TelePOVM— A generalized quantum teleportation scheme

G. Brassard
P. Horodecki
T. Mor

In this paper, we show that quantum teleportation is a special case of a generalized Einstein–Podolsky–Rosen (EPR) nonlocality. On the basis of the connection between teleportation and generalized measurements, we define ***conclusive teleportation****. We show that perfect conclusive teleportation can be obtained with any pure entangled state, and it can be arbitrarily approached with a particular mixed state.*

1. Introduction

Quantum information processing [1–3] is concerned with the processing of information in which the basic units are two-level quantum systems [4, 5] (such as spin-$\frac{1}{2}$ particles and the polarization of individual photons) known as quantum bits, or *qubits*. The state of a qubit is given by $|\phi\rangle = \alpha|0\rangle + \beta|1\rangle = \binom{\alpha}{\beta}$, where α and β are complex amplitudes subject to the normalization condition $|\alpha^2| + |\beta|^2 = 1$, and $|0\rangle \equiv \binom{1}{0}$ and $|1\rangle \equiv \binom{0}{1}$ are the basis state vectors. When the state of two or more qubits cannot be expressed as a tensor product of individual qubits, we say that the system is in an *entangled* state. Entanglement is at the heart of spectacular phenomena in quantum information theory, such as quantum computation, entanglement-based quantum cryptography, quantum error correction, quantum communication complexity, and more.

The special properties of entangled states were first noted by Einstein, Podolsky, and Rosen (EPR) [6], and a proof that they exhibit behavior that cannot be explained by classical local realistic theories was first obtained by Bell [7]. The EPR–Bohm state of a pair of qubits, known as the *singlet state*, is the most important illustration of entanglement:

$$|\Psi^-\rangle = \frac{1}{\sqrt{2}}|01\rangle - \frac{1}{\sqrt{2}}|10\rangle. \tag{1}$$

This state can be complemented to a basis for the state of two qubit systems [8] by adding the three states $|\Psi^+\rangle = \frac{1}{\sqrt{2}}|01\rangle + \frac{1}{\sqrt{2}}|10\rangle$, $|\Phi^-\rangle = \frac{1}{\sqrt{2}}|00\rangle - \frac{1}{\sqrt{2}}|11\rangle$, and $|\Phi^+\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$. These four states, which should have been called the *BMR states* in honor of Braunstein, Mann, and Revzen, who first presented them, together form the *BMR basis*. Following the established terminology, we use the terms *Bell states* and *Bell basis* instead, and we call two entangled qubits (in any Bell state) an *EPR pair*.

One of the most fascinating applications of entanglement is *quantum teleportation* [9], which is one of the pillars of quantum information theory (see [1, 10]) and has been realized experimentally on several occasions. Quantum teleportation is a process that enables the transmission of an unknown quantum state via a previously shared EPR pair with the help of only two classical bits transmitted on a classical channel. Assume that Alice (the sender) has a qubit in an unknown quantum state, which she wishes to transmit to Bob (the receiver). This would seem to be impossible if a quantum channel were not available to Alice and Bob at the time transmission had to take place. But assume that a quantum channel was available at some point in the past—perhaps when Alice and Bob were in physical contact—and assume that they are capable of storing quantum information faithfully. As a preprocessing step, when the quantum channel is available, Alice can prepare a Bell state, store one particle in her quantum memory, and use the channel to send the other particle to Bob, who stores

Written on the occasion of Charlie Bennett's sixtieth birthday, with fondness and admiration.

0018-8646/04/$5.00 © 2004 IBM

it in *his* quantum memory. At this point, we say that Alice and Bob share an EPR pair. Later on, when the quantum channel may no longer be available, Alice receives an unknown quantum state $|\phi\rangle = \binom{\alpha}{\beta}$. To teleport this state to Bob, she performs a joint measurement on the two particles that are in her hands: the unknown quantum state and her share of the EPR pair. This measurement destroys state $|\phi\rangle$ in her laboratory, but it produces two classical bits. Using a classical channel, she sends her two-bit result to Bob, who performs some unitary operation on his particle, "transforming" it into the (still unknown) original state $|\phi\rangle$.

More precisely, the unknown state to be teleported by Alice and the EPR pair shared between Alice and Bob (say, in the singlet state) form a three-qubit system in the joint state:

$$|\Psi\rangle_{123} = |\phi\rangle_1 |\Psi^-\rangle_{23} = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}_1 \left(\frac{1}{\sqrt{2}} |01\rangle_{23} - \frac{1}{\sqrt{2}} |10\rangle_{23} \right),$$

where the subscripts serve to denote the particles as follows: The subscript 1 pertains to the particle whose state has to be teleported, the subscript 2 to Alice's share of the EPR pair, and the subscript 3 to Bob's share. Teleportation is based on the fact [9] that this initial state can be written equivalently as

$$|\Psi\rangle_{123} = \frac{1}{2} \left[|\Phi^+\rangle_{12} \begin{pmatrix} -\beta \\ \alpha \end{pmatrix}_3 + |\Phi^-\rangle_{12} \begin{pmatrix} \beta \\ \alpha \end{pmatrix}_3 + |\Psi^+\rangle_{12} \begin{pmatrix} -\alpha \\ \beta \end{pmatrix}_3 - |\Psi^-\rangle_{12} \begin{pmatrix} \alpha \\ \beta \end{pmatrix}_3 \right]. \qquad (2)$$

A *Bell measurement* by Alice on her particles (1) and (2) produces two classical bits. These bits specify one of four possible results, chosen with equal probability in this case since the amplitude of each of the Bell states in Alice's particles is $\pm\frac{1}{2}$ prior to the measurement. Using this classical outcome, Alice knows into which of the following states Bob's particle (3) has been projected:

$$\begin{pmatrix} -\beta \\ \alpha \end{pmatrix}, \quad \begin{pmatrix} \beta \\ \alpha \end{pmatrix}, \quad \begin{pmatrix} -\alpha \\ \beta \end{pmatrix}, \quad \text{or} \quad \begin{pmatrix} \alpha \\ \beta \end{pmatrix}.$$

Alice then sends these two bits to Bob over a classical channel. This allows him to choose the appropriate rotation from

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \text{or} \quad \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

by which he can rotate the state of his particle (3) back into the desired unknown state $|\phi\rangle = \binom{\alpha}{\beta}$. Alternatively, this process can be described by a quantum circuit [11].

The minimal resources required for faithful teleportation are one EPR pair, which is *independent* of $|\phi\rangle$, and two classical bits. This may seem rather mysterious because 1) using the Bloch sphere formalism, the state of the particle to be teleported can be described by a point on a unit sphere (assuming that the state to be teleported was pure), hence by two *real* numbers and certainly not by two bits; and 2) even from those two classical bits, neither Alice nor Bob can learn anything about the unknown parameters of the teleported state because these bits are easily seen to be purely random, and therefore independent of $|\phi\rangle$.

