

# The Road to Quantum Computational Supremacy



Cristian S. Calude and Elena Calude

*This paper is dedicated to the memory of Jon Borwein (1951–2016) whose broad mathematical interests included also quantum computing.*

A hyper-fast quantum computer is the digital equivalent of a nuclear bomb; whoever possesses one will be able to shred any encryption and break any code in existence.<sup>1</sup> [50]

## 1 Fairy Tales or More Cautionary Tales?

Following the development of Shor's quantum algorithm [81] in 1994 and Grover's quantum algorithm [44] two years later, quantum computing was seen as a bright beacon in computer science, which led to a surge of theoretical and experimental results. The field captured the interest and imagination of the large public and media, and not surprisingly, unfounded claims about the power of quantum computing and its applications proliferated.

A certain degree of pessimism began to infiltrate when experimental groups floundered while attempting to control more than a handful of qubits. Recently, a broad wave of ambitious industry-led research programmes in quantum computing—driven

---

<sup>1</sup>A typical example of incorrect, largely spread, myth quoted from a recent mystery novel.

---

C. S. Calude (✉)

Department of Computer Science, University of Auckland, Private Bag 92019,  
Auckland, New Zealand  
e-mail: [c.calude@auckland.ac.nz](mailto:c.calude@auckland.ac.nz)

E. Calude

Institute of Natural and Computational Sciences, Massey University at Albany, Private Bag  
102-904 North Shore MSC, Auckland, New Zealand  
e-mail: [e.calude@massey.ac.nz](mailto:e.calude@massey.ac.nz)

© Springer Nature Switzerland AG 2020

D. H. Bailey et al. (eds.), *From Analysis to Visualization*,  
Springer Proceedings in Mathematics & Statistics 313,  
[https://doi.org/10.1007/978-3-030-36568-4\\_22](https://doi.org/10.1007/978-3-030-36568-4_22)

by D-Wave Systems,<sup>2</sup> the tech giants Google, IBM, Microsoft, Intel and start-ups like Rigetti Computing and Quantum Circuits Incorporated—has emerged<sup>3</sup> and bold claims about a future revolutionised by quantum computing are resurfacing.

Governments are also involved: phase 1 (2015–2019) £330 million of the UK government programme on quantum technologies [89] is rolling and the European Commission has announced a €1 billion initiative in quantum technology [39]. The European flagship quantum programme, whose explicit goal is to stimulate a “second quantum revolution”, aims to “build a universal quantum computer able to demonstrate the resolution of a problem that, with current techniques on a supercomputer, would take longer than the age of the universe” by 2035, [78]; see also Figure 1.

Undoubtedly, these programmes are extremely beneficial to the development of various quantum technologies, but are the claims about the future of quantum computing realistic? “We tend to be too optimistic about the short run, too pessimistic about the long run”, said recently Preskill [73]; see also [8, 85].

## 2 Quantum Algorithmics

First and foremost, *quantum computing cannot compute all partial functions a universal Turing machine can calculate because only total functions can be computed by quantum circuits* [13]. Consequently, quantum computing potential advantages could come only from faster than classical computations.

While Shor’s algorithm, Deutsch–Jozsa algorithm and various others in the “black-box” paradigm<sup>4</sup> are believed to provide an exponential speed-up over classical computers, this is far from the case in general. We said “believed” because the superiority of Shor’s quantum algorithm over classical ones is still an open problem and various techniques allowing efficient classical simulation of quantum algorithms have been successfully developed [6, 26, 43] even for some “black-box” quantum ones [5, 28, 51, 52].

In fact, since the introduction of Shor’s and Grover’s algorithms some twenty years ago, the development within the field of quantum algorithmics has been rather slow—see [76] for a global picture—and many of them are novel uses of a handful of core quantum algorithms. So, why are there so few quantum algorithms that offer speed-up over classical algorithms? Although written more than a decade ago, Shor’s article [82] is still actual:

---

<sup>2</sup>The company’s relatively steady progress in producing and selling the first series of D-Wave quantum computers has gone from 28 qubits in 2007 to more than 2,000 in their 2000Q™ System machine [35]. In September 2019, the 5,000-qubit D-Wave machine called “Advantage” has been delivered to the Los Alamos National Laboratory [90].

<sup>3</sup>Of course, the industry work is based and has continued the academic efforts, sometimes using successful experimentalists from academia, like Google does.

<sup>4</sup>Where access to a quantum black-box or “oracle” with certain structural properties is assumed.

# Quantum Technologies Timeline

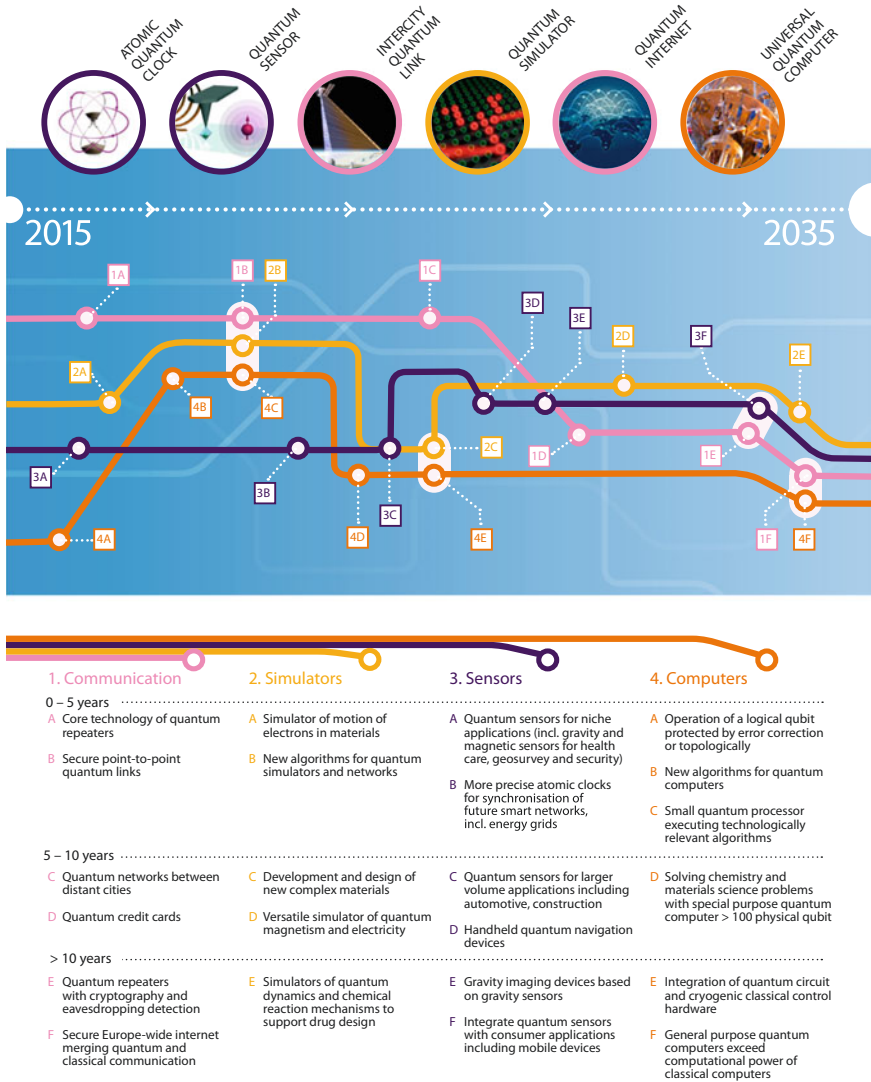


Fig. 1 Quantum timeline: 2015–2035 [78]

