ATOMS

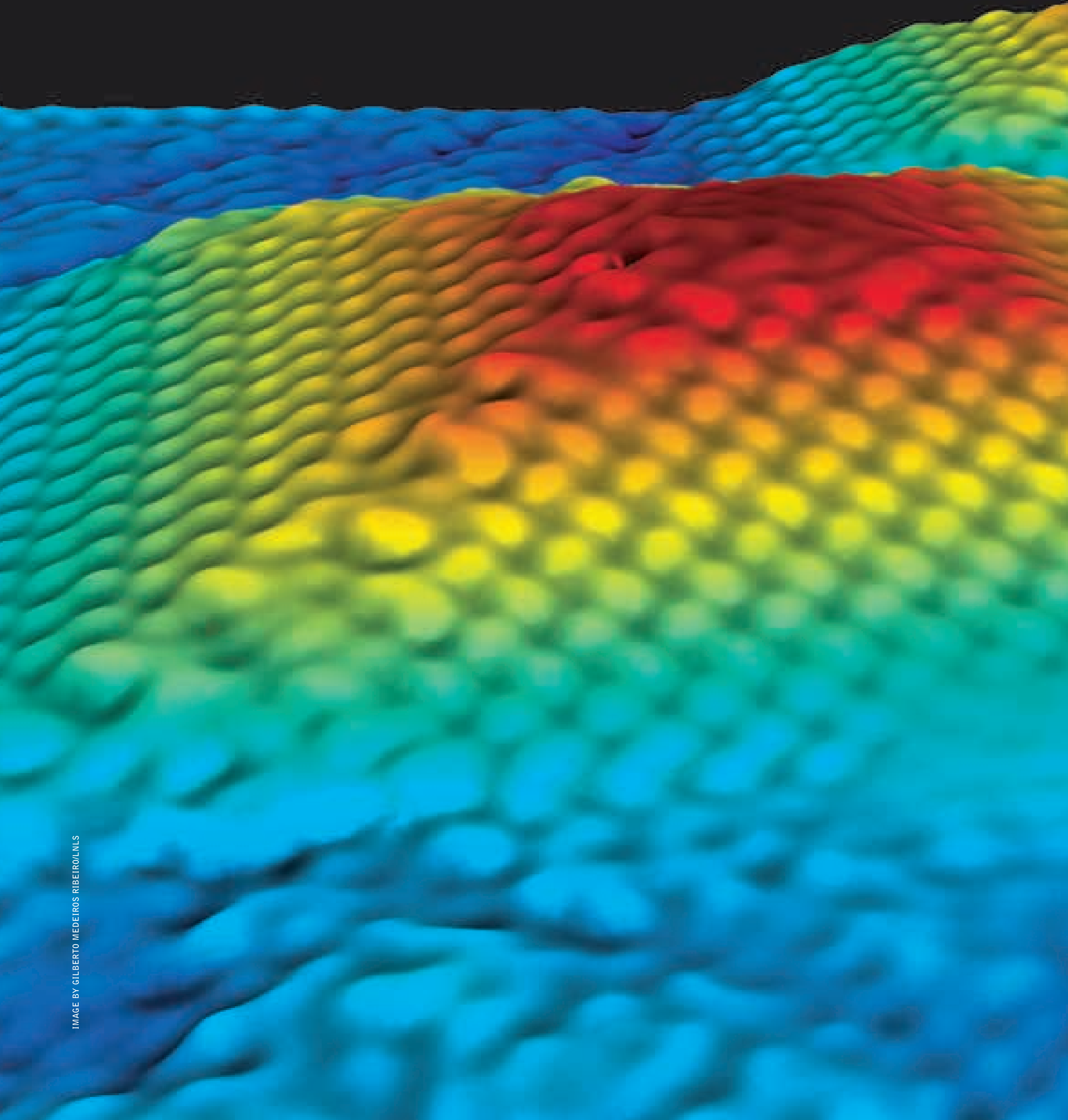
