Azerbaijan Journal of High Performance Computing, Vol 4, Issue 1, 2021, pp. 53-59
https://doi.org/10.32010/26166127.2021.4.1.53.59

Quantum Computing and Communications

Antonio Manzalini

Telecom Italia, Technology Innovation, Turin, Italy, antonio.manzalini@telecomitalia.it

*Correspondence: A. Manzalini, Telecom Italia, Technology Innovation, Turin, Italy, antonio.manzalini@telecomitalia.it

Abstract

Today, like never before, we are witnessing a pervasive diffusion of ultra-broadband fixed-mobile connectivity, the deployment of Cloud-native 5G network and service platforms, and the wide adoption of Artificial Intelligence. It has the so-called Digital Transformation of our Society: as a matter of fact, the transformative role of Telecommunications and Information Communication Technologies (ICT) has long been witnessed as a precursor of scientific progress and economic growth in the modern world.

Nevertheless, this transformation is still laying its foundations on Electronics and the impending end of Moore's Law: therefore, a rethinking of the long-term ways of doing computation and communications has been already started. Among these different ways, quantum technologies might trigger the next innovation breakthrough in the medium long-term.

In this direction, the paper provides an overview of the state of the art, challenges, and opportunities posed by an expected second wave of quantum technologies and services.

Keyword: Quantum computing, progress of ICT, QOC systems, quantum services, quantum computers

1. Introduction

Software-Defined Network (SDN) and Network Function Virtualization (NFV) are offering, today, the opportunity of designing and operating 5G (5th Generation) telecom infrastructures with unprecedented flexibility. In fact, an orchestrated use of Cloud, Edge-Fog computing, and network real/virtual resources can deliver a continuum of capabilities, functions, and services.

Innovation and sustainability of future telecom network scenarios will have to face several techno-economic challenges, such as: the transmission and processing of enormous, and increasing, the quantity of data with ultra-low latencies, automation of management and control processes, the fulfillment of the strict requirements of resilience, security and privacy, optimization of energy consumption, and so on.

Today, this global transformation is still laying its foundations on Electronics and the impending end of Moore's Law: therefore, a rethinking of the ways of doing computation and communications has been already started. Quantum technologies might create the conditions for the next innovation breakthrough meeting the above requirements.

The first quantum revolution started decades ago and has already brought quantum technologies into our everyday life. Chips for computers and smart-phone, systems for medical imaging (Nuclear Magnetic Resonance, Positron Emission Tomography), LED and lasers, etc., are all based on technologies exploiting the quantum mechanics principles.

We are witnessing a new impressive growth of interests in quantum technologies applications, with several investments from public and private organizations worldwide. In particular, there are three quantum phenomena, well known and demonstrated in Physics, which are expected to be at the basis of this second revolution: superposition, entanglement, and measurement. In particular:

- Superposition concerns the property of quantum objects to stay in the linear combination of multiple states until they are observed.
- Entanglement is defined as the possibility that two or more quantum objects stay intrinsically linked, into an intertwined composite state, regardless of how far apart the objects are from one another.
- Measurement regards the collapse and disruption of a quantum state from a coherent probabilistic superposition state into a discrete one.

When quantum technologies become mature enough to control and exploit these three phenomena, then the impact of this second revolution will cross many markets, ranging from Telecom and ICT to Medicine, to Finance, to Transportation, and so on.

2. Future applications of Quantum Technologies

International innovation activities and Standardization Bodies identify four primary application areas of quantum technologies and services, showing different TRL (Technology Readiness Levels): Communications, Computing, Simulations, Sensing, and Metrology.

- Quantum Computing concerns the exploitation of the three principles of superposition, entanglement, and measurements to speed up over classical computers in solving complex optimization and combinatorial problems.
- Quantum Communications includes two main sub-domains: the so-called quantum-safe communications and the “teleporting” of qubits (e.g., Quantum Internet, whose TRL is 1-2). Quantum-safe communications leverage on systems such as Quantum Key Distribution (QKD) and Quantum Random Number Generators (QRNG), which have a TRL 7-9, and as such reaching the market.
- Quantum simulations concerns all those applications where well-controlled quantum systems are used to simulate the behavior of other systems, which are less accessible and more complex for a direct simulation (TRL 6-9).
- Quantum sensing and metrology include those applications where high sensitivity of quantum systems to environmental influences can be exploited to measure physical properties and timing with more precision (e.g., magnetic and heat sensors, gravimeters, GPS-free navigators, clocks; TRL is 4-9).

