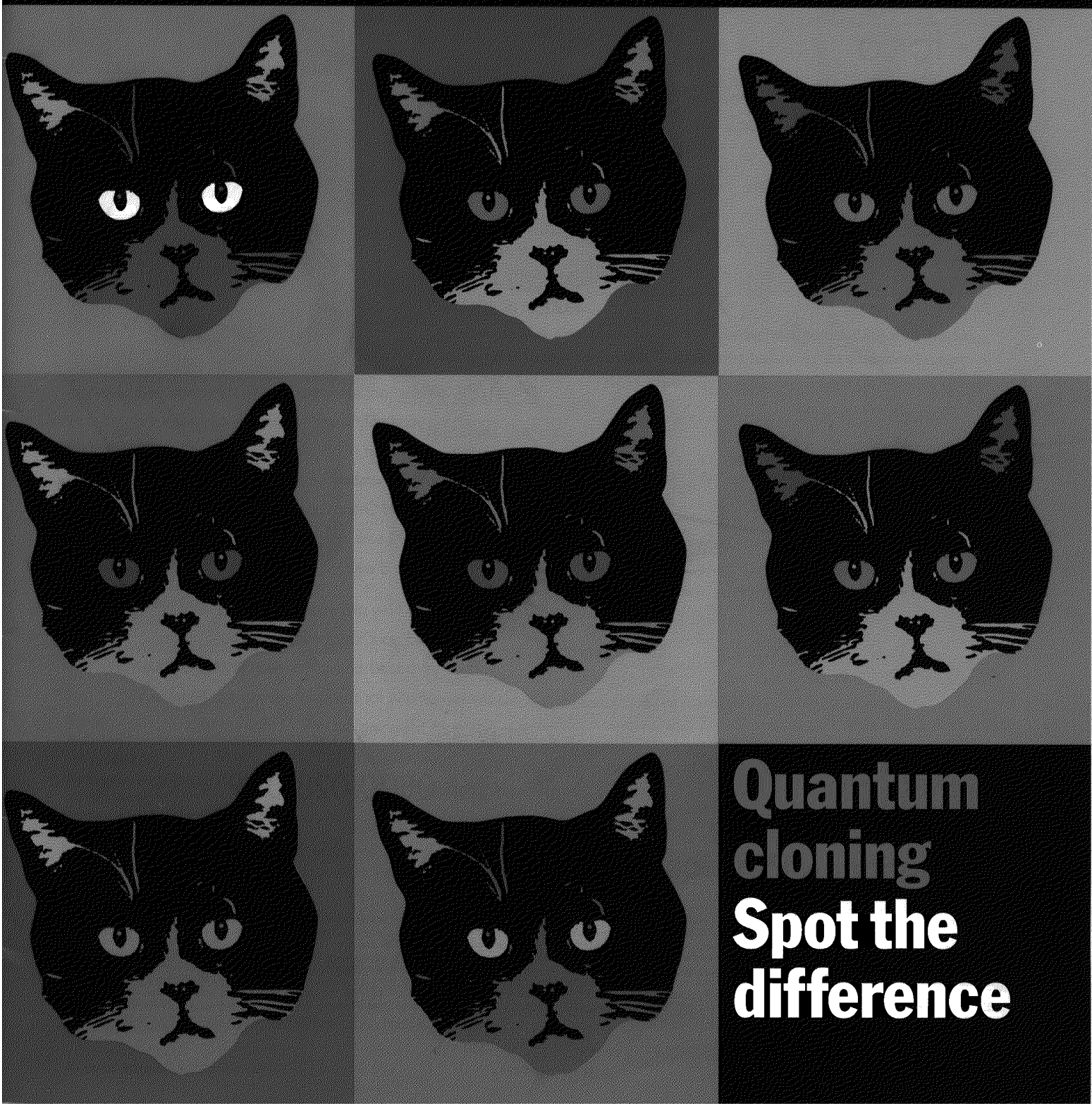
PhysicsWorld

NOVEMBER 2001 physicsweb.org VOLUME 14 NO 11

Setting the international standard Nobel secrets **To the rescue: lasers and art**



