FROM NIELS BOHR TO QUANTUM COMPUTING[*]

Klaus Mølmer, Department of Physics and Astronomy, University of Aarhus, Denmark[†]

Abstract

Quantum mechanics replaces determinism with probabilistic predictions for measurement outcomes and describes microscopic particles by wave functions as if they are simultaneously at different locations. The paradoxical properties of quantum mechanics caused painstaking discussions between Schrödinger, Einstein and Bohr who disagreed fundamentally about the meaning of the theory. Today, scientists and engineers try to harness the hotly debated issues of those discussions for technological applications in quantum encrypted data transmission and in quantum computing that uses quantum states to do many calculations in parallel.

INTRODUCTION

In 1913, Niels Bohr introduced his model of the atom with an electron orbiting the atomic nucleus as a satellite in orbit around a planet. In 1926 this description was replaced by Schrödinger's wave function which abandons the classical position and momentum of the electron and introduces a wave function which provides probabilistic information about where the electron will be found in an experiment. In 1927, Albert Einstein questioned whether the path that a particle takes through a double-slit apparatus could be determined by measurement in an experiment and, hence, reveal a "hidden" reality beneath the wave formalism. In 1935, with Podolsky and Rosen, he proposed that wave functions of two particles could be prepared such that probing of one particle would turn the probabilistic description of the other one into a state of definite position – "spooky action at a distance". Niels Bohr offered replies to both challenges which refined the interpretation of the theory, but both Einstein and Schrödinger remained skeptical, and physicists still have no single, common interpretation of the quantum theory.

For decades, a "shut up and calculate" attitude reigned and quantum mechanics was successfully employed in all areas of physics and chemistry, while only a small group of scientists kept pursuing the paradoxical aspects of the theory and the interpretation debate. This, however, changed after test experiments by John Clauser and Alain Aspect in the 1970's and 1980's showed that we may actually prepare quantum systems in the laboratories and demonstrate the features proposed as Gedanken experiments by Einstein. Not only, did this lead to a revived interest in the discussions of foundations, it also inspired a whole new approach to experimental quantum research, with an aim to design, prepare, and control, rather than merely observe quantum states and their evolution. It was quickly appreciated that cooling of atoms, squeezing of light, control of molecular wave packets … would enable new precise studies and applications, but also truly revolutionary possibilities emerged.

Among them were ideas to employ quantum mechanisms for applications outside of physics: quantum money that cannot be counterfeited, unbreakable quantum cryptograhy, and quantum computing. Richard Feynman's 1982 proposal for quantum computing also included the idea to simulate quantum many-body physics and chemistry by use of a suitably controllable quantum system.

Research in quantum computing has received much attention since the theoretical proposal of promising algorithms in the mid 1990's. Following generous funding for more than a decade, the European Union has just released its plan to sponsor a 1 Bn € Flagship in Quantum Technologies, engaging both Industry and Academia. Similar activities are operated at national level, and big companies like Google, IBM, Microsoft, Alibaba are very active in the area. A Canadian company, D-Wave, already offers a quantum computer/simulator on the market.

Table 1: Classical and Quantum Computer

	Classical Laptop	**Quantum Computer**
Processor	Intel i7	Not known
Clock	3.3 GHz	1 kHz
RAM	6 Gb	1000 bits
Price	1000 $	1 Billion $

Table 1 presents a brief comparison of some properties of conventional classical computers (left) and our optimistic expectations to the performance of a quantum computer (right). The reader may note that existing classical computers are about a million times faster, a million times larger and a million times cheaper (!) than their anticipated quantum counterpart. How can that be? This article will answer that question and review aspects of quantum computing from their basic principles, over the algorithms that they may employ to the physical architectures pursued in current research.

FROM BITS TO QUBITS

In modern computers data is encoded in physical properties such as voltages, currents, magnetizations, light intensities, etc., restricted to explore a pair of values designated to represent the logical bit values 0 and 1. Computing takes place as a physical process, involving suitable interactions among different physical components, and rules of digital logic show that basic one-bit and two-bit operations suffice to carry out any computation. In the electronics computer, the transistor accommodates the

[*] Work supported by the European Union's Horizon 2020 research and innovation program under grant agreement No 712721; and the ARL-CDQI through cooperative agreement W911NF-15-2-0061; and by the Villum Foundation.

