Bill Wootters is a professor of physics at Williams College in Williamstown, Massachusetts. **Wojciech Zurek** is a laboratory fellow in the theoretical division of Los Alamos National Laboratory in New Mexico.

INTERNATIONAL YEAR OF Quantum Science and Technology

The no-cloning theorem

William K. Wootters and Wojciech H. Zurek

People gather, copy, and distribute information all the time. But in the quantum world, the laws of physics impose a severe restriction on copying: It is impossible to make a perfect copy of an unknown state.

The principle of superposition is a cornerstone of quantum mechanics. It says that when two evolving states solve the Schrödinger equation, any linear combination of the two is also a solution. For that reason, waves from the two slits in the double-slit experiment simply add together to create the familiar interference pattern. As it happens, the superposition principle also prohibits the arbitrary copying of quantum states.

Linearity, unitarity, and cloning

To see why, imagine a machine that copies the state of a photon or an electron. When the original enters, two copies come out, each having the same state as the original. If such a machine were successful, it would convert the state $|\diamondsuit\rangle$ to $|\diamondsuit\diamondsuit\rangle$ and $|\heartsuit\rangle$ to $|\heartsuit\heartsuit\rangle$, where the fanciful symbols $|\diamondsuit\rangle$ and $|\heartsuit\rangle$ represent arbitrary states. The problem arises when we send a linear combination, $|s\rangle = a|\diamondsuit\rangle + b|\heartsuit\rangle$, through the hypothetical cloner. If $|\diamondsuit\rangle$ and $|\heartsuit\rangle$ are cloned correctly, then because of the linearity of quantum mechanics, the output for their superposition must be the superposition of the outputs, $|e\rangle = a|\diamondsuit\diamondsuit\rangle + b|\heartsuit\heartsuit\rangle$. But we want $|s\rangle|s\rangle = (a|\diamondsuit\rangle + b|\heartsuit\rangle)(a|\diamondsuit\rangle + b|\heartsuit\rangle)$, the original and a copy of $|s\rangle$. That is not the state $|e\rangle$ we get! The figure illustrates the general argument with a specific example.

The difficulty stems from the inherent nonlinearity of copying: When one asks for "two of the same," a square $|s\rangle|s\rangle$ of the original $|s\rangle$ is requested. The desire for a squared state is in conflict with the strict linearity of quantum theory. As a result, a single cloner cannot make a perfect copy of every quantum state. So what states can it clone?

Thus far, we have considered the linearity of quantum mechanics. But quantum evolutions preserve probability. The norm $\langle e|e\rangle$ of the state emerging from the copier must be the same as $\langle s|s\rangle$ of the original. The only difference between the two norms, expressed in terms of $|\diamondsuit\rangle$ and $|\heartsuit\rangle$, is in the cross term. Thus the equation $\langle\heartsuit|\diamondsuit\rangle = \langle\heartsuit|\diamondsuit\rangle^2$ must be satisfied by any two states that are perfectly copied. That simple equation has profound consequences: It shows that a quantum copier can work only when the possibilities for the original are orthogonal—that is, the scalar product $\langle\heartsuit|\diamondsuit\rangle$ vanishes.

One reaches the same conclusion after recognizing that quantum evolutions are unitary—they preserve the scalar product of any two states. So for states that can be copied, one again gets $\langle\heartsuit|\diamondsuit\rangle = \langle\heartsuit|\diamondsuit\rangle^2$. That is no surprise; unitarity follows from linearity and preservation of the norm.

Quantum evolutions are reversible, so one can imagine running the copier in reverse to delete the extra copy in states such as $|\diamondsuit\diamondsuit\rangle$ or $|\heartsuit\heartsuit\rangle$. Since uncopying also preserves the scalar product, it follows that perfect copying or deleting is possible only for sets of states that are orthogonal.

The optimistic assumption that a copier will work according to specs for the arbitrary states $|\diamondsuit\rangle$ and $|\heartsuit\rangle$ was naive. Perfect copying can be achieved only when the two states are orthogonal, and even then one can copy those two states (or perhaps a larger collection of mutually orthogonal states) only with a copier specifically built for that set of states. Thus, for example, one can design a copier for any orthogonal pair of polarization states of a photon, but a copier that works for $\{|\updownarrow\rangle, |\leftrightarrow\rangle\}$ will fail for $\{|\nearrow\rangle, |\nwarrow\rangle\}$, and vice versa.

