PHYSICAL REVIEW
LETTERS

VOLUME 69 16 NOVEMBER 1992 NUMBER 20

Communication via One- and Two-Particle Operators on Einstein-Podolsky-Rosen States

Charles H. Bennett
IBM Research Division, T. J. Watson Research Center, Yorktown Heights, New York 10598

Stephen J. Wiesner
74 Parkman Street, Brookline, Massachusetts 02146
(Received 16 June 1992)

As is well known, operations on one particle of an Einstein-Podolsky-Rosen (EPR) pair cannot influence the marginal statistics of measurements on the other particle. We characterize the set of states accessible from an initial EPR state by one-particle operations and show that in a sense they allow two bits to be encoded reliably in one spin-$\frac{1}{2}$ particle: One party, "Alice," prepares an EPR pair and sends one of the particles to another party, "Bob," who applies one of four unitary operators to the particle, and then returns it to Alice. By measuring the two particles jointly, Alice can now reliably learn which operator Bob used.

PACS numbers: 03.65.Bz, 42.50.Dv, 89.70.+c

It is well known that while remote measurements on the two separated particles of an Einstein-Podolsky-Rosen (EPR) [1] pair, such as the singlet state of two spin-$\frac{1}{2}$ particles,

$$\sqrt{1/2}(|\uparrow\downarrow\rangle-|\downarrow\uparrow\rangle)\,, \tag{1}$$

can be used to establish nonlocal correlations over a spacelike interval, these correlations cannot be used for superluminal communication. In particular, no manipulation of one member of an EPR pair can influence the marginal statistics of measurements on the other member, for example, causing it to have a nonzero expectation of some spin component. Here we consider an arbitrary manipulation of one EPR particle, which can be modeled in full generality as a unitary interaction of that particle with an outside system or "ancilla," initially in a pure state. We show that such interactions can be used to prepare all and only those states of the joint system (two particles and ancilla) that yield unperturbed marginal statistics for all measurements on the other particle, with which the ancilla did not interact. By choosing an appropriate ancilla, and projecting it out at the end, one can thus prepare any pure or mixed state of the two EPR particles having unperturbed marginal statistics for the untreated particle.

Specializing to the case without ancilla, the interaction can be viewed simply as a preparation of the two particles by a unitary operation on only one of them, and the set of states that can be prepared comprises all and only those two-particle pure states having unperturbed marginal statistics for measurements on the untreated particle (in the case of two-particle pure states, this also implies unperturbed marginal statistics for the treated particle). We point out that the set of two-particle states preparable by one-particle operators is a proper subset, *but not a subspace*, of the full four-dimensional Hilbert space of the two particles. Nevertheless, it includes four mutually orthonormal states, a fact which can be exploited to accomplish the seemingly paradoxical feat of transmitting two bits reliably via a single spin-$\frac{1}{2}$ particle. As indicated above, this is done with the help of a second particle, the EPR twin of the first particle, which never leaves the hands of the intended receiver of the message.

We now demonstrate the equivalence between states accessible through one-particle operators and states with random marginal statistics for the untreated particle.

A general expression for a pure state of the tripartite system comprising the two EPR particles and the ancilla is

$$|\Phi\rangle=|\uparrow\uparrow\rangle|A\rangle+|\downarrow\downarrow\rangle|B\rangle+|\uparrow\downarrow\rangle|C\rangle+|\downarrow\uparrow\rangle|D\rangle\,, \tag{2}$$

where $|\uparrow\uparrow\rangle$, $|\downarrow\downarrow\rangle$, $|\uparrow\downarrow\rangle$, and $|\downarrow\uparrow\rangle$ are a complete orthonormal set of spin states for the two particles, and $|A\rangle$, $|B\rangle$, $|C\rangle$, and $|D\rangle$ are four unnormalized states of the ancilla, not necessarily orthogonal, and obey only the joint normalization constraint

$$\langle A|A\rangle+\langle B|B\rangle+\langle C|C\rangle+\langle D|D\rangle=1\,. \tag{3}$$

The full space of such states could be accessed, for example, by allowing the ancilla, in a normalized standard initial state $|I\rangle$, to interact simultaneously with *both* particles, initially in the EPR state $\sqrt{1/2}(|\uparrow\downarrow\rangle-|\downarrow\uparrow\rangle)$.

