PHYSICISTS TRIUMPH AT GUESS MY NUMBER

Quantum entanglement looks like telepathy when three physicists get together on a game show.

Andrew M. Steane and Wim van Dam

Let's meet tonight's lucky contestants, ladies and gentlemen, all ready to play *Guess My Number*, for the grand prize of ONE MILLION DOLLARS!"

The suave host turns to the group of three eager-looking people, and addresses the young woman first:

"You are Alice, from Cambridge, Massachusetts, and, I think, a research physicist?"

"Yes."

"We don't get many of those on the show. Welcome to *Guess My Number*!

"And next we have Bob, a quantum mechanic from Oxford, England. Good to have you, Bob!"

Bob moves to join Alice as the host continues smoothly on to the last guest.

"And last, but not least, welcome to Charles, a computer scientist from New York. It's good to have three people from such completely different walks of life . . ."

Charles begins to say, "Well actually . . . ," but the host moves straight on with the show, a professional who knows well the value of every second on prime-time television.

"Ladies and gentlemen, in a moment Alice, Bob, and Charles are going to step into the three isolation booths and play *Guess My Number*. But before they do so, let's make sure we all know the rules of the game.

"Alice, Bob, and Charles, you are going to sit in our three isolation booths. You can each take anything you can carry into the booths, but once you are in there, you will not be able to communicate with each other, or with anyone else, except me, until the end of the game. Do you understand?"

A calm murmur of "Yes" comes from the contestants. They seem quite happy and eager to get on with the game.

"I see you are each carrying a small case. You seem well prepared! Now, one of you will be the decision maker. Have you already elected your decision maker?"

The contestants indicate their agreement that Alice will be the decision maker.

"Good! Now, this is how the game works. I have before me a bowl of apples. Once you are all in the booths, I will take up to four apples from the bowl and divide them between the three of you. Before giving them out, I may cut one or more apples in half, but I will not cut them into any smaller pieces. So each of you will receive either nothing, or half an apple, or one apple, or one and a half apples, and so on. Although you won't know how many apples I started with, you will know that you have shared between you a whole number of apples—or possibly no apples at all! I hope everything is clear so far? We wouldn't want to miss that million-dollar jackpot just for a little misunderstanding, would we?"

The laborious detailing of the rules is really for the benefit of the viewers, of course, and the host is doing her best to keep it interesting.

"Now, you ask, how are you going to win that jackpot? Well, tonight, that's going to be up to you, Alice. As decision maker, all you have to do is decide whether you think you and your two fellows have, between you, an even or an odd number of apples. Is it an even number, like zero, two or four, or an odd number, either one or three? And remember, you only have one of the three pieces of the puzzle! Ladies and gentlemen, that looks a like a tough job for our decision maker, Alice! So we at *Guess My Number* will allow her fellow contestants, Bob and Charles, to lend her a hand. Bob and Charles, you will each have a flag, and after looking at your piece of apple you can hold your flag either up or down. Alice can't see what you are doing, but I will inform her of the position of each of your two flags, either up or down. With this information, and knowing what she herself received, she will then make her choice.

"Each round that Alice's team beats the odds and chooses correctly will bring them closer to the grand prize, and if they complete ten successful rounds, they will win the million-dollar jackpot! But if they guess incorrectly, the game will be over and they will leave with one of several merchandise prizes furnished by our sponsors. That's all there is to it!"

The audience has been listening hard, and some begin to think through whether Bob and Charles will be able to tell Alice what she needs to know. Old hands have come along with their own schemes; they are itching to have a go at the game. The host, with a twinkle in her eye, addresses the obvious question to the contestants.

"Now, you three have, I am sure, gotten together beforehand to work out a scheme to win at *Guess My Number*. So have many contestants before you, but none have managed to beat the system. Would you care to share with us the method you propose to use?"

The contestants demur. They are keeping their secret to themselves! The contestants on this game always do. These ones appear quite confident and keen to get down to business, but so have the many poor triplets before them who went away with a consolation prize, not the big jackpot for ten correct answers in a row.

"Alice, Bob, and Charles, please enter your isolation

ANDREW M. STEANE *is a university lecturer at the Centre for Quantum Computation in the department of physics, University of Oxford, England.* WIM VAN DAM *is completing his PhD at the Centre for Quantum Computation and Centrum voor Wiskunde en Informatica in Amsterdam, The Netherlands.*

booths, and good luck!"

