PHOTO: ADOBE STOCK/BARTEK WRÓBLEWSKI

Cool computer: the Finnish-German company IQM is developing quantum computers that use superconducting circuits known as Squids to compute. These are cooled with such a cryostat to temperatures close to absolute zero, which is minus 459.67 degrees Fahrenheit.

QUANTUM COMPUTING'S LEAPS AND BOUNDS

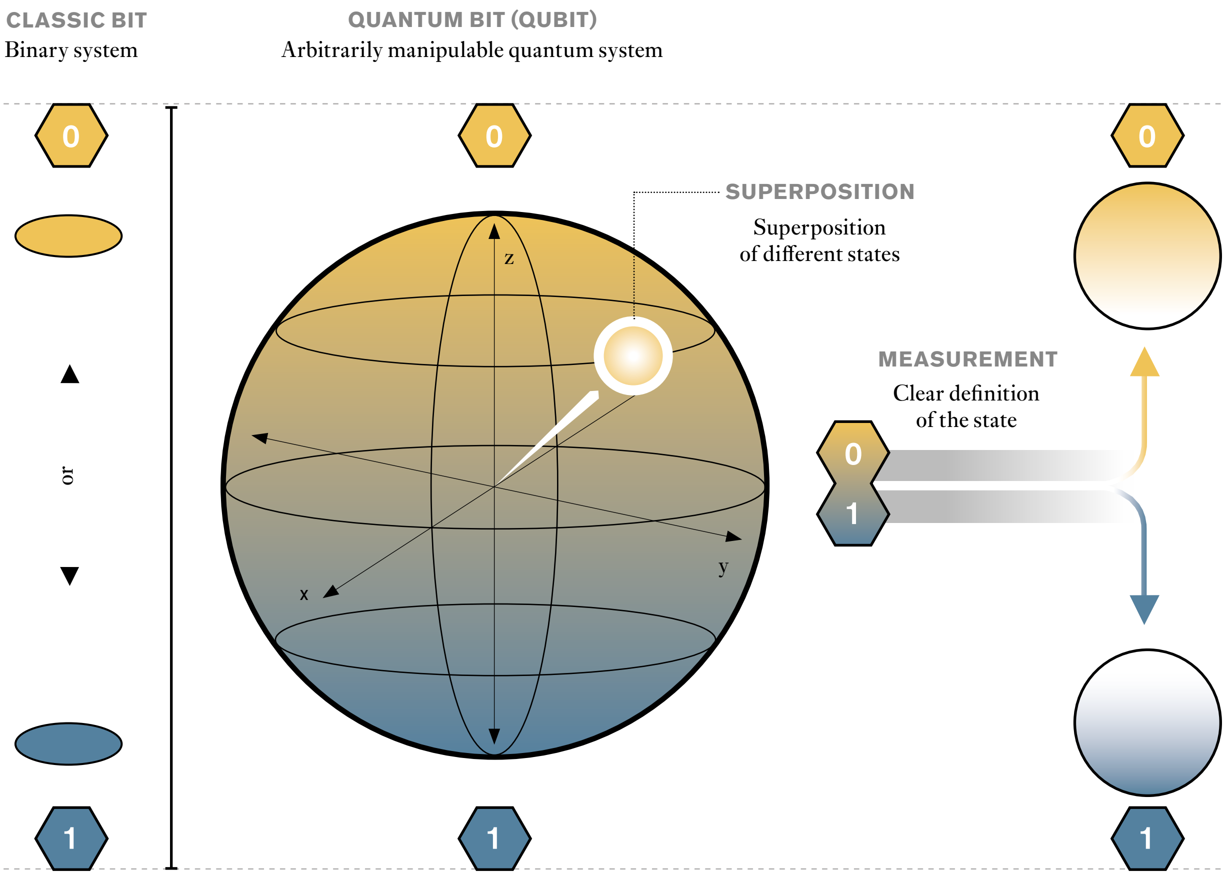
TEXT: ROLAND WENGENMAYR

With the expectation that they will be able to solve problems that stump even today's best computers, both governments and private financiers are investing heavily in the development of quantum computers. The team led by Ignacio Cirac, a Director at the Max Planck Institute of Quantum Optics in Garching, is researching what computers will actually be able to do in the years to come. As the research reveals, not all hopes are likely to be fulfilled so soon.