The first possible reason is that quantum computers operate in a manner so different from classical computers that our techniques for designing algorithms and our intuitions for understanding the process of computation no longer work. The second reason is that there really might be relatively few problems for which quantum computers can offer a substantial

speed-up over classical computers, and we may have already discovered many or all of the important techniques for constructing quantum algorithms.

Best quantum algorithms typically provide a quadratic or low-order polynomial speed-up [42]. Furthermore, there are pointers [1, 20] suggesting that quantum computers cannot offer more than a (perhaps small) polynomial advantage for NP-complete problems,<sup>5</sup> and such a speed-up would struggle to compete with the heuristic approaches commonly used to solve them in practice. However, even a polynomial-order speed-up could be of significant benefit for problems requiring exact solutions or for problems that can classically be solved in sub-exponential time, like the graph isomorphism problem (see [31]).

Grover's quantum algorithm [44] is an interesting example: access to an unsorted quantum database that can be queried with a quantum input is given, and asked if it contains a specific entry. Grover's algorithm offers a *provable* speed-up. However, the speed-up is not exponential and, more importantly, the problem it solves is far from being realistic: the cost of constructing the quantum database could negate any advantage of the algorithm, and in many classical scenarios one could do much better by simply creating (and maintaining) an ordered database. Using Grover's algorithm as a subroutine for solving problems in image processing is more efficient because the cost of preparing the quantum "database" can be spread out over several calls [59]; this strategy motivated a new hybrid quantum-classical paradigm for embedded quantum annealing algorithms [9]. Other applications are discussed in [66].

Quantum simulation, quantum-assisted optimisation and quantum sampling are believed to offer near-term quantum solutions to hard problems that may lead even to commercialisation [65].

### 3 What Is Quantum Computational Supremacy?

The quantum computational advantage for simulating quantum systems was first stated by Feynman in 1982, in one of the pioneering papers in quantum computing [41] (the other one was Manin [62]). What is the justification of Feynman's insight? According to the data processing inequality [16, 34], (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 [12]. Manin [62] and Feynman [41] have argued that a quantum computer might not need to have so much knowledge. This line of reasoning seemingly inspired Deutsch [37] to state

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

---

<sup>5</sup>Perhaps the most important class of "difficult computational problems" such as the well-known travelling salesman problem, which have applications in almost every area of science and beyond, from planning and logistics to microchip manufacturing.

A spectacular support for this postulate came from Shor’s 1994 polynomial factoring quantum algorithm [81] in spite of the fact that the problem whether factoring is in  $\mathbf{P}$  was, and still is, open. The belief that factoring integers is computationally hard<sup>6</sup> is essential for much of modern cryptography and computing security. In 2002, Hemaspaandra, Hemaspaandra and Zimand [48], improving results in [21, 83], showed that there are tasks on which polynomial-time quantum machines are exponentially faster almost everywhere than any classical—even bounded-error probabilistic—machine.

In 2011, the syntagm “quantum supremacy” was coined and discussed<sup>7</sup> by J. Preskill in his Rapporteur talk “Quantum Entanglement and Quantum Computing” [72] 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.

Recently, quantum supremacy was described in [22] 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.

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? Just as there is no current proof that  $\mathbf{P} \neq \mathbf{NP}$ —one of the important open problems in classical complexity theory—there is no mathematical proof for the Postulate of quantum computation; in fact, the Postulate is not amenable to a proof. The hypothesis  $\mathbf{P} \neq \mathbf{NP}$  can be used for deriving useful results; similarly, adopting assumptions in terms of both quantum physics and classical complexity theory—which can be justified heuristically or experimentally—can lead to precise statements which can be proved or disproved. The following two assumptions

**The postulate of noise:** Quantum systems are inherently noisy.

**The Extended Church–Turing Thesis:** A probabilistic Turing machine can efficiently simulate any realistic model of computation.

have been used by Kalai [53] to challenge the Postulate of quantum computation. Here “efficiently” means “with at most polynomial overhead”; the adjective “realistic” (or “reasonable” as an alternative) refers to a “physically realisable in principle”. It

<sup>6</sup>For results pointing to the opposite assumption see [6, 19, 26, 43, 68].

<sup>7</sup>The use of the word “supremacy”—which denotes “the state or condition of being superior to all others in authority”—was criticised in [91] because the syntagm “white supremacy” is associated with the racial segregation and discrimination of the apartheid regime of South Africa. Proposals like “quantum advantage” or “quantum superiority” have been discussed [77], but to date, none has gained ground.

is worth mentioning that these assumptions are themselves challengeable; see, for example, [22] for the Extended Church–Turing Thesis.

A quantum computational supremacy experiment has to prove both a lower bound and an upper bound. In Google’s proposed experiment—to be discussed in detail in Section 6—the upper bound is given by a quantum algorithm running on a quantum computer with 49 qubits<sup>8</sup>—a mathematical fact and an engineering artefact (the construction of the quantum machine); the lower bound is necessary for proving that no current classical computer can simulate the sampling in a reasonable time from the output distributions of pseudo-random quantum circuits.

Upper bounds are positive results while lower bounds are negative. Upper bounds are useful when we want to show that a problem can be solved by a “good” algorithm. But if we want to argue that no algorithm solving a problem can be better than a given one, or perhaps that some problem is so hard that we can’t possibly hope to find a good solution to it, we need lower bounds.

In mathematics and theoretical computer science, it is well known that negative results are more difficult to prove than positive ones. In classical computability theory, it is more difficult to prove incomputability than computability, and in complexity theory lower bounds are more difficult to prove than upper bounds [84]. The superiority of Shor’s quantum algorithm [81] is a prime example. A methodology for proving lower bounds in quantum computing is discussed in [45, pp. 144–149]. Sometimes unproved claims about the quantum superiority of a quantum algorithm have been shown to be incorrect: an example is the superiority of Deutsch’s quantum algorithm over any classical one, see [28, 37, 51].

