QUANTUM COMPUTER QUEST

After a 30-year struggle to harness quantum weirdness for computing, physicists finally have their goal in reach.

BY ELIZABETH GIBNEY

When asked what he likes best about working for Google, physicist John Martinis does not mention the famous massage chairs in the hallways, or the free snacks available just about anywhere at the company's campus in Mountain View, California. Instead, he marvels at Google's tolerance of failure in pursuit of a visionary goal. "If every project they try works," he says, "they think they aren't trying hard enough."

Martinis reckons that he is going to need that kind of patience. In September, Google recruited him and his 20-member research team from the University of California, Santa Barbara, and set them to work on the notoriously difficult task of building quantum computers: devices that exploit the quirks of the quantum world to carry out calculations that ordinary computers could not finish in the lifetime of the Universe.

© 2014 Macmillan Publishers Limited. All rights reserved

EQUINOX GRAPHICS/SPL

It is a vision that has frustrated Martinis and many other physicists ever since it was proposed in the early 1980s. In practice, the quantum effects essential in such a computer are incredibly fragile and hard to control: if one stray photon or vibration from the outside hits the device in the wrong way, the calculation will collapse. Even today, after three decades of effort, the best quantum computers in the world are barely able to do school-level problems such as finding the prime factors of the number 21. (Answer: 3 and 7.)

The result has been a rate of progress so slow that sceptics often compare quantum computing to fusion energy: it is a revolutionary technology that always seems to be decades away.

But maybe not. Many physicists in the field think that their 30-year slog may finally be on the verge of paying dividends. Not only can they now generate quantum bits, or 'qubits', that last for minutes instead of nanoseconds, they are also much better at correcting the system when errors arise from outside perturbations and other causes. At the same time, quantum-software engineers are coming up with applications that could justify the expense of developing these machines, such as finding new catalysts for industrial processes.

> "THERE ARE NO FUNDAMENTAL ROADBLOCKS LEFT."

The prospects for useful and profitable quantum computers are good enough to have drawn Google into the game, along with IBM and Microsoft, among others. Several academic groups are also pushing the technology in practical directions. At the Delft University of Technology in the Netherlands, for example, the government-backed QuTech Centre is bringing researchers together with the Dutch high-tech industry. Delft physicist Ronald Hanson says that he will be able to make the building blocks of a universal quantum computer in just five years, and a fully functional — if bulky and inefficient — demonstration machine in a little more than a decade.

Martinis says that he has no fixed timetable, but is just as optimistic. "We got a lot of things working in the last couple of years," he says. "It is still possible that nature just won't allow it to work, but I think we have a decent chance."

SEVENTIES CHILD

The conceptual foundations of quantum computing were laid during the 1970s and early 1980s — most notably by the late US physicist Richard Feynman, whose lecture on the subject, published[1] in 1982, is widely credited with launching the field. The basic insight is that conventional computers are 'either–or' machines, meaning that the tiny silicon circuit that encodes a given bit of information acts like a switch that is either open or closed. This means that it can represent choices such as 'true' or 'false', or the 1s and 0s of binary arithmetic. But in the quantum realm, 'either–or' gives way to 'both–and': if binary 1s are represented by, say, electrons that are spinning clockwise, and 0s by electrons spinning counterclockwise, then the subatomic laws that govern those particles make it possible for a given quantum bit to be both 1 and 0 at the same time.

By extension, the set of qubits comprising the memory of a quantum computer could exist in every possible combination of 1s and 0s at once. Where a classical computer has to try each combination in turn, a quantum computer could process all those combinations simultaneously — in effect, carrying out calculations on every possible set of input data in parallel. And because the number of combinations increases exponentially with the size of the memory, the quantum computer has the potential to be exponentially faster than its classical counterpart.

That insight became much more than a scientific curiosity in 1994, when the US mathematician Peter Shor developed an algorithm that would allow a quantum computer to factor large numbers very quickly[2]. Such factorization is prohibitively time-consuming for standard computers, which is why it forms the basis for widely used encryption techniques. Shor's algorithm meant that in principle, quantum computers could crack that encryption.

Then two years later, Lov Grover, a researcher at Bell Labs in Murray Hill, New Jersey, devised another algorithm that showed how quantum computers could radically speed up searches of massive databases[3].

The demonstration of such obviously important applications quickly attracted researchers and funding — accompanied by claims that working quantum computers would be ready in a matter of years. "But in hindsight they were naive," says Hanson. Researchers have been able to make some progress by devising special-purpose quantum devices that are tailored for solving specific problems (see *Nature* **491,** 322–324; 2012 and *Nature* **498,** 286–288; 2013). But achieving the ultimate goal — a general-purpose, digital quantum computer that can be programmed to carry out any algorithm — has proved much tougher.