[†] email address : moelmer@phys.au.dk

interactions between pairs of data bits, represented as electric voltages and the miniaturization of transistors and integration of circuit elements on chips have led to the incredible performance of modern computers.

The idea behind quantum computers is the simple observation that if a data bit can be encoded in discrete states |Ψ> = |0> or |1> such as the spin states of an electron or a nucleus or the electronic ground and excited states in an atom, then we can also prepare and manipulate *superposition states* of the form:

$$|\Psi > = a|0 > + b|1 >.$$

Such a state, in a sense, represents data values 0 and 1 at the same time, and we call it a quantum bit or qubit. Two qubits may simultaneously populate all four product states |00>, |01>, |10> and |11>, and N bits may simultaneously populate states representing all 2^N possible numbers that can be written by N bits.

Logical one- and two-bit operations such as NOT and XOR have quantum equivalents, and any classical computation can be implemented on a register of qubits, by a sequence of unitary processes, i.e., as the time evolution imposed by a suitable sequence of one-body and two-body interactions. The Schrödinger equation is linear, and an initial superposition state therefore must evolve into a superposition of the output states resulting from each input - the same way as a wavefunction, representing a particle at several locations, evolves during a scattering process into a final state wavefunction with several final locations or scattering directions. When applied to our multibit quantum register, we thus obtain the tantalizing possibility that a single run of a sequence of (gate) operations that constitutes our algorithm performs a simultaneous calculation on all possible input register states.

Just one quantum operation per second on 100 qubits, is equivalent to $2^{100} \sim 10^{30}$ classical bit operations per second and such a modest device, thus, vastly outperforms all existing computer resources since the existing billions of modern PC processors can perform “only” about 10^{20} bit operations per second.

Such a massively parallel processing power sounds too good to be true, and it *is*, indeed, too good to be true.

When the computer has finished its calculation, the results exist in the register superposition state, but readout is a measurement process and yields only a single, random outcome while all the other output state components of the superposition state are lost in the measurement process.

QUANTUM ALGORITHMS

The quantum computer was discussed by Feynman in 1982, but, due to the read-out problem, it was largely regarded as a foundational, rather than a useful concept, similar to Schrödinger’s cat and the Gedankenexperiments by Einstein. This, however, changed dramatically when Peter Shor in 1994 suggested an algorithm that can use quantum mechanics to solve the hard mathematical problem of prime factoring. We have no efficient method to find the factors of a large number, $N=x\cdot y$, and merely trying candidate values takes a number of trials roughly proportional to the smallest factor which may be of order $\sqrt{N}$ and thus scales exponentially with the data size of the input number (number of digits).

Note that while finding a factor may require tests of many candidate values, we only request the read-out of one output value in the end, and Shor’s algorithm exactly proposes how quantum parallel evolution may yield a final state with an almost certain measurement outcome that reveals the factors of N.

Widely used encryption schemes employ a mathematical operation on the secret message which takes a large number N as a parameter; N can be safely announced publicly by the recipient of the message, as long as she is the only one who knows its factors. She is therefore the only one who can subsequently decrypt the received message, as this operation requires use of the factors x and y and another mathematical function. In the war on terror (and out of curiosity concerning even their best allies’ smart phone conversations) several countries operate systematic eavesdropping activities, but without the ability to decrypt messages such activities make no sense.

Shor’s algorithm thus spurred great interest and funding for research and development of quantum technologies to enable construction of physical platforms capable to evolve and maintain quantum superposition states of many individual systems. In particular, military and intelligence authorities became interested, but with the proposal of other applications and algorithms and a growing number of connected applications for communication, sensing, synchronization, navigation, … , broader interests are now directed to quantum information technologies.

BUILDING A QUANTUM COMPUTER

The potential of quantum computing can only be released if we can build an actual device that allows coherent manipulation of single quantum two-level systems with high precision and over the times scales needed to carry out algorithms with, typically, thousands or millions of computational steps. The need for well isolated, long lived systems contrasts our need to interact efficiently with them and induce interactions between them, but a number of candidates currently compete for the functions as qubits. Figure 1 displays different physical systems that can serve as quantum bits. The figure illustrates schematically that these systems operate with quantum states differing by large or small energies (vertical axis), and that they may preserve a quantum superposition state for shorter or longer times (horizontal axis). Atomic states may be kept coherent for seconds and if one can address nuclear spin states even hours, while they may be addressed by rapid laser pulses driving single logical operations in just a fraction of a microsecond.

