Journal of Engineering Science *Vol. XXVIII, no. 1 (2021), pp. 83 - 90*
Fascicle *Electronics and Computer Science* *ISSN 2587-3474*
Topic *Computers and Information Technology* *eISSN 2587-3482*

https://doi.org/10.52326/jes.utm.2021.28(1).08
UDC 004:530.145

QUANTUM COMPUTING

Titu-Marius I. Băjenescu*, ORCID ID: 0000-0002-9371-6766

Swiss Technology Association, Electronics Group Switzerland
*Corresponding author: Titu-Marius I. Băjenescu, *tmbajenesco@gmail.com*

Received: 18. 12. 2020
Accepted: 10. 02. 2021

Abstract. The quantum computer, is a "supercomputer" that relies on the phenomena of quantum mechanics to perform operations on data. Object of suppositions, sometimes far-fetched, quantum mechanics gave birth to the quantum computer, a machine capable of processing data tens of millions of times faster than a conventional computer. A quantum computer doesn't use the same memory as a conventional computer. Rather than a sequence of 0 and 1, it works with qubits or quantum bits. The quantum computer is a combination of two major scientific fields: quantum mechanics and computer science. Quantum mechanics, on which this computer is based, governs the movement of bodies in the atomic, molecular and corpuscular domains, is a theory whose logic is totally contrary to intuition and it is essential to use mathematics to fully grasp it. Quantum computing is the sub-domain of computer science that deals with quantum computers using quantum mechanical phenomena, as opposed to those of electricity exclusively, for so-called "classical" computing. The quantum phenomena used are quantum entanglement and superposition. The article examines some aspects related to the development, operation, advantages and difficulties, applications and future of the quantum computer.

Keywords: *Quantum theory, quantum information, quantum mechanics, photon teleportation, quantum computer, EPR paradox, qbits.*

Introduction

It was in the early 1980s that scientists began to realize that the future of the computer was based on quantum theory. Indeed, they became aware that today's computer was approaching its limits because you can't miniaturize to infinity. The hypothesis that emerged from this realization was that the next evolution of the computer would be based on quantum theory. However, this theory is older than that. The physicist Richard Feynman was the first to study the question in the 1960s [1].

The principle of the quantum computer is based on the properties of quantum mechanics. Einstein, himself, challenged quantum mechanics and proposed an experiment, which he called the EPR paradox, to prove that quantum mechanics was inaccurate. However, this experiment could only be carried out in 1981 by Alain Aspect because the technology of the time did not allow its realization. The result of this experiment proved, without any dispute, that quantum mechanics governed the movement of atoms [2, 3].

In 1996, Lov Grover (Lucent Technologies) designed a quantum algorithm that only needs √n queries to an oracle *f* to find an element that satisfies *f* in a non-ordered database of size *n*, where classical computation requires *n* queries to the same oracle [4].

From 1999 to 2002, Isaac Chuang (IBM Research) designed and built a quantum computer which, although limited to 7 bits, was used to show that physics can indeed experimentally implement the new algorithmic principles imagined at the theoretical level by Peter Shor and Lov Grover.

The first computation of a quantum computer took place in 2001 [5]. This first calculation is 15=3*5. This computation may seem insignificant and extremely simple but it is very important because it opens the way to practical applications.

History of the quantum computer

In 1993, Charles Bennett (IBM Research), Gilles Brassard (Université de Montréal) and other scientists discovered the premises of the quantum computer because they highlighted a property of quantum information. This property goes against all the rules of classical physics. This team of scientists is setting up a teleportation protocol that uses the properties of the EPR link discovered by Einstein [6]. The EPR link is a kind of bond between two particles. This means that the two particles are linked together and any action on one causes the other to react. So, if the state of one of the two particles changes, the other particle will undergo the same change at the same time. It is thanks to this protocol that Anton Zeilinger (University of Vienna) carried out the first photon teleportation in 1997.