The three make their way into the booths, each carrying a case that looks quite heavy for its size. The audience can see them through the window, but they can't see each other. They open their cases on the desks before them, and get their flags ready.

The host fills the time gap with a bit of patter, and the musicians provide a suitably tension-building background. The first three pieces of apple are distributed, passed through a little drawer on each booth. We see Alice, Bob, and Charles all adjusting something inside their cases, then Bob and Charles swiftly raise or lower their flags. The host reminds the audience that the contestants can take anything they like into the booths, but the booths are carefully isolated against every form of communication, including radio transmission or low-frequency sound.

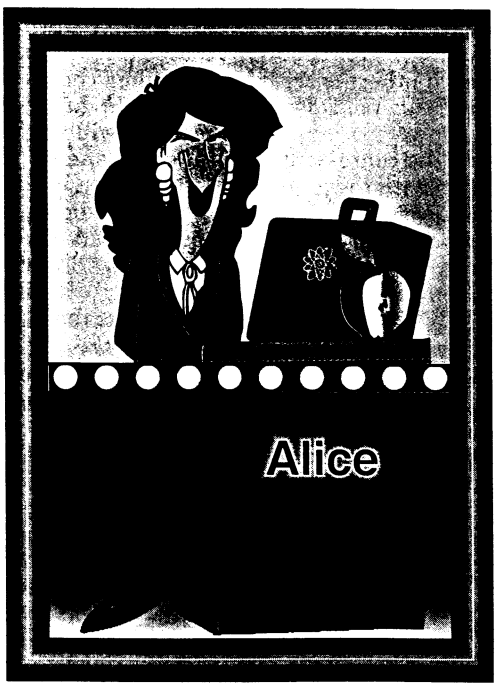
"Alice, I see Bob's flag is up, and Charles's flag is down. Have you reached your decision?"

"Yes, Debbie. I think it's an even number of apples."

"Alice, you said an even number, and I can reveal to you that I divided up two apples, which is an even number, so you are right!"

The audience breathes a sigh of relief. But the game moves immediately on to another round. The apples are divided and distributed, Bob and Charles indicate with their flags, and, to mounting astonishment, Alice guesses right again and again. Eight times, nine times, then ten times, and a big fanfare sounds the winning of the jackpot. An excited round of applause greets the news, and the contestants are invited to step out and learn of their success.

Of course, this is going to happen by chance every eighteen or so runs of the game (see later), and the designers of the program have based their calculations on this, knowing that the program will be much more successful if someone wins the jackpot every now and then.



The host asks Alice, Bob, and Charles if they would like to play again, for a chance to either double or halve their winnings. Of course, since the unfavorable 18-to-1 odds lead to statistically expected losses of $416 000, everyone knows that the only sensible thing is to quit while they are on top. But these three seem super-confident. There is no dissuading them, and the game continues, this time with a vengeance: The apples are divided into multiples of a quarter, not just a half! But surely something is up? Alice continues to get it right every time. Another ten times! The audience suspects the game has been rigged. The host senses the atmosphere is getting cool. Time for a commercial break!

Among the more alert viewers back at home, the scientific background of the three contestants did not go unnoticed. Nevertheless, the mathematically trained quickly worked out that once Alice looks at her own apple, she can reduce to eight the sixteen possibilities for Bob's and Charles's apples, using the rule that the total is a whole number of apples. Four of these eight possibilities make an even number, four an odd. Bob and Charles can use their flags to further reduce the possibilities for Alice, so that half the time she knows the required result, and half the time she has to guess, giving her an overall 75% chance of success per round. However, that is as far as they can go. Whatever strategy they choose, and whatever prior information they shared before the game, they can't pin down the remaining possibilities for Alice any further. One of them needs to be allowed to send another bit of information! (In the harder version using quarter apples, Alice needs two further bits, making four in all. This is a maximum; further subdividing the apples does not increase the information needed by Alice, though the proof of this is more involved.) The program designers no doubt employed some mathematicians, maybe backed up by some information scientists, to confirm exactly this argument.

Telepathy or science?

The astute viewers couldn't help noticing, though, an interesting combination of quantum physics and information science among this bunch of contestants. They called up their local quantum information physicist, who listened carefully to the whole setup, then with a smile explained:

"This is a simple but clear example of what we call entanglement-assisted communication. It is described in two papers by Richard Cleve, Harry Buhrman and Wim van Dam[1,2] (and some of the questions had been raised though not answered by Ilan Kremer[3]). Those contestants are well-known characters to us, and what they are carrying in their three cases is a technological marvel, but something perfectly well allowed by the laws of physics: namely, three small quantum information processors, storing a collection of ten pre-entangled triplets of quantum bits, or qubits.