The problem is the extreme fragility of quantum effects: any slight influence from the outside world will cause a qubit to collapse so that it no longer represents many different states at once. If qubits are going to be useful in real-world calculations, they must be kept in the strictest isolation and manipulated with care — extremely difficult tasks. They also need to remain in their quantum states for much longer than it takes to perform a computing step — typically a microsecond or so.

To achieve those goals, physicists are pursuing a two-fold strategy: extending the life of qubits and reducing how often they go wrong, and devising algorithms that can correct any errors that do occur.

The qubit design currently favoured by many researchers is based on microchip-scale circuits made from superconductors, materials that lose all resistance to the flow of electricity at very low temperatures. Thanks to a quantum phenomenon known as the Josephson effect, electric currents flowing around tiny loops in such circuits can circle both clockwise and counterclockwise at once, so are perfect for representing a qubit. Such circuits are tricky to implement, says Martinis. "You have to work many years to figure out all the physics." But after a decade spent refining designs and learning how to isolate the circuits from the environment, his group and others have increased qubit lifetimes by a factor of 10,000, meaning that they can now regularly maintain their state for around 50 to 100 microseconds. They have also slashed the rate at which errors occur by finding better ways to manipulate and control their qubits as the computation proceeds.

Lifetimes have been tougher to boost for qubits that are based on the spins of electrons or atomic nuclei, because these spins are easily flipped by the magnetic fields of neighbouring particles. In October, however, Andrea Morello and Andrew Dzurak, physicists at the University of New South Wales in Sydney, Australia, announced[4] that they had eliminated such interference by embedding spin-qubits in purified silicon that contains no magnetic isotopes of the element. The resulting qubits lived as long as 30 seconds.

In 1997, physicist Alexei Kitaev of the California Institute of Technology in Pasadena proposed[5] a more radical approach: make qubits out of anyons, which are states of matter that arise from the collective properties of many particles, yet behave as just one particle. Some anyons have another special property: their quantum state reveals a history of their recent interactions. If these anyons were used as qubits, Kitaev argued, the order of their interactions could encode information. And because this encoding is effectively spread throughout the system, the qubits would have a natural protection against errors arising in any individual part.

Known as 'topological qubits', these entities remain theoretical, but the idea shows enough promise that Microsoft and a number of other companies are investing in efforts to create them in the laboratory.

Even with the most robust qubits, however, errors are inevitable. That is also the case in ordinary computers, but errors are particularly

NATURE.COM
To hear about quantum-computer development, see:
go.nature.com/b2jda4

© 2014 Macmillan Publishers Limited. All rights reserved

troublesome in a quantum computer because they grow exponentially with the number of qubits. "One of the real tricks of eventually building a quantum computer is finding a way to get around that," says David Cory, an experimental quantum physicist at the University of Waterloo in Canada.

That means implementing some form of quantum error correction. In standard computers, correcting for errors can be as simple as starting off with multiple copies of each bit. A majority vote among the copies can reveal whether any one of them has later flipped from a 1 to 0 or vice versa. That does not work in the quantum world because it is impossible to copy a qubit without destroying its quantum state. But qubits can be compared, so theorists have tried to devise correction schemes that ask various pairs of qubits whether they have the same or different values, and then use the answers to deduce whether individual qubits have gone wrong.

Until recently, a big problem was that qubits typically made about one error in every ten computer steps, and the available correction schemes could not begin to keep up. "Theorists were saying we need average error rates to be, say, 1 in 100,000 operations," says John Morton, an experimental physicist at University College London. In April this year, however, Martinis and his group announced[6] that they had demonstrated a 'surface-code' scheme that spreads the quantum information of a qubit among several physical qubits, similar to what Kitaev proposed for topological qubits. In its publication, the group described how it had used this technique to implement 5 qubits of information in a way that could handle error rates as high as 1 per 100 operations — a rate that they and others[7] are now able to achieve (see page 10).

"WE'RE SOMEWHERE BETWEEN THE INVENTION OF THE TRANSISTOR AND THE INVENTION OF THE INTEGRATED CIRCUIT."

ONWARDS AND UPWARDS

Together, improvements in qubit error rates and the ability of codes to cope with errors have radically changed the outlook of the field, says Morton. "What makes it an exciting time is that we can now focus on scaling up," he says.

At the QuTech Centre, Hanson agrees. "There are no fundamental roadblocks left," he says. He is now advertising for 5 electrical engineer professorships, and looking for 40 technicians and researchers, so that he can scale up from laboratory experiments to practical technology. Their main tasks will be to figure out how to fabricate large-scale qubit arrays, how to control the quantum computation and read out the results and how to connect up the quantum circuitry to classical electronics that reside on the same chip.

