Counting on Quanta

Modern quantum physics holds quite a few promises in store: quantum computers and simulators will be able to trawl through huge quantities of data at lightning speed, accelerate the development of new drugs or facilitate the search for materials for, say, energy engineering. The research being carried out by **Ignacio Cirac**, Director at the **Max Planck Institute of Quantum Optics** in Garching, is helping to fulfill these promises.

TEXT **ROLAND WENGENMAYR**

This story starts with a train delay, requiring a phone call to Ignacio Cirac's office while en route. Fortunately, the Director at the Max Planck Institute of Quantum Optics in Garching can move our meeting to a slightly later time. We plan to talk about his research field, quantum information, which holds the keys to allowing the world of physics to realize a number of promising future technologies.

The call made via the cellular network is a good reason to consider how much physics has already made its mark on modern communications technology. Quantum physics is involved in just about everything: from semiconductor electronics to the laser that enables connections across the world at the speed of light via the global fiber-optic network. How much more will future quantum technology change our lives? No one can predict this today, as physicists like Cirac are still in the process of laying the foundations.

IMPORTANT FOUNDATIONS FOR THE QUANTUM COMPUTER

The stress of the journey is quickly forgotten in the relaxed atmosphere in Cirac's office. The Spaniard prefers a quiet, thoughtful environment. We are sitting in the warm September sun, surrounded by light quanta, and move our thoughts into an abstract microcosm. This is where our intuition, which is shaped by relatively large objects, quickly comes up against its limits. Cirac is one of the pioneers of a discipline that has brought such ideas as quantum computers, quantum simulators and quantum cryptography (cf. MAXPLANCKRESEARCH 2/2015, p. 60) into the world. He is just as interested in technology as he is in mathematics and the basic questions of quantum physics, and the field of quantum information is the ideal setting for him to combine these three passions.

In the 1990s, Ignacio Cirac and Peter Zoller jointly developed important foundations for a possible quantum computer technology. Zoller, a professor of theoretical physics at the University of Innsbruck, was a scientific mentor of the young Ignacio Cirac, who, between 1996 and 2001, likewise conducted research at the University of Innsbruck. Cirac then became Director at the Max Planck Institute of Quantum Optics. >