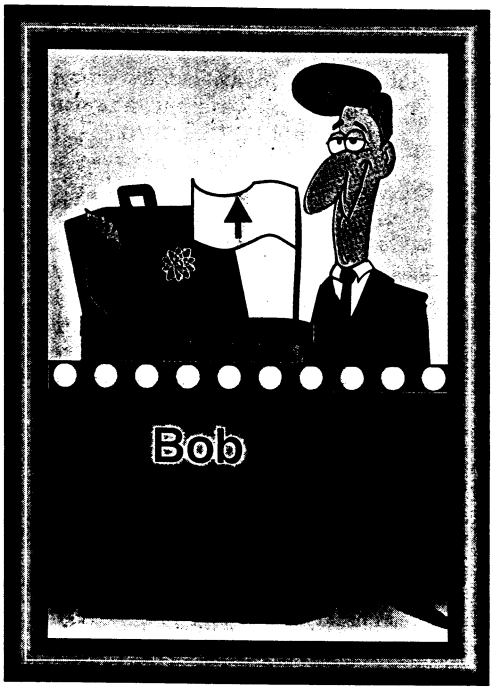
"Unlike classical bits, that encode only binary information (like even/odd or up/down) as a 0 or a 1, quantum bits are represented by a quantum state that can either be one of the definite states $|0\rangle$ and $|1\rangle$, or a linear combination of those states. Furthermore, quantum theory predicts, and recent experiments have confirmed, that pairs or larger groups of particles can be prepared in a joint quantum state, which they maintain even when separated by large distances. In such an 'entan-

gled state,' the particles behave in some respects like a single entity.

"Before the show, Alice, Bob, and Charles prepared ten triplets of qubits, every one in the completely entangled state $|000\rangle + |111\rangle$. Each contestant has, placed in their information processors, one qubit in the triplet. Their goal is to encode information in the joint state without destroying the entanglement, and then to reveal the winning answer by measurement.

"During the game, the moderator gives Alice, Bob, and Charles, respectively, x_a, x_b, x_c apples, where $x_i = 0$, 1/2, 1 or 3/2, and $i = a$, b, or c. (Actually, x_i can be larger than 3/2, as long as $x_a + x_b + x_c = 4$, but adding two apples to any contestant's total doesn't affect the result). They then each go to the first so far unused qubit in their processor, and apply the rotation $|0\rangle\langle 0| + \exp(x_i\pi\sqrt{-1})\,|1\rangle\langle 1|$. The resulting joint state is either $|000\rangle + |111\rangle$ (when $x_a + x_b + x_c$ is even) or $|000\rangle - |111\rangle$ (when $x_a + x_b + x_c$ is odd).

"To enable Alice to know which of these two orthogonal states they jointly own, each person next applies the Hadamard rotation, $|0\rangle \rightarrow (|0\rangle + |1\rangle)/\sqrt{2}$, $|1\rangle \rightarrow (|0\rangle - |1\rangle)/\sqrt{2}$, to their qubit. The resulting state is a three-qubit superposition of all the states of even parity, $(|000\rangle + |011\rangle + |101\rangle + |110\rangle)/2$ or all the states of odd parity, $(|111\rangle + |100\rangle + |010\rangle + |001\rangle)/2$. They each measure their qubit (in the basis $|0\rangle$, $|1\rangle$), which results in the collapse of the superposition state to one of its components. Bob and Charles tell Alice the result of their measurement, by a simple agreed scheme such as flag up means zero, flag down means one, and Alice, having her own measurement result already at hand, immediately knows the parity of the three measurement results and so the answer to the original problem."



