Superbroadcasting of Mixed States

Giacomo Mauro D'Ariano,* Chiara Macchiavello,† and Paolo Perinotti‡

INFM, unità di Pavia and Dipartimento di Fisica "A. Volta," QUIT Group§, via Bassi 6, I-27100 Pavia, Italy

(Received 28 February 2005; published 5 August 2005)

We derive the optimal universal broadcasting for mixed states of qubits. We show that the no-broadcasting theorem cannot be generalized to more than a single input copy. Moreover, for four or more input copies it is even possible to purify the input states while broadcasting. We name such purifying broadcasting *superbroadcasting*.

DOI: 10.1103/PhysRevLett.95.060503 PACS numbers: 03.67.Hk, 03.65.−w

Broadcasting—namely, distributing information over many users—suffers in-principle limitations when the information is quantum, and this poses a critical issue in quantum information theory for distributed processing and networked communications. For pure states an ideal broadcasting coincides with the so-called *quantum cloning*, corresponding to an ideal device capable of producing from a finite number N of copies of the same state $|\psi\rangle$ a larger number $M > N$ of output copies of the same state, for a given set of input states. Since such a transformation is not isometric, it cannot be achieved by any physical machine on a generally nonorthogonal set of states (this is essentially the content of the *no-cloning* theorem [1–3]). The situation is more involved when the states are mixed, since from the point of view of each single user, the local mixed state is indistinguishable from the partial trace of an entangled state, and there are infinitely many joint states corresponding to ideal broadcasting. For this reason in the literature [4] the word *broadcasting* is used technically to denote a map whose output has identical local states, versus the word *cloning* used for the case of tensor product of identical states.

Since ideal cloning is not possible, the quantum information encoded on pure states can be broadcast only approximately, and this posed the problem of optimizing the broadcasting, e.g., by maximizing an input-output fidelity equally well on all pure states. In the literature this kind of optimized broadcasting is called *optimal universal cloning* [5–8]. For mixed states the no-cloning theorem is not logically sufficient to forbid ideal broadcasting. In Ref. [4] the impossibility of broadcasting has been proved in the case of one input copy and two output copies for a set of density operators generally nonmutually commuting. Later, in the literature (see, for example, Ref. [9]) this result has been often implicitly considered as the generalization of the no-cloning theorem to the case of mixed input states. In the present Letter we will show that this assertion cannot be generalized to more than a single input copy. In particular, for numbers of input copies $N \geq 4$ the no-broadcasting theorem does not hold, and it is even possible to purify while broadcasting. We named such a procedure *superbroadcasting* (see Fig. 1).

We now present the theoretical derivation of our result.

Let us consider a general broadcasting channel from N to M copies, namely, a completely positive (CP) trace-preserving map from states on $\mathcal{H}_{\text{in}} \doteq \mathcal{H}^{\otimes N}$ to states on $\mathcal{H}_{\text{out}} \doteq \mathcal{H}^{\otimes M}$ that is invariant under permutations of input copies and of output copies. Moreover, we take the broadcasting to be universal, namely, the broadcasting map B is covariant under the group of unitary transformations of $\mathcal{H}$, more precisely,

$$\mathrm{B}\,(U^{\otimes N}\rho^{\otimes N}U^{\dagger\otimes N}) = U^{\otimes M}\mathrm{B}(\rho^{\otimes N})U^{\dagger\otimes M}. \tag{1}$$