Quantum cloning

Spot the difference

It is impossible to make perfect copies or "clones" of unknown quantum states, but approximate copies could still have many uses in quantum computing

Quantum cloning

Vladimir Bužek and Mark Hillery

A COMPUTER is a physical device that consists of components that are all subject to the laws of physics. Since computers deal exclusively in information, there is a close connection between information and physical systems. But what happens if the components inside the computer become so small that they must be described by quantum mechanics rather than classical physics? The seemingly unstoppable decrease in the size of transistors and other components will force the computer industry to confront this question in the near future.

However, a small band of far-sighted physicists has been thinking about these problems for almost two decades. Starting with the work of Paul Benioff, Richard Feynman, David Deutsch and Charles Bennett in the mid-1980s, the field of "quantum information" has grown to become one of the most exciting areas of modern physics. These early pioneers realized that the representation of information by quantum systems, such as single electrons or photons, was an opportunity rather than a problem.

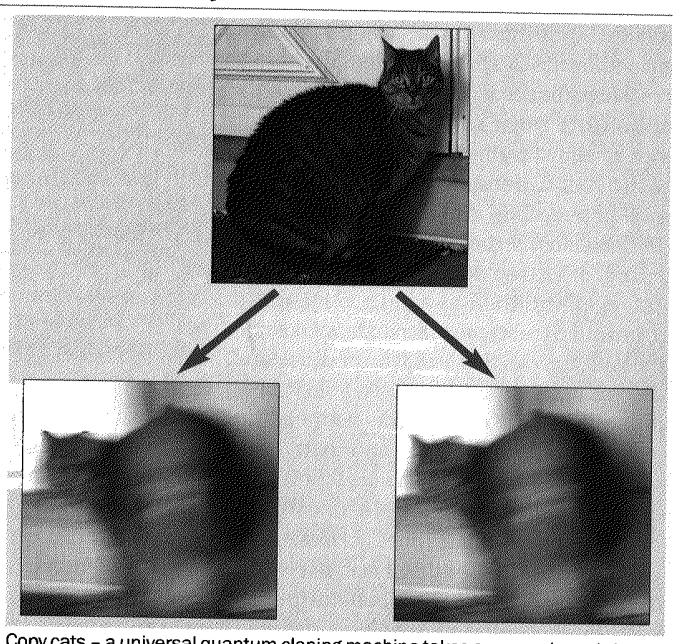
Classical information is represented by bits, which can have a value of either 0 or 1. Quantum information is represented by quantum bits or "qubits", which are two-state quantum systems. One basis state of the qubit, the $|0\rangle$ state, corresponds to 0, while the $|1\rangle$ state corresponds to 1.

For example, our qubit might be an electron. Electrons have internal angular momentum or "spin" and we can choose the "up" and "down" spin directions as our two basis states. And if our qubit is a photon, we can use the polarization states of the photon as basis states. If the photon is travelling in the z direction, then its polarization will lie in the x–y plane: we can choose vertical and horizontal polarization in this plane as our basis states.

A qubit, unlike a classical bit, can exist in two states at the same time. The electron spin could, for example, point in the horizontal direction, which can be represented as the sum of the "up" and "down" states. The fact that qubits can exist in these superposition states gives quantum information unusual properties.

One of these properties was discovered before the field of quantum information ever existed. In 1982 Nick Herbert, an independent scientist, proposed a method for sending messages faster than the speed of light – which would contradict special relativity. This proposal was, needless to say, greeted with considerable scepticism, and physicists immediately focused on finding the flaws in the argument.

Attention concentrated on a kind of amplifier that was essential to Herbert's proposal. This amplifier had the property that it could perfectly "clone" photons. In other words, if a single photon in an arbitrary polarization state was sent into the device, a large number of photons in exactly the same polarization state would appear at its output. Leonard Mandel of the University of Rochester, Roy Glauber of Harvard University and Peter Milonni of the Los Alamos National Laboratory showed, independently, that spontaneous emission added enough noise to the amplification process to prevent Herbert's proposal from working.