The alternative approach presented in this paper sheds new light on this mystery. We interpret teleportation in the light of a seminal 1993 paper of Hughston, Jozsa, and Wootters (HJW) [12], which itself was anticipated by an extraordinary paper [13] written by Schrödinger only one year after the original 1935 EPR paper [6]. A slightly more restricted scenario than the one discussed by HJW was previously presented by Gisin [14] in 1989. Specifically, we use the language of generalized measurements to express the ideas of HJW and then we present the teleportation process as a special case of generalized EPR nonlocality.

A *positive operator valued measure* (POVM) provides the most general physically realizable measurement in quantum mechanics [5]; hence, we also refer to POVMs as "generalized measurements." Formally, a POVM is a collection of positive operators A_i on a Hilbert space $\mathcal{H}_n$ of dimension n that sum up to the identity $A_1 + \cdots + A_r = I_n$. (An operator is positive if all of its eigenvalues are positive or zero.) Standard measurements, which are usually described by some Hermitian operator in quantum mechanics texts, arise as a special case when $A_i = |\psi_i\rangle\langle\psi_i|$ and $A_i A_j = \delta_{ij} A_i$. We discuss here only rank-one POVMs, in which each of the $A_i = q_i|\psi_i\rangle\langle\psi_i|$ is proportional to a projection operator but the operators are not necessarily orthogonal to each other, so that r can be greater than n. Neumark's theorem states that, at least in principle, any POVM can be implemented by the adjunction of an ancilla in a known state, followed by a standard measurement in the enlarged Hilbert space [5].

To describe the EPR nonlocality and its generalization, we first define the notion of ρ-ensembles (any ensemble with density matrix ρ) [12]. An ensemble of quantum states is defined by a collection of normalized states $|\psi_1\rangle, \cdots, |\psi_m\rangle$ taken with *a priori* probabilities $p_1, \cdots, p_m$, respectively, so that $\sum_i p_i = 1$. Any such ensemble can be associated with its *density matrix*,

$$\rho = \sum_{i=1}^{m} p_i |\psi_i\rangle\langle\psi_i|.$$

For instance, for the completely mixed state in two dimensions, $\rho = \frac{1}{2}I$, the following are all legitimate ρ-ensembles:

$$
\begin{aligned}
&E_1 = \left\{ |\psi_1\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, |\psi_2\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}; p_1 = p_2 = \frac{1}{2} \right\};\\
&E_2 = \left\{ |\psi_1\rangle = \begin{pmatrix} 1/\sqrt{2} \\ 1/\sqrt{2} \end{pmatrix}, |\psi_2\rangle = \begin{pmatrix} 1/\sqrt{2} \\ -1/\sqrt{2} \end{pmatrix}; p_1 = p_2 = \frac{1}{2} \right\};\\
&E_3 = \left\{ |\psi_1\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, |\psi_2\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}, |\psi_3\rangle = \begin{pmatrix} 1/\sqrt{2} \\ 1/\sqrt{2} \end{pmatrix}, \right.\\
&\qquad\qquad \left. |\psi_4\rangle = \begin{pmatrix} 1/\sqrt{2} \\ -1/\sqrt{2} \end{pmatrix}; p_i = \frac{1}{4},\ 1 \le i \le 4 \right\};\\
&E_4 = \left\{ |\psi_1\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}, |\psi_2\rangle = \begin{pmatrix} \alpha \\ -\beta \end{pmatrix}, |\psi_3\rangle = \begin{pmatrix} \beta \\ \alpha \end{pmatrix}, \right.\\
&\qquad\qquad \left. |\psi_4\rangle = \begin{pmatrix} \beta \\ -\alpha \end{pmatrix}; p_i = \frac{1}{4},\ 1 \le i \le 4 \right\}. \qquad (3)
\end{aligned}
$$

Classical physics is "realistic" in the sense of Einstein, which means that any property of a classical system that one might want to measure exists prior to the measurement, and therefore the outcome of the measurement is definite (at least in principle). However, when a quantum system (say a qubit) is in a state that is well defined in one basis, say $\binom{1}{0}$ in the *rectilinear* basis $\{\binom{1}{0}; \binom{0}{1}\}$, its state is undefined in any other basis, in the following classical sense: a measurement in the *diagonal* basis $\{\binom{1/\sqrt{2}}{1/\sqrt{2}}; \binom{1/\sqrt{2}}{-1/\sqrt{2}}\}$, for instance, does not have a definite outcome that can be predicted. Repeating the same experiment several times can yield different results, even if the measurement is perfect and has no errors. Only the probabilities of possible outcomes can be calculated. This is an instance of the well-known uncertainty relations [5, §4.3].

The EPR "paradox" [6] is as follows. If Alice and Bob share a singlet, the state of Bob's particle is classically undefined by itself. Indeed, a random answer would be obtained should Bob measure his particle in any basis whatsoever. However, if Alice measures her particle in a basis of her choice, say the rectilinear or the diagonal basis defined above, she obtains full knowledge of the (pure) state of Bob's particle. Assuming that a quantum state is as "real" as the state of a classical object, and assuming that Alice's measurement cannot affect the state of Bob's particle instantaneously when Alice and Bob are far apart, Einstein, Podolsky, and Rosen (in this reinterpretation due to Bohm) concluded that the state of Bob's particle must previously have been defined in *both* bases, contradicting the uncertainty relations. From this, they concluded that there must be some deeper reality that is not captured by quantum mechanics, and therefore quantum mechanics must be incomplete. Today we know, thanks to Bell [7], that this "deeper reality" cannot exist if it is to be local and consistent with the predictions of quantum mechanics. Ironically, the EPR "paradox," together with Bell's theorem and subsequent experimental verifications of the effect predicted by quantum mechanics, has become the most convincing evidence *against* the existence of the local realistic theories that were so dear to Einstein.

We refer to the following fact as the *EPR nonlocality*: The state of Bob's particle, previously undefined, becomes completely specified by Alice's remote operation. Thus, the EPR nonlocality is *not* a nonlocality in the sense of [7], but the profound feature that allows us to "create" quantum states from different ensembles, as was discussed in the original EPR analysis [6] and in Schrödinger's subsequent paper [13].

Using the language of ρ-ensembles, EPR nonlocality is described as follows: If Alice and Bob share an EPR pair, Alice can choose whether Bob's state will be projected in ρ-ensemble E_1 or E_2, as defined in Equation (3), by choosing an appropriate measurement to perform on her share of the EPR pair. Thus, while Bob holds the completely mixed state $\rho = \frac{1}{2}I$, Alice has additional information regarding his state.