Entanglement-assisted communication complexity

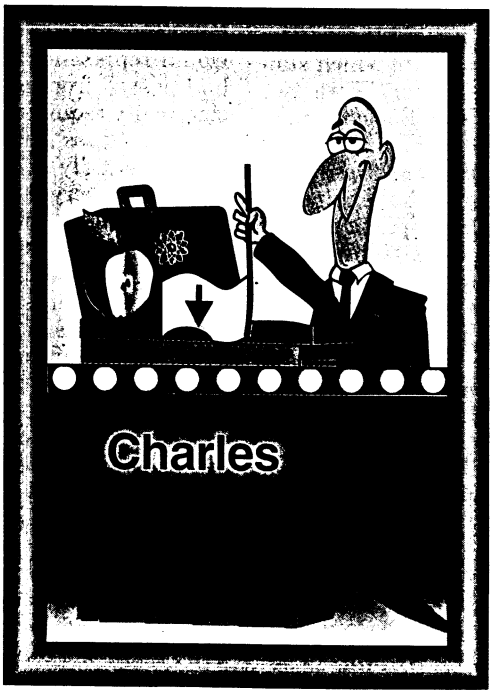
The game of *Guess My Number* is just an introduction to the concept of entanglement-assisted communication. What is striking about the subject is that the communication is all classical: Only classical bits and pieces are transmitted and received, so one would have thought that classical reasoning about the amount of information required to be sent would be valid. That it is not is a particularly clear illustration that the science of information cannot be divorced from physics.

It is obvious that what is going on is closely related to the famous Bell inequalities for nonlocal correlations between Einstein-Podolsky-Rosen (EPR) pairs, although it is equally well known that Bell–EPR correlations cannot in themselves be used for communication. That is, the existence of entanglement at separated spatial locations does not reduce the number of communication bits needed to convey a piece of information between the locations. In entanglement-assisted communication, we accept this fact, and examine instead situations where the knowledge sought by Alice, or any of the parties, is a function of classical information which, like the entanglement, is initially distributed among the parties. Typically the sought-after knowledge will have the size of a single bit (an even or odd number of apples, in the case of *Guess My Number*), which will be small enough that the fundamental restrictions on communication are not violated.

Note that entanglement-assisted communication is very close to quantum communication, because classical bits plus entanglement can serve to transmit quantum bits by teleportation.[4]

Guess My Number involves just a one or two bit difference between the information that must be transmitted in a classical solution and the minimum required for the "correct" solution. It is natural to ask whether larger savings from quantum entanglement are possible. One way is to offer Alice, Bob, and Charles m rounds of apples all at once, and ask Alice to give a single yes/no reply to the question: Does every round in the set contain an even number? Clearly, with entanglement assistance, she can use the method given above and require only m signals from Bob and m from Charles, making $2m$ in total, while it can be shown[5] that the classical limit requires at least $3m$ communicated bits.

A somewhat more powerful generalization can be made in another direction. Suppose we allow more contestants to play the game. Rather than just three parties, as in *Guess My Number*, we consider k parties who wish to know whether their k lots of apple segments all add up to an even or an odd number of whole apples, and furthermore we allow the apples to be more finely divided. To quantify the communication complexity CC(P) of a distributed problem P, we consider one classical bit, broadcast from one party to every other party, to constitute one bit of communication. So for *Guess My Number* (*Gmn*) we have for the quantum communication complexity $CC_q(Gmn) = 2$ and $CC_q(m\text{-round } Gmn) = 2m$, compared to the classical lower bounds $CC_c(Gmn) \geq 3$ and $CC_c(m\text{-round } Gmn) \geq 3m$. The result for the k-party game, obtained by Buhrman and coworkers,[5] is a proof that as the number of parties increases, the reduction in communication complexity becomes greater: The classical complexity $CC_c(k\text{-party } Gmn) \geq (k \log k) - k$ becomes much larger than the quantum complexity $CC_q(k\text{-party } Gmn) = k - 1$, where the latter requires an entangled state of k qubits. In the limit of many parties (large k), this last quantum complexity is an arbitrarily small frac-



tion of what would be required classically. Far from being of no use at all for communication, entanglement seems now to be extremely useful.

Then again, given the severe difficulty of creating, maintaining and manipulating multipartite entanglement in practice, perhaps this reduction by a factor of $CC_c/CC_q \sim \log k$ is not so exciting. What we would really like is a large reduction in communication complexity, without the need to involve many parties. It turns out this can be achieved. Buhrman, Cleve and Avi Wigderson[6] showed a general way to adapt Lov Grover's searching algorithm[7] to the communication scenario, allowing them to derive a result for the important "disjointness function," which can be viewed as the answer to the question: Do Alice and Bob both have the same day free on some date in their private n-page diaries? To solve this problem, a reliable answer can be obtained using prior entanglement with $CC_q(Disj_n) \leq \sqrt{n} \log n$, whereas every classical probabilistic protocol has a complexity linear in n, that is, $CC_c(Disj_n) \sim n$.