In 1994, Peter Shor, from the AT&T laboratories, had devised an algorithm using this property to factorize very large numbers in "polynomial" time, which means, in mathematical language, that increasing the size of the encryption keys would no longer be an insurmountable obstacle.

How the quantum computer works

We have seen that we are only at the beginning of the quantum computer and that this computer is based on the principle of quantum mechanics [7].

Today's computers use bits that have two states that are either 0 or 1. A quantum computer doesn't use the same memory as a conventional computer. Rather than a sequence of 0 and 1, it works with qubits or quantum bits. These qubits will have the state 0, the state 1 but also, and this is what makes them very interesting, they will also have both states at the same time that is to say 0 and 1. Indeed, it is on this principle of superposition, which is that a qubit has both states 0 and 1, that the quantum computer is based. This state of superposition, specific to qbits, gives a quantum computer a computing capacity that is impossible to achieve otherwise [8].

The state of a register of 2 qubits could then be 0, 1, 2 or 3, but also a superposition of any part of these four basic states, or even all four at once. The state of a register of n qubits could be a superimposition of any set of the 2n possible values on n bits, including a superimposition of all these values at the same time, whereas a classic n-bit register can only contain, at each instant, one of these values.

Therefore, since the calculations will transform the state of such registers, any operation performed during a quantum calculation will be able to act simultaneously on 2n different values. This brings a massive parallelism: if a function can be computed with 2n different arguments, all its values will be computed simultaneously. The laws of quantum physics impose that these simultaneous calculations are reversible and deterministic, which

does not reduce what can be calculated, but they do not allow to copy the state of a register into another register [9, 10]. Therefore, in a program, we will not be able to assign the value of one quantum variable to another, nor will we be able to use this value several times. This property forces us to invent a new algorithm and programming languages that respect the laws of quantum mechanics.

Once a computation is completed, the desired result is one of the values superimposed in a register. To extract the result, physicists will have to perform what they call a measurement of this register. According to the laws of quantum physics, this measurement will produce one of the superimposed values in the register, each with a certain probability and, at the same time, it will reduce the superimposition contained in the register to a single value, the one chosen [11]. The measure therefore causes the superimposed states to collapse. The right value will eventually be obtained if the quantum algorithm has been well designed. So, the goal of the quantum algorithm is to bring the probability of obtaining a relevant result as close to 1 as possible, and this by performing as few operations as possible.

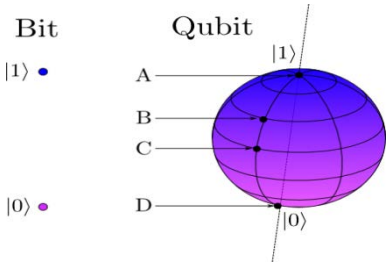

Figure 1. Entanglement is an extraordinary resource.

Let's take two objects, A and B, which each have several possible states. While classical physics tells us that the state of the pair A,B is none other than the pair of the state of A and the state of B, in quantum mechanics this assertion is no longer true. Indeed, it may be that the pair A,B has a state, whereas neither A nor B has a state of their own. It is then said that A and B are intertwined. Unparalleled in the classical world, entanglement is an extraordinary resource [12]. For example, if A and B are registers of qubits, and if they have been entangled during a calculation, we can imagine the state of the pair A,B as inseparably linking each of the values superimposed in A to one or more of the values superimposed in B. Thus, if we measure A, its state is reduced to only one of the values it contained, but the state of B is also reduced, at the same time, to the superposition of the values that were linked to the one that remained in A. This is true if A and B are side by side, but remains true if they have been millions of kilometres apart after being entangled. The couple A, B is always the couple A, B no matter how far apart they are.

Advantage of the quantum computer

We saw earlier that the quantum computer was the result of the use of qubits.

The main advantage of this computer is the saving of time. Indeed, the fact that qubits can have state 0 and state 1 at the same time saves a considerable amount of time. To illustrate this, let's take a simple example, the opening of a padlock.