Another issue is correctness: how do we know that the quantum computer solution is indeed correct—quantum computing is a probabilistic type of computation—if we can’t check it with a reliably tested classical computer? For a promising approach see [11, 25]. Meantime we note that even classical correctness is a very difficult problem. The Ackermann  $A$  function [10] is a singular example: computing the value of  $A(x, y)$  is prohibitively difficult because the function is computable but not primitive recursive, but testing the predicate  $A(x, y) = z$  is very easy [27].

Finally, the discussion about quantum 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 supremacy, if achieved, won’t make classical computing obsolete*. In fact, the hybrid approach combining quantum and classical computing, briefly mentioned in Section 2, could be a good strategy in solving some (many) difficult problems [9].

---

<sup>8</sup>A qubit is a 2-state quantum system. There are many ways to build qubits, hence not all qubits are equal. The magic number 49 (or 50) refers to qubits in the quantum circuit model which are more difficult to control than the qubits used by the D-Wave machine [29] (to embed a complete graph of  $N$  vertices in D-Wave hardware Chimera graph we need approximately  $N^2$  qubits, so 2,048 D-Wave qubits correspond to about fully connected 45 qubits) or the trapped atom qubits used by specialised quantum simulators [18, 93].

## 4 Criteria for Quantum Computational Supremacy

Harrow and Montanaro [46] have proposed a reasonable list of criteria for a quantum supremacy experiment. According to them, we need to have:

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, and
5. a verification method that can efficiently distinguish between the performances of the quantum algorithm from **any** classical competitor using the allowed resources.

Large integer factoring is a typical problem for a quantum supremacy experiment. Indeed, it is well defined, it has huge practical importance, there are efficient quantum algorithms solving it (Shor's algorithm and variants [19, 81]), the complexity-theoretic assumption is that no classical algorithm can factor essentially faster than the current ones and the solution is quickly verifiable. This seems an almost ideal candidate, except for (a) the strong complexity-theoretic assumption [68] and (b) the lack of a near-term hardware running such a quantum algorithm for sufficiently large integers (say a 2,048-bit number), see [46]. A possible solution for (b) could be a hybrid (quassical) approach [9].

Harrow and Montanaro [46] state that “we do not require that the computational task<sup>9</sup> is of practical interest”. This is a strong assumption in itself which is adequate only for a foundational study.

Table 1 in [46], p. 205, lists seven plausible approaches to quantum computational supremacy: factoring, single photons passing through a linear-optical network (boson sampling), quantum circuits on many qubits and only a few layers of quantum gates (low-depth circuits), random quantum circuits containing gates that either all commute or do not commute (instantaneous quantum polynomial time, IQP), quantum approximate optimisation algorithms (QAOA), quantum adiabatic optimisation and quantum analogue simulation. These approaches are then evaluated according to usefulness, assumption implying no classical simulation and difficulties to solve on a quantum computer and to verify. Factoring is the only useful problem, simulation is often useful, adiabatic optimisation could be useful and the remaining three problems do not seem to be useful. Factoring is the hardest to solve on a quantum computer, boson sampling, adiabatic optimisation and analogue simulation are easy and the remaining three are moderately difficult. Only factoring is easy to verify. The complexity-theoretic assumptions are generally very strong, assessing their plausibility is a very difficult task and, generally, conclusions are rather controversial. A detailed complexity-theoretic analysis of various possible quantum supremacy experiments can be found in [4]. The papers [4, 46] are exceptionally singular in offering balanced and more formal analyses.

---

<sup>9</sup>Their formulation for what we call a computational problem.

## 5 Is the Quest for Quantum Computational Supremacy Worthwhile?

Apart publicity and marketing, is the effort of demonstrating the quantum computational supremacy justified? What are the (possible) benefits? Can the claim of quantum computational supremacy be falsified?

We will start with the second question. The main benefit could be foundational and philosophical: a better understanding of the nature of quantum mechanics through its computational capabilities.<sup>10</sup> Such a gain will boost the efforts of not only building larger scale quantum computers but also, and, more importantly, developing new and powerful algorithms for these machines possibly leading to solutions to important practical problems. From this perspective, the answer to the first question is affirmative.

Let us examine closer the foundational gain. A successful quantum supremacy experiment could be a complement to Bell experiment: the latter refuted local hidden models of quantum mechanics, while the former *seems* to invalidate the Extended Church–Turing Thesis [92]. The paper [46] discusses the advantages of a successful quantum supremacy experiment, even one that barely surpasses any classical competitor, illustrated with hard-to-simulate classical systems like protein folding or fluid dynamics. Here we suggest a different perspective which motivated the tentative formulation above. The Extended Church–Turing Thesis—which incidentally has nothing to do with either Church nor Turing—is a foundational principle of classical complexity theory which ensures that the polynomial-time class  $\mathbf{P}$  is well defined.<sup>11</sup> The Thesis places strong constraints, one of them being that *the model of computation is digital*. For example, analogue computers are excluded because they assume infinite arithmetic precision. Furthermore, it is known that an infinite precision calculator with operations  $+$ ,  $\times$ ,  $=0?$ , can factor integers in polynomial time (see [80, 87]).<sup>12</sup> But, are quantum computers a “reasonable” model of computation? Are quantum systems digital? At first glance quantum computers (and, more generally, quantum systems) appear to be analogue devices, since a quantum gate is described by a unitary transformation, specified by complex numbers; a more in-depth analysis is still required.

What does it take to refute the claim of quantum computational supremacy? This amounts to prove that any computation performed by any quantum computer can be simulated by a classical machine in polynomial time, a weaker form of the Extended Church–Turing Thesis. This statement cannot be proved for the same reasons the

---

<sup>10</sup>A beautiful result regarding the computational power of algorithmic random strings was proved in [33]. This was used as a test of quality for quantum randomness in [30].

<sup>11</sup>The Thesis equating feasible computation with polynomial-time computation has significantly less “evidence” than the Church–Turing Thesis; in fact, according to [36], it “lacks evidence”.

<sup>12</sup>Feynman’s 1982 intuition (Section 3) was substantiated in [61] by running a quantum analogue emulation. The quantum version of analogue computers, continuous-variable quantum computers, have been theoretically studied [54]; the model in [86] offers a universal gate set for both qubits and continuous variables.



Church–Turing Thesis cannot be proved: obviously, they may be disproved. The paper [69] presents efficient classical boson sampling algorithms and a theoretical analysis of the possibility of scaling boson sampling experiments; it concludes that “near-term quantum supremacy via boson sampling is unlikely”.

## 6 Google Quantum Computational Supremacy

In the landscape of various proposals for quantum computational supremacy experiments, Google’s approach is not only well documented, but had chances to be completed really very soon [67]. 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.<sup>13</sup> This computational task is difficult because as the grid size increases, the *memory needed to store everything increases classically exponentially*.<sup>14</sup> 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 [40], to simulate the behaviour of the grid of 42 qubits. 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.