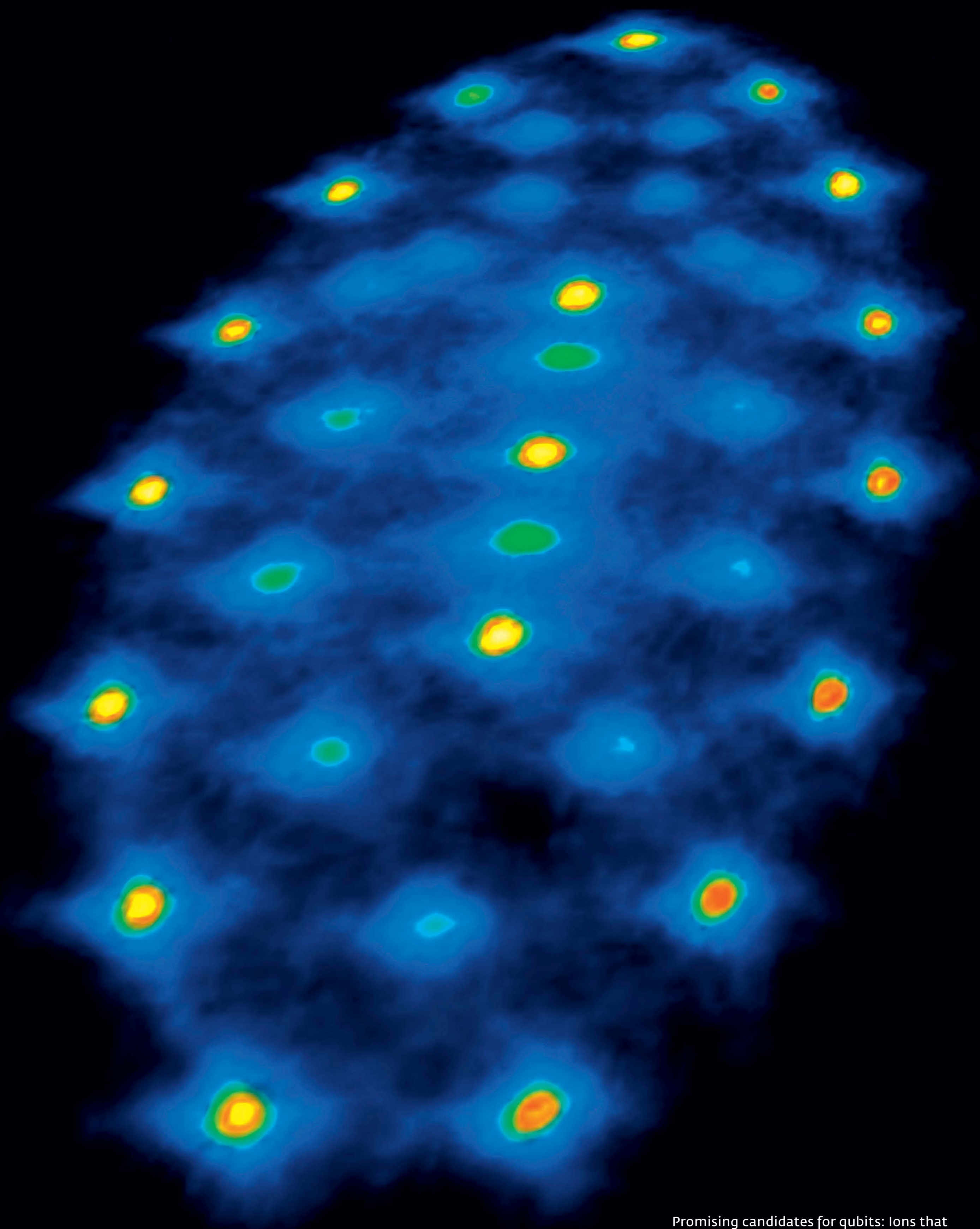
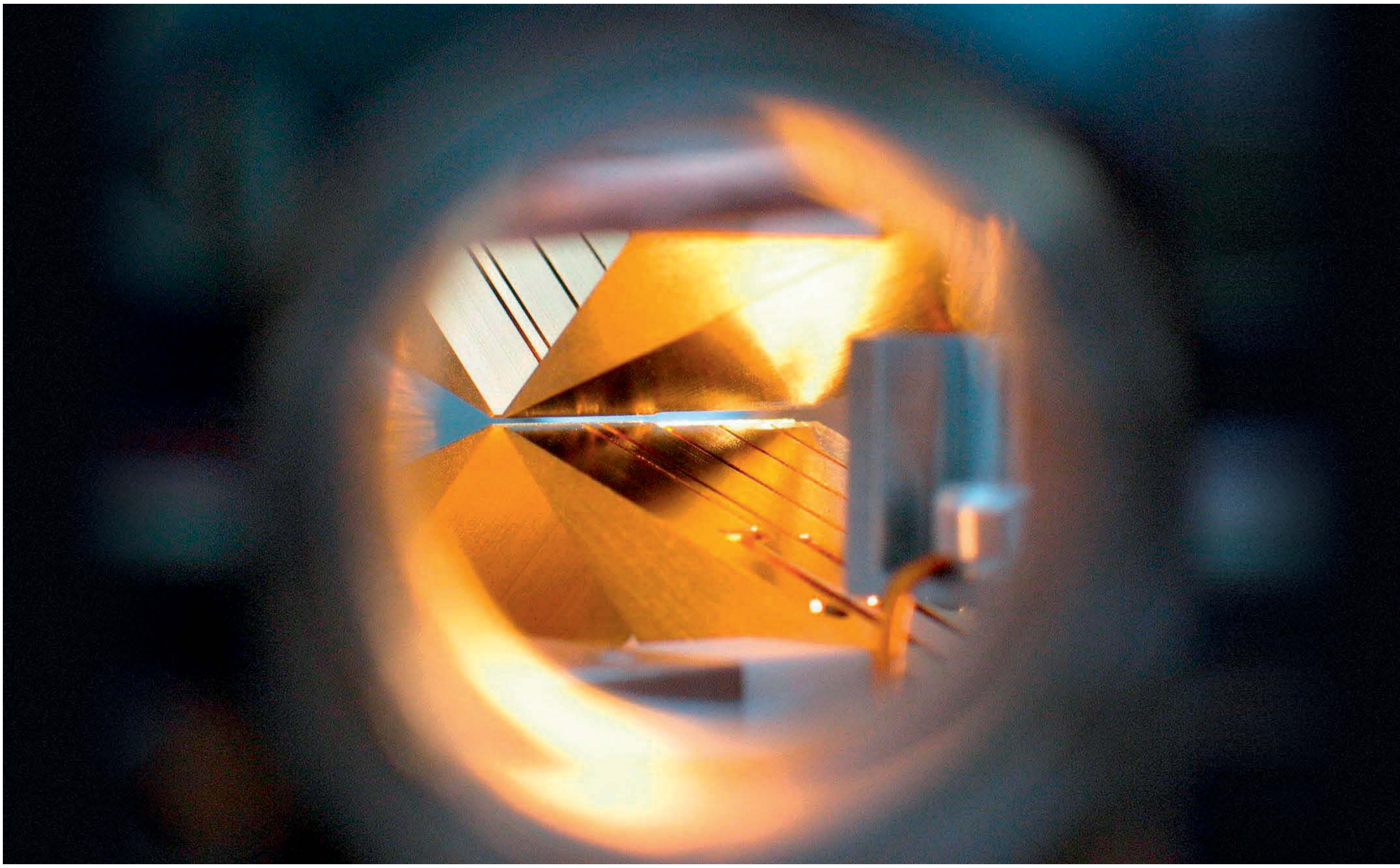