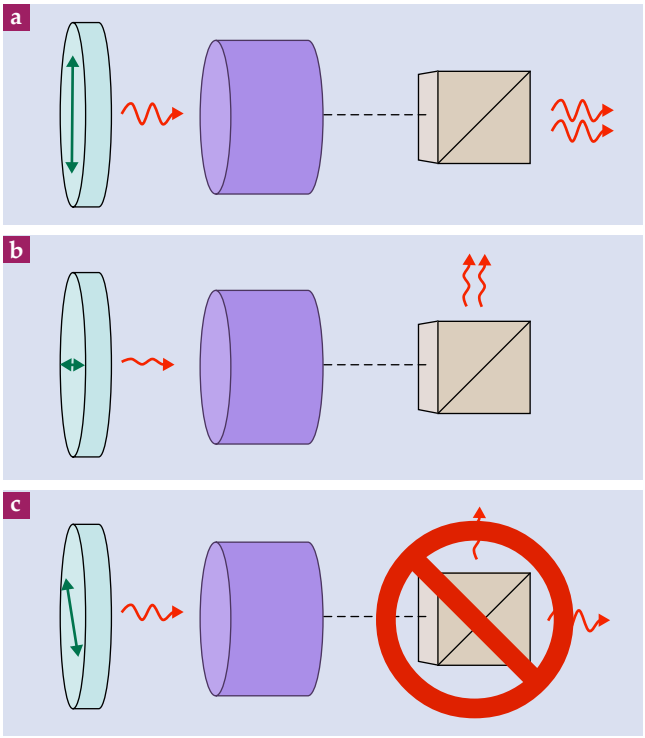
In sum, one cannot make a perfect copy of an unknown quantum state, since, without prior knowledge, it is impossible to select the right copier for the job. That formulation is one common way of stating the no-cloning theorem.

Quantum cryptography

The impossibility of cloning may seem at first an annoying restriction, but it can also be used to one's advantage—for instance, in a quantum key distribution scheme devised by Charles Bennett and Gilles Brassard in 1984. The idea is for the sender, Alice, to transmit many photons to the receiver, Bob, with the aim of ultimately creating a shared, secret, random string of zeros and ones. Such a random string can later be used as a key for encrypting and decrypting messages. For example, armed with a coded binary message and the key, Bob can decode the message by reversing the binary ciphers in all the positions where the key has a "1."

In the Bennett–Brassard scheme, each of Alice's photons is prepared at random in one of four possible polarization states: $|\updownarrow\rangle$, $|\leftrightarrow\rangle$, $|\nearrow\rangle$, or $|\nwarrow\rangle$. An eavesdropper, Eve, would like to get a copy of each photon for herself, but she also wants to pass an accurate copy on to Bob, or else her presence will be detected later when Alice and Bob check a random sample to see if Eve has disturbed their signals. Notice, though, that because of the no-cloning theorem, Eve cannot succeed in her task. As discussed earlier, if her cloning device can successfully copy the vertical and horizontal polarizations, it will fail to copy faithfully either of the two diagonal polarizations. Thus the prohibition against cloning helps preserve privacy.

Although Eve cannot perfectly copy the photons Alice sends to Bob, she can, in fact, do a pretty good job of approximately cloning Alice's transmission. Indeed, optimal approximate cloning is, in principle, one of the best methods Eve can use against quantum cryptography. Fortunately for Alice and Bob, it is possible to place strict theoretical limits on the fidelity



THERE IS NO PERFECT QUANTUM COPIER. Imagine a device that could clone an arbitrary quantum state. **(a)** A vertically polarized photon would yield two vertically polarized photons, both of which make the "vertical" choice at a polarizing beamsplitter. **(b)** A horizontally polarized photon would yield two horizontally polarized photons, both of which make the "horizontal" choice. **(c)** Because quantum mechanics is linear, a diagonal polarization—a superposition of vertical and horizontal—can produce only the measurement outcomes represented in panels a and b; it could not produce the outcome shown. But such an outcome would be possible if the diagonal polarization were cloned correctly. The linearity of quantum mechanics thus prohibits the cloning of arbitrary states.

of any such copying scheme. The study of approximate cloning is currently an active area of both theoretical and experimental research and is discussed in detail in the additional resources provided at the end of this Quick Study.

Causality, copying, and collapse

If cloning *were* possible, one could communicate instantaneously over a distance. Suppose Alice and Bob share two photons in the entangled polarization state, $|\zeta\rangle = (|{\leftrightarrow}{\updownarrow}\rangle - |{\updownarrow}{\leftrightarrow}\rangle)/\sqrt{2}$. The state $|\zeta\rangle$ can be expressed in any orthogonal basis with the paired polarization states always oriented along perpendicular axes; for example, $|\zeta\rangle = (|{\nearrow}{\nwarrow}\rangle - |{\nwarrow}{\nearrow}\rangle)/\sqrt{2}$. So to send information to Bob, Alice might measure her photon in one of two bases, {|↕⟩, |↔⟩} or {|↗⟩, |↖⟩}, her choice of basis encoding "0" or "1." Alice's measurement collapses $|\zeta\rangle$ into an eigenstate of the polarization she measures. If she chooses "0," Bob's photon will end up either |↔⟩ or |↕⟩, whereas "1" prepares it in one of the diagonal states.

