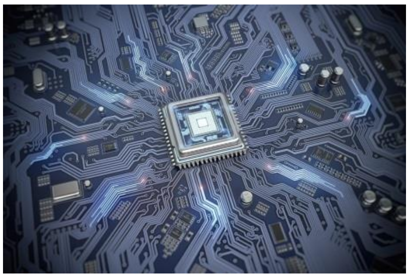
ASSEMBLÉE NATIONALE

SCIENCE AND TECHNOLOGY BRIEFINGS
PARLIAMENTARY OFFICE FOR SCIENTIFIC AND TECHNOLOGICAL ASSESSMENT

SÉNAT

Briefing 15 — July 2019

Quantum Technologies: Quantum Computing



Summary:

- *Theorised in the 1980s, quantum computing has been the subject of great interest over the past few years. Recent technical progress suggests significant computational possibilities in the face of growing needs.*
- *However, there are still many technological challenges to be overcome. Various competing technologies have emerged; attention should be paid to their development while taking media announcements with a grain of salt.*
- *We are already seeing use cases for the potential and specificities of quantum technologies. Far from being a "threat" to current technologies, quantum computing will likely exist alongside them and complement them.*

Mr. Cédric Villani, MP (National Assembly), First Vice-Chairman

Numerical computing is becoming increasingly important to the growing needs of our society, forcing industry players into a race for greater performance. Currently, **the most powerful supercomputers are** "**petaflop**" (one million billion operations per second) **and will soon be "exaflop"** (one billion billion operations per second). For example, a petaflop supercomputer can run a 24-hour weather forecast in 30 minutes where it would take more than a year for a personal computer to do the same. They are one of the largest categories of expenses for the organisations that use them[1] (research centres, manufacturers, etc.) due to their electricity consumption,[2] their cooling systems to avoid overheating and fires, and the purchase price itself.[3] However, supercomputers are essential to handling the increasing volume and speed of data processing and the growth of ever-increasing digital simulations.[4]

While technological development has been able to count on an exponential increase of computers' transistor density until now (thanks to Moore's law),[5] it is reaching a threshold expected in 2022. A technological breakthrough is needed. In this context, quantum computing appears to be an ambitious solution.

The principle and promise of quantum computing

In a classical computer, the basic brick of information is the bit, which can have one of two values (states), either 0 or 1.[6] In the world of quantum computing, its equivalent is called the **qubit**.[7] A qubit refers to a physical object (an atom, ion, electron, photon, etc.) in a quantum state.[8] In accordance with the **superposition principle**,[9] a qubit's state is **a combination of states of 0 and 1;** thanks to **entanglement,**[10] **different qubits can be linked together**. Sets of qubits form a **"quantum register"**. In classical physics, adding an extra bit can only describe one more value; in quantum physics, adding a new qubit doubles the theoretical computing power.[11] So, a **quantum machine of 10 qubits can simultaneously process 2^{10}= 1,024 states** (compared to 10 for a classical 10-bit machine). **Adding 10 qubits equates accordingly to about 15 years of progress in classical machines according to Moore's Law.** As the size of a problem increases, a quantum computer becomes exponentially more efficient than a classical computer at solving it.

The current objective of various market players, whether industrial or academic, is to create a computer with several hundred or even thousands of qubits capable of **competing in speed and reliability with classical advanced supercomputers.**

This power and its later progression would completely revolutionise our society in which digital technology has taken an increasingly important place. **Quantum computers would allow major breakthroughs in many areas by efficiently solving issues that are known to be complex or time- and/or energy-consuming.**

Quantum computing with qubits

Quantum **numerical computing** takes inspiration from classical computer processors to execute a series of operations on a quantum register using logic gates (or functions).[12] In 2000, David DiVincenzo, then a researcher at IBM, proposed five conditions, known as the "DiVincenzo Criteria",[13] considered necessary for a computer to be considered quantum:

- have a **physical medium with well characterised qubits** (whose properties and behaviour are known);

- identify and control these qubits' **initial quantum state**;

- maintain the **quantum coherence** for the time needed for the calculation by isolating the system. As a result of external disturbances, qubits eventually lose their quantum aspect. This is the phenomenon of **decoherence**,[14] which prevents further calculation. The greater the number of entangled qubits, the higher the risk of decoherence;

- be able to **perform all necessary quantum logic gate operations** with a low rate of error and decoherence;

- be able to precisely **measure** qubits' **final state** when the calculation is complete. The observation of a quantum system is probabilistic: it provides the expected result "on average", but it may vary each time the calculation is executed. Therefore, it may be necessary to repeat it several times.[15]

In practice, these criteria are far from easy to fulfil and, despite many announcements, no "quantum" machine fully and completely fulfils them, particularly regarding managing the phenomenon of decoherence.