The EPR nonlocality was further generalized by Hughston, Jozsa, and Wootters [12], by allowing Alice to perform generalized measurements (POVMs). This enables her to select for Bob's particle *any* ρ-ensemble that gives rise to the same density matrix ρ, and also to learn precisely the (pure) state on which it is projected. Note, however, that she cannot choose ρ, nor the resulting state in Bob's hands, but she can choose the ρ-ensemble and learn the final state. Generating ρ-ensembles at a distance is the generalization of the EPR nonlocality, in which only standard measurements are used. We refer to this generalized EPR nonlocality as the EPR–HJW nonlocality.

In particular, Alice can create ρ-ensemble E_4 [still from Equation (3)]. We show in Section 2 that creating this ensemble corresponds to the teleportation process, provided we add the classical transmission by Alice of the outcome of her measurement. Thus, teleportation is a special case of generating ρ-ensembles at a distance, when Alice uses a specific POVM and the operations performed by Alice and Bob are independent of the parameters of the (unknown) state. We call this view of the teleportation process "TelePOVM," or "teleportation via generalized measurements." Applications to quantum cryptography are given in Section 3.

The next natural step is to use this approach to generalize the concept of teleportation by removing the requirement that the transmitted state must always be recoverable. In Section 4, we define the concept of *conclusive teleportation*. The term "conclusive" is useful in quantum information theory [5]. Consider the following scenario: You are presented with a qubit and told that it is in one of two possible nonorthogonal states. No measurement can tell you the state with certainty all the time. Some measurements will optimize your probability of making the correct guess, but those will never tell you with certainty what the state was. However, there exist conclusive measurements (also called unambiguous measurements) that will tell you what the state was with positive probability, in which case the information is always correct. Such measurements are made at the expense of spoiling the quantum state irreversibly and losing all information when the outcome is inconclusive.

Here we adapt this terminology by introducing the notion of conclusive teleportation, in which the teleportation process is successful *with some positive probability*. When Alice and Bob use an entangled pure state that is not fully entangled, our conclusive teleportation scheme allows them to teleport an unknown quantum state with a fidelity of unity, but at the price of occasional failures. As with conclusive measurements, the sender in a conclusive teleportation scheme will know whether or not teleportation has succeeded. For many applications (for instance, quantum cryptography [15–20]) one would prefer performing this conclusive teleportation rather than attempting to use directly some imperfect entanglement in the original teleportation scheme, which would lead to a teleportation fidelity smaller than unity [21]. (The fidelity of a state ρ relative to a pure state $|\psi\rangle$ is given by $\langle\psi|\rho|\psi\rangle$.) Although never published before (except in the *arXiv.org* e-Print archive *quant-ph* [22]), the concepts of TelePOVM and conclusive teleportation were discovered and presented many years ago, in the first version of this paper. Our conclusive teleportation is trivially related to the "filtering method," which makes it possible to *concentrate entanglement from a single pair* of partially entangled qubits. Indeed, given such a filtering method, Alice and Bob can create a perfect EPR pair from their partially entangled pair (with some probability of success), and, if successful, use this EPR pair for performing perfect teleportation: The net result is identical to conclusive teleportation. Conversely, using conclusive teleportation, Alice can transmit to Bob (again with some probability of success) one half of an EPR pair that she has created at her site: The net result is identical to the filtering method. The first version of this paper therefore independently reinvented a concept equivalent to the filtering method, which had been devised shortly before [23, 24]. Our subsequent version of this current paper, also "published" only in *quant-ph* [25], was written after both our conclusive teleportation and the filtering method had become well known and had been thoroughly analyzed [26].

As further generalization of the teleportation process, we can use a two-way classical communication channel and let Bob also perform a conclusive measurement. Surprisingly, we show in Section 5 that this type of process enables conclusive teleportation to succeed even when the shared entanglement is in some specific mixed state. In this case, the process yields an arbitrarily high fidelity, but the success probability goes to zero as the required fidelity goes to unity. We use the term *quasi-conclusive teleportation* for this process. The idea of performing quasi-conclusive teleportation with mixed states was first presented in [26], inspired by our concept of conclusive teleportation [22] in the first version of the current paper and by Popescu's analysis of teleportation via mixed entangled states [27]. The example of quasi-conclusive teleportation that we provide here, however, is the simplest possible because it involves only two qubits. The issue of quasi-conclusive teleportation with a fixed probability of success is discussed in [26].

Finally, we would like to stress that in the subsequent analysis, we consider only *noncollective* (or *single-pair*) protocols. These are protocols in which we never perform collective operations on two or more shared entangled pairs, as we would if we performed standard entanglement distillation [28]. It makes the eventual implementation of such protocols much more likely than that of collective protocols.

2. TelePOVM

Suppose that Alice and Bob share some two-particle entangled pure state in any dimension, such that the reduced density matrix in Bob's hands is ρ. Then, according to Hughston, Jozsa, and Wootters [12], any measurement on Alice's side, performed on her part of the entangled state, creates a specific ρ-ensemble in Bob's hands. For any fixed ρ, recall that all ρ-ensembles are indistinguishable (the density matrix fully describes whatever is observable about a quantum system) unless additional information exists somewhere. For example, in the Bennett–Brassard-84 (BB84) cryptographic scheme [15], Bob receives the same density matrix ρ whether Alice uses the rectilinear or the diagonal basis, but he receives different ρ-ensembles depending on the basis used by Alice. He cannot distinguish between the two ρ-ensembles or even obtain any information about which ρ-ensemble was used unless he receives more information from Alice. In BB84, Bob is expected to measure the qubit in a randomly chosen basis, but instead he could keep it alive in a quantum memory if he had one. Upon receiving additional information from Alice (the basis), he learns which ρ-ensemble he has. In this particular case, this allows him to perform the appropriate measurement and learn the state with certainty. Prior to receiving this information from Alice, Bob could get (at best) some probabilistic information about the state sent by Alice.

Similarly, the Bennett, Brassard, and Mermin (BBM) version [18] of Ekert's EPR scheme [17] provides a simple example of the HJW meaning of ρ-ensembles: When Alice chooses to measure her member of the singlet state in the rectilinear basis or in the diagonal basis, she "creates" a different ρ-ensemble in Bob's hands, E_1 or E_2, respectively. Bob can distinguish the two states to find Alice's bit after receiving additional information from Alice, who tells him the basis (hence her choice of a ρ-ensemble). Alice's choice of measurement determines the ρ-ensemble, and her result tells her which of the states is in Bob's hands. If the measurement is chosen in advance and Alice tells Bob its one-bit outcome, he can know precisely the state of the qubit in his hands without having to measure it.

The generalization offered by HJW replaces the standard measurement by a generalized measurement (POVM), so that the number of results can be larger than the dimension of the Hilbert space in Alice's site or in Bob's site. Thus, the HJW–EPR nonlocality argument makes it possible for the set of states that can appear at Bob's to be nonorthogonal. Furthermore, if Alice sends him additional information (the result of her measurement), Bob will know in which of these states his particle currently exists. This is a very interesting result of [12], and we now show that teleportation provides a fascinating application for it.

