Promising Real-Life Applications of Quantum Computing

Rania Al-Maghraby, MSc
Owner & General Manager, OneWayForward Inc.
rania@onewayforward.info

Abstract: **This paper explores the research areas of Quantum Computing, and the real-life applications in which this new field of research can transform human lives on earth. We first introduce the idea of Quantum Computing and how it is different from traditional computing, then we highlight main application areas and use cases of quantum technologies that will enhance people life and turn many experiments that had never been feasible before into a handy undertaking. The purpose of this paper is to emphasize the importance of Quantum Computing as a research area and the promising life changing applications that can come out of applied research in this field.**

Index Terms: **Quantum Computing, Computer Science, Computer Engineering, Applied Research**

I. Introduction

Quantum Computing is a research field at its infancy, like those old days when you tried to program a code by writing without having the ability to run it actually on a real computer. The current state of the this field shows that it's still far from being in the reach of researchers' hand at a wide scale, because of the lab technologies is relies upon. Actual experiments are limited to certain research institutes and commercial companies who have invested in building real quantum processors within the environment necessary to apply quantum physics interactions. However, many developments can still be done from a research point of view by exploring different applications and developing relevant algorithms.

"The story of quantum computers begins in 1981 with Richard Feynman, probably the most famous physicist of his time. At a conference on physics and computation at the Massachusetts Institute of Technology, Feynman asked the question: Can we simulate physics on a computer? The answer was—not exactly. Or, more precisely—not all of physics. One of the branches of physics is quantum mechanics, which studies the laws of nature on the scale of individual atoms and particles. If we try to simulate quantum mechanics on a computer, we run into a fundamental problem. The full description of quantum physics has so many variables that we cannot keep track of all of them on a computer." [1]

So the main motive behind the idea of Quantum Computing emerged from two fold concern: the need to study real-world natural phenomena, and the limitations of the traditional computing capacity and ability to cope with the requirements to fulfill this need. The best way to simulate and study the physical nature is to use its components to do computations. The basis lies in quantum physics and mathematics sciences.

II. Basic Idea

A quantum processor is mainly consisting of particles that are acting in certain physical nature when subjected to certain physical conditions.

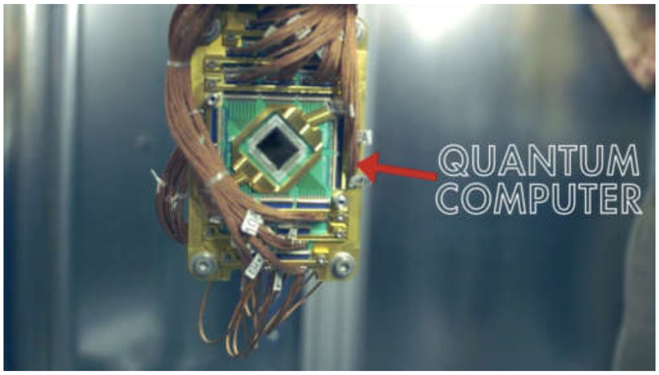


Fig. 1 The Quantum Processor

The *Bloch sphere* is a representation of a *qubit* (quantum bit), the fundamental building block of quantum computers. Qubits are made up of controlled particles and the means of control (e.g. devices that trap particles and switch them from one state to another). A qubit is the quantum version of a bit, and its quantum state can take values of |0>, |1>, or both at once, a phenomenon known as superposition. The half angle bracket notation |> is conventionally used to distinguish qubits.

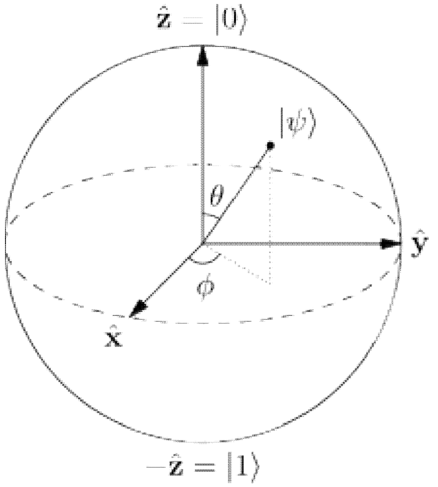


Fig. 2 The Bloch Sphere

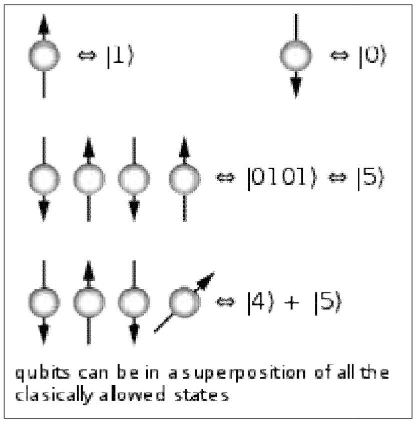
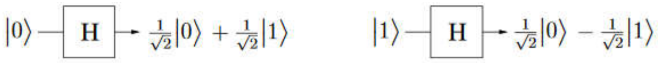