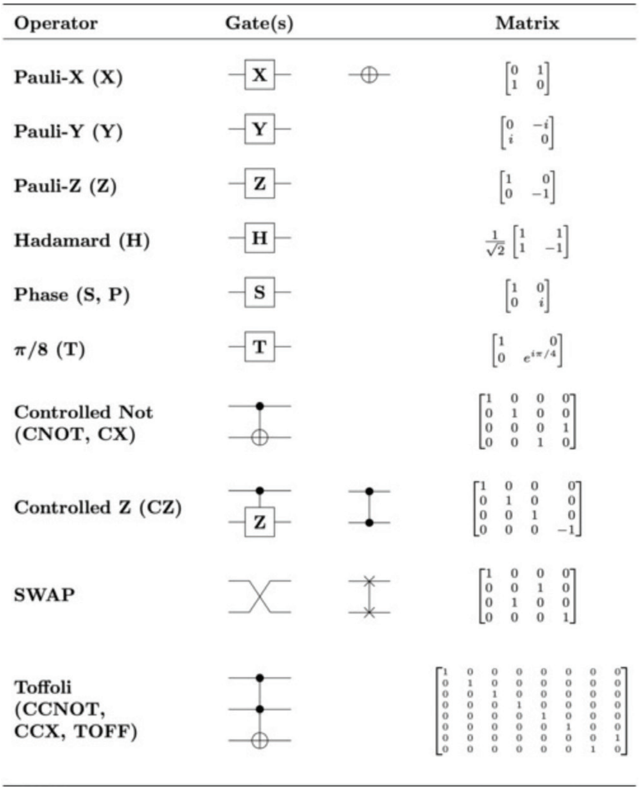
The following two sections will focus on Quantum Computing and Quantum Communications, which are the two applications that might impact the telecom and future internet scenarios more profoundly.

3. Quantum Computing

As a digital system manipulates Bits, a quantum system manipulates Qubits, the basic unit of quantum information. A Qubit can be coded by a quantum system having two states (or two levels), for example, the spin of an electron (spin up and spin down) or the polarization of a photon.

A weird property of quantum information is that a qubit can stay simultaneously with two values 0 and 1 (superposition of states), until it collapses, for example, when a measurement is made. In other words, while a Bit is either 0 or 1, a qubit can be seen as a linear combination of the two states (0, 1) with coefficients that are complex numbers. This allows representing the interactions between quantum states in terms of constructive and destructive interference of quantum information waves.

This means that two qubits can be in a superposition of four states, three qubits can be in a superposition of eight states, and so on. Therefore, generalizing while N bit can take one of 2^N possible permutations, N qubit can stay in a superposition of all 2^N possible permutations. This has remarkable consequences in computation. A quantum register - associated with N qubits - may have a state which is the superposition of all 2^N values simultaneously: therefore, applying a quantum operation to the quantum register would result in altering all 2^N values at the same time. This property allows quantum computers to elaborate qubits with "a sort of parallel computation," reducing



Operator	Gate(s)	Matrix
Pauli-X (X)	X	$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$
Pauli-Y (Y)	Y	$\begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$
Pauli-Z (Z)	Z	$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$
Hadamard (H)	H	$\frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$
Phase (S, P)	S	$\begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$
$\pi/8$ (T)	T	$\begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}$
Controlled Not (CNOT, CX)		$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$
Controlled Z (CZ)	Z	$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}$
SWAP		$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$
Toffoli (CCNOT, CCX, TOFF)		$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$

Fig. 1. Quantum Logic Gates (source https://en.wikipedia.org/wiki/Quantum_logic_gate)

the processing time (from exponential to polynomial time) to solve complex issues.

In general, there are two main classes of quantum computers:

- Analog quantum computers include annealers, adiabatic computers, i.e., systems that solve problems by directly manipulating the interactions between qubits rather than breaking actions into more abstract gate operations.
- Gate-based quantum computers, sometimes referred to as universal quantum computers, use logical gate operations (AND, OR, etc.) on qubits. Quantum logic gates are the building blocks of quantum circuits: CNOTs and unitary single-qubit operations form a universal set of quantum computing (figure 1).