Handling qubit errors

Quantum computing only makes sense if errors and decoherence remain marginal. In classical computing, when we seek to limit the transmission errors of a message in a "noisy" communication channel, one solution is to send several copies of the message so that at least one of them arrives intact. To limit noise in quantum computing, a similar approach based on **quantum correcting codes** is being considered.[16] It consists in **multiplying the physical qubits** (the physical medium of the information) **to make a few logical qubits work** (capable of handling the information perfectly and carrying out the logical calculation). The physical qubits that result in errors will be relayed by the other qubits to complete the operation in progress. With current technology, **the ratio between physical and logical qubits varies between 10^3 and 10^5. In other words, to operate 50 logical qubits that are available to the user, it takes between 50,000 and 5 million physical qubits**. While recent progress has been aimed at reducing this ratio, we cannot yet exploit this error correction in practice since the most recent quantum machine prototypes only have about **50 physical qubits** whose characteristics vary depending on the technology used.

The various physical media of information

Different forms of qubits are currently being developed at the same time. They each have advantages and drawbacks and varying degrees of maturity. Among the most technologically advanced is the oldest type of qubit which uses **trapped ions** and was used for the first time in 1995.[17] Some ions are held in a cavity (which acts as a trap) and are controlled by electromagnetic pulses (via a laser) that change their quantum state. Currently, systems of 5 to 20 qubits have been made with an error rate on operations of 2 to 5%. Trapped ions have a long decoherence time of about one second, which compensates for the slowness of the logic gates. However, it still seems that large-scale integration will be difficult for this technology. The **cold atoms** technique replaces trapped ions with neutral atoms.[18] In this framework, coherence can be maintained for about a millisecond, while passing a logic gate takes 1 microsecond (1,000 times less time). Finally, **superconducting qubits**[19] based on Josephson junctions[20] developed in the late 1990s are currently the most commonly used qubits in the form of "transmons".[21] This technique uses a pair of bound electrons[22] which, when coupled with a microwave cavity,[23] induces a slight change of frequency according to the qubit's state so that it can be measured.[24]

Investors are choosing the technology that seems the most promising to them, even though none of these various methods has yet been fully successful. **The scientific challenge is to identify the most cost-effective form of qubit in the short or medium term that is best suited for large-scale integration.** For its part, up to now business has seemed to favour superconducting qubits.

Regularly, announcements are made on the development of quantum processors with an increasing number of qubits. In 2018, Google announced a system of 72 (superconducting) qubits;[25] in 2017, Intel and IBM reached 49 and 50 qubits respectively[26] (also superconductors). But their performance was not documented, **making it difficult to rigorously evaluate their announcements.** However, each architecture, which is based on a physical support that, in theory, meets the DiVincenzo criteria, has its own characteristics, particularly in terms of coherence time, reliability, etc. **Therefore, it is important to choose an international standard that allows for an objective comparison of qubit quality and accounts for the specificities of each technology.**[27]

Alternative approaches are also emerging. Since 2012, some qubits have been produced using the **spin**[28] **of electrons in a semiconductor material (silicon).** This approach is being explored at CEA-Leti (Grenoble, France), by Intel at the Dutch centre QuTech (*Technische Universiteit* Delft), and UNSW (*University of New South Wales*) in Australia with coherence times that are sufficient to perform calculations. Additionally, using silicon would allow us to adapt the current electronic and microelectronic manufacturing standards and envisage large-scale mass production to **propel France forward in the field of qubit tech-**

nologies.

