The Road to Quantum Computational Supremacy

Cristian S. Calude
University of Auckland, New Zealand
www.cs.auckland.ac.nz/~cristian

22 September, 2018

The quantum computational advantage for simulating quantum systems was first stated by Feynman in 1981. What is the justification of Feynman's insight? According to the data processing inequality [10], (classical) post-processing cannot increase information. This suggests that to run an accurate classical simulation of a quantum system one must know a lot about the system before the simulation is started. Manin [16] and Feynman [12] have argued that a quantum computer might not need to have so much knowledge.

This line of reasoning seemingly inspired Deutsch [11] to state

> **The postulate of quantum computation***:*
> *Computational devices based on quantum mechanics will be computationally superior compared to digital computers.*

What is quantum computational supremacy?

A spectacular support for this postulate came from Shor's 1994 polynomial factoring quantum algorithm [20] in spite of the fact that the problem whether factoring is in **P** was, and still is, open.

In 2011 the syntagm "quantum supremacy" was coined and discussed by J. Preskill in his Rapporteur talk "Quantum Entanglement and Quantum Computing" [19] at the 25th *Solvay Conference on Physics* (Brussels, Belgium, 19–22 October 2011):

> *We therefore hope to hasten the onset of the era of quantum supremacy, when we will be able to perform tasks with controlled quantum systems going beyond what can be achieved with ordinary digital computers.*

What is quantum computational supremacy?

Recently, quantum computational supremacy was described in [6] as follows:

> *Quantum supremacy is achieved when a formal computational task is performed with an existing quantum device which cannot be performed using any known algorithm running on an existing classical supercomputer in a reasonable amount of time.*

Brief critique of the concept of quantum computational supremacy

Note the imprecision in the above formulation: the comparison is made with “any known algorithm running on an existing classical supercomputer” and the classical computation takes “a reasonable amount of time”. Can this imprecision be decreased or, even better, eliminated?

Quantum computational supremacy suggests a misleading comparison between classical and quantum computing: if a quantum computer can outdo **any** classical computer on one problem we have quantum supremacy, even if classical computers could be at least as good as quantum ones in solving many (most) other problems. Put it bluntly, *quantum computational supremacy, if achieved, won’t make classical computing obsolete.*

Quantum computational supremacy under the microscope

A quantum computational supremacy experiment has to prove both a lower bound and an upper bound.

In Google's proposed experiment [17] the upper bound is given by a quantum algorithm (running on a quantum computer with 49 qubits) sampling from the output distribution of pseudo-random quantum circuits built from a universal gate set—a mathematical fact and an engineering artefact (the construction of the quantum machine).

The lower bound is necessary for proving that no classical computer can simulate the sampling in reasonable time.

Proving lower bounds is notoriously more difficult than demonstrating upper bounds.

Criteria for quantum computational supremacy

Harrow and Montanaro [13] have proposed a reasonable list of criteria for a quantum computational supremacy experiment:

1. a well-defined computational problem,
2. a quantum algorithm solving the problem which can run on a near-term hardware capable of dealing with noise and imperfections,
3. an amount of computational resources (time/space) allowed to any classical competitor,
4. a small number of well-justified complexity-theoretic assumptions,
5. a verification method that can efficiently distinguish between the performances of the quantum algorithm from **any** classical competitor using the allowed resources.

The proposed experiment is not about solving a problem: it is the computational task of sampling from the output distribution of pseudo-random quantum circuits built from a universal gate set.

This computational task is difficult because as the grid size increases, the *memory needed to store everything increases classically exponentially*. But, do we *really need* to store everything?

The required memory for a $6 \times 4 = 24$–qubit grid is just 268 megabytes, less than the average smartphone, but for a $6 \times 7 = 42$–qubit grid it jumps to 70 terabytes, roughly 10,000 times that of a high-end PC. Google has used Edison, a supercomputer housed by the US National Energy Research Scientific Computing Center and ranked 72 in the Top500 List [1], to simulate the behaviour of the grid of 42 qubits.

Google quantum computational supremacy

The classical simulation stopped at this stage because going to the next size up *was thought to be currently impossible: a 48-qubit grid would require 2,252 petabytes of memory, almost double that of the top supercomputer in the world.* The path to quantum computational supremacy was obvious: if Google could solve the problem with a 50–qubit quantum computer, it would have beaten every other computer in existence.

Simple and clear!

Google was on track to deliver before the end of 2017!

Let us note that many, if not most, discussions about quantum computational supremacy focus on the most exciting possibilities of quantum computers, namely the upper bound.

What about the lower bound? Google's main article on this topic [6] refers cautiously to the lower bound in the abstract:

> *We extend previous results in computational complexity* to argue more formally *that this sampling task must take exponential time in a classical computer.*

They do not claim to have a proof for the lower bound, just a "better formal argument".

Proving the lower bound...

> **Memory assumption**. *Sampling this distribution classically requires a direct numerical simulation of the circuit, with computational cost exponential in the number of qubits.*

The assumption was corroborated by the statement:

> *Storing the state of a 46–qubit system takes nearly a petabyte of memory and is at the limit of the most powerful computers. [17]*

Proving the lower bound...

The **Memory assumption** is crucial for the proposed lower bound, and, indeed, this was confirmed very soon. The paper [18] proved that a supercomputer can simulate sampling from random circuits with low depth (layers of gates) of up to 56 qubits.

Better results have been quickly announced, see for example [7]. The limits of classical simulation are not only unknown, but hard to predict.

In spite of this, IBM has announced a prototype of a 50–qubit quantum computer, stating that it “aims to demonstrate capabilities beyond today’s classical systems” with quantum systems of this size [2].

Digression: again about the importance of lower bounds

Ewin Tang (an 18-year-old undergraduate student at UT Austin) has recently proved [21] that classical computers can solve the "recommendation problem" – given incomplete data on user preferences for products, can one quickly and correctly predict which other products a user will prefer? – with performance comparable to that of a quantum computer.

Is this significant? **Yes**, because quantum computer scientists had considered this problem to be one of the best examples of a problem that quantum computers can solve exponentially faster than their classical ones.

The quantum solution in [15] was hailed as one of the first examples in *quantum machine learning and big data* that would be unlikely to be done classically. . .

Current state of the art

According to [3]

> *The successful classical simulation does not undercut the rationale for quantum supremacy experiments. The truth, ironically, is almost the opposite: it being possible to simulate 49–qubit circuits using a classical computer is a precondition for Google's planned quantum supremacy experiment, because it's the only way we know to check such an experiment's results!*

The goal is to get via quantum computing as far as you can up the mountain of exponentiality provided people still see you from the base. Why? Because it's there. "It is not the mountain we conquer but ourselves", as Edmund Hillary aptly said.

Three lessons

- Do not underestimate the importance of mathematical modelling and proving (lower bounds, in particular).
- A trend in quantum computing is emerging: when a problem is solved efficiently in quantum computing, it draws more attention and often produces better classical alternatives than existed before. Some of the new efficient classical solutions, see for example [9, 4, 5, 14, 21], have been directly inspired by the quantum work.
- The conversation on quantum computing, quantum cryptography and their applications needs an infusion of modesty (if not humility), more technical understanding and clarity as well as less hype. Raising false expectations could be harmful for the field.

The race continues! See more in [8].

References

[1] Edison supercomputer in TOP 500 ranking.
https://www.top500.org/list/2017/06/?page=1, June 2017.

[2] IBM builds 50-qubit quantum computer.
http://techvibesnow.com/ibm-builds-50-qubit-quantum-computer/, November 2017.

[3] S. Aaronson.
Shtetl-Optimized – 2^n is exponential, but 2^{50} is finite.
https://www.scottaaronson.com/blog/?p=3512, November, 12 2017.

References (cont.)

[4] A. A. Abbott.
The Deutsch-Jozsa problem: De-quantisation and entanglement.
Natural Computing, 11(1):3–11, 2011.

[5] A. A. Abbott and C. S. Calude.
Understanding the quantum computational speed-up via de-quantisation.
Electronic Proceedings in Theoretical Computer Science, 26:1–12, 2010.

