Questioning quantum speed

The promised speed of a quantum computer is usually explained in terms of its ability to make many calculations in parallel. But, as **Philip Ball** reports, many quantum theorists reject this idea and point to other explanations entirely

Philip Ball is a science writer and journalist based in London, UK, e-mail p.ball@btinternet.com

In the 1980s, University of Oxford physicist David Deutsch had an insight that would spawn an entirely new goal for physicists. He argued that a computer that manipulates information according to quantum rules rather than classical physics might work much faster than conventional machines. Subsequent studies confirmed that idea, although the rudimentary experiments on quantum computing have so far used only a handful of quantum bits. But even though the awesome speed that Deutsch forecast has not yet been unleashed, that power is evidently available in principle from quantum physics.

When he began thinking about these ideas, Deutsch was a committed proponent of the "many worlds" interpretation of quantum mechanics, which holds that every possible state of a quantum wavefunction is realized in parallel universes. Deutsch argued that the quantum speed-up comes from the fact that in effect a quantum computer performs many calculations at the same time in these "other worlds", whereas a classical computer has only one world in which to work. He called this "quantum parallelism".

The many-worlds interpretation of quantum theory was derived from Hugh Everett's ideas in the 1950s, but it remains controversial to this day and is rejected by many quantum theorists. All the same, Deutsch's notion of quantum parallelism has stuck – the standard explanation in popular descriptions of quantum-computing speed-up is still that massively parallel computation takes place, whether or not it involves other universes.

The common proposition for how a quantum computer works is that its quantum bits (qubits) can be placed in superposition states, encoding not just a binary 1 or 0 but any combination of the two. This means that, while the superposition is sustained, the quantum computer can juggle simultaneously with many more potential "solutions" to a computational problem than can a classical machine, accounting for its remarkable speed.

It's a nice intuitive picture – but is it true? "I don't believe it for a minute," says quantum theorist Christopher Fuchs of Raytheon BBN Technologies, a US-based company that is currently developing real quantum processors from superconducting circuits. "The source of the speed-up is something of an entirely different character," he argues.

He isn't alone. Several other quantum physicists take issue with the "parallelism" picture, saying that at best it is only a crude representation, and perhaps a total misrepresentation. "I agree that this is not at all the right way to explain what is going on, though I've been guilty of doing it myself," says David Poulin of the Université de Sherbrooke in Quebec, Canada.