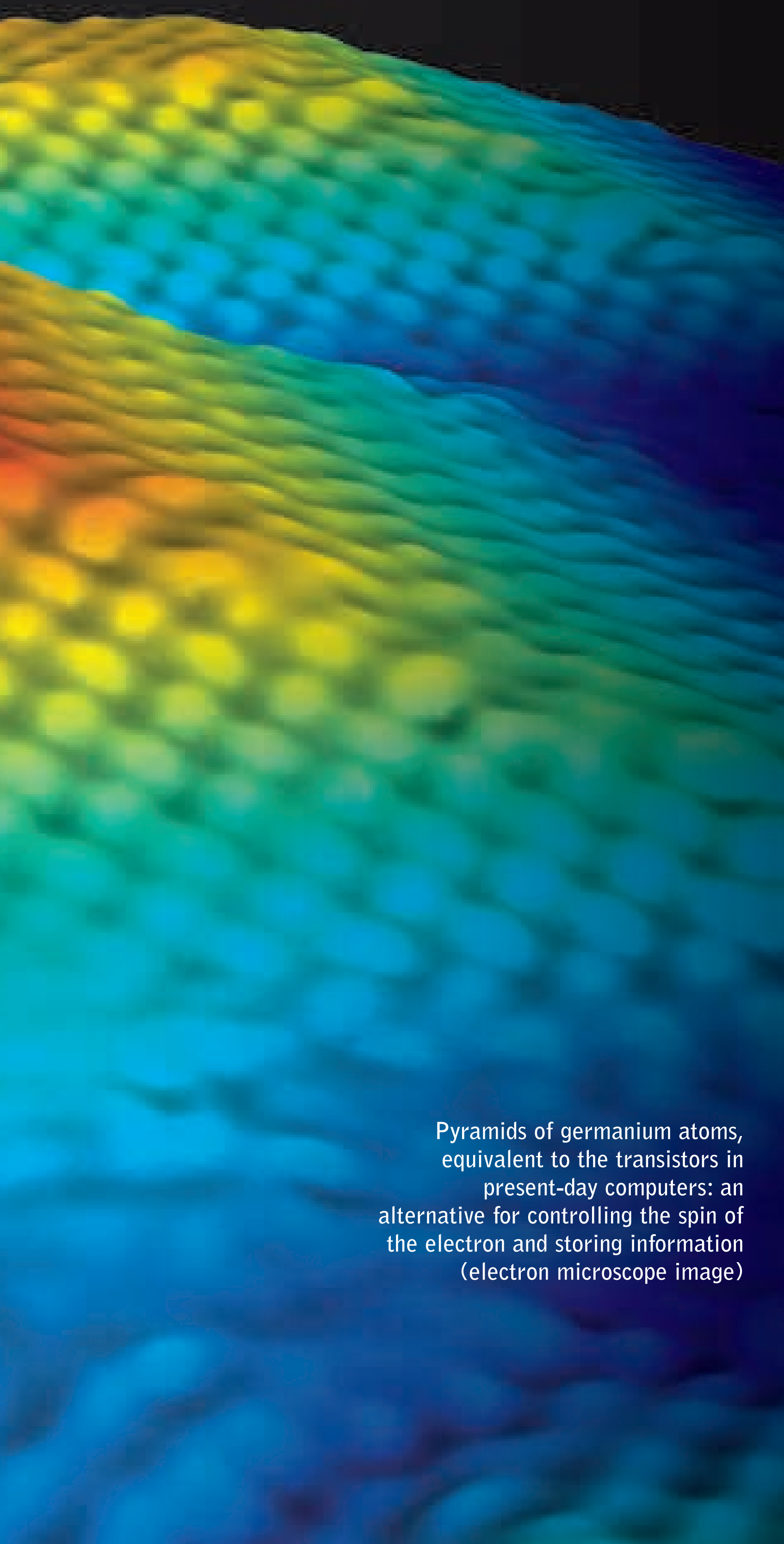