The abstract of the main paper describing the theory behind the experiment [22] reads<sup>15</sup>:

A critical question for the field of quantum computing in the near future is whether quantum devices without error correction can perform a well-defined computational task beyond the capabilities of state-of-the-art classical computers, achieving so-called quantum supremacy. *We study the task of sampling from the output distributions of (pseudo-)random quantum circuits, a natural task for benchmarking quantum computers. Crucially, sampling this distribution classically requires a direct numerical simulation of the circuit, with computational cost exponential in the number of qubits.* This requirement is typical of chaotic systems. *We extend previous results in computational complexity to argue more formally that this sampling task must take exponential time in a classical computer.* We study the convergence to the chaotic regime using extensive supercomputer simulations, modelling circuits with up to 42 qubits—the largest quantum circuits simulated to date for a computational task that approaches quantum supremacy. We argue that while chaotic states are extremely sensitive to errors, quantum supremacy can be achieved in the near-term with approximately fifty superconducting qubits. We introduce cross entropy as a useful benchmark of quantum circuits which approximates the circuit fidelity. We show that the cross entropy can be efficiently

---

<sup>13</sup>For another promising quantum simulation see [32].

<sup>14</sup>But, do we *really need* to store everything?

<sup>15</sup>Our emphasis.

measured when circuit simulations are available. *Beyond the classically tractable regime, the cross entropy can be extrapolated and compared with theoretical estimates of circuit fidelity to define a practical quantum supremacy test.*

Google was on track to deliver before the end of the year. Alan Ho, an engineer in Google’s quantum AI lab, revealed the company’s progress at a quantum computing conference in Munich, Germany. According to [79]:

His team is currently working with a 20-qubit system that has a “two-qubit fidelity” of 99.5 per cent—a measure of how error-prone the processor is, with a higher rating equating to fewer errors. For quantum supremacy, Google will need to build a 49-qubit system with a two-qubit fidelity of at least 99.7 per cent. Ho is confident his team will deliver this system by the end of this year.

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? The article [22] 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”. Indeed, they do not claim to have a proof for the lower bound, just a “better formal argument”. Their argument is reinforced later in the introduction:

State-of-the-art supercomputers cannot simulate universal random circuits of sufficient depth in a 2D lattice of approximately  $7 \times 7$  qubits with any known algorithm and significant fidelity.

Does Google’s experiment satisfy the criteria discussed in Section 4? The problem is well defined, albeit a simulation, not a computational problem,<sup>16</sup> the quantum algorithm solving the problem will run on a quantum computer—promised to be built before the end of 2017<sup>17</sup>—capable of dealing with noise and imperfections, the classical competitor would be allowed a reasonable amount of computational resources and there is a plausible verification. The weakest part comes from the complexity-theoretic assumption [22]:

**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. [67]

---

<sup>16</sup>One could argue that the task itself is rather uninteresting and without obvious applications. Indeed, all the time nature is doing quantum “things” that we don’t know how to solve classically. For example, the structure of atoms can in general only be determined experimentally, but nature manages it with near-perfect fidelity. If Google achieved the goal—an undisputable big technical feat—the meaning of the achieved “supremacy” could still be debatable.

<sup>17</sup>When pressed for an update, a spokesperson [for Google] recently said that ‘we hope to announce results as soon as we can, but we’re going through all the detailed work to ensure we have a solid result before we announce’. Reference [15], 24 January 2018. The goal was not reached as of 30 September 2019.

## 7 IBM Challenge

The Memory assumption is crucial for the proposed lower bound, and, indeed, this was confirmed very soon. The paper [71] proved that a supercomputer can simulate sampling from random circuits with low depth (layers of gates) of up to 56 qubits.

With the current rate of progress in quantum computing technologies, 50-qubit systems will soon become a reality. To assess, refine and advance the design and control of these devices, one needs a means to test and evaluate their fidelity. This in turn requires the capability of computing ideal quantum state amplitudes for devices of such sizes and larger. In this study, we present a new approach for this task that significantly extends the boundaries of what can be classically computed. We demonstrate our method by presenting results obtained from a calculation of the complete set of output amplitudes of a universal random circuit with depth 27 in a 2D lattice of  $7 \times 7$  qubits. We further present results obtained by calculating an arbitrarily selected slice of 237 amplitudes of a universal random circuit with depth 23 in a 2D lattice of  $8 \times 7$  qubits. Such calculations were previously thought to be impossible due to impracticable memory requirements. *Using the methods presented in this paper, the above simulations required 4.5 and 3.0 TB of memory, respectively, to store calculations, which is well within the limits of existing classical computers.*<sup>18</sup>

Better results have been quickly announced, see, for example, [23]. 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 [49].

## 8 Latest Developments

At 2018 Consumer Electronics Show in Las Vegas, Intel CEO Brian Krzanich reported, “the successful design, fabrication and delivery of a 49-qubit superconducting quantum test chip” [56]. The 49-qubit superconducting quantum test chip is called “Tangle Lake” after a chain of lakes in Alaska known for extreme cold temperatures. At the event, Mike Mayberry, managing director of Intel Labs said: “We expect it will be five to seven years before the industry gets to tackling engineering-scale problems, and it will likely require 1 million or more qubits to achieve commercial relevance”. In [74] J. Preskill aptly said: “Quantum computers with 50-100 qubits may be able to perform tasks which surpass the capabilities of today’s classical digital computers, but noise in quantum gates will limit the size of quantum circuits that can be executed reliably. ...Quantum technologists should continue to strive for more accurate quantum gates and, eventually, fully fault-tolerant quantum computing”. Jay Gambetta, from IBM Thomas J. Watson Research Center believes that “a universal fault-tolerant quantum computer, which has to use logical qubits, is still a long way off”, [15]. E. Tang (then an 18-year-old undergraduate student at UT Austin) has recently proved [88] that classical computers can solve the “recommendation

---

<sup>18</sup>Our emphasis.

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 and the quantum solution in [55] was hailed as one of the first examples in *quantum machine learning and big data* that would be unlikely to be done classically... In October 2018, Bravyi, Gosset and König [24] have presented an argument—based on non-locality—which suggests that a certain quantum algorithm requiring only constant-depth quantum circuits can be a suitable candidate for showing quantum computational supremacy.

## 9 Closing Remarks

Recall that the computational power of quantum computing is less than that of a universal Turing machine [13], so quantum computing potential advantages could come only from faster than classical computations.