Let Alice and Bob share an EPR pair (say, the singlet state). Consider the following POVM $\mathcal{A}$:

$$A_1 = \frac{1}{2}|\phi_1\rangle\langle\phi_1| = \frac{1}{2}\begin{pmatrix} |\alpha|^2 & \beta\alpha^* \\ \beta^*\alpha & |\beta|^2 \end{pmatrix};$$

$$A_2 = \frac{1}{2}|\phi_2\rangle\langle\phi_2| = \frac{1}{2}\begin{pmatrix} |\beta|^2 & -\beta^*\alpha \\ -\beta\alpha^* & |\alpha|^2 \end{pmatrix};$$

$$A_3 = \frac{1}{2}|\phi_3\rangle\langle\phi_3| = \frac{1}{2}\begin{pmatrix} |\beta|^2 & \beta^*\alpha \\ \beta\alpha^* & |\alpha|^2 \end{pmatrix};$$

$$A_4 = \frac{1}{2}|\phi_4\rangle\langle\phi_4| = \frac{1}{2}\begin{pmatrix} |\alpha|^2 & -\beta\alpha^* \\ -\beta^*\alpha & |\beta|^2 \end{pmatrix}; \qquad (4)$$

with complex parameters α and β such that $|\alpha|^2 + |\beta|^2 = 1$, and with $\langle\phi_1| = (\alpha, \beta)$, $\langle\phi_2| = (\beta, -\alpha)$, $\langle\phi_3| = (\beta, \alpha)$, and $\langle\phi_4| = (\alpha, -\beta)$. These matrices have positive eigenvalues and sum up to the unit matrix; therefore they form a POVM. Following the arguments of HJW, applying such a POVM to one member of two particles in a Bell state is equivalent to a choice of a specific ρ-ensemble consisting of four possible states. If the result of the POVM is A_i, the other member of the EPR pair is projected onto a state $|\psi_i\rangle$ orthogonal to $|\phi_i\rangle$: It will be in one of the states $|\psi_1\rangle = \binom{\beta}{-\alpha}$, $|\psi_2\rangle = \binom{\alpha}{\beta}$, $|\psi_3\rangle = \binom{\alpha}{-\beta}$, or $|\psi_4\rangle = \binom{\beta}{\alpha}$, and Alice will know which one it is. Alice can send Bob two bits of information to tell him the outcome of her measurement, and this allows Bob to know the state of his qubit. Then Bob can obtain one of the states at his choice, say $\binom{\alpha}{\beta}$, by performing an appropriate rotation, according to the two classical bits he has received. Exactly two bits are required here because the POVM has four outcomes. It is crucial to notice that the POVM given by Equation (4) is applied by Alice only, and therefore Bob's operation to recover $\binom{\alpha}{\beta}$ depends only on the two classical bits and *not* on the parameters α and β. Hence, this operation can be carried out even if Bob does not know them. The process described so far does not yet quite correspond to quantum teleportation, however, because (it seems that) Alice needs to know α and β in order to perform the POVM, hence (it seems that) it does not provide a means for Alice to teleport an *unknown* quantum state to Bob.

Recall that Neumark's theorem tells us that every POVM on a system ρ_{sys} can be performed as a standard measurement provided that an appropriate ancilla is added to the system [5, 29]. Usually the state of the ancilla is known to the scientist in order to implement a known POVM. Assume now that Alice wants to teleport an unknown state $|\phi\rangle = \binom{\alpha}{\beta}$ to Bob. We have just seen that she can do that by applying POVM (4) to her half of an EPR pair shared with Bob. But how can she do this if she does not know α and β? The solution is to use the unknown state $|\phi\rangle$ as ancilla and perform a Bell measurement on the ancilla and the system. The first operator, A_1, results from the measurement of projection operator $P_1 = |\Phi^+\rangle\langle\Phi^+|$ in the Hilbert space of Alice's particle together with the ancilla. Applying the technique described in [5, §9.5], we obtain the terms of A_1 as follows:

$$(A_1)_{mn} = \sum_{rs} (P_1)_{mr,ns}(\rho_{\text{aux}})_{sr},$$

where $\rho_{\text{aux}} = |\phi\rangle\langle\phi|$ is the state of the ancilla, the mn are the indices of the particle, and the sr are those of the ancilla. The case $m = 0$, $n = 0$ corresponds to multiplying the upper left block of P_1 by the density matrix ρ_{aux} of the ancilla and computing the trace of the resulting matrix. This yields

$$\text{Tr}\begin{pmatrix} \frac{1}{2} & 0 \\ 0 & 0 \end{pmatrix}_{rs} \begin{pmatrix} |\alpha|^2 & \beta^*\alpha \\ \beta\alpha^* & |\beta|^2 \end{pmatrix}_{sr} = \frac{1}{2}|\alpha|^2,$$

which is indeed the upper left entry of A_1 in Equation (4). The $m = 1$, $n = 0$ case (second line, first column in A_1) follows from a similar multiplication but with the lower left block of P_1. In the same way, we calculated the other elements of that operator, and the other three Bell operators, and we verified that a Bell measurement on the system and the ancilla corresponds indeed to applying POVM (4) on the system.

It should be stressed again that Alice's measurement does *not* depend on the parameters α, β, and therefore these need not be known to her. Moreover, she cannot learn anything about these parameters, since all four results of her generalized measurement corresponding to POVM (4) can happen with equal probability. Also, since Alice and Bob start with a shared EPR pair, the initial state of Bob's particle is the maximally mixed state $\rho = \frac{1}{2}I$, which is the reduced state of a maximally entangled state. Thus, we see that the Bell measurement part of quantum teleportation is equivalent to the creation at a distance of the specific ρ-ensemble E_4 from Equation (3). This can be achieved even if Alice and Bob do not know the state of the ancilla [perhaps $|\phi\rangle = \binom{\alpha}{\beta}$ was chosen by someone else], and this is exactly the process of teleportation of an unknown state.

This process will also teleport a density matrix (a mixed state) or a particle entangled with some other system. It is also easy to generalize it to fully entangled states in higher dimensions, as discussed in [9].

3. Generating ρ-ensembles in quantum key distribution

To see another application of the ideas presented above, we consider a scenario taken from quantum cryptography [16]. Suppose that Alice has in mind ρ-ensemble E_3 from Equation (3), where $\rho = \frac{1}{2}I$. The four states in E_3 correspond to the four BB84 states used for quantum key distribution [15]. If Alice wants to send a sequence of random BB84 states to Bob in order to establish a secret key, and if she does not care which state she sends in each signal, she does not need to send the states at all. Instead, she sends him a member of some entangled state such that the reduced density matrix in Bob's hands is $\rho = \frac{1}{2}I$. Then she applies the appropriate POVM that creates the desired ensemble E_3 in Bob's hands. This is a reformulation of the BBM version [18] of Ekert's EPR scheme [17], in which an EPR pair is shared by Alice and Bob. We had seen earlier that Alice could create at Bob's either the $\frac{I}{2}$-ensemble E_1 or E_2, at her choice, by applying a measurement in the rectilinear or the diagonal basis on her share of the EPR pair. However, since the probability of each basis is $\frac{1}{2}$, Alice's full operation, including the choice of basis, can also be described by a POVM that leads to ρ-ensemble E_3. In this way, Alice is freed from the burden of choosing the basis: It is taken care of by nature.

