From the Einstein-Bohr Debate to Quantum Information: a New Quantum Revolution?

1. A short history of the quantum revolutions: from concepts to technology and vice-versa

The development of quantum mechanics in the beginning of the 20th century obliged scientists and philosophers to change their worldview [1]. Based on the *revolutionary concept of wave-particle duality*, it became possible to understand and quantitatively describe the stability of matter, the mechanical and thermal properties of materials, the interaction between radiation and matter, and many other properties of the microscopic world that had been impossible to understand with classical physics. A few decades later, that *conceptual revolution* enabled a *technological revolution*. It is indeed quantum mechanics that allowed physicists and engineers to invent the transistor and the laser – at the root of our *information-based society* – as well as other wonderful applications such as magnetic resonance imaging, to name only one.

After such an accumulation of successes, one might think that by 1960, all the interesting questions about quantum mechanics had been raised and answered, and that one could focus on applying it. However, with his now-famous paper of 1964 [2], John Bell drew the attention of physicists to *a second revolutionary concept, entanglement*: quantum mechanics describes a pair of entangled objects as a single global quantum system, impossible to be thought of as two individual objects, even if the two components are far apart. The notion of quantum entanglement had been introduced by Einstein, Podolsky and Rosen in a 1935 paper [3], in order to argue that the formalism of quantum mechanics was incomplete, a conclusion strongly opposed by Bohr [4]. The most remarkable feature of Bell's work was undoubtedly the possibility to determine experimentally whether or not Einstein was right to conclude that quantum mechanics should be completed by introducing properties (physical reality) attached locally to each particle. The experimental tests of *Bell's inequalities* gave an unambiguous answer [5]: the properties of an entangled pair of particles are more than the sum of properties attached to each member of the pair. A few decades after the 1964 paper, the physics of entanglement is flourishing, and thousands of theoretical and experimental papers are found when one types *Bell's inequalities* into a search engine.

Starting in the 1970s, another concept has progressively become more and more important in quantum physics: the quantum description of *single objects*, in contrast to the statistical use of quantum mechanics to describe properties of large ensembles (for instance, the many atoms or molecules of a vapor). That question had also been the subject of debates involving Bohr, Einstein, Schrödinger, and others [6]. The development of experimental methods to isolate, observe and manipulate single microscopic objects [7] such as electrons, ions, atoms and even photons obliged physicists to consider the quantum evolution of single objects, and inspired the development of new theoretical approaches, the so-called Quantum Monte Carlo Wave Function simulations. More recently, progress in nanofabrication and in experimental methods have allowed physicists to create artificial quantum objects that push the border of the quantum world to larger and larger systems that still need to be described as single quantum objects.

It is not an exaggeration to say that the realization of the importance of entanglement and the clarification of the quantum description of single objects have been at the root of a *second conceptual quantum revolution*. It may well be that this once purely intellectual pursuit will also lead to *a new technological revolution*. Indeed, physicists have endeavored to use the control of individual quantum objects and apply entanglement to conceptually new ways of transmitting and processing information. These are the new fields of *quantum cryptography, quantum teleportation, quantum computation* and *quantum simulation*. If it keeps its promises, quantum information may have a dramatic impact on our societies, but we do not yet know the end of the story.

2. The first quantum revolution

Five years after the introduction by M. Planck of the quantization of energy exchanges between light and matter [8], A. Einstein took a major step further in 1905, by proposing the quantization of light itself to understand the photoelectric effect [9]. R. A. Millikan found experimental evidence in favor of Einstein's hypothesis [10]. Convincing evidence of the existence of atoms – doubted until the beginning of the twentieth century – was provided by various observations and arguments, including Einstein's explanation of Brownian motion [11]. Together with many other experiments, these observations convinced physicists and philosophers to accept the granularity of matter and energy in the microscopic world. Moreover, N. Bohr's 1913 model of the atom gave for the first time a quantitative description of the stability of atoms and of the way they emit or absorb light [12].

It took another decade to establish a comprehensive paradigm of quantum mechanics, centered around the 1925 formalisms of Heisenberg on the one hand, and Schrödinger on the other. The latter was a wave equation for matter, completing a beautiful duality: like light, matter can behave as either a particle or a wave, elaborating on the original idea of L. de Broglie [13]. The former, however, relied on the mathematics of matrices. The two formalisms were shown to be equivalent by Dirac. The success of this formalism was incredible. It became possible to understand chemical bonds, the electrical and thermal properties of matter, to describe particle physics, to understand exotic properties of matter such as superconductivity (the absence of electric resistance in some conductors at low temperature), or superfluidity (the absence of viscosity of liquid Helium at low temperatures). Studies in light-matter interaction were refined by orders of magnitudes, fitting perfectly within the quantum mechanical framework, which had been refined to be applied both in the elementary phenomenon (quantum electrodynamics) as well as in complex situations encountered in condensed matter. But in the early 1950s, quantum mechanics still appeared as a game to be played by physicists purely for the sake of progress in knowledge, without any impact on everyday life.

