem in BQP does not appear to have been found yet, nor it appears to be shown that such problem cannot exist [15]. But in 2014, a quantum algorithm was shown to provide a better Constraint Satisfaction Problem approximation guarantee than any known classical algorithm [11]. Even though this result was matched the following year by a classical algorithm [5], it does show that there are NP-Complete problems of which Quantum algorithms can exploit the structure, beyond Grover's search.

Aaronson, driven by the intuition that simulating quantum circuits is hard on classical machines, conjectured in 2009 that BQP is not contained in the polynomial hierarchy (PH), and therefore NP, altogether [2]. That is, there could be problems that quantum computers can solve in polynomial time (with a certain probability), that could neither be solved nor verified in polynomial time by classical computers. Such a result could indicate that there might be a class of interesting algorithms that quantum computers would solve efficiently. A problem that shows that $BQP^A \not\subset PH^A$, relative to an oracle A, was found in 2018, providing evidence that $BQP \not\subset NP$ [12; 19].

As for the developments of physics, recent discoveries in Quantum Field Theory have enabled the possibility of a new kind of machine that could solve NP-Complete problems in polynomial time [16]. This would be a significant breakthrough, however, as the authors note, this is still only a theoretical result, that has consequences that still need to be observed experimentally.

New Algorithms and Results What is considered a major promise in terms of quantum speedup came shortly after Aaronson's reference paper, the HHL algorithm [13]. The HHL algorithm can solve certain linear systems in sub-linear time in the number of equations. It should be noted that this algorithm is subject to the overhead of passing from a classical state to a quantum state and back. Similarly the Quantum Fourier Transform

[1] With Dr. Pearce's permission to excede 2 pages.

(QFT), whose full power cannot be harnessed directly on classical states, the HHL algorithm could be used be used to provide speedup as a building block for another algorithm [3]. Just like the QFT is part of Shor's factoring algorithm. In fact algorithms leveraging HHL, that could achieve exponential speedup, have been found, notably in the field of Machine Learning [3]. More quantum ML algorithms that claim some degree of speed up exist, some of which have been demonstrated on quantum hardware [21]. In general though it remains unclear how much is the advantage of many of these algorithms [7].

The force that pushed the early stages of development of quantum computing, quantum simulations, is still driving research in the field. Quantum simulations have applications in Quantum Chemistry that could have a major impact, such as Drug Discovery [8]. Quantum Chemical algorithms often revolve around finding the eigenstates of the electronic Hamiltonian of a molecule. A hybrid quantum classical algorithm for finding eigenvalues of large systems was discovered and experimentally demonstrated in 2014 [17], claiming to provide exponential speedup over conventional methods. More recently, this hybrid approach has been made into a fully quantum algorithm that enables faster convergence [22].

One result that captured much media attention, appearing on the popular magazine WIRED [2] for instance, was that of the experiment designed by Google AI Quantum, in which the authors claim to have performed a computation that could have never been done on Classical Hardware [4]. However it must be noted that the computation performed was artificially constructed, as opposed to being a real-world problem, making the experiment more of a proof of concept.

At the same time Computers that exploit quantum properties of nature are starting to be commercially available, the first being D-Wave System's Quantum Annealers [10], which the company claims to have a competitive advantage over classical computers, though it's field of application is limited. Other companies such as Microsoft [9] and IBM [14] are offering services to the public, capable of running quantum programs on physical quantum hardware. It is possible that as quantum hardware becomes available, we will start to run quantum algorithms that perform well, possibly without formal justification, the same way the Simplex Algorithm was very effective in practice, long before we had a formal justification of such performance [18].

Conclusion By observing the results mentioned above one can conclude that significant progress in quantum algorithms has been made, perhaps in a slightly different direction than earlier expectations. The current computers are often defined as Noisy Intermediate-Scale Quantum (NISQ) and still have limitations [18]. There are optimistic views according to which "We are only one creative algorithm away from valuable near-term applications" [4], and pessimistic ones that claim that quantum computing in the NISQ era is not competitive against classical computing [15]. While it is difficult to make claims about how close we are to quantum supremacy (at least for real world problems), it is reasonable to believe that we are approaching a technical-scientific level where quantum computers could be useful for solving specific real world problems.