Copy cats – a universal quantum cloning machine takes any quantum state and produces two imperfect copies that are identical to each other. The maximum "fidelity" of a $1 \rightarrow 2$ quantum cloner is 5/6.

Around the same time a different and more general approach to the problem of cloning quantum states was taken by William Wootters and Wojciech Zurek, then at the University of Texas at Austin. Rather than confine themselves to amplifiers, Wootters and Zurek considered all possible quantum-mechanical transformations. They showed that any transformation that starts with a single particle in an arbitrary quantum state and finishes with two particles in that same state must violate the rules of quantum mechanics. Perfect cloning is therefore impossible, and this result is now known as the no-cloning theorem (see box on the left of page 26).

The burgeoning field of quantum cryptography relies on the fact that quantum information cannot be cloned, so an eavesdropper cannot copy an unknown quantum message. Quantum information can also be processed in ways that are not possible with classical information. This means that a computer that works with quantum information could, in

The no-cloning theorem

In order to clone an unknown state, $|\Psi\rangle$, we need a device known as a quantum cloner. This cloner is initially prepared in a state $|S\rangle$ that does not depend on $|\Psi\rangle$. We also need a particle that has been prepared in a known state, denoted as $|0\rangle$, onto which the information will be copied. In 1982 Wootters and Zurek presented a very simple proof that the perfect-cloning transformation for unknown quantum states is impossible. Here we present a different proof that is due to Horace Yuen of Northwestern University in Illinois.

Let us represent the cloning operation by an operator **U**. The cloning process for two initial states, $|\Psi\rangle$ and $|\tilde{\Psi}\rangle$, can be written as

$\mathbf{U}(|\Psi\rangle|0\rangle|S\rangle) = |\Psi\rangle|\Psi\rangle|S'\rangle$

$\mathbf{U}(|\tilde{\Psi}\rangle|0\rangle|S\rangle) = |\tilde{\Psi}\rangle|\tilde{\Psi}\rangle|S''\rangle$

where $|S'\rangle$ is the state of the quantum copier after $|\Psi\rangle$ has been cloned, and $|S''\rangle$ is the state after $|\tilde{\Psi}\rangle$ has been cloned. We can transform the second equation to read

$(\langle S|\langle 0|\langle\tilde{\Psi}|)\mathbf{U}^{-1} = \langle S''|\langle\tilde{\Psi}|\langle\tilde{\Psi}|$

If we now multiply the left-hand side of the first equation by $(\langle S|\langle 0|\langle\tilde{\Psi}|)\mathbf{U}^{-1}$, and the right-hand side by $\langle S''|\langle\tilde{\Psi}|\langle\tilde{\Psi}|$, we find

$\langle\tilde{\Psi}|\Psi\rangle = (\langle\tilde{\Psi}|\Psi\rangle)^2\langle S''|S'\rangle$

This equation can be satisfied if $\langle\tilde{\Psi}|\Psi\rangle = 0$, that is if $|\Psi\rangle$ and $|\tilde{\Psi}\rangle$ are orthogonal. If they are not, we can divide through by $\langle\tilde{\Psi}|\Psi\rangle$ to give

$1 = \langle\tilde{\Psi}|\Psi\rangle\langle S''|S'\rangle$

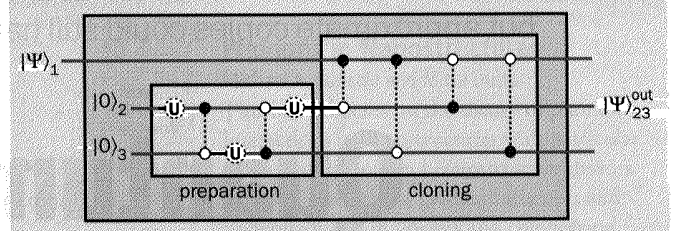
In quantum theory the magnitudes of both $\langle\tilde{\Psi}|\Psi\rangle$ and $\langle S''|S'\rangle$ must be, by definition, less than or equal to 1. Therefore, the only way this equation can be satisfied is if $|\langle\tilde{\Psi}|\Psi\rangle| = |\langle S''|S'\rangle| = 1$. For this to happen $|\Psi\rangle$ must be identical to $|\tilde{\Psi}\rangle$, and $|S'\rangle$ must be identical to $|S''\rangle$.

