PHYSICS

For Quantum Information, Two Wrongs Can Make a Right

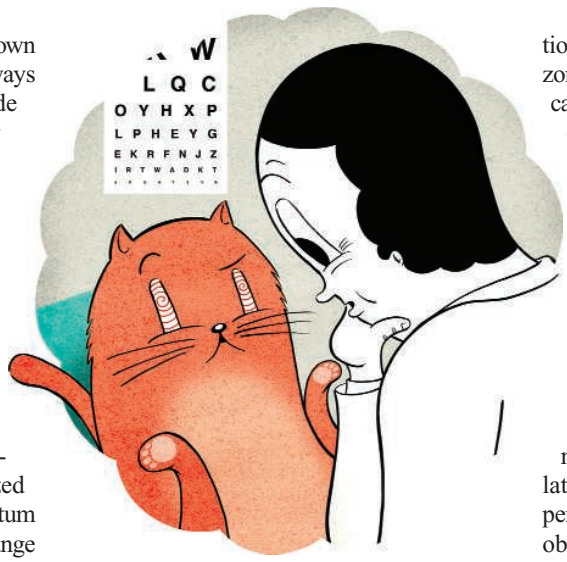
A channel too noisy to send quantum information can send secret messages, and, when combined with a similarly noisy channel, can reliably send quantum states.

Jonathan Oppenheim

Can you reliably send information down a telegraph wire that doesn't always transmit signals correctly? Claude Shannon put classical information theory on a firm footing when he showed that you can correct for transmission errors as long as there is some tiny correlation between what gets sent and what is received. What's more, Shannon quantified how much information could be reliably communicated. From its onset, classical information theory was intimately entwined with communication. The birth of quantum information theory began from an apparently different direction—cryptography—when it was realized that if you can reliably send someone quantum states, then you can use those states to exchange private messages that cannot be cracked by even the most powerful computer (*1*). This cannot be done classically without exchanging a physical key beforehand that is as long as the message you want to send. However, we are still wrestling with the corresponding question that was so central to classical information theory: How much quantum information can we reliably send down a noisy channel? On page 1812 of this issue, Smith and Yard (*2*) have discovered that we may be further from answering this question than we think, but that intriguing clues might come from the very place that initially sparked our interest in quantum information: cryptography.

Classically, a telegraph wire that is so noisy that no information can be reliably sent through it is useless. These are called zero-capacity channels. But what about the quantum case, such as trying to send information (which might be conveyed by the polarization of a single photon) through a fiber-optic cable that is so noisy it cannot be used to send any quantum state reliably?

Because our intuition tends to be classical, it was generally believed that a channel that cannot convey quantum information would also be useless. Yet a few years ago, the Horodecki brothers and I found that although these channels cannot be used to send quantum states, they can be used to send classical private messages. Indeed, one can classify all states that, if shared over some channel, are private (*3*). What's more, this privacy is verifiable, which means that practical cryptography can be performed over these zero-capacity fibers (*4*). The belief that quantum cryptography required being able to reliably send quantum states turned out to be wrong.



Quantum blindsight. "You appear to be blind in your left eye and blind in your right eye. Why you can see with both eyes is beyond me..."

Now, Smith and Yard, using results from (*5*), have shown a remarkable property of these zero-capacity quantum channels that can send private messages: They can be combined with another channel that also has zero capacity and can be used to convey quantum information. To find that two zero-capacity channels have finite capacity is a bit like finding out that 0 + 0 = 1 (see the illustration). Each channel individually is useless for sending quantum information, but when used together, they can be used to reliably send a quantum system in any state.

Despite how perplexing this result appears from a classical perspective, there is a fairly simple way to illustrate it. Let us start with the main idea behind cryptography. Consider two parties, Alice (A) and Bob (B), who can talk on the telephone and exchange quantum states—for example, polarized photons or qubits. These are represented by vectors in a linear superposition of two states, $|0\rangle$ and $|1\rangle$, so that the horizontal polarization of a photon is $|0\rangle$, the vertical polarization is $|1\rangle$, and linear superposition can give rotations to any angle. Imagine that Alice and Bob can succeed in sharing a maximally entangled quantum state whose wave function ψ_0 can be represented as $|\psi_0\rangle = (|00\rangle_{AB} + |11\rangle_{AB})/\sqrt{2}$. In this case, Alice and Bob have their qubits in a superposition of the $|00\rangle$ quantum state and $|11\rangle$ state, with Alice (A) possessing one of the qubits and Bob (B) in possession of the other.