We shall now show that interactions of the ancilla with only one of the EPR particles (say the first) can prepare all states $|\Phi\rangle$ having random marginal statistics for measurements on the other particle. The interaction of an ancilla in initial state $|I\rangle$ with the first EPR particle can be described by a unitary operator U in the smaller product Hilbert space of the ancilla and the first particle. By unitarity of U, the two states

$$\begin{aligned} U(|I\rangle|\uparrow\rangle)&=|J\rangle|\uparrow\rangle+|K\rangle|\downarrow\rangle\,,\\ U(|I\rangle|\downarrow\rangle)&=|L\rangle|\uparrow\rangle+|M\rangle|\downarrow\rangle \end{aligned} \tag{4}$$

are orthonormal. Here $|J\rangle$, $|K\rangle$, $|L\rangle$, and $|M\rangle$ are (unnormalized) states of the ancilla after the interaction. The orthonormality of the two states of Eq. (4) is equivalent to the constraints

$$\begin{aligned} &\langle J|L\rangle+\langle K|M\rangle=0\,,\\ &\langle J|J\rangle+\langle K|K\rangle=\langle L|L\rangle=\langle M|M\rangle=1\,. \end{aligned} \tag{5}$$

Applying the appropriate extension of U to the larger system comprising the ancilla in initial state $|I\rangle$ and the two particles in an initial EPR state, $\sqrt{1/2}(|\uparrow\downarrow\rangle-|\downarrow\uparrow\rangle)$, yields the state

$$|\Phi\rangle=\sqrt{1/2}(-|\uparrow\uparrow\rangle|L\rangle+|\downarrow\downarrow\rangle|K\rangle+|\uparrow\downarrow\rangle|J\rangle-|\downarrow\uparrow\rangle|M\rangle)\,. \tag{6}$$

This can be seen to be of the same form as Eq. (2) but with the constraints

$$\langle A|A\rangle+\langle D|D\rangle=\langle B|B\rangle+\langle C|C\rangle=\tfrac{1}{2} \tag{7}$$

and

$$\langle A|C\rangle+\langle D|B\rangle=0\,. \tag{8}$$

We now show that these constraints, sufficient for a state $|\Phi\rangle$ to be produced by manipulation of the first particle only, are already implied by the requirement of correct marginal statistics for measurements of the second particle's spin along the z, x, and y axes, respectively. Correct marginal statistics for the second particle's z spin component imply that the two orthogonal vectors

$$|A\rangle|\uparrow\uparrow\rangle+|D\rangle|\downarrow\uparrow\rangle,\quad |B\rangle|\downarrow\downarrow\rangle+|C\rangle|\uparrow\downarrow\rangle$$

each have magnitude $\sqrt{1/2}$, in turn implying Eq. (7). Similarly, correct marginal statistics for the second particle's x and y spin components, together with Eq. (7), imply, respectively, the real and imaginary parts of Eq. (8). Therefore, all states $|\Phi\rangle$ of the tripartite system having correct marginal statistics for measurements on the second, untreated EPR particle [equivalent to the constraints of Eqs. (7) and (8) on Eq. (2)] can be made from an EPR pair by interaction of an ancilla with the first particle alone. We already have noted that *only* such states of the tripartite system can be made by this means, because the ability to make a state with nonrandom marginal statistics for the untreated particle would provide a superluminal communication channel.

Specializing to the case without ancilla, the set of two-particle pure states that can be made from an initial EPR state by unitary transformations acting only on the first particle consists of all and only those two-particle pure states yielding correct marginal statistics for measurements on the untreated particle. These states can be described by an expression like Eq. (2) but with scalar coefficients a, b, c, and d,

$$|\phi\rangle=a|\uparrow\uparrow\rangle+b|\downarrow\downarrow\rangle+c|\uparrow\downarrow\rangle+d|\downarrow\uparrow\rangle\,, \tag{9}$$

obeying the scalar analogs of Eqs. (7) and (8), viz.,

$$|a|^2+|d|^2=|b|^2+|c|^2=\tfrac{1}{2} \tag{10}$$

and

$$a^*c+d^*b=0\,. \tag{11}$$

Eliminating three dependent variables, the set of states preparable from an initial EPR state by unitary operators on the first particle can be expressed in terms of five real angles