This means that perfect cloning is only possible if $|\Psi\rangle$ and $|\tilde{\Psi}\rangle$ are either orthogonal or identical. Therefore, the ideal cloning device for *arbitrary* quantum states does not exist.

It should be stressed that the no-cloning theorem does not forbid the copying of known states. Therefore, a cloning device designed specifically for a single, known input state can be constructed. However, if our cloning machine copies some states perfectly, there are other states that it will not copy properly and, consequently, there is no machine that will copy all input quantum states perfectly.

For more details see H Yuen 1986 Amplification of quantum states and noiseless photon amplifiers *Phys. Lett.* **113A** 405.

Logical network for quantum cloner



It is useful to represent the unitary transformations that occur in quantum information processing as a network of quantum logic gates. The qubits passing through the network are represented as horizontal lines, and the gates that act on the qubits are attached to the lines. Each gate takes its input qubit(s), performs an operation on it (them), and sends it (them) on. The qubits are imagined to move through the network from left to right, so the gates on the left act first. Networks allow us to build up more complicated operations from simpler ones.

The cloning network acts on three qubits. Qubit 1, $|\Psi_1\rangle$, is the one we wish to copy. Qubit 2, $|0_2\rangle$, will have the information from qubit 1 copied onto it, while qubit 3, $|0_3\rangle$, is essentially the "working space" that is needed for the cloning operation. The cloning network consists of two parts. The first part prepares qubits 2 and 3 in a particular quantum state, and the second part copies the information from qubit 1 onto qubit 2 (mostly) and qubit 3. Qubits 1 and 2 contain the final copies.

The preparation is performed by three single-qubit rotations (denoted as **U**) and two controlled-NOT gates. The copying is done by four controlled-NOT gates. A controlled-NOT gates has two inputs: the control qubit (denoted as ● in the figure), and the target qubit (denoted as ○). The state of the control qubit does not change as it passes through the gate. If the state of the control qubit is $|0\rangle$, the state of the target qubit does not change either. However, if the state of the control qubit is $|1\rangle$, a NOT operation is applied to the target qubit, so $|0\rangle$ becomes $|1\rangle$, and vice versa.

principle, perform some computational tasks much faster than a computer that works classically. Quantum computing is now a very active area of research (see *Physics World* March 1998 pp33–57).

Universal cloning machines

The no-cloning theorem caused people to ignore the whole subject of quantum cloning until the mid-1990s, when the present authors began to investigate the approximate copying of quantum information. The work of Wootters and Zurek had shown that perfect copying is not possible, but suppose one is interested in imperfect copies: how good can the copies be and how can they be produced?

In 1996 we proposed a "universal quantum cloning machine" that produces two imperfect copies of a single qubit. The word "universal" refers to the fact that the quality of the copies does not depend on the input state: in other words, the input photon, for example, could be polarized in *any* direction in the x–y plane (see box on the right above). Copy quality is measured by a quantity called the fidelity, which is the overlap between the quantum state of the copy, $|\Psi_{copy}\rangle$, and that of the ideal output state, $|\Psi_{ideal}\rangle$. The ideal output state is, of course, the same state as the input qubit. The fidelity is defined as the magnitude of the inner product of the states, $|\langle\Psi_{copy}|\Psi_{ideal}\rangle|$, and can range from zero, which means that there is no overlap whatsoever, to unity, which corresponds to a perfect copy.

