INTERNATIONAL CENTRE OF EXCELLENCE FOR EDUCATION IN MATHEMATICS

Quantum computing

Raymond Vozzo, School of Mathematical Sciences, University of Adelaide

It was Richard Feynman who first proposed the idea of a computer running according to the laws of quantum mechanics. In 1982, Feynman noted that a quantum system of particles cannot be simulated efficiently by an ordinary (classical) computer, (that is, the system cannot be simulated without an exponential slowdown in efficiency). But a quantum computer could overcome this problem. Since then much work has been done exploring this possibility but it was not until 1994 when Peter Shor proposed an algorithm for a quantum computer to factorise integers into prime numbers in polynomial time that interest in the subject really peaked.

Quantum information is essentially based around two dimensional quantum systems such as spin-1/2 particles (e.g. electrons) or polarised light. Mathematically this means exploring the direct products (or tensor products) of Hilbert spaces.

In classical computing, information is transmitted as a sequence of zeroes and ones. These are called bits. Bits are either 0 or 1 but not both at the same time and they are very easy to work with. They can, for example, be copied. In quantum information theory, the quantum bit, or qubit, plays the role of the bit. Unlike a classical bit, a qubit can be 0 and 1 at the same time. It also has other strange properties that cause its behaviour to deviate significantly from that of the bit.

The Project which I worked on during the summer of 2004-2005 was to understand firstly the basic theory of quantum computing and secondly Shor's proof that a quantum computer could factorise integers into primes in polynomial time. I wrote up a report on what I learnt for my supervisor Professor Michael Murray.

Raymond received an ICE-EM Vacation Scholarship in January 2005.
See www.ice-em.org.au/students.html#scholarship.