⇔ |1⟩
⇔ |0⟩
⇔ |0101⟩ ⇔ |5⟩
⇔ |4⟩ + |5⟩
qubits can be in a superposition of all the clasically alowed states

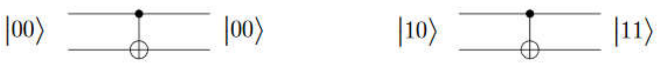
Fig. 3 Qubit States

It is hard to do any interesting computation with only a single qubit. Like classical computers, quantum computers use *quantum registers* made up of multiple qubits. When collapsed, quantum registers are bit strings whose length determines the amount of information they can store. In superposition, each qubit in the register is in a superposition of |1〉 and |0〉, and consequently a register of n qubits is in a superposition of all 2^n possible bit strings that could be represented using n bits. [9]

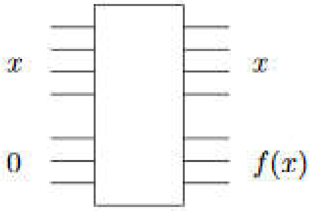
An elementary quantum operation is analogous to an elementary gate like the AND or NOT gate in a classical circuit. It operates upon either a single qubit or two qubits. One of the most important examples is the Hadamard gate, denoted by H, which operates on a single qubit. [11]


$|0\rangle$
H
$\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$
$|1\rangle$
H
$\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$

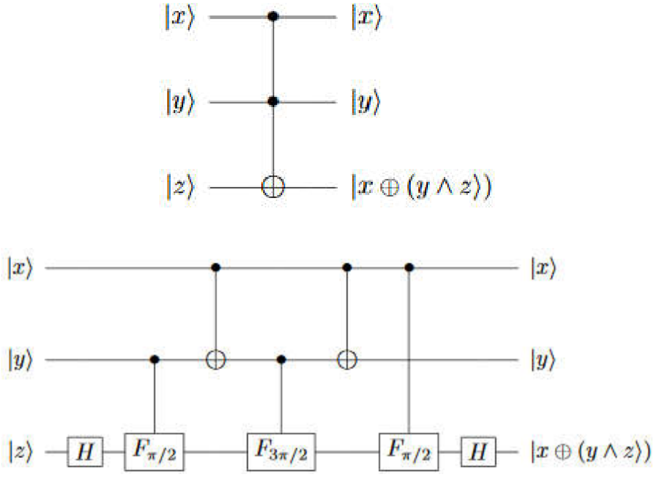
Another basic gate is the controlled- NOT, or CNOT. It operates upon two qubits, with the first acting as a control qubit and the second as the target qubit. The CNOT gate flips the second bit if and only if the first qubit is a 1. [11]



A quantum circuit takes some number n of qubits as input, and outputs the same number of qubits. In the diagram these n qubits are carried by the n wires going from left to right. The quantum circuit consists of the application of a sequence of elementary quantum gates to single qubits and pairs of qubits. [11]



The following is an example of a Toffoli gate and its decomposition:



III. Computational Complexity

Quantum computation introduces a number of new complexity classes to the polynomial hierarchy. Probably the most studied complexity class is Bounded-error Quantum Polynomial time, or BQP. BQP is the quantum extension of BPP: the class of decision problems solvable in polynomial time by an innately probabilistic quantum Turing machine, with the same error constraint as defined for BPP. Unlike BPP, it is suspected that P⊂BQP, which would mean that quantum computers are capable of solving some problems in polynomial time that cannot be solved efficiently by a classical Turing machine! [9]