Both of the copies produced by the "$1 \rightarrow 2$" universal quantum cloner are identical and have a fidelity of 5/6 for all input states. In the late 1990s Nicolas Gisin of Geneva University and Serge Massar, then at Tel-Aviv University, and, independently, Dagmar Bruss of Oxford University and co-workers, showed that 5/6 is the maximum mean fidelity that can be achieved by the cloning process.

The optimum fidelity of 5/6 can also derived by demanding that the cloner does not make faster-than-light communication possible, in effect reversing the reasoning of Herbert. This was first achieved by Gisin, who showed that if the fidelity was greater than 5/6, then the cloning procedure would make superluminal signalling possible.

Two groups – one led by Francesco De Martini at the University of Rome *La Sapienza*, the other led by Guang-Can Guo of the University of Science and Technology of China in Hefei – have achieved the maximal fidelity of 5/6 in experi-

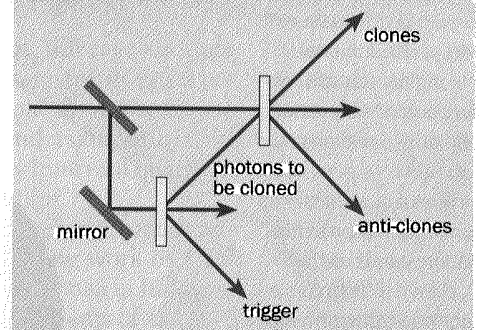
ments. Guo and co-workers used a linear approach, while the Rome group used optical parametric amplifiers, which are nonlinear (see Huang *et al.* and De Martini *et al.* in further reading).

Around the same time Christoph Simon, Gregor Weihs and Anton Zeilinger of the University of Vienna in Austria proposed a closely related nonlinear approach based on a device known as a parametric down-converter. In conventional down-conversion a crystal of a material with nonlinear optical properties, such as potassium dihydrogen phosphate (KDP), is used to convert a photon with a frequency of 2ω into two photons of frequency ω.

However, the KDP crystal can also be used as an amplifier – in this case a "pump" beam with a frequency of 2ω amplifies a weak beam at frequency ω as it passes through the crystal (see figure 1). There are three output beams: two at frequency ω, and a third at frequency 2ω. The photons in one of the beams of frequency ω are the clones, while those in the other beam are "anti-clones" (i.e. photons with polarizations that are orthogonal to that of the original photon). The third beam is just the output of the pump beam.

The performance of the universal quantum cloner should be compared to the procedure in which one simply takes the input qubit, measures it to estimate its quantum state and then produces two copies of the estimated quantum state (see box on page 28). Cloning via this "optimal measurement procedure" produces an arbitrary number of identical copies with a fidelity of 2/3.

1 Cloning via down-conversion



The Vienna group has proposed a universal cloning machine in which the pump pulse (blue line) is split at a beamsplitter. The main part of the pump is directed at a nonlinear crystal, while the smaller part of the pump pulse is reflected from a mirror and then enters a second crystal, where a photon pair is created (red lines). The lower of these photons serves as a trigger; the upper photon is the system to be cloned. This photon is directed at the first crystal, where it stimulates the emission of photons with the same polarization and direction. These are the clones. The photons travelling in the downward direction are polarized in the orthogonal direction and are therefore "anti-clones". The path lengths are adjusted in such a way that the photon to be cloned and the pump pulse reach the first crystal simultaneously.

More general cloning machines

It is possible to generalize universal quantum cloners by allowing more inputs and more outputs. Gisin and Massar showed how to construct a cloner that takes N identical qubits at the input and produces M copies at the output, where M is greater than N. In this case the fidelity is $(NM+N+M)/[M(N+2)]$. For example, if three copies are produced from one input the fidelity is 7/9, and if three copies are produced from two inputs, then the fidelity is 11/12. If we consider the $1 \rightarrow M$ cloner in the limit that M becomes infinite, the fidelity is 2/3, which is the same value obtained by the optimal measurement method.