IMAGE BY GILBERTO MEDEIROS RIBEIRO/LNLS

FOR DOING CALCULATIONS



Pyramids of germanium atoms, equivalent to the transistors in present-day computers: an alternative for controlling the spin of the electron and storing information (electron microscope image)

Brazilian physicists in the worldwide race in search of the quantum computer

RICARDO ZORZETTO

Published in April 2003

At least in the heads of physicists, a new kind of computer is starting to be assembled, capable of carrying out in minutes calculations that the most rapid existing supercomputers would take billions of years to do. It is the quantum computer, so-called for working in a way that is completely different from common computers, following the laws of quantum mechanics, the part of physics that explains the phenomena that occur in the world of the atoms, and often defy common sense. Although nobody knows for sure what the appearance of this computer will be like, it will possibly have a monitor, keyboard and a mouse, like today's equipment. The most noteworthy modification should take place in the processor: instead of having silicon chips (integrated circuits) with millions of transistors, it should rely on a few dozen atoms.

To start with, the interest in producing a quantum computer was merely academic: physicists wanted to verify the possibility of carrying out logical operations based on properties of atoms and to prove the forecasts of quantum mechanics. But the capacity for calculating of these computers – theoretically infinite, because it doubles with every atom that is added to the processor – opened up the prospect for strategic applications: the quantum computer could break security codes that protect banking transactions and even the defense systems of nations. It is to avoid disasters with the discovery of these codes that in countries like the United States, even the Department of Defense is funding studies to develop equipment of this kind. Today, the quest for controlling the intrinsic properties of atoms and molecules is not restricted to the universities. Information technology giants, such as IBM, Microsoft and Hewlett Packard, are investing heavily in research in the area, with an eye on the market for microprocessors and memories, which has a turnover of US$ 100 billion a year.

Years or even decades are likely to pass by until a computer that works on the basis of properties of atomic particles reaches the stores. The current stage of development of quantum computing would be equivalent to choosing the material to be used to build the foundations of a building. Physicists are trying to discover the most feasible alternative for using as a basis for a quantum computer: atoms caught in magnetic traps, atomic nuclei submitted to magnetic fields, electrons caught in small pyramids (quantum dots) or even corpuscles of light (photons). It is a stage comparable with the 50s, in the beginnings of computing, with the invention of the transistor, which was to replace electronic valves.

Although it is probable that the first quantum computer will come out of some American laboratory, in view of the heavy investments that researchers there receive, Brazil is not out of the contest. Since studies in this area started, there have been important contributions. Even before talking about a quantum computer, at the beginning of the 80s, Amir Caldeira, from the State University of Campinas (Unicamp), was already showing that some quantum systems on an atomic scale – or even behaving like giant atoms – would lose energy to the environment that surrounds them. This phenomenon, quantum dissipation, is associated with another, decoherence, which leads to an undesirable effect: the loss of quantum information before it can be interpreted.

Now it is physicists from Minas Gerais and Rio de Janeiro that are working together, studying a third kind of computer, the semiquantum, which brings together characteristics of the classical and quantum ones, and should get round a few technical difficulties. "We believe that it will be faster than the common computer and slower than the quantum one", says Carlos Monken, a physicist from the Federal University of Minas Gerais (UFMG) and the coordinator of the team.

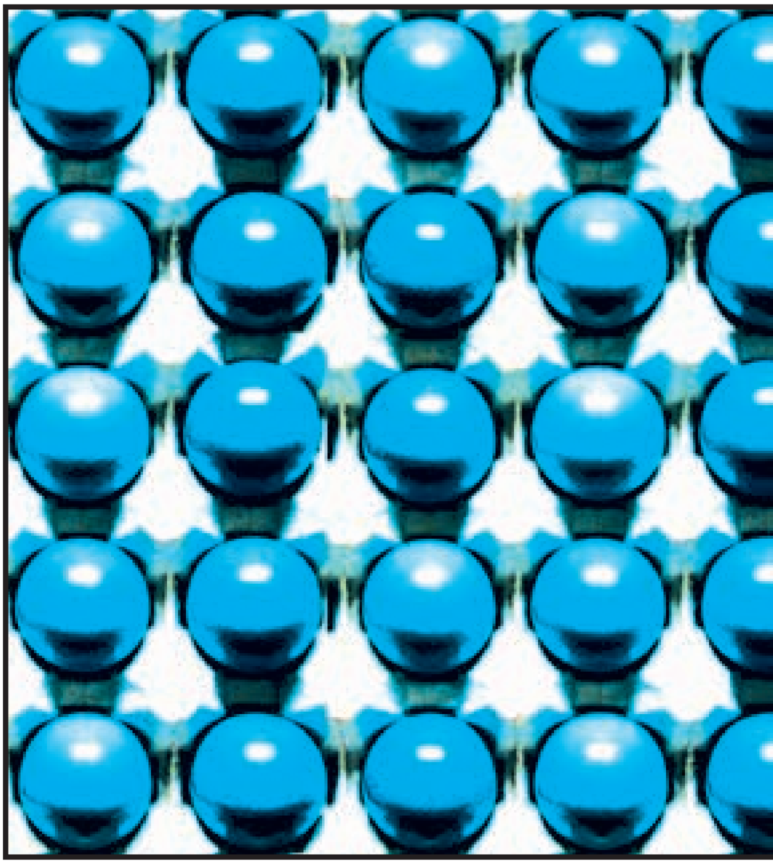
There was a leap forward in research in this area in the country, with the creation of the Millennium Institute of Quantum Information in 2001. Maintained by the Ministry of Science and Technology, it has a budget of R$ 5.2 million and gathers together teams from Rio de Janeiro, Alagoas, Minas Gerais, São Paulo and Pernambuco. Its coordinator, Luiz Davidovich, of the Federal University of Rio de Janeiro (UFRJ), is investigating properties of atoms and photons caught in cavities made up of mirrors and produced in an entangled form, interconnected by a species of telepathic property: everything that happens with one particle affects the other.

Based on twin particles, the group from UFRJ proposed the first experiment for transferring the state of one particle to another distant one, called quantum teleportation, which was popularized with the science fiction series Star Trek. In an article published in 2001 in *Physical Review Letters*, which merited a comment in *Nature*, the physicists from Rio de Janeiro showed that it is possible to protect from decoherence the quantum state of an atom in a magnetic trap, one of the options thought up for the prototypes of quantum computers.

The secret of the performance of this kind of computer is the way it handles the unit of information, the bit. In the common – or classical – computer, the bits are registered by transistors, tiny devices in an electronic circuit that allow an electrical signal to pass or not, and are parts of the processor and the memory chips. When carrying out a command, the classical computer associates with each bit just one of two values: either 0 or 1. As each transistor interprets just one bit at a time and the number of transistors in a chip is limited – a Pentium 4 processor, for example, has 40 million transistors –, the calculating capacity of today's computers is becoming restricted, warns Iuri Pêpe, from the Optical Properties Laboratories of the Federal University of Bahia (UFBA).

In the world of atomic particles – some hundred thousand times smaller than a transistor –, this ratio is not one of exclusion, but of superposition. However strange it may seem, instead of assuming only one value or another (0 or 1), the quantum bit, or qubit, as it is abbreviated, can represent the infinite value existing between 0 and 1, including 0 and 1. All at the same time. It is a property of atomic particles known as superposition of quantum states that should govern the functioning of the new machines.