The electronics and information age: quantum mechanics applied

Even if the public is not always aware, the applications of quantum physics are all around us in electronics and photonics. The transistor was invented in 1948 by solid-state physicists, after fundamental reflections about the quantum nature of electrical conduction [14]. This invention and its descendents, micro-fabricated integrated circuits [15], clearly had a monumental impact. Like the steam engine over a century earlier, the transistor changed our lives and gave birth to a new era, the information age.

The second technological progeny of quantum mechanics is the laser, developed in the late 1950s [16]. Some of its applications are obvious in every day life: bar code readers, CD recorders and players, medical tools, etc. Less visible but perhaps more important is the use of laser light in telecommunications, where it dramatically boosts the flow of information: terabits (millions of millions of information units) per second can be transmitted across the oceans through a single optical fiber.

Basic research on atom-photon interactions has continued to develop, leading to applications. For example, in 1997 a Nobel Prize was given to S. Chu, C. Cohen-Tannoudji and W. D. Phillips for the development of methods for the cooling and trapping of atoms with lasers. Cold atoms are now used in a new generation of gravimeters based on atom interferometry, which allow us to explore the underground. Another spectacular application is cold atomic clocks, whose accuracy is now better than 10^{-17} (one second accuracy in three billion years – almost the age of the universe!) Better clocks will improve the accuracy of the global positioning system (GPS), as well as fast information transfer. Coming full circle, these improved clocks and gravimeters can be applied to fundamental questions, such as tests of general relativity, or the search for slow variation of fundamental physical constants. The first quantum revolution, with its interplay between basic questions and applications, is still at work.

3. From Einstein's questions to Bell's inequalities tests: entanglement comes of age - The Bohr-Einstein debate

Quantum mechanics was constructed at the price of several radical – and sometimes painful – revisions of classical concepts. For instance, to take into account particle-wave duality, quantum mechanics had to renounce the idea of a classical trajectory, as stated by the celebrated Heisenberg inequalities. One can also illustrate this renunciation of classical trajectories by remarking that in an interference experiment the particle "follows many paths at once."

Such renunciations were so radical that several – including Einstein and de Broglie – could not admit their inevitability, and so differed from Bohr, who had carved the Rosetta Stone of interpretation of the new theory under the name “the Copenhagen interpretation”. Einstein did not challenge the formalism and its provisions directly, but seemed to think that the renunciations put forward by Bohr could only signify the incompleteness of quantum formalism. This position led to Homeric debates when Einstein tried to find an inconsistency in Heisenberg inequalities, and Bohr always came up with a convincing rebuttal.

But in 1935, Einstein raised a completely different objection. Rather than considering the behavior of a single quantum particle, for which the Heisenberg relations state that the position and the velocity cannot be both perfectly defined, Einstein considered *two quantum particles*, and he discovered that the quantum formalism allowed this pair to be in a totally new kind of quantum state, named *an entangled state* by Schrödinger. In such a state, both the velocities of the two particles and their positions are strictly correlated. Therefore, by making a measurement of the position of one of the two particles, one can know with certainty the position of the other one. But we could instead have measured the velocity of the first particle and then infer the value of the velocity of the second. Since we could have waited until the last moment to choose between measuring the position or the velocity of the first particle, this choice could not have affected the second particle, because no influence can propagate faster than light according to Einstein’s relativity. Both the position and the velocity of the second particle were thus perfectly well determined before the measurement, Einstein argued, a possibility not envisaged by the standard formalism of Quantum Mechanics, which is thus incomplete. The reasoning was published in March 1935, in a paper authored by Einstein, Podolsky, and Rosen [3]. Bohr was reportedly shattered by the EPR paper, and it took him no more than four months to get his reply published [4]. He concluded that the EPR reasoning was not sufficient to conclude that quantum mechanics is incomplete. I have read Bohr’s paper many times, and I must admit that the detailed reasoning is not the clearest. But isn’t it Bohr himself who declared that “truth and clarity are complementary”, i.e., that by trying to be too clear, one may loose the depth of the scientific reasoning? In contrast to Bohr, Schrödinger reacted positively to the EPR paper, and coined the term “entanglement” to characterize the lack of factorability of an EPR state [17]. Actually, it seems that most of the physicists did not care much, since at that time it appeared that adopting one or the other point of view was only a matter of interpretation of quantum formalism. Indeed, Einstein and Bohr did not disagree on the results of the calculation, but on the conclusion to draw about the need or the possibility to complete that formalism.

