THE ART OF QUANTUM COMPUTING

Can ‘spooky action at a distance’ be harnessed to build a new class of computers?

by Miya Knights

A RACE IS ON to build a different kind of computer that will exploit the peculiarities of the quantum world to accomplish number-crunching feats that are currently impossible. The principles by which a ‘quantum computer’ would work are quite different from those governing today’s ‘classical’ computers. Despite current processor and memory designs already having to take quantum-mechanical effects into account, quantum computing is something far stranger.

BIT AND QUBITS
Classical computers work by manipulating binary digits, or bits. Quantum computers work by manipulating qubits. A classical bit
can take the values 1 or 0. A qubit can be 1 or 0, or both at the same time. This ‘superposition’ of states is possible because of the ambiguity inherent in quantum mechanics, in which an observable property of an object can possess more than one value at once.

Classical computers encode their bits in discrete voltages, representing a binary 1 as a voltage above 2.4V, for example, and a binary 0 as a voltage below 0.8V. Quantum computers encode their qubits in quantum states, such as the spin (up or down) of an atom, or the polarisation (horizontal or vertical) of a photon of light. Unlike classical computing, in which small voltage errors do not matter, quantum computers are very sensitive to slight errors in their qubit values.

Once a quantum computer has more than one qubit, it’s possible to exploit another aspect of quantum mechanics called entanglement, which Albert Einstein described as “spooky action at a distance”. According to quantum mechanics, two entangled quantum states have to be described by reference to each other; even though the atoms, ions or fundamental particles that hold the states may be physically separated. This is counter-intuitive, but has become a well-accepted part of modern science. As Niels Bohr once said: “Anyone who is not shocked by quantum theory has not understood it.”

By exploiting entanglement, the state of one qubit can be linked to the state of another; so that setting one qubit to register the value 1 or 0 sets the other to the same value, despite the physical separation. This ability of qubits to become entangled enables quantum gates to be built.

To be useful, a quantum computer must also give an answer to a computation. Getting the qubits from their ambiguous, superposed state to an unambiguous state is done by a process called ‘quantum measurement’, which turns each ambiguous qubit state into a definite 1 or 0. The answer to the computation is given by the sequence of 1s and 0s that results from the process of quantum measurement.

**THE POWER OF UNCERTAINTY**

Why bother with all this strangeness? The answer is that computations performed by quantum computers could be incredibly powerful. A quantum computer could test every possible combination of input values for its qubits simultaneously. Each time a

Above, left to right:
Two barium ions in a trap (University of Washington); a surface electrode ion trap made at NIST; part of an optical bench; a two-layer alumina ion trap; part of Christopher Monroe’s ion trap experiment.
However, progress is being made. In 1995 Christopher Monroe and David Wineland, working at the US National Institute of Standards and Technology (NIST) built the first two-qubit logic gate using trapped beryllium ions. In 2005, a team led by Professor Rainer Blatt at the Institut für Experimentalphysik in Austria built a prototype of a quantum computer using several calcium ions. His group has entangled up to eight calcium ions, the most yet. However, a useful quantum computer would need hundreds or thousands of qubits.

Prototype quantum computers have already proved themselves against classical computers, although not in real-life situations. Professor Christopher Monroe, now at the University of Michigan, says: “An example from our laboratory has been a database search algorithm, where the number of queries before finding an element in the database is smaller (on average) than is possible with a classical computer. But the database only stored four elements, so that’s not useful. Furthermore, the clock speed on existing tiny quantum computers is very slow.”

Monroe’s approach to developing quantum computers has been to use ion traps. By carefully arranging electric and magnetic fields, an ion can be held at a point in space.

qubit is added to the quantum computer, its computational power doubles. If a quantum computer has 1000 qubits, it can test $2^{1000}$ combinations of inputs at once. There are about $2^{200}$ fundamental particles in the universe, so even if every one of them were part of a cosmic classical computer, it would fall far short of being able to store the information held in 1000 qubits.

Quantum computers could therefore be fundamentally more powerful than ordinary computers. The best computers of today cannot factorise numbers with more than 512 bits. In 1994, computer scientist Peter Shor, working at AT&T’s Bell Labs, showed that quantum computers would always finish the factorisation of a large number in fewer steps than a classical computer. Even if the classical computer has a much faster clock, for numbers with a large sequence of digits, the quantum computer will finish more quickly. Since the protection afforded us by modern cryptography is based on the difficulty of factorising large numbers, there’s plenty of interest in developing workable quantum computers.

BUILDING A QUANTUM COMPUTER
The trouble is, no one has yet managed to build one. Each time physicists add another qubit to a quantum computer, it makes the engineering task more difficult. Adding qubits makes the quantum computer much more vulnerable to decoherence, in which the state of the qubit degrades. Decoherence can be caused by interactions with the external world, and so far it has proved such a problem that experimenters find it difficult to maintain coherence in their systems for more than a few seconds.

Above, left to right: a multizone ion trap, which can confine ions in any of 10 zones; experiment detail; the laser system used in trapped barium-ion quantum computing experiments at the University of Washington
Trapping the ion isolates it, which makes it easier to avoid decoherence. The problem with ion traps as a basis for quantum computers, however, is that adding more than a few ion qubits poses tough engineering problems.