Let us now present a more interesting example. Let Alice prepare the state

$$|\chi\rangle_{23} = a|0_\times 0_\times\rangle_{23} + b|1_\times 1_\times\rangle_{23},$$

where

$$|0_\times\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$$

and

$$|1_\times\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$$

are the basis states in the diagonal basis, and a and b are real numbers such that $a^2 + b^2 = 1$. Alice sends one particle from $|\chi\rangle_{23}$ to Bob and she keeps the other. Now, let Alice measure her particle using a standard measurement in the computational (rectilinear) basis. As a result, the following ρ-ensemble is generated in Bob's hands:

$$\left\{\frac{1}{\sqrt{2}}\begin{pmatrix} a+b \\ a-b \end{pmatrix}, \frac{1}{\sqrt{2}}\begin{pmatrix} a-b \\ a+b \end{pmatrix}; p_1 = p_2 = \frac{1}{2}\right\}.$$

This operation yields the Bennett-92 scheme for quantum key distribution with two non-orthogonal states [19], in the same way that the EPR scheme becomes identical to BB84 if Alice measures her share of the entanglement in randomly chosen bases.

4. Conclusive teleportation with any pure entangled state

We introduce a novel use for one-way classical communication from Alice to Bob in the teleportation process. Consider a scenario according to which Alice wants to teleport a quantum state to Bob, but she does not mind very much if it is lost in transit, provided she can tell whether or not teleportation has been successful. This can happen, for instance, if the state is known to her—perhaps it is a half EPR pair or one of the BB84 states that she has chosen herself—because then she can produce arbitrarily many copies and attempt teleporting them one by one until successful. We can also imagine situations in which Alice has many unknown quantum states and it is sufficient for her purpose if a few of them make it safely to Bob—we can think of a space probe picking up quantum dust at random here and there in the universe and teleporting some of it back to Earth for analysis. We define this process as *conclusive teleportation*. After performing a measurement that tells her whether the teleportation has succeeded, Alice uses the classical channel to tell Bob the outcome. In this way, Bob knows whether or not he can safely use the teleported state.

The most natural scenario in which conclusive teleportation is useful is when Alice and Bob share a pure entangled state that is not fully entangled, because in this case standard teleportation cannot work. Before we explore this direction, however, we point out that Alice and Bob might want to use conclusive teleportation even when they do share a fully entangled state. Let us say for instance that Alice cannot perform a full Bell measurement. Instead, she can perform a measurement that distinguishes the singlet state from the other three (triplet) states. Rather than sending two bits, she sends Bob a single bit telling him whether or not the outcome of her measurement corresponds to the singlet. In 25% of her measurements, Alice measures the singlet state, in which case she tells Bob that teleportation has been successful, and Bob does not need to perform any operation on his particle. For the other 75% of her measurements, Alice reports teleportation failure to Bob. This process could make sense if classical bits were more expensive than shared quantum states—an admittedly unlikely proposition—or if fast teleportation of arbitrary states (such as BB84 states) were required. Much more significantly, this process makes teleportation possible even when Alice or Bob are technologically limited and cannot perform the required measurements (Alice) or rotations (Bob). Linear optics, in which Alice can distinguish only some Bell states but not all of them, provides an excellent context in which this kind of conclusive teleportation is useful.

We now turn to the more interesting process of conclusive teleportation when Alice and Bob share a pure entangled state that is not fully entangled. For instance, let Alice and Bob share the state

$$|\zeta\rangle_{23} = a|00\rangle_{23} + b|11\rangle_{23}\,,$$

where a and b are real numbers such that $a^2 + b^2 = 1$ and neither a nor b is 0. This state is completely general because any entangled pure state of two qubits can be written in this form up to a possible bilateral change of basis, owing to the Schmidt decomposition [5, 12]. Let us see what happens if Alice and Bob use this state directly to teleport quantum state $|\phi\rangle_1 = \binom{\alpha}{\beta}_1$. Mimicking the method of [9], the state of the three particles is written using the Bell states in a way similar to Equation (2):

$$\begin{aligned}|\Psi\rangle_{123} &= |\phi\rangle_1|\zeta\rangle_{23} = \begin{pmatrix}\alpha\\ \beta\end{pmatrix}_1 (a|00\rangle_{23} + b|11\rangle_{23})\\ &= \frac{1}{\sqrt{2}}\left[|\Phi^+\rangle_{12}\begin{pmatrix}a\alpha\\ b\beta\end{pmatrix}_3 + |\Phi^-\rangle_{12}\begin{pmatrix}a\alpha\\ -b\beta\end{pmatrix}_3\right.\\ &\qquad \left. + |\Psi^+\rangle_{12}\begin{pmatrix}a\beta\\ b\alpha\end{pmatrix}_3 + |\Psi^-\rangle_{12}\begin{pmatrix}-a\beta\\ b\alpha\end{pmatrix}_3\right].\end{aligned}$$

If Alice and Bob were to use the standard teleportation process, a Bell measurement by Alice would still give rise to the same POVM as before. But, in contrast to the case of using a fully entangled state, the states created in Bob's hands also depend on a and b, and not only on the state of the ancilla $|\phi\rangle_1$. For example, if Alice measures $|\Phi^+\rangle$, which happens with probability $(|\alpha|^2a^2 + |\beta|^2b^2)/2$, the state of Bob's particle is projected onto

$$|\phi^{\text{out}}\rangle = \frac{1}{\sqrt{a^2|\alpha|^2 + b^2|\beta|^2}}\begin{pmatrix}a\alpha\\ b\beta\end{pmatrix}. \qquad (5)$$

If Bob wanted to retrieve the teleported state via a unitary transformation that might depend on a and b but not on unknowns α and β, he would fail because his state $|\phi^{\text{out}}\rangle$ could not be rotated back to the desired target state $|\phi\rangle = \binom{\alpha}{\beta}$. Indeed, it is easy to compute from Equation (5) that $|\phi^{\text{out}}\rangle = |\phi\rangle$ if $|\phi\rangle = \binom{1}{0}$ or if $|\phi\rangle = \binom{0}{1}$. It follows by linearity that only the identity transformation would map $|\phi^{\text{out}}\rangle$ to $|\phi\rangle$ in these two cases. But clearly, in general the identity transformation does not work, since the resulting fidelity $|\langle\phi|\phi^{\text{out}}\rangle|^2$ of the output state would be $(|\alpha|^2a + |\beta|^2b)^2/(|\alpha|^2a^2 + |\beta|^2b^2)$, which is in general smaller than 1.

