Probabilistic Cloning and Identification of Linearly Independent Quantum States

Lu-Ming Duan and Guang-Can Guo*

*Department of Physics and Nonlinear Science Center, University of Science and Technology of China,
Hefei 230026, People's Republic of China*
(Received 19 February 1998)

We construct a probabilistic quantum cloning machine by a general unitary-reduction operation. With a postselection of the measurement results, the machine yields faithful copies of the input states. It is shown that the states secretly chosen from a certain set $S = \{|\Psi_1\rangle, |\Psi_2\rangle, \ldots, |\Psi_n\rangle\}$ can be probabilistically cloned if and only if $|\Psi_1\rangle, |\Psi_2\rangle, \ldots,$ and $|\Psi_n\rangle$ are linearly independent. We derive the best possible cloning efficiencies. Probabilistic cloning has a close connection with the problem of identification of a set of states, which is a type of $n + 1$ outcome measurement on n linearly independent states. The optimal efficiencies for this type of measurement are obtained. [S0031-9007(98)06263-2]

In quantum mechanics, a combination of unitary evolution together with measurements often yields interesting results, such as the quantum programming [1], the purification of entanglements [2], and the teleportation [3] and preparation [4] of quantum states. Here, we discuss such a combination in the field of quantum cloning. With the development of a quantum information theory, quantum cloning has become a field of growing interest [5–19]. We should discriminate two kinds of quantum cloning. If a cloning machine performs merely unitary operations, it is called deterministic cloning, since unitary evolution is deterministic. On the other hand, if a cloning machine performs measurements as well as unitary operations, with a postselection of the measurement results, it is called probabilistic cloning, since the desired copies are produced only with certain probabilities. There are two different types of statements for the quantum no-cloning theorem. The first [5] asserts that an arbitrary unknown state cannot be cloned, whether deterministically or probabilistically, since the linearity of quantum operations forbids such a replication; and the second [7–9] states that deterministic cloning of nonorthogonal states is impossible because of the unitarity of the evolution. The quantum no-cloning theorem does not rule out the possibility of probabilistic cloning of nonorthogonal states. In fact, two nonorthogonal states can indeed be probabilistically cloned [18]. Then, what property characterizes the set of states able to be probabilistically cloned? In this paper, we show that the states secretly chosen from a certain set can be probabilistically cloned if and only if they are linearly independent. We also derive the best possible cloning efficiencies.

It is appropriate to emphasize differences between the probabilistic cloning and the inaccurate quantum copying more extensively discussed in recent literature [10–17]. The inaccurate copying process is unitary and thus deterministic. For nonorthogonal states, the state fidelity can never attain 1. Arbitrary unknown states are able to be inaccurately copied. In contrast, only linearly independent states can be probabilistically cloned. The probabilistic cloning machine yields faithful copies of the input states with certain nonzero probabilities of success. For this machine, the inaccurate copies are discarded.

The $1 \rightarrow 2$ cloning machine produces two copies of the input state. Similarly, we may consider $1 \rightarrow m$, and even $1 \rightarrow \infty$, cloning machines. We will show that the probabilistic cloning is closely related to the problem of identification of a set of states. The identification measurement differs from Helstrom's minimal error probability decision [20]. It is in fact an $n + 1$ outcome measurement on n possible input states $|\Psi_1\rangle, |\Psi_2\rangle, \ldots,$ and $|\Psi_n\rangle$. The outcome i ($i = 1, 2, \ldots,$ or n) indicates that the state is definitely $|\Psi_i\rangle$, whereas the $n + 1$ outcome is "failure," indicating the case that we cannot identify what the state really is from the measurement result. The Helstrom measurement does not determine what the state really is. It is succeeded by a guess, and the minimal error probability is required in the guess.

We start by showing that only linearly independent states can be probabilistically cloned. This is the following theorem.

Theorem 1.—The states secretly chosen from the set $S = \{|\Psi_1\rangle, |\Psi_2\rangle, \ldots, |\Psi_n\rangle\}$ can be probabilistically cloned by a general unitary-reduction operation if and only if $|\Psi_1\rangle, |\Psi_2\rangle, \ldots,$ and $|\Psi_n\rangle$ are linearly independent.

Proof.—Any operation in quantum mechanics can be represented by a unitary evolution together with a measurement [21]. To get faithful copies of the pure input states $|\Psi_i\rangle$, the output states of the cloning machine are also pure. This requires that the measurement in the cloning machine should be performed with a postselection of the measurement results. A measurement with a postselection of the measurement results is described by a projection operation, and, like the unitary evolution, it is linear in the state vector. Hence, similar to the original proof of the no-cloning theorem [5], this linearity forbids faithful cloning of linearly dependent quantum states, whether in a deterministic or in a probabilistic fashion. Our task remains to prove the

converse; that is, to show that if $|\Psi_1\rangle$, $|\Psi_2\rangle$, …, and $|\Psi_n\rangle$ are n linearly independent states of a system A, there exist a unitary operation U and a measurement M, which together yield the following evolution:

$$|\Psi_i\rangle|\Sigma\rangle \overset{U+M}{\to} |\Psi_i\rangle|\Psi_i\rangle, \qquad (i = 1, 2, \ldots, n), \qquad (1)$$

where $|\Sigma\rangle$ is the input state of an ancillary system B.

Systems A and B each have an N-dimensional Hilbert space with $N \geq n$.

To prove the above statement, we introduce a probe P with an n_p-dimensional Hilbert space, where $n_p \geq n + 1$. Suppose $|P_0\rangle$, $|P_1\rangle$, …, and $|P_n\rangle$ are $n + 1$ orthonormal states of the probe P. If there exists a unitary operator U to make

$$U(|\Psi_i\rangle|\Sigma\rangle|P_0\rangle) = \sqrt{\gamma_i}\,|\Psi_i\rangle|\Psi_i\rangle|P_0\rangle + \sum_{j=1}^{n} c_{ij}|\Phi_{AB}^{(j)}\rangle|P_j\rangle, \qquad (i = 1, 2, \ldots, n), \qquad (2)$$

where $|\Phi_{AB}^{(1)}\rangle$, $|\Phi_{AB}^{(2)}\rangle$, …, and $|\Phi_{AB}^{(n)}\rangle$ and n normalized states of the composite system AB (not generally orthogonal), we measure the probe P after the evolution. The cloning attempt has succeeded, and the output state of the system AB is kept if and only if the measurement outcome of the probe is P_0. With probability γ_i of success, this measurement projects the composite system AB into the replicated state $|\Psi_i\rangle|\Psi_i\rangle$, where $i = 0, 1, \ldots,$ or n. The parameters γ_i are called the cloning efficiencies. For any input state $|\Psi_i\rangle$, the probabilistic cloning machine should succeed with a nonzero probability. This requires that all of the γ_i be positive real numbers. Therefore, the evolution (1) can be realized in physics if Eq. (2) holds with positive efficiencies. To prove existence of the unitary evolution described by Eq. (2), we notice the following fact.

Lemma 1.—If two sets of states $|\phi_1\rangle$, $|\phi_2\rangle$, …, $|\phi_n\rangle$, and $|\tilde{\phi}_1\rangle$, $|\tilde{\phi}_2\rangle$, …, $|\tilde{\phi}_n\rangle$ satisfy the condition

$$\langle\phi_i \,|\, \phi_j\rangle = \langle\tilde{\phi}_i \,|\, \tilde{\phi}_j\rangle,$$

$$(i = 1, 2, \ldots, n; j = 1, 2, \ldots, n), \qquad (3)$$

there exists a unitary operator U to make $U|\phi_i\rangle = |\tilde{\phi}_i\rangle$, $(i = 1, 2, \ldots, n)$.

The $n \times n$ inter-inner-products of Eq. (2) yield the matrix equation

$$X^{(1)} = \sqrt{\Gamma}\,X^{(2)}\sqrt{\Gamma^+} + CC^+, \qquad (4)$$

where the $n \times n$ matrices $C = [c_{ij}]$, $X^{(1)} = [\langle\Psi_i \,|\, \Psi_j\rangle]$, and $X^{(2)} = [\langle\Psi_i \,|\, \Psi_j\rangle^2]$. The diagonal efficiency matrix Γ is defined by $\Gamma = \text{diag}(\gamma_1, \gamma_2, \ldots, \gamma_n)$; hence, $\sqrt{\Gamma} = \sqrt{\Gamma^+} = \text{diag}(\sqrt{\gamma_1}, \sqrt{\gamma_2}, \ldots, \sqrt{\gamma_n})$. Lemma 1 shows that if Eq. (4) is satisfied with a diagonal positive-definite matrix Γ, the unitary evolution (2) can be realized in physics.

To prove that there is a diagonal positive-definite matrix Γ to satisfy Eq. (4), first we show that the matrix $X^{(1)}$ is positive definite. This is the following lemma.

Lemma 2.—If n states $|\Psi_1\rangle$, $|\Psi_2\rangle$, …, and $|\Psi_n\rangle$ are linearly independent, the matrix $X^{(1)} = [\langle\Psi_i \,|\, \Psi_j\rangle]$ is positive definite.

Proof of Lemma 2.—For an arbitrary n-vector $B = (b_1, b_2, \ldots, b_n)^T$, the quadratic form $B^+ X^{(1)} B$ can be expressed as

$$B^+ X^{(1)} B = \langle\Psi_T \,|\, \Psi_T\rangle = |||\Psi_T\rangle||^2, \qquad (5)$$

where

$$|\Psi_T\rangle = b_1|\Psi_1\rangle + b_2|\Psi_2\rangle + \cdots + b_n|\Psi_n\rangle. \qquad (6)$$

Since the states $|\Psi_1\rangle$, $|\Psi_2\rangle$, …, and $|\Psi_n\rangle$ are linearly independent, the summation state $|\Psi_T\rangle$ does not reduce to zero for any n-vector B, and its norm is thus always positive. By definition, the matrix $X^{(1)}$ is positive definite.

Since $X^{(1)}$ is positive definite, from continuity, for small enough but positive γ_i, the matrix $X^{(1)} - \sqrt{\Gamma}\,X^{(2)}\sqrt{\Gamma^+}$ is also positive definite. So the Hermitian matrix $X^{(1)} - \sqrt{\Gamma}\,X^{(2)}\sqrt{\Gamma^+}$ is able to be diagonalized by a unitary matrix V as follows:

$$V^+(X^{(1)} - \sqrt{\Gamma}\,X^{(2)}\sqrt{\Gamma^+})V = \text{diag}(m_1, m_2, \ldots, m_n), \qquad (7)$$

where all of the eigenvalues m_1, $m_2, \ldots,$ and m_n are positive real numbers. In Eq. (4), the matrix C can be chosen as

$$C = V\,\text{diag}(\sqrt{m_1}, \sqrt{m_2}, \ldots, \sqrt{m_n})V^+. \qquad (8)$$

Equation (4) is thus satisfied with a diagonal positive-definite efficiency matrix Γ. This completes the proof of Theorem 1.

In the above proof, the condition of linear independence of the n states $|\Psi_1\rangle$, $|\Psi_2\rangle$, …, and $|\Psi_n\rangle$ plays an essential role. If $|\Psi_1\rangle$, $|\Psi_2\rangle$, …, and $|\Psi_n\rangle$ are linearly dependent, there exists an n-vector B to make $B^+ X^{(1)} B = 0$, and the matrix $X^{(1)}$ is therefore only positive semidefinite. With a diagonal positive-definite matrix Γ, in general, $X^{(1)} - \sqrt{\Gamma}\,X^{(2)}\sqrt{\Gamma^+}$ is no longer a positive-semidefinite matrix. But the matrix CC^+ is positive semidefinite. So Eq. (4) cannot be satisfied. This shows in an alternative way that n linearly dependent states $|\Psi_1\rangle$, $|\Psi_2\rangle$, …, and $|\Psi_n\rangle$ cannot be probabilistically cloned by any unitary-reduction operation.

Deterministic cloning can be regarded as a special case of the probabilistic cloning, with all of the cloning efficiencies $\gamma_i = 1$. For nonorthogonal states, at least some of the γ_i are less than 1. If all of the $\gamma_i = 1$, i.e., $\Gamma = I_n$, Eq. (4) reduces to $X^{(1)} = X^{(2)}$. This is possible if and only if the states $|\Psi_1\rangle$, $|\Psi_2\rangle$, …, and $|\Psi_n\rangle$ are orthogonal to each other. Hence, nonorthogonal states can not be deterministically cloned by the same machine. This is a well-known result, and it has important implications in quantum cryptography [22–25].

In the following, we derive the best possible efficiencies γ_i able to be attained by a probabilistic cloning machine. A general unitary evolution of the system ABP can be decomposed as

$$U(|\Psi_i\rangle |\Sigma\rangle |P_0\rangle) = \sqrt{\gamma_i} |\Psi_i\rangle |\Psi_i\rangle |P^{(i)}\rangle + \sqrt{1 - \gamma_i} |\Phi_{ABP}^{(i)}\rangle, \qquad (i = 1, 2, \ldots, n), \qquad (9)$$

where $|P_0\rangle$ and $|P^{(i)}\rangle$ are normalized states of the probe P (not generally orthogonal) and $|\Phi_{ABP}^{(1)}\rangle$, $|\Phi_{ABP}^{(2)}\rangle, \ldots,$ and $|\Phi_{ABP}^{(n)}\rangle$ are n normalized states of the composite system ABP (not generally orthogonal). Without loss of generality, in Eq. (9) the coefficients before the states $|\Psi_i\rangle |\Psi_i\rangle |P^{(i)}\rangle$ and $|\Phi_{ABP}^{(i)}\rangle$ are assumed to be positive real numbers. Obviously, Eq. (2) is a special case of Eq. (9) with $|P_0\rangle$ and all $|P^{(i)}\rangle$ being the same state and $|\Phi_{ABP}^{(i)}\rangle$ having a special decomposition. We denote the subspace spanned by the states $|P^{(1)}\rangle$, $|P^{(2)}\rangle, \ldots, |P^{(n)}\rangle$ by the symbol S_0. During the cloning process, after the unitary evolution a measurement of the probe with a postselection of the measurement results projects its state into the subspace S_0. After this projection, the state of the system AB should be $|\Psi_i\rangle |\Psi_i\rangle$, so all of the states $|\Phi_{ABP}^{(i)}\rangle$ ought to lie in a space orthogonal to S_0. This requires that $|\Phi_{ABP}^{(j)}\rangle$ be annihilated by the projection operator $|P^{(i)}\rangle \langle P^{(i)}|$ for any i and j; i.e.,

$$|P^{(i)}\rangle \langle P^{(i)}| \, |\Phi_{ABP}^{(j)}\rangle = 0,$$

$$(i = 1, 2, \ldots, n; j = 1, 2, \ldots, n). \qquad (10)$$

Under the condition (10), inter-inner-products of Eq. (9) yield the following matrix equation:

$$X^{(1)} = \sqrt{\Gamma} \, X_P^{(2)} \sqrt{\Gamma^+} + \sqrt{I_n - \Gamma} \, Y \sqrt{I_n - \Gamma^+}, \quad (11)$$

