From Quantum Speed-up to Supremacy and Advantage

Cristian S. Calude
University of Auckland

Dubna, 7 July 2021

Quantum computing was first introduced by Paul Benioff and Yuri I. Manin in 1980 and Richard Feynman in 1982 and intensively researched afterwards.

Quantum algorithms are probabilistic and can give the correct answer with high probability; the probability of failure can be decreased by re-running the algorithm.

The most popular model of quantum computing is the *circuit (gate) model* in which quantum algorithms are built from a small set of quantum gates.

Adiabatic quantum computing model, proposed in 2000, relies on the adiabatic theorem to do computations.

These two models are "roughly" equivalent.

Quantum computing timeline

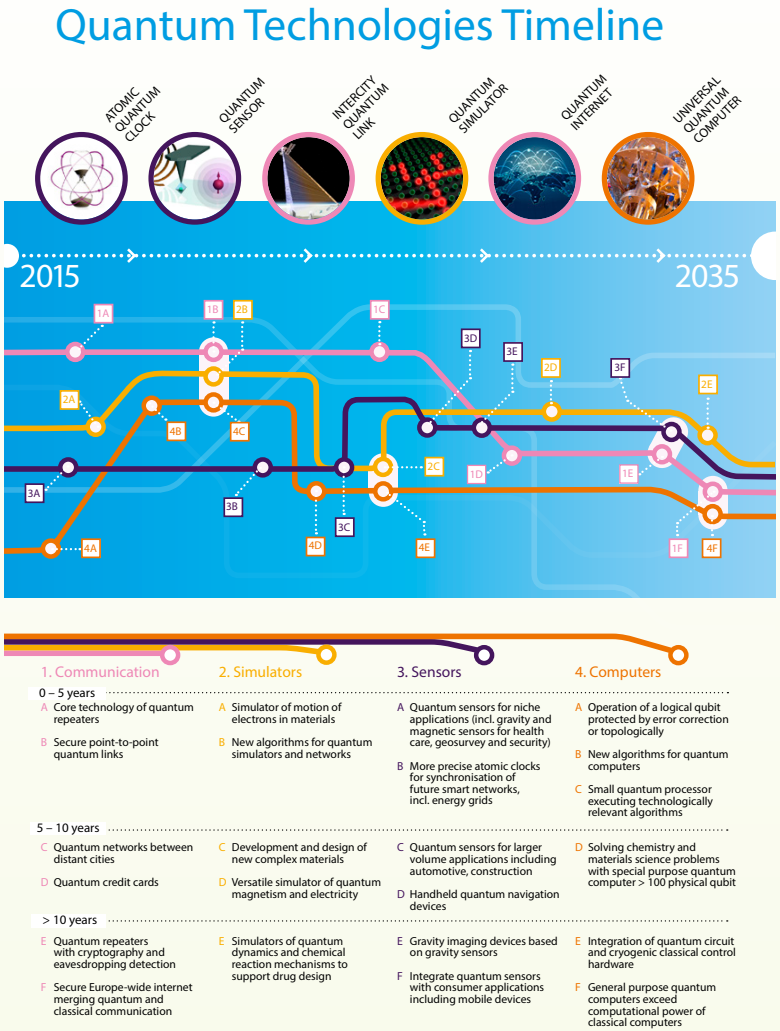

Figure 1: Quantum timeline: 2015–2035, Quantum Manifesto, 2016

Unlike the intermediate states of a classical bit (e.g. any voltages between the "standard" 0 and 1) which can be easily distinguished, but do not exist from an informational point of view, quantum intermediate states cannot be reliably distinguished, even in principle, from the basis states, but do have an informational "existence".

A superposition state $|\varphi\rangle$ is a qubit state vector represented by a linear combination of basis states conventionally denoted by $|0\rangle$ and $|1\rangle$, that is

$$|\varphi\rangle = \alpha|0\rangle + \beta|1\rangle,$$

where α, β are complex numbers with $\alpha^2 + \beta^2 = 1$.

