THE POWER OF DISCORD

BY ZEEYA MERALI

Physicists have always thought quantum computing is hard because quantum states are incredibly fragile. But could noise and messiness actually help things along?

M. WEINBERGER

In 2008, quantum physicist Andrew White found himself building a "ridiculous machine" in his lab at the University of Queensland in Brisbane, Australia.

White had spent years working on quantum computation, attempting to exploit subatomic physics to create a device with the potential to outperform its best macroscopic counterparts. And he had learned that it was a tough job: the required quantum systems are fragile, and demand immaculate laboratory conditions to survive long enough to be of any use. Now White was setting out to test an unorthodox quantum algorithm that seemed to turn that lesson on its head. In this scheme, messiness and disorder would be virtues, not vices — and perturbations in the quantum system would drive computation, not disrupt it.

"I honestly thought, there's no way this will work," says White. But when he turned his ridiculous machine on, it ran[1].

White's experiment is just one of several in recent years that have suggested a fresh approach to quantum computers. The conventional view is that such devices should get their computational power from quantum entanglement — a phenomenon through which particles can share information even when they are separated by arbitrarily large distances. But the latest experiments suggest that entanglement might not be needed after all. Algorithms could instead tap into a quantum resource called discord, which would be far cheaper and easier to maintain in the lab. More experiments will be required to convince the many sceptics that the approach will work. But if it pans out, the era of widespread quantum computation could arrive sooner than anyone expected.

UNPRECEDENTED SPEED

The idea of quantum computing dates from the 1980s, when Nobel-prizewinning physicist Richard Feynman realized that a machine using quantum rules could whizz through calculations that would take a standard computer billions of years. Classical computers have to encode their data in an either/or fashion: each bit of information takes a value of 0 or 1, and nothing else. But the quantum world is the realm of both/and. Particles can exist in 'superpositions' — occupying many locations at the same time, say, or simultaneously spinning clockwise and anticlockwise.

So, Feynman argued, computing in that realm could use quantum bits of information — qubits — that exist as superpositions of 0 and 1 simultaneously. A string of 10 such qubits could represent all 1,024 10-bit numbers simultaneously. And if all the qubits shared information through entanglement, they could race through myriad calculations in parallel — calculations that their classical counterparts would have to plod through sequentially (see 'Quantum computing').

NATURE.COM
For more on possible routes to quantum computing, visit:
go.nature.com/fdxdio

The notion that quantum computing can be done only through entanglement was cemented in 1994, when Peter Shor, a mathematician at the Massachusetts Institute of Technology in Cambridge, devised an entanglement-based algorithm[2] that could factorize large numbers at lightning speed — potentially requiring only seconds to break the encryption currently used to send secure online communications, instead of the years required by ordinary computers. In 1996, Lov Grover at Bell Labs in Murray Hill, New Jersey, proposed an entanglement-based algorithm[3] that could search rapidly through an unsorted database; a classical algorithm, by contrast, would have to laboriously search the items one by one.

But entanglement has been the bane of many a quantum experimenter's life, because the slightest interaction of the entangled particles with the outside world — even with a stray low-energy photon emitted by the warm walls of the laboratory — can destroy it. Experiments with entanglement demand ultra-low temperatures and careful handling. "Entanglement is hard to prepare, hard to maintain and hard to manipulate," says Xiaosong Ma, a physicist at the Institute for Quantum Optics and Quantum Information in Vienna. "It has been thoroughly investigated for years, with people expending much time and effort, but achieving little efficiency." The current entanglement record-holder intertwines just 14 qubits (ref. 4), yet a large-scale quantum computer would need several thousand. Any scheme that bypasses entanglement would be warmly welcomed, says Ma.

Clues that entanglement isn't essential after all began to trickle in about a decade ago, with the first examples of rudimentary quantum computation. In 2001, for instance, physicists at IBM's Almaden Research Center in San Jose and Stanford University, both in California, used a 7-qubit system to implement Shor's algorithm[5], factorizing the number 15 into 5 and 3. But controversy erupted over whether the experiments deserved to be called quantum computing, says Carlton Caves, a quantum physicist at the University of New Mexico (UNM) in Albuquerque.