Another way to generalize the universal quantum cloner is to consider cloning systems with more than two levels. For example, suppose that we want to clone a four-dimensional system, such as two qubits. In general, it will be possible to assign a quantum state to the entire two-qubit system, but not to the individual qubits. This means that it is best to treat the two qubits as a single unit rather than treating them separately. In particular, cloning each qubit individually is not the best method; it is necessary to design a device that clones the state of both qubits at once.

Universal cloners of this type have been explored by the present authors and by Reinhard Werner of the University of Braunschweig in Germany. The fidelity that can be achieved decreases as the dimension of the system increases. The maximum fidelity of 5/6 that is possible for a single two-level qubit becomes 4/5 for a two-qubit system, and 1/2 for an infinite level system. It is worth noting that a fidelity of 1/2 is no better than producing two copies by taking the original as one copy and a random state as the other. To date no experiments have been performed on higher-dimensional cloning.

State-dependent cloners

A different approach to cloning was pioneered by Lu-Ming Duan and Guo in Hefei. They considered a situation in which one is not interested in cloning all possible states, but only those in a particular set. It had been known since the work of Horace Yuen in 1986 (see box on the left of page 26) that if this set contains only mutually orthogonal states, then perfect cloning is possible every time we attempt to clone particles. Orthogonal states can be perfectly distinguished by measuring them. And once they have been distinguished, they can be reproduced. Cloning orthogonal states is therefore not much of a challenge. However, if the set contains non-orthogonal states, perfect deterministic cloning is not possible.

Duan and Guo presented a proposal for a cloner that produces perfect copies of non-orthogonal states, but only some of the time. When a qubit in one of the allowed states is the input, the machine indicates that it has successfully produced two perfect clones. However, if the machine indicates that it has failed to produce clones, the two qubits that emerge are discarded.

The important parameter for this type of machine is the probability of successfully producing copies, and this probability depends on the set of allowed input states. For example, if this set contains only two states, $|\Psi_1\rangle$ and $|\Psi_2\rangle$, the overlap or inner product of which, $|\langle\Psi_1|\Psi_2\rangle| = r$, is real and non-negative, then the probability of success is $1/(1+r)$. This probability is 1 when the states are orthogonal (i.e. when $|\langle\Psi_1|\Psi_2\rangle| = r = 0$), and decreases to 1/2 as the states become more and more parallel. For example, if the states we want to clone are the vertical-polarization state and a polarization state at an angle of 45° to the vertical, the probability of success is 0.56.

Continuous degrees of freedom, such as the position of a particle or the electric field of an electromagnetic wave, can also be used to encode quantum information. In 1998 Jeff Kimble and co-workers at Caltech managed to transfer or "teleport" a continuous degree of freedom in the laboratory. In teleportation, the quantum state is transferred to another particle or photon, but the original state is destroyed. Kimble and co-workers teleported the quantum state of one mode of the electromagnetic field onto another mode. The next challenge is to actually copy or clone continuous degrees of freedom, rather than simply teleporting them.

Optimal quantum measurement

One way to attempt to copy a quantum particle would be to measure it and then use the result of the measurement to prepare additional particles in a state that is close to the state of the original particle. We could, for example, measure the polarization of a photon: if the result is vertical, we would then prepare two vertically polarized photons as our clones, and similarly if the result is horizontal.