This $|\psi_0\rangle$ state is pure, meaning that nothing in the external world can be correlated with it. As a result, Alice and Bob can perform measurements in this $|0\rangle$, $|1\rangle$ basis and obtain a string of correlated and secret bits (their measurement outcomes will be that they each obtain 0 or each obtain 1). This string can then be used to share a private message (*6*). Any channel that can be used to share $|\psi_0\rangle$ can be used to share any other state of their choosing and is said to have positive channel capacity. Likewise, if they can share the state $|\psi_1\rangle = (|00\rangle_{AB} - |11\rangle_{AB})/\sqrt{2}$, which is also maximally entangled but has negative phase, then they can also share a private message and send quantum states.

Now, consider a channel that half of the time results in $|\psi_0\rangle$ being shared and the other half of the time results in $|\psi_1\rangle$ being shared. One can show that this channel can only send classical messages—it cannot create entanglement unless $|\psi_0\rangle$ is shared more often than $|\psi_1\rangle$ (or vice versa). To make it more interesting, the channel also sends a flag—an additional state that labels which of the two maximally entangled states has been sent. If Alice and Bob can distinguish the two flags by performing measurements on them, then they will know which entangled state they share, and they can then send private messages or quantum states as before. They can even perform a correction to the state to convert $|\psi_1\rangle$ into $|\psi_0\rangle$.

As it turns out, there exist flags that can be completely distinguished when Bob holds the entire flag, yet are arbitrarily difficult to distinguish when Alice and Bob hold different parts of the flag and must perform measurements on them in separated labs (*7*) (even if they could communicate classically with a

Department of Applied Mathematics and Theoretical Physics, University of Cambridge, Cambridge CB3 0WA, UK. E-mail: jono@damtp.cam.ac.uk

telephone). In such cases, they will hardly ever know whether they share $|\psi_0\rangle$ or $|\psi_1\rangle$, and their ability to send quantum states to each other is arbitrarily close to zero (one can make it exactly zero by adding small errors). However, this state is still useful for sending private messages, because Alice and Bob can still just measure as they did before in the $|0\rangle$, $|1\rangle$ basis to obtain a secret key. An eavesdropper may know whether they share $|\psi_0\rangle$ or $|\psi_1\rangle$ but not whether they obtained $|00\rangle$ or $|11\rangle$ after measurement. Thus, channels that produce these flagged states can be used to share private messages, but they cannot be used to send quantum information—they have zero quantum capacity.

Now consider another zero-capacity channel, an erasure channel, that, with probability ½, lets the quantum state through perfectly, and the rest of the time it erases the state; the receiver Bob knows an error occurred because he will measure the error state $|e\rangle$. Such a channel turns out to be useless by itself for sending quantum information, but if Alice first uses the previous zero-capacity private channel and then puts her half of the flag down the erasure channel, then half of the time Bob can combine Alice's part of the flag that he receives from this channel with the other half that he received from the zero-capacity private channel. He can then distinguish the flag. So, half of the time, he will know whether they share $|\psi_0\rangle$ or $|\psi_1\rangle$, and he can perform a correction so that they both share the $|\psi_0\rangle$ state. This means that ¾ of the time, Alice and Bob share $|\psi_0\rangle$ instead of $|\psi_1\rangle$. This is significantly greater than half the time, and enough to create entanglement and get a positive channel capacity.

By using both the zero-capacity private channel and the zero-capacity erasure channel together, Alice and Bob can send any quantum state reliably. In the case above, the inputs that Alice sends through the two channels are not even entangled, but only classically correlated. What's more, this procedure can be easily generalized. All cryptographic protocols must distill the private states of (*3*), and the above protocol can be adapted to work for all of them.

This result raises many questions, not the least of which is what this work may say about the yet unknown formula for quantum capacity. We do not know the optimal procedure for activating a private channel, whether every channel that has zero capacity (but is not classical) can have positive capacity when combined with another zero-capacity channel, or even whether every such zero-capacity channel is also a private channel. Whatever the answers, it is clear that the structure of quantum information theory is much richer than most of us ever anticipated.