We now present a different approach. We find a measurement that generates the desired states in Bob's hands with perfect fidelity. The price we pay for this perfection is that the process cannot be carried out with 100% probability of success. This yields a conclusive teleportation scheme. To explain how it works, let us return to the case of standard teleportation, with a fully entangled initial EPR pair $|\Phi^+\rangle$ available to Alice and Bob, and let us separate the Bell measurement into two measurements, one following the other:

1. A measurement that checks whether the state is in the subspace spanned by $|00\rangle$ and $|11\rangle$, or in the subspace spanned by $|01\rangle$ and $|10\rangle$. As a result, we get one classical bit, and the quantum state is projected onto the relevant subspace.
2. A measurement in the appropriate subspace—according to the result of the previous step—that measures one of the two possible Bell states in that subspace, $|\Phi^\pm\rangle$ or $|\Psi^\pm\rangle$, respectively. The outcome of this second measurement is another classical bit.

When the state is not fully entangled, such as $|\zeta\rangle_{23}$, we still follow the first step of that two-step process. To see the outcome, note that the state of the three particles can also be written as

$$\begin{aligned}|\Psi\rangle_{123} = \frac{1}{2}&\left[(a|00\rangle_{12} + b|11\rangle_{12})\begin{pmatrix}\alpha\\ \beta\end{pmatrix}_3 + (a|00\rangle_{12}\right.\\ &- b|11\rangle_{12})\begin{pmatrix}\alpha\\ -\beta\end{pmatrix}_3 + (b|01\rangle_{12} + a|10\rangle_{12})\begin{pmatrix}\beta\\ \alpha\end{pmatrix}_3\\ &\left. + (b|01\rangle_{12} - a|10\rangle_{12})\begin{pmatrix}-\beta\\ \alpha\end{pmatrix}_3\right].\end{aligned}$$

The first step projects $|\Psi\rangle_{123}$ on either the first two possibilities or the last two, with equal probability. In the second step, let us assume that the result of the first step was the subspace spanned by states $|00\rangle$ and $|11\rangle$, which we consider as basis vectors $\binom{1}{0}$ and $\binom{0}{1}$, respectively, in that subspace. (A similar analysis can easily be done for the other case, in which the result of the first step is the subspace spanned by states $|01\rangle$ and $|01\rangle$.)

In this $\{|00\rangle; |11\rangle\}$ subspace, Alice now performs a second measurement, but not in the Bell basis. Instead, Alice performs a POVM that conclusively distinguishes between the two states $\binom{a}{b} = a|00\rangle + b|11\rangle$ and $\binom{a}{-b} = a|00\rangle - b|11\rangle$, which are the first two states in the above expression. Assuming without loss of generality that $a^2 \geq b^2$, the POVM elements in that subspace are

$$A_1 = \begin{pmatrix} b^2 & ba \\ ba & a^2 \end{pmatrix}; \qquad A_2 = \begin{pmatrix} b^2 & -ba \\ -ba & a^2 \end{pmatrix};$$

$$A_3 = \begin{pmatrix} 1 - (b^2/a^2) & 0 \\ 0 & 0 \end{pmatrix}.$$

Such a POVM can never give a wrong result, and it gives an inconclusive result when the outcome is A_3. (This POVM is from [5, §§9.5, 9.6] and [30] in the context of distinguishing between the two states of the Bennett-92 quantum key distribution scheme [19].) It is the optimal process for obtaining a perfect conclusive outcome, and a conclusive result is obtained with probability $1 - (a^2 - b^2)$. In our case, this is the probability of successful teleportation. Alice tells Bob whether she succeeded in teleporting the state by sending him one bit; in addition to this bit, she still has to send Bob the two bits for distinguishing among the four possible states, so that he can perform the required rotation to retrieve the correct teleported state $|\phi\rangle = \binom{\alpha}{\beta}$. Of course, three full bits of classical communication is overkill. The communication of one five-state classical system—a *pentit*?—would suffice, with one of the states reserved to communicate teleportation failure.

When used for distinguishing between non-orthogonal states, this POVM allows us to obtain the optimal conclusive information about the state of the system. However, there are other (simpler) measurements that yield more expected *Shannon* information, at the price of not being conclusive. In the same sense, conclusive teleportation does not yield the optimal average fidelity, but the fidelity is unity when it is successful. For many applications, this is what really matters, as we have argued earlier.

The conclusive teleportation process demonstrates that any pure entangled state presents some quantum nonlocality. This fact can also be seen by applying the filtering method [23, 24] to pure states.

5. Arbitrarily good conclusive bilocal teleportation via mixed states

In a perfect conclusive teleportation, as described in the previous section, Alice performs a teleportation process that is sometimes successful, and when it is successful, the fidelity of the teleported state is unity. In an imperfect conclusive teleportation, Alice performs a teleportation process that is sometimes successful, and even when it *is* successful, the fidelity of the teleported state is less than unity, but still better than anything that could be achieved with a standard teleportation.

The original idea of teleportation involves only one-way classical communication from Alice to Bob. We now extend this concept[1] by allowing two-way communication between Alice and Bob, resulting in a *bilocal* protocol. For simplicity, we do not consider the most general type of bilocal protocols—the so-called *ping-pong* protocols [31]. We only allow Alice and Bob to operate independently of each other's operations. A ping-pong protocol could improve the probability of success [i.e., increase the $p'(p)$ described below] by allowing several "paths" of successful distillation depending on the outcomes of the measurements in each step of the protocol. In our protocol, communication is used only to verify that the state has been teleported. This generalization of teleportation makes sense, since in many cases classical communication is treated as a free or very inexpensive resource.

We have shown in the previous section that perfectly reliable conclusive teleportation can be achieved when pure entangled states are shared. We now show that it is possible to perform arbitrarily good bilocal conclusive teleportation when some mixed states are used. Arbitrarily good conclusive teleportation, which we call "quasi-conclusive teleportation," is not described by a particular POVM, $\mathcal{A} = \{A_1, \cdots, A_m\}$, but by a series of POVMs, $\mathcal{A}^n = \{A_1(n), \cdots, A_m(n)\}$, where n is the index of this series. For any ε, we can find an n such that POVM $\mathcal{A}^n$ yields conclusive teleportation fidelity better than $1 - \varepsilon$ when successful. However, perfect fidelity cannot be achieved because the success probability goes to zero as ε goes to zero. Thus, we show that quasi-conclusive teleportation can be achieved successfully when an appropriate mixed state is available as an entanglement resource for Alice and Bob.