To find the right combination of the classical padlock, you would have to try, one by one, each of them until the padlock opens. However, the quantum padlock tries all possible combinations at the same time and can find the right combination much faster than the classic padlock.

Difficulties of such a computer

Prototypes are already appearing, with a maximum of 50 qbits, but these are very noisy, i.e. the results they give are still too often erroneous. There are several problems that scientists will have to solve. First of all, there is the problem of reading information. Indeed, we know that quantum mechanics is indeterministic [13]. That is to say, we do not know the

state of the atoms. For example, if we perform a calculation, we do not know the result and reading this result destroys the information. To be clearer, if we perform a complicated calculation, we will only know the final result. Indeed, the intermediate results will be inaccessible, otherwise the information will be destroyed and thus the calculations will stop.

This problem has not yet been solved by scientists. However, we have seen that a team of researchers had carried out the following factorization: 15=3*5. This is due to the fact that there was no intermediate result. Therefore, this problem of loss of information exists only when we need to know intermediate results and does not exist when only the final result interests us [14].

The second problem is the physical realization of a quantum computer. Scientists have several leads. Indeed, qubits can be of different types. They can be photons, therefore light, molecules or atoms. But it is the method of molecules or atoms that is the most promising. Indeed, nuclear magnetic resonance, which creates a magnetic field greater than 2 Tesla, is capable of changing the quantum state of the nuclei of molecules and atoms. However, this method has a constraint: helium and liquid nitrogen must be regularly replaced to ensure superconductivity because the products tend to evaporate.

The main problem facing quantum computing is building computers [15]. Compared to a normal computer, a quantum computer is an extremely complex machine: they operate at a temperature close to absolute zero (-273 ºC), the qubits support are superconducting and the components to be able to read and manipulate the qubits are not simple either.

A priori and with the materials that quantum computers are being built with, it does not seem that miniaturization is too feasible. But there is already research on new materials that could be used to create more accessible quantum computers [16].

The future of the quantum computer; when is it due?

Unfortunately, that question cannot be answered precisely. Indeed, it would be risky to give a precise date because we have seen that many obstacles are on the road to this new type of computer. In addition to the technical problems, there is an additional difficulty [17].

Indeed, the arrival of the quantum computer depends largely on the interest it can generate for governments. Because technological advances are very rapid when there is competition. Examples of this phenomenon can be found in history, for example, nuclear fusion to produce industrial energy. For years, experimental reactors lived in a state of general indifference. Then suddenly, following the interest shown by the United States in an atmosphere of competition with Europe and the rest of the world in mastering this energy of the future, the ITER programme came to fruition and became the best example of this phenomenon [18].

In the field of quantum physics, it is the government authorities that fund research. So it is these authorities who are competing and who decide on the interest that such a computer has for their country. However, if one country makes significant funds available to fund research on the quantum computer, the authorities in other countries capable of carrying out such research will, in a way, be obliged to react and thus fund the research.

Google may have achieved quantum supremacy, but some of other projects have the potential to achieve this soon, including those of IBM, IonQ, Rigetti and Harvard University. These groups are using several distinct approaches to building a quantum computer.

Google, IBM and Rigetti are performing quantum calculations using superconducting circuits. IonQ uses trapped ions. The Harvard initiative uses rubidium atoms. Microsoft's approach concerns "topological qubits" [19-23].

It would appear that the United States of America has grasped the interest of developing such a computer. It is said to have encouraged its research laboratories and companies to acquire technological mastery of it and to generalise its use for its own benefit, well ahead of its competitors [24,25]. Today, it is well known that the ability of American science and industry to rely on networks of very large computers is one of the principal means of ensuring their supremacy. Thus, according to all this information, some scientists have ventured to advance a date for the development of the quantum computer. According to them, this computer will be designed short after 2020 [26 - 28].