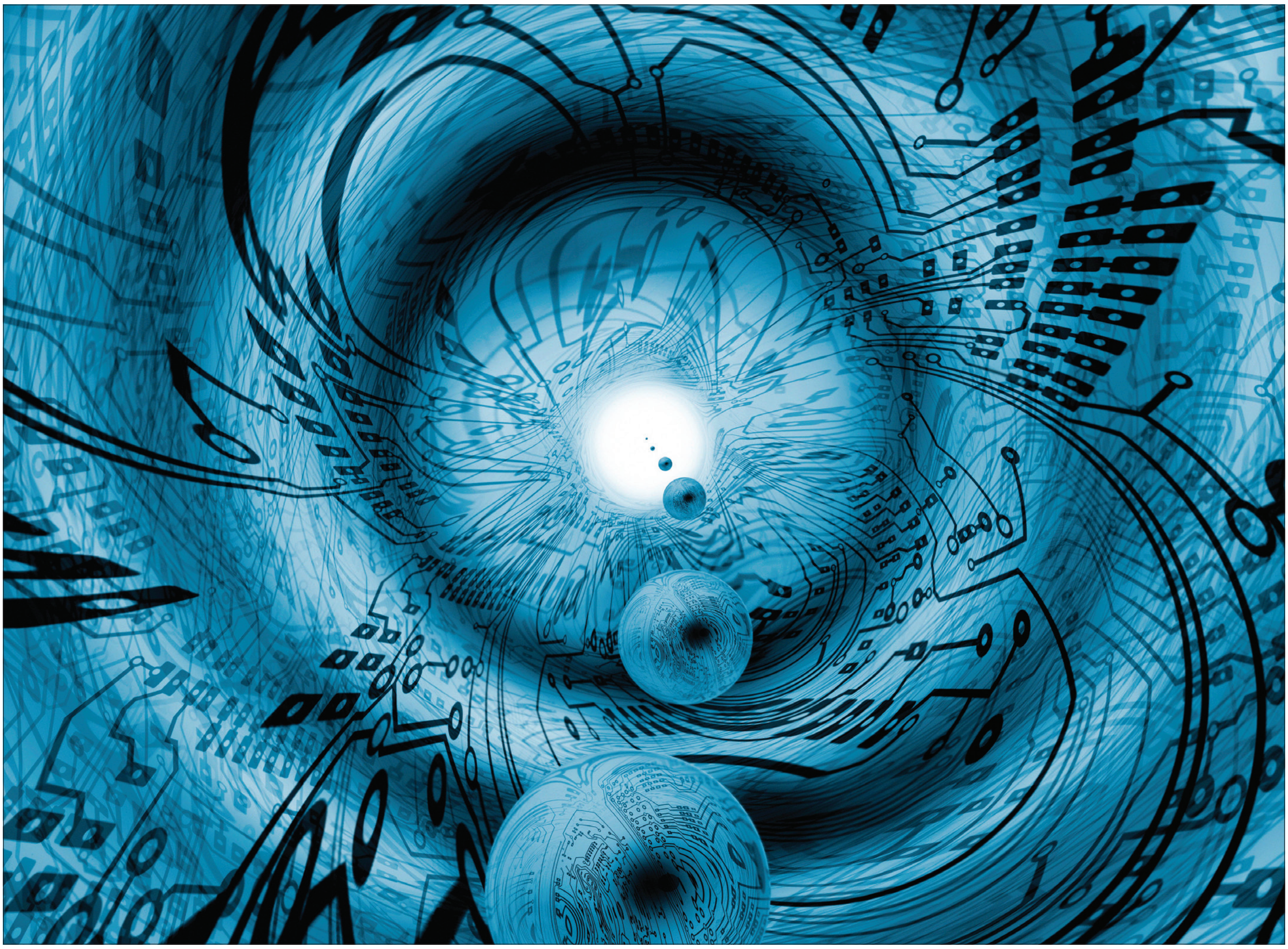
Other explanations for how quantum computers achieve their speed-up have been around for some time. But none is universally accepted, and most apply only to certain realizations of quantum computing. And perhaps because they lack the neatness and intuitive appeal of parallelism, they are given little air time in popular accounts. In fact, some researchers feel that the origin of quantum speed-up is still an entirely open question. According to Maarten van den Nest of the Max Planck Institute of Quantum Optics in Garching, Germany, "understanding the essential features of quantum physics accounting for this increased power is a fundamental but largely unsolved problem".

Only one universe

Deutsch's original formulation of quantum computing was located squarely within the many-worlds picture. He was convinced that a consideration of this behaviour "places an intolerable strain on all interpretations of quantum theory other than Everett's". That view was strongly challenged by physicist Andrew Steane, also at Oxford, who in 2000 posted a preprint on the *arXiv* server with the combative title "A quantum computer only needs one universe" (arXiv:quant-ph/0003084; later published as *Stud. Hist. Phil. Sci. B – Stud. Hist. Phil. Mod. Phys.* **34** 469). "Quantum superposition does not permit quantum computers to 'perform many computations simultaneously'," Steane argued. "Quantum computation is therefore not well described by interpretations of quantum mechanics that invoke the concept of vast numbers of parallel universes."

This argument has been sharpened by a theoretical demonstration that a quantum computation does not in general have access to all the possible states of the quantum variables (called the Hilbert space). Poulin and colleagues showed two years ago that, unless the timescales are truly astronomical, the volume of Hilbert space physically accessible to a quantum system is only a tiny fraction of the entire set.

None of the explanations for how quantum computers achieve speed-up is universally accepted



Mehau Kulyk/Science Photo Library

Other-worldly Do quantum computers achieve speed-up by performing calculations in many parallel universes?

While Deutsch didn't suggest that quantum parallelism requires access to *all* of Hilbert space – every possible quantum state of a wavefunction – Poulin's work shows that a quantum system is able to explore much less of it than might be imagined.

For Steane and many other quantum theorists, the real key to quantum speed-up was instead the phenomenon of entanglement – the ability to place two qubits in co-dependent states, in which a measurement performed on one of them instantly fixes the state of the other one. So, for example, if two entangled spins are anticorrelated, a measurement revealing one of them to be "up" compels the other to be "down".