Photo: MPI of Quantum Optics

Promising candidates for qubits: Ions that are confined in an electric trap and appear here as bright spots can serve as elementary computing units in a quantum computer.



Trapped in a Paul trap: Ions are ensnared in an alternating electric field generated by four electrodes. Ignacio Cirac and Peter Zoller proposed the charged particles as qubits.

The big moment in Cirac's life as a researcher came in 1994. At the time, he was working as a postdoc with Zoller at the University of Colorado in Boulder, at the Joint Institute for Laboratory Astrophysics. Zoller and Cirac listened to a talk given by Artur Ekert. This Polish-British physicist is now well known for a protocol he developed that can be used to transmit quantum-cryptographically encrypted messages that can't be intercepted. "He talked about quantum computers and how fantastic it would be to be able to build them – but nobody knew how," recounts Cirac.

IONS WERE THE BEST CANDIDATES FOR QUBITS

This gave Cirac and Zoller the crucial idea. As theoreticians, they worked with a technique that was tried and tested in atomic clocks, and that they then remodeled into a fundamental tool kit for quantum computers. The approach is based on individual ions – electrically charged atoms – that are confined in ion traps by electric and magnetic fields.

The trap technology was already so advanced in the early 1990s that the ions trapped inside them could be controlled extremely well. This made them the best candidates available for quantum bits, or qubits for short. Qubits are the equivalent to the bits of conventional computer technology. In the paper they published in 1995, Cirac and Zoller showed that, with sophisticated trap control and precisely tailored laser pulses directed at the ions, the particles can be addressed as qubits, and quantum logic operations can be carried out.

Only three months later, one of David Wineland's teams at the National Institute of Standards and Technology, likewise in Boulder, demonstrated experimentally that Cirac's and Zoller's theoretical proposal works in principle.