Canadian company D-Wave is developing analogue processors using alternative quantum annealing which aims to converge a system of several qubits to a final state corresponding to an (optimized) minimum of energy, the final state being the information sought. Starting with 128 qubits in 2011, these machines are now reaching 2,048 qubits.[29] Some applications have already been developed in the fields of the science of materials, optimization, or advanced machine learning technology.[30] **However, there is a debate in the scientific community about the quantum advantage of these machines over algorithms suited to supercomputers.**

The short- and medium-term outlook for use

In the short term, and assuming no major technological breakthrough in engineering, we can only build and use NISQ machines (see text box). These require the development of error-tolerant algorithms.

Another way to valorise quantum potential consists in combining one or more quantum processors of a few qubits corrected by an architecture composed of classical bits. These hybrid systems allow us to optimise **each technology's field of expertise** and to use "**quantum acceleration**" for specific needs along the model of powerful graphic processing units (GPU) used for supercomputers. Generally, **quantum computers will no doubt only be able to solve a specific type of problem, not completely substitute classical machines.**

NISQ technology[*] (*Noisy Intermediate-Scale Quantum technology*):

In 2018, John Preskill, a physician at Caltech, introduced the technological concept of "NISQ" or "noisy quantum", **mid-sized quantum computers with 50 to 100 physical qubits for which errors are not corrected.** While this limits the complexity of the problems that these machines can solve, it is nonetheless interesting to further this line of research to create an offer for the market that can boost investment in the short term while we wait for "perfect" quantum computers (i.e. with a very low error rate) or computers with a very large number of qubits processed with error correction codes.

[*] PRESKILL, John. "Quantum Computing in the NISQ era and beyond." *Quantum*, 2018, vol. 2, p. 79.

Conclusions and perspectives

Theorised several decades ago, quantum computers have only begun to attract interest from manufacturers in recent years. However, many technological and theoretical obstacles still need to be overcome before their use becomes widespread and we see "quantum supremacy" over classical computers. Manufacturers have entered into fierce competition with high stakes; they often make impressive announcements that should be taken with a grain of salt, since not all the qubits announced have the same quality. Developing an international qubit standard would make it easier to compare the various technologies. In the most optimistic scenario, the next few years will probably see a cohabitation between classical processors and quantum processors to take advantage of the specificities of each depending on what is needed. In the short term, several dozens of qubits, even imperfect ones, can be useful, especially for the acceleration of optimization problem solving, the marketing of which will enable virtuous cycles of investment that are essential for long-term development.

The OPECST websites:

http://www.assemblee-nationale.fr/commissions/opecst-index.asp

http://www.senat.fr/opecst/

Experts consulted

Mr. Alain Aspect, physicist at the Institut d'Optique (Institute of Optics), member of the Office's Scientific Council.

Ms. Astrid Lambrecht, research director at CNRS (French National Centre for Scientific Research), director of the CNRS Institute of Physics (INP/CNRS), member of the Office's scientific council.

Ms. Fanny Bouton, a journalist specialising in new technologies.

Mr. Antoine Browaeys, Research Director at the Institut d'Optique.

Mr. Philippe Chomaz, Executive Scientific Director of the Direction de la recherche fondamentale (Directorate of Fundamental Research) at CEA (French Atomic Energy and Renewable Energy Agency).

Mr. Bruno Desruelle, CEO of the start-up Muquans.

Mr. Philippe Duluc, Big Data & Security Technical Director at Atos.

Mr. Daniel Estève, Research Director and head of the Quantronique group at CEA.

Mr. Olivier Ezratty, a consultant specializing in new technologies and the author of the blog "Opinions libres".

Mr. Philippe Grangier, Research Director at CNRS and head of the Quantum Optics Group at the Institut d'Optique.

Mr. Serge Haroche, Emeritus Professor at the Collège de France and the 2012 Nobel Prize winner in Physics.

Mr Christophe Jurczak, Managing Director of the Quantonation Investment Fund.

Mr. Iordanis Kerenidis, CNRS research director at the Institut de Recherche en Informatique Fondamentale - RIF (Institute for Fundamental Computing Research).

Ms. Pascale Senellart, Research Director at the CNRS Laboratory of Photonics and Nanostructures (LPN) and co-founder of the start-up Quandela.

Mr. Miklos Santhas, Research Director at the Laboratoire d'Informatique Algorithmique: Fondements et Applications - LIAFA (Algorithmic Computer Science Laboratory: Foundations and Applications).