We first distill [28] the mixed state and then use it for teleportation. Consider the state

$$\rho_p = p|\Psi^-\rangle\langle\Psi^-| + (1-p)|00\rangle\langle 00| \qquad 0 < p < 1,$$

[1] The most general teleportation channel involving all local quantum operations plus two-way classical communication (LQCC) protocols was introduced in [26]. That paper also introduced the concepts of quasi-distillation and arbitrarily good teleportation via mixed states for spin-1 states.

which is a mixture of a singlet (with probability p) and a $|00\rangle$ state (with complementary probability $1 - p$). Let the bilocal action of Alice and Bob be described in the following way, where V_1 and W_1 are specified later [in Equation (7)]:

$$\rho_p \to \rho' \equiv \frac{V_1 \otimes W_1(\rho) V_1^\dagger \otimes W_1^\dagger}{\mathrm{Tr}\,(V_1 \otimes W_1(\rho) V_1^\dagger \otimes W_1^\dagger)}. \tag{6}$$

This can be realized by Alice and Bob performing independent generalized measurements. More precisely, Alice performs the measurement defined by the pair of operators

$$\{V_1, V_2 \equiv \sqrt{I - V_1 V_1^\dagger}\}$$

and Bob performs the measurement defined by the pair of operators

$$\{W_1, W_2 \equiv \sqrt{I - W_1 W_1^\dagger}\}.$$

In other words, Alice's POVM is the set $\mathcal{A} = \{A_1 = V_1^\dagger V_1, A_2 = V_2^\dagger V_2\}$ and Bob's POVM is the set $\mathcal{B} = \{B_1 = W_1^\dagger W_1, B_2 = W_2^\dagger W_2\}$. When the outcome of both Alice and Bob is 1, which corresponds to the first operator in each lab (V_1 and W_1, respectively), transformation (6) has been successfully achieved.

After receiving the result of their measurements, Alice and Bob communicate classically in order to keep only those particles for which both results correspond to the successful case. To show that quasi-conclusive teleportation can be performed, we define the sequence of POVM operators:

$$V_1(n) = W_1(n) = \begin{pmatrix} 1/n & 0 \\ 0 & 1 \end{pmatrix}. \tag{7}$$

After the action of the corresponding POVM, the new state is

$$\rho' = \rho_{p'} \equiv p'|\Psi^-\rangle\langle\Psi^-| + (1 - p')|00\rangle\langle 00|,$$

with the parameter p' depending on the input parameter p as follows:

$$p'(p) = \frac{1}{1 + \dfrac{1-p}{np}}.$$

The probability of successful transition from ρ_p to $\rho_{p'}$ is

$$P_{p \to p'} = \frac{1 + (n-1)p}{n^2}.$$

Thus, one can produce a state that has arbitrarily good fidelity, $F(\rho_p) = \langle\Psi_{12}^-|\rho_p|\Psi_{12}^-\rangle$, with respect to a perfect singlet, which obviously makes possible arbitrarily good conclusive teleportation. Unfortunately, the probability of successful teleportation decreases to zero when fidelity goes to unity. Nevertheless, the probability of success remains positive even if the required fidelity level is arbitrarily close to perfection.

One natural question is whether or not it is possible to make teleportation arbitrarily good by the use of other mixed states. We do know, however, that there are entangled mixed states that *cannot* be used for arbitrarily faithful quasi-conclusive teleportation. Indeed, in the case of Werner states—states in which one fully entangled state is mixed with the completely mixed state—arbitrarily good conclusive distillation is known to be impossible [32], and it follows that arbitrarily faithful quasi-conclusive teleportation is impossible as well. In fact, the entanglement fidelity (the fidelity relative to a fully entangled state) cannot be increased for those states: The best value $F_{\max}$ is the same as the initial value F_0 before the conclusive process. Thus, following [26], the maximal conclusive teleportation fidelity is equal to $(2F_0 + 1)/3$, which is less than unity except for the trivial case in which the initial state is fully entangled.

It has recently been discovered that quasi-conclusive teleportation via mixed states is impossible if we are restricted to one-way communication. This will be the subject of a subsequent paper.

6. Concluding remarks

In this paper, we have presented a new way of viewing the teleportation of an unknown quantum state. We have shown that teleportation is a special and particular case of generating ρ-ensembles at a distance, hence a special case of generalized EPR nonlocality—the HJW–EPR nonlocality. We believe that this view of teleportation reduces some of the mystery of that process. In particular, it sheds light on why two classical bits suffice for the teleportation of a qubit. We have also demonstrated the usefulness of the HJW-generalized EPR nonlocality, and of understanding that any ρ-ensemble can be generated nonlocally. We believe that understanding the connection between these two important forms of nonlocality significantly improves our understanding of entanglement.

On the basis of the connection between teleportation and generalized measurements, we have presented the process of conclusive teleportation, a teleportation process that is successful with positive probability. We have shown that any pure entangled state can be used to conclusively teleport an arbitrary qubit with fidelity of unity. More surprisingly, some mixed states can also be used to achieve the quasi-conclusive teleportation of one qubit with fidelity arbitrarily close to unity.

Acknowledgments

The work of G. B. is supported in part by grants from Canada's NSERC, Québec's FQRNT, the Canada Research Chair program, the MITACS Network of

Centres of Excellence, and the Canadian Institute for Advanced Research. The work of P. H. is supported by Grant No. 2PO3B 103 16 from the Polish Committee for Scientific Research. The work of T. M. is supported in part by the Israel MOD Research and Technology Unit. We are grateful to Asher Peres of Technion for helpful discussions and to an anonymous referee for pointing out a mistake in the submitted version of this paper. Part of the work described in this paper was done at the AQIP'99 conference.

