Chapter 10

The No-Cloning Theorem

The basis of quantum cryptography

Last Update: 31/12/11

The no-cloning theorem says that there is no device which will produce an exact copy of an arbitrary quantum state without altering the original. Any practical device can be applied only to systems of a specific limited type, of course, so what exactly do we mean by "arbitrary"?. We can limit consideration to a particular class of systems. This is made precise by specifying a particular Hilbert space. The no-cloning theorem then states that there is no unitary operator which will copy an arbitrary quantum state of the Hilbert space in question. The difficulty in making a copy 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 is unitary (other than the collapse of the wavepacket).

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 even in principle. 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 and Zurek (1982) and by Dieks (1982). The proof is as follows.

Suppose 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 are required to transform this initial state into a copy of any arbitrary 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,

$$U\left(|\phi\rangle \otimes |s\rangle\right) = |\phi\rangle \otimes |\phi\rangle \qquad (1)$$

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

$$U\left(|\psi\rangle \otimes |s\rangle\right) = |\psi\rangle \otimes |\psi\rangle \qquad (2)$$

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

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

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

$$\langle\psi|\otimes\langle\psi\|\phi\rangle\otimes|\phi\rangle=\left(\langle\psi|\phi\rangle\right)^2 \qquad (4)$$

But (3) and (4) must be equal, so we conclude that $\langle\psi|\phi\rangle=\left(\langle\psi|\phi\rangle\right)^2$, 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: simple but profound.

References

Dieks, D. (1982), "Communication by EPR devices", Phys.Lett. A, **92**, 271-271, 1982.

Wootters, W.K., and Zurek, W.H. (1982), "A Single Quantum Cannot Be Cloned", Nature, **299**, 802-803, 1982.