We will restrict attention to qubits, namely $\mathcal{H} \simeq \mathbb{C}^2$. Upon using the Choi-Jamiolkowsky representation [10]

$$R_{\mathrm{B}} = \mathrm{B} \otimes \mathrm{I}(|I\rangle\rangle\langle\langle I|), \qquad \mathrm{B}(Q) = \mathrm{Tr}_{\text{in}}[(I_{\text{out}} \otimes Q^{\tau})R_{\mathrm{B}}], \tag{2}$$

where Q denotes a state on $\mathcal{H}_{\text{in}}$, and R_{B} is a positive operator on $\mathcal{H}_{\text{out}} \otimes \mathcal{H}_{\text{in}}$, the covariance condition (1) is equivalent to invariance of R_{B} under the group representation $U_g^{\otimes M} \otimes U_g^{*\otimes N}$, U_g denoting the $j = \frac{1}{2}$ representation, for $g \in \mathbb{SU}(2)$ [the symbol $|I\rangle\rangle$ denotes the maximally entangled vector $|I\rangle\rangle = \sum_n |n\rangle \otimes |n\rangle$, and the superscript τ denotes transposition with respect to the orthonormal basis $\{|n\rangle\}$]. In the Choi-Jamiolkowsky representation the trace-preserving condition on the CP map reads

$$\mathrm{Tr}_{\text{out}}[R_{\mathrm{B}}] = I_{\text{in}}, \tag{3}$$

where I_{in} denotes the identity on $\mathcal{H}_{\text{in}}$. For the unitary group $\mathbb{SU}(2)$ the complex conjugate representation of any unitary representation, say, V_g, is unitarily equivalent to the direct representation, i.e., $V_g^* = CV_gC^{\dagger}$, under the π-rotation C around the y axis. The explicit form of C actually depends on the particular representation V_g: for the tensor representation $U_g^{\otimes N}$ one has $C \equiv i\sigma_y^{\otimes N}$. It is then convenient to rewrite the map as follows

$$\mathrm{B}\,(Q) = \mathrm{Tr}_{\text{in}}[(I_{\text{out}} \otimes \tilde{Q})S_{\mathrm{B}}] \tag{4}$$

with

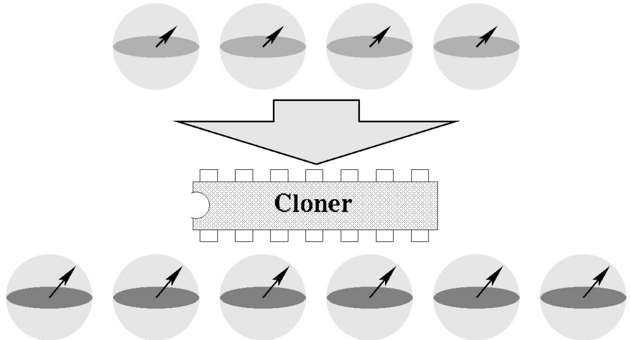

FIG. 1. With four or more input copies the no-broadcasting theorem can be violated. One can actually increase the purity of local states while broadcasting, corresponding to a stretching of the Bloch vector. In this purifying broadcasting mechanism, called *superbroadcasting*, the available information on the state of the input copies cannot increase due to the detrimental correlations among the output copies.

$$\tilde{Q} \doteq CQ^\tau C^\dagger, \qquad S_\mathrm{B} \doteq (I_\mathrm{out} \otimes C) R_\mathrm{B} (I_\mathrm{out} \otimes C^\dagger), \tag{5}$$

and now covariance of the CP map B corresponds to invariance of S_B under the representation $U_g^{\otimes(N+M)}$. A tensor product representation $U_g^{\otimes L}$ decomposes into irreducible components according to the Wedderburn decomposition of spaces

$$\mathcal{H}^{\otimes L} = \bigoplus_{j=\langle\langle L/2\rangle\rangle}^{L/2} \mathcal{H}_j \otimes \mathbb{C}^{d_j}, \tag{6}$$