But what on earth would quantum computers be good for? They promise to solve a few tasks whose complexity is too much for today's supercomputers. "These are complicated problems that each require a great many equations to be solved," explains Cirac: "The design of chemical compounds, for example, or new materials – and maybe even equations that are contained in such applications as weather forecasts." Powerful computers are used for modeling in all these fields, but they can't provide an exact solution of the equations because their computing power is limited. So they have to work with greatly simplified approximation methods, meaning with compromises that are often unsatisfactory. Quantum computers, in contrast, can theoretically solve some of these problems through "quantum parallelism" – quantum-doped massively parallel computing, as it were – in an acceptable time frame.

"Quantum computers are specialists," emphasizes Cirac. They won't be replacing the computers on our desks. "In principle, they can solve the same tasks as conventional computers," ex-

Photo: MPI of Quantum Optics

» In principle, quantum computers can solve the same tasks as conventional computers, but they use different natural laws than normal computers.

plains the Max Planck Director, "but they use different natural laws than normal computers."

COMPUTERS USE ELECTRON CLOUDS

The basic concepts of modern computers and quantum computers are indeed similar at first sight. Established computer technology uses bits – zeros and ones – mainly in the form of electron clouds, but increasingly also in the form of photons, or light quanta. It executes logic operations using logic gates and stores the intermediate results in registers. Quantum bits, quantum logic gates and quantum registers will work in a similar way in a quantum computer.

The fundamental difference is evident when a qubit is examined in greater detail. Qubits are typically individual electrons, photons or atoms. They are therefore much smaller than digital bits. This ultimate miniaturization automatically immerses one in a strange microworld. "The logic of quantum mechanics rules here," explains Cirac with a smile, "and its laws are slightly unusual." Quantum computers can thus achieve things that conventional computers aren't capable of.

A qubit has two quantum states, which correspond to the zero and the one of a conventional bit. As a quantum particle, it can additionally be in a superposition of these two states, and that is the crucial difference. Physicists also call this the state of Schrödinger's cat – in remembrance of a thought experiment proposed by Erwin Schrödinger. It involves a radioactive atom that can decay randomly, triggering a poisoning mechanism that kills a poor cat in a box. As long as the lid of the box is closed, no information is available as to whether the atom has decayed or not – that is, whether the cat is dead or alive. From a quantum mechanical point of view, the two cat states in the box are superimposed.

The qubit therefore has an infinite number of intermediate states – in contrast to the two states of the digital bit. But this applies only as long as its state isn't measured in the classical sense, meaning by opening Schrödinger's box. As soon as that happens, the qubit jumps into one of the two fundamental states, which represent zero or one. It is now known whether the cat is still alive or not. Consequently, if one wants to use the added value of qubits from quantum information technology, the cat must first remain undisturbed in the box.

But the superposition of the two states within a qubit is just the beginning. Even a Ronaldo can't score a soccer goal all on his own – it takes a well-coordinated team. A crucial key to the computing power of future quantum computers, in turn, is the ability to prepare several qubits in a shared quantum state – in a superposition of the superposition, so to speak. This complex collective state is called entanglement, and it is the reason for some of the eccentric properties of quantum mechanics.

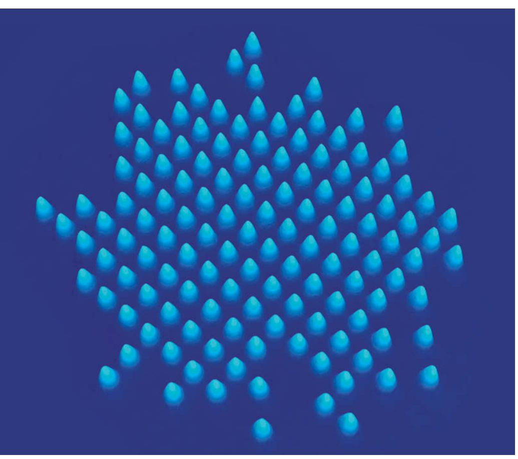
In the quantum computer, entanglement must operate as a quantum mechanical arithmetic unit. The operation can be imagined in simplified form as follows: The task is written into a set of qubits and then the entangled quantum system is left to work in peace. In principle, the enormous computing power of the quantum parallelism of entanglement contains all possible solutions to the task and runs through them. In this way, even relatively small numbers of qubits can develop a computing power that beats all conventional computers.