$$|\phi\rangle=\frac{\cos\theta}{\sqrt{2}}(e^{i\alpha}|\uparrow\uparrow\rangle+e^{i\beta}|\downarrow\downarrow\rangle)+\frac{\sin\theta}{\sqrt{2}}(e^{i\gamma}|\uparrow\downarrow\rangle+e^{i\delta}|\downarrow\uparrow\rangle)\,, \tag{12}$$

with one remaining constraint,

$$\delta+\gamma=\pi+\alpha+\beta\,. \tag{13}$$

The symmetry of Eqs. (12) and (13) with respect to the coefficients of $|\downarrow\uparrow\rangle$ and $|\uparrow\downarrow\rangle$ implies that unitary operations on one particle of an EPR pair, without ancilla, cannot influence the marginal statistics of *either* particle, not even the one the operator has acted upon. By contrast, if an ancilla is used, the marginal statistics of the treated particle can be arbitrarily manipulated, but those of the untreated particle must remain random, as they were in the original EPR state.

It is noteworthy that the manifold defined by Eqs. (12) and (13), i.e., the set of states preparable by one-particle unitary operators on an initial EPR state, is a proper subset, but not a subspace, of all two-particle pure states. On the one hand it includes states such as

$$\begin{aligned} &\sqrt{1/2}(|\uparrow\downarrow\rangle-|\downarrow\uparrow\rangle),\quad \sqrt{1/2}(|\uparrow\downarrow\rangle+|\downarrow\uparrow\rangle)\,,\\ &\sqrt{1/2}(|\uparrow\uparrow\rangle-|\downarrow\downarrow\rangle),\quad \sqrt{1/2}(|\uparrow\uparrow\rangle+|\downarrow\downarrow\rangle)\,, \end{aligned} \tag{14}$$

which form a complete basis for the four-dimensional Hilbert space, but on the other hand it does not include states such as $|\uparrow\uparrow\rangle$, whose creation, from an initial EPR state, could be used to send a measurable signal to the observer of the untreated particle.

The orthonormality of Eq. (14) means that manipulations of one particle of a separated EPR pair, while they cannot be used to communicate directly with the untreated particle, can be used to encode four reliably distinguishable messages in the two-particle system. To perform this feat, Alice, the intended receiver of the message, first prepares a pure EPR state and lends one particle of the pair to Bob, the intended sender. Bob then operates on the particle via one of four unitary operators so as to put the two-particle system into a chosen one of the four states of Eq. (14) and then returns the treated particle to Alice. Now possessing both particles, Alice can in principle measure them jointly in the orthonormal basis of Eq. (14), and so reliably learn which operator Bob applied.

From one viewpoint, this is surprising, because Bob has communicated a two-bit message by unitarily operating on a single spin-$\frac{1}{2}$ particle. Thinking too classically, one might be tempted to say that his manipulations have therefore placed the *treated* particle into four reliably distinguishable states, contradicting a basic principle of quantum mechanics that such a particle can have only two reliably distinguishable states. But the scheme also depends on the untreated particle. It therefore might be better to say, as Schumacher suggests [2], that one of the two bits is sent forward in time through the treated particle, while the other bit is sent backward in time to the EPR source, then forward in time through the untreated particle, until finally it is combined with the bit in the treated particle to reconstitute the two-bit message. Because the bit "sent backward in time" cannot be used to transmit a meaningful message without the help of the other particle, no opportunity for time travel or superluminal communication is created, just as none is created in the classic EPR experiment in which simultaneous measurements are used to establish non-message-bearing correlations over a spacelike interval.

The communication of two bits via two particles, one of which remains fixed while the other makes a round trip, is no more efficient in number of particles or number of transmissions than the obvious scheme of directly encoding each bit in one transmitted particle. Nevertheless, the EPR scheme has the advantage of allowing some of the particle transmissions to take place before the message has been decided upon, perhaps at cheaper "off-peak" rates. Thus Alice might prepare a number of EPR pairs in advance and send one member of each pair to Bob during off-peak hours. Subsequently, during peak hours, Bob could use each of these particles to send a two-bit message back to Alice, or Alice could use each of her remaining unsent particles to send a two-bit message to Bob.