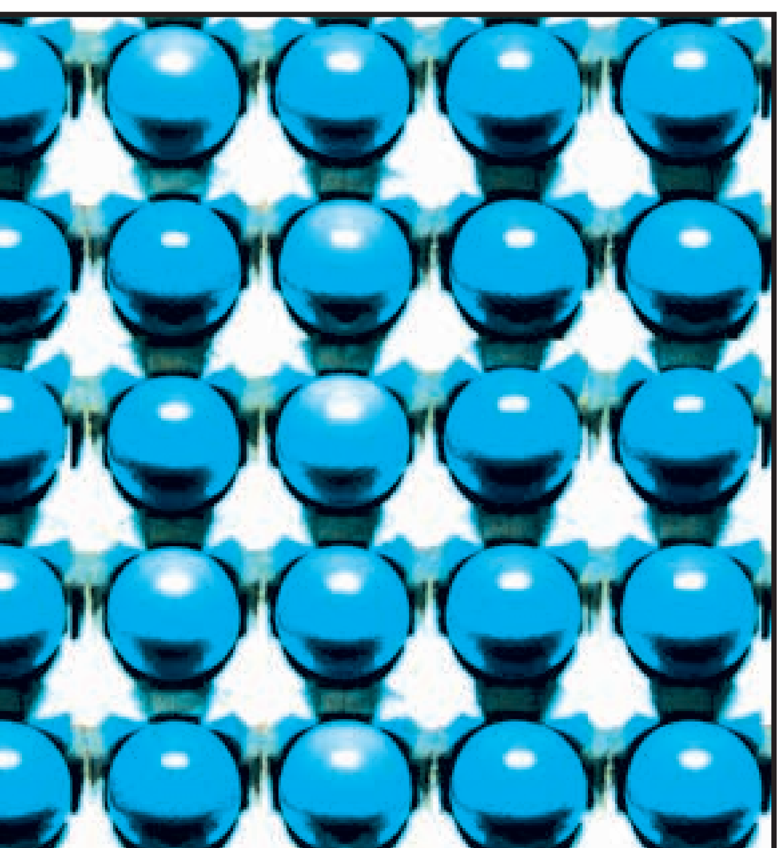
It is this superposition of states that allows each qubit to handle infinite bits of information simultaneously, as if they were countless common computers acting at the same time on



one calculation and guaranteeing the quantum computer a matchless superiority in processing. Well, at least in theory, because the superposition of states also generates a difficulty. Another rule of quantum mechanics – the uncertainty principle, according to which it is impossible to know the position and the velocity of a particle at the same time – prevents one from knowing all the values that the qubits may take on at a single time when doing some calculation. The theory indicates that the computer should behave like a quantum one while processing the information and as a classical one when providing the results of the operations. Could there then be an advantage in building a computer of this kind?

The answer is yes, provided that one knows how to take advantage of the superposition of quantum states. To do so, the physicists are dealing with the probability of getting a specific result. One example: there are at least two ways of discovering how many people in a group of ten like chocolate ice cream. In both of them, each interviewee can only answer yes or no. The first manner, adopted by today's computer, is to ask each person if they like chocolate ice cream. Afterwards, add up the replies and get the final result in a total of ten consecutive operations (ten questions and the final totting up). The quantum computer manages to give the answer in a single operation, provided that one wants to know not the individual replies, but what percentage of them answers yes to the query. The secret lies in putting to the computer different questions, in an intelligent way", explains physicist Reinaldo Oliveira Vianna, from UFMG.

Prototypes - The closest one gets to a quantum computer is today in the experimental physics laboratories of universities in America, Europe and even in Brazil – like at UFMG, UFRJ and the University of São Paulo (USP). Even so, the pieces of equipment that have been built are only primitive prototypes, which carry out very simple operations, such as the calculation of the divisors of the number 15, or a search in a database with only eight items. But this is only the beginning, of course. There is no physical barrier to carrying out quantum computing on a large scale", avers Ivan Oliveira, a researcher from the Brazilian Center for Physical Researches (CBPF), in Rio. "The computer will be made. It is a question of time and investment." With physicists from USP and from the Federal University of Espírito Santo (UFES), Oliveira uses nuclear magnetic resonance, the same technique that produces images of the human body, to carry out basic logical operations (sums, divisions and multiplications) with atomic nuclei.



PHOTOGRAPH BY EDUARDO CESAR

Rows of atoms: possible basis for the quantum computer

Even the physicists doubted this idea of using atoms and molecules to deal with information. In 1959, American Richard Feynman (1918-1988, Nobel Prize in 1965) felt in the flesh the skepticism of his colleagues when he put forward this possibility. The disbelief persisted until 1973, when chemist Charles Bennett, from IBM, showed the possibility of carrying out reversible logical operations – precisely the opposite to what happens in today's computers, in which the bits used for a given calculation are undone. Almost ten years later, Paul Benioff, of the Argonne National Laboratory, in the United States, put forward the first model of a quantum computer, capable of carrying out these reversible operations.

Only in 1994 did this subject acquire strategic importance. It was when Peter Shor, a scientist from AT&T, presented a process for calculating that would allow a quantum computer to reveal the components of numbers with thousands of digits in less steps and more quickly than the classical computer (the number 15, for example, can be broken down into 3 and 5). His juggling with numbers is the basis of the data protection systems adopted by Brazilian banks, which have a turnover of from R$ 2.5 trillion to R$ 6 trillion per month, in 50,000 to 80,000 encoded transactions. "A quantum computer could perhaps have a processing power that would make it possible to break this code in the course of one day and not over one year", comments Maurício Ghetler, the technology director of Banco Santos. "But this is not the system's only protection, and, the moment a piece of equipment of this kind is available, the financial system will use other forms of protection."

Later on, physicist Lov Grover, from the Bell Laboratories, proposed a mathematical procedure that would make it possible for a quantum computer to carry out searches in a database in a way that would make it more efficient as the size of the database increases. According to this method of calculating, known as Grover's algorithm, while a common computer has to carry out an average of two operations to do one search in a database with four records, the quantum computer needs

THE PROJECTS

■ **MINAS GERAIS**

Development of Quantum Algorithms

COORDINATOR
Carlos Henrique Monken – UFMG

INVESTMENT
R$ 631,245.00 (CNPq/MCT)

■ **RIO DE JANEIRO**

Quantum Computing by Nuclear Magnetic Resonance

COORDINATOR
Alberto Guimarães Passos Filho – CBPF

INVESTMENT
R$ 7,200.00 (CNPq/MCT)

COORDINATOR
Ivan dos Santos Oliveira Júnior –- CBPF

INVESTMENT
R$ 7,200.00 (CNPq/MCT)

Quantum Information Institute

COORDINATOR
Luiz Davidovich – UFRJ

INVESTMENT
R$ 2,144,000.00 (CNPq/MCT)

■ **SÃO PAULO**

Non-Perturbative Methods in Correlated Electronic Systems

COORDINATOR
Amir Ordacgi Caldeira – Unicamp

INVESTMENT
R$ 80,657.74 (FAPESP)

Nanostructured Materials Investigated by Tunneling and Atomic Force Microscopy

COORDINATOR
Gilberto Medeiros Ribeiro – LNLS

INVESTMENT
R$ 501,136.62 (FAPESP)

A Study of Slow Dynamics in Polymers Through NMR

COORDINATOR
Tito José Bonagamba – IFSC/USP

INVESTMENT
R$ 93,704.14 (FAPESP)

only one step. For a query in a file with 16 records, a classical computer would do, on average, eight searches, and the quantum computer, four.

The discoveries by Shor and Grover gave a thrust to studies in the area – the number of publications on the theme went up, even in more general scientific magazines. It was in an article in Nature, for example, that Daniel Gottesman, from Los Alamos National Laboratory, and Isaac Chuang, from IBM, demonstrated that another property of quantum mechanics, teleportation, would make it possible to build a quantum computer with today's technology. Chuang had already revealed that it would be feasible to manipulate the alignment of atomic nuclei in relation to a magnetic field. Just like the needle of a compass, some atomic nuclei show magnetism – it would be enough for them to be controlled by means of nuclear magnetic resonance. In January this year, in *Nature*, Chuang corroborated another calculating process, which indicates whether a coin is genuine (one side is heads, the other, tails) or false (it has two heads or two tails), looking at just one of the sides. Any person needs to observe both sides of the coin before giving a minimally reliable reply.