It took another 30 years until John Stuart Bell totally changed the situation, when he discovered that taking Einstein's point of view seriously leads to inequalities in contradiction with the predictions of quantum mechanics. The debate had thus shifted from the domain of epistemology to the domain of physics, since it could be settled by questioning nature or by doing an experiment. Three pioneering experiments were carried out in the early 1970s. Two of them, by Clauser and Freedman, and by Fry, vindicated quantum mechanics against Bell's inequalities [18]. But these experiments were still different from the ideal scheme on which the theoretical debate was based, and it took us almost a decade to take advantage of the dramatic progress in optics (in particular in lasers), and come up with a series of experiments closer and closer to the core of the debate. These experiments were eventually carried out in 1981-1982 [19, 20]. The last experiment addressed for the first time the crux of Einstein's reasoning, since it was possible to rapidly switch the settings of the measuring apparatuses at the last moment, in order to prevent any possibility of communication at a velocity respecting the velocity of light speed limit. The result was clear: Bell's inequalities were still violated. Bohr was right: a pair of entangled particles, even widely separated in a relativistic sense, remained one global object that could not be considered as made of distinct components with individual properties. Further experiments have all confirmed a clear violation of Bell's inequalities, in schemes more and more ideal[a].

4. The second quantum revolution in action: quantum information

After the experimental observation of the violation of Bell's inequalities, it could be thought that it was the end of the story. But in fact some physicists, in particular Feynman [21], realizing that entanglement is definitely different from wave particle duality, proposed using it for new applications, and laid the groundwork for a new field of research, *quantum information*. Quantum information involves totally *new ways of transmitting and processing information*, such as quantum cryptography, quantum teleportation, quantum computing and quantum simulation. If these new

[a] A new, more precise and refined series of tests like these was performed in the 1990s [5], and a new generation of experiments is underway. M. Giustina, A. Mech, S. Ramelow, B. Wittmann, J. Kofler, J. Beyer, A. Lita, B. Calkins, T. Gerrits, S. Nam, R. Ursin, and A. Zeilinger, "Bell violation using entangled photons without the fair-sampling assumption," Nature **497** (7448), 227-230 (2013); B. G. Christensen, K. T. McCusker, J. B. Altepeter, B. Calkins, T. Gerrits, A. E. Lita, A. Miller, L. K. Shalm, Y. Zhang, S. W. Nam, N. Brunner, C. C. W. Lim, N. Gisin, and P. G. Kwiat, "Detection-Loophole-Free Test of Quantum Nonlocality, and Applications," Physical Review Letters **111** (13) (2013).

methods become practical and available on a large scale, they may well change our society as deeply as the inventions of the transistor, the integrated circuit and the laser, i.e., the fruits of the first quantum revolution, our society into the Information and Communication society.

Quantum cryptography [22]

Cryptography is the science of encoding and/or transmitting a secret message without its being read/understood by a third party. Both encoding and code-breaking have progressed due to advances in mathematics and to the ever-increasing power of computers. When contemplating the continuing progress of encrypting and code-breaking over the ages, it seems clear that the security of an encrypted transmission can be assured only on the hypothesis that the adversary (who is trying to break the code) has neither more advanced mathematics nor more powerful computers than the sender and intended receiver.

By contrast, in quantum cryptography, the security of a transmission rests on the fundamental physical laws at work in quantum mechanics. There, it is possible to detect an eavesdropper by using the trace that is *necessarily* left by him/her [23, 24], since in quantum physics all measurements perturb the system in some way. In quantum cryptography one can check the absence of such a trace, and then be certain that the message has passed without having been read by a spy.

In the method invented by A. Ekert [23], the extraordinary features of entanglement are used in a fascinating way. Two partners, Alice and Bob, can obtain two identical copies of encoding keys (to be used later), i.e., random series of 0 and 1, without the possibility that a spy intercepts the key, since the key does not exist before Alice and Bob effect their measurements. If a spy manages to make the key appear and take a copy of it, his/her presence will be revealed by the observation that Bell's inequalities are not violated, in contrast with the situation where there is no spy.

Many demonstrations of quantum cryptography have been carried out, and commercial systems are already available and experimented in commercial (banking) or government (elections) activities.

Quantum computing [25, 26]

In the early 1980s, the fundamental assumption in information theory—that all computers are conceptually equivalent— started to be challenged. Several scientists, for instance R. Landauer or D. Deutsch, suggested that if one had a quantum computer, one could implement radically new algorithms to perform certain tasks. A breakthrough happened in 1994 when P. Shor [27] showed that a quantum computer should allow one to factor large numbers in times much shorter than with conventional methods. Factorization belongs to a class of problems (complexity class) whose solution (with classical computers) requires a time super-polynomial in the size of the problem (that is, the time needed grows faster than any power of the number of digits in the number to be factored). With a quantum computer running Shor's algorithm, on the other hand, the computation time would only grow as a power of the size of the number[b]. This discovery had considerable conceptual implications, since it showed that, contrary to what had been thought previously, the complexity class of a problem was not independent of the type of machine used. It was also the starting point of an immense experimental effort worldwide aiming at realizing a quantum computer capable of implementing quantum algorithms like Shor's.