Ever since entanglement was first highlighted by Albert Einstein and his co-workers in 1935, it has been seen as perhaps the central "weirdness" of quantum theory. The weird thing about it is that as soon as one of the qubits is measured, the second qubit assumes its correlated value *immediately*, faster even than information could be sent between the two qubits via a light signal. In Einstein's view, in which faster-than-light communication is forbidden by special relativity, this "non-local" influence showed that quantum theory was incomplete and must be underpinned by a deeper layer of reality. His idea was that each quantum entity is described by "hidden variables" that already have specific values before they are measured. But subsequent theory and experiment has shown that entanglement is indeed a genuinely non-local effect, and incompatible with hidden variables.

As Steane wrote in his paper, a quantum computation "uses entanglement to generate and manipulate a physical representation of the correlations between logical entities, without the need to completely represent the logical entities themselves". In other words, the computer uses the entangled relationships between qubits to manipulate them together rather than one by one – doing only what is necessary, without extraneous intermediate steps.

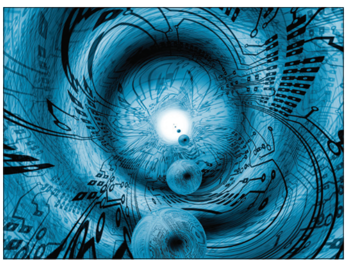
Therefore, says Fuchs, "Quantum computers can skip steps that would have to have been taken on a classical computer. Computational steps somehow 'count for more' on a quantum computer with respect to the necessary classical steps. That's a completely different idea than parallelism." Although Steane feels his argument remains valid today, he admits that "it is an issue of interpretation that cannot be settled by an experiment or a mathematical proof of some kind".

Meanwhile, Dan Browne of University College London suggests that quantum-computational speed-up is more about the *interference* that is possible between quantum states than it is about entanglement. Quantum interference is familiar from the double-slit experiment for quantum particles. It is subtly different from classical wave interference, and arises from correlations between the probabilities of particles' positions that make the joint probability differ from the sum of the individual ones. Entanglement is one facet of interference, because it too involves correlations, but it's possible to have interference without entanglement.

Casting doubt on entanglement

For a long time it was widely believed that entanglement could indeed account for the rapidity of quantum computation. That view was cast in doubt, however, by a paper written last year by Van den Nest (*Phys. Rev. Lett.* **110** 060504), in which he outlined a scheme by which quantum computation could be carried out using an amount of entanglement that, by many standard measures, could be arbitrarily small. "Even when the amount of entanglement present in the computation turns out to be very small," says Van den Nest, "the computation may still be just as powerful as a fully fledged quantum computer that uses lots of entanglement."

However, he adds, "Asking how large the entanglement must be to yield useful quantum computations is too vague a question to be meaningful, since there are many non-equivalent ways of quantifying it." It may even turn out, Van den Nest says, "that entanglement plays no decisive role for quantum speed-ups in the first place". Indeed, work done 15 years ago by Daniel Gottesman (now at the Perimeter Institute in Waterloo, Canada) that formed his PhD thesis at the California Institute of Technology, has long shown that it is certainly not a sufficient ingredient. "High amounts of entanglement do not guarantee speed-ups," Van den Nest says.



One oddity of quantum experiments is that their outcomes can depend on the order in which you make the measurements

Gottesman's thesis contained a theoretical technique he developed for studying a class of quantum logic gates that are commonly known as the Clifford group. With this technique, known as the "stabilizer formalism", many of the current quantum information-processing algorithms can be constructed from the Clifford group, in particular those designed to correct errors that develop in the computation. "Quantum circuits built using the Clifford group are able to make very entangled states, or states consisting of large superpositions, and can cause widespread interference between different branches of the wavefunction," Gottesman explains.

Despite that, the stabilizer formalism shows that there is an efficient classical algorithm that can simulate the gates in the Clifford group. In other words, at least for this class of quantum gates, neither entanglement nor interference guarantees any advantage over classical circuits. "Therefore, Clifford group gates cannot give you an exponential speed-up over classical computation," says Gottesman.

Out of context

Robert Raussendorf of the University of British Columbia in Vancouver, Canada, suggests that we are currently more clueless than ever about where the quantum speed-up comes from. If it's not from the vastness of Hilbert space (of which Deutsch's many-worlds view was one expression), not from entanglement and not interference, then what? "As far as I am aware, right now it's pretty silent in the theatre where this question is played out – that's because the main candidates are all dead," Raussendorf says.