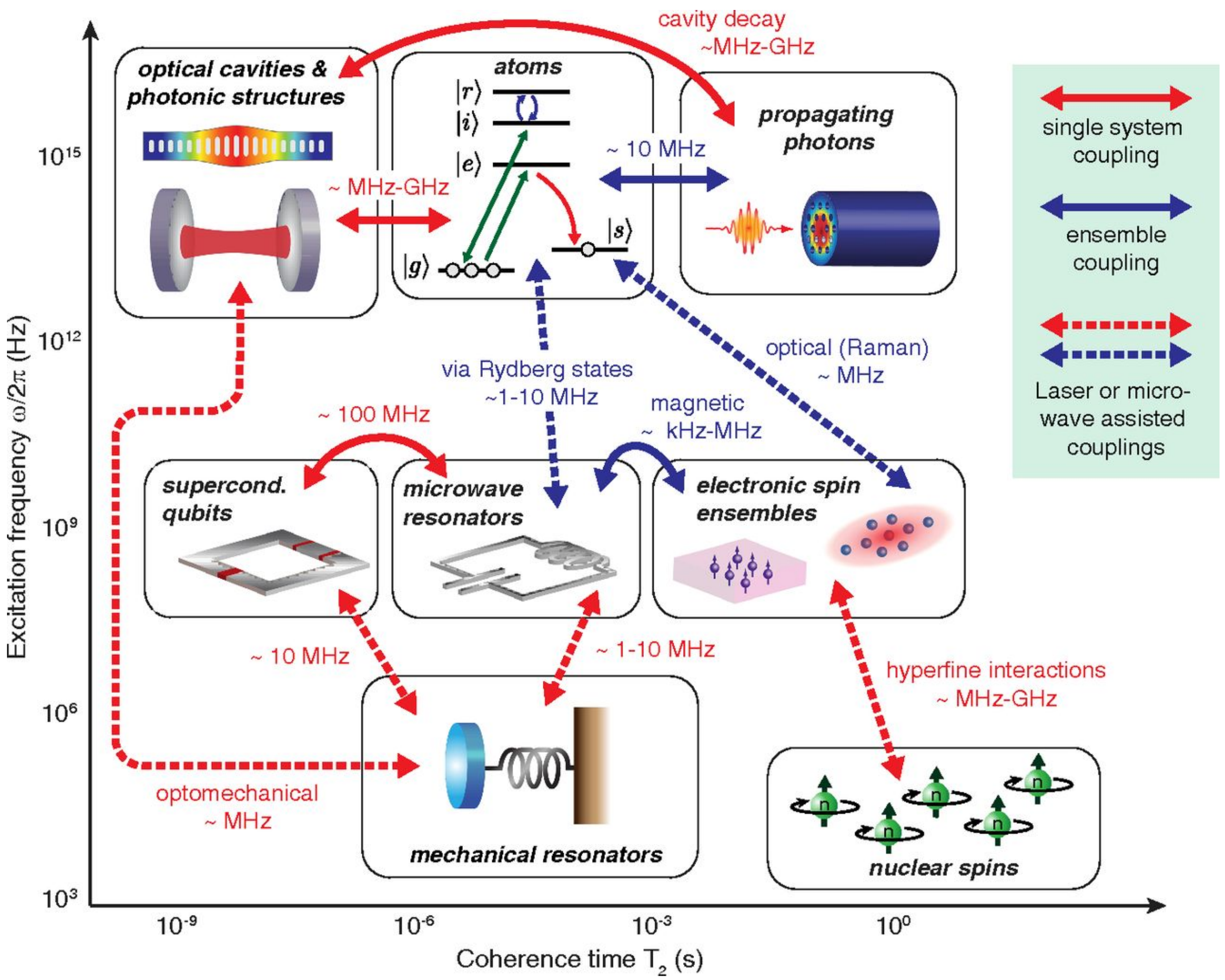

Figure 1: The diagram shows a selection of candidate physical systems for storage manipulation and transport of quantum states. The individual systems are placed in the diagram according to their characteristic excitation frequencies (vertical axis) and state storage life times (horizontal axis). The arrows indicate the existence of coupling mechanisms among the systems together with the corresponding coupling strengths g_{eff}. The red and the blue arrows represent the coupling between single systems and the coupling to and between ensembles of many systems, respectively. Couplings represented by dashed lines are accomodated by additional classical laser or microwave fields to bridge the different excitation energies. (Figure from G. Kurizki et al, PNAS **112**, 3866–3873 (2015), doi: 10.1073/pnas.1419326112)