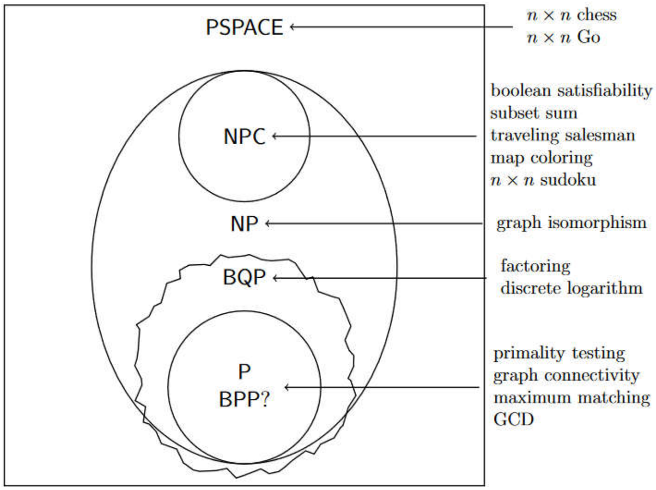


Fig. 4 The relationship between complexity classes

"Since the recent birth of quantum computing, the most important efforts have been invested in the search for new quantum algorithms that would show evidence of significant drops in complexity compared with classical algorithms. Obtaining new and convincing results in this area is clearly a crucial issue for making progress in quantum computing ... The quantum parts of algorithms are mostly described by drawing pictures of quantum gate networks, which are to quantum computing what logical gate circuits are to classical computing." [10]

IV. Research Updates

The most recent development in the field of Quantum Computing which represents a step forward towards wide scale uses of quantum computers is the latest announcement by Intel Technologies, which arrived at a test chip of 17-qubit superconducting which was delivered to QuTech, Intel's quantum research partner in the Netherlands. [2]

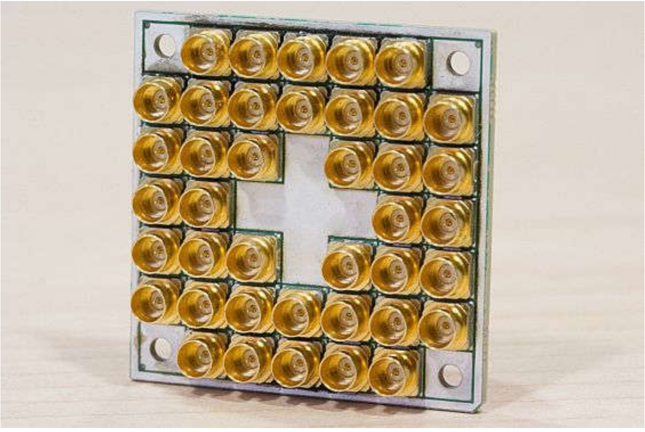


Fig. 5 Intel's chip of 17-qubit superconducting

In university research labs, an international team led by University of Surrey scientists were successful in manipulating atoms of phosphorous within silicon crystals, controlling their shape and size, essentially making them dance. To date, the majority of quantum computers have been made using materials that are not mass-produced, and often using atoms suspended in vacuum. This development highlight growing global dynamism towards creating functional quantum computers. [3]

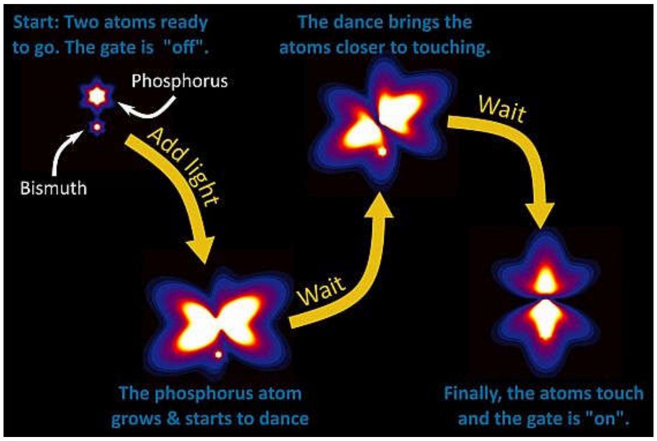


Fig. 6 Scientists were successful in manipulating atoms of phosphorous within silicon crystals, controlling their shape and size, essentially making them dance.

IBM in May 2017 announcing its most complex quantum system yet (at 16 and 17 quantum qubits of quantum volume, as opposed to the previous 5 qubit processor) while Google says it is on track this year to unveil a processor with so-called "quantum supremacy"—capabilities no conventional computer can match. [3]

Quantum computing is already redefining computer science and engineering, and all systems as we know them nowadays are going to be insecure and obsolete as the quantum computers get more usable and popular as current computers. This may take some time to happen but it will eventually occur.

