IMPACT 11 …ON TECHNOLOGY: Quantum computing

Quantum mechanics lies at the heart of what might prove one day to be a revolution in the way in which calculations are carried out in a new generation of computers. *Quantum computing* is potentially capable of solving in seconds problems that conventional computing might be unable to solve in the lifetime of the universe. It might also undermine one of the most cherished aspects of commerce, war, and government: secrecy.

Conventional digital computing is based on the manipulation of strings of 0s and 1s, or *bits* ('binary digits'). Each bit might be realized in practice by the physical state of an object, such as a potential difference across a semiconductor junction or the state of polarization ('left-circularly polarized' or 'right-circularly polarized') of a photon. These physical states, denoted 0 and 1, are represented by the wavefunctions ψ_0 and ψ_1 and a conventional digital computer can be regarded as a device for carrying out operations on $|\psi_0|^2$ and $|\psi_1|^2$. A state in quantum mechanics, however, might be described by a linear combination of these wavefunctions, such as $c_0\psi_0 + c_1\psi_1$, with arbitrary (or, at least, specified) values of the two coefficients and a quantum computer carries out operations on the amplitudes, not their square moduli. A superposition of states like $c_0\psi_0 + c_1\psi_1$ is called a *qubit* (for 'quantum bit'). The central idea of quantum computing is starting to emerge: instead of carrying out operations on certain states of the system individually, computations can be carried out on several, and perhaps many, states simultaneously.

The core of conventional computing consists of various logical circuits such as AND and NOT gates. An AND gate gives an output of 1 only if both its inputs are 1, otherwise the output is 0; a NOT gate gives an output of 0 if the input is 1, and an output of 1 if the input is 0. Conventional computers string together these and other so-called 'Boolean operations' and realize them in terms of potential differences at semiconductor junctions. You might suspect that because a quantum computer carries out operations on the wavefunction rather than the probability itself that the logical circuits will in some sense be acting as the square-root of the usual Boolean operations. That is, instead of NOT acting on bits, the square-root of NOT (denoted √NOT) will be acting on qubits. Something like that turns out to be the case.

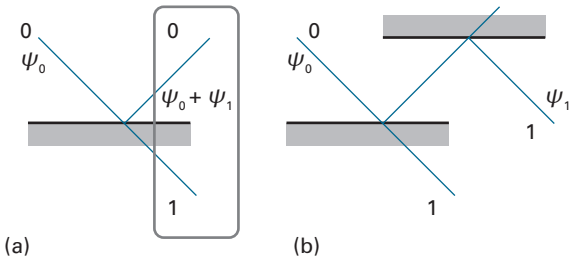

Figure 1 (a) A photon with wavefunction ψ_0 incident on a half-silvered mirror from above is either reflected (state 0) or transmitted (state 1); the final state is therefore the qubit represented by the linear combination $\psi_0 + \psi_1$. (b) The linear combination $\psi_0 + \psi_1$ recombines to result in a photon emerging below the second half-silvered mirror with the wavefunction ψ_1; that is, in the state 1.

As a simple illustration, consider √NOT in order to see that it has a real, physically realizable meaning. Consider the arrangement in Fig. 1, which shows a photon incident on a half-silvered mirror. If the photon is reflected it enters what can be regarded as the state 0 and if it is transmitted it enters what can be regarded as the state 1: the states are physically distinct as the photon occupies different parts of space. However, because no observation of the location of the photon has been made, there are equal probabilities that it is in either state and the qubit, which is now described by the linear combination $\psi_0 + \psi_1$, has been generated from the state 0 (the incident photon was above the mirror). If the photon were to be detected, half the time it would be found above the mirror (0) and half the time below (1).

Now suppose a second similar arrangement is joined to the first, as in Fig. 1b. According to quantum mechanics, the linear combination $\psi_0 + \psi_1$ recombines in the second arrangement to result in a photon that emerges below the second half-silvered mirror; that is, in the state 1. In other words, the combination of the two arrangements acts as a NOT gate. The implication is that each individual component contributes √NOT, because the succession √NOT√NOT is equivalent to NOT.

Quantum computation is obviously a highly subtle technology, but it is just starting to emerge into practical implementations. It builds conceptually on the postulates of quantum mechanics and will make use of the quantized real systems encountered in the text.