Applications

There are several possible applications for the quantum computer. First of all, there is the scientific field. This computer could be used to make calculations and simulations that take a lot of time to be carried out by conventional computers. This will allow science to advance much faster because scientists will waste less time waiting for calculations or simulations to be done by the computer [29].

The first application is molecular simulation, the ability to describe matter on a very small scale, the atomic scale [30, 31]. This molecular simulation has many applications, such as finding new drugs or more resistant materials. These are often referred to as room temperature superconducting materials, capable of transferring energy without any loss [32, 33]. Molecular simulation is also interested in chemical reactions, which could make it possible, for example, to design new fertilisers.

The other family is optimization problems, which are the domain of operational research. This consists of finding optimal solutions to problems that have a very large number of possibilities. For example, optimising road traffic or finding the optimal load for a ship [34]. The most plausible application is cryptography, the science of encryption. Nowadays, encryption keys are, to be 100% sure of their effectiveness, as long as the message you want to transmit. This is Vernam's one-time pad (also called a "disposable mask"). It has, for example, been used to encrypt the red phone between Washington and Moscow. The major disadvantage of this encryption process was the size of the key, which had to be as long as the message to be sent [35]. Until then, it was transported via the diplomatic pouch, which is not 100% secure.

The quantum computer will solve this problem [36, 37]. Security will then be ensured by the laws governing quantum mechanics and not by mathematical theorems.

In routing the encryption key, the corresponding information will be transmitted through photons, each of which is polarized.

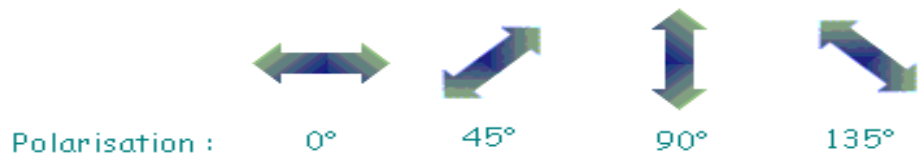

Figure 2 Polarization of the photons.

Polarization is measured by an angle varying from 0° to 180° and can take four values: 0°, 45°, 90°, and 135°. When the photons are polarized from 0° to 90°, the polarization is called rectilinear polarization. For those polarized from 45° to 135°, one speaks about diagonal polarization:

In order to detect the polarization of photons, it is possible to use a polarizing filter followed by a photon detector [38]. If the filter is oriented at 0°, when a photon polarized at 0° passes through it, it is recorded by the detector. Conversely, if the photon is polarized at 90°, the detector will not record anything. In the last case where a photon is diagonally polarized, it would be recorded every other time. In the same way, if the filter is oriented at 135°, the same phenomenon will occur as for rectilinearly polarized photons, i.e. rectilinearly polarized photons will be detected every other time and the others will be detected or not [38].

Ford optimizes road traffic and fights congestion. Thanks to a quantum-inspired algorithm, the manufacturer is able to assign a given route to each vehicle, for an average journey gain of 8% [39, 40].

OLED display materials developer *OTI Lumionics* is boosting its research into new materials by using quantum inspired technology to simulate a constituent molecule of OLED materials.

Case Western Reserve University (CWRU) is perfecting magnetic resonance imaging (MRI) technology. Using the quantum approach, the university has succeeded in improving image quality by 30% and reducing image acquisition time by a factor of three.

The Canadian company D-Wave has just released its fourth model: the D-Wave 2000Q. As its name suggests, it has twice as many quantum bits, with its 2000 qbits [41]. During tests, the machine was able to achieve calculation times 1,000 to 10,000 times faster than with conventional processors. However, it was necessary to design algorithms specific to this machine to obtain this result.

Application of quantum machine learning can help in improving pattern recognition, which, in turn, will make it easier for scientists to predict extreme weather events and potentially save thousands of lives a year [42]. With quantum computers, meteorologists will also be able to generate and analyse more detailed climate models, which will provide greater insight into climate change and ways to mitigate it.