where $\langle\langle x\rangle\rangle$ denotes the fractional part of x (i.e., $\langle\langle L/2\rangle\rangle = 0$ for L even and $\langle\langle L/2\rangle\rangle = 1/2$ for L odd), and the multiplicity d_j can be evaluated by recurrence on L by adding a qubit at a time, giving $d_j = \frac{2j+1}{L/2+j+1}\binom{L}{L/2+j}$ [11]. Equation (6) is also called *Clebsch-Gordan series*. The spaces $\mathcal{H}_j$ and $\mathbb{C}^{d_j}$ are called *representation* and *multiplicity* spaces, respectively. With the above decomposition the group representation writes $U_g^{\otimes L} = \oplus_{j=\langle\langle L/2\rangle\rangle}^{L/2} U_g^{(j)} \otimes I_{d_j}$, whereas an operator invariant under $U_g^{\otimes L}$ has the form $\oplus_{j=\langle\langle L/2\rangle\rangle}^{L/2} I_j \otimes W^{(j)}$, I_j denoting the identity over the representation space $\mathcal{H}_j$, and $W^{(j)}$ an operator on the multiplicity space $\mathbb{C}^{d_j}$. On the other hand, an operator invariant under the permutation group $\mathbb{P}_L$ of the L copies of the representation has the form $\oplus_{j=\langle\langle L/2\rangle\rangle}^{L/2} Z_j \otimes I_{d_j}$, where Z_j is any operator on the representation space $\mathcal{H}_j$ (this is the so-called Schur-Weyl duality) [12]. Since the operator S_B is invariant under $\mathbb{P}_M \times \mathbb{P}_N$ it must be of the form $S_\mathrm{B} = \oplus_{j=\langle\langle M/2\rangle\rangle}^{M/2} \oplus_{l=\langle\langle N/2\rangle\rangle}^{N/2} S_{jl} \otimes I_{d_j} \otimes I_{d_l}$, where S_{jl} is a positive operator over $\mathcal{H}_j \otimes \mathcal{H}_l$. By further decomposing $\mathcal{H}_j \otimes \mathcal{H}_l = \oplus_{J=|j-l|}^{j+l} \mathcal{H}_J$ into invariant subspaces and imposing invariance of S_B under $U_g^{\otimes(M+N)}$, one obtains the general form

$$S_\mathrm{M} = \bigoplus_{j=\langle\langle M/2\rangle\rangle}^{M/2} \bigoplus_{l=\langle\langle N/2\rangle\rangle}^{N/2} \bigoplus_{J=|j-l|}^{j+l} s_{j,l,J} P_J^{(j,l)} \otimes I_{d_j} \otimes I_{d_l}, \tag{7}$$

for positive coefficients $s_{j,l,J}$, $P_J^{(j,l)}$ denoting the orthogonal projector over the irreducible representation J coming from the couple j, l.

The trace preservation condition is now equivalent to

$$\mathrm{Tr}_\mathrm{out}[S_\mathrm{M}] = \sum_{j=\langle\langle M/2\rangle\rangle}^{M/2} \bigoplus_{l=\langle\langle N/2\rangle\rangle}^{N/2} \times \mathrm{Tr}_j\left[\bigoplus_{J=|j-l|}^{j+l} d_j s_{j,l,J} P_J^{(j,l)}\right] \otimes I_{d_l} = I_\mathrm{in}. \tag{8}$$

Since $\mathrm{Tr}_j[P_J^{(j,l)}]$ is invariant under $U_g^{(l)}$, one can easily see that $\mathrm{Tr}_j[P_J^{(j,l)}] = \frac{2J+1}{2l+1} I_l$, whence the latter condition becomes

$$\bigoplus_{l=\langle\langle N/2\rangle\rangle}^{N/2} \sum_{j=\langle\langle M/2\rangle\rangle}^{M/2} \sum_{J=|j-l|}^{j+l} d_j s_{j,l,J} \frac{2J+1}{2l+1} I_l \otimes I_{d_l} = I_\mathrm{in}, \tag{9}$$

namely,

$$\sum_{j=\langle\langle M/2\rangle\rangle}^{M/2} \sum_{J=|j-l|}^{j+l} d_j s_{j,l,J} \frac{2J+1}{2l+1} = 1, \qquad \forall\ \langle\langle N/2\rangle\rangle \le l \le \frac{N}{2}, \tag{10}$$

with positive coefficients $s_{j,l,J}$.

