The No-Cloning Theorem

Last Update: 19th June 2008

The no-cloning theorem says that there is no unitary operator which will copy an arbitrary quantum state. It is understood that a particular Hilbert space has been specified, so by 'arbitrary' is meant any state of the Hilbert space in question. The difficulty does not arise, therefore, simply because the definition of 'arbitrary' is too broad. Also, the stipulation that the operator be unitary does not seem to be restrictive, in that all physical evolution other than the $\Re$-process is unitary.

In classical computing it is taken for granted that digital data can be copied with absolute fidelity. The no-cloning theorem says that the equivalent for a quantum computer is not possible. The no-cloning theorem is therefore a substantial restriction on the facilities available to the programmer of a quantum computer. However, the no-cloning theorem is even more important in quantum cryptography, where the impossibility of copying an unknown quantum state is essential to the security of the information.

Given the huge importance of the theorem, it is remarkable for two things: firstly that it is so very simple to prove, and secondly, that it was not discovered until as late as 1982, by Wootters & Zurek (1982) and by Dieks (1982). The proof follows.

We assume that we are provided with a vector, $|s\rangle$, from the relevant Hilbert space, in some standard initial state. This is the 'clay' from which our copy is to be moulded. We require to transform this initial state into a copy of any state, say $|\phi\rangle$ or $|\psi\rangle$, with which we are provided. Thus, the initial pair of states, $|s\rangle$ and $|\phi\rangle$, is to be transformed into two copies of $|\phi\rangle$ via a unitary transformation, U. We can write this as,

$$U|\phi\rangle \otimes |s\rangle = |\phi\rangle \otimes |\phi\rangle \qquad \text{(QM9.1)}$$

But this must work for an arbitrary state of the specified Hilbert space. So for some other state, $|\psi\rangle$, we must also have,

$$U|\psi\rangle \otimes |s\rangle = |\psi\rangle \otimes |\psi\rangle \qquad \text{(QM9.2)}$$

Taking the dot product of the LHSs of these two equations gives,

$$\langle\psi| \otimes \langle s|U^{+}U|\phi\rangle \otimes |s\rangle = \langle\psi|\varphi\rangle\langle s|s\rangle = \langle\psi|\varphi\rangle \qquad \text{(QM9.3)}$$

where we have made use of the unitary nature of U. Similarly, taking the dot product of the RHSs of the two equations gives,

$$\langle\psi| \otimes \langle\psi\|\phi\rangle \otimes |\phi\rangle = (\langle\psi|\phi\rangle)^{2} \qquad \text{(QM9.4)}$$

But (QM9.3) and (QM9.4) must be equal, so we conclude that $\langle\psi|\phi\rangle = (\langle\psi|\phi\rangle)^2$, and hence that $\langle\psi|\phi\rangle$ is 0 or 1. Hence, the unitary copier, U, can only copy a set of orthonormal states, at best. It cannot copy an arbitrary state.