No-Cloning Theorem[1]

There is no quantum-mechanical device which outputs a *perfect* copy of an *arbitrary* pure quantum state $|\psi\rangle$ while leaving the original intact. Such an apparatus would be described by a unitary operator $\hat{U}$ acting as

$$\hat{U}|\psi\rangle \otimes |0\rangle = |\psi\rangle \otimes |\psi\rangle \, ,$$

where $|0\rangle$ is a known 'blank' input state. However, due to the linearity of the operator $\hat{U}$ this equation is consistent only if the input states $|\psi\rangle$ are pairwise orthogonal. A contradiction arises if one requires that the device work correctly for non-orthogonal states as well. It is also impossible to duplicate (or *broadcast*) non-commuting *mixed* states.

Two proofs of the No-Cloning theorem [1,2] have been published in 1982, both triggered by a claim that the use of →entangled states would allow one to transmit information with superluminal speed. However, the proposed scheme cannot be implemented since it relies on the perfect cloning of quantum states. Seen the elementary nature of its proof, the No-Cloning theorem and its generalization to mixed states [3] have been discovered surprisingly late.

The No-Cloning theorem captures a fundamental aspect of the structure of quantum mechanics. Its limiting character plays an important role in the theory of →quantum information. For example, the theorem forbids to copy the information carried by a state $|\psi\rangle$ at the end of a →quantum computation. Thus, although desirable, no safety copies of the result embodied in the state $|\psi\rangle$ can be made, it cannot be distributed to other parties or multiplied for →quantum state reconstruction. At the same time, the security of →quantum cryptography relies on the No-Cloning theorem: if two parties establish a secret key by exchanging quantum states through a quantum channel, eavesdroppers are not able to reliably copy the states unknown to them. The theorem is consistent with →quantum teleportation since the unknown input state is destroyed irretrievably once the process has been completed.

Quantum cloning machines have been devised to produce one or more *approximate* copies of an unknown quantum state [4]. To achieve optimal cloning the devices take into account the number N of identically prepared (unknown) input states, the number M of desired output copies, whether pure or mixed states should be duplicated, and whether the cloner is required to work for arbitrary input states, i.e. *universally*, or for a limited set of input states only. Optimal cloning machines are conceptually linked to →quantum state reconstruction and the impossibility to use →quantum correlations for signaling.

[1] Stefan Weigert (University of York, UK) in *Compendium of Quantum Physics: Concepts, Experiments, History and Philosophy*, edited by F. Weinert, K. Hentschel, D. Greenberger, and B. Falkenburg (Springer, in print)

Literature

Primary
[1] W. K. Wootters and W. H. Zurek: A single quantum cannot be cloned. Nature 299, 802-803 (1982)
[2] D. Dieks: Communication by EPR devices. Phys. Lett. A 92, 271 (1982) 271-272
[3] H. Barnum, C. Caves, C. Fuchs, R. Jozsa, and B. Schumacher: Noncommuting Mixed States Cannot Be Broadcast. Phys. Rev. Lett. 76, 2818-2821 (1996)
[4] V. Bužek and M. Hillery: Quantum copying: beyond the no-cloning theorem. Phys. Rev. A 54, 1844-1852 (1996)

Secondary
[5] A. Peres: How the no-cloning theorem got its name. Fortschr. Phys. 51, 458-461 (2003)
[6] N. D. Mermin: *Quantum Computer Science.* (Cambridge University Press, Cambridge 2007, 39-40)
[7] V. Scarani, S. Iblisdir, N. Gisin, and A Acín: Quantum Cloning. Rev. Mod. Phys. 77, 1225-1256 (2005)