Ignacio Cirac should actually have reason to be enthusiastic. The Director at the Max Planck Institute of Quantum Optics in Garching near Munich is a pioneer in the development of quantum computers. With the aid of quantum physics, these computers will be able to process some tasks, for example, in logistics or the development of new drugs and materials, much faster than today's computers. This hope is driving state institutions to enter a practical bidding war when it comes to their funding of quantum technology – and especially quantum computing. The German government has earmarked two billion euros for this area from 2021 to 2025, the U.S. government has also pledged about a billion dollars over four years, and the EU Commission has invested about the same amount in a flagship program that will run for ten years. However, China is outdoing them all by spending ten billion euros in one swoop on an institute for quantum information science. In addition to numerous startups, large companies such as Google and IBM are also competing in the race to create the first quantum computers – and they accompany every advance with a certain amount of media furor. The companies and their investors are putting hundreds of millions of euros into developing quantum computers.

So Ignacio Cirac's research field is clearly booming – a fact that not only inspires enthusiasm in the physicist, but also a certain anxiety. Like many of his colleagues who are well versed in the field of quantum information, he fears this hype about quantum information technologies could soon turn into disinterest should there be a lack of success. "The field is not only being driven by researchers but now also by investors," says Cirac. But, he says, they might not have enough patience. Given the enormous technical challenges, Cirac expects at least another ten-year, if not a twenty- to thirty-year wait before truly application-ready universal quantum computers will hit the scene. "But the hype won't last that long," he stresses, "and in the end, when quantum computing isn't ready in time, we scientists will get the blame." The great vision of the future is universal, i.e., freely programmable, quantum computers. They are the counterpart of digital computers. In a similar manner to digital bits, they calculate with

⟶



GRAPHIC: GCO AS PER VOLKSWAGEN AKTIENGESELLSCHAFT 2019

Ambiguous bit: unlike a classical bit, a quantum bit can also assume superpositions of the states 0 and 1, which can be represented by the coordinates x, y, and z on a sphere and occur with a certain probability during a measurement. Since this means that quantum computers can test different solutions in parallel, they should be able to handle some tasks faster than classical computers.

quantum bits or qubits for short. When it comes to certain tasks, their computational power stems from the rules of the quantum world: unlike a digital bit, a qubit cannot just assume either the states 0 or 1 but can also be in a superposition of both states. In addition, multiple qubits can also be superpositions which are called entangled states. This entanglement forms the arithmetic unit of a quantum computer.

There could be many applications for a universal quantum computer. “One typical example is the traveling salesman problem,” says Cirac. The traveling salesman has to visit a certain number of cities and wants to calculate the shortest route. “Now, how does the computing time required by a digital computer for this grow with the number of cities?” the physicist asks, and immediately comes up with the answer: “It grows exponentially!” This is typical of such combinatorial problems, he says, and they manifest themselves in a variety of ways with one example existing in the technology that makes computing times on conventional computers explode. And not only that: the memory required for computing can snowball.

We’ve all seen how something can explode exponentially during the Covid pandemic. This is illustrated by the legend of how chess was invented. Enthusiastic about the new game, the king wants to give the inventor a reward of his own choice. The inventor who, unlike the king, is mathematically gifted, thinks about this and then wishes for rice according to the following rule: for the first square of the chessboard, one grain of rice, for the second two grains, and then for each subsequent square, always double the number. Mathematically, this results in the number 2^{64}-1 for 64 squares on the board, which looks harmless as a power in this form but is in fact immense. The king would have to give the chess game inventor a quantity of rice equivalent to around two thousand times the world's current annual production.

Such an exponential explosion also makes solving tasks from fields of physics and chemistry difficult – but quantum computers could handle these quite soon. One example is when it comes to specifically developing new active medical ingredients or new materials, such as practical materials that conduct electricity without resistance. If you want to calculate the properties of chemical reactions of molecules and materials as precisely as possible, you inevitably have to take quantum properties into account. Or to put it more precisely: the complex interaction of electrons. Even a present-day supercomputer cannot calculate the behavior of such a quantum many-body system. Hence, programs used for material development, for example, use highly simplified approximation models. Their predictive power is correspondingly underdeveloped. In principle, quantum computing can enable much more precise material design. The underlying idea goes back to the American physics Nobel Prize winner Richard Feynman. The idea states that if you want to precisely calculate a quantum system, you must take an adapted second quantum system that is suitable as an adequate substitute. But unlike the hardly accessible object of study, such as the electron collective in a superconductor, this second quantum system must be easily controllable from the outside in the same manner as a computational device. This is exactly what a quantum computer excels at, namely as a quantum simulator.

Simulators for physics research

If you compare this to the history of classical computers, quantum simulators are the counterpart of analog computers. These were highly specialized computers that simulated, for example, the aerodynamic properties of an aircraft under development. Unlike digital computers, which process information in portions as bits, analog computers continuously reproduced a particular system, for example, mechanically or electronically. Analog computers had their golden age when digital computers were not yet so powerful. Today, in the early stages of quantum computing, the situation is similar. For a while now, quantum simulators have been becoming increasingly interesting for tackling at least basic physics research questions. For example, this is being researched by Immanuel Bloch's group. He is also a Director at the Max Planck Institute of Quantum Optics with whom Cirac's team is also collaborating.

As much separates the quantum simulator, which is available today or will at least be in the near future, from the universally programmable quantum computer as does an old analog computer from today's PC. Cirac's team is, therefore, pursuing a dual strategy. Some of the algorithms being developed by the Garching-based researchers will only be able to run on powerful, error-corrected universal quantum computers in the distant future. The rest should be usable as soon as possible on the already available quantum computers with relatively few qubits and demonstrate the first advantages, in particular in quantum simulation. "We want to show that you can already do something useful on quantum computers that you can't do on classical computers," Cirac says, "for example, predict the properties of some new materials." To achieve this, he is also cooperating with Google Research.

Several physical systems are competing in the quantum computer hardware race. Immanuel Bloch's group, for example, uses ultracold atoms as qubits; these are trapped in a spatial lattice of laser beams and controlled by laser light. Google, on the other hand, is developing chips that use tiny superconducting circuits as quantum bits. In 2019, Google researchers used one such quantum processor called Sycamore, which contained 53 working qubits, to demonstrate for the first time that a quantum computer computes a task better than the most powerful conventional supercomputer. "However, this was a purely academic task with no meaningful application," says Cirac about this celebrated breakthrough. And Markus Hoffmann of Google Research in Munich compares it to the Wright brothers' first powered flight hop: "This flight has gotten us to the first island that couldn't be accessed before – but this island is still barren." He also stresses that Google Research is realistic about the technical development level of quantum computers, but he is also optimistic. Google expects the next milestones to be a hundred superconducting qubits, then a thousand, and finally – in about a decade – a million.

The limits of quantum computers

Even a hundred qubits would allow application in materials development. If you want to precisely calculate the properties of a microscopically small piece of superconductor, which are determined by a hundred strongly interacting electrons, you end up with a problem that has 2100 unknowns. This is far more than the universe has stars and would conceivably over-

→

whelm all conventional large computers. A quantum computer, on the other hand, would need only a hundred entangled qubits to solve the task. But how will it do this?

Mari Carmen Bañuls, a senior researcher in Cirac's department, attempts to explain the procedure: "You write your instructions into the quantum bits that prepare them in a particular quantum state." The task to be computed, which uses a particular quantum algorithm, lies in the way the quantum bits are initially entangled. "Then you allow the system to develop for a certain amount of time," the physicist explains, "and then you take a measurement to get the result." This is, in a way, comparable to cooking in a pressure cooker: you put the ingredients in, close the pot, and start the cooking process. After the time stated in the recipe, you check to see if the stew was a success. During cooking, only the pressure indicator provides information about what is happening in the pot – but at least you have that.

In the quantum world, you are not even allowed a display like this while the entangled qubits are doing their thing. And this is where another peculiarity comes into play: quantum information is extremely sensitive. Even a minimal intervention is the equivalent of a measurement that causes the entanglement to collapse immediately. So, you must not take a look until the time specified in the quantum recipe is up, in other words: make a measurement, and then – maybe – get the desired result. This is because quantum mechanics has another peculiarity. It only describes probabilities with which certain quantum states occur. Hence a quantum computer would not return 1 + 1 = 2 but would output the result 2 only with a certain, but precisely calculable probability. This is another indication that the use of quantum computers will only be useful for special tasks for which such uncertainty is tolerable or there is no alternative.

Cirac's team is also exploring what those tasks might be. Because, despite the bold visions of the future, a great deal is still open here: "We're also investigating what quantum computers *can't* do," Cirac emphasizes. This, he says, is to prevent valuable resources from being wasted on unachievable goals.