[2] https://www.wired.com/story/quantum-computing-here-but-not-really/

References

[1] S. Aaronson. The limits of quantum. *Scientific American*, 298(3):62–69, 2008.

[2] S. Aaronson. Bqp and the polynomial hierarchy. In *Proceedings of the forty-second ACM symposium on Theory of computing*, pages 141–150, 2010.

[3] S. Aaronson. Read the fine print. *Nature Physics*, 11(4):291–293, 2015.

[4] F. Arute, K. Arya, R. Babbush, D. Bacon, J. C. Bardin, R. Barends, R. Biswas, S. Boixo, F. G. Brandao, D. A. Buell, et al. Quantum supremacy using a programmable superconducting processor. *Nature*, 574(7779):505–510, 2019.

[5] B. Barak, A. Moitra, R. O'Donnell, P. Raghavendra, O. Regev, D. Steurer, L. Trevisan, A. Vijayaraghavan, D. Witmer, and J. Wright. Beating the random assignment on constraint satisfaction problems of bounded degree. *CoRR*, abs/1505.03424, 2015.

[6] M. Boyer, G. Brassard, P. Høyer, and A. Tapp. Tight bounds on quantum searching. *Fortschritte der Physik: Progress of Physics*, 46(4-5):493–505, 1998.

[7] M. Broughton, G. Verdon, T. McCourt, A. J. Martinez, J. H. Yoo, S. V. Isakov, P. Massey, M. Y. Niu, R. Halavati, E. Peters, et al. Tensorflow quantum: A software framework for quantum machine learning. *arXiv preprint arXiv:2003.02989*, 2020.

[8] Y. Cao, J. Romero, and A. Aspuru-Guzik. Potential of quantum computing for drug discovery. *IBM Journal of Research and Development*, 62(6):6–1, 2018.

[9] M. Corporation. Azure quantum. https://azure.microsoft.com/en-us/services/quantum/, 2020.

[10] I. D-Wave Systems. Practical quantum computing. technology overview. https://www.dwavesys.com/sites/default/files/Dwave_Tech%20Overview2_F.pdf, 2020.

[11] E. Farhi, J. Goldstone, and S. Gutmann. A quantum approximate optimization algorithm applied to a bounded occurrence constraint problem. *arXiv: Quantum Physics*, 2014.

[12] H. Goldberg and S. H. Liu. Oracle separation of bqp and the polynomial hierarchy. 2019.

[13] A. W. Harrow, A. Hassidim, and S. Lloyd. Quantum algorithm for linear systems of equations. *Physical review letters*, 103(15):150502, 2009.

[14] IBM. Ibm quantum — systems. https://www.ibm.com/quantum-computing/technology/systems, 2020.

[15] G. Kalai. The argument against quantum computers. In *Quantum, Probability, Logic*, pages 399–422. Springer, 2020.

[16] V. Kreinovich, L. Longpré, and A. Beltran. Qft+ np= p quantum field theory (qft): A possible way of solving np-complete problems in polynomial time. In *Quantum Computing: An Environment for Intelligent Large Scale Real Application*, pages 229–249. Springer, 2018.

[17] A. Peruzzo, J. McClean, P. Shadbolt, M.-H. Yung, X.-Q. Zhou, P. J. Love, A. Aspuru-Guzik, and J. L. O'brien. A variational eigenvalue solver on a photonic quantum processor. *Nature communications*, 5:4213, 2014.

[18] J. Preskill. Quantum computing in the nisq era and beyond. arxiv. *arXiv preprint arXiv:1801.00862*, 2018.

[19] R. Raz and A. Tal. Oracle separation of bqp and ph. In *Proceedings of the 51st Annual ACM SIGACT Symposium on Theory of Computing*, STOC 2019, page 13–23, New York, NY, USA, 2019. Association for Computing Machinery.

[20] P. W. Shor. Why haven't more quantum algorithms been found? *Journal of the ACM (JACM)*, 50(1):87–90, 2003.

[21] G. Verdon, J. Pye, and M. Broughton. A universal training algorithm for quantum deep learning. *arXiv preprint arXiv:1806.09729*, 2018.

[22] S. Wei, H. Li, G. Long, et al. A full quantum eigensolver for quantum chemistry simulations. *Research*, 2020:1486935, 2020.