The NOT gate, for example is accomplished by a laser π-pulse causing complete stimulated transfer between resonantly coupled energy eigenstates. The equivalent of a transistor, in which one data value controls another one, needs the evolution of one atom to depend on the state of another one – respecting that both atoms may populate superposition states before during and after the operation. In ion traps this coupling between different atoms is induced by the recoil imparted by photon absorption and emission and the Coulomb interaction between the ions which is sensitive to their motion. Neutral atoms may be excited into states with interacting dipole moments, which can effectively mediate two-bit quantum gates over micrometer distances. To build large architectures and to reach high precision gates among all register atoms is a big challenge, and is so far restricted to of order 20 atoms, with the best two-bit gates having success probabilities about 99.97 %.

In solid state systems such as semiconductor quantum dots and superconductor circuits, the coherence times are typically much smaller, but so are the gate times, and industrial efforts to build quantum processing devices currently focus on these systems. IBM and Google both promise release of 50 quantum bit devices in the near future. The Canadian D-Wave machine already operates a system of 1000 superconducting qubits, with a possibility to control time dependent couplings between some but not all qubits. This machine "solves its own Hamiltonian", and effectively finds minimum energy configurations of complex (classical) spin modes, but has no clear pathway to implementation of digital computing algorithms.

Since we will never reach infinite data storage times and 100 % perfect gate operations, quantum computers will rely on strategies to reduce and to repair errors. Robust storage in many particles, and error correction codes exist for that purpose, but they come with high demands on the added physical resources.

HYBRID QUANUM SYSTEMS AND THE THE QUANTUM INTERNET

Figure 1 also features photons, and nano- and optomechanical devices, which have favorable lifetimes but which need further efforts to restrict their dynamics to two-dimensional quantum state manifolds. These systems are oscillators and may be easily excited to higher states. They provide, however, ideal means to transfer quantum states and to mediate interactions between other degrees of freedom. Atomic quantum computers may be so large that we have to use light to couple and enable gates among remote atoms, and superconducting circuits may have too short lifetimes to store data for an entire computation, while they may be transferred to a microwave photon and further onto an electron spin excitation in a gas or solid material. These are arguments for the construction of hybrid architectures where each physical component is individually optimized to perform only certain tasks, while other components may be better suited for others.

In a future quantum information society, we may find the exchange and sharing of quantum messages as pertinent as the exchange of classical messages between our current computing and communication devices. For this purpose, guided or freely propagating electromagnetic fields would seem indispensable. Figure 1, thus, illustrates with arrows, how we may benefit from coupling and transfer of states among the different systems.

WHAT IF WE FAIL ?

Research in Quantum Computing brings many fields of physics together, and brings promises to help solve outstanding problems in physics. *E.g*,, many-body physics is prohibitively complicated to solve from first principles due to the curse of dimensionality, but this is exactly what the quantum computer handles so well. This had led to ideas both to simulate many-body and particle physics by engineering the relevant Hamiltonian on a system of controllable qubits, and to make algorithms that allow solution of the mathematical wave equations, diagonalization of matrices, identification of variational minima, of relevance to physics and chemistry. Some of these goals may be more tolerant towards errors and easier to achieve than the prime factoring problem.

Quantum computing research puts severe demands on our ability to control quantum systems experimentally and on our imagination and creativity to exploit different aspects of the theory. If brought into the present, Niels Bohr, Albert Einstein and Erwin Schrödinger would, undoubtedly, have been excited by the theoretical and experimental research in quantum information science. They may still not have agreed with each other on the interpretation of the theory, but the many laboratory demonstrations of the superposition principle, entanglement, and the effects of measurements might have been able to lead their discussion to a new level.

Shortly before Niels Bohr died in 1962, he reflected on the lessons taught by quantum mechanics: “If we should one day wake up and realize that it had all been just a dream, we would still have learned something”.

This statement also holds for the effort to tame quantum effects for information technologies. Even if we fail to build a quantum computer, we will pick up multiple technologies along the way, and quantum mechanics will never be the same!