Despite not yet much easy to develop and experiment, quantum computing algorithms can still be developed and submitted for simulation on publicly available labs at research arms of large enterprises. For example, IBM has made access to simulators and actual hardware of five and 16 qubits available as part of the IBM Q experience, which provides resources to learn and experiment with. They also have a quantum SDK, or Quantum Information Software Kit (QISKit) to make building circuits easy. See [4] for reference.

At the Russian Quantum Center (RCC or RQC) International Conference on Quantum Technologies (ICQT-2017), Harvard professor and RCC co-founder Mikhail Lukin presented results that shook up the conference as well as the industry at large. His announcement: his team had successfully created a 51-qubit quantum computer of a type that can –again, in theory – execute general computations.

According to a conference press release: “Lukin’s team has already solved several physical problems, extremely difficult to model with the help of ‘classical’ supercomputers ... To verify the results of these calculations, Lukin and his colleagues had to develop a special algorithm that allowed similar calculations to be performed in a very crude form on ordinary computers. The results on the whole coincided, it confirmed that the 51-qubit system of scientists from Harvard is working in practice.” [15]

V. Real-Life Applications

Currently, quantum computers are already in utilization in production environments at large corporations, including Google, IBM, NASA, etc. The most popular commercial provider of Quantum Computing hosting and processing environment is D-Wave Systems, a company based in North America, that also provides research and educational support services.

For the past 10 years, the number of qubits on D-Wave's QPUs has been steadily doubling each year. This trend is expected to continue. To create QPUs with numbers of qubits up to around 10,000, the current fabrication process can simply be scaled to add more qubits in the same way that they are arranged currently.

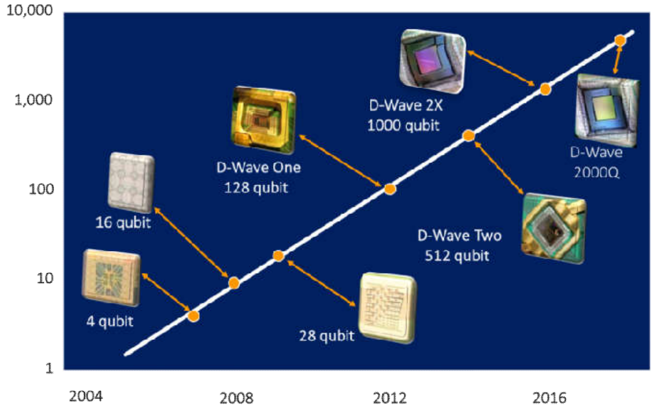


Fig. 7 Quantum Processor Development

In an interview with the CEO of the D-Wave company he said: "Google has created what they call the Quantum Artificial Intelligence Lab, where they’re exploring using our computer for AI applications or learning applications. And NASA has a whole set of problems that they’re investigating, ranging from doing things like looking for exoplanets to [solving] logistic problems and things like that. I’d say within five years, it’s going to be a technology that will be very much in use in all sorts of businesses." [6]

"While business applications within quantum computing are mostly hopeful theories, there’s one area where experts agree quantum could be valuable: optimization. Using quantum computing to create a program that “thinks” through how to make business operations faster, smarter and cheaper could revolutionize countless industries." [14]

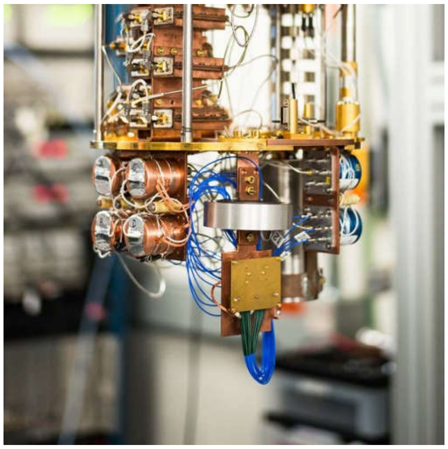


Fig. 8 View of Quantum Computer

While applications are in essence unlimited and not fully predictable, in the following we show some examples of tangible use cases that prove the promising advancements that quantum computing can provide to human life, thanks to the enormous processing capabilities of the quantum technology:

- Economy and Finance:
    - Analysis and simulation of stock portfolios for investment decisions
    - Agricultural and planting applications
    - More effective fraud detection and risk optimization in real time
- Medicine:
    - Research and development of medical sciences, e.g. analysis of DNA sequences which are usually of large size data
    - Bio-engineering and telemedicine relying on heavy image processing and analysis
    - Faster and more accurate diagnosis of critical diseases like cancer
    - Drug discovery and production at scale
- Natural Sciences:
    - Experiments that were too costly and time consuming to simulate and study are more convenient to carry out using the quantum computing power
    - Forecasting and time series analysis

