Parallel Computing: Technology Trends
I. Foster et al. (Eds.)

doi:10.3233/APC200019

Will We Ever Have a Quantum Computer?

M.I. Dyakonov[1]

Laboratoire Charles Coulomb, Université Montpellier, France

Abstract. In the hypothetical quantum computing one replaces the classical two-state **bit** by a quantum element (**qubit**) with two **basic** states, ↑ and ↓. Its arbitrary state is described by the wave function $\psi = a\uparrow + b\downarrow$, where a and b are complex amplitudes, satisfying the normalization condition. Unlike the classical bit, that can be only in **one** of the two states, ↑ or ↓, the qubit can be in a continuum of states defined by the quantum amplitudes a and b. **The qubit is a continuous object**. At a given moment, the state of a quantum computer with N qubits is characterized by 2^N quantum amplitudes, which are continuous variables restricted by the normalization condition only. Thus, the hypothetical quantum computer is an **analog machine** characterized by a super-astronomical number of continuous variables (even for N~100÷1000). Their values cannot be arbitrary, they must be under our control. Thus the answer to the question in title is: When physicists and engineers will learn to keep under control this number of continuous parameters, which means - **never**.

Keywords. Quantum computing, qubits

1. Introduction

The idea of quantum computing was first put forward in a rather vague form by the Russian mathematician Yuri Manin in 1980. In 1981 it was independently proposed (also in a vague form) by Richard Feynman. Realizing that (because of the exponential increase of the number of quantum states) computer simulations of quantum systems become impossible when the system is large enough, he advanced the idea that to make them efficient the computer itself should operate in the quantum mode: "Nature isn't classical and if you want to make a simulation of Nature, you'd better make it quantum mechanical, and by golly it's a wonderful problem, because it doesn't look so easy". David Deutsch in 1985, formally described the universal quantum computer, as a quantum analog of the Universal Turing machine.

The subject did not attract much attention until Peter Shor in 1994 proposed an algorithm allowing to factor very large numbers on an *ideal* quantum computer much faster compared to the conventional (classical) computer. This outstanding theoretical result has triggered an explosion of general interest in quantum computing and many thousands of research papers, mostly theoretical, have been and still continue to be published at an increasing rate.

[1] Laboratoire Charles Coulomb, Université Montpellier, cc 070, 34095 Montpellier, France **michel.dyakonov@gmail.com**

2. Progress

During the last 20 years one can hardly find an issue of any science digest magazine, or even of a serious physical journal, that does *not* address quantum computing. Quantum Information Centers are opening all over the globe, funds are generously distributed, and breathtaking perspectives are presented to the layman by enthusiastic scientists and journalists. Many researchers feel obliged to justify whatever research they are doing by claiming that it has some relevance to quantum computing.

Computer scientists are proving and publishing new theorems related to quantum computers at a rate of ~ *ten articles per day*. A huge number of proposals have been published for various physical objects that could serve as quantum bits, or *qubits.* As of October 7, 2019, Google gives 6 970 000 results for "quantum computing", and 201 000 results for "quantum computing with", and these numbers increase every day. The impression has been created that quantum computing is going to be the next technological revolution of the 21st century. When will we have useful quantum computers? The most optimistic experts say: "In 10 years", others predict 20 to 30 years (note that those expectations have remained unchanged during the last 20 years), and the most cautious ones say: "Not in my lifetime". The present author belongs to the meager minority answering "Not in any foreseeable future", and this point of view is being explained below.

At a given moment the state of the *classical* computer is described by a sequence (↑↓↑↑↓↑↓↓…), where ↑ and ↓ represent *bits* of information – realized as the *on* and *off* states of individual transistors. With N transistors, there are 2^N different possible states of the computer. The computation process consists in a sequence of switching some transistors between their ↑ and ↓ states according to a prescribed program.

In *quantum* computing one replaces the classical two-state element by a quantum element with two *basic states*, the quantum bit, or *qubit.* The simplest object of this kind is the electron internal angular momentum, *spin*, with the peculiar quantum property of having only *two* possible projections on *any* axis: +1/2 or -1/2 (in units of the Planck constant). For some chosen axis, we again denote the two basic quantum states of the spin as ↑ and ↓.