After a certain time, the quantum arithmetic unit is stopped and the result read out. If the timespan and the programming were selected with skill, the solution to the task will have been obtained.

A FURTHER CONCEPT: ATOMS IN AN OPTICAL LATTICE

Today, various concepts for the architecture of quantum computers are being investigated. These concepts differ in the details of how they work, but the picture described here conveys a basic sense of the operating principle of quantum computers.

In 1998, Cirac and Zoller published a second influential concept, which physicists today are putting to the test in many other variants besides ions in traps. In this proposal, a cloud of electrically neutral atoms is cooled to a few millionths of a degree above absolute zero. A three-dimensional lattice made of laser beams is then laid through this cloud. The individual atoms are drawn to the points of intersection much like



Atoms are arranged in an optical lattice like eggs in an egg carton. Such a system could also serve as the computing core of a quantum computer.

eggs slip into the wells of an egg carton. Arranged in this way, they can be manipulated as qubits.

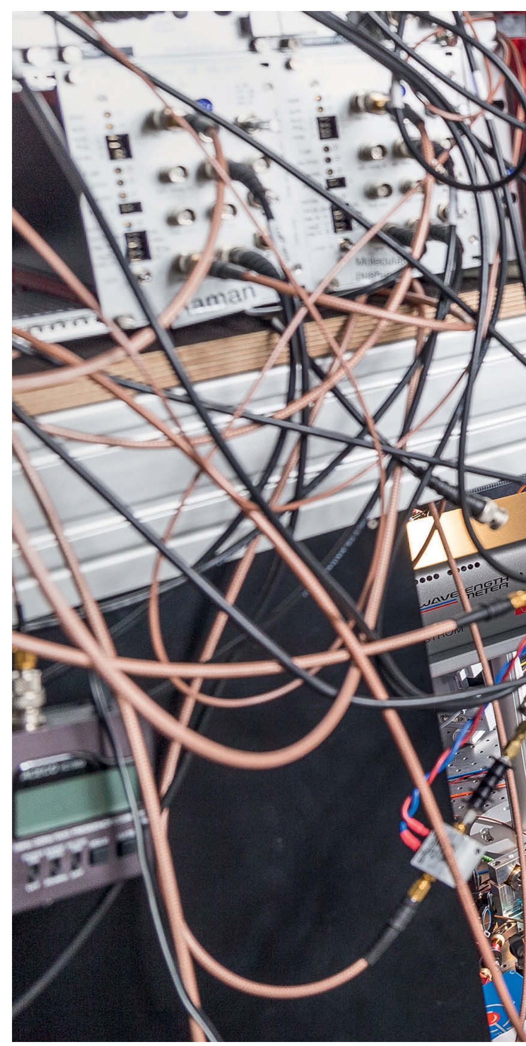
The optical lattice has the advantage over ion technology that it can control many thousands, even hundreds of thousands of qubits simultaneously. However, they can't yet be controlled as well as trapped ions. The ion technology, in contrast, long resisted combining a larger number of qubits, as the ions repel each other electrically. Now, however, both technologies are increasingly overcoming their weaknesses and coming closer to each other.

Despite the promising approaches, there is still a long way to go before we have true quantum computers, regardless of the promises made by the first commercial suppliers and the millions invested in their development, also by companies like Microsoft, IBM and Intel. "I am convinced that they will be built," says Cirac, "but it may take another ten, twenty or even fifty years."