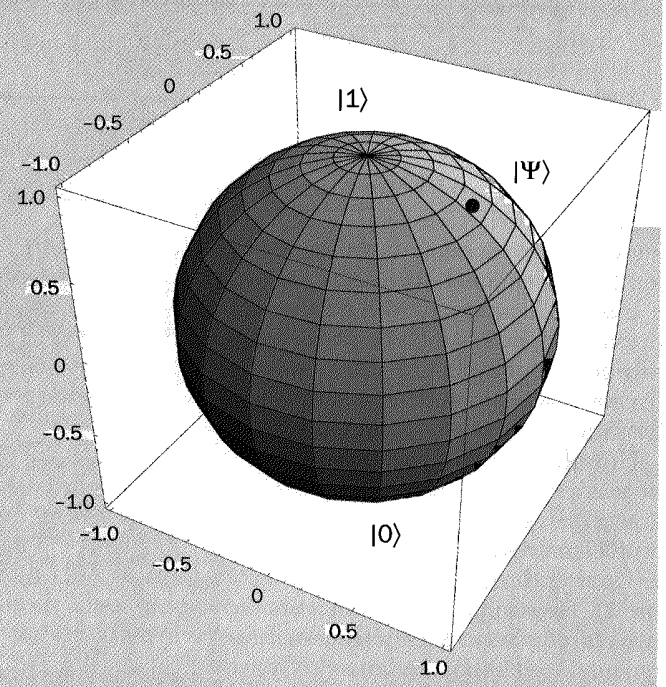
However, this is not a particularly good way to clone a quantum particle. The measurement converts the quantum information in the photon's polarization state into classical information; it tells us that the polarization was either vertical or horizontal, even if the photon was actually in a superposition of both polarizations. In transforming the quantum information contained in the original photon into classical information, and then using the classical information to create the clones, something is lost. A fully quantum device, such as the universal quantum cloner, will produce better copies.

To determine how much information we can gain about an unknown quantum state by this method, consider a qubit prepared in an unknown quantum state

$|\Psi\rangle = \cos(\theta/2)|0\rangle + \exp(i\phi)\sin(\theta/2)|1\rangle$

This state can be represented as a point on what is known as the Bloch sphere. This is a sphere of unit radius with its centre at the origin of a three-dimensional co-ordinate system. The south pole of the sphere corresponds to the state $|0\rangle$, and the north pole to the state $|1\rangle$. The angle θ is effectively the latitude of the point corresponding to $|\Psi\rangle$ on the sphere, and ϕ is the longitude. Trying to determine $|\Psi\rangle$ is essentially the same as trying to determine the longitude and latitude of the point that corresponds to this state on the Bloch sphere.

If we are measuring in the $\{|0\rangle, |1\rangle\}$ basis, the result of our measurement will be either $|0\rangle$ or $|1\rangle$, which only tells us that $|\Psi\rangle$ is more likely to be in either the northern or southern hemisphere. Although this is not much information to have when trying to figure out where $|\Psi\rangle$ really is, it does help. Indeed, we can actually estimate $|\Psi\rangle$ with a fidelity of 2/3. And if we have N qubits all prepared in the state $|\Psi\rangle$, instead of just one, the fidelity becomes $(N+1)/(N+2)$. The larger N is, therefore, the better we can estimate $|\Psi\rangle$ and produce a better copy.



We have already seen that a universal cloner for an infinite-dimensional system, of which a variable with continuous degrees of freedom is an example, is not a useful device. This suggests that we should consider cloners that are designed to copy a certain class of states. Nicolas Cerf of the Free University of Brussels has developed a family of such cloners, including one that can copy coherent states with a fidelity of 2/3. Coherent states are relatively simple to produce; over sufficiently short times the output of a laser is a coherent state. As the cloner requires only a linear, phase-insensitive amplifier, such as a laser amplifier, and various beamsplitters, it should be possible to build one in the laboratory in the not too distant future.

The universal NOT gate

Cloning represents one kind of transformation that can be carried out on an unknown qubit, but it is not the only one. Suppose that we are given a qubit in an unknown state and we want to transform it into the state that is orthogonal to this initial state. This process is known as "complementing" and is carried out by a device known as a "spin-flipper" or a "universal NOT gate".

A classical NOT gate changes 0 to 1, and vice versa. A quantum NOT gate transforms states in a particular basis into states that are orthogonal to them: e.g. $|0\rangle$ goes to $|1\rangle$, and vice versa. A universal NOT gate is more general because it is not restricted to any particular basis; a universal NOT gate transforms any input qubit state into the orthogonal state.