An even more striking difference between the classical and the entanglement-assisted solution was described by Ran Raz[8] for a problem involving an m-dimensional vector space. This problem could be viewed as a game like *Guess My Number* (though probably not on prime-time TV) having two contestants, Alice and Bob. Alice is given a vector and a specification of two orthogonal sub-spaces, and Bob is given a rotation matrix, all specified to a precision of order log m bits. The total amount of information they are supplied is therefore of order $n \approx m^2 \log m$. The object of the game is essentially to guess: Into which subspace does Bob's matrix rotate Alice's vector? With two subspaces to choose from, the answer is a Boolean function, R. It is not too difficult to show that the answer can be found very efficiently with entanglement-assisted communication: $CC_q(R_n) \leq \log n$. It is more challenging to show that the classical communication complexity has a lower bound $CC_c(R_n) \geq n^{1/4} / \log n$, which is significantly higher than the quantum complexity.

The separation described by Raz is termed "exponential," because the classical communication complexity grows exponentially faster in the input size n than the quantum complexity does. (Other types of exponential separation are described by Andris Ambainis and collaborators[9] as well as by Buhrman and collaborators[6].) In the same way, the separation in the disjointness problem discussed above is called "quadratic," but this does not make the result less impressive. In fact, if we examine the ratio $CC_c(Disj_n) / CC_q(Disj_n)$, we find that the "quadratic" reduction in complexity is much larger than the "exponential" one.

The question of which distributed problems allow a significant "quantum reduction" and which don't is the focus of much current research. But results that have already been obtained, like the solutions to *Guess My Number* and other problems described above, were completely unexpected and have already given us some profound insights into the properties of quantum mechanical systems and the nature of information itself.

Consider the information accounting in these protocols. Since the classical protocol requires, say, n bits to be transmitted, but the entanglement-assisted protocol only needs something like $\sqrt{n} \log n$ transmitted bits, then presumably each transmitted bit is somehow doing the work of $\sqrt{n} / \log n$ bits. The way to make sense of that nonsensical statement is to realize that what is transmitted is not, strictly speaking, an abstract classical bit, but rather a two-valued classical signal. In other words: A real physical entity or change is transmitted, and it is because this entity is coupled to the entangled systems at either end of each transmission that the surprising gain is seen. By calling the entity classical, when in fact all entities are quantum mechanical, we just mean that the whole process is insensitive to whether the transmitted entity is in a mixed or a pure state, so it can be sent safely down traditional communication channels without corrupting the transmission. This is, of course, a tremendously easier form of transmission than one that has to preserve the full quantum state.

Experimental prospects

A laboratory demonstration of entanglement-enhanced communication would be, in our opinion, a landmark in quantum physics and quantum information science. It would represent the first time that classical information had passed from one place to another with less than the classically required amount of communication.

The *Guess My Number* protocol is now close to being experimentally achievable. All that is required is a reliable Greenberger, Horne, and Zeilinger (GHZ) experiment[10] (see the "Reference Frame" column by N. David Mermin in PHYSICS TODAY, June 1990, page 9) that has the ability to apply simple single-qubit rotations. The GHZ experiments that have been reported to date,[11,12] though impressive, don't satisfy the demands of the game. The NMR quantum information processing experiments allow some of the properties of the GHZ state $|000\rangle + |111\rangle$ to be demonstrated,[11] but the technique provides no way to assign Alice, Bob, and Charles to independent regions of spacetime. The quantum optics experiments of Dik Bouwmeester and coworkers[12] do allow a realization of the GHZ state with separated measurements on the three particles, but only a tiny fraction (10^{-10}) of the ensemble of photon triplets is in the GHZ state, so Bob and Charles would do better to use a classical strategy rather than risk sending no information to Alice in almost every run. (We don't allow the contestants to post-select which runs they want to use, because that involves the communication of

FURTHER READING

For more information on the rapidly growing fields of quantum computing and quantum information theory, see the following items in PHYSICS TODAY.

Articles:

Charles H. Bennett, "Quantum Information and Computation," October 1995, page 24;

Serge Haroche and Jean-Michel Raimond, "Quantum Computing: Dream or Nightmare?" August 1996, page 51;

John Preskill, "Battling Decoherence: The Fault-Tolerant Quantum Computer," June 1999, page 24;

"Search and Discovery" news reports:

"Labs Demonstrate Logic Gates For Quantum Computation," March 1996, page 21;

"Exhaustive Searching is Less Tiring With a Bit of Quantum Magic," October 1997, page 19;

"The Steps of Grover's Search Algorithm," October 1997, page 20;

"Quantum Teleportation Channels Opened in Rome and Innsbruck," February 1998, page 18;

"What Really Gives a Quantum Computer Its Power?" January 2000, page 20.

huge amounts of information to Alice, which is also worse than a purely classical strategy.)