Does the paper [71] destroy the quest for quantum computational supremacy? Is there any incompatibility between the classical simulation reported in [71] and the IBM statement cited at the end of Section 7? Tentatively we answer with no to both questions. The following paragraph [2] is relevant:

This paper<sup>19</sup> 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, with sampling-based quantum supremacy, was always to target the “sweet spot”, which we estimated at around 50 qubits, where classical simulation is still possible, but it’s clearly orders of magnitude more expensive than doing the experiment itself. If you like, the goal is to get as far as you can up the mountain of exponentiality, conditioned on people still being able to see you from the base. Why? Because you can. Because it’s there.<sup>20</sup> Because it challenges those who think quantum computing will never scale: explain this, punks! But there’s no point unless you can verify the result.

Here are a few more lessons. The first is not to underestimate the importance of mathematical modelling and proving (lower bounds, in particular). As the title of the blog [2] says, “ $2^n$  is exponential, but  $2^{50}$  is finite”, the difference between exponential and polynomial running times is asymptotic and in some concrete cases it is a challenge to find finite evidence for the difference. Furthermore, proving that a problem is in  $\mathbf{P}$  itself is not a guarantee that there is an algorithm in  $\mathbf{P}$  that is practically useful: primality has been known to be in  $\mathbf{P}$  since 2002, but all known deterministic algorithms are too slow in practice, so probabilistic tests of primality continue to be used.

---

<sup>19</sup>That is, [71].

<sup>20</sup>“It is not the mountain we conquer but ourselves”, as Edmund Hillary aptly said.

Second, 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.

Third, 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, [5, 7, 28, 51, 52, 88], have been directly inspired by the quantum work.

Finally, the race quantum versus classical is running so fast—a sample is given by the references posted/published since October 2017, the month when the paper [71] was posted—that by the time this paper is printed some results discussed here could be obsolete. One fact is certain: as of 30 September 2019, the quantum computational supremacy was not (yet?) demonstrated.

## 10 P.S. Quantum Desperation

Two<sup>21</sup> important articles have been published in quantum computing on 23–24 October 2019. The first, written by a Google team and published in the prestigious journal *Nature* [14], announces the experimental realisation of quantum supremacy with a programmable machine with 53 qubits:

*Our Sycamore processor takes about 200 seconds to sample one instance of a quantum circuit a million times our benchmarks currently indicate that the equivalent task for a state-of-the-art classical supercomputer would take approximately 10,000 years. This dramatic increase in speed compared to all known classical algorithms is an experimental realization of quantum supremacy for this specific computational task, heralding a much-anticipated computing paradigm.*

This paper has sparked a huge interest not only in the quantum community but the whole world. Announcements and comments have instantly appeared in prestigious science magazines like *New Scientist*, “Google reigns supreme” and “It’s official: Google has achieved quantum supremacy”, major newspapers like *The Washington Post*, “Bravo for Google’s ‘quantum supremacy.’ Here’s what needs to happen next” and worldwide broadcasters like *BBC*, “Google claims ‘quantum supremacy’ for computer”. Not everybody was convinced even at an intuitive level of understanding: *Reuters*: “Google unveils quantum computer breakthrough; critics say wait a qubit”, *The Financial Post*: “Google claims ‘quantum supremacy’ with quantum computer breakthrough, but skeptics don’t agree”, to cite only two sources.

The inventor of the concept of quantum supremacy is also cautious [75]:

The Google team has apparently demonstrated that it’s now possible to build a quantum machine that’s large enough and accurate enough to solve a problem we could not solve before...

---

<sup>21</sup>Section 10 added on January 24, 2020.

The second paper, written by an IBM team, was posted in the archive [70] and is summarised as follows:

We argue that an ideal simulation of the same task can be performed on a classical system in 2.5 days and with far greater fidelity. This is in fact a conservative, worst-case estimate, and we expect that with additional refinements the classical cost of the simulation can be further reduced.

Could both reports be correct?

Interestingly, immediately after publishing the paper [14] *Nature* published also an anonymous editorial [38] including the following significant paragraphs:

As the world digests this achievement – including the claim that some quantum computational tasks are beyond supercomputers – it is too early to say whether supremacy represents a new dawn for information technology. ... At the very least, quantum computers as a routine part of life are likely to be decades or more into the future.

...

Instead of proceeding with caution, a quantum gold rush is under way, with investors joining governments and companies to pour large sums of money into developing quantum technologies. Unrealistic expectations are being fuelled that powerful general-purpose quantum computers could soon be on the horizon. Such misguided optimism could be dangerous for the future of this still-fledgling field.

Undoubtedly, Google’s technological achievement is remarkable, and it helps building the case for a possible quantum supremacy by achieving a high upper bound. *The real problem is that there is no formal argument for the lower bound*, see Section 4, the supplementary material to [14] and the mathematical discussion in [60]. Furthermore, *it is not for IBM<sup>22</sup> or anybody else to disprove the lower bound claimed by Google<sup>23</sup>: the onus is on Google to prove it.*

Where does “desperation” in the title of this section come from? As noted in [47]

It has taken Google 13 years<sup>24</sup> to get this far. Without a profitable device, research could dry up. It happened to Apollo, programme. It has happened at times with AI.

There are very few agreements in quantum computing, but one is that the area has been showered with money in recent years but has delivered very little practical solutions. How long can the flow of money continue? There is a sense that the answer is not too encouraging, so something had/has to be done. Downgrading the mathematical notion of quantum speed-up<sup>25</sup> to quantum supremacy was meant to help, but not without a price. The origin, merit and pitfalls of this concept have been recently discussed by its inventor J. Preskill in a thoughtful article in *Quanta Magazine* [75]. One main objection pointed there is that the “word exacerbates the already overhyped

---

<sup>22</sup>Although they did before [71].

<sup>23</sup>Comments like “Tellingly, not even IBM thinks the simulation would be especially easy – nor, as of this writing, has IBM actually carried it out”. Reference [3] are irrelevant.

<sup>24</sup>And a tone of money (our comment).

<sup>25</sup>Note that Grover’s quantum algorithm [44] *proved a quantum speed-up* 25 years ago, yet insufficient to justify quantum computing practicality.

reporting on the status of quantum technology”. This was echoed also in the IBM paper [70]:

For the reasons stated above, and since we already have ample evidence that the term “quantum supremacy” is being broadly misinterpreted and causing ever growing amounts of confusion, we urge the community to treat claims that, for the first time, a quantum computer did something that a classical computer cannot with a large dose of skepticism due to the complicated nature of benchmarking an appropriate metric.

The current tendency seems to move the arguments from the mathematics and science to media propaganda.

Google’s demonstration should give these skeptics pause. To all appearances, a 53-qubit device really was able to harness 9 quadrillion amplitudes for computation, surpassing (albeit for a special, useless task) all the supercomputers on earth. Quantum mechanics worked: an outcome that’s at once expected and mind-boggling, conservative and radical. [3]

Interestingly, this is not a new tactic in settling quantum mechanics controversies and a most prominent example is the famous Einstein–Bohr disagreement on the Copenhagen interpretation. Einstein view [17, p. 29]:

The theory reminds me a little of the system of delusions of an exceedingly intelligent paranoiac.

opposed Bohr’s “shut up and calculate!” attitude (using Mermin’s expression [64]). According to Lakatos [58, pp. 59–60], [57, p. 105]:

After 1925, Bohr and his associates introduced a new and unprecedented lowering of critical standards for scientific theories. This led to a defeat of reason within modern physics and to an anarchist cult of incomprehensible chaos.