References

1. C. H. Bennett and P. W. Shor, "Quantum Information Processing," *IEEE Trans. Info. Theory* **44,** 2724–2742 (1998).
2. M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press, Cambridge, England, 2000.
3. J. Gruska, *Quantum Computing*, McGraw-Hill Book Co., Inc., New York, 2000.
4. C. W. Helstrom, *Quantum Detection and Estimation Theory*, Academic Press, Inc., New York, 1976.
5. A. Peres, *Quantum Theory: Concepts and Methods*, Kluwer Academic Publishers, Dordrecht, the Netherlands, 1993.
6. A. Einstein, B. Podolsky, and N. Rosen, "Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?", *Phys. Rev.* **47,** 777–780 (1935).
7. J. S. Bell, "On the Einstein–Podolsky–Rosen Paradox," *Physics* **1,** 195–200 (1964).
8. S. L. Braunstein, A. Mann, and M. Revzen, "Maximal Violation of Bell Inequalities for Mixed States," *Phys. Rev. Lett.* **68,** 3259–3261 (1992).
9. C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, "Teleporting an Unknown Quantum State Via Dual Classical and Einstein–Podolsky–Rosen Channels," *Phys. Rev. Lett.* **70,** 1895–1899 (1993).
10. C. M. Caves, "Quantum Teleportation—A Tale of Two Cities," *Science* **282,** 637–638 (1998).
11. G. Brassard, S. Braunstein, and R. Cleve, "Teleportation as a Quantum Computation," *Physica D* **120,** 43–47 (1998).
12. L. P. Hughston, R. Jozsa, and W. K. Wootters, "A Complete Classification of Quantum Ensembles Having a Given Density Matrix," *Phys. Lett. A* **183,** 14–18 (1993).
13. E. Schrödinger, "Probability Relations Between Separated Systems," *Proc. Cambridge Phil. Soc.* **32,** 446–452 (1936).
14. N. Gisin, "Stochastic Quantum Dynamics and Relativity," *Helv. Phys. Acta* **62,** 363–371 (1989).
15. C. H. Bennett and G. Brassard, "Quantum Cryptography: Public Key Distribution and Coin Tossing," *Proceedings of the International IEEE Conference on Computers, Systems and Signal Processing*, Bangalore, India, 1984, pp. 175–179.
16. C. H. Bennett, G. Brassard, and A. K. Ekert, "Quantum Cryptography," *Sci. Amer*. **267,** No. 4, 50–57 (October 1992).
17. A. K. Ekert, "Quantum Cryptography Based on Bell's Theorem," *Phys. Rev. Lett.* **67,** 661–663 (1991).
18. C. H. Bennett, G. Brassard, and N. D. Mermin, "Quantum Cryptography Without Bell's Theorem," *Phys. Rev. Lett.* **68,** 557–559 (1992).
19. C. H. Bennett, "Quantum Cryptography Using Any Two Nonorthogonal States," *Phys. Rev. Lett.* **68,** 3121–3124 (1992).
20. E. Biham, B. Huttner, and T. Mor, "Quantum Cryptographic Network Based on Quantum Memories," *Phys. Rev. A* **54,** 2651–2658 (1996).
21. N. Gisin, "Nonlocality Criteria for Quantum Teleportation," *Phys. Lett. A* **210,** 157–159 (1996).
22. T. Mor, "TelePOVM—New Faces of Teleportation"; see *http://arXiv.org/abs/quant-ph/9608005/*; presented at the workshop, "A Golden Jubilee event of the TIFR on the Foundation of Quantum Theory" (no proceedings), Tata Institute of Fundamental Research (TIFR), Bombay, India, September 1996.
23. N. Gisin, "Hidden Quantum Nonlocality Revealed by Local Filters," *Phys. Lett. A* **210,** 151–156 (1996).
24. C. H. Bennett, H. Bernstein, S. Popescu, and B. Schumacher, "Concentrating Partial Entanglement by Local Operations," *Phys. Rev. A* **53,** 2046–2052 (1996).
25. T. Mor and P. Horodecki, "Teleporting Via Generalized Measurements, and Conclusive Teleportation"; see *http://arXiv.org/abs/quant-ph/9906039/*; 1999.
26. M. Horodecki, P. Horodecki, and R. Horodecki, "General Teleportation Channel, Singlet Fraction and Quasi-Distillation," *Phys. Rev. A* **60,** 1888–1898 (1999).
27. S. Popescu, "Bell's Inequalities Versus Teleportation: What Is Nonlocality?" *Phys. Rev. Lett.* **72,** 797–799 (1994).
28. C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin, and W. K. Wootters, "Purification of Noisy Entanglement and Faithful Teleportation Via Noisy Channels," *Phys. Rev. Lett.* **76,** 722–725 (1996).
29. A. Peres, "How to Differentiate Between Non-Orthogonal States," *Phys. Lett. A* **128,** 19 (1988).
30. A. K. Ekert, B. Huttner, G. M. Palma, and A. Peres, "Eavesdropping on Quantum-Cryptographical Systems," *Phys. Rev. A* **50,** 1047–1056 (1994).
31. A. Peres and W. K. Wootters, "Optimal Detection of Quantum Information," *Phys. Rev. Lett.* **66,** 1119–1122 (1991).
32. N. Linden, S. Massar, and S. Popescu, "Purifying Noisy Entanglement Requires Collective Measurements," *Phys. Rev. Lett.* **81,** 3279–3282 (1998).

Received July 15, 2003; accepted for publication September 3, 2003

Gilles Brassard *Département IRO, Université de Montréal, C.P. 6128, Succursale Centre-Ville, Montréal (Québec), H3C3J7 Canada (brassard@iro.umontreal.ca).* In 1979, Dr. Brassard received a Ph.D. degree in theoretical computer science from Cornell University, where he focused on the use of oracles in public-key cryptography. He joined the Université de Montréal in 1979 and was promoted to the rank of Full Professor in 1988. His interests include all aspects of quantum information processing, which lies at the intersection of computer science and quantum mechanics. Among his main achievements are the co-invention of quantum cryptography, privacy amplification, quantum teleportation, and quantum entanglement distillation. He has received numerous recognitions throughout his career, such as the Steacie Fellowship (1992), the Prix Urgel-Archambault (1992), the Steacie Prize (1994), Scientist of the Year (La Presse, 1995), the Killam Research Fellowship (1997), and the Prix Marie-Victorin (2000). Dr. Brassard is a Fellow of the Royal Society of Canada (1996), a foreign member of the Latvian Academy of Sciences (1998), Canada Research Chair in Quantum Information Processing (2001), and a Fellow of the Canadian Institute for Advanced Research (2002).

Paweł Horodecki *Faculty of Applied Physics and Mathematics, Gdańsk University of Technology, 80-952 Gdańsk, Poland (pawel@mifgate.mif.pg.gda.pl).* Dr. Horodecki graduated from the University of Gdańsk in 1995 and earned a Ph.D. degree from the Technical University of Gdańsk in 1999. His research interests are in quantum information theory and the foundations of quantum physics. He received a Foundation for Polish Science Fellowship in 1998 and a DAAD Research Fellowship (Hanover) in 1999, and was Fujitsu Visiting Professor of DAMTP in Cambridge University in 2003. Dr. Horodecki is a coauthor of *Quantum Information* (Springer-Verlag, 2001). His primary achievements include pioneering research on the entanglement of mixed states, in particular, *bound entanglement*.

Tal Mor *Computer Science Department, Technion – Israel Institute of Technology, 32000, Israel (talmo@cs.technion.ac.il).* Dr. Mor received an M.Sc. degree from Tel-Aviv University (Israel) in 1993, and a Ph.D. (more precisely, D.Sc.) degree from Technion (Haifa, Israel) in 1997. Subsequently, he did postdoctoral work on all aspects of quantum information processing at the Université de Montréal (Québec, Canada) and the University of California at Los Angeles. He is currently a faculty member in the Computer Science Department at Technion. Dr. Mor's current research activities include work on entanglement and other nonclassical aspects of quantum computing and communication, on the security of quantum cryptography (theory and practice), and on various practical aspects and short-term applications of quantum computing.