In view of the collapse induced by Alice's measurement, Bob's photon, in a sense, gets the message. But Bob doesn't. He cannot simply ask his photon, "What's your state?" A quantum measurement is a multiple-choice test. It poses questions such as, "Are you |↕⟩ or |↔⟩?" Eigenstates of the measured observable are the only legal answers. If he wrongly measures in the basis complementary to that selected by Alice, Bob will randomize the state of his photon and, in effect, erase Alice's message. And to choose correctly, he needs to know the message. That's the proverbial catch-22.

Direct measurement fails, but what if Bob were able to clone his photon first? Copying |↕⟩ or |↗⟩ into $|{\updownarrow}{\updownarrow}{\updownarrow}\ldots\rangle$ or $|{\nearrow}{\nearrow}{\nearrow}\ldots\rangle$ would introduce valuable redundancy. Even a "wrong measurement" on some of the copies would not erase Alice's message, as other copies would remain for Bob to query with complementary questions. And the right question would lead to a consensus; all copies would give the same answer in the multiple-choice test. Many copies of his photon would thus allow Bob to find out the state and thereby read Alice's message. But as noted earlier, amplification requires a copier tailored to the right basis. So the superluminal communication-via-cloning scheme is foiled by the no-cloning theorem.

What if Bob uses a copier for, say, just the basis {|↕⟩, |↔⟩}? If Alice sends "0," the copier works. But for the diagonal input states $(|{\updownarrow}\rangle \pm |{\leftrightarrow}\rangle)/\sqrt{2}$, it produces $(|{\updownarrow}{\updownarrow}{\updownarrow}\ldots\rangle \pm |{\leftrightarrow}{\leftrightarrow}{\leftrightarrow}\ldots\rangle)/\sqrt{2}$. The two multiphoton states are equally probable and determined by the measurement at Alice's end. That state of affairs is indistinguishable from what happens when Alice sends "0" and Bob's properly working copier is equally likely to generate $|{\updownarrow}{\updownarrow}{\updownarrow}\ldots\rangle$ or $|{\leftrightarrow}{\leftrightarrow}{\leftrightarrow}\ldots\rangle$. The bottom line is that Bob's basis-specific copier is of no use for communication.

Nevertheless, the redundancy in states like $(|{\updownarrow}{\updownarrow}{\updownarrow}\ldots\rangle \pm |{\leftrightarrow}{\leftrightarrow}{\leftrightarrow}\ldots\rangle)/\sqrt{2}$ is of interest, as it sheds light on the origin of the "collapse" in quantum measurements. Each such state looks, to the casual observer, like many copies of just one preferred polarization. For example, $(|{\updownarrow}{\updownarrow}{\updownarrow}\ldots\rangle + |{\leftrightarrow}{\leftrightarrow}{\leftrightarrow}\ldots\rangle)/\sqrt{2}$ is a superposition of many copies of two polarizations. Yet if Bob detects any one of the photons in, say, the state |↔⟩, all the other photons will agree, just as when Alice sends a "0." The branch $|{\updownarrow}{\updownarrow}{\updownarrow}\ldots\rangle$ then becomes inaccessible, and all further data will point to the single remaining possibility. This consistency—this agreement among the photons—looks like a collapse. Such considerations suggest a strong affinity between a copier and a measuring apparatus. Both impose their choice of preferred states. Only states that respect the "symmetry breaking" can be found out or copied. Other states are converted into superpositions of redundant branches that collapse into a single option when probed by an initially ignorant observer.

Phrases like "Bob's photon gets the message" or "Bob erases the message" suggest that a definite underlying pure state of Bob's unobserved photon exists as soon as Alice makes her measurement. Such language is natural in that it provides a convenient picture that agrees with experimental results. However, the fact that an unknown quantum state cannot be discovered by a measurement or revealed by cloning suggests that not only is it unknown, but it does not even exist in the usual sense. Indeed, the nature of a quantum state is still the subject of lively debate, and the restriction on copying expressed by the no-cloning theorem is an important part of the discussion.

Further Reading

- V. Bužek, M. Hillery, "Quantum copying: Beyond the no-cloning theorem," *Phys. Rev. A* **54**, 1844 (1996).
- V. Scarani, S. Iblisdir, N. Gisin, A. Acín, "Quantum cloning," *Rev. Mod. Phys.* **77**, 1225 (2005).
- N. J. Cerf, J. Fiurášek, "Optical quantum cloning," in *Progress in Optics*, vol. 49, E. Wolf, ed., Elsevier (2006), p. 455.

PT