Several groups have started to develop the basic elements of a quantum computer: quantum bits and quantum gates. A quantum logic gate performs basic operations on quantum bits – or "qubits" – just as an electronic logic gate manipulates ordinary bits. However, in contrast to normal bits, which can take only one of the two values 0 and 1, quantum bits can be put in a superposition of 0 and 1. A quantum logic gate must thus be capable of combining two quantum bits to produce an entangled state, which is the superposition of the four possible combinations (0,0), (0,1), (1,0), (1,1), of the basic two-qubit states. It is the possibility to work with such entangled states that opens new, incommensurate possibilities as compared to the classical algorithms. To give a flavor of it, let us notice that if one entangles ten qubits, the number of combinations of 0 and 1 states is now $2^{10} = 1024$, while for 20 entangled qubits it is 2^{20} = about 1 million. This means that with a limited number of qubits, constituting a quantum register, one can in principle store a huge amount of information, and that any operation acting on an entangled state can process a huge quantity of information, realizing a kind of massively parallel computing.

Experimental research on quantum gates is extremely active, and has already obtained important results. Many approaches are being explored, with a diversity of physical realizations of qubits, including atoms, ions, photons, nuclear spins, Josephson junctions and RF circuits [28].

[b] It may make an enormous difference: see for instance the example in ref. 25, where the factorisation time of a 400 digit number can be reduced from the universe age to a few years.

For all these systems, there are large unknowns. A universal quantum computer would rely on the ability to entangle hundreds of thousands of quantum bits, and perform thousands of operations before decoherence disrupts the quantum register. Decoherence results from the interaction with the outside world, and its effect is to wash out entanglement, putting previously entangled objects into a state where they behave as separated objects. The scalability to a large number of entangled qubits may turn out to be overwhelmingly difficult, since it is generally observed that decoherence dramatically increases when the number of the entangled particles increases. An entire community of experimentalists and theorists are engaged in that quest. Understanding and reducing the effects of decoherence may well be the key question facing quantum computation as a technological revolution. But even in the absence of an efficient quantum computer, the idea of quantum computation is certainly a milestone in computation science.

Quantum simulation

In contrast to quantum computing with quantum gates and qubits, another kind of quantum computing is already operational, that is, quantum simulation. Quantum simulation is in fact what was primarily suggested in Feynman's paper [21] of 1982, often considered as the starting point of quantum information. In this paper, Feynman shows first that it is absolutely impossible to store a quantum state of many entangled quantum systems in a classical computer, since this would demand a number of bits larger than the number of atoms in the universe. He then concludes that the only support for such a huge quantity of information is a quantum system involving many entangled elementary quantum systems. A quantum computer made of many entangled quantum bits would be such a system. But there is another possibility, which has already led to several experimental implementations, including in my own laboratory. It consists of considering a situation difficult to investigate directly, for instance, many entangled electrons in a material, and simulating it with a system similar but offering more possibilities of study, such as many ultra-cold atoms in a potential synthetized with laser beams [29].

A first example is the case of electrons in a perfect crystal, i.e., in a perfect periodic potential. We can simulate such a situation by placing many ultra-cold atoms (atoms with motion perfectly controlled at the quantum level) in a potential constituted of laser standing waves whose intensity is modulated in an absolutely perfect periodic way along the three dimensions of space. This realizes a perfect lattice of potential wells where the atoms may be trapped. The cold atoms system has two main advantages.

Firstly, one has many observation tools allowing experimentalists to directly observe the atoms and record their distribution in space, or the distribution of their velocities. Secondly, one can change parameters such as the height of the barrier between neighbor trapping sites in contrast to the case of electrons in a piece of material, where the parameters are given by the very nature of the material and can hardly be modified. By lowering the barriers between the sites where atoms were trapped, experimentalists could observe a transition from a situation where the atoms are fixed to a situation where they can propagate freely [30]. This would correspond to a transition from an insulating to a supra-conducting state in the case of electrons, and such a quantum transition, called a Mott transition, had been predicted decades ago, but never observed directly until it was studied with ultra-cold atoms.

Another example, which has been studied in several laboratories including mine [31, 32, 33], is a completely different situation. The atoms are plunged in a disordered potential realized with laser beams, where the intensity varies randomly in space, achieving a disordered potential that we can describe accurately with the tools of statistical optics. This has allowed us to observe another emblematic phenomenon of condensed matter physics, Anderson localization [34, 35]. This fully quantum phenomenon was predicted more than fifty years ago. The prediction was that when the randomness of the potential is large enough (or equivalently the density of impurities in a material is large enough), the motion of the particles (the electrons in a material) would not only be hindered, but even totally stopped due to a quantum interference between the many multiple-scattering paths. This is again a quantum phase transition, which has never been observed directly with electrons in materials, but has been directly observed and studied with ultra-cold atoms [35].

To describe such condensed matter situations, only idealized theoretical models exist, and it often happens that we have no exact solutions with these models. Quantum simulators allow one to implement these models, explore their solutions by changing the parameters, and check whether some of these solutions correspond to the observed phenomena.