The trouble was that the computations were done at room temperature, using liquid-based nuclear magnetic resonance (NMR) systems, in which information is encoded in atomic nuclei using an internal quantum property known as spin. Caves and his colleagues had already shown[6] that entanglement could not be sustained in these conditions. "The nuclear spins would just be jostled about too much for them to stay lined up neatly," says Caves. According to the orthodoxy, no entanglement meant no quantum computation.

The NMR community gradually accepted that they had no entanglement, says Jiangfeng Du, an NMR-computing specialist at the University of Science and Technology of China, in Hefei. Yet the computations were producing real results. In 2001, Du and his colleagues published the first experiment to explicitly perform a quantum search without exploiting entanglement[7].

"These experiments really called into question what gives quantum computing its power," says Animesh Datta, a physicist at the University of Oxford, UK. If researchers hope to build a large-scale quantum computer, they need to understand how the computation works.

ORDER OUT OF DISORDER

Datta, at the time a graduate student supervised by Caves at UNM, began to search for an alternative explanation. He came across discord, an obscure measure of quantum correlations first proposed[8] in 2000 by Wojciech Zurek, a quantum physicist at the Los Alamos National Laboratory in New Mexico. Discord quantifies how much a system can be disrupted when people observe it to gather information. Macroscopic systems are not affected by observation, and so have zero discord. But quantum systems are unavoidably affected because measurement forces them to settle on one of their many superposition values, so any possible quantum correlations, including entanglement, give a positive value for discord.

The concept was largely ignored for years because it seemed so abstract, says Vlatko Vedral, a quantum physicist at the University of Oxford, who in 2002 independently derived a mathematical expression for discord[9] in collaboration with Leah Henderson at the University of Bristol, UK. "But that changed when Datta connected discord to quantum computing."

"Discord could be like sunlight, which is plentiful but has to be harnessed in a certain way to be useful."

Datta had seized on an algorithm[10] proposed a few years earlier by NMR researchers Emanuel Knill, now at the US National Institute of Standards and Technology in Boulder, Colorado, and Raymond Laflamme, now at the University of Waterloo in Canada. Knill and Laflamme challenged the idea that quantum computing requires physicists to painstakingly prepare a set of pristine qubits in the lab.

In a typical optical experiment, the pure qubits might consist of horizontally polarized photons representing 1 and vertically polarized photons representing 0. Physicists can entangle a stream of such pure qubits by passing them through a processing gate such as a crystal that alters the polarization of the light, then read off the state of the qubits as they exit. In the real world, unfortunately, qubits rarely stay pure. They are far more likely to become messy, or 'mixed' — the equivalent of unpolarized photons. The conventional wisdom is that mixed qubits are useless for computation because they cannot be entangled, and any measurement of a mixed qubit will yield a random result, providing little or no useful information.

But Knill and Laflamme pondered what would happen if a mixed qubit was sent through an entangling gate with a pure qubit. The two could not become entangled but, the physicists argued, their interaction might be enough to carry out a quantum computation, with the result read from the pure qubit. If it worked, experimenters could get away with using just one tightly controlled qubit, and letting the others be battered by environmental noise and disorder. "It was not at all clear why that should work," says White. "It sounded as strange as saying they wanted to measure someone's speed by measuring the distance run with a perfectly metered ruler and measuring the time with a stopwatch that spits out a random answer."

Datta supplied an explanation[11]. With Caves and Anil Shaji, a physicist then at UNM, he calculated that the computation could be driven by the quantum correlation between the pure and mixed qubits — a correlation given mathematical expression by the discord.

It was a bold claim, says Kavan Modi, an expert on discord at the Centre for Quantum Technologies at the National University of Singapore. "Before that, if you announced that discord was as important for computation as entanglement — if not more so — at a conference, people would laugh out loud at you." But it seemed shocking only because, at the time, physicists had never really analysed computation in real-world scenarios that included mixed states. "It's true that you must have entanglement to compute with idealized pure qubits," says Modi. "But when you include mixed states, the calculations look very different."

Datta and his colleagues presented experimenters with a testable discord-based scheme. White doubted it would work, but jumped at the prospect of trying it out. "I'm a lazy experimenter, so I loved the thought of quantum computation without the hassle of entanglement," he laughs.

