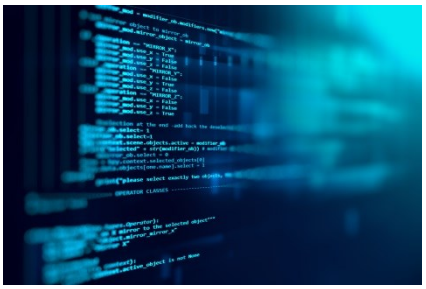
SCIENCE AND TECHNOLOGY BRIEFINGS
PARLIAMENTARY OFFICE FOR SCIENTIFIC AND TECHNOLOGICAL ASSESSMENT

Briefing 16 — July 2019

Quantum Technologies: Quantum Programming



Source: monsitj/AdobeStock

Summary

- *Quantum computing pertains to both the physical information medium (qubits) and the programming languages used to manipulate them and optimise how they are used. These two fields, while seemingly separate, must be developed in parallel.*
- *Quantum programming research is concerned with both the machine language that controls qubits and the creation of user interfaces, whatever the qubit technology used.*
- *The potential power of quantum computing coupled with optimised quantum algorithms will solve high-stakes problems, such as optimisation calculations.*

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

While the success of IT is based in part on the considerable progress made in the field of electronics in recent decades (especially in miniaturisation according to Moore's law),[1] the development of increasingly effective algorithms and computer programmes (traditionally grouped under the term "*software*") has also played a major role in its growth.

Developers do not need to know how a computer physically works to write conventional programs. In fact, most of the time they use **high-level programming languages**[2] that are oriented towards the problems to be solved and that allow them to overcome the hardware's specificities. In contrast, a computer only understands **low-level languages** that have the processor perform the basic operations on the bits, and this depends on its physical architecture. To effectively translate high-level programs into basic instructions, many **compilation**[3] **and optimisation processes** have been developed in recent decades.

Similarly, **we will need to know how to program an operational quantum computer effectively** and account for its specificities. Quantum programming is radically different from classical programming[4] and is beginning to establish itself as a field in its own right, indispensable and complementary to hardware development.

The development of quantum programming languages

Controlling qubits and quantum logic gates requires specific programming to integrate the probabilistic dimension of quantum computing which varies from the determinism of classical physics. One of the objectives of current research in software development is to develop **suitable programming environments** in advance which can be used by programmers as soon as quantum machines of sufficient capacity are available.

The creation of quantum programming languages pertains, on the one hand, to low-level languages that depend on the qubits technology used[5] and its characteristics (coherence time, logic gates, etc.),[6] and, on the other hand, to high-level languages independent of the physical system. Between the two, new compilation methods need to be developed. Several programming platforms have already been developed: some by academic teams (such as the QUIPPER language),[7] others by manufacturers who combine them with online simulation tools (like the Q# language developed by Microsoft[8] or the AQASM and pyAQASM languages by Atos). Quantum computation libraries are also already available that complement current, classical programming languages such as Python. The platforms developed are generally freely available or in the cloud to encourage participation in research and allow the greatest number of developers to become familiar with quantum programming. It is important to **develop programming skills quickly using these new methods to meet the quickly growing demand**. To this end, many teaching programmes in quantum computing have been set up near research centres, such as at TU Delft (*Technische Universiteit*, the Netherlands) and at Télécom ParisTech.

In the context of training and research, **quantum computer emulation by conventional machines** also plays a vital role in testing algorithms despite the absence of a truly quantum processor. The *Quantum*

Learning Machine (QLM) made by Atos is a programming platform that simulates a quantum computer that would have 30 to 41 qubits on a conventional supercomputer. It integrates the technical characteristics specific to each qubit technology (the logic gates' response time, decoherence, etc.) and their current reliability, which is very useful for low level applications.

Research into the development of quantum programming, although less expensive than hardware development, has seen very little funding in the first phase of the flagship European Forum on Quantum Technologies that began in October 2018[9]. **Investment efforts must nevertheless be made in this area to anticipate how quantum machines will be used and applied.** In France, the ANR SoftQPro project[10] was granted €500,000 of funding through 2022, bringing together CEA, Atos, and several university computer science laboratories to develop methods for optimising quantum programs.

Quantum algorithms and applications

Only about sixty classes of quantum algorithms have been developed to date as the research is quite recent.

In theory, they allow us to solve certain issues more efficiently than a conventional machine, for example in arithmetic (factorisation of large numbers,[11] *see box text*) and optimisation problems which seek the minimum and/or the maximum of a given quantity. The very broad range of sectors is concerned by optimisation issues, from healthcare and chemistry (molecular configuration) to finance (portfolio optimisation), logistics, and resource management.