From a practical standpoint, the unitary transformations Bob would apply to his particle to transform the initial EPR state into the other three states of Eq. (14) are quite easy to implement, being simply 180° rotations about the z, x, and y axes. On the other hand, for Alice to reassemble the two spin-$\frac{1}{2}$ particles into a jointly measurable entity appears technologically infeasible. However, another version of the EPR effect [3], involving pairs of particles entangled in position and momentum instead of spin, might allow experimental realization of an analogous four-way coding scheme. For example (see Fig. 1), Alice could use parametric down-conversion [4] in a nonlinear crystal X to produce the EPR-like two-photon state $\Psi=\sqrt{1/2}(|AC\rangle+|DB\rangle)$, where $|AC\rangle$ represents a two-photon state with photons in beams A and C and $|DB\rangle$ represents a two-photon state with photons in beams D and B. The wave vectors of the four outgoing beams satisfy the relation $\mathbf{k}_A+\mathbf{k}_C=\mathbf{k}_D+\mathbf{k}_B=\mathbf{k}$, where $\mathbf{k}$ is the wave vector of the incoming beam incident on X. Additional conditions $|\mathbf{k}_A|=|\mathbf{k}_D|$ and $|\mathbf{k}_B|=|\mathbf{k}_C|$, though not necessary for down-conversion, are convenient for our purposes, and can be enforced through appropriate placement of the crystal and pinholes defining the beams.

In order to receive a two-bit message from Bob, Alice keeps beams A and D under her control, but allows Bob to handle beams B and C, which together contain one of the down-converted photons. Bob encodes his four-way choice by applying a chosen one of four treatments to beams B and C as they pass through the dashed region in Fig. 1, before returning to the portion of the apparatus operated by Alice. Bob's four treatments are as follows:

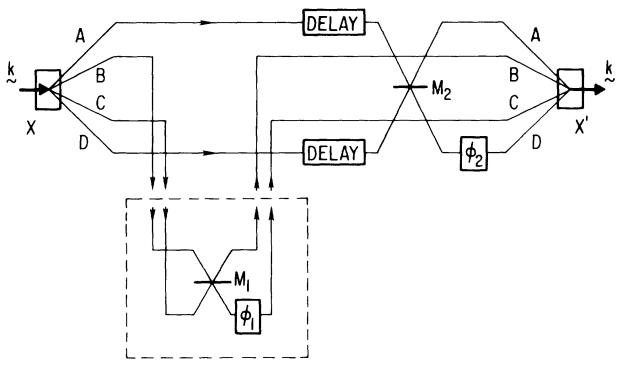

FIG. 1. Possible implementation of four-way coding using parametric down- and up-conversion. Incoming photon of wave vector $\mathbf{k}$ is parametrically down-converted by crystal X into a superposition of two-photon states, with one photon in beams B and C and the other in beams A and D. Sender encodes a chosen one of four messages by applying a phase shift ϕ_1 of 0 or π and including or removing the double-sided mirror M_1, which, if removed, swaps beams B and C. Receiver interprets message by performing a random one of four analogous manipulations on beams A and D, using phase shifter ϕ_2 and mirror M_2. Only if sender and receiver perform the same manipulations can an up-converted photon be recovered from crystal X'.

(1) Do nothing, leaving the original state $\sqrt{1/2}(|AC\rangle + |DB\rangle)$ unaltered. (2) Introduce a half-wave retardation in one of the beams, for example by setting phase shifter $\phi_1 = \pi$, yielding state $\sqrt{1/2}(|AC\rangle - |DB\rangle)$. (3) Optically interchange beams B and C, e.g., by removing the two-sided mirror M_1, yielding state $\sqrt{1/2}(|AB\rangle + |DC\rangle)$. (4) Perform both the above actions, yielding state $\sqrt{1/2}(|AB\rangle - |DC\rangle)$. Bob then returns beams B and C to Alice. Just as in the spin-$\frac{1}{2}$ particle implementation, Bob's action on one particle has placed the entire two-particle, four-beam system into one of four orthogonal states, which in principle can be distinguished with perfect efficiency.