5. Conclusion: towards a second technological quantum revolution?

The second quantum revolution was first a conceptual revolution, based on the recognition of the revolutionary character of entanglement and on the manipulation and control of individual quantum objects, allowing experimentalists to entangle them. Quantum information has emerged as a consequence of this conceptual revolution, and one may wonder if it will change our society as deeply as the first quantum revolution did, bringing us into the information and communication society. We do not yet know the answer, but we can contemplate what has already been accomplished and what is left as an open question.

Quantum cryptography is already out of research laboratories, and one can even buy quantum cryptography systems from startup companies. This is not an insignificant application, when one considers the growing concern about privacy of communications. The fact that the security is absolute, at least as long as the laws of quantum physics remain valid, means dramatic progress. Indeed, one should remember that if somebody records a message encoded with a standard cryptography method today, it is very likely that a decade from now, it will be possible to decipher the message, owing to the continuous increase in the power of classical computers, and this may be very harmful. In contrast, a message encoded with quantum cryptography methods will remain secret forever, as far as quantum mechanical basic laws are not found to be false. This is why there are many efforts at the moment to develop quantum cryptography, on the one hand by extending the range of its implementation, which is not yet at the scale of continental or of intercontinental communications, and on the other hand by making its implementation more and more user friendly, and not reserved to sophisticated users such as governments or banks.

In contrast, it is fair to say that at the moment nobody knows whether it will be possible to build a general purpose quantum computer made of many quantum gates allowing one to entangle tens of thousands of quantum bits. At the moment, the world record is of fourteen entangled qubits realized with ions, and it is very unlikely that such technologies can be scaled up by a factor of more than one thousand, if no fundamental breakthrough happens. One should not underestimate, however, the fact that one has several examples of artificial quantum bits that have been realized with nanotechnologies, for instance, Josephson junctions or RF circuits operating in the quantum regime. With such artifacts, one has the perspective to scale up the number of entangled qubits, just like the technologies of microelectronics has made it possible to implant thousands, then millions and billions of transistors on a single wafer to realize the extraordinary modern microprocessors. But for the time being no such system exists, and this is why the alternative of quantum simulators is so attractive in order to attack important problems of condensed matter involving many entangled particles. Interesting results have already been obtained and constitute remarkable proofs of principle. There is reasonable hope that such simulators will allow us to understand hopefully intriguing material such as high critical temperature supraconductors, or more modestly amorphous silicon, essential for cheap photovoltaic cells.

From a conceptual point of view, it should be emphasized that trying to entangle more and more elementary quantum objects may have far reaching consequences. Nobody knows whether fighting the harmful effects of decoherence is just a matter of improving the technology, or if one will find an absolute scale beyond which it becomes impossible to entangle quantum particles. If this happened, it would not only mean that we have to renounce a quantum computer in the form that we are contemplating at the moment, but it would also be an extraordinary fundamental discovery, since it would mean that the frontier between the quantum world and the classical world has been identified. This question is still totally open, although it was raised almost one century ago, at the very beginning of quantum mechanics, when Bohr argued that in order to read the results of experiments on quantum objects, we need classical measuring apparatus. But he never told us where to put the frontier between quantum and classical objects.

Whatever the outcome of that quest, we will understand the quantum world much better. And on the other hand, I have no doubt that even if we don't have a quantum computer, we will have a host of quantum technologies stemming from the second quantum revolution.

Finally, I would like to express my thanks to two first class engineers who were intrumental for the success of the 1982 experiments, Gérard Roger and André Villing. There were also the already mentioned two (then) young master students, Philippe Grangier and Jean Dalibard, who joined me in the years 1981-1982 to complete the experiments for which I have received the Balzan Award. They have 'grown up' since that time, and are now famous quantum physicists. It was a privilege to have them with me at an early stage of their carrier.

Reference notes

[1] M. Jammer, "*The Philosophy of Quantum Mechanics*", New York: Wiley (1974): 303. This book was written too early to render full justice to Bell's contribution, but it is a very valuable source of historical details and references for the first quantum revolution.

[2] J. S. Bell, "*On the Einstein-Podolsky-Rosen-Paradox*", Physics **1**,195-200 (1964).

[3] A. Einstein, B. Podolsky, and N. Rosen, "*Can quantum-mechanical description of physical reality be considered complete?*," Physical Review **47** (10), 0777-0780 (1935).

[4] N. Bohr, “*Can quantum-mechanical description of physical reality be considered complete?,*” Physical Review **48** (8), 696-702 (1935).

[5] A. Aspect, “*Bell’s inequality test: more ideal than ever*,” Nature **398** (6724), 189-190 (1999).

[6] See chapter 10 in ref.1.