Recently, there is an apparent change [63, p. 9]:

while Einstein won and would continue to win all the logical battles, Bohr was decisively winning the propaganda war.

Let’s hope that in quantum computing mathematics and science will prevail over propaganda.

**Acknowledgements** We thank N. Allen for fruitful discussions and suggestions, specifically for insight on Feynman’s paper [41], and R. Brent, R. Goyal, L. Hemaspaandra, K. Pudenz, R. Hua, K. Svozil and an anonymous referee for excellent critical comments and suggestions. This work has been supported in part by the Quantum Computing Research Initiatives at Lockheed Martin.

## References

1. Aaronson, S.: The limits of quantum. *Sci. Am.* 62–69 (2008)
2. Aaronson, S.: Shtetl-optimized  $-2^n$  is exponential, but  $2^{50}$  is finite (2017). <https://www.scottaaronson.com/blog/?p=3512>

3. Aaronson, S.: Why Google's quantum supremacy milestone matters. *The New York Times* (2019). <https://www.nytimes.com/2019/10/30/opinion/google-quantum-computer-sycamore.html>
4. Aaronson, S., Chen, L.: Complexity-theoretic foundations of quantum supremacy experiments. Technical report No. 200, Electronic Colloquium on Computational Complexity (2016)
5. Abbott, A.A.: The Deutsch-Jozsa problem: De-quantisation and entanglement. *Nat. Comput.* **11**(1), 3–11 (2011)
6. Abbott, A.A.: De-quantisation of the quantum Fourier transform. *Appl. Math. Comput.* **291**(1), 3–13 (2012)
7. Abbott, A.A., Calude, C.S.: Understanding the quantum computational speed-up via de-quantisation. *EPTCS* **26**, 1–12 (2010)
8. Abbott, A.A., Calude, C.S.: Limits of quantum computing: a sceptic's view (presented by Jon Borwein). *Quantum for quants* (2016). <http://www.quantumforquants.org/quantum-computing/limits-of-quantum-computing/>
9. Abbott, A.A., Calude, C.S., Dinneen, M.J., Hua, R.: A hybrid quantum-classical paradigm to mitigate embedding costs in quantum annealing. *Int. J. Quantum Inf.* **1950042**, 40 (2019)
10. Ackermann, W.: On Hilbert's construction of the real numbers. *Math. Ann.* **99**, 118 (1928)
11. Aharonov, D., Ben-Or, M., Eban, E., Mahadev, U.: Interactive proofs for quantum computations (2017). <https://arxiv.org/abs/1704.04487>
12. Allen, N.: Email to C. S. Calude. Accessed 19 Nov 2017
13. Allen, E.H., Calude, C.S.: Quassical computing. *Int. J. Unconv. Comput.* **14**, 43–57 (2018)
14. Arute, F., Arya, K., Babbush, R., Bacon, D., Bardin, J.C., Barends, R., Biswas, R., Boixo, S., Brandao, F.G.S.L., Buell, D.A., Burkett, B., Chen, Y., Chen, Z., Chiaro, B., Collins, R., Courtney, W., Dunsworth, A., Farhi, E., Foxen, B., Fowler, A., Gidney, C., Giustina, M., Graff, R., Guerin, K., Habegger, S., Harrigan, M.P., Hartmann, M.J., Ho, A., Hoffmann, M., Huang, T., Humble, T.S., Isakov, S.V., Jeffrey, E., Jiang, Z., Kafri, D., Kechedzhi, K., Kelly, J., Klimov, P.V., Knysh, S., Korotkov, A., Kostritsa, F., Landhuis, D., Lindmark, M., Lucero, E., Lyakh, D., Mandrá, S., McClean, J.R., McEwen, M., Megrant, A., Mi, X., Michielsen, K., Mohseni, M., Mutus, J., Naaman, O., Neeley, M., Neill, C., Niu, M.Y., Ostby, E., Petukhov, A., Platt, J.C., Quintana, C., Rieffel, E.G., Roushan, P., Rubin, N.C., Sank, D., Satzinger, K.J., Smelyanskiy, V., Sung, K.J., Trevithick, M.D., Vainsencher, A., Villalonga, B., White, T., Yao, Z.J., Yeh, P., Zalcman, A., Neven, H., Martinis, J.M.: Quantum supremacy using a programmable superconducting processor. *Nature* **574**, 505–510 (2019)
15. Ball, P.: The era of quantum computing is here. *Outlook: Cloudy*, Quanta Magazine (2018). <https://www.quantamagazine.org/the-era-of-quantum-computing-is-here-outlook-cloudy-20180124>
16. Beaudry, N.J., Renner, R.: An intuitive proof of the data processing inequality. *Quantum Inf. Comput.* **12**(5–6), 432–441 (2012)
17. Becker, A.: *What Is Real? The Unfinished Quest for the Meaning of Quantum Physics*. Basic Books, New York (2018)
18. Bernien, H., Schwartz, S., Keesling, A., Levine, H., Omran, A., Pichler, H., Choi, S., Zibrov, A.S., Endres, M., Greiner, M., Vuletić, V., Lukin, M.D.: Probing many-body dynamics on a 51-atom quantum simulator. *Nature* **551**, 579, EP –, 11 (2017)
19. Bernstein, D.J., Heninger, N., Lou, P., Valenta, L.: Post-quantum RSA (2017). <https://cr.ypt.to/papers/pqrsa-20170419.pdf>
20. Bernstein, E., Vazirani, U.: Quantum complexity theory. In: *Proceedings of the 25th Annual ACM Symposium on Theory of Computing*, San Diego, California, 16–18 May 1993, pp. 11–20. ACM Press (1993)
21. Berthiaume, A., Brassard, G.: Oracle quantum computing. *J. Mod. Opt.* **41**, 195–199 (1992)
22. Boixo, S., Isakov, S.V., Smelyanskiy, V.N., Babbush, R., Ding, N., Jiang, Z., Bremner, M.J., Martinis, J.M., Neven, H.: Characterizing quantum supremacy in near-term devices (2017). [arXiv:1608.00263](https://arxiv.org/abs/1608.00263) [quant-ph]
23. Boixo, S., Isakov, S.V., Smelyanskiy, V.N., Neven, H.: Simulation of low-depth quantum circuits as complex undirected graphical models (2018). <https://arxiv.org/pdf/1712.05384.pdf>