where the $n \times n$ matrices $Y = [\langle \Phi_{ABP}^{(i)} | \Phi_{ABP}^{(j)} \rangle]$ and $X_P^{(2)} = [\langle \Psi_i | \Psi_j \rangle^2 \langle P^{(i)} | P^{(j)} \rangle]$, and I_n is the $n \times n$ unit matrix. Following the proof of Lemma 2, Y, and thus $\sqrt{I_n - \Gamma} \, Y \sqrt{I_n - \Gamma^+}$, are positive-semidefinite matrixes, so $X^{(1)} - \sqrt{\Gamma} \, X_P^{(2)} \sqrt{\Gamma^+}$ should also be positive semidefinite. On the other hand, if $X^{(1)} - \sqrt{\Gamma} \, X_P^{(2)} \sqrt{\Gamma^+}$ is a positive-semidefinite matrix, following the proof of Theorem 1, Eq. (11) can be satisfied with a special choice of $|\Phi_{ABP}^{(i)}\rangle$, and then Lemma 1 shows that the states $|\Psi_1\rangle$, $|\Psi_2\rangle, \ldots,$ and $|\Psi_n\rangle$ are able to be probabilistically cloned. We thus get the following theorem.

Theorem 2.—The states $|\Psi_1\rangle$, $|\Psi_2\rangle, \ldots,$ and $|\Psi_n\rangle$ can be probabilistically cloned with a diagonal efficiency matrix Γ if and only if the matrix $X^{(1)} - \sqrt{\Gamma} \, X_P^{(2)} \sqrt{\Gamma^+}$ is positive semidefinite.

The semipositivity of the matrix $X^{(1)} - \sqrt{\Gamma} \, X_P^{(2)} \sqrt{\Gamma^+}$ gives a series of inequalities about the efficiencies γ_i. The best possible cloning efficiencies γ_i are obtained by solving these inequalities and then taking the maximum over all possible choices of the normalized states $|P^{(i)}\rangle$. For example, if there are only two states $|\Psi_1\rangle$ and $|\Psi_2\rangle$, Theorem 2 shows that the cloning efficiencies γ_1 and γ_2 satisfy

$$\frac{\gamma_1 + \gamma_2}{2} \le \max_{|P^{(i)}\rangle} \frac{1 - |\langle \Psi_1 | \Psi_2 \rangle|}{1 - |\langle \Psi_1 | \Psi_2 \rangle|^2 |\langle P^{(1)} | P^{(2)} \rangle|} = \frac{1}{1 + |\langle \Psi_1 | \Psi_2 \rangle|}, \qquad (12)$$

where we assumed $|\langle \Psi_1 | \Psi_2 \rangle| \neq 1$. The equality in Eq. (12) holds if and only if $\gamma_1 = \gamma_2$ and $\langle P^{(1)} | P^{(2)} \rangle \langle \Psi_1 | \Psi_2 \rangle = |\langle \Psi_1 | \Psi_2 \rangle|$. The best possible efficiencies obtained from Theorem 2 depend on inner products of the input states. This is a natural result since probabilistic cloning is possible only for a known set of states. Theorem 2 is a basic result in determining the best possible cloning efficiencies.

The analysis of the $1 \to 2$ probabilistic cloning can be directly extended to include the $1 \to m$ probabilistic cloning. The extension is straightforward, and we omit its proof. The result is the following.

Theorem 3.—The states $|\Psi_1\rangle$, $|\Psi_2\rangle, \ldots,$ and $|\Psi_n\rangle$ can be probabilistically replicated into m faithful copies with a diagonal efficiency matrix Γ if and only if the matrix $X^{(1)} - \sqrt{\Gamma} \, X_P^{(m)} \sqrt{\Gamma^+}$ is positive semidefinite.

The matrix $X_P^{(m)}$ in Theorem 3 is defined by $X_P^{(m)} = [\langle \Psi_i | \Psi_j \rangle^m \langle P^{(i)} | P^{(j)} \rangle]$. The $1 \to \infty$ probabilistic cloning is of special interest. It is closely related to the problem of identification of the states $|\Psi_1\rangle$, $|\Psi_2\rangle, \ldots,$ and $|\Psi_n\rangle$. On the one hand, if we have infinitely many