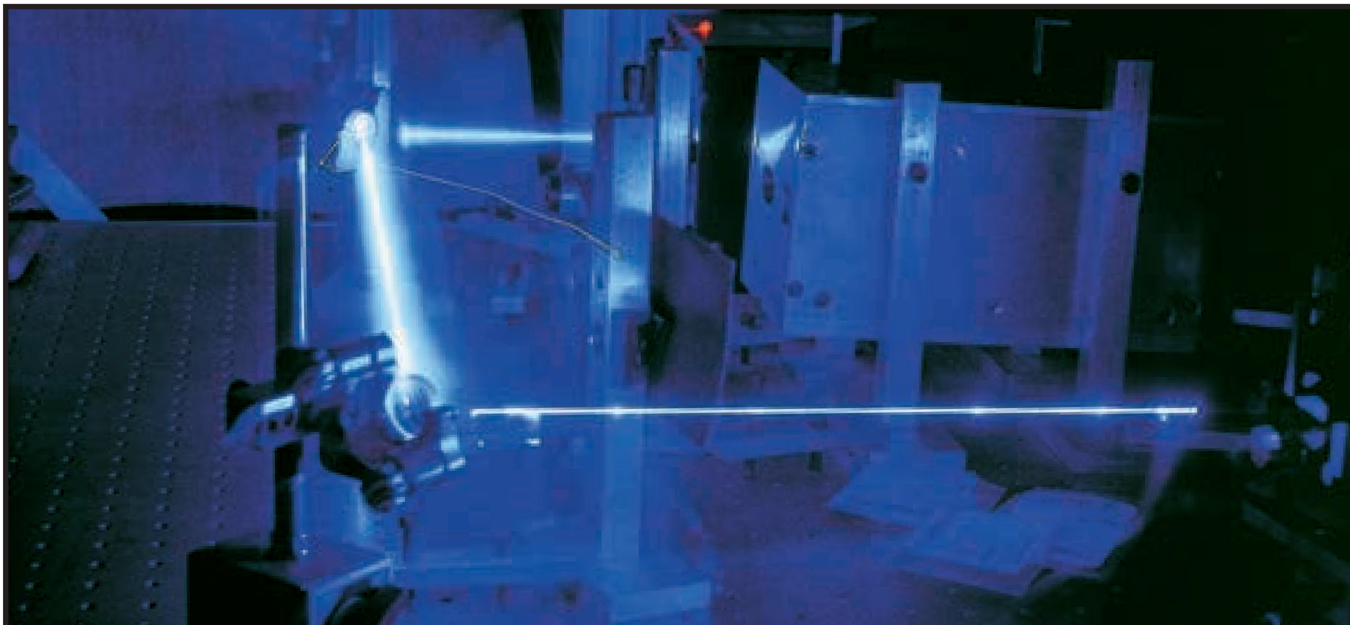
One question still bothers researchers: in practice, would the processing of calculations carried out by a quantum computer really be quicker than the classical one? To find out, you would have to build a piece of equipment with several dozens of qubits, which would then be close to a real quantum computer. It doesn't even have to be very big. A computer of this kind with some 300 qubits would be capable of handling more quantum states than atoms on the Universe, which is equivalent to number 1 followed by 80 zeroes.

For Reinaldo Oliveira Vianna, from UFMG, the experiments carried out to date, with about 7 qubits, are not sufficient to show that the quantum method of carrying our calculations is quicker. "The preparation of the data in the form of qubits may take time, as it is still complicated to produce hundreds of qubits", the physicist explains. "It is only going to be possible to discover if the quantum computer really is more agile if one is constructed."

Version from Minas - As no one has managed to surpass the barrier of a dozen qubits in the quantum computer, Vianna, Carlos Monken and Sebastião Pádua, from UFMG, alongside Paulo Henrique Souto Ribeiro, from UFRJ, all connected with the Millennium Insitute, are examining an alternative that seems to be simpler. This is the semi-quantum computer, inspired on a model proposed by Jeffrey Yepez, of the Air Force Research Laboratory, of the United States. This hybrid equipment carries out the processing of information in the quantum way, by means of photons, and stores the results on a classical memory chip. It should be quicker than the classical computer, for needing less qubits for processing the same quantity of information, as the calculation of the team from Minas show.