However, an *arbitrary* spin state is described by the *wave function* $\psi = a\uparrow + b\downarrow$, where a and b are complex numbers, satisfying the condition $|a|^2 + |b|^2 = 1$, so that $|a|^2$ and $|b|^2$ are the *probabilities* for the spin to be in the basic states ↑ and ↓ respectively.

In contrast to the classical *bit* that can be only in *one of the two* states, ↑ and ↓, the *qubit* can be in a *continuum* of states defined by the quantum amplitudes a and b. This property is often described by the rather mystical and frightening statement that the qubit can exist *simultaneously* in *both* of its ↑ and ↓ states. (This is like saying that a vector in the xy plane directed at 45° to the x-axis *simultaneously* points *both* in the x- and y-directions - a statement that is true in some sense, but does not have much useful content.)

Note that since a and b are complex numbers satisfying the normalization condition, and since the overall phase of the wave function is irrelevant, there remain two free parameters defining the state of a single qubit (exactly like for a classical vector whose

orientation in space is defined by two polar angles). This analogy does not apply any more when the number of qubits is 2 or more.

With two qubits, there are $2^2 = 4$ basic states: (↑↑), (↑↓), (↓↑), and (↓↓). Accordingly, they are described by the *wave function* $\psi = a(\uparrow\uparrow) + b(\uparrow\downarrow) + c(\downarrow\uparrow) + d(\downarrow\downarrow)$ with 4 complex amplitudes *a, b, c*, and *d*. In the general case of *N* qubits, the state of the system is described by 2^N complex amplitudes restricted by the normalization condition only.

While the state of the classical computer with *N bits* at any given moment coincides with *one* of its 2^N possible discreet states, the state of a quantum computer with *N* qubits is described by the *values of* 2^N *continuous variables,* the quantum amplitudes.

This is the origin of the supposed power of the quantum computer, but it is also the reason for it's great fragility and vulnerability. The information processing is supposed to be done by applying unitary transformations (*quantum gates*), that change these amplitudes *a, b, c*... in a precise and controlled manner. The number of qubits needed to have a useful machine (i.e. one that can compete with your laptop in solving certain problems, like e.g. factoring very large numbers by Shor's algorithm) is estimated to be $10^3 - 10^5$. Thus the number of continuous variables describing the state of such a quantum computer at any given moment is at least 2^{1000} ($\sim 10^{300}$) which is much, much greater than the number of particles in the whole Universe (this is only $\sim 10^{80}$)!

At this point a normal engineer, or an experimenter, looses interest. Indeed, possible errors in a classical computer consist in the fact that one or more transistors are switched off instead of being switched on, or vice versa. This certainly is an unwanted occurrence, but can be dealt with by relatively simple methods employing *redundance*.

In contrast, accomplishing the Sisyphean task of keeping under control 10^{300} *continuous variables* is absolutely unimaginable. However, the QC theorists have succeeded in transmitting to the media and to the general public the belief that the feasibility of large-scale quantum computing has been *proved* via the famous *threshold theorem*: once the error per qubit per gate is below a certain value, indefinitely long quantum computation becomes feasible, at a cost of substantially increasing the number of qubits needed (the *logical* qubit is encoded by several *physical* qubits). Very luckily, the number of qubits increases only *polynomially* with the size of computation, so that the total number of qubits needed must increase from $N = 10^3$ to $N = 10^6$–10^9 only (with a corresponding increase of the *unimaginable* number of 2^N continuous parameters defining the state of the whole machine!!!).

3. Experimental studies

Experimental studies related to the idea of quantum computing make only a small part of the huge QC literature. They represent the *nec plus ultra* of the modern experimental technique, they are extremely difficult and inspire respect and admiration. The goal of such proof-of-principle experiments is to show the possibility to realize the basic quantum operations, as well as to demonstrate some elements of quantum algorithms.

The number of qubits used is below 10, usually from 3 to Apparently, going from 5 qubits to 50 (the goal set by the ARDA Experts Panel road map for the year 2012!) presents hardly surmountable experimental difficulties and the reasons for this should be understood. Most probably, they are related to the simple fact that $2^5 = 32$, while $2^{50} = 1125899906842624$.