But he says that recently a new candidate has appeared on the scene, called "contextuality" – a notion that goes back to work done in 1967 by Simon Kochen and Ernst Specker, which examined hidden-variable theories in a manner analogous to that published the previous year by the Northern Irish physicist John Bell. Bell's theorem helped to prove that the existence of hidden variables is not compatible with the non-local effects that are apparently manifested by entangled states. This led to the now widely accepted belief that hidden variables do not exist.

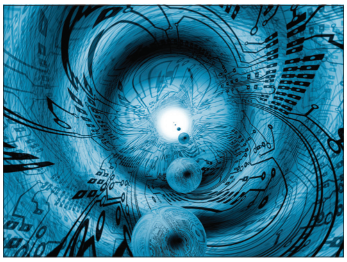
Kochen and Specker, meanwhile, considered the implications of hidden variables for the issue of experimental context. One oddity of quantum experiments is that their outcomes can depend on the order in which you make the measurements of the variables – for example, whether you measure a particle's position or momentum first. In other words, there's a dependence on the context of measurement. In contrast, outcomes in classical experiments are non-contextual: you get the same result regardless of the order of measurements. Kochen and Specker showed that any hidden-variables theory is incompatible with the contextuality that we see in quantum mechanics.

Recently, Joseph Emerson of the University of Waterloo in Canada and his colleagues have argued that, rather than the non-locality of entanglement, it could be the contextuality of quantum physics that supplies the hidden resource needed for at least some forms of quantum speed-up. "Contextuality is the first speed-up candidate about which I am excited," says Raussendorf.

The myth of quantum spice

Some feel that this debate about the "how" of quantum computation is a red herring. "Researchers attending most conferences in quantum computing never mention these issues, or only in discussions over beer," says Franco Nori of the University of Michigan in the US. Most people in the field, he says, are focused on immediate practical issues, such as "how to achieve longer coherence times for entangled qubits, how to achieve more operations within each coherence time, how to couple and uncouple qubits controllably, and so on".

But for others, the problems in explaining quantum speed-up bear on the whole matter of how quantum computers are sold – sometimes literally so. That was clear in the heated debate about whether "the world's first commercial quantum computer" advertised by the Canadian company D-Wave in 2012 was a true quantum computer at all, or just a fancy box of tricks



It is very difficult to describe how a quantum computer works using everyday language

that made token nods towards quantum effects.

"The question has, as far as I am aware, mostly been interpreted as seeking a resource, a kind of quintessential quantum spice," says Raussendorf. "The science-fiction version of this line of thought is that quantum spice can be bought by the ounce in future computer stores, and a hundred dollars' worth allows one to do such-and-such a computation." But that's not how it is.

"It is very difficult to describe how a quantum computer works using everyday language," Browne admits. Indeed, there may never be a one-size-fits-all answer, which is perhaps why any simple account of how a quantum computer does its job is doomed to be incomplete if not misleading. "I consider it unlikely that there is a single simple concept that is capable of capturing where quantum speed-up comes from," says Van den Nest. He says there are several non-equivalent ways of viewing classical computation as being a subset of quantum computation, and in each case the "ingredient" needed to release the power of the quantum approach might be different.

This difficulty is part of the reason why it is hard to find things that quantum computers *can* do – so far, only a small number of algorithms have been proposed that are well suited to particular problems, such as factorization and searching. "There isn't a straightforward way of making use of what quantum mechanics has to offer," says Browne. "Designing good quantum algorithms is a very difficult task," Van den Nest agrees. "I believe this task could be made lighter if we were to arrive at a systematic understanding of the possible ways to move from classical to quantum computing" – in other words, if we had a better grasp of which aspect of quantum physics the advantages ultimately stem from.

But Gottesman wonders if we can ever really grasp that. "My own feeling is that quantum speed-up is a property of quantum mechanics as a whole and is not something you can definitively pinpoint the source of," he says. "If you have 'enough' of quantum mechanics available, in some sense, then you have a speed-up, and if not, you don't."

At the same time, this ambiguity could be a virtue, since it leaves space for researchers to draw inspiration from diverse views. After all, even if a quantum computer does indeed require only one universe, Deutsch's vision of a multiplicity helped him to launch the field. Critics might dismiss the idea, but not what it produced. "For the most part these debates are metaphysical," says Poulin, "but they can nonetheless be useful because thinking about these questions can lead to new methods to process quantum information."