24. Bravyi, S., Gosset, D., König, R.: Quantum advantage with shallow circuits. *Science* **362**, 308–311 (2018)
25. Broadbent, A.: How to verify a quantum computation. *Theory Comput.* **14**, 1–37 (2018)
26. Browne, D.E.: Efficient classical simulation of the quantum Fourier transform. *New J. Phys.* **9**(5), 146 (2007)
27. Calude, C.: Super-exponentials nonprimitive recursive, but rudimentary. *Inf. Process. Lett.* **25**(5), 311–316 (1987)
28. Calude, C.S.: De-quantizing the solution of Deutsch’s problem. *Int. J. Quantum Inf.* **5**(3), 409–415 (2007)
29. Calude, C.S., Calude, E., Dinneen, M.J.: Adiabatic quantum computing challenges. *ACM SIGACT News* **46**(1), 40–61 (2015)
30. Calude, C.S., Dinneen, M.J., Dumitrescu, M., Svozil, K.: Experimental evidence of quantum randomness incomputability. *Phys. Rev. A* **82**(2), 022102 (2010)
31. Calude, C.S., Dinneen, M.J., Hua, R.: QUBO formulations for the graph isomorphism problem and related problems. *Theor. Comput. Sci.* 1950042–40 (2019). <https://doi.org/10.1142/S0219749919500424>
32. Campbell, E.: Random compiler for fast Hamiltonian simulation. *Phys. Rev. Lett.* **123**, 070503 (2019)
33. Chaitin, G.J., Schwartz, J.T.: A note on Monte Carlo primality tests and algorithmic information theory. *Commun. Pure Appl. Math.* **31**(4), 521–527 (1978)
34. Cover, T.M., Thomas, J.A.: *Elements of Information Theory*. Wiley, New York (1991)
35. D-Wave Systems (2017). <https://www.dwavesys.com/d-wave-two-syste>
36. Davis, M.: Interview with Martin Davis. *Not. Am. Math. Soc.* **55**(560–571) (2008)
37. Deutsch, D.: Quantum theory, the Church-Turing principle and the universal quantum computer. *Proc. R. Soc. Lond. Ser. A Math. Phys. Sci* (1934–1990) **400**(1818), 97–117 (1985)
38. Editorial: A precarious milestone for quantum computing will suffer if supremacy is overhyped. Everyday quantum computers are still decades away. *Nature* **574**, 453–454 (2019)
39. European flagship quantum programme (2017)
40. Edison supercomputer in TOP 500 ranking (2017). <https://www.top500.org/list/2017/06/?page=1>
41. Feynman, R.P.: Simulating physics with computers. *Int. J. Theor. Phys.* **21**, 467–488 (1982)
42. Fürer, M.: Solving NP-Complete problems with quantum search. In: Laber, E.S., Bornstein, C., Nogueira, L.T., Faria, L. (eds.) *LATIN 2008: Theoretical Informatics*. LNCS, vol. 4957, pp. 784–792. Springer, Berlin (2008)
43. Griffiths, R., Niu, C.: Semiclassical Fourier transform for quantum computation. *Phys. Rev. Lett.* **76**(17), 3228–3231 (1996)
44. Grover, L.K.: A fast quantum mechanical algorithm for database search. In: *Proceedings of the Twenty-Eighth Annual ACM Symposium on the Theory of Computing*, pp. 212–219. ACM Press (1996)
45. Gruska, J.: *Quantum Computing*. McGraw-Hill, London (1999)
46. Harrow, A.W., Montanaro, A.: Quantum computational supremacy. *Nature* **549**(7671), 203–209 (2017)
47. Havean, D.: Beware quantum winter. Google’s quantum breakthrough is the first step on a long road. Let’s make sure we don’t stumble. *New Scientist*, p. 21. Accessed 2 Nov 2019
48. Hemaspaandra, E., Hemaspaandra, L.A., Zimand, M.: Almost-everywhere superiority for quantum polynomial time. *Inf. Comput.* **175**(2), 171–181 (2002)
49. IBM builds 50-qubit quantum computer (2017). <http://techvibesnow.com/ibm-builds-50-qubit-quantum-computer/>
50. Ignatius, D.: *The Quantum Spy*. W. W. Norton, New York (2018)
51. Johansson, N., Larsson, J.-Å.: Efficient classical simulation of the Deutsch-Jozsa and Simon’s algorithms. *Quantum Inf. Process.* **16**(9), 233 (2017)
52. Johansson, N., Larsson, J.-Å.: Quantum simulation logic, oracles, and the quantum advantage. *Entropy* **21**(8), 800 (2019)