If the input to a universal NOT gate is $|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle$, where α and β are complex numbers, then the output will be $|\Psi_\perp\rangle = \beta^*|0\rangle - \alpha^*|1\rangle$. This is actually an anti-unitary transformation: if a unitary transformation is applied to $|\Psi\rangle$, then the output could be $|\Psi'\rangle = \beta|0\rangle - \alpha|1\rangle$. Since only unitary operations are allowed in quantum mechanics, the U-NOT transformation cannot be carried out perfectly. However, it can be carried out approximately, with a maximum fidelity of 2/3.

This level of fidelity can be achieved by measuring the original qubit (see box above), but there is also an unusual connection between a U-NOT gate and a cloning gate. Recall that the circuit for a quantum cloner involved three qubits, two of which ended up as clones. What happens to the third qubit? It turns out that its state at the output is the same as the state that would be produced by an optimal U-NOT gate. Therefore, the cloning circuit acts as both an optimal cloner and as an optimal U-NOT gate.

This phenomenon also occurs in the parametric down-converter cloner. As we noted, this device has two output beams, one of which contains the clones. The other beam contains photons in the ideal U-NOT output state.

Conclusion

The properties of classical and quantum information are not the same. While classical information can be perfectly cloned and complemented, quantum information cannot. As we have seen, both these operations can only be carried out ap-

proximately for qubits. However, these approximate processes are useful in understanding and designing applications of quantum information.

In quantum cryptography, for instance, the eavesdropper cannot make a perfect copy of the message transmitted between two parties, but he or she can make an approximate copy. It will therefore be important to understand the limits of quantum cloning to determine exactly how well quantum cryptography can protect secret information.

Quantum cloners can also be used to measure incompatible observables, as shown by the pioneering work of Giacomo Mauro D'Ariano at the University of Pavia in Italy and colleagues. For example, the x and y components of the spin of an electron cannot be measured simultaneously. However, if the electron is sent through a cloner, the x component can be measured on one of the clones, and the y component on the other. This type of measurement allows us to gain approximate information about both components, although it does not enable us to beat the uncertainty principle.

Cloning could also be useful in quantum computing. Ernesto Galvao and Lucien Hardy of Oxford University in the UK have shown that it can be more efficient to take a qubit, clone it, and perform operations on the clones in parallel, rather than performing the operations sequentially on the initial qubit.

Quantum cloning is one of the basic tools of quantum information processing. Its potential has only begun to be explored, and it is sure to find further applications as a building block of more complicated quantum procedures.

Further reading

D Bruss *et al.* 1998 Optimal universal and state-dependent quantum cloning *Phys. Rev.* **A57** 2368

V Bužek and M Hillery 1996 Quantum copying: beyond the nocloning theorem *Phys. Rev.* **A54** 1844

G M D'Ariano, C Macchiavello and M F Sacchi 2001 Joint measurements via quantum cloning *J. Opt.* **B3** 44

F De Martini, V Mussi and F Bovino 2000 Schrödinger cat states and optimum universal quantum cloning by entangled parametric amplification *Opt. Commun.* **179** 581

N Gisin and S Massar 1997 Optimal quantum cloning machines *Phys. Rev. Lett.* **79** 2153

N Herbert 1982 FLASH – a superluminal communicator based upon a new kind of quantum measurement *Found. Phys.* **12** 1171

Y-F Huang *et al.* 2001 Optical realization of universal quantum cloning *Phys. Rev.* **A64** 012315

M A Nielsen and I L Chuang 2000 *Quantum Computation and Quantum Information* (Cambridge University Press)

C Simon, G Weihs and A Zeilinger 2000 Optimal quantum cloning via stimulated emission *Phys. Rev. Lett.* **84** 2993

R F Werner 1998 Optimal cloning of pure states *Phys. Rev.* **A58** 1827

W K Wootters and W H Zurek 1982 A single quantum cannot be cloned *Nature* **299** 802

Vladimir Bužek is at the Research Center for Quantum Information of the Institute of Physics, Slovak Academy of Sciences, Dubravska cesta 9, 842 28, Bratislava, Slovakia. **Mark Hillery** is at the Department of Physics and Astronomy, Hunter College of the City University of New York, 695 Park Avenue, New York, NY 10021, US