PHYSICS IN ACTION

Quantum computers get real

A quantum computer has successfully factorized a number for the first time

From **Jonathan Jones** at the Centre for Quantum Computation, Clarendon Laboratory, Oxford, UK

Quantum mechanics is an extremely successful theory, but also a troubling one. For many years progress was made by concentrating on the obvious applications, and not worrying too much about the counterintuitive world view that quantum mechanics implies. More recently, however, the development of quantum-information theory has reversed this approach. If we take seriously what quantum mechanics seems to be telling us about the world, we can use this "quantum weirdness" to do apparently impossible things (see *Physics World* March 1998 pp33–57).

Probably the most famous application of quantum mechanics is the quantum computer, which is capable of performing calculations that are impossible with any classical device. At first the questions that quantum computers could tackle were rather esoteric, but in 1994 Peter Shor of AT&T Laboratories showed how a quantum computer could factor large numbers, thus rendering most modern cryptographic systems potentially obsolete.

However, building a quantum computer has proved to be extremely difficult. In essence, the difficulty arises because the quantum bits (qubits) that make up the computer must be isolated from the outside world. Unwanted interactions between the qubits and the environment lead to decoherence, in which the mysterious but useful quantum properties are degraded to give classical behaviour.

To make matters worse, the computer must also have strong interactions with its environment so that it can be controlled. Reconciling these apparently contradictory requirements is one of the reasons why building a quantum computer is so difficult, and explains why little progress was made for many years despite heroic efforts.

NMR to the rescue

The situation changed in 1996 when David Cory and co-workers at the Massachusetts Institute of Technology (MIT) showed how nuclear magnetic resonance (NMR) – a technique best known for its applications in medical imaging and in chemistry – could be used to build small quantum computers. NMR systems are easily controlled by the magnetic component of electromagnetic fields and are only weakly affected by decoherence, and so progress was extremely rapid. Within two years, several two-qubit computers had been developed, and simple algorithms had been implemented. The race was on to build bigger and better NMR quantum computers, and to use them for more interesting tasks.

Compute this – Isaac Chuang loads the vial containing the seven-qubit quantum-computer molecules into the NMR apparatus.

1 This perfluorobutadienyl iron complex is used as a system of seven qubits. The large purple sphere represents a cyclopentadienyl (C_5H_5) ring. The seven nuclei used were the five naturally occurring fluorine-19 nuclei (green) and the two specifically labelled carbon-13 nuclei (blue). The remaining atoms simply form a structural framework and play no part in the computation.

The lead in this race has been held by several different research groups, but has now been decisively claimed by Isaac Chuang's group at Stanford University and IBM's Almaden Research Center in California. Chuang and co-workers have implemented the simplest example of Shor's quantum-factoring algorithm (L Vandersypen *Nature* 2001 **414** 883).

To factor really large numbers requires a quantum computer with several thousand qubits, but only a few dozen are needed to factorize relatively small numbers. Chuang's group first realized that the smallest sensible number to try, $N = 15$, could in fact be factored using only seven qubits.

Shor's algorithm does not factor N directly: rather it determines the period of the function $a^x \bmod N$, where a is a randomly chosen small number with no factors in common with N, and x is an integer. The value of $a^x \bmod N$ is the remainder that is left over when a^x divided by N. Once the period of this function is known, N can be rapidly factored using classical number theory. (For example, in the case where $N = 15$ and $a = 11$, we see that $11^0 \bmod 15 = 1$, $11^1 \bmod 15 = 11$, $11^2 \bmod 15 = 1$, $11^3 \bmod 15 = 11$, and so on, giving a period of 2.)

Quantum factoring works by using quantum parallelism to try out all possible values of x simultaneously, and then applying a so-called quantum Fourier transform to pick out the period. For the special case of $N = 15$, this period is always either 2 or 4, making it particularly easy to implement the algorithm and determine the period.

Architecture of a quantum computer

The remaining steps in the implementation are relatively conventional, but they represent a technological *tour de force*. The simplified algorithm was converted into a circuit of quantum logic gates, and standard techniques were used to simplify this circuit by deleting extraneous gates or replacing them with simplified versions. Chuang's group then designed and synthesized a suitable molecule containing seven spin-half nuclei that could be independently addressed (see figure 1).

The quantum logic circuit was then translated into the natural programming language for an NMR device, in which periods of free evolution under the spin system's inherent interactions are alternated with the application of controlled pulses of radiofrequency (RF) electromagnetic radiation.

The final program contained about 300 independently controlled RF pulses taken from a repertoire of 14 basic designs, far more than the dozen or so pulses found in implementations of simple algorithms and in conventional NMR experiments. Each of the 14 basic RF pulses was carefully shaped in amplitude and phase to give optimal control of the targeted spin. Despite this unprecedented complexity, the pulse sequence performed as expected to produce essentially unambiguous results. The deviations that were observed could be explained well using a simple model of decoherence based on experimental parameters.

The high quality of the experimental results suggests that this is not the limit of what can be achieved with NMR quantum computing, and we can expect to see even more impressive demonstrations within the next few years.

Quantum test-bed

There are, however, several fundamental difficulties with extending NMR systems beyond a few dozen qubits, and it seems extremely unlikely that any NMR quantum computer will ever outperform classical devices. This has triggered a second area of research: the use of NMR to develop basic techniques that will find applications in other quantum-information technologies. Cory and co-workers have made many contributions to this area, and have now used NMR to demonstrate a simple technique for reducing the effects of decoherence.

Simple models of decoherence assume that qubits lose their coherence independently, but in reality there will usually be correlations in the processes that affect neighbouring qubits. This leads to the idea of decoherence-free "subspaces", in which logical qubits encoded in states of two or more physical qubits are effectively immune to certain sorts of correlated decoherence. This phenomenon is familiar in NMR, where certain states of two-spin systems, known as zero-quantum coherences, are largely unaffected by magnetic fields. Now Cory and colleagues at MIT, Columbia University and Los Alamos National Laboratory have used this idea to implement a single logical qubit in a two-qubit decoherence-free subspace. They have shown that the logical qubit can be manipulated while remaining invulnerable to one kind of correlated decoherence (E Fortunato *et al.* 2002 *New J. Phys.* **4** 5).

Although NMR research is unlikely to lead directly to real fully fledged quantum computers, it remains a superb method for investigating the underlying principles. These recent results show why NMR is likely to remain the leading quantum-computing technology for the foreseeable future.

Ball lightning comes down to Earth

The strange properties of ball lightning can be explained in terms of metallic nanoparticles without introducing any extraordinary new physical processes

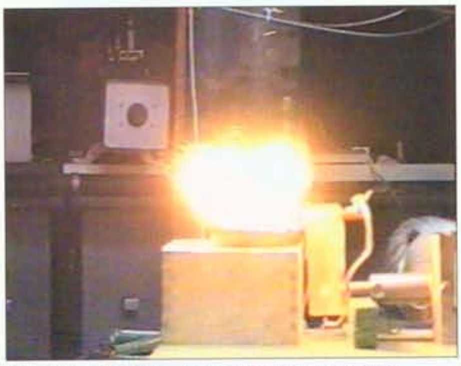
From **John Abrahamson** in the Department of Chemical and Process Engineering, University of Canterbury, Christchurch, New Zealand

Ball lightning – a slow-moving ball of light about 30 centimetres across that is occasionally seen at ground level during thunderstorms – has puzzled scientists for centuries. Benjamin Franklin, for instance, made several attempts to observe this mysterious phenomenon over 200 years ago. In one attempt he tried to make ball lightning from ordinary lightning – inspired by reports of a Russian contemporary who had been killed by such a ball after directing a lightning strike into his laboratory.

Franklin also tried to reproduce an experiment in which a small ball of lightning was reported to have been made with a high-voltage van de Graaff generator in England in 1757. Both times he failed.

Indeed, as long ago as 1854 François Arago, the French physicist well known for his work on light, stated that ball lightning was "one of the most inexplicable problems of physics today". Such has been the mystery of ball lightning that for many years large numbers of scientists doubted if it actually existed at all.

So what progress have we made in understanding ball lightning? It has been especially difficult to explain the longevity of the ball (which ranges from several seconds to several minutes), its stability and the way it releases energy. Many theories have been put forward over the centuries, from a localized gaseous plasma with strangely stable properties through to the suggestion by the Nobel-prize winner Peter Kapitza that ball lightning was caused by focused electromagnetic waves. Nuclear reactions and antimatter have also been proposed as explanations.



1 Flash in the pan – many attempts have been made to produce ball lightning in the laboratory. In this experiment Russian physicists used a pulsed erosion discharge to evaporate a target made of wax and resin. They were able to produce a glowing ball that lasted for almost half a second.

However, these theories have all been unsatisfactory in some respect. While they may have agreed with observations for one or even two properties (e.g. the power radiated or the stability), they either could not relate to, or were in conflict with, other observed properties (e.g. the long lifetime).

Of course, one theory was that ball lightning did not exist. Rather it was an optical illusion, perhaps the result of temporary blindness caused by normal lightning. This has become increasingly doubtful, however, as there are now more than 10 000 reports of ball lightning in the scientific literature. These sightings have been reported in all kinds of environments, and include simultaneous sightings of the same event by people in different locations. About 20 sightings have been made by practising scientists, some well known in scientific circles, and this number was recently doubled by sightings reported in a special issue of the *Philosophical Transactions of the Royal Society* on the theme of ball lightning that was edited by the author. Some of these reports contain graphic descriptions of rapid movements and changes in the internal structure of the ball.

How does natural ball lightning compare with man-made luminous bodies? Plasma discharges exist for only for a few milliseconds after they release their energy, and several decades of expensive fusion research have failed to increase this time. Similarly, hydrocarbon flames cannot last beyond a few milliseconds without a continuous feed of fuel. Some pulsed electrical discharges (called "erosion discharges") have produced small luminous volumes that last for about five seconds, with shorter times for larger volumes (figure 1). Recently nanoparticles coated with iron have been made to glow by oxidation for many seconds. Such "pyrophoric" materials, which are closely related to fireworks, become luminous when released into the air. The military are investigating these materials as potential decoys for heat-seeking missiles.

Two years ago James Dinniss and I proposed a model of ball lightning based on the oxidation of silicon nanoparticles in the atmosphere following a lightning strike (*Nature* 2000 **403** 519). We proposed that the silicon nanoparticles were formed as a result of the reaction of silicon oxides and carbon in the soil: at the high temperatures created by the lightning strike, the carbon in the soil chemically reduces the silicon oxides to the metallic form of silicon. Laboratory experiments confirmed that nanoparticles containing silicon could be produced in this way.

The oxidation process that is responsible for the production of light remains slow because of the formation of an oxide layer, which prevents oxygen molecules getting to the silicon metal underneath. Using accepted values for the oxidation rate of silicon – a process that has been intensively studied in the semiconductor industry – we found that