

Science and Technology: Bit by bit; Quantum computing;

The Economist. London: Apr 3, 2004. Vol. 371, Iss. 8369; pg. 90

(Copyright 2004 The Economist Newspaper Ltd. All rights reserved.)

Computing is driving the philosophical understanding of quantum theory

FOR evidence of the power of simplicity, you need look no further than a computer. Everything it does is based on the manipulation of binary digits, or bits--units of information that can be either 0 or 1. Using logical operations to combine those 0s and 1s allows computers to add, multiply and divide, and from there go on to achieve all the feats of the digital age. But at each step of the complex operations involved, each bit has a definite value.

The same cannot be said of many properties in quantum physics, such as the spin of an atomic nucleus (loosely speaking, which way it is pointing) or the position of an electron orbiting such a nucleus. At a small scale, such properties can have more than one value at once. In 1994, Peter Shor, a mathematician then at AT&T's Bell Laboratories in New Jersey, realised that a computer that used such quantum properties to represent information could factorise large numbers extremely quickly. This is an important problem, because much of modern cryptography is based on the difficulty of factorising large numbers--so being able to do so quickly would render many modern codes easily breakable. Then, in 1996, a colleague of Dr Shor's at Bell Labs, Lov Grover, showed that such a quantum computer would be able to search through an unsorted database much faster than an ordinary computer--another important application.

With these insights, quantum computing, which had first been thought of as a possibility in the early 1980s, became a hot topic of research. It was clear to many physicists that using "qubits"--which, unlike ordinary bits, can exist in a "superposition" of the values 0 and 1 simultaneously--might yield an exponential improvement in computing power. This is because a pair of qubits could be in four different states at once, three qubits in eight, and so forth. What Dr Shor and Dr Grover showed was that the improvement, if the technological hurdles could be overcome, would be not hypothetical, but real, and useful for important problems.

The technology necessary to manipulate qubits, in their various incarnations, is challenging. So far, nobody has managed to get a quantum computer to perform anything other than the most basic operations. But the field has been gathering pace, and was the topic of much discussion among the scientists gathered in Montreal for the annual March meeting of the American Physical Society, the largest physics conference in the world.

There are currently several different approaches to quantum computing, all of which rely on fundamentally different technologies, including ultra-cold ions that are cooled by lasers, pulses of laser light, nuclear-magnetic resonance and solid-state devices such as superconducting junctions or quantum dots (which are confined clouds of electrons). What all these technologies have in common is that they can be used to invoke and exploit the bizarre phenomenon of superposition.

Superposition is not simple. Though a qubit may, for a while, be in a state of superposition between 0 and 1, it must eventually choose between the two. And in even the best quantum computers, that choice, or "decoherence", happens in a fraction of a millisecond. Just how the choice is made, and how to prolong the preceding period of "coherence" that allows quantum computations to be made, constitute a long-

unexplained gap at the heart of modern physics. For nearly 80 years, since the inception of quantum theory in the 1920s, most physicists were content to gloss over the process. What is perhaps surprising is that the technological challenge of quantum computing is now a driving force behind efforts to understand the most abstract and philosophical underpinnings of quantum mechanics.

Echoes of the future

Until a qubit interacts with the macroscopic world, which follows the classical laws of physics, it behaves according to the laws of quantum mechanics, which are well understood, at least by physicists. However, the interaction with the classical world--decoherence--and hence exactly where the divide between the quantum and classical worlds lies, are not well understood. When decoherence is deliberately provoked, the process is known as measurement. Before a qubit is measured, for example, it could have a 90% chance of being 1, and a 10% chance of being 0. After the measurement, it takes on one of these two values. But the details of how it chooses between the two are something that, until the advent of quantum computing, most physicists chose to remain agnostic about. Some even quipped that the answer to that question was beyond the realm of physics. Measurement was thought to occur instantaneously, and its effects were added to the theory ad hoc.

But decoherence, though it occurs on a short time scale, happens gradually, unlike the instantaneous idea of measurement. It can thus be investigated. Wojciech Zurek, of America's Los Alamos National Laboratory in New Mexico, discussed his research group's efforts to investigate decoherence. They recently proved that the rate at which decoherence occurs can be measured by something called the Loschmidt echo. The Loschmidt echo, named after a 19th-century German physicist, is an observable experimental measure of the sensitivity of a quantum system to changes in the energy of the system. (The exact form it takes depends on what sort of physical system is being considered.) Dr Zurek expects that the link between decoherence and the Loschmidt echo should aid theoretical understanding of decoherence.

In a less abstract tack, several papers presented at the conference showed how decoherence could actually be combated. Although the naive expectation is that any interaction between the qubits of a quantum system and the outside world will provoke decoherence, it turns out that the right kind of external signals can in fact prolong the period of coherence.

Chikako Uchiyama of Yamanashi University, in Japan, discussed how, in the general case, the application of very short pulses, poetically known as bang-bang pulses, at regular intervals can serve not only to suppress decoherence, but also to maintain entanglement--the quantum coupling between several qubits which allows computations to get done. It turns out that, in the absence of such pulses, disentanglement happens even faster than decoherence, so there is even more of a need to suppress it. The specific form of the pulses, Dr Uchiyama says, depends on the quantum-computing technology in question--in nuclear magnetic resonance, the pulses could be of the magnetic field, while for quantum dots, it would be the electric field that is pulsed.

Kaveh Khodjasteh of the University of Toronto looked at a related question, focusing on decoherence rather than disentanglement. He showed how a quantum error-correcting code which introduced only one extra qubit for error correction would create a robust system for quantum computation which had tolerance for faults caused by spontaneous emission, another bizarre quantum effect. (Error-correcting codes are used to ensure the integrity of quantum calculations.) Many quantum error-correcting codes have been proposed before, but most require a large overhead of qubits--some need up to eight times as many qubits as those necessary for a computation, while Mr Khodjasteh's code needs only one extra qubit, no matter how many

are being used for the computation.

Several other speakers at the conference focused on detailed descriptions of how decoherence occurs in specific systems, such as superconducting junctions, or quantum dots. The promise of quantum computation, spurred on by the insights of Dr Shor and Dr Grover, is inciting physicists to probe, experimentally and theoretically, the junction between the quantum and the classical. They seem to be finding that the process of decoherence is more gradual, quantifiable and open to investigation than was previously suspected. Though a useful quantum computer is probably still many years away, the field of quantum computing is well on its way to solving its first problem.