SUMMARY

Governments and companies are currently investing heavily in the development of a quantum computer that could solve some tasks much faster than the best computers available today.

It may be decades before there is a universally programmable quantum computer, mainly because its calculations can be very error-prone and quantum information is very sensitive. Researchers at the Max Planck Institute for Quantum Optics, among others, are therefore working on error correction and validation of quantum calculations.

Today, quantum simulators can already be used for investigations in basic physics research. Soon, they could also facilitate the development of new materials and drugs.

After all, even a universally programmable quantum computer cannot solve arbitrary problems. And to fulfill the hopes placed in this computer at all, the one million qubits targeted by Google in around ten years will not even be enough. This is not least due to the difference between physical and logical qubits, as Google researcher Markus Hoffmann explains.

One example of a physical quantum bit is an atom suspended in a light lattice or a microscopic superconducting circular current. But because these physical bits are so susceptible to interference from the environment, there is a plan to combine several physical qubits into one logical qubit to store quantum information in it in a much more stable way. In superconducting technology, as Google is exploring, a logical qubit would consist of a thousand synchronized physical qubits.

In a universal quantum computer, many ancilla quantum bits distributed between and around the logical qubits will be added. They will measure disturbances as additional sensors. All of this is intended to answer the challenge that the actual logical qubits may not be checked for errors while they are in the process of computing, which is what a conventional computer would do. A test would be a prohibited measurement, but based on the information from the ancilla qubits and the results of the logical qubits, the algorithm can make meaningful error correction

Such concepts for a universal, error-corrected quantum computer are estimated to come with a large price tag. "That amounts to maybe a hundred million physical qubits," Cirac says: "A quantum computer like this would fill our entire institute with its vacuum and cooling devices!" Hence with today's technology, as Cirac points out, these requirements are "crazy", and this is precisely why he's concerned about the current hype. In his view, even fundamental technical challenges have not yet been mastered.

New ideas from initial applications

Thomas Monz from the University of Innsbruck, on the other hand, is surprisingly laid back. He is part of a