The situation is different for quantum simulators – specialized, slimmed-down versions of the quantum computer. The department of Immanuel Bloch, a fellow Director in Garching with whom Cirac closely collaborates, is already carrying out the first quantum simulations with optical lattices. The quantum simulator goes back to an idea that American physics Nobel laureate Richard Feynman presented in the early 1980s. He – and not only he – was bothered by a fundamental problem with which physics still struggles today: although it can generate the exact equations for the behavior of complex systems made up of many quantum particles, it can't provide an exact solution for them. "We even fail for a system of just one hundred electrons," says Ignacio Cirac.

ONE QUANTUM SYSTEM IS MODELED USING ANOTHER ONE

Feynman came to a radical conclusion: the behavior of a quantum system can only be modeled efficiently by using another quantum system. Electrons, for example, determine the properties of matter. But they're not readily accessible, so it is difficult to investigate their behavior. A quantum simulator, however, could simulate it using qubits that can be controlled directly. Even with only a few dozen qubits, a quantum simulator could thus reproduce the properties of many fundamental building blocks of matter very accurately. Quantum simulators therefore promise to revolutionize the development of new materials. They



Not just a theory: The concepts developed by Ignacio Cirac's group are also implemented experimentally in the laboratories of Immanuel Bloch's department at the Max Planck Institute of Quantum Optics. Here, Cirac stands next to a laser bench with numerous optical instruments that are used to generate optical lattices.

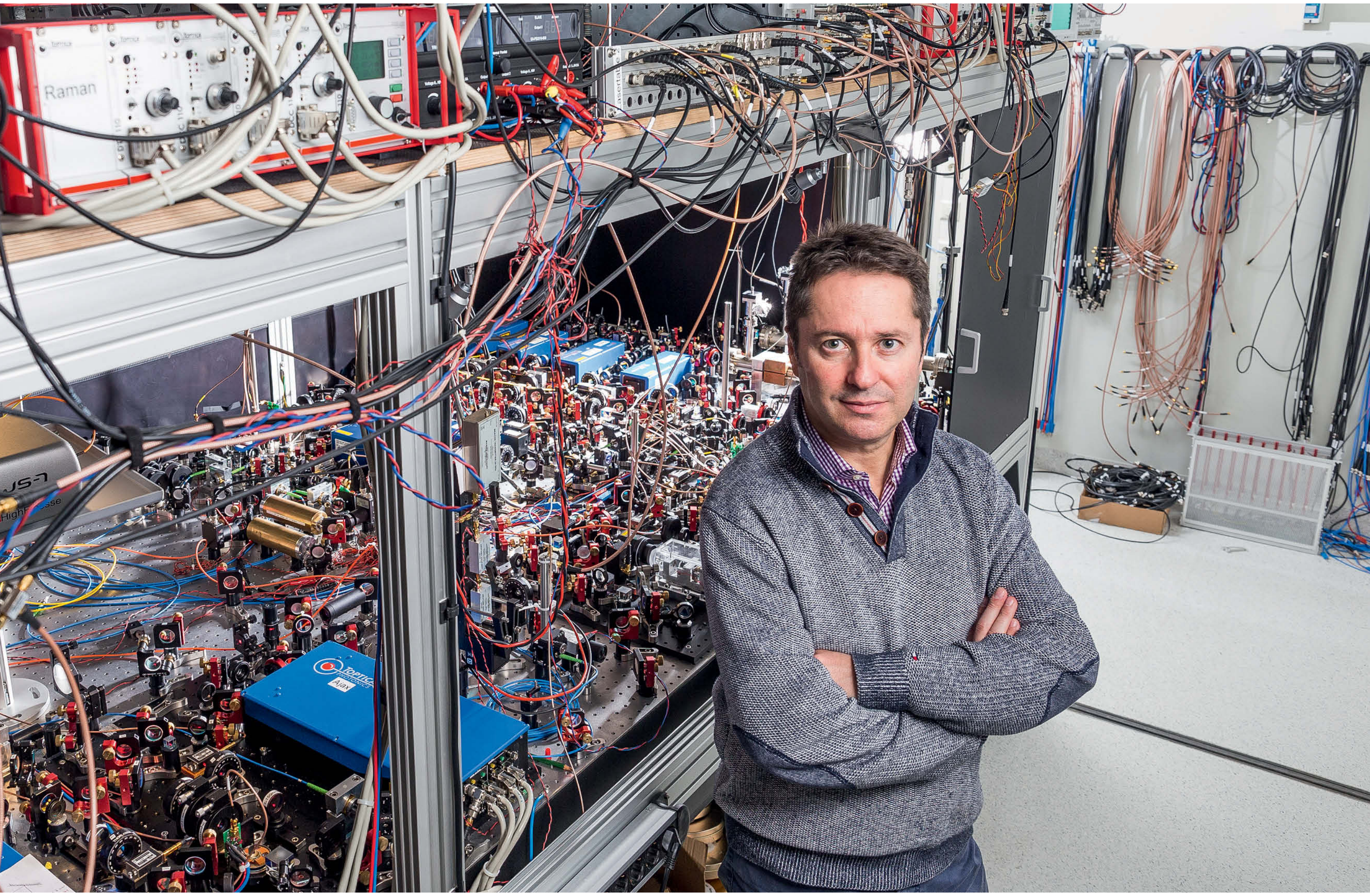
Photo: MPI of Quantum Optics

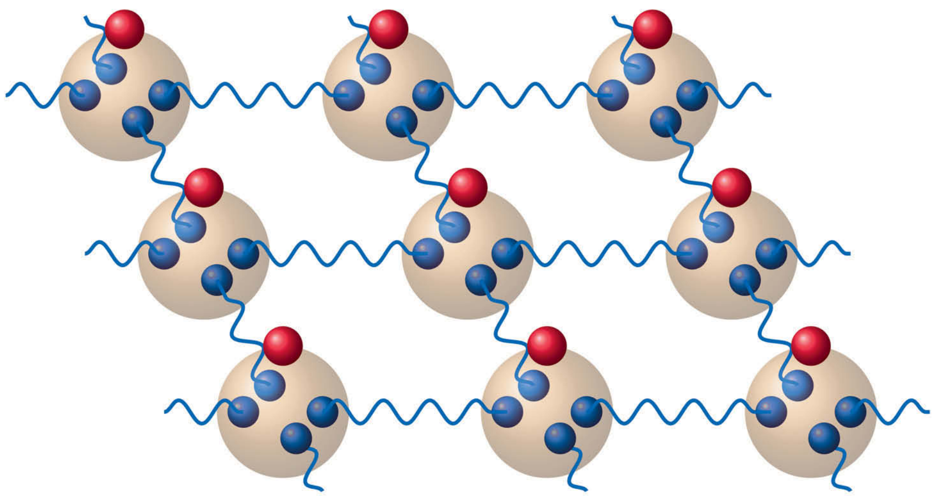
» Cirac's team is primarily interested in using quantum information methods to advance physics in other fields.

could assist in solving the mystery of high-temperature superconductivity, for instance, and in developing better superconductors.

Quantum simulators and quantum computers are the hardware, and quantum algorithms are their software. In 1994, when Cirac and Zoller had the idea of quantum computer components, American mathematician Peter Shor had just developed such an algorithm. Quantum computers can use it to factorize numbers much faster than modern computers. Factorization is the reverse of multiplication. This means it involves division, but in a way that results in prime numbers. For example, 15 is split up into 3 and 5. This example is trivial, of course. "But just imagine this for a number with 200 digits," says the

Photo: Axel Griesch





Left Determining the properties of a quantum system of real particles (red spheres) is as complicated as it gets, as all particles interact among each other. The physicists in Garching therefore describe each real particle with four virtual particles (blue spheres), each of which is entangled with a virtual particle of a neighboring particle (indicated by the wavy lines). Because the virtual particles are projected onto the real particle (indicated by the large beige-colored spheres), physicists call this "projected entangled pair states" (peps) – one example of a tensor network.

Right-hand page Ignacio Cirac talks with András Molnár and Yimin Ge (left to right) about how tensor networks can be used as algorithms to simulate an unknown quantum system by means of a known one.

physicist: "All of today's supercomputers taken together would fail."

What looks like academic mental acrobatics has a very topical practical significance. Most of today's common encryption methods for messages rely on eavesdroppers being unable to crack the number codes used for encryption in this way, or at least not in a viable time span. Functional quantum computers could thus crack these encryption methods. There is a good reason why secret services are extremely interested in quantum information technologies.

ACCELERATED SEARCH IN UNORDERED DATABASES

But also other technical applications are conceivable today: the so-called Grover algorithm, for example, would accelerate searches in unordered databases enormously. IT experts see this as making great progress, given the vast and ever-increasing amounts of data now being processed in many computer applications.

Cirac's team is interested primarily in using quantum information methods to advance physics in other fields. In addition to the physics of condensed matter – materials research within physics – the main focus of interest is particle physics, which is carried out in the large accelerator facilities. Here, too, the important thing is to understand complex quantum effects involving large numbers of particles in order to gain a deeper understanding of the origin of matter and forces.

In all these fields, a new mathematical method from quantum information could be of assistance – the so-called tensor networks. Cirac is counting on these. One of his teams has just developed a new quantum algorithm on this basis. The doctoral students András Molnár from Hungary and Yimin Ge from Austria struggle to provide a graphic explanation. "Imagine a chain of one hundred spheres that can be either red or blue," explains Ge. But all the colors of the spheres in the chain are superimposed. "Even on a computer screen, it's not possible to display what this would look like," says the mathematician.

ALGORITHM FOR A MANY-PARTICLE SYSTEM

Tensor networks, however, can precisely describe the behavior of the chain of spheres. Their color superposition is an illustrative image for the superimposed states of one hundred qubits, of course. The Garching-based researchers can now use their algorithm to compute how such a complex system develops over time if the spheres are allowed to change color. They can use rules to adapt their algorithm to the typical behavior of real quantum systems of many particles – such as a semiconductor crystal.

This is how physical systems minimize their energy bill, which is why water freezes to ice as the temperature drops. "For our spheres, for example, we

Graphic: Thorsten B. Wahl

could introduce the rule that it costs ten virtual euros if two neighboring spheres ultimately have different colors," says Ge. With this rule and the instruction to be economical, the chain of spheres will, over time, approach a state of uniform color, just as many quantum systems transition into a collective quantum state at low temperatures.

Although the result was easy to predict intuitively in this simple example, the path to the solution is difficult to describe in a mathematical model. Similarly, the scientists in Garching can also train their system for a physical behavior whose outcome can't be easily anticipated. They could, for instance, simulate as yet unknown properties of new materials.

At present, no one can say what impact this basic research will have on our culture. But looking at the key role physics developments play in today's information and communications technology suggests that the impact could be very significant indeed. ◀

Photo: Axel Griesch

TO THE POINT

- **Quantum computers can manage tasks that would overwhelm even today's supercomputers in practicable computing time, as they can carry out massively parallel quantum computations with the aid of the quantum physical entanglement of qubits.**
- **In the near future, quantum simulators – simpler versions of a universal quantum computer – could already be solving complex physical problems and assisting in the development of new materials.**
- **Max Planck scientist Ignacio Cirac, together with Peter Zoller from the University of Innsbruck, has proposed two concepts for the practical design of quantum computers and simulators: with ions in electromagnetic traps or with atoms trapped in lattices made of laser beams.**

GLOSSARY

Qubit: Like a conventional bit, a quantum bit, or qubit for short, has two states that represent zero and one; unlike a bit, however, it can also assume all superposition states in between.

Tensor network: A mathematical method to describe the state of a quantum system consisting of many particles. Tensors, which are mathematical functions, serve here as building blocks that, when put together, provide a description for the desired state.

Entanglement: When two or more quantum particles such as atoms are entangled with each other, they are in a superposition state of one property before a measurement. With the measurement on one particle, this property is then fixed not only on the measured particle, but immediately also on the particles with which it is entangled.