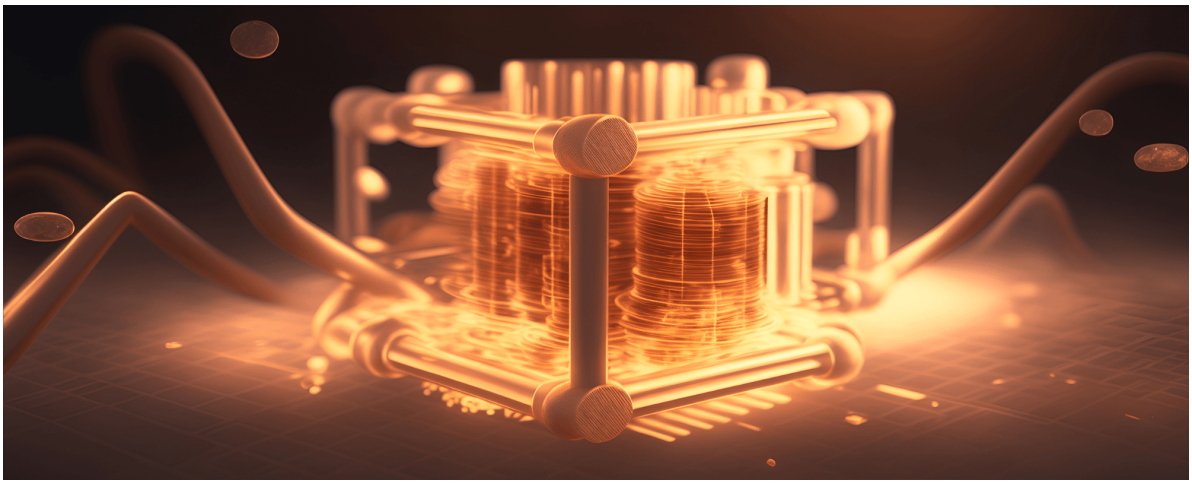
THE SECOND QUANTUM REVOLUTION

Quantum physics and information: new technologies for the 21st century

Ignacio Cirac, Antonio Acín



Abstract representation of a quantum computer with particles. Conceptualization: Luisa Quiroga

Information is a key concept in our society that has a direct impact on our daily lives: from the time we get up until we go to bed, thousands of messages are exchanged via internet or mobile data networks, together with thousands of operations of varying complexity run on a variety of information processing devices, from supercomputers to the mobile phones we carry in our pockets. The changes made by information to how we live, both individually and as a community, have been so profound that our society is often known as the information society. The importance and impact of this concept can be readily understood when we consider that an enormous number of jobs, companies, investments and political decisions revolve around information.

All information applications operate in bits, which are simply their basic unit and can have two values: 0 or 1. Our internet connection at home or work, our smartphone's memory or our laptop's processing speed: they are all measured in bits. A computer is basically a device that takes information coded in bits, performs operations on them following the steps described in an algorithm and then sends us the result converted back into bits. When we send an email to a friend on the other side of the globe, the information is transferred in bits coded in light, which are sent through an optical fibre.

Quantum physics was another revolution that was born in the 20th century. It is the formalism that explains all the microscopic phenomena that take place around us. As it involves objects that are minutely small, its impact on our society is not so clear at first sight. However, this conclusion is erroneous because it is superficial. On the one hand, within the domain of basic science, the predictions of quantum physics transformed our understanding of nature, as, in many aspects, they are very different from the predictions made by the Newtonian physics that has prevailed until now. On the other, on a more applied level, quantum physics has been and is crucial for understanding materials, chemistry and molecular structure and, therefore, a large part of modern science and technology. Applications such as the laser, with its multiple uses from reading barcodes in the supermarket to performing complex surgery, or the transistor, which is an essential component in any computer, could only be developed thanks to the understanding of the microscopic world provided by quantum physics.

Quantum particles for processing and transmitting information: the paradigm shift