Conclusion

We have seen that it is now 20 years since scientists realized that the conventional computer would soon reach its limits. This is why some of them have seen in quantum mechanics the future of the computer. However, many problems very quickly got in the way of their dream. Indeed, the quantum computer made all scientists dream because it has, in theory, no speed limit. But quantum mechanics is still very poorly mastered, which poses a huge problem when you want to build a machine based on it. Indeed, the reading of quantum information and the physical construction of the computer are still to this day an almost insurmountable obstacle.

However, all the promises made by the quantum computer encourage scientists to continue their research and to multiply experiments. It is the promises made by this exceptional computer that will enable it to see the light of day. Indeed, the considerable benefits derived from this machine have prompted the United States of America to fund research on the quantum computer and thus be able to realize it short after 2020.

This formidable machine will probably never be marketed to the general public. Indeed, although it has many advantages, the problems to develop it are too complicated to realize it in an industrial way. That is why only scientists and companies that need these incredible capabilities, such as the military or video game manufacturers, will be able to use it.

References

1. Feynman R. P. (1982), "Simulating Physics with Computers", Int. J. Theor. Phys., No. 6/7, 21 (1982).
2. Nielsen M. E. and Isaac L. Chuang, (2011), "Quantum Computation and Quantum Information", Cambridge U. Press.
3. Press W. H., Saul A., TeukolskyWilliam T. Vetterling, Brian P. Flannery (2007), "Numerical Recipes: The Art of Scientific Computing", 3rd edn. Cambridge University Press.
4. Pacher C., Abidin A., Lörunser T., Peev M., Ursin R., Zeilinger A., Larsson J. (2016), "Quantum Information Processing", 15, 327
5. Greenberger D. M., Horne M.A., Zeilinger A. (2007), 2007 arXiv0712.0921G
6. Shimony A. (2017), in "The Stanford Encyclopedia of Philosophy", ed. by Edward N. Zalta (Fall 2017 Edition), https://plato.stanford.edu/archives/fall2017/entries/bell-theorem/
7. Leibfried D., Blatt R., Monroe C. and Wineland D. (2003), Review of Modern Physics 75, 281
8. Vool U. and Michel Devoret (2017), arXiv:1610.03438v2.
9. Wiliams C. P. (2011), "Explorations in Quantum Computing", Springer.
10. I. A. Boutle, J. E. Eyre, and A. P. Lock (2014), "Seamless Stratocumulus Simulation across the Turbulent Gray Zone", Mon. Wea. Rev., 142 (2014).
11. Castelvecchi D. (2017), "Quantum Computers Ready to Leap out of the Lab", Nature, 541 (2017).
12. Childs A. and van Dam W. (2010), "Quantum Algorithms for Algebraic Problems", Rev. Mod. Phys., 82 (2010).
13. D. Deutsch (1985), "Quantum Theory, the Church-Turing Principle and the Universal Quantum Computer", Proc. Roy. Soc. London, Ser. A, 400 (1985).
14. Dudhia J. (2014), "A History of Mesoscale Model Development", Asia-Pacific J. Atmos. Sci., No. 1, 50 (2014).
15. M. Hawkins (2017), "Complex Supercomputer Upgrade Completed", ECMWF Newsletter, No. 151 (2017).
16. Hong S. Y. and Dudhia J. (2012), "Next-generation Numerical Weather Prediction: Bridging Parameterization, Explicit Clouds, and Large Eddies", Bull. Amer. Meteorol. Soc., 93 (2012).
17. Landauer R. (1961) "Irreversibility and Heat Generation in the Computing Process", IBM J. Res. Dev., 5 (1961).
18. MetOffice Science Strategy (2015): "2016-2021, Delivering Science with Impact", (MetOffice, 2015), http://www.metoffice.gov.uk/research/overview.
19. Montanaro A. (2016), "Quantum Algorithms: An Overview", npj Quantum Information, 2 (2016).
20. National Centers for Environmental Prediction Strategic Plan 2015-2019. Version 4, February 27 (NCEP, 2015), http:www.ncep.noaa.gov/director/strategic_plan/strategic_plan.pdf.
21. Lauritzen P. H., Jablonowski C., Taylor M. A., and Nair R. D. (Eds.) (2011), "Numerical Techniques for Global Atmospheric Models", Lecture Notes in Computational Science and Engineering, 80 (2011).
22. Brunet G., Jones S., and Ruti P. (Eds.), (2015), "Seam less Prediction of the Earth System: From Minutes to Months", WMO, No. 1156 (WMO, 2015).
23. Shin H. H. and S.-Y. Hong, (2013), "Analysis of Resolved and Parameterized Vertical Transports in Convective Boundary Layers at Gray-zone Resolutions", J. Atmos. Sci., 70 (2013).
24. Shor P. W. (1997), "Polynomial-time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer," Siam J. Computing, No. 5, 26 (1997).
25. Simmons A. J. and Hollingsworth A. (2002), "Some Aspects of the Improvement in Skill of Numerical Weather Prediction", Quart. J. Roy. Meteorol. Soc., 128 (2002).
26. Wedi N., Hamrud M., and G. Mozdzynski (2013), "A Fast Spherical Harmonics Transform for Global NWP and Climate Models", Mon. Wea. Rev., 141 (2013).
27. Smith J. and Mosca M. (2012), "Algorithms for Quantum Computers", in Handbook of Natural Computing,Springer, Berlin,
28. Trabesinger A. (2017), "Quantum Computing: Towards Reality", Nature Outline, 543 (2017).
29. Tygert M. (2010), "Fast Algorithms for Spherical Harmonic Expansions", III, J. Comput. Phys., 229 (2010).