White was already practised at using polarized photons. He ran the computation as prescribed by Datta and, by averaging the values of the pure qubit over 2,000 runs, successfully summed the diagonal elements of a 2×2 matrix of numbers[1]. "It's a small matrix, but this was a proof-of-principle to show that you get the right answer in a reasonable number of runs, as predicted," says White.

The team confirmed that the qubits were not entangled at any point. Intriguingly, when the researchers tuned down the polarization

quality of the one pure qubit, making it almost mixed, the computation still worked. "Even when you have a system with just a tiny fraction of purity, that is vanishingly close to classical, it still has power," says White. "That just blew our minds." The computational power only disappeared when the amount of discord in the system reached zero. "It's counter-intuitive, but it seems that putting noise and disorder in your system gives you power," says White. "Plus, it's easier to achieve."

For Ma, White's results provided the "wow! moment" that made him take discord seriously. He was keen to test discord-based algorithms that used more than the two qubits used by White, and that could perform more glamorous tasks, but he had none to test. "Before I can carry out any experiments, I need the recipe of what to prepare from theoreticians," he explains, and those instructions were not forthcoming.

Although it is easier for experimenters to handle noisy real-world systems than pristine ones, it is a lot harder for theoretical physicists to analyse them mathematically. "We're talking about messy physical systems, and the equations are even messier," says Modi. For the past few years, theoretical physicists interested in discord have been trying to formulate prescriptions for new tests. Such experiments are essential if advocates of discord are to win over the wider physics community, says Antonio Acín, a quantum physicist at the Institute of Photonic Sciences in Barcelona, Spain. He notes that no one has yet proved that discord is essential to computation — just that it is there. Rather than being the engine behind computational power, it could just be along for the ride, he argues. Last year, Acín and his colleagues calculated that almost every quantum system contains discord[12]. "It's basically everywhere," he says. "That makes it difficult to explain why it causes power in specific situations and not others."

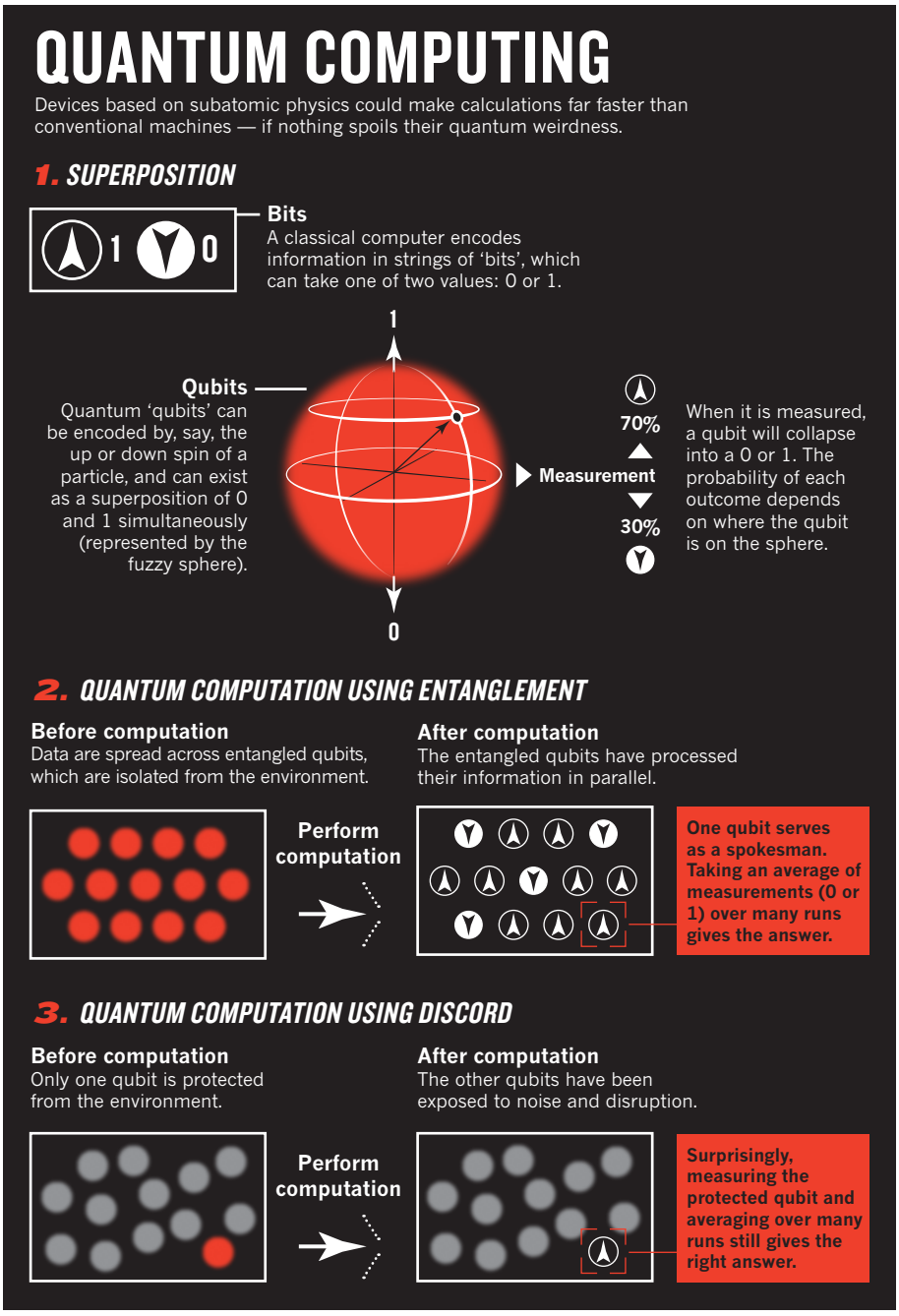
Modi shares the concern. "Discord could be like sunlight, which is plentiful but has to be harnessed in a certain way to be useful. We need to identify what that way is," he says.