- Information Technology:
    - Data searches and analysis of big data warehouses
    - Software tests and simulations that are too complex and time consuming for current computers
    - Artificial Intelligence and automation of many applied use cases, including traffic management, IoT and smart objects, where fast response and analysis of huge data collected by sensors is highly enhanced using the quantum processing capabilities
    - Algorithms design, where most limitations of traditional computing, in terms of processing time and space, are now much superseded by the quantum paradigm
- Management Optimization:
    - Supply chain and procurement: scenario analysis and decision making with regard to space and cost efficiency, distribution channels, transportation optimization, etc.
    - Asset and resource management: probabilistic modeling for cost savings and lifecycle management
    - Analytical capabilities in general, which leads to more insightful decision making process

VI. Threats of Quantum Computing

One of the threats that come with use of quantum computing is security issues pertaining to the fast processing capabilities of quantum computers which threatens all traditional information security techniques; passwords and encryptions that are used to take years to breach using current computers can now be cracked in almost no time.

"One area in which quantum computing is already having an impact is encryption. The most widely used techniques for encrypting and protecting transactions depend on the impossibility of swiftly finding the prime factors of large numbers. For example, it would take a classical computer 10.79 quintillion years to break the 128-bit AES encryption standard, while a quantum computer could conceivably break this type of encryption in approximately six months. This has led to a search for encryption methods that would be resistant to attacks from quantum computers—to make information systems quantum resistant." [8]

References

[1] Andris Ambainis, *What Can We Do with a Quantum Computer?*, Institute for Advanced Study, USA, 2014, https://www.ias.edu/ideas/2014/ambainis-quantum-computing.

[2] ITP Digital Media Inc., *Intel delivers 17-Qubit chip*, http://www.itp.net/615586-intel-delivers-17-qubit-chip?tab=article, November 2017.

[3] ITP Digital Media Inc., *Surrey University team announces breakthrough in quantum computing*, http://www.itp.net/613928-surrey-university-team-announces-breakthrough-in-quantum-computing?tab=article, July 2017.

[4] IBM Q online quantum computing experimental composer: https://quantumexperience.ng.bluemix.net/qx/editor

[5] D-Wave Systems, The Quantum Computing Company, https://www.dwavesys.com

[6] Interview with the CEO of D-Wave Systems, McKinsey & Company, https://www.mckinsey.com/industries/high-tech/our-insights/the-growing-potential-of-quantum-computing, February 2016.

[7] Accenture Labs, *Innovating with Quantum Computing*, https://www.accenture.com/t00010101T000000__w__/br-pt/_acnmedia/PDF-45/Accenture-Innovating-Quantum-Computing-Novo.pdf, 2017

[8] Deloitte Insights, *From fantasy to reality*, https://dupress.deloitte.com/dup-us-en/focus/signals-for-strategists/quantum-computing-enterprise-applications.html, April 2017

[9] Emma Strubell, *An Introduction to Quantum Algorithms*, https://people.cs.umass.edu/~strubell/doc/quantum_tutorial.pdf, 2011

[10] Philippe Jorrand, *A Programmer's Survey of the Quantum Computing Paradigm*, https://interstices.info/upload/docs/application/pdf/quantum_computing.pdf, year unknown.

[11] S. Dasgupta, C.H. Papadimitriou, and U.V. Vazirani, *Algorithms*, McGraw-Hill, 2006

[12] Edwin Pednault, *Quantum Computing: Breaking Through the 49 Qubit Simulation Barrier*, IBM Research Blog, 2017, https://www.ibm.com/blogs/research/2017/10/quantum-computing-barrier

[13] Michal Charemza, *Examples of Quantum Circuit Diagrams*, Warwick University, 2006

[14] *Quantum Computing Is Going Commercial With the Potential to Disrupt Everything*, Newsweek magazine, 2017

[15] Jason Bloomberg, *This Is Why Quantum Computing Is More Dangerous Than You Realize*, Forbes, 2017

About the Author

Ms. Rania Al-Maghraby, MSc Computer Science, is the owner and general manager of the OneWayForward Inc., a sole proprietary management consultation firm based in Egypt, with business activities extending across the regional and global landscape (www.onewayforward.com). She is the founder of the EAITSM Inc. NPO (www.eaitsm.org), an activist organization in the IT Service Management field with region-wide extension. Personal website: http://www.onewayforward.info.