It is our hope that the ion trap experiments being actively pursued in several labs will soon reach a stage where this game could be played.[13,14] Admittedly, the walls between the booths of Alice, Bob, and Charles would only be a few microns thick, and made of nothing, but we can trust these three not to talk to each other. Before each round of the game, they set up three trapped ions in the GHZ state, then they each separately receive their number from the host and adjust the duration of a laser pulse addressed to their ion, and each one reads out the final state of their ion by resonance fluorescence. Reported experimental achievements to date indicate that an overall reliability of one run of the experiment (determined by the fidelity of the prepared GHZ state and the precision of the rotations and measurements) could be expected to attain the 60% level fairly soon. Thus, Alice could choose right with certainty roughly 60% of the time and be forced to make a random choice otherwise, for an overall chance of guessing right of order $(0.6 \times 1) + (0.4 \times 1/2) = 0.8$. These odds would be a statistically significant departure from the classical 75% odds after about a thousand rounds of the game, with no remaining "loopholes" connected with detector efficiencies or other experimental factors.

As soon as such an experiment is done, the classical data would speak for themselves: The most likely explanation of the phenomenon, without quantum theory, would be that the contestants managed to cheat—since that is a much more likely hypothesis than the other one which suggests itself, namely that they used telepathy!

References

1. R. Cleve, H. Buhrman, Phys. Rev. A **56**, 1201 (1997).
2. H. Buhrman, R. Cleve, W. van Dam, preprint, http://xxx.lanl.gov/abs/quant-ph/9705033.
3. I. Kremer, "Quantum Communication," master's thesis, The Hebrew Univ. of Jerusalem (1995).
4. C.H. Bennett, G. Brassard, C. Crépeau, R. Josza, A. Peres, W.K. Wootters, Phys. Rev. Lett. **70**, 1895 (1993).
5. H. Buhrman, W. van Dam, P. Høyer, A. Tapp, Phys. Rev. A **60**, 2737 (1999).
6. H. Buhrman, R. Cleve, A. Wigderson, in *Proceedings of the 30th Annual ACM Symposium on Theory of Computing (STOC'98)*, ACM Press, New York (1998) p. 63.
7. L. Grover, Phys. Rev. Lett. **79**, 325 (1997).
8. R. Raz, in *Proceedings of the 31st Annual ACM Symposium on Theory of Computing (STOC'99)*, ACM Press, New York (1999), p. 358.
9. A. Ambainis, L. J. Schulman, A. Ta-Shma, U. Vazirani, A. Wigderson, in *Proceedings of the 39th Annual Symposium on Foundations of Computer Science (FOCS'98)*, IEEE Computer Society, Los Alamitos, California (1998), p. 342.
10. D. M. Greenberger, M. A. Horne, A. Zeilinger, in *Bell's Theorem, Quantum Theory and Conceptions of the Universe*, M. Kafatos, ed., Kluwer Academic, Dordrecht, The Netherlands (1989), p. 73; D. M. Greenberger, M. A. Horne, A. Shimony, A. Zeilinger, *Amer. J. Phys.* **58**, 1131 (1990).
11. R. Laflamme, E. Knill, W. H. Zurek, P. Catasti, S. V. S. Mariappan, Phil. Trans. Royal Soc. London A, **356**, 1941 (1998); R. J. Nelson, D. G. Cory, S. Lloyd, preprint, http://xxx.lanl.gov/abs/quant-ph/9905028.
12. D. Bouwmeester, J-W. Pan, M. Daniell, H. Weinfurter, A. Zeilinger, Phys. Rev. Lett. **82**, 1345 (1999).
13. Q. A. Turchette, C. S. Wood, B. E. King, C. J. Myatt, D. Leibfried, W. M. Itano, C. Monroe, D. J. Wineland, Phys. Rev. Lett. **81**, 3631 (1998).
14. H. C. Nägerl, D. Leibfried, H. Rohde, G. Thalhammer, J. Eschner, F. Schmidt-Kaler, R. Blatt, Phys. Rev. A **60**, 145 (1999).

■