By contrast, the *theory* of quantum computing, which largely dominates in the literature, does not appear to meet any substantial difficulties in dealing with millions of qubits. Various noise models are being considered, and it has been proved (under certain assumptions) that errors generated by "local" noise can be corrected by carefully designed and very ingenious methods, involving, among other tricks*, massive parallelism*: many thousands of gates should be applied simultaneously to different pairs of qubits and many thousands of measurements should be done simultaneously too.

An important issue is related to the *energies* of the ↑ and ↓ states. While the notion of *energy* is of primordial importance in all domains of physics, both classical and quantum, it is not in the vocabulary of QC theorists. (Surprisingly, they also have no use for other indispensable attributes of Quantum Mechanics, like Hamiltonian and Schroedinger equation).

They implicitly assume that the energies of all 2^N states of an ensemble of qubits *are exactly equal*. Otherwise, the existence of an energy difference ΔE leads to oscillations of the quantum amplitudes with a frequency $\Omega = \Delta E/\hbar$, where $\hbar$ is the Planck constant, and this is a basic fact of Quantum Mechanics. (For example, one of the popular candidates for a qubit, the electron spin, will make a precession around the direction of the Earth's magnetic field with a frequency ~ 1 MHz). Should the Earth's magnetic field be screened, and if yes, with what precision?

Whatever is the nature of qubits, some energy differences will necessarily exist because of stray fields, various interactions, etc. resulting in a chaotic dynamics of the whole system, which will completely disorganize the performance of the quantum machine. I am not aware of any studies of this very general problem.

Let us recall that our laptops have originated from the construction of the elementary **electronic calculator** which replaced the abacus in the 60is. Step by step improvements and developments of this simple device resulted in the supercomputers that we have today.

With quantum computing, this natural process has been reversed: the field started with fantastic promises of breaking security codes and changing our world forever. However, after more than 20 years of unprecedented hype there still is nothing real to show. Forget "quantum supremacy" and factoring atrociously large numbers. Just show us some working quantum device, however simple, e.g. a quantum school calculator which could perform operations like 3+5, or 3x5, and maybe even factor 15 by using Shor's algorithm! I would not mind if this quantum calculator had the size of a 3 story building and immersed in liquid Helium...

However, 25 years after Shor's seminal theoretical work, which triggered the whole field of quantum computing, and many, many billions of dollars spent, these

elementary tasks are still far beyond our capabilities. This fact does not inspire any confidence.

4. Conclusions.

The hypothetical quantum computer is a system with an unimaginable number of continuous degrees of freedom - the values of the 2^N quantum amplitudes with $N \sim 10^3$–10^5 . These values cannot be arbitrary, they should be under our control with a high precision (which has yet to be defined).

Riding a bike, after some training, we learn to successfully control 3 degrees of freedom: the velocity, the direction, and the angle that our body makes with respect to the pavement. A circus artist manages to ride a one-wheel bike with 4 degrees of freedom. Now, imagine a bike having 1000 (or 2^{1000} !) joints that allow free rotations of their parts with respect to each other. Will anybody be capable of riding this machine?

Thus, the answer to the question in title is: As soon as the physicists and the engineers will learn to control this number of degrees of freedom, which means - *NEVER*.

References

Some previous papers of the author on the same subject:

Quantum computing: a view from the enemy camp, Future Trends in Microelectronics. The nano Millenium, S. Luryi, J. Xu, and A. Zaslavsky (eds), Wiley (2002), pp. 307-318; arXiv:cond-mat/0110326

State of the art and prospects for quantum computing. Future Trends in Microelectronics. Frontiers and Innovations, S. Luryi, J. Xu, and A. Zaslavsky (eds), Wiley (2013), pp. 266-285; arXiv:1212.3562

Prospects for quantum computing: extremely doubtful, J. of Modern Physics, Conf. Series, **33**, 1460357 (2014); arXiv:1401.3629

The case against quantum computing, IEEE Spectrum, (March issue, 2019)
https://spectrum.ieee.org/computing/hardware/the-case-against-quantum-computing