[7] H. Dehmelt, “*Experiments with an isolated subatomic particle at rest*”, Rev. Mod. Phys. **62**, 525530 (1990); W. Paul, “*Electromagnetic traps for charged and neutral particles*”, Rev. Mod. Phys. 62, 531540 (1990) ; G. Binnig and H. Rohrer, “*Scanning tunnelling microscopy from birth to adolescence*”, Rev. Mod. Phys. **59**, 615-625 (1987); S. Haroche, “*Nobel Lecture: Controlling photons in a box and exploring the quantum to classical boundary*,” Reviews of Modern Physics 85 (3), 1083-1102 (2013); D. J. Wineland, “*Nobel Lecture: Superposition, entanglement, and raising Schrödinger’s cat*,” Reviews of Modern Physics 85 (3), 1103-1114 (2013).

[8] M. Planck, XX, Verkandl. Deut. Phys. Ges., Dec 14 (1900).

[9] A. Einstein, *Über einen die Erzeugung und Verwandlung des Lichtes bettrefenden heuristischen Gesichtpunkt*, Ann. Physik, **17**, 132 (1905); *Zur Theorie der Lichterzeugung und Lichtabsorption*, Ann. Physik, **20**, 199 (1906).

[10] R. A. Millikan, “*A direct determination of ``h.”* ”, Phys. Rev., **4**, 73 (1914); *A Direct Photoelectric Determination of Planck‘s „h“*, **7**, 362 (1916).

[11] A. Einstein, *Zur Theorie des Brownschen Bewegung*, Ann. Physik, **19**, 371 (1906).

[12] N. Bohr, “*On the Constitution of Atoms and Molecules*,” Philosophical Magazine **26** (155), 857-875 (1913); N. Bohr, “*On the Constitution of Atoms and Molecules*,” Philosophical Magazine **26** (153), 476-502 (1913); N. Bohr, “*On the Constitution of Atoms and Molecules*,” Philosophical Magazine **26** (151), 1-25 (1913).

[13] L. de Broglie, *Recherches sur la théorie des quanta*, Thèse de doctorat, Paris (1924), Annales de Physique, $10^{\text{è}}$ série, vol. III, 22-128 (1925).

[14] J. Bardeen and W. H. Brattain, “*The Transistor, A Semi-Conductor Triode*”, Phys. Rev. **74**, 230231 (1948).

[15] J. S. Kilby, “*Turning Potential into Reality: The Invention of the Integrated Circuit*”. Z. I. Alferov, *“The double heterostructure concept and its applications in physics, electronics and technology*”. Herbert Kroemer, “*Quasi-Electric Fields and Band Offsets: Teaching Electrons New Tricks*”: Nobel Lectures (2000), Physics 1996-2000 (World Scientific), also available at http://www.nobel.se/physics/laureates/2000/.

[16] Charles H. Townes, “*Production of coherent radiation by atoms and molecules*”. Nicolay G. Basov, “*Semiconductor lasers*”, A. M. Prokhorov, “*Quantum*

electronics", (1964), in Nobel Lectures, Physics 1963-1970 (Elsevier), also available at http://www.nobel.se/physics/.

[17] E. Schrödinger, "*Discussion of probability relations between separated systems*," Proceedings of the Cambridge Philosophical Society 31, 555-563 (1935).

[18] See references in J.F. Clauser and A. Shimony, *"Bell's theorem: Experimental tests and implications"*: Rep. Prog. Phys. **41**, 1881 (1978).

[19] A. Aspect, P. Grangier, and G. Roger, *"Experimental realization of Einstein-Podolsky-Rosen-Bohm Gedanken Experiment: a new violation of Bell's inequalities"*: Physical Review Letters **49**, 91 (1982).

[20] A. Aspect, J. Dalibard, and G. Roger, *"Experimental tests of Bell's inequalities using variable analysers"*: Physical Review Letters **49**, 1804 (1982).

[21] R. P. Feynman, *"Simulating physics with computers*": International Journal of Theoretical Physics **21** (6-7), 467-488 (1982).

[22] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, *"Quantum cryptography"*: Review of modern physics **74,** 145-195 (2002).

[23] A. K. Ekert, *"Quantum cryptography based on Bell's theorem"*, Phys. Rev. Lett. **67**, 661 (1991).

[24] C. H. Bennett, G. Brassard, N. D. Mermin, "*Quantum cryptography without Bell's theorem"*, Physical-Review-Letters.**68,** 557 (1992) and references therein.

[25] J. Preskill, Course Notes for Physics 219: *Quantum Computation*, http://www.theory.caltech.edu/~preskill/ph219.

[26] M. A. Nielsen, I. Chuang-Isaac, and K. Grover-Lov, "*Quantum Computation and Quantum Information"*, American-journal-of-physics **70**, 558-559 (2002); M. A. Nielsen, and I. Chuang-Isaac, "*Quantum Computation and Quantum Information"*, Cambridge University Press (200).

[27] P. W. Shor, "*Algorithms for quantum computation: discrete logarithms and factoring"*, Proceedings.-35th-Annual-Symposium-on-Foundations-of-Computer-Science (ed. by S. Goldwasser) 124-34, IEEE Comput. Soc. Press, Los Alamitos, CA (1994).

