Oblivious Remote State Preparation

Debbie W. Leung[1,2] and Peter W. Shor[3]

[1]*IBM T.J. Watson Research Center, P.O. Box 218, Yorktown Heights, New York 10598*
[2]*Mathematical Science Research Institute, 1000 Centennial Drive, Berkeley, California 94720*
[3]*AT&T Labs–Research, Florham Park, New Jersey 07932*

(Received 31 January 2002; revised manuscript received 9 January 2003; published 26 March 2003)

We characterize the class of remote state preparation (RSP) protocols that use only forward classical communication and entanglement, deterministically prepare an exact copy of a general state, and do so *obliviously*—without leaking further information about the state to the receiver. We prove that any such protocol can be modified to require from the sender *only* a single specimen of the state, without increasing the classical communication cost. This implies Lo's conjectured lower bound on the cost for these protocols. We relate our RSP protocols to the *private quantum channels* and establish a one-to-one correspondence between them.

DOI: 10.1103/PhysRevLett.90.127905 PACS numbers: 03.67.Hk, 03.67.Dd

Teleportation [1] is a protocol that enables a quantum state to be transmitted from a sender ("Alice") to a receiver ("Bob") using only quantum entanglement and classical communication. To communicate any state in a two-dimensional Hilbert space (qubit), it suffices for Alice and Bob to share one EPR state (ebit), $(1/\sqrt{2}) \times (|00\rangle + |11\rangle)$ and for Alice to send two classical bits (cbits) to Bob. More generally, $\log d$ ebits and $2\log d$ cbits are sufficient for the teleportation of a d-dimensional quantum state. These resources are also necessary, because teleportation preserves the entanglement shared between the transmitted state and any other systems, and can be used to share entanglement or to perform superdense coding [2]. As the procedure for teleportation does not depend on the transmitted state, pure states cannot be sent with fewer resources.

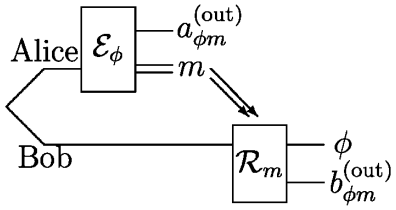
More recently, Lo [3] studied methods to transmit pure quantum states using entanglement and classical communication when the sender has knowledge of the transmitted state. This communication task is called remote state preparation (RSP). RSP protocols more economical than teleportation were found for certain ensembles [4]. The suggested possibility to trade off the two resources were studied in detail in the asymptotic regime [5,6].

Resource lower bounds for RSP of pure states are generally difficult to establish. Unlike teleportation, RSP of pure states needs not preserve the entanglement of the transmitted system with other systems, so that neither lower bound for teleportation applies. For instance, the classical communication cost for RSP of an arbitrary pure d-dimensional state is only lower bounded by $\log d$ cbits (Holevo's bound [7]), in contrast to the $2\log d$ cbits required for teleportation. In Ref. [3], Lo conjectured that $2\log d$ cbits are necessary for RSP. But Ref. [5] found probabilistic RSP protocols that use only $\log d$ cbits on average, yet suggested Lo's conjecture be true in some scenarios, such as when the required amount of classical communication is nonprobabilistic, or when Bob obtains no extra information about the prepared state beyond what is contained in his copy.

In this Letter, we prove a stronger result that implies Lo's conjecture under circumstances to be defined. We use the term "generic ensemble" to describe an ensemble of states whose density matrices span the operators acting on the input Hilbert space (when there is a subset of $d^2 - 1$ linearly independent density matrices in d dimensions). We say that an RSP protocol is oblivious to Bob if he cannot obtain more information about the prepared state than is contained in a single specimen, even if he deviates from the protocol. A protocol is called faithful if it is exact and deterministic. Finally, a protocol is said to be oblivious to Alice if it requires from her only a specimen of the transmitted state, but not her knowledge of it. With these definitions, we can state our result: *If an RSP protocol for a generic ensemble of pure states uses only forward communication and entanglement, and is faithful and oblivious to Bob, then it can be modified to be oblivious to Alice at no extra classical communication cost.* An immediate corollary is that such an RSP protocol uses at least as much classical communication as required in teleportation. Our work also provides insights on how knowledge of the prepared states enables resource tradeoff in RSP. We will describe an explicit procedure for the modification, and detail intermediate results including a characterization of faithful RSP protocols without back communication and lemmas on state change induced by measuring part of an entangled state. We also establish a one-to-one correspondence between our class of RSP protocols and (exact) private quantum channels [8,9].

We now consider the conversion of a faithful RSP protocol oblivious to Bob and using no back communication to a protocol oblivious to Alice. We denote by ϕ the d-dimensional state (and its density matrix) to be transmitted. We first characterize the most general faithful protocol without back communication as follows:

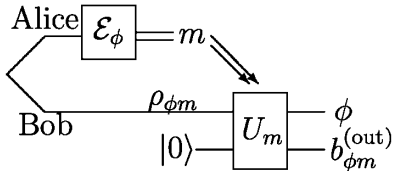
 © 2003 The American Physical Society



(1)