Upon writing the input state $\tilde{Q} = \tilde{\rho}^{\otimes N}$ in the Bloch vector form, we have the decomposition

$$\tilde{\rho}^{\otimes N} = \left[\tfrac{1}{2}(I - r\vec{k}\cdot\vec{\sigma})\right]^{\otimes N} = (r_+ r_-)^{N/2} \bigoplus_{l=\langle\langle N/2\rangle\rangle}^{N/2} \sum_{n=-l}^{l} \left(\frac{r_-}{r_+}\right)^n |ln\rangle\langle ln| \otimes I_{d_l}, \tag{11}$$

where $0 \le r \le 1$, and $r_\pm \doteq \frac{1}{2}(1 \pm r)$, and $|ln\rangle$ denotes the eigenstate of the angular momentum component $\vec{k}\cdot\vec{J}^{(l)}$ with eigenvalue n. From Eq. (10) we see that the broadcasting channels from N to M make a convex set, with the extreme points classified by functions φ and Φ corresponding to a given choice $j = \varphi(l)$, $J = \Phi(l)$, namely, to the choice of coefficients

$$s_{j,l,J}^{(\varphi,\Phi)} = \frac{2l+1}{2J+1} \frac{1}{d_j} \delta_{j,\varphi(l)} \delta_{J,\Phi(l)}, \tag{12}$$

or to the Choi-Jamiolkowsky operator

$$S_\mathrm{M}^{(\varphi,\Phi)} = \bigoplus_{l=\langle\langle N/2\rangle\rangle}^{N/2} \frac{2l+1}{2\Phi(l)+1} \frac{1}{d_{\varphi(l)}} P_{\Phi(l)}^{(\varphi(l),l)} \otimes I_{d_{\varphi(l)}} \otimes I_{d_l}. \tag{13}$$

Using the expression (13) for extremal broadcasting channels and Eq. (11) for the input state we can evaluate the output state

$$\mathrm{M}_{(\varphi,\Phi)}(\rho^{\otimes N}) = (r_+ r_-)^{N/2} \bigoplus_{l=\langle\langle N/2\rangle\rangle}^{N/2} \frac{2l+1}{2\Phi(l)+1} \frac{1}{d_{\varphi(l)}} \sum_{n=-l}^{l} \left(\frac{r_-}{r_+}\right)^n \mathrm{Tr}_l \left[(I_{\varphi(l)} \otimes |ln\rangle\langle ln|) P_{\Phi(l)}^{(\varphi(l),l)}\right] \otimes I_{d_{\varphi(l)}}. \tag{14}$$

In terms of Clebsch-Gordan coefficients, this can be rewritten as

$$\mathrm{M}_{(\varphi,\Phi)}(\rho^{\otimes N}) = (r_+ r_-)^{N/2} \sum_{l=\langle\langle N/2\rangle\rangle}^{N/2} \frac{2l+1}{2\Phi(l)+1} \frac{d_l}{d_{\varphi(l)}} \sum_{n=-l}^{l} \left(\frac{r_-}{r_+}\right)^n \sum_{m=-\varphi(l)}^{\varphi(l)} \langle \Phi(l)m+n|\varphi(l)m, ln\rangle^2 |\varphi(l)m\rangle\langle\varphi(l)m| \otimes I_{d_{\varphi(l)}}. \tag{15}$$