Both Hanson and his colleague Lieven Vandersypen, who leads Delft's efforts to develop spin qubits embedded in the tiny semiconductor crystals known as quantum dots, aim to build arrays of 17 qubits in the next 5 years. This, they say, is the minimum to demonstrate that the surface-code scheme works as hoped. To create a single virtual qubit that remains correct over the hours it takes to run real algorithms may mean spreading its information over 100 physical qubits. Each extra qubit increases the complexity of the hardware. But once a team has acquired the know-how to create a few dozen physical qubits, they believe, growing to the hundred they need to make a handful of virtual qubits should be much easier. "Then it's a case of ambitious engineering to go to 100, or 1,000. I hope that in 10 years we'll be talking about 100s of qubits," says Vandersypen.

At the Swiss Federal Institute of Technology in Zurich, however, theoretical physicist Matthias Troyer cautions that the goal of hundreds of qubits will not be easy or cheap to achieve. Assuming that quantum chips will be as least as hard to manufacture as semiconductor chips, Troyer estimates that working out how to wire up, manipulate and fabricate qubits in bulk will be a US$10-billion problem. That poses a crucial question, he says. "Why should one do it?"

Troyer has spent the past three years looking for an answer — a 'killer app' for quantum computing that would make the development costs worthwhile. The two classic examples, code-cracking and searching databases, are not good enough, says Troyer. Shor's algorithm will require thousands of qubits to do any serious factorization, he says, and there are other forms of encryption that a quantum computer would do nothing to solve. And although quantum computers may search databases faster, they are still limited by the time it takes to feed the data into the circuit, which would not change.

Troyer thinks that a much more fruitful application for the near future is the modelling of electrons in materials and molecules — something that quickly becomes too difficult for today's supercomputers. At first, this, too, seemed a long shot. His early estimates suggested that it would take a quantum computer as long as 300 years to simulate the molecular dynamics of even a small molecule — such as the iron sulphide inside the ferredoxin proteins that are involved in nitrogen fixation in plants. "Clearly, that was on the border of being science fiction," he says. But by rewriting the software[8], he brought the figure down to 30 years — then to just 300 seconds. "Just like in classical computing, where one has to sit down and optimize the algorithm," he says, "the same is needed for a quantum algorithm."

With around 400 encoded qubits, Troyer says, it would be possible to analyse ways to improve industrial nitrogen fixation — the energy-intensive process that turns the unreactive molecule in air into fertilizer. This reaction is now carried out on an industrial scale using the 116-year-old Haber process, but that uses up about 5% of the natural gas produced each year worldwide. Troyer thinks that a quantum computer could help to design a catalyst that would be much more energy-efficient than the current ones. "That would be worth building a quantum computer for," he says.

Other killer applications might be searching for new high-temperature superconductors, or improving the catalysts used to capture carbon from the air or from industrial exhaust streams. "All these are important questions. If it makes progress there, easily that's your 10 billion," says Troyer.

For now, however, Martinis and other veterans of the field caution that quantum computing is still in the early stages. Although industry is now deep into the research, no one even has one of these things to play with. Quantum computing today is comparable to conventional computing in the years after the Second World War, he says, when every device was a laboratory experiment that had been crafted by hand. "We're somewhere between the invention of the transistor and the invention of the integrated circuit," he concludes. At Google, the project has the buzz of a Silicon Valley start-up, says Martinis, albeit one with hefty backing. After years of the hard work of perfecting qubits, he is happy to finally be able to focus on building a quantum computer that can actually solve real problems. "Google created a new name for scientists working on the hardware effort, 'quantum engineers'," says Martinis. "This is a dream job for me." ■

Elizabeth Gibney *is a reporter for* Nature *based in London.*

1. Feynman, R. P. *Int. J. Theoret. Phys.* **21,** 467–488 (1982).
2. Shor, P. W. *Proc. 35th Ann. Symp. Found. Comp. Sci. IEEE* 124–134 (1994).
3. Grover, L. K. *Proc. 28th Ann. ACM Symp. Theory Comput.* 212–219 (1996).
4. Muhonen, J. T. *et al. Nature Nanotechnol.* http://dx.doi.org/10.1038/nnano.2014.211 (2014).
5. Kitaev, A. Y. *Ann. Phys.* **303,** 2–30 (2003).
6. Barends, R. *et al. Nature* **508,** 500–503 (2014).
7. Hart, T. P. *et al. Phys. Rev. Lett.* **113,** 220501 (2014).
8. Poulin, D. *et al.* Preprint at http://arxiv.org/abs/1406.4920 (2014).

© 2014 Macmillan Publishers Limited. All rights reserved