53. Kalai, G.: How quantum computers fail: quantum codes, correlations in physical systems, and noise accumulation (2011). [arXiv:1106.0485](https://arxiv.org/abs/1106.0485) [quant-ph]
54. Kendon, V.M., Nemoto, K., Munro, W.J.: Quantum analogue computing. *Philos. Trans. R. Soc. Lond. A: Math. Phys. Eng. Sci.* **368**(1924), 3609–3620 (2010)
55. Kerenidis, I., Prakash, A.: Quantum recommendation system. In: Papadimitrou, C.H. (ed.) 8th Innovations in Theoretical Computer Science Conference (ITCS 2017), pp. 49:1–49:21. Dagstuhl Publishing, Germany, Schloss Dagstuhl - Leibniz-Zentrum für Informatik (2017)
56. Krzanich, B.: 2018 CES: Intel advances quantum and neuromorphic computing research (2018). <https://newsroom.intel.com/news/intel-advances-quantum-neuromorphic-computing-research/>
57. Lakatos, I.: Falsification and the methodology of scientific research programmes. In: *Can Theories be Refuted?*, pp. 59–60. Springer, Dordrecht (1976)
58. Lakatos, I.: Falsification and the methodology of scientific research programmes. In: *The Methodology of Scientific Research Programmes. Philosophical Papers Volume 1*. Cambridge University Press, Cambridge (1978). Online publication (2012)
59. Lanzagorta, M., Uhlmann, J.K.: Hybrid quantum-classical computing with applications to computer graphics. In: *ACM SIGGRAPH 2005 Courses, SIGGRAPH '05*. ACM, New York (2005)
60. Lipton, R.J., Regan, K.W.: Quantum supremacy at last? <https://rjlipton.wordpress.com/2019/10/27/quantum-supremacy-at-last/>. Accessed 27 Oct 2019
61. Lloyd, S.: Universal quantum simulators. *Science* **273**(5278), 1073–1078 (1996)
62. Manin, Y.I.: Vychislimoe i nevychislimoe [Computable and Noncomputable] (in Russian). *Sov. Radio*. 13–15 (1980). (Last accessed 30 Nov 2017). <http://www.worldcat.org/title/vychislimoe-i-nevychislimoe/oclc/11674220>
63. Maudlin, T.: The defeat of reason. *Boston Rev.* (2018). <http://bostonreview.net/science-nature-philosophy-religion/tim-maudlin-defeat-reason>
64. Mermin, N.D.: What is wrong with this pillow? *Phys. Today* **42**(4), 9 (1989)
65. Mohseni, M., Read, P., Neven, H., Boixo, S., Denchevand, V., Babbushand, R., Fowler, A., Smelyanskiy, V., Martinis, J.: Commercialize early quantum technologies. *Nature* **543**, 171–174 (2017)
66. Montanaro, A.: Quantum algorithms: an overview. *Npj Quantum Inf.* **2**, 15023, EP–, 01 (2016)
67. Neill, C., Roushan, P., Kechedzhi, K., Boixo, S., Isakov, S.V., Smelyanskiy, V., Barends, R., Burkett, B., Chen, Y., Chen, Z., Chiaro, B., Dunsworth, A., Fowler, A., Foxen, B., Graff, R., Jeffrey, E., Kelly, J., Lucero, E., Megrant, A., Mutus, J., Neeley, M., Quintana, C., Sank, D., Vainsencher, A., Wenner, J., White, T.C., Neven, H., Martinis, J.M.: A blueprint for demonstrating quantum supremacy with superconducting qubits. [arXiv:1709.06678](https://arxiv.org/abs/1709.06678) [quant-ph]
68. Nene, M.J., Upadhyay, G.: Shor’s algorithm for quantum factoring. In: Choudhary, R.K., Mandal, J.K., Auluck, N., Nagarajaram, H.A. (eds.) *Advanced Computing and Communication Technologies: Proceedings of the 9th ICACCT, 2015*, pp. 325–331. Springer Singapore, Singapore (2016)
69. Neville, A., Sparrow, C., Clifford, R., Johnston, E., Birchall, P.M., Montanaro, A., Neville, A.L.A., Sparrow, C., Clifford, R., Johnston, E., Birchall1, P.M., Montanaro4, A., Laing, A.: No imminent quantum supremacy by boson sampling (2017). <https://arxiv.org/pdf/1705.00686.pdf>
70. Pednault, E., Gambetta, J.: On “Quantum Supremacy”. <https://www.ibm.com/blogs/research/2019/10/on-quantum-supremacy/>. Accessed 24 Oct 2019
71. Pednault, E., Gunnels, J.A., Nannicini, G., Horesh, L., Magerlein, T., Solomonik, E., Wisnieff, R.: Breaking the 49-qubit barrier in the simulation of quantum circuits (2017). <https://arxiv.org/abs/1710.05867>
72. Preskill, J.: Quantum computing and the entanglement frontier. In: Gross, D., Henneaux, M., Sevrin, A. (eds.) *The Theory of the Quantum World*, pp. 63–80. World Scientific Publishing, Singapore (2012). [arXiv:1203.5813](https://arxiv.org/abs/1203.5813) [quant-ph]
73. Prreskill, J.: BES Roundtable on quantum computing opportunities in chemical and materials sciences. [http://www.theory.caltech.edu/~preskill/talks/DOE\\_BES\\_2017\\_Preskill.pdf](http://www.theory.caltech.edu/~preskill/talks/DOE_BES_2017_Preskill.pdf). Accessed 31 Oct 2017

74. Preskill, J.: Quantum computing in the NISQ era and beyond (2018). <https://arxiv.org/abs/1801.00862>
75. Preskill, J.: Why I Called It ‘Quantum Supremacy’ (2019). <https://www.quantamagazine.org/john-preskill-explains-quantum-supremacy-20191002/>
76. Quantum algorithm zoo (2017). <http://math.nist.gov/quantum/zoo/>
77. Quantum advantage. The quantum pontiff (2017). <http://dabacon.org/pontiff/?p=11863>
78. Quantum Manifesto (2016). [http://qurope.eu/system/files/u7/93056\\_Quantum%20Manifesto\\_WEB.pdf](http://qurope.eu/system/files/u7/93056_Quantum%20Manifesto_WEB.pdf)
79. Reynolds, M.: Google on track for quantum computer breakthrough by end of 2017 (2017). <https://www.newscientist.com/article/2138373-google-on-track-for-quantum-computer-breakthrough-by-end-of-2017/>
80. Shamir, A.: Factoring numbers in  $O(\log n)$  arithmetic steps. *Inf. Process. Lett.* **8**(1), 28–31 (1979)
81. Shor, P.W.: Algorithms for quantum computation: discrete logarithms and factoring. In: *Proceedings of the 35th Annual Symposium of on Foundations of Computer Science, Santa Fe, NM, 20–22 Nov 1994*. IEEE Computer Society Press (1994). [arXiv:quant-ph/9508027](https://arxiv.org/abs/quant-ph/9508027)
82. Shor, P.W.: Why haven’t more quantum algorithms been found? *J. ACM* **50**(1), 87–90 (2003)
83. Simon, D.: On the power of quantum computation. *SIAM J. Comput.* **26**(5), 1474–1483 (1997)
84. Sipser, M.: *Introduction to the Theory of Computation*, 1st edn. International Thomson Publishing (1996); 3rd edn. (2013)
85. Svozil, K.: Quantum hocus-pocus. *Ethics Sci. Environ. Polit. (ESEP)* **16**(1), 25–30 (2016)
86. Takeda, S., Furusawa, A.: Universal quantum computing with measurement-induced continuous-variable gate sequence in a loop-based architecture. *Phys. Rev. Lett.* **119**, 120504 (2017)
87. Tamma, V.: Analogue algorithm for parallel factorization of an exponential number of large integers: li-optical implementation. *Quantum Inf. Process.* **15**(12), 5243–5257 (2016)
88. Tang, E.: A quantum-inspired classical algorithm for recommendation systems. In: *Proceedings of the 51st Annual ACM SIGACT Symposium on Theory of Computing, STOC 2019*, pp. 217–228. ACM, New York (2019)
89. UK programme on quantum technologies (2017). <http://uknqt.epsrc.ac.uk>
90. Wheatley, M.: D-Wave debuts new 5,000-qubit quantum computer. <https://siliconangle.com/2019/09/24/d-wave-debuts-new-5000-qubit-quantum-computer/>. Accessed 24 Sept 2019
91. Wiesner, K.: The careless use of language in quantum information (2017). <https://arxiv.org/abs/1705.06768>
92. Yao, A.C.-C.: Classical physics and the Church-Turing thesis. *J. ACM (JACM)* **50**(1), 100–105 (2003)
93. Zhang, J., Pagano, G., Hess, P.W., Kyprianidis, A., Becker, P., Kaplan, H., Gorshkov, A.V., Gong, Z.X., Monroe, C.: Observation of a many-body dynamical phase transition with a 53-qubit quantum simulator. *Nature* **551**, 601–604, 11 (2017)