Mr. Sébastien Tanzilli, Research Director and CNRS Quantum Technologies Project Manager.

Mr. Georges Uzbelger, AI/Advanced Analytics Solution at IBM France.

Mr. Benoit Valiron, Assistant Professor at Centrale Supélec.

Mr. Benoit Wintrebert, Innovation Advisor at the French Ministry of the Armed Forces.

Contribution by Mr. Yann Michel, researcher at CNRM/GMAP.

Contribution of Mr. Volker Beckmann, Calculation and Data Scientific Assistant Director, National Institute of Nuclear Physics and Particle Physics, CNRS.

Scientific coordination by Sarah Tigrine, Scientific Advisor (with support from Mr. Gaëtan Douéneau).

Reference works consulted:

- "Comprendre l'informatique quantique" O. Ezratty, November 2018 (e-book)

- Reports from the American Academies: National Academies of Science, Engineering, and Medicine. 2018 Quantum Computing: Progress and Prospects. The National Academies Press, Washington, DC. DOI: https://doi.org/10.17226/25196.

- "Clefs du CEA" issue no. 66- June 2018 "Révolutions quantiques "

Note: in concurrence with the Ethics Officer of the French National Assembly, Cédric Villani has recused himself from the ATOS Scientific Council - a non-decision-making body - for the duration of his work on quantum technologies for the Office.

References

(1) The estimated global revenue for high-performance computing (HPC) is currently at around €25-30 billion with an increase of 7% per year, potentially reaching €40 billion in 2022.

(2) For example, the US supercomputer Summit (93 petaflops) has a peak consumption of 15 MW, equivalent to the power consumption of 7,000 households.

(3) There is little public communication on supercomputers' average selling price, but it can be estimated between €10 and €200 million.

(4) The global forecast model of Météo-France (ARPEGE) integrates 9x10^8 (nearly a billion) observations per month, uses about 3 million lines of code, and produces more than 10 TB of data per day. "Météo France should multiply its computing power by five thanks to the acquisition of a new supercomputer in 2019 that will come into service in 2020. This investment is essential to Météo France maintaining its current position, requiring investments in heavy computing of €12 to 29 million per year over the 2019-2024 period."

(Source: Senate fact-finding mission "Ecology, sustainable development and mobility", schedule 159 "Expertise, geographic information and meteorology", and annex budget "Air monitoring and exploitation" https://www.senat.fr/commission/fin/pjlf2018/np/np10c/np10c_mono.html#toc25)

(5) In 1965, Gordon E. Moore (one of the three founders of Intel) laid out what we now call Moore's Law: that the density of transistors (the number of transistors per unit of area), from which classical computers derive their power, should double every two years. This prediction has been surprisingly accurate, and process size has steadily shrunk in recent years to reach 10 nm (1 nm = 10^{-9} m) in 2017. However, progress is reaching its physical limits as we are reaching the size of the atom.

(6) In a computer, bits are manipulated using electronic components called transistors, which have two states: ON (value 1) and OFF (value 0). Current processors contain around one billion transistors.

(7) The term "qubit", a portmanteau of "quantum" and "bit", first appeared in 1995 in a publication written by physicist Benjamin Schumacher in the field of quantum information theory: "Quantum coding", Benjamin Schumacher, *Phys. Rev.* A 51, 2738 - Published 1 April 1995.

(8) See Briefing N° 13: "Quantum technologies: introduction and issues" from the Office http://www2.assemblee-nationale.fr/content/download/79022/810034/version/2/file/Note_TechnologiesQuantiques_Introduction_versionFinale.pdf

(9) The ability of a quantum body to be in different states at the same time. Therefore, the overall state of a system at a given time becomes a linear combination of all possible states at that instant.

(10) When two separate particles (in this case, two qubits) are entangled, their quantum states become bound to each other and cannot be described separately.

(11) If a qubit represents the superposition of 2 states, two qubits describe 4 possible states, and three qubits imply the superposition of 8 states...thus, for N quantum bits, there are 2^N possible states.