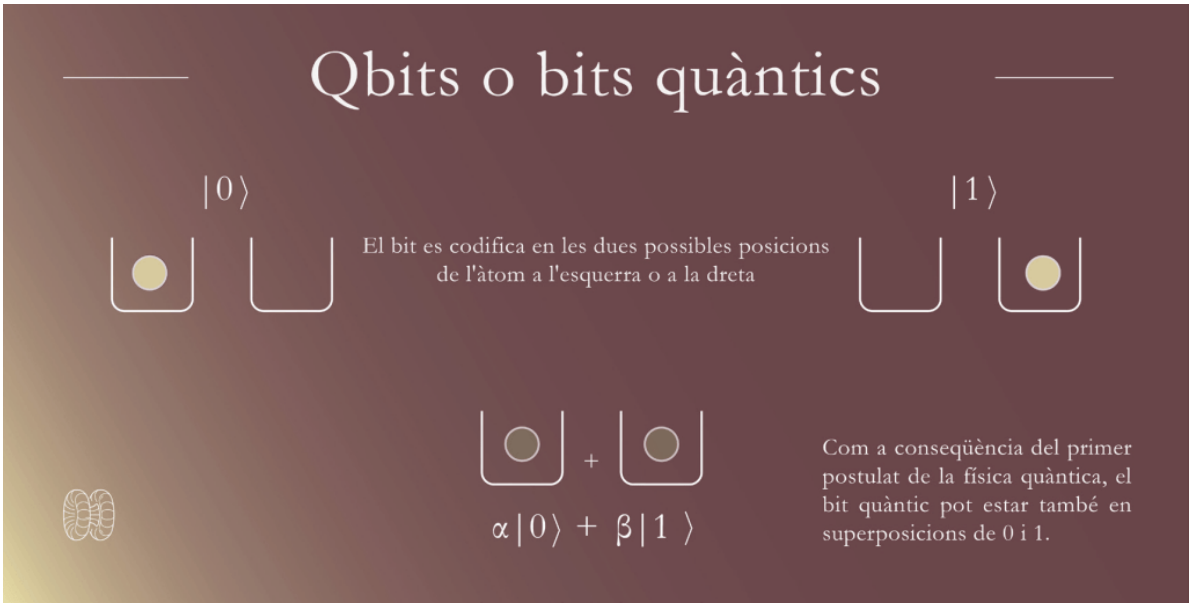
Quite a few decades ago, a number of researchers started to ask themselves what would happen if information and quantum physics were to be combined. After having read the previous paragraphs, the question may even seem simple and logical: what would happen if we were to use quantum particles, such as atoms or light photons, to transmit and process information? To put it another way: what happens if we store the bits in quantum particles? At that time, in spite of being a very exciting question from a conceptual and theoretical viewpoint, it was a possibility closer to science-fiction, given the current state of the art. Since then, the information technologies have made enormous progress, and ideas that at the time seemed to be more suited to the realm of science-fiction have become realities. Specifically, we now have the knowledge and the techniques to store bits in quantum particles such as atoms or photons. So what can we expect from combining information and quantum physics? This is the big question that the new science and technology discipline of quantum information seeks to answer.

It was understood relatively quickly that using bits coded in quantum particles opened up new opportunities for processing and sending information. Simply putting a bit in a quantum particle produced something different from what we had known until now. For example, let’s see what happens when we create a bit using an atom that can be in two positions, as shown in the image: when it is on the left, the bit’s value is 0, and when it is on the right, its value is 1. Now let’s open any textbook on quantum physics. Don’t be afraid, you won’t have to read very much: reading the theory’s first postulate is enough, which is usually enounced in the first pages. Remember that a theory’s postulates are not discussed; they are accepted.

> The information technologies have made enormous progress in the last decades and ideas that seemed to be more suited to the realm

> of science-fiction have become realities. We now have the knowledge and the techniques to store bits in quantum particles such as atoms or photons

So the first postulate of quantum physics says that if a quantum particle can be in two states, it can also be in a third state consisting of the superposition of one state on the other. The concept of superposition is difficult to understand, as superpositions take place in the microscopic world of atoms and molecules, which we can't see with our eyes, or smell or touch; in the world in which we live, which we do perceive, they disappear. So there is no analogy that we can use to explain superposition: it is a very special part of this tiny, tiny world. But a concept being hard to understand does not mean that it is not the right one for describing nature. And, in fact, the concept of quantum superposition is one of the ingredients used to explain experiments performed on a microscopic scale. Let's go back to our coded bit in the quantum particle: what implications does the superpositions postulate have? We see from its application that the quantum bit, also known as qubit, is different from the bit used until now, the classic bit, as it can be in either of the two usual values of 0 and 1, but also in any superposition of these values. So the basic quantum information unit, the qubit, is richer than its classic analogue.



Graphic representation of qbits or quantum bits

Quantum computers

Having made this observation, it is worth reviewing all the uses made of information and seeing how they change when subjected to the phenomena of quantum physics, such as the superpositions we mentioned earlier. How can we calculate and solve problems when we code them in quantum bits? This question takes us immediately to the idea of the quantum

computer. What is a quantum computer? To answer this question, it is useful to remind ourselves again of what a classic computer is: a machine that inputs information coded in bits, performs a series of transformations to solve a problem, and sends back the solution in bits again. So, at the risk of seeming to state the obvious, a quantum computer is nothing more than the translation of this idea to a quantum environment: a machine that is able to process information in quantum bits to solve problems. The difference lies in the fact that this processing is carried out using the phenomena of quantum physics, for which there is nothing comparable in our classic macroscopic world and which, therefore, are inaccessible to our present-day classic computers. In other words, the quantum computer can use more operations, it has access to more tools for solving complex problems and, consequently, it can provide solutions to these problems much more efficiently. This situation is also known as quantum advantage. This should not be interpreted in the sense that all problems will be solved more efficiently on a quantum computer and, in fact, there are problems for which a quantum computer and a classic computer perform equally well. However, there are other problems for which quantum computing does have an advantage.