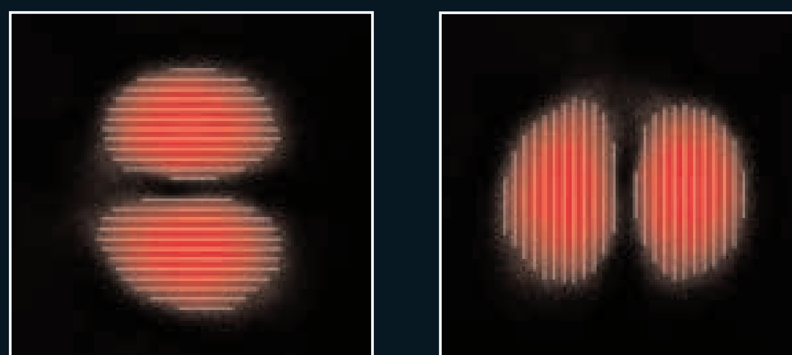
Monken's group also made some more progress, in the way of storing the information in the quantum computer. Usually, the unit of information is associated with the direction of vibration (polarization) of the photons, corpuscles of light that behave like electromagnetic waves vibrating in space, like cords being shaken. The team from UFMG managed to associate another characteristic to the polarization of light, horizontal or vertical: the spatial form of the photon. By making the corpuscle of light pass through a special crystal, the physicists succeed in splitting it into two parts, which are propagated in parallel, aligned horizontally or vertically. They thereby encoded in a single photon not one qubit, but two: one in the direction of polarization, and another in the spatial alignment, as shown in an article to be published in *Physical Review Letters*.

In USP's São Carlos Physics Institute, a team led by Tito Bonagamba is looking for a way of overcoming the loss of quantum information (decoherence) during the processing of the data with nuclear magnetic resonance. In experiments with liquid crystal, carried out with Ivan Oliveira, Roberto Sarthour and Alberto Passos Guimarães Filho, from the CBPF, and Jair Checon de Freitas, from UFES, Bonagamba described with precision the decoherence time of quantum information: one qubit is capable of storing it for up to 15 thousandths of a second. The team is now proposing new ways of carrying



PHOTOGRAPH BY RODRIGO QUEIROZ

The half quantum, half classical computer: on an optic table like the one above, researchers from Minas and Rio associate the direction of the vibration of light (white stripes) with the spatial form of the photons (vertical or horizontal ellipses). Accordingly, they add one more piece of information per qubit.



CARLOS MONKEN/UFMG

out quicker experiments or preserving the information for longer, guaranteeing the possibility of doing complex calculations.

Antonio Vidiella-Barranco and José Antonio Roversi, from Unicamp, are working in a different way: they are manipulating the information with photons and ions (atoms with an electrical charge) trapped in cavities formed by mirrors. In *Physics Letters A* of July 2001, they showed that it is possible to perform logical operations with this system. "We proposed an alternative that involves a more robust system for storing the information (the vibration of ions), associated with light, which is good for transmitting data", says Barranco. In another work, they indicated that it is possible to recover the original information, even after it has been lost through decoherence. By throwing a beam of light on top of another, trapped in the cavity, they developed a scheme where everything happens as if the operations could take place with time frozen.

Pyramids - Because of the difficulty of controlling a sufficient number of qubits that a quantum computer must have, to be able to work in systems that use photons or nuclear magnetic resonance, some physicists are betting that the most promising alternative is the imprisoned ions. But electronic engineer Gilberto Medeiros Ribeiro, from the National Laboratory of Synchrotron Light (LNLS), in Campinas, disagrees. For him, the final form of a quantum processor will be some kind of semicondutor, as happened with present-day computers. "Today's computer started with valves and afterwards migrated to semicondutors", says Ribeiro, who is producing structures that are hundreds of times smaller than transistors, quantum dots, pyramids with a base of 20 nanometers and 3 nanometers high – a nanometer is one millionth part of a millimeter. Inside of them, a single electron is trapped, with the objective of controlling the direction of its rotation, or spin, in order to carry out logical operations.

Ribeiro has now shown it to be possible to control the number of electrons trapped in quantum dots of indium arsenide, a semiconducting material that forms islets on gallium arsenide. In an article to be published in *Physical Review Letters*, he indicates how to foresee the distribution and the size of quantum dots in another semiconducting material, germanium deposited on silicon. At the moment, Ribeiro and Harry Westfahl, from the LNLS, and Amir Caldeira, from Unicamp, are studying the decoherence time of the information stored in the spin of the electrons in the quantum dots, with the support of HP Brazil. It will not be easy to arrive at the quantum computer, but what is going to be learnt in search of it should compensate for the effort. •