A measurement that projects the qubit $\alpha|0\rangle + \beta|1\rangle$, onto the basis $\{|0\rangle, |1\rangle\}$ will produce the outcome $|1\rangle$ with probability $|\beta|^2$, and the outcome $|0\rangle$ with probability $|\alpha|^2$.

With the exception of limit cases $\alpha = 0$ and $\beta = 0$, the measurement irrevocably disturbs the state:

> *If the value of the qubit is initially unknown; then, there is no way to determine a and b with any conceivable measurement.*

However, *after* performing the measurement, the qubit will "collapse" to a known state: $|0\rangle$ or $|1\rangle$.

The *parallelism* of quantum computing comes from the Principle of Superposition.

Even every qubit is in a superposition $\alpha|0\rangle + \beta|1\rangle$, it contains *no more information than a classical bit*: the reason is that information can be extracted only by measurement.

Unknown quantum states cannot be cloned, hence it's impossible to measure a qubit in two different ways (even, indirectly, by using a copy trick, that is copying and measuring the copy).

The quantum evolution of a qubit is described by a "unitary operator", that is an operator induced by a unitary matrix which may be viewed as a qubit gate.

Classical gates have quantum counter-parts, like

$$\mathrm{NOT} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$

but the converse is not true: the square-root of NOT

$$\sqrt{\mathrm{NOT}} = \frac{1}{2}\begin{pmatrix} 1+i & 1-i \\ 1-i & 1+i \end{pmatrix}$$

satisfies the equality

$$\sqrt{\mathrm{NOT}} \cdot \sqrt{\mathrm{NOT}} = \mathrm{NOT}\,, \tag{1}$$

but no classical binary gate that satisfies (1).

Does it mean that quantum computing can compute more functions than classical computing?

The answer is negative. In fact, quantum algorithms compute much less than classical ones: the reason is that quantum algorithms compute only total functions, i.e. functions which are defined for every input.

The classical universal Turing machine, which simulates any other Turing machine, cannot be computed by any quantum algorithm.

Question: Why quantum computing? Because of the *belief/hope* that quantum algorithms can solve faster hard problems.

The simplest way to illustrate the power of quantum computing is to solve the so-called Deutsch's problem. Consider a Boolean function $f : \{0,1\} \to \{0,1\}$ and suppose that we have a black box to compute it. We would like to test whether f is constant (that is, $f(0) = f(1)$) or balanced ($f(0) \neq f(1)$).

Classically, the test can be done with two computations of f, $f(0)$ and $f(1)$, plus one comparison. Is it possible to do it better? The answer is affirmative: there is a quantum solution in which the quantum box for f is called only once.
The explanation consists in the ability of a quantum computer to be in a blend of states: we can compute $f(a|0\rangle + b|1\rangle)$, for suitable a, b, from which we can extract the information telling us with probability one whether $f(|0\rangle)$ is equal or not to $f(|1\rangle)$.

Can we match classically this complexity? Deutsch's answer was no. ▸ Really?

According to physicist M. Dyakonov (The Case Against Quantum Computing):

> *. . . the number of continuous parameters describing the state of . . . a useful quantum computer at any given moment must be . . . about* 10^{300} *. . . Could we ever learn to control the more than* 10^{300} *continuously variable parameters defining the quantum state of such a system? My answer is simple.* No, never.

A quantum algorithm is a speed-up *if it solves a problem in a time provable smaller than any classical algorithm solving the problem.*

A speed-up requires proofs for a lower bound and an upper bound.

Grover's quantum algorithm (1996) is a polynomial speedup for solving the following problem:

> *given an unsorted database that can be queried with an input, determine whether it contains a specific entry.*

However, the problem it solves is far from being realistic. The cost of constructing the quantum database necessary for the algorithm 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.

Shor's famous quantum algorithm for factoring (1994) is *not (yet?)* a speed-up.

Can quantum computers solve NP-complete problems in (quantum) polynomial time?

The prevalent belief in the quantum complexity community is that *quantum computers can offer no more than a polynomial advantage over the best classical ones.* Such a speedup would even struggle to compete with the heuristic approaches commonly used to solve many hard problems in practice.

In cases where exact solutions are needed a polynomial-order speedup could still be of significant practical benefit.

In 2011 physicist John Preskill proposed and discussed the syntagm "quantum computational supremacy" – a significantly weaker form of speedup:

> *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.*

More precisely:

> *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.*

The plan for **quantum supremacy** was to build the first quantum computer capable of performing a task no current classical computer can.

How? By building a 50-qubit quantum universal gate for simulating the behaviour of a random arrangement of quantum circuits, arguably a **task** that takes classically an exponential time to do (cf. Characterizing Quantum Supremacy in Near-Term Devices, 2017).

This computation is difficult because as the grid size increases, the memory needed to store everything increases exponentially:

1. for a $24 = 6 \times 4$-qubit grid is just 268 megabytes, less than your average smartphone;
2. for a $42 = 6 \times 7$-qubit grid is 70 terabytes, roughly 10,000 times that of a high-end PC;
3. a $48 = 6 \times 8$-qubit grid would require 2.252 petabytes of memory, almost double the memory of the *currently top supercomputer*.

Hence:

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

Can a classical computer solve this problem? Google said no, because of the **Memory assumption** ...

Within weeks, IBM proved that the assumption was false: Breaking the 49-Qubit Barrier in the Simulation of Quantum Circuits.

In September 2019 Google claimed quantum supremacy with an array of 54 qubits used to "perform a series of operations in 200 seconds that would take a supercomputer about 10,000 years to complete" and IBM argued that their classical supercomputer Summit needs ... 2.5 days.

Can they be both correct?

Google claim of quantum supremacy: main difficulty and meaningfulness (less)

While Google team has achieved a big technical feat, they failed to prove the lower bound, so they didn't show "quantum supremacy".

Google's claim is based on a quantum simulation rather than a quantum computation and the task itself is rather uninteresting and without obvious applications.

In fact, nature is doing quantum 'things' that we don't know how to 'do' classically. For example, the structure of atoms can in general only be determined experimentally, but nature manages just fine, with near perfect fidelity. Protein folding is another example.

IBM positions

IBM (which successfully challenged Google supremacy claim in 2017) have commented in 2019 on their quantum computing webpage:

> *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.*

However, in June 2021, their quantum computing webpage says:

> *We design our quantum computers to solve very specific, complex computational problems that are* absolutely impossible to solve using classical supercomputers, no matter how large or powerful.

Is quantum supremacy meaningless?

- The short answer is **No**.
- Building better quantum computers is a worthy goal.
- While for almost 30 years there was little progress in designing fast quantum algorithms, any such algorithm can be potentially "de-quantised" into a classical one. A spectacular example is E. Tang (then an 18-year-old undergraduate student at UT Austin) classical algorithm for the "recommendation problem" – given incomplete data on user preferences for products, can one quickly and correctly predict which other products a user will prefer?

Quantum supremacy is at least controversial, so what's next?

In December 2020 a Chinese team claimed the first demonstration of a 'quantum advantage': quantum simulations that seem to be prohibitively slow on classical computers.

In early 2021 a joint paper by D-Wave System, Google, Simon Fraser University team has reported the use of the D-Wave Advantage to simulate geometrically frustrated magnets in which topological phenomena can emerge from competition between quantum and thermal fluctuations. Measurements indicate a dynamical advantage in the quantum simulation compared with spatially local update dynamics of path-integral Monte Carlo.

A few lessons

1. Do not to underestimate the importance of mathematical modelling and proving (e.g. lower bounds). The difference between exponential and polynomial running times is asymptotic and it is a challenge to find finite evidence for the difference: 2^n is exponential, but 2^{50} is finite.
2. 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.
3. As the Chinese team wrote 'quantum advantage' "would require long-term competitions between faster classical simulations and improved quantum devices".

Answer

Yes!

Quantum Algorithms Struggle Against Old Foe: Clever Computers, Quanta Magazine un-censored version

▸ Quantum computing skepticism