It should be mentioned that it is also possible to simulate quantum–gates computers by using classical computers. A variety of software libraries can be used, each with different purposes: a comprehensive list of tools is available on Quantiki (Quantiki, n.d.). Simulation can be made, for instance, using OpenCL (Open Computing Language) (Kelly, A., 2018), which is a general-purpose framework for heterogeneous parallel computing on standard hardware, such as CPUs, GPUs, DSP (Digital Signal Processors), and FPGAs (Field-Programmable Gate Arrays).

There are multiple ways to build gate-based quantum computers manipulating qubits: superconductors and trapped ions are presently the most advanced implementations (Roadmap, O. O. Q. P., 2020).

3.1. Quantum Algorithms and Software

Most of the optimization problems in the fields of ICT and Telecommunications are currently solved with algorithms for finding suboptimal solutions because of the high cost of finding an optimal solution. A selection of these problems includes, e.g., network planning, joint optimization of multiple functions, such as radio channel estimation, data detection and synchronization, Data Center resources, and energy optimization.

Today, analog quantum computers (e.g., D-Wave) are already being used to solve combinatorial and optimization problems. Nevertheless, quantum annealers are not properly quantum computers: they are specialized computing systems based on quantum heuristics. In most cases, the problem to be solved is encoded into an Ising-type Hamiltonian, which is then embedded into a quantum hardware graph to be solved by a quantum annealer.

Gate-based quantum computers adopt another approach. For instance, figure 2 shows the comparison of the two approaches for executing quantum algorithms workflows. In the gate-based approach, the problem is formulated in a way for selecting a proper quantum algorithm. Then the quantum algorithm is transformed in a quantum circuit (i.e., using quantum gates), which is either executed on a quantum processor or simulated.

In both cases (analog and gate-based quantum computers), random fluctuations (e.g., heat or quantum-mechanical phenomena) could occasionally flip or randomize the state of qubits: this introduces errors and potentially derails the validity of the calculations. For this reason, many of these quantum systems require particular vacuum environments, the adoption of cryogenic systems, and error corrections methods. In particular, quantum error correction involves a substantial multiplication of resources: the number of physical qubits required may be orders of magnitude greater than the

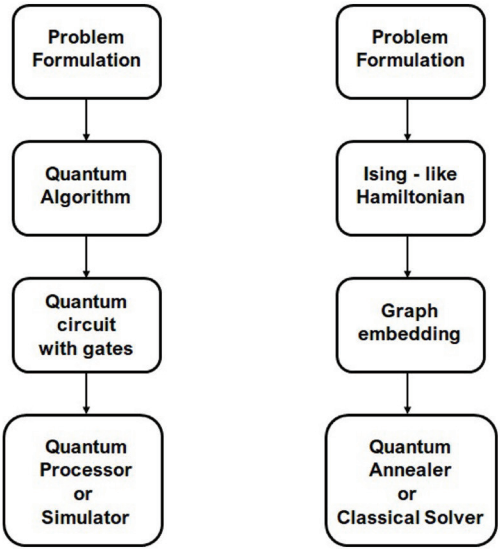


Fig. 2. Quantum algorithms workflows: on a gate-model computer (left), on a quantum annealer (right).

number of error-free logical qubits seen by the algorithm.

In general, we may say that there are two main quantum algorithms derived from Shor's algorithm for factoring (capable of breaking much public-key cryptography) and the Grover algorithm for searching. The website "Quantum Zoo" (Jordan, S., 2014) has gathered a comprehensive list of said classes of algorithms, briefly describing their operation. Concerning software languages and tools, the scenario is very active but still somewhat fragmented: the reference (Fingerhuth, M., Babej, T., & Wittek, P., 2018) provides an overview of open-source software projects and encourages the coalition of larger communities.

3. Quantum Communications

Electronics is currently beginning to face physically fundamental limitations (well described by the Moore law), posing some concerns about the long-term applicability of current electronics technologies for facing future communications requirements.

As mentioned, the most mature applications concern quantum-safe communications, specifically QKD and QRNG, which are already reaching the market. In this section, nevertheless, we look at the medium-long term applications. It is a common belief, for example, that, in the future, electronic technologies will be more and more complemented by Quantum Optics (QO), to develop Quantum Optical Communications (QOC).

QO has been a well-established field of research in physics since the end of the seventies. While telecom optics has been used mainly for wavelengths transmission with lasers over optical fibers, QO is a clever technique to transport and control optical signals with a more significant number of degrees of freedom. Decades of advances in QO have resulted from today in the techno-economic conditions where it is possible to start considering the concrete feasibility of QOC systems.