Figure 1 shows a more practical but imperfectly efficient detection method, one which usually fails, but, when it succeeds, tells Alice accurately which choice Bob made. To begin the detection Alice uses her own phase shifter ϕ_2 and removable two-sided mirror M_2 to apply a randomly chosen one of four treatments to beams A and D, analogous to the treatments applied by Bob to beams B and C. Beams A and D together contain the other photon, i.e., the one not handled by Bob.

Finally Alice merges all four beams in a nonlinear crystal X' similar to X, taking care to match propagation times and beam directions so as to create conditions suitable for parametric up-conversion, the inverse of the down-conversion that occurred in crystal X. If an up-converted photon of wave vector $\mathbf{k}$ emerges from crystal X', Alice will know that her choice of treatment of the photon in beams A and D matched Bob's treatment of the photon in beams B and C. Otherwise, Alice's null result indicates that her treatment differed from Bob's, or that up-conversion, while optically possible, failed to occur due to the imperfect efficiency of the process.

Leaving aside questions of practicality, either of these schemes would appear to provide an intrinsically untapable communication channel, since the two bits Bob inscribes in his particle are utterly unintelligible without the other particle, which remains in Alice's hands. This would appear to offer a more elegant means of private communications than previous quantum cryptographic schemes [5–9] which require the users to publicly test some of the data exchanged through the quantum channel, in order to certify the privacy of the rest. However, the appearance of intrinsic security is illusory, since an active adversary could effectively tap into the channel by intercepting all the particles on their way to and from Bob, substituting others in such a way as to impersonate Alice to Bob and Bob to Alice. To defend against this attack Alice and Bob would also need to publicly test some of their data, rendering the present scheme cryptographically equivalent to previous schemes, while retaining its distinctive quantum information-theoretic feature of packing two bits into a single transmitted two-state particle.

The above coding scheme can be generalized to prepare a pair of n-state particles in any one of n^2 orthogonal states by operations on only one of the particles, if the original state is maximally entangled, e.g.,

$$|\Psi\rangle = \left(\sum_{j=1}^{n} |j\rangle |j\rangle \right) \Big/ \sqrt{n} , \tag{15}$$

where $|j\rangle$ are a complete orthonormal set of single-particle states. Still more generally, if Bob's particle has an m-dimensional Hilbert space and Alice's retained particle an n-dimensional one, the maximum number of orthogonal states of the joint system accessible through Bob's manipulation of his particle is the lesser of m^2 and mn. These states span the full joint Hilbert space if $m \geq n$; but if $m < n$, the accessible states of Alice's particle lie in a proper subspace spanned by the m-independent relative states present in the initial superposition.

We wish to thank Anton Zeilinger for suggesting parametric up-conversion as a possible practical means of reuniting the separated EPR particles, and Asher Peres, Benjamin Schumacher, and William Wootters for showing how to generalize the coding scheme to particles with more than two-dimensional Hilbert spaces.

[1] A. Einstein, B. Podolsky, and N. Rosen, Phys. Rev. **47**, 777 (1935); D. Bohm, *Quantum Theory* (Prentice Hall, Engelwood Cliffs, NJ, 1951).

[2] B. Schumacher (private communication).

[3] M. A. Horne and A. Zeilinger, in *Symposium on the Foundations of Modern Physics*, edited by P. Lahti and P. Mittelstaedt (World Scientific, Singapore, 1985), pp. 435–439; M. A. Horne, A. Shimony, and A. Zeilinger, Phys. Rev. Lett. **62**, 2209–2212 (1989).

[4] D. C. Burnham and D. L. Weinberg, Phys. Rev. Lett. **25**, 84–87 (1970); R. Ghosh and L. Mandel, Phys. Rev. Lett. **59**, 1903–1905 (1987).

[5] C. H. Bennett and G. Brassard, in *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, December 1984* (IEEE, New York, 1985), pp. 175–179.

[6] A. Ekert, Phys. Rev. Lett. **67**, 677 (1991).

[7] C. H. Bennett, G. Brassard, and N. D. Mermin, Phys. Rev. Lett. **68**, 557–559 (1992).

[8] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, J. Cryptology **5**, 3 (1992).

[9] A. K. Ekert, J. G. Rarity, P. R. Tapster, and G. M. Palma, Phys. Rev. Lett. **69**, 1293–1295 (1992).