Now, we are interested in the single output copy, which is the broadcast state. This is given by the partial trace of Eq. (15) over $M-1$ copies. The evaluation of the partial trace needs the matching between the Wedderburn decomposition and the qubit tensor product representation. According to the Schur-Weyl duality the multiplicity space of the Wedderburn decomposition supports a unitary irreducible representation of the permutation group $\mathbb{P}_M$ of the M qubits. Therefore, one has the identity for any operator X_j on $\mathcal{H}_j \otimes \mathbb{C}^{d_j}$

$$\sum_{l\in\mathbb{P}_M} \pi_l X_j \pi_l^\dagger = \frac{M!}{d_j} \mathrm{Tr}_{\mathbb{C}^{d_j}} [X_j] \otimes I_{d_j}, \tag{16}$$

where π_l denotes the generic permutation. In particular, for $X_j = |jm\rangle\langle jm| \otimes |1\rangle\langle 1|$, $|1\rangle$ denoting any fixed vector of $\mathbb{C}^{d_j}$, one has

$$|jm\rangle\langle jm| \otimes I_{d_j} = \frac{d_j}{M!} \sum_{l\in\mathbb{P}_M} \pi_l X_j \pi_l^\dagger. \tag{17}$$

Clearly, one can always choose the given vector of the irreducible representation as [11]

$$|jm\rangle \otimes |1\rangle = |jm\rangle \otimes |\Psi_-\rangle^{\otimes (M/2)-j}, \tag{18}$$

where $|\Psi_-\rangle$ denotes the singlet. We can then take the partial trace of both sides of Eq. (17). For each permutation, say, π_s, which exchanges the last qubit with one belonging to a singlet, one has $\mathrm{Tr}_{M-1}[\pi_s X_j \pi_s^\dagger] = \frac{I}{2}$, and we have $(M-2j)(M-1)!$ permutations of this kind. On the other hand, for each permutation, say, π_m, which exchanges the last qubit with one belonging to the j multiplet, one has $\mathrm{Tr}_{M-1}[\pi_m X_j \pi_m^\dagger] = \mathrm{Tr}_{j-(1/2)}[|jm\rangle \times \langle jm|]$ and there are $2j(M-1)!$ permutations of this kind. Using the explicit form of the Clebsch-Gordan coefficients one can derive the following identity

$$\mathrm{Tr}_{j-(1/2)}[|jm\rangle\langle jm|] = \frac{1}{2} I + \frac{m}{2j} \vec{k} \cdot \vec{\sigma}. \tag{19}$$

Substituting the above formula when performing the partial trace of both sides of Eq. (17), one obtains the following expression for the single copy output density operator

$$\rho'_{(\varphi,\Phi)}(r) = (r_+ r_-)^{N/2} \times \sum_{l=\langle\langle N/2\rangle\rangle}^{N/2} \frac{2l+1}{2\Phi(l)+1} d_l \sum_{m=-\varphi(l)}^{\varphi(l)} \sum_{n=-l}^{l} \left(\frac{r_-}{r_+}\right)^n \times \langle \Phi(l)m+n|\varphi(l)m, ln\rangle^2 \frac{1}{2}\left(I + \frac{2m}{M} \vec{k} \cdot \vec{\sigma}\right). \tag{20}$$

We are now in position to analyze the broadcast state, in particular, its Bloch vector. In Eq. (20) we see that the input and the output Bloch vectors are parallel, and clearly $[\rho', \rho] = 0$. On the other hand, the length of the output Bloch vector is given by

$$r'_{(\varphi,\Phi)}(r) = (r_+ r_-)^{N/2} \sum_{l=\langle\langle N/2\rangle\rangle}^{N/2} \frac{2l+1}{2\Phi(l)+1} d_l \sum_{m=-\varphi(l)}^{\varphi(l)} \times \sum_{n=-l}^{l} \left(\frac{r_-}{r_+}\right)^n \langle \Phi(l)m+n|\varphi(l)m, ln\rangle^2 \frac{2m}{M}. \tag{21}$$

We are now interested in maximizing the length of the output Bloch vector. Since r' is linear on the convex set of broadcasting channels, we just need to consider extremal maps and look for the maximum $r'_{\mathrm{opt}}(r) = \max_{(\varphi,\Phi)}\{r'_{(\varphi,\Phi)}(r)\}$. It is possible to prove [13] that the maximal $r'_{(\varphi,\Phi)}(r)$ is achieved for $\varphi(l) = M/2$ and for $\Phi(l) = |l - \frac{M}{2}|$, independently of r. For pure states these optimal maps coincide with those of optimal universal cloning transformations [5–8]. Also, it can be shown [13] that our optimal map gives the same results achievable using the procedure of Ref. [11].