[6] S. Boixo, S. V. Isakov, V. N. Smelyanskiy, R. Babbush, N. Ding, Z. Jiang, M. J. Bremner, J. M. Martinis, and H. Neven.
Characterizing quantum supremacy in near-term devices.
`arXiv:1608.00263` [quant-ph], April 2017.

References (cont.)

[7] S. Boixo, S. V. Isakov, V. N. Smelyanskiy, and H. Neven.
Simulation of low-depth quantum circuits as complex undirected graphical models.
`https://arxiv.org/pdf/1712.05384.pdf`, January 2018.

[8] C. Calude and E. Calude.
The road to quantum computational supremacy.
http://arxiv.org/abs/1712.01356v2, November 2017.

[9] C. S. Calude.
De-quantizing the solution of Deutsch's problem.
International Journal of Quantum Information, 5(3):409–415, Jun 2007.

[10] T. M. Cover and J. A. Thomas.
Elements of Information Theory.
John Wiley & Sons, New York, 1991.

References (cont.)

[11] D. Deutsch.
Quantum theory, the Church-Turing principle and the universal quantum computer.
Proceedings of the Royal Society of London Series A, 400:97–117, Jan 1985.

[12] R. P. Feynman.
Simulating physics with computers.
International Journal of Theoretical Physics, 21:467–488, 1982.

[13] A. W. Harrow and A. Montanaro.
Quantum computational supremacy.
Nature, 549(7671):203–209, 09 2017.

References (cont.)

[14] N. Johansson and J.-Å. Larsson.
Efficient classical simulation of the Deutsch–Jozsa and Simon's algorithms.
Quantum Information Processing, 16(9):233, Aug 2017.

[15] I. Kerenidis and A. Prakash.
Quantum recommendation system.
In C. H. Papadimitrou, editor, *8th Innovations in Theoretical Computer Science Conference (ITCS 2017)*, pages 49:1–49:21. Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany, 2017.

References (cont.)

[16] Y. I. Manin.
Vychislimoe i nevychislimoe [Computable and Noncomputable] (in Russian). Sov. Radio. pp. 13–15. (Checked 30 November 2017).
http://www.worldcat.org/title/vychislimoe-i-nevychislimoe/oclc/11674220, 1980.

[17] C. Neill, P. Roushan, K. Kechedzhi, S. Boixo, S. V. Isakov, V. Smelyanskiy, R. Barends, B. Burkett, Y. Chen, Z. Chen, B. Chiaro, A. Dunsworth, A. Fowler, B. Foxen, R. Graff, E. Jeffrey, J. Kelly, E. Lucero, A. Megrant, J. Mutus, M. Neeley, C. Quintana, D. Sank, A. Vainsencher, J. Wenner, T. C. White, H. Neven, and J. M. Martinis.
A blueprint for demonstrating quantum supremacy with superconducting qubits.

References (cont.)

arXiv:1709.06678 [quant-ph].

[18] E. Pednault, J. A. Gunnels, G. Nannicini, L. Horesh, T. Magerlein, E. Solomonik, and R. Wisnieff.
Breaking the 49-qubit barrier in the simulation of quantum circuits.
https://arxiv.org/abs/1710.05867, October 2017.

[19] J. Preskill.
Quantum computing and the entanglement frontier.
In H. M. Gross, D. and A. Sevrin, editors, *The Theory of the Quantum World*, pages 63–80, Singapore, November 10 2012. World Scientific Publishing.
arXiv:1203.5813 [quant-ph].

References (cont.)

[20] P. W. Shor.
Algorithms for quantum computation: discrete logarithms and factoring.
In *Proceedings of the 35th Annual Symposium of on Foundations of Computer Science, Santa Fe, NM, Nov. 20-22, 1994*. IEEE Computer Society Press, November 1994.
`arXiv:quant-ph/9508027`.

[21] E. Tang.
A quantum-inspired classical algorithm for recommendation systems.
`https://arxiv.org/pdf/1807.04271.pdf`, July 2018.