(12) In classical computing, logic gates (AND, OR, NAND, NOR, etc.) describe the basic operations performed on bits. For example, the AND gate inputs 2 bits and returns 1 if each of the two entries is equal to 1 and 0 in the other three cases. These gates have quantum analogues (Hadamard, Pauli gate, etc.), but their behaviour is much more complex to describe.

(13) DiVincenzo, David P. "The physical implementation of quantum computation". *Fortschritte der Physik: Progress of Physics*, 2000, vol. 48, no. 9-11, p. 771-783.

(14) The phenomenon of decoherence reflects a loss of quantum information due to the system's environment. The system's wave function (the state) is "scattered" by the multiple external interactions and ends up losing its undulatory character and, thus, its quantum behaviour. The notion of decoherence was highlighted in 1970 by the physicist Dieter Zeh, allowing us to better understand the border between the quantum and classical world. Classical objects may just be quantum objects that have undergone decoherence through interaction with their environment.

(15) We cannot simply repeat the measurement because it will have destroyed the quantum state. In quantum mechanics, observations made on a system modify its state; it is therefore impossible to "read" the value of a qubit without destroying it. This property poses several challenges to quantum algorithms, but it is also one of the keys to the security and inviolability of quantum cryptography protocols.

(16) The idea here is similar, but, in quantum mechanics, a state cannot be duplicated: one cannot observe the value of a given qubit to make an identical "backup copy". This challenge is the reason for the complex answers to the issue of correcting qubit errors.

(17) Monroe, Chris, Meekhof, D. M., King, B. E., et al. "Demonstration of a fundamental quantum logic gate". *Physical review letters*, 1995, vol. 75, no 25, p. 4714.

(18) Ions are atoms to which electrons have been added or removed.

(19) A superconductive material does not apply any resistance to the passage of an electric current and, therefore, dissipates no energy. However, it does work in the cold: -271.3°C (1.8 degrees above absolute zero).

(20) The Josephson effect refers to the appearance of a current between two superconducting layers, themselves separated by a non-superconductive insulating or conductive material. Quantum mechanics provides the "tunnel effect" between these two layers, i.e. the ability for an electron to cross the potential inductance barrier, even if its energy is less than the minimum energy required to cross this barrier (Josephson junction).

(21) Transmons, which refer to "*transmission-line shunted plasma oscillation qubit*", were developed at Yale University in 2007 (Koch, Jens, et al. "Charge-insensitive qubit design derived from the Cooper pair box." *Physical Review A 76.4* (2007): 042319.).

(22) A Cooper pair refers to two electrons paired in a metal at a very low temperature despite the repulsive force caused by their electrical charge of the same sign. This bond between two electrons is the basis of superconductivity according to the so-called "BCS" theory, named after its inventors John Bardeen, John Schrieffer, and Leon Cooper. The latter were awarded the 1972 Nobel Prize for Physics for this theory.

(23) A microwave cavity (or resonator) is a cavity in which a wave (here in the microwave range, i.e. around 2.5 GHz) resonates with the cavity's walls.

(24) These superconducting circuits are called QED circuits (*Quantum ElectroDynamics* circuits). The field of quantum electrodynamics was developed by Serge Haroche, the 2012 Nobel Prize winner in Physics.

(25) https://ai.googleblog.com/2018/03/a-preview-of-bristlecone-googles-new.html

(26) At IBM, there is an operational prototype tested in its laboratories which should be put into production for its customers at the end of 2019.

(27) That's why IBM has introduced a metric, "quantum volume", which measures the degree of use of a quantum machine based on the combined parameters of the number of qubits, the error rate, the connectivity, and the set of quantum gates available. (https://www.zdnet.fr/actualites/informatique-quantique-ibm-assure-que-c-est-pour-les-annees-2020-39881483.htm). Atos is also exploring this path with its QLM simulator that integrates the physical characteristics of various technologies to compare how they perform when executing a reference quantum program.

(28) Under the influence of a magnetic field, electrons, comparable to rotating electrical charges, behave like little magnets and allow only two possible orientations. This is called the electron's spin, which can only have one of two values: *up* and *down* or +1/2 and -1/2. Discovered in 1925, spin is now one of a quantum particle's properties in the same way as its mass or its position.

(29) The machines sold by D-Wave currently cost about €15 million.

(30) https://www.dwavesys.com/quantum-computing/applications