Monroe’s group has performed ion-trapping experiments on a semiconductor chip. He says: “We and other groups have only trapped a couple of ion qubits in these chip traps, and they have problems that still need to be worked out before they’re ready to do a quantum computation. But I’m confident there will be great progress on this front.”

Building an ion chip trap is a laborious process. “The trap was designed and fabricated by a student in the Michigan group, Dan Stick,” Monroe says. “He spent two years devising ways to lithographically carve and etch three-dimensional electrodes out of a chunk of gallium arsenide semiconductor material. More recently, other groups – particularly the groups of Dave Wineland at NIST and Richard Slusher at Lucent Technologies – have shown how to do this much more easily in a different geometry.”

David Wineland, group leader of ion storage at NIST, says: “As with Chris Monroe’s group, we want to fabricate a device in such a way that making many traps involves the same number of steps as making one. So we turned to lithography; micro-electromechanical systems and related techniques. We found a way to make traps where all the electrodes lie in a single plane. Such 2D geometries are easier to fabricate than 3D structures.”

But Monroe adds: “Problems have surfaced concerning the reduction of electrical noise emanating from the electrodes that trap these atoms. We have learned that this noise, while not well understood, can be suppressed by simply cooling the electrodes with liquid nitrogen. In the future, we may need to cool to [much lower] liquid helium temperatures to get rid of this noise almost completely.”

**SOLID STATE**

“The consensus is that ion traps are particularly promising, mainly due to their history of being the only system to have demonstrated all the necessary ingredients, albeit with only a few quantum bits,” says Monroe. “We know exactly what we need to do to scale up the ion trap, with no fundamental roadblocks in the way – but it will be technically difficult.”

Another approach would be to use superconducting circuits, which Monroe says have been improving greatly in the past five years. But he adds: “Many feel that some type of solid-state structure will ultimately rule due to their ‘easy’ scalability.”

Ion traps and solid-state approaches each have their advantages, according to Dr Boris Blinov, who leads the trapped-ion quantum-computing group at the University of Washington.

“Solid-state methods are very attractive from the point of view of fabrication,” he says...
says. “However, qubits in solid state are prone to decoherence, and the bulk of research in solid-state qubit systems has been on trying to understand and overcome that decoherence. Trapped ions and atoms, on the other hand, enjoy extremely low decoherence rates. Trapped ions are currently seen by many as the most likely way to succeed in the short term. A trapped-ion quantum computer will probably look nothing like the solid-state computers we use every day. But if it works, it works.”

Wineland cautions: “I’d say almost any prediction about what a quantum computer will look like will, with high probability, be wrong. Ion trappers are encouraged because we can at least see a straightforward path to making a large processor; but the technical problems are extremely challenging. It might be fair to say that ion traps are currently in the lead; however, a good analogy might be that we’re leading in a marathon race, but only one metre from the start line.”

**NICHE OR WORLD-CHANGING?**

Quantum computers, if they can be developed, may be uniquely useful for certain applications, such as cryptography, or processing every pixel in an image, but less useful for programming with general-purpose algorithms.

“It is very unlikely that within 10 years a quantum computer will be able to do general tasks better than a classical machine,” said Monroe. “However, I believe it is extremely likely that there will be niche applications for quantum computers that will outperform classical machines within 10 years. One example from physics is the simulation of simple quantum systems that cannot be modelled efficiently on classical computers.”

Blinov agrees: “I can foresee small-scale quantum computations and quantum simulations, and more advanced quantum communications systems in 10 years. It would be optimistic to expect a full-scale quantum computer running by then.”

We may have to wait a while for the first commercial quantum computers to become available. But looking further into the future, it is possible that this era – of early quantum computers – will be recognised as the time when an untapped aspect of nature was first harnessed.

David Deutsch, who laid a lot of the theoretical groundwork for quantum computing, writes in his book ‘The Fabric of Reality’: “The earliest inventions for harvesting nature were tools powered by human muscles [then] human beings managed to domesticate certain animals and plants. Another new type of technology began when human beings created pottery, bricks, wheels, metal artefacts and machines. To do this they had to think about, and understand, the natural laws governing the world, harnessing some of the materials, forces and energies of physics.

“In the 20th century, information was added to this list when the invention of computers allowed complex information processing to be performed outside human brains.

“Quantum computation, which is now in its early infancy, is a distinct further step in this progression. It will be the first technology that allows useful tasks to be performed in collaboration between parallel universes. A quantum computer would be capable of distributing components of a complex task among vast numbers of parallel universes, and then sharing the results.”

**PAINTING PHYSICS**

The University of Washington’s Boris Blinov says: “I narrowly escaped becoming an artist when I was 14, choosing physics instead. Naturally, art has remained an important part of my life, but until recently it followed its own path. That is until I realised that I can paint physics. I’d been thinking about creating paintings based on abstract physics concepts for quite a while. The entanglement was first on the list, but now I am planning to do more, such as ‘Hg EDM’ and ‘Wavefunction Collapse’, and maybe even ‘Fault-Tolerant Quantum Computing’.”

*Above and left: Blinov and ‘Cadmium Yellow Entangled’*