faithful copies of the input state, the state can be definitely determined. On the other hand, if the input state is definitely determined, we can generate infinitely many faithful copies. The best possible efficiencies for the $1 \to \infty$ probabilistic cloning are determined by the semipositivity of the matrix $X^{(1)} - \sqrt{\Gamma} \, X_P^{(\infty)} \sqrt{\Gamma^+} = X^{(1)} - \Gamma$, where we assumed $|\langle \Psi_i | \Psi_j \rangle| < 1$ for $i \neq j$. Are these the optimal efficiencies for the identification measurement on the states $|\Psi_1\rangle$, $|\Psi_2\rangle, \ldots,$ and $|\Psi_n\rangle$? We show that it is indeed the case by directly proving the result.

Theorem 4.—The states $|\Psi_1\rangle$, $|\Psi_2\rangle, \ldots,$ and $|\Psi_n\rangle$ can be identified, respectively, with the efficiencies γ_1, $\gamma_2, \ldots,$ and γ_n if and only if the matrix $X^{(1)} - \Gamma$ is positive semidefinite.

Proof.—By definition, the identification is an $n + 1$ outcome measurement on the states $|\Psi_1\rangle$, $|\Psi_2\rangle, \ldots,$ and $|\Psi_n\rangle$. From the general representation theorem for quantum operations [21], a general measurement on system A can be represented by a unitary operation U on the composite system ABP, succeeded by a Von Neumann's

type of measurement on the probe P, where B indicates an ancillary system. In the identification measurement, with the measurement outcome P_i $(i = 1, 2, \ldots, n)$, the state should be definitely $|\Psi_i\rangle$; whereas with the $n + 1$ outcome P_{n+1}, the state is not definitely determined, and the measurement fails. Hence, the unitary operation U on the composite system ABP can be generally expressed as

$$U(|\Psi_i\rangle |\Psi_{BP}^{(0)}\rangle) = \sqrt{\gamma_i} |\Psi_{AB}^{(i)}\rangle |P_i\rangle + \sqrt{1 - \gamma_i} |\Phi_{AB}^{(i)}\rangle |P_{n+1}\rangle, \qquad (i = 1, 2, \ldots, n), \tag{13}$$

where γ_i is the measurement efficiency with the input state $|\Psi_i\rangle$, and $|P_1\rangle$, $|P_2\rangle, \ldots$, and $|P_{n+1}\rangle$ are $n + 1$ orthonormal states of the probe P. $|\Phi_{AB}^{(i)}\rangle$, $|\Psi_{BP}^{(0)}\rangle$, and $|\Psi_{AB}^{(i)}\rangle$ are normalized states of the composite system AB, BP, and AB, respectively (not generally orthogonal). Obviously, after the evolution (13), a Von Neumann's type of measurement described by the projection operators $|P_i\rangle\langle P_i|$ $(i = 1, 2, \ldots, n + 1)$ definitely determines the input state with probability γ_i of success. Inter-inner-products of Eq. (13) yield the matrix equation

$$X^{(1)} = \Gamma + \sqrt{I_n - \Gamma} [\langle \Phi_{AB}^{(i)} | \Phi_{AB}^{(j)} \rangle] \sqrt{I_n - \Gamma^+}. \tag{14}$$

Similar to the proof of Theorem 2, semipositivity of the matrix $X^{(1)} - \Gamma$ thus becomes the necessary and sufficient condition for identification of the states $|\Psi_1\rangle$, $|\Psi_2\rangle, \ldots$, and $|\Psi_n\rangle$. This is the content of Theorem 4.

Theorem 4 determines the optimal measurement efficiencies. For example, if there are three states $|\Psi_1\rangle$, $|\Psi_2\rangle$, and $|\Psi_3\rangle$, and if $|\Psi_1\rangle$ is orthogonal to $|\Psi_2\rangle$ and $|\Psi_3\rangle$, but $|\Psi_2\rangle$ is not orthogonal to $|\Psi_3\rangle$, then the optimal efficiencies are given by $\gamma_1 = 1$, and $(\gamma_2 + \gamma_3)/2 \leq 1 - |\langle \Psi_2 | \Psi_3 \rangle|$. The equality holds if and only if $\gamma_2 = \gamma_3$. This is essentially the result gained in Refs. [26–28], where the identification of two nonorthogonal states is considered. For n linearly independent and generally nonorthogonal states, the optimal efficiencies γ_1, $\gamma_2, \ldots$, and γ_n are obtainable by solving a series of inequalities from the semipositivity of the matrix $X^{(1)} - \Gamma$.

In summary, we have shown that only linearly independent states can be probabilistically cloned with nonzero probabilities of success. The best possible cloning efficiencies are derived. We establish connection between the probabilistic cloning and the identification measurement, and obtain the optimal measurement efficiencies for n linearly independent states.

---

*Electronic address: gcguo@sunlx06.nsc.ustc.edu.cn

[1] M. A. Nielsen and I. L. Chuang, Phys. Rev. Lett. **79**, 321 (1997).

[2] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin, and W. K. Wootters, Phys. Rev. Lett. **76**, 722 (1996).

[3] C. H. Bennett, G. Brassard, C. Crepeau, R. Jozsa, A. Peres, and W. K. Wootters, Phys. Rev. Lett. **70**, 1895 (1993).

[4] M. Brune, S. Haroche, J. M. Raimond, L. Davidovich, and N. Zagury, Phys. Rev. A **45**, 5193 (1992).

[5] W. K. Wootters and W. H. Zurek, Nature (London) **299**, 802 (1982).

[6] D. Dieks, Phys. Lett. **92A**, 271 (1982).

[7] H. P. Yuen, Phys. Lett. **113A**, 405 (1986).

[8] G. M. D'Ariano and H. P. Yuen, Phys. Rev. Lett. **76**, 2832 (1996).

[9] H. Barnum, G. M. Caves, C. A. Fuchs, R. Jozsa, and B. Schumacher, Phys. Rev. Lett. **76**, 2818 (1996).

[10] V. Buzek and M. Hillery, Phys. Rev. **54A**, 1844 (1996).

[11] D. Mozyrsky, V. Privman, and M. Hillery, Phys. Lett. A **226**, 253 (1997).

[12] N. Gisin and B. Huttner, Phys. Lett. A **228**, 13 (1997).

[13] V. Buzek, V. Vedral, M. Plenio, P. L. Knight, and M. Hillery, Phys. Rev. A **55**, 3327 (1997).

[14] M. Hillery and V. Buzek, Phys. Rev. A **56**, 1212 (1997).

[15] D. Bruß, D. P. DiVincenzo, A. Ekert, C. Macchiavello, and J. A. Smolin, LANL e-print quant-ph/9705038.

[16] N. Gisin and S. Massar, Phys. Rev. Lett. **79**, 2153 (1997).

[17] D. Bruß, A. Ekert, and C. Macchiavello, LANL e-print quant-ph/9712019.

[18] L. M. Duan and G. C. Guo, LANL e-print quant-ph/9704020.

[19] M. Horodecki and R. Horodecki, LANL e-print quant-ph/9705003.

[20] C. W. Helstrom, *Quantum Detection and Estimation Theory* (Academic, New York, 1976); C. A. Fuchs, LANL e-print quant-ph/9601020.

[21] K. Kraus, *States, Effects, and Operations* (Springer-Verlag, Berlin, 1983); H. Barnum, M. A. Nielsen, and B. Schumacher, LANL e-print quant-ph/9702049.

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

[23] C. H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992).

[24] S. M. Barnett and S. J. D. Phoenix, Phys. Rev. A **48**, R5 (1993).

[25] A. Ekert, B. Huttner, G. M. Palma, and A. Peres, Phys. Rev. A **50**, 1047 (1994).

[26] D. Dieks, Phys. Lett. A **126**, 303 (1988).

[27] A. Peres, Phys. Lett. A **128**, 29 (1988).

[28] G. Jaeger and A. Shimony, Phys. Lett. A **197**, 83 (1995).