Continuing with IT applications, one very active and highly topical field is that of machine learning, where computers are trained with lots of data so that they learn and enable us to solve significant problems. How does a quantum computer learn? Once again, this is a very important question with potential practical applications: it is this question that quantum machine learning seeks to answer.

Quantum cryptography

However, we know that information is used for thousands of applications beyond computing. For example, to set up a global communication network, internet, in which bits are sent anywhere in the world. What structure would a quantum internet have, where the goal is to transmit quantum bits between any two points? What are the laws of quantum communication? One key aspect of present-day communication is privacy: almost as important as being able to send information from one place to another is to be able to do this securely, so that a possible spy or enemy does not have access to the messages being sent. The field of cryptography provides us with the tools for designing private transmission methods. In this case, quantum bits once again offer new possibilities for encrypting information and enable us to design so-called *quantum cryptography* protocols, which provide a new type of security based on the laws of quantum physics.

We could go on to list all the possible uses of information in our society and try to understand how they would be affected by the laws of quantum physics. However, we will not do this in this introduction, because this is not the goal being pursued here and because there are other articles in this monographic issue of *IDEES* that analyse many of these possible applications. Some, such as quantum computers or quantum communication, are very logical; others are more speculative. For example, nowadays, computers are used to compose music, so we could look at the process of generating music using quantum effects. Consequently, the contributions to this monographic issue of *IDEES* offer a fuller, more detailed vision of the field.

Conclusions

We would like to conclude this introduction with two messages. The first should be very clear: information is a crucial concept in our society and quantum physics gives us new tools for processing and transmitting this information. This message has already been accepted around the world, and companies large and small, and government agencies are undertaking significant initiatives and investments. Closer to home, a few years ago, the European Commission launched the Quantum Flagship, a pan-European initiative in quantum technologies. We find ourselves at a very interesting – and very dynamic – point in time, in which all the main stakeholders are working together to understand how we can exploit quantum technologies to their full potential.

wever, a considerable degree of complexity is involved in operating with quantum superpositions: any quantum information application, for example, a quantum computer, performs operations in quantum bits. To obtain an advantage, one necessary – albeit insufficient – prerequisite is to have these bits in superposed states. However, in practice, it is not easy to maintain superpositions, as any uncontrolled interaction with the environment can destroy them. The fragility of quantum effects explains why the development of quantum information technologies must still overcome a number of significant challenges.

> Almost as important as being able to send information from one place to another is to be able to do this securely. Quantum cryptography offers new possibilities for encrypting information and enable us to design protocols that provide a new type of security

The second message is a call for cautious optimism or optimistic caution. Preparing, handling, storing and sending qubits is much more complicated than doing the same with classic bits. If the quantum bit ceases to be superposed, it becomes a classic bit that can only have two values, 0 or 1, and any quantum advantage is lost. However, maintaining superpositions is a complex task as noise and uncontrolled interactions with the environment destroy them. Consequently, qubits must be prepared and processed in an environment that is isolated from the exterior, for example, at very low temperatures, so that we can handle them in a controlled manner. Here lies the key technological challenge. This explains why, in spite of years of effort, the existing quantum computers or quantum communication systems are still beset by significant difficulties that limit their practical implementation. The road ahead is bumpy and full of obstacles. However, the motivation and the ultimate goal are clear, and a number of results have been obtained that prove that quantum information technologies will allow us to solve problems that today are constraining our progress and well-being as a society.

Ignacio Cirac

Juan Ignacio Cirac Sasturáin is director of the Max Planck Institute of Quantum Optics and honorary professor at the Technical University of Munich. Holder of a PhD in Physics from the Complutense University of Madrid, he is a specialist in quantum technologies. He is a member the Spanish, German and Bavarian Academies of Science. He has received several awards, including the Prince of Asturias Award, the BBVA Frontiers of Knowledge Award, the Wolf Prize, the Micius Quantum Prize, and the Benjamin Franklin, Max Planck and Niels Bohr medals.

Antonio Acín

Antonio Acín Dal Maschio is ICREA professor at the Institute of Photonic Sciences (ICFO), where he supervises the Quantum Information Theory group. Holder of a PhD in Physics from the University of Barcelona, he is a specialist in quantum technologies. His research work has been acknowledged with four European Research Council (ERC) grants. Since 2016, he has directed the AXA Chair in Quantum Information Sciences.