As an example, in Fig. 2 we plot the *scaling factor* $p(r) = r'_{\mathrm{opt}}(r)/r$ for the maps maximizing r' for $N = 5$ and several values of M. One can see that for a wide range of values of r, one has $p(r) \geq 1$. This corresponds to a purification of the local states, and since one also has a number of copies at the output $M > N$ greater than the number of inputs, it is actually a broadcasting with simultaneous purification, what we call *superbroadcasting*. Clearly, for $M \leq N$ one has more purification than for $M > N$, corresponding to the purification protocol [11]. The superbroadcasting occurs for $N \geq 4$ input copies. As a rule, one has purification below some value $r_*(N, M)$ of the input purity for a bounded number $M \leq M_*(N)$ of the output copies. In Fig. 3 we plot $r_*(N, N+1)$ and $r_*(N, M_*(N))$ versus the number of input copies N. After

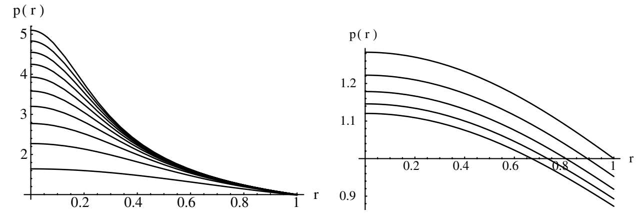

FIG. 2. The scaling factor $p(r)$ vs r. On the left: for $M = N + 1$ and $N = 10, 20, 30, 40, 50, 60, 70, 80, 90, 100$ (from the bottom to the top). On the right: for $N = 5$ and $5 \leq M \leq 9$ (from the top to the bottom).

the threshold at $N = 4$ corresponding to $r_*(4, 5) = 0.787$, one has a monotonic increase of $r_*(N, N + 1)$ and $r_*(N, M_*(N))$ toward asymptotic purity, with power laws $2N^{-2}$ and N^{-1}, respectively. For larger M one has a generally higher threshold for N, and smaller values of $r_*(N, M)$. For $N = 4$ one has superbroadcasting for up to $M = 7$, for $N = 5$ up to $M = 21$, and for $N = 6$ up to $M = \infty$. Notice that perfect broadcasting [corresponding to $p(r) = 1$] can be achieved under the same conditions of superbroadcasting (clearly generally by a different map). We remind the reader that we have considered broadcasting of universally covariant sets of mixed states. Indeed, for smaller sets of input states it can be shown that superbroadcasting is possible also for $N = 3$ input copies (as for equatorial phase-covariant mixed states [13]), and, for even smaller sets, one cannot exclude superbroadcasting also for $N = 2$.

In conclusion, we have derived the optimal universal broadcasting for mixed states of qubits, optimal in the sense that it maximizes the purity of local states. For pure states and $M > N$ the map coincides with the optimal universal cloning transformation [5–8], whereas for $N \geq M$ it is equivalent to the optimal purification map of Ref. [11]. Thus our optimal broadcasting map generalizes/interpolates between optimal cloning and optimal purification. We have shown that the no-broadcasting theorem [4] for noncommuting mixed states cannot be generalized to more than a single input copy, and for $N \geq 4$ input copies one can even purify the state while broadcasting, below some maximum value of the purity. We named such a phenomenon *superbroadcasting*. The possibility of superbroadcasting does not correspond to an increase of the available information about the original input state ρ, due to detrimental correlations between the local broadcast copies, which does not allow us to exploit their statistics. This phenomenon was already noticed in Ref. [14], in an asymptotic analysis of the rate of optimal purification procedures. Notice that the correlations alone among qubits cannot be erased by any physical process, since the decorrelating map which sends a state to the tensor product of its partial traces is nonlinear. From the point of view of single users our broadcasting protocol is actually a purification (for states sufficiently mixed), and the same broadcasting process transfers some noise from the local states to the correlations between them. We think that the present result opens new interesting perspectives in the ability of distributing quantum information in a noisy environment.