30. Walters D., Boutle I., Brooks M., et al. (2017), "The Met Office Unified Model Global Atmosphere 6.0/6.1 and JULES Global Land 6.0/6.1 Configurations", Geosci. Model Dev., 10 (2017).
31. Wedi N., Hamrud M., and Mozdzynski G. (2013), "A Fast Spherical Harmonics Transform for Global NWP and Climate Models", Mon. Wea. Rev., 141 (2013).
32. Williamson D. L. (2017), "The Evolution of Dynamical Cores for Global Atmospheric Models", J. Meteorol. Soc. Japan, 85 (2007).
33. G. Zangl, D. Reinert, P. Tripods, and M. Baldauf (2015), "The ICON (ICOsahedral Non-hydrostatic) Modelling Framework of DWD and MPI-M: Description of the Nonhydrostatic Dynamical Core", Quart. J. Roy. Meteorol. Soc., 141 (2015).
34. Martin F. (2019), "Top 10 Unexpected future applications of quantum computers", https://listverse.com/2019/01/10/top-10-unexpected-future-applications-of-quantum-computers/
35. Zygelman B. (2018), "A first introduction to quantum computing and information", Springer.
36. Magniez F. "Introduction au calcul quantique", http://www.lri.fr/quantum
37. Fujii K. (2015), "Quantum Computation with Topological Codes", Springer Briefs in Mathematical Physics Bernstein D., Buchmann J., Dahmen E. (2008), „Post-Quantum Cryptography", Springer.
38. Buterin V. (2013), "Bitcoin is Not Quantum-Safe, and How We Can Fix it when Needed", Bitcoin Magazine. bitcoinmagazine.com/6021/bitcoin-is-not-quantum-safe-and-how-we-can-fix/
39. Diffie W., Hellman M. (1976) "New Directions in Cryptography". IEEE Transactions on Information Theory, IT-22: 644–54
40. Hagar A. (2011), "Quantum Computing", The Stanford Encyclopedia of Philosophy. plato.stanford. edu/entries/qt-quantcomp/
41. McMahon D. (2008), "Quantum Computing Explained", John Wiley & Sons, Inc., Hoboken, New Jersey.
42. Jan-Markus Schwindt, (2017), "Conceptual Basis of Quantum Mechanics", Springer.