⟶

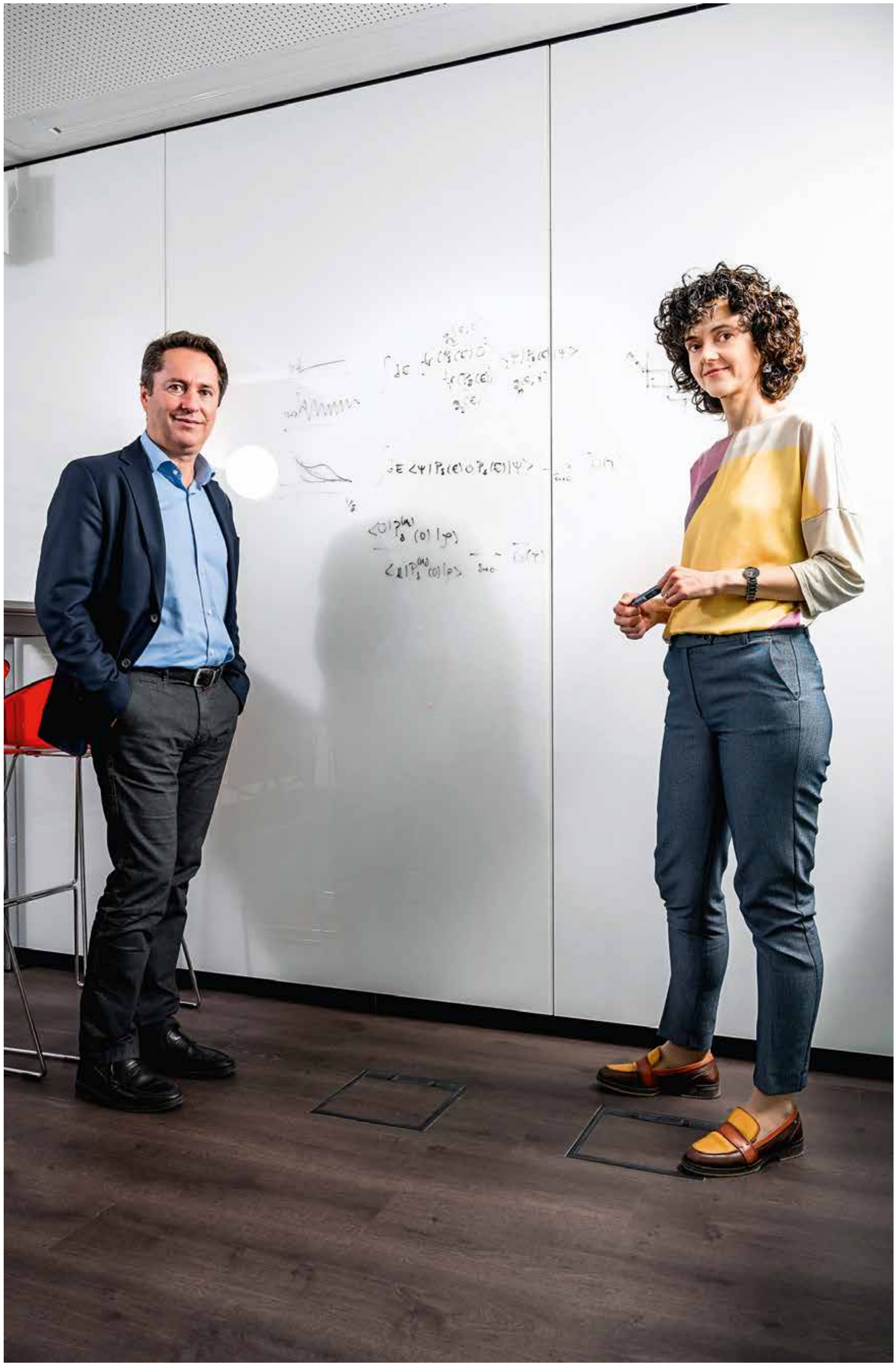


PHOTO: BETHEL FATH FOR MPG

Research with a short- and long-term perspective: Ignacio Cirac and Mari Carmen Bañuls explore how quantum computers can provide useful insights with relatively few qubits. In addition, they are developing algorithms for universally programmable systems with about one million qubits.

team led by Rainer Blatt that is pushing a different technology. The researchers use electrically charged calcium atoms that float – in a string like beads – in an electromagnetic trap called the Paul trap. They are controlled by laser beams. The advantage of these calcium ions is that they interact very strongly with each other due to their electrical repulsion. This can be used for very powerful entanglement. As many as 24 qubits could be entangled in this ion quantum computer.

"It doesn't sound like much, but this entanglement is very stable," Monz says. He is also CEO of the startup Alpine Quantum Technologies (AQT), which already sells ion quantum computers on the commercial market. His group at the University of Innsbruck, supported by AQT, recently demonstrated successful quantum error correction for the first time in collaboration with Forschungszentrum Jülich. "To do this, we connected seven physical qubits each to form logical qubits," Monz says. The idea is simple: after a certain computation time, states of some physical qubits forming a logical qubit usually diverge due to errors; then the majority of qubits matching in state probably show the correct result. "Quantum error correction, after all, is simply about redundancy," Monz says.

To better deal with the error-prone nature of quantum computations, Cirac and his team have launched a project: "We're working on verifying computational results," he says: "I think this is an important question to ask." After all, it needs to be ensured that quantum computers produce reliable results. This kind of debugging must also be carried out repeatedly by established computer technology.

Despite all the limitations, despite the obstacles that quantum computers must still overcome before they can be used for broader applications, Cirac is convinced that once they exist, they will lead us to unexpected ideas. The inspiring effect of the progress in development also motivates him to move quickly to initial, smaller applications. He's certain that: "If you were to interview me again in fifteen years, the most important applications of quantum physics won't be the ones we're talking about today!"

←

GLOSSARY

QUANTUM COMPUTER
Computing with quantum bits, which – unlike digital bits – can also assume superpositions of the states 0 and 1. Moreover, the states of several such qubits can be entangled with each other. This allows them to process different solutions to a computational task in parallel and arrive at solutions to some problems significantly faster than conventional computers.

QUANTUM SIMULATOR
The name given to a specialized quantum computer that makes do with far fewer qubits than a freely programmable quantum computer and can solve special tasks, for example, in the field of materials science.

Model of a quantum system: crossed laser beams form a lattice that resembles an egg carton. In its cavities, atoms can be trapped that can simulate quantum phenomena. Such systems are also candidates for universal quantum computers.

GRAPHIC: CHRISTOPH HOHMANN (MCQST CLUSTER)