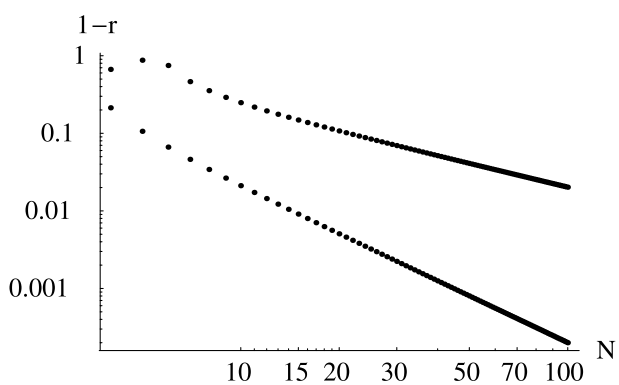

FIG. 3. Logarithmic plot vs N of $1 - r_*(N, N + 1)$ (bottom) and $1 - r_*(N, M_*(N))$ (top), where $r_*(N, M)$ denotes the maximum purity for which one has superbroadcasting from N to M copies, $M_*(N)$ being the maximum number of output copies for N inputs (the area above the lower plot is the region in which superbroadcasting is possible). The two asymptotic behaviors are N^{-1} and $2N^{-2}$.

This work has been co-founded by the EC under the program ATESIT (Contract No. IST-2000-29681), and QUPRODIS (Contract No. IST-2002-38877). P. P. acknowledges support from the INFM under Project No. PRA-2002-CLON. G. M. D. acknowledges partial support by the MURI program administered by the U.S. Army Research Office under Grant No. DAAD19-00-1-0177.

*Electronic address: dariano@unipv.it
†Electronic address: chiara@unipv.it
‡Electronic address: perinotti@fisicavolta.unipv.it
§URL: http://www.qubit.it

[1] W. K. Wootters and W. H. Zurek, Nature (London) **299**, 802 (1982).
[2] D. Dieks, Phys. Lett. **92A**, 271 (1982).
[3] H. P. Yuen, Phys. Lett. **113A**, 405 (1986).
[4] H. Barnum, C. M. Caves, C. A. Fuchs, R. Jozsa, and B. Schumacher, Phys. Rev. Lett. **76**, 2818 (1996).
[5] V. Bužek and M. Hillery, Phys. Rev. A **54**, 1844 (1996).
[6] N. Gisin and S. Massar, Phys. Rev. Lett. **79**, 2153 (1997).
[7] D. Bruss *et al.*, Phys. Rev. A **57**, 2368 (1998).
[8] R. F. Werner, Phys. Rev. A **58**, 1827 (1998).
[9] Rob Clifton, Jeffrey Bub, and Hans Halvorson, Found. Phys. **33**, 1561 (2003).
[10] G. M. D'Ariano and P. Lo Presti, Phys. Rev. A **64**, 042308 (2001).
[11] J. I. Cirac, A. K. Ekert, and C. Macchiavello, Phys. Rev. Lett. **82**, 4344 (1999).
[12] W. Fulton and J. Harris, *Representation Theory: A First Course* (Springer-Verlag, Berlin, 1991).
[13] F. Buscemi, G. M. D'Ariano, C. Macchiavello, and P. Perinotti (to be published).
[14] M. Keyl and R. F. Werner, Ann. Henri Poincaré **2**, 1 (2001).