We could make you a quantum computer

By Roger Highfield

 Beam me up Scotty (Take your time)

RESEARCH on teleportation is creating ripples of excitement for the insights it provides into the ability of quantum computers, which could out-perform "classical" computers as thoroughly as conventional PCs have beaten the abacus.

The effort to build a quantum computer was stimulated by the realisation by Rolf Landauer, Richard Feynman, Paul Benioff, David Deutsch, Charles Bennett and others that computers must obey the laws of physics, and that the realm of microelectronics is fast shrinking to the atomic realm ruled by quantum mechanics.

Computers can operate at any size because information is fungible, that is, it maintains its utility no matter its physical form or size.

That means information can be carried by particles of light, electrons or the spinning nuclei of atoms, all of which are ruled by quantum lore. "The physical world is quantum mechanical, therefore information is essentially quantum mechanical," said Rolf Landauer of IBM, pioneer of the physics of computing.

He illustrated why quantum properties are important: a classical computer shuffles information in the form of binary numbers, those containing only the digits 1 and 0, which it remembers as the "on" and "off" positions of tiny switches, or "bits".

By contrast, the switches in a quantum computer can be
both "on" and "off" at the same time, a superposition. A so-called "qubit" could do two calculations at once, two qubits would do four and so on.

Quantum computers have another odd property. They can be run backwards and forwards. Their potential utility became clear when Peter Shor, a researcher at AT&T Laboratories, showed that a quantum computer could crack codes much faster than conventional machines. Then Lov Grover of Bell Laboratories, proved their utility in sorting through lists.

There is a catch with quantum computing. Anything, any disturbance - including that needed to read the result of a calculation - upsets a quantum computer. Its qubits are said to "decohere": to fall completely into one or another of their possible simultaneous states, to the exclusion of the others.

Copying quantum information also causes corruption and is precisely the reason why quantum encryption is so powerful, an idea demonstrated by IBM's Charles Bennett.

Although handy for encryption, the principle is a nuisance when it comes to building a quantum computer. None the less, progress has been made by storing information on charged particles held in a magnetic trap, particles of light, and "artificial atoms", tiny structures - quantum dots.

While at Los Alamos National Laboratory in New Mexico, Isaac Chuang, with Neil Gershenfeld of MIT, took another important step by demonstrating that quantum computing can be carried out with ordinary liquids in a beaker at room temperature.

Each molecule contains atoms, and the nuclei of atoms act like tiny bar magnets. These can point in only two directions, "up" and "down", because of a property called "spin". A single nucleus can therefore act as a qubit, its spin pointing perhaps up for "off" and down for "on". A given spin lasts a relatively long time and can be manipulated with nuclear magnetic resonance, a technique used by chemists for years.

Thus each molecule can act as a "little computer" and is capable of as many simultaneous calculations as there are ways of arranging its spin, according to Chuang, now with IBM Research, who has tackled some simple problems with chloroform.

Does this mean the first quantum computer is about to
appear on the market? His colleague, Charles Bennett, has a standard response: "Definitely in the next millennium."


Information about Telegraph Group Limited and Electronic Telegraph.

"Electronic Telegraph" and "The Daily Telegraph" are trademarks of Telegraph Group Limited. These marks may not be copied or used without permission. Information for webmasters linking to Electronic Telegraph.