Isaac Newton Institute for Mathematical Sciences

Quantum Information Science

16 August – 17 December 2004

Organisers: Dr CH Bennett (IBM Yorktown), Dr DP DiVincenzo (IBM Yorktown), Professor N Linden (Bristol), Professor S Popescu (Bristol)

Like other parts of mathematics, information and computation theory began as an abstraction from nature. The word calculation originally referred to the manipulation of pebbles, and a digit was a finger or toe. Today we live in the midst of an information revolution based on these abstractions, crystallized by Turing, Shannon, von Neumann, and others in the mid 20th century. But it has lately become evident that their notion of information was too narrow, and that quantum theory, developed a few years earlier by physicists, provides a more natural and general arena within which to formulate notions of information and computation. Aside from its conceptual elegance, the quantum approach explains and predicts a range of distinctive and potentially useful phenomena, including new kinds of cryptography and the possibility of dramatically speeding up some hard computations if a quantum computer can be built.

Traditionally, information carriers have been viewed as what a physicist would call classical objects, whose states are in principle reliably distinguishable, can be copied and observed without disturbance, and which combine in a straightforward Cartesian manner, so the state of n information carriers requires n times as many parameters to describe as the state of one. This scaling reflects the self-evident idea that to precisely describe a composite system, it is necessary and sufficient to precisely describe each of its parts.

These commonsense ideas do not fully describe the behavior of actual information carriers, which, like all other physical systems, obey quantum laws. By contrast to the classical realm, not all states of a quantum system are reliably distinguishable, the state of a quantum system cannot generally be copied nor observed without disturbing it, and the number of parameters required to describe the collective state of n quantum systems grows exponentially with n. Mathematically, a quantum state corresponds to a direction (ray) in a vector space (Hilbert space) of dimensionality equal to the system's maximum number of reliably distinguishable states. States are reliably distinguishable if and only if their rays are orthogonal. In the simplest case, called a quantum bit or *qubit,* and exemplified by a single polarized photon, the Hilbert space has two dimensions. For n qubits, the states occupy a space of 2^n dimensions; quantum computers derive their power from the ability to perform controlled rotations in this large space during intermediate stages of the computation. For any composite quantum system (e.g. two or more qubits), the vast majority of states are *entangled*—i.e. definite states of the whole that cannot be associated with a definite state of each part. The most famous entangled state, the so-called singlet state of two photons, may be described as a state of perfect oppositeness of polarization, even though neither photon has a definite polarization by itself. Entanglement is ubiquitous: when two initially unentangled systems interact, the usual result is that they become entangled.

If entanglement is so widespread, why did it remain undiscovered until the 20th century? The answer is like the parable of the fish asking other fishes where the ocean is: entanglement is nearly invisible because of entanglement. Most systems in nature, except microscopic ones like single photons, interact so strongly with their environment as to become entangled with it almost immediately. Under these conditions, the system's internal entanglement disappears, and the system appears to be in a probabilistic mixture of classical states, each describable by a number of parameters growing only linearly in the size of the system. Using privacy as a metaphor for entanglement, one might say that most macroscopic systems are like celebrities, whose private lives are so heavily eavesdropped on as to be destroyed and replaced by simplistic caricatures such as one reads on the Web.

If entanglement is so fragile, how can it be useful? Will it not always be destroyed too quickly for a would-be quantum computer to deliver any speedup? A surprising negative answer comes from the theory of quantum error control. In principle, though not yet in practice, it is possible to build a macroscopic quantum computer in which, though the computer interacts quite strongly with its environment, the quantum data within is so well shielded as to remain uneavesdropped on and therefore undisturbed. In retrospect, quantum error control is like classical error control but twice as hard. To make a classical computer work reliably, unwanted information (noise) must be prevented from leaking in to disturb the data, but it is OK for information about the data to leak out. To make a quantum computer work, information must be prevented from leaking either in or out, a task that while daunting appears possible.