[28] L. M. K. Vandersypen, M. Steffen, G. Breyta, Yannoni, M. H. Sherwood, I. L. Chuang, "*Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance"*, Nature **414**, 883 (2001); D. Jaksch, J. I. Cirac, P. Zoller, S. L. Rolston, R. Cote, and M. D. Lukin, "*Fast quantum gates for neutral atoms*," Physical Review Letters **85** (10), 2208-2211 (2000); C. Monroe, D. M. Meekhof, B. E. King, W. Itano, D. J. Wineland, "*Demonstration of a fundamental quantum logic gate"*, Physical-Review-Letters **75**, 4714 (1995); S. Guide M. Riebe, G. P. T. Lancaster, C. Becher, J. Eschner, H. Haffner, F. Schmidt-Kaler, I. L. Chuang, R. Blatt,

"*Implementation of the Deutsch-Jozsa algorithm on an ion-trap quantum computer"*, Nature **421**, 48 (2003); A. Rauschenbeutel, G. Nogues, S. Osnaghi P. Bertet, M. Brune, J. M. Raimond, S. Haroche, "*Coherent operation of a tunable quantum phase gate in cavity QED"*, Physical-Review-Letters **83**, 5166 (1999); D. Vion, A. Aassime, A. Cottet P. Joyez, H.Pothier, C. Urbina, D.Esteve, M. H. Devoret, "*Manipulating the quantum state of an electrical circuit* », Science **296**, 886 (2002) and references therein; J. M. Martinis, S. Nam, J. Aumentado, and C. Urbina, "*Rabi oscillations in a large Josephson-junction qubit*," Physical Review Letters **89** (11) (2002); J. Majer, J. M. Chow, J. M. Gambetta, J. Koch, B. R. Johnson, J. A. Schreier, L. Frunzio, D. I. Schuster, A. A. Houck, A. Wallraff, A. Blais, M. H. Devoret, S. M. Girvin, and R. J. Schoelkopf, "*Coupling superconducting qubits via a cavity bus*," Nature **449** (7161), 443-447 (2007); A. Blais, J. Gambetta, A. Wallraff, D. I. Schuster, S. M. Girvin, M. H. Devoret, and R. J. Schoelkopf, "*Quantum-information processing with circuit quantum electrodynamics*," Physical Review A **75** (3) (2007).

[29] I. Bloch, J. Dalibard, and W. Zwerger, "*Many-body physics with ultracold gases*," Reviews of Modern Physics **80** (3), 885-964 (2008).

[30] M. Greiner, O. Mandel, T. Esslinger, T. W. Hansch, and I. Bloch, "*Quantum phase transition from a superfluid to a Mott insulator in a gas of ultracold atoms,"* Nature **415** (6867), 39-44 (2002).

[31] J. Billy, V. Josse, Z. C. Zuo, A. Bernard, B. Hambrecht, P. Lugan, D. Clement, L. Sanchez-Palencia, P. Bouyer, and A. Aspect, "*Direct observation of Anderson localization of matter waves in a controlled disorder*," Nature **453** (7197), 891-894 (2008); F. Jendrzejewski, A. Bernard, K. Muller, P. Cheinet, V. Josse, M. Piraud, L. Pezze, L. Sanchez-Palencia, A. Aspect, and P. Bouyer, "*Three-dimensional localization of ultracold atoms in an optical disordered potential*," Nature Physics **8** (5), 398-403 (2012).

[32] G. Roati, C. D'Errico, L. Fallani, M. Fattori, C. Fort, M. Zaccanti, G. Modugno, M. Modugno, and M. Inguscio, "*Anderson localization of a non-interacting Bose-Einstein condensate*," Nature **453** (7197), 895-U836 (2008).

[33] S. S. Kondov, W. R. McGehee, J. J. Zirbel, and B. DeMarco, "*Three-Dimensional Anderson Localization of Ultracold Matter*," Science **333** (6052), 66-68 (2011).

[34] P. W. Anderson, "*Local Moments and Localized States*," Reviews of Modern Physics **50** (2), 191-201 (1978).

[35] A. Aspect and M. Inguscio, "*Anderson localization of ultracold atoms,"* Physics Today **62** (8), 30-35 (2009).

Questions and Comments

Peter Meier-Abt

Thank you very much for this brilliant talk. So, I'm not a physicist, but let me ask one question. I worked in Basel, and you probably know the people there… quantum physics and quantum computing is very popular, and they always said, that a quantum computer is possible. When talking to physicists in Zurich, they were very sceptical, and said they have been talking about that for a long time, and that quantum computers will probably never exist. Now, what is your opinion?