In general, as shown in Figure 3, QOC is synonymous with applications, such as Quantum Key Distribution (QKD) and super-dense coding (Wang, J., Paesani, S., Ding, Y., et al., 2018), capable of exploiting quantum mechanics principles to transport classical or even quantum bits of information. On the other hand, Quantum Optical Networks (QON) extends the concept of QOC since they can transport, elaborate and store quantum information (qubits).

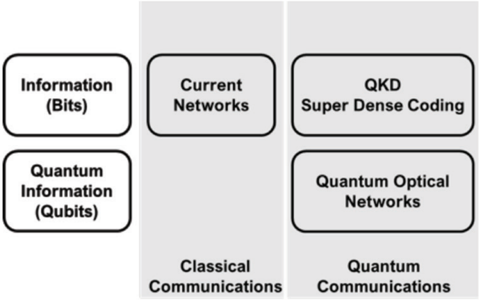


Fig. 3. Classical vs. Quantum Communications.

QON are not simply networks made of Wavelength Division Multiplexing (WDM) systems, add-drop multiplexers, and optical cross-connects nodes (which are used for multiplexing/demultiplexing, extracting, and routing different channels of light into an optical network). QON leverage phenomena with no counterpart in classical networks, such as no-cloning, quantum measurement, entanglement, and teleporting, which determine the emergence of new networking and computing capabilities.

Remarkably, these phenomena create an exponential speed-up for transporting and elaborating quantum information (e.g., in terms of qubits). At the same time, these phenomena impose new and challenging constraints on the design and operations of a QON. On the other hand, in QON, differently from classical optical networks, the no-cloning theorem hinders any uncontrollable inter-switching of an evil observer of quantum information: this prevents quantum information from being transmitted to more than a single destination. Moreover, novel router metrics should be defined, as it is, for example, the entanglement distribution that determines the connectivity of a quantum network for teleporting qubits.

Conclusions

The first quantum revolution has already brought quantum technologies into our everyday life for decades. Chips for computers and smart-phone, systems for medical imaging (Nuclear Magnetic Resonance, Positron Emission Tomography), LED and lasers, etc., are all based on technologies exploiting the quantum mechanics principles.

A second revolution seems to be underway, leveraging the three quantum principles of superposition, entanglement, and measurement. It is safe to predict that the second wave of quantum technologies could significantly impact many markets, ranging from Telecom and ICT to Medicine, to Finance, to Transportation, and so on. Significant work is still needed to develop enabling components and systems, but significant investments are being made worldwide across public and private organizations in light of the potential opportunities and threats.

A technological breakthrough is needed in quantum communications for developing quantum repeaters: this would be a critical step for long-distance QKD and distributed quantum computing. Concerning quantum computing, a roadblock mitigates random fluctuations that occasionally flip or randomize the state of qubits during processing. Innovative qubits coding (e.g., in topological computing) availability of efficient quantum error correction methods is the expected vital milestone. Quantum software scenario is very active but rather fragmented: significant efforts are directed to define languages to enable Programmers to work at the high level of abstraction.

Standardization efforts are also set to help to coordinate and accelerating the progress of quantum technologies. Multiple groups such as ANSI, ITU, IETF, ETSI, GSMA, and IEEE produce significant efforts. One relevant key aspect concerns integrating future quantum nodes and equipment (today, for example, QDK systems) in classic infrastructure (e.g., 5G): this requires the definition of interfaces and abstraction for management and control.

References

Fingerhuth, M., Babej, T., & Wittek, P. (2018). Open source software in quantum computing. *PloS one, 13*(12), e0208561.

Jordan, S. (2014). Algebraic and number theoretic algorithms. *Quantum Algorithm Zoo, The National Institute of Standards and Technology (NIST), http://math. nist. gov/quantum/zoo/, accessed Jan, 23,* 24.

Kelly, A. (2018). Simulating quantum computers using OpenCL. *arXiv preprint arXiv:1805.00988.*

Quantiki (n.d.) Quantum Information Portal and Wiki, available at https://quantiki.org/wiki/list-qc-simulators

Roadmap, O. O. Q. P. (2020). Every Photon Counts. *OIDA Report, 3,* 1-70.

Wang, J., Paesani, S., Ding, Y., et al. (2018). Multidimensional quantum entanglement with large-scale integrated optics. *Science, 360*(6386), 285-291.

Submitted: 25.07.2020
Accepted: 19.05.2021