References

1. C. Bennett, G. Brassard, in *Proceedings of the IEEE Conference on Computers, Systems, and Signal Processing* (IEEE, New York, 1984), pp. 175–179.
2. G. Smith, J. Yard, *Science* **321**, 1812 (2008); published online 21 August 2008 (10.1126/science.1162242).
3. K. Horodecki, M. Horodecki, P. Horodecki, J. Oppenheim, *Phys. Rev. Lett.* **94**, 160502 (2005).
4. K. Horodecki *et al.*, *Phys. Rev. Lett.* **100**, 110502 (2008).
5. G. Smith, J. A. Smolin, A. Winter, *IEEE Trans. Info. Theory* **54**, 4208 (2008).
6. A. K. Ekert, *Phys. Rev. Lett.* **67**, 661 (1991).
7. T. Eggeling, R. Werner, *Phys. Rev. Lett.* **89**, 097905 (2002).

10.1126/science.1164543

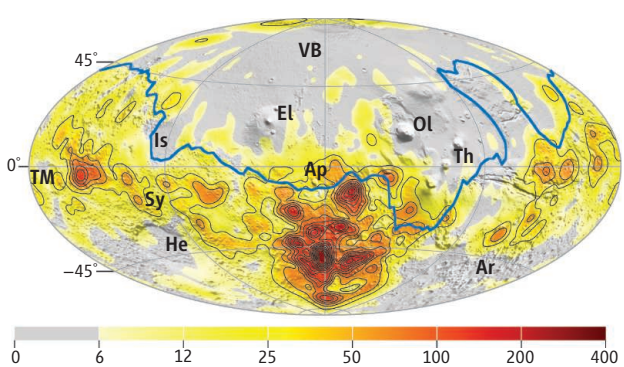
PLANETARY SCIENCE

The Past Martian Dynamo

Numerical dynamo modeling studies may explain the observation that strong magnetic fields are only found in Mars' southern hemisphere.

Benoit Langlais[1] and Hagay Amit[2]

Measurements by Mars Global Surveyor (MGS) have revealed intense magnetic anomalies mostly located south of the crustal dichotomy, the topographic boundary separating the southern cratered highlands and the northern smooth lowlands. Assuming the dynamo of Mars was similar to that of Earth—dipolar, axial, and centered, the magnetic dichotomy implies that the magnetization of the northern hemisphere was erased at some time, and thus that the dynamo stopped operating very early in its history (*1*). On page 1822 of this issue, Stanley *et al.* propose an alternative model in which the dynamo is driven by a hemisphere-scale heat flux pattern at the core-mantle boundary (CMB) (*2*). The proposed thermal constraint is compatible with martian mantle convection models (*3*) and can also explain the crustal dichotomy (*4*). In this new scenario, the much weaker crustal magnetization in the northern hemisphere is not a result of a post-dynamo process such as a giant impact (*5*), but rather, it was never magnetized in the first place.



A magnetic dichotomy. Predicted magnetic field intensity (nT) at 300 km altitude (from (*17*), iso-contours are 25 nT), on top of a shaded relief of the martian surface. Northern hemisphere magnetic field anomalies are of the same order of magnitude as terrestrial magnetic field anomalies at similar altitude, and approximately one-tenth of what is measured in the southern hemisphere. The large impact craters, as well as the large volcanic provinces, show no appreciable magnetic fields at high altitude. Blue line represents the crustal dichotomy. VB, Vastitas Borealis; El, Elysium; Ol, Olympus; Is, Isidis; Th, Tharsis; Ap, Apollinaris Patera; TM, Terra Meridiani; Sy, Syrtis Major; He, Hellas; Ar, Argyre.

Thermal core-mantle coupling can explain some features related to Earth's dynamo. Evidence suggests that the heterogeneous lower mantle affects convection and dynamo action in Earth's outer core. Paleomagnetic field models time-averaged over the past 5 million years show deviations from axial symmetry (*6*). Core flow models time-averaged over the past 150 years show persistent nonaxisymmetric features (*7*), and the seismic properties of the upper part of Earth's inner core also exhibit an east-west hemispheric dichotomy (*8*).

Dynamo simulations with heterogeneous heat flux boundary conditions have been used to study the possible impact of the mantle on Earth's dynamo (*9*). The models successfully

[1]Laboratoire de Planétologie et Géodynamique, CNRS UMR 6112, Université de Nantes, 44322 Nantes cedex 3, France. E-mail: benoit.langlais@univ-nantes.fr [2]Équipe de Géomagnétisme, Institut de Physique du Globe de Paris, CNRS UMR 7154, 75252 Paris cedex 5, France. E-mail: hagay@ipgp.jussieu.fr