Alain Aspect

To have a general quantum computer, that is to say, a computer on which you can implement a general kind of algorithm, it would demand at least a hundred thousands entangled qubits. But I have explained that when you want to entangle more and more qubits, decoherence is more and more harmful. The world record at the moment, which is held by Reiner Blatt in Innsbruck, is 14 (one four) entangled ions. So there's a long way to go. My personal belief is that, either we find something new, for instance, some sub-space of the Hilbert Space that is well-protected from decoherence, or we will not have a quantum computer in its most general form.

This quest is, however, fascinating for the following reason. I explained that if we have a really large number of entangled qubits, it's like Schrödinger's cat, and this addresses an important question about the frontier between the quantum and the classical world. Nobody knows where this frontier is. Now there is a possibility that by trying to entangle more and more qubits, people will discover a fundamental reason why we cannot pass a certain scale. This would answer the question of the frontier between quantum and classical worlds. It is still an extraordinarily important question, and in my opinion, this is one of the good reasons to try to build a quantum computer.

On the other hand, there is a simpler version of a quantum computer, which is a quantum simulator, as proposed by Feynman in his paper in 1982. Such simulators, I'm pretty sure, will give results that we could not calculate by normal techniques.

So the answer about the possibility of a quantum computer is 'maybe yes, maybe no'. Make your choice.

Peter Meier-Abt

Thank you very much. A question from Professor Quadrio Curzio?

Alberto Quadrio Curzio

I am an economist, and I really admired your presentation on the one hand, but am worried by it on the other, because these days the speed of computers is already too fast for dealing with economic systems. In fact, the speed and the power of ICT and computers has split the world economy into at least three "sectors": the real economy, which deals with goods, commodities and services connected to them; the financial and banking economy, which is strictly connected with the real sector by financing it; the high speed financial sector, which grows continuously in increasingly sophisticated trading systems. While the first two sectors move at a relatively similar speed, the third one moves much faster.

My question is: what is going to happen when this kind of quantum information is applied to economic systems? Are we going to have an "econo-quantum", which has a speed so high that no one will be able to control it? In the past we had political economics, then mathematical economics and then physics-economics. In the future will we have quantum economics?

I think that these revolutionary events might have enormous consequences on the markets, because the speed of transactions increases more and more, and even now it is already practically impossible to control the speed of the computer in buying and selling financial assets. The split between the world yearly GDP and the total amount of yearly financial transactions is continuously increasing, and so it is more and more difficult for institutions to regulate markets.

I understand that my question is a little bit outside the field, but I think it is a fundamental one for economists.

Alain Aspect

You are right. Physicists have always considered this kind of question. For instance, progress in relativity and quantum mechanics gave the atomic bomb. This is another example where physics can have bad consequences. I think there is only one answer: it's regulation. I mean, there are treaties against nuclear bombs being developed everywhere. It belongs to governments to make such regulations.

Where does physics come in the solution? In providing tools. Physicists have provided the tools to check that the treaties on nuclear arms are respected. Similarly, if governments make rules against fast trading, we can provide accurate methods to check that people do not violate the rules about the timing. But we physicists, or you economists, cannot implement the rules. Economists can explain to governments why they should make rules, and we can provide the tools to implement the rules. So we should work hand in hand.

Peter Meier-Abt

Thank you very much. We have time for one last question.

Milan Ilic, journalist

You mentioned your colleague Anton Zeilinger. He lives in Vienna, and I know him personally. He has recently been elected President of the Austrian Academy of Sciences, and my question regards him: have we already been witnesses to the beginning of the third revolution in the field of cryptography? Because as far as I know, several years ago, Zeilinger proved that he could send crypted messages – *Verschränkungen* – under the Danube for several kilometres.

Alain Aspect

Anton Zeilinger is part of a big European consortium, which was strongly supported by the European Union, a program that has demonstrated practical quantum cryptography. It has been very successful. As an outcome of it, there have been several start-up companies. There is one in France, and in many other countries as well. A very advanced one is in Switzerland. It is called ID Quantique and was put forward by former students and collaborators of Nicolas Gisin. And ID Quantique is so successful – if we can speak of success – that Swiss banks are using quantum cryptography for preserving the banking secret (you can comment on that if you want…). But it was also used in Switzerland to communicate the results of the votes from one office to another, just to show that it can really work in the real world. And so there's absolutely no doubt that quantum cryptography will be used.

Last week I met the European commissioner on new technologies, Nellie Kroes. She was extremely excited about quantum. And I'm pretty sure that quantum cryptography will be used, maybe not on iPhones, but at least when you really want to be sure of secrecy. You should realize one point: if nowadays people register messages encoded with the RSA method, so that they cannot decipher the messages today, they will be able to decipher the messages ten year from now, with the increase in computers' power. And it may be harmful.

In contrast, if you use quantum cryptography, in principle, it's forever, unless we discover that quantum mechanics has a flaw. But as far as quantum mechanics works, quantum cryptography is secure.

Thus, I am not sure regarding quantum computing, but I am pretty sure regarding quantum cryptography. Also regarding quantum simulators, I'm pretty sure we're going to have results.

Peter Meier-Abt

Thank you all very much.