Du and Ma are independently conducting experiments to address these points. Both are attempting to measure the amount of discord at each stage of a computation — Du using liquid NMR and electron-spin resonance systems, and Ma using photons. They hope to have results by the end of the year.

A finding that quantifies how and where discord acts would strengthen the case for its importance, says Acín. But if these tests find discord wanting, the mystery of how entanglement-free computation works will be reopened. "The search would have to begin for yet another quantum property," he adds.

Vedral notes that even if Du and Ma's latest experiments are a success, the real game-changer will be discord-based algorithms for factorization and search tasks, similar to the functions devised by Shor and Grover that originally ignited the field of quantum computing. "My gut feeling is that tasks such as these will ultimately need entanglement," says Vedral. "Though as yet there is no proof that they can't be done with discord alone."

Zurek says that discord can be thought of as a complement to entanglement, rather than as a usurper. "There is no longer a question that discord works," he declares. "The important thing now is to find out when discord without entanglement can be exploited most usefully, and when entanglement is essential." ■ SEE NEWS P.18



Zeeya Merali *is a freelance writer based in London.*

1. Lanyon, B. P., Barbieri, M., Almeida, M. P. & White, A. G. *Phys. Rev. Lett.* **101,** 200501 (2008).
2. Shor, P. in *Proc. 35th Annual Symp. Foundations Comp. Sci.* 124–134 (IEEE Press, 1994).
3. Grover, L. K. in *Proc. Twenty-Eighth Annual ACM Symp. Theory Comput.* 212–219 (ACM, 1996).
4. Monz, T. *et al. Phys. Rev. Lett.* **106,** 130506 (2011).
5. Vandersypen, L. M. K. *et al. Nature* **414,** 883–887 (2001).
6. Braunstein, S. L., Caves, C. M., Josza, R., Linden, N., Popescu, S. & Shack, R. *Phys. Rev. Lett.* **83,** 1054–1057 (1999).
7. Du, J. *et al. Phys. Rev. A* **64,** 042306 (2001).
8. Zurek, W. H. *Ann. der Physik (Leipzig)* **9,** 853–862 (2000).
9. Henderson, L. & Vedral, V. *J. Phys. A* **34,** 6899 (2002).
10. Knill, E. & LaFlamme, R. *Phys. Rev. Lett.* **81,** 5672–5675 (1998).
11. Datta, A., Shaji, A. & Caves, C. M. *Phys. Rev. Lett.* **100,** 050502 (2008).
12. Ferraro, A., Aolita, L., Cavalcanti, D., Cucchietti, F. M. & Acín, A. *Phys. Rev. A* **81,** 052318 (2010).