There are the so-called **NP-complete** problems[12] where testing all the possibilities is the most effective method of solving it we know, but where checking the proposed solution is fast. For these problems, solution algorithms' execution times vary exponentially according to the size of the input data and require very long execution times on conventional machines. "Quantum" algorithms could reduce them considerably. **The "traveling salesman" problem is one of the best-known examples of this type of problem,** aiming to calculate the shortest route for a traveling salesman given that he must visit each city he is responsible for once and only once.[13]

The difference between classical and quantum algorithms: Shor's algorithm as an example

Current encryption methods are based on factorising large integers, for example via the RSA protocol(*) used since the 1970s. Indeed, this problem proves especially difficult for a conventional computer to solve. As early as 1994, American researcher Peter Shor wrote an algorithm that, if there were a quantum computer capable of implementing it, would allow integer factors to be factored in a time exponentially faster than the classical algorithms, and would thus become a threat to the security of the encryption protocols we use.

Solving a factorization problem consists in transforming it into a period search problem (or frequency, which is the reciprocal of a period). One way of thinking about this concept is to imagine a book that contains many pages and is also periodic: In fact, it would be made up of the same story repeated every n pages, n being the period(**).

The classical way is to go through all the pages from the beginning until you find two identical ones. As the book is very big, this method requires a lot of time and memory.

The paradigm of Shor's quantum algorithm is different: at first, the superposition principle allows qubits to represent all the pages of the book at the same time. Thanks to a "Fourier transformation", a mathematical method used in many fields of physics to break down a signal according to an independent variable which can be interpreted in physics as its frequency or pulsation, we can then identify and amplify the frequency (or period) most likely to measure it. Thus, with the quantum method, we do not need to know the precise content of the book, which makes the calculation much faster.

(*) See the Briefing from the Office on "Quantum Technologies: Quantum and Post-Quantum Cryptography"

(**) Analogy inspired by the article: https://www.larecherche.fr/traquer-les-failles-des-algorithmes

Combining classical and quantum processors would be ideal for optimizing the computation time for this type of problem, since qubits can efficiently explore each possible solution which conventional bits could then quickly check. **This is a good example of the potential for complementarity between the two technologies.** A study is also underway on combining the potential of quantum computing with deep learning techniques.[14]

While these applications look promising, **current quantum machines are too limited and unreliable to perform calculations that are currently inaccessible to (classical) supercomputers and to fully explore the field of quantum possibilities**. The tests are still carried out on a very small number of qubits, but this does allow us to confirm algorithm models and research tracks. An experimental demonstration of the superiority of quantum computation, called "**quantum supremacy**",[15] would require at least a hundred qubits, a major challenge to launching a virtuous cycle of research and production.

Conclusion and recommendations

The fields of quantum programming and algorithmics must not be neglected to fully deploy quantum computing's potential and respond to specific applications, such as optimization calculations that have many applications. Although it is difficult to predict when a quantum computer with several hundred or even thousands of qubits will be available, we must still prepare for it using methods such as quantum emulators. This method may also allow us to serendipitously discover new issues that are out of the reach of classical processers but that can be handled by quantum registers.

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 specialising 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 Laboratoire de photonique et nanostructures (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.

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)

- A report 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) 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.

(2) "High-level" refers to the level of the machine, as opposed to the "low-level" language that corresponds to the instructions given to the machine's processor.

(3) In computing, compilation refers to the translation of the high-level code written by the user into instructions for a low-level language that is understandable by the machine. For example, an optimized compiler increases the speed at which instructions are executed or reduces the memory space occupied.

(4) Indeed, the principles of quantum physics impose constraints on quantum bits, for example the impossibility of copying a value.

(5) Several qubit technologies are currently being studied, such as trapped ions, cold atoms, spin qubits, or superconducting qubits. See the Briefing on "Quantum Technologies: Quantum Computers" from the Office.

(6) see the Briefing on "Quantum Technologies: Quantum Computers" from the Office.

(7) https://www.mathstat.dal.ca/~selinger/quipper/

(8) https://www.lemondeinformatique.fr/actualites/lire-microsoft-pousse-sur-github-une-formation-au-developpement-quantique-72407.html

(9) http://www.cnrs.fr/fr/premiers-laureats-pour-linitiative-europeenne-sur-les-technologies-quantiques

(10) https://anr.fr/Projet-ANR-17-CE25-0009

(11) See the Briefing from the Office on "Quantum Technologies: Quantum and Post-Quantum Cryptography".

(12) There are thousands of Np-complete problems, including the knapsack problem and the longest path problem.

(13) Direct applications of the traveling salesman problem pertain to logistics and delivery systems, for example; but less obvious applications have been showcased, such as optimizing an industrial machine's movement to reduce the time it takes an electric drill to drill a given number of holes.

(14) https://www.nature.com/articles/d41586-019-00771-0 for an analysis of the Havlíček, V. et al. study Nature 567, 209-212 (2019).

(15) Several expressions aim to compare a quantum computer's performances with those of a supercomputer. The expression "quantum advantage" refers to the case where a quantum method processes a problem more quickly than a supercomputer; "Quantum supremacy" is the situation where quantum technology would make processing inaccessible to classical computers.