In Eq. (1), the entangled state shared by Alice and Bob is a maximally entangled state in two d'-dimensional systems, $|\Phi_{d'}\rangle = (1/\sqrt{d'})(|11\rangle + \cdots + |d'd'\rangle)$. We do not require $d = d'$. Alice's most general action is to apply to her half of $|\Phi_{d'}\rangle$ a trace preserving quantum operation $\mathcal{E}_\phi$, parametrized by ϕ to reflect possible use of her knowledge of it. Since the communication is classical, $\mathcal{E}_\phi$ should output some classical message m to be sent to Bob, with probability $(p_\phi)_m$. Note that $\sum_m (p_\phi)_m = 1$. The remaining classical or quantum output is represented by $a_{\phi m}^{(\mathrm{out})}$. Bob's most general action is to apply to his quantum system a quantum operation $\mathcal{R}_m$ that depends on m but not on ϕ. For a faithful protocol, $\mathcal{R}_m$ is *trace preserving* and it always outputs a copy of ϕ, along with some extra output $b_{\phi m}^{(\mathrm{out})}$. We omit input ancillae to $\mathcal{E}_\phi$ and $\mathcal{R}_m$, which merely redefine the quantum operations.

We now simplify the above circuit. Since Bob's operation $\mathcal{R}_m$ is trace preserving, it can be implemented by attaching a $|0\rangle$ state and applying a joint unitary operation U_m [10]. We can also trace out $a_{\phi m}^{(\mathrm{out})}$ without affecting Bob's pure output state ϕ nor the distribution $(p_\phi)_m$ for the messages. Now, Alice's operation $\mathcal{E}_\phi$ only outputs classical data and is just a POVM (positive operator valued measure) measurement. The simplified circuit is given by



(2)

where $\rho_{\phi m}$ denotes the state of Bob's half of the shared system given the message m.

We now apply the conditions that ϕ is drawn from a generic ensemble and that the protocol is oblivious to Bob. They imply that $b_{\phi m}^{(\mathrm{out})}$ and $(p_\phi)_m$ are independent of ϕ and can be written as $b_m^{(\mathrm{out})}$ and p_m; otherwise Bob can gain information about the identity of ϕ without disturbing his single copy, violating the no-imprinting condition [11] for a generic ensemble of states. Using the state change due to U_m,

$$\rho_{\phi m} = \mathrm{Tr}_2[U_m^\dagger(\phi \otimes b_m^{(\mathrm{out})})U_m], \tag{3}$$

where Tr_2 denotes the partial trace of the second tensor component. Throughout the paper, *italicized* numerical subscripts are sometimes added to an operator or operation to clarify which tensor components (in the equation) it is acting on.

We can obtain an important identity by describing Bob's state before he receives the message m in two different ways,

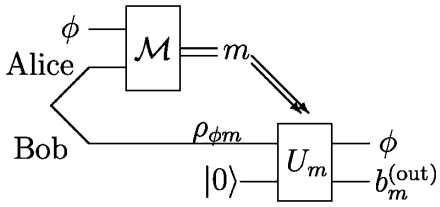
$$\sum_m p_m \rho_{\phi m} = \frac{I}{d'}. \tag{4}$$

Substituting Eq. (3) into Eq. (4),

$$\sum_m p_m[\mathrm{Tr}_2\, U_m^\dagger(\phi \otimes b_m^{(\mathrm{out})})U_m] = \frac{I}{d'}. \tag{5}$$

We define a map $\mathcal{F}$ so that $\mathcal{F}(\phi)$ is given by the left side of Eq. (5). $\mathcal{F}$ is linear since p_m, U_m, and $b_m^{(\mathrm{out})}$ are all independent of ϕ, and $\mathcal{F}$ is uniquely defined since the set of possible ϕ forms a generic ensemble. The right side of Eq. (5) implies that $\mathcal{F}$ is the completely randomizing operation, $\mathcal{F}(\cdot) = I/d'$.

Now we describe a modified protocol which is oblivious to Alice. She applies a ϕ-independent measurement $\mathcal{M}$ jointly to a single specimen of ϕ and her half of $|\Phi_{d'}\rangle$:



(6)

We claim that, if the POVM elements of $\mathcal{M}$ are given by

$$M_m = dd' p_m\, \mathrm{Tr}_3[(I_1 \otimes U_{m23}^T) \times (|\Phi_d\rangle\langle\Phi_d|_{12} \otimes b_{m3}^{(\mathrm{out})\,T}) \times (I_1 \otimes U_{m23}^*)], \tag{7}$$

Bob will indeed receive the same classical and quantum outputs as in the original RSP protocol.

We first verify that $\{M_m\}$ is a POVM acting on a $d \times d'$ system. According to Eq. (3), $I_1 \otimes U_{m23}^T$ takes a $d \times d \times \dim[b_m^{(\mathrm{out})}]$ system to a $d \times d' \times 1$ system. The Tr_3 in Eq. (7) then ensures M_m acts on a $d \times d'$ system. Each M_m is manifestly positive semidefinite. Furthermore, let $\mathcal{I}$ denote the identity operation. Using Eq. (5),

$$\sum_m M_m^T = dd'(\mathcal{I} \otimes \mathcal{F})(|\Phi_d\rangle\langle\Phi_d|) = I \otimes I, \tag{8}$$

so that $\{M_m\}$ is indeed a POVM.

It remains to verify that the original and the modified protocols are identical from Bob's point of view. In the modified protocol, let $\mathbf{b}$ be the state in Bob's half of the shared system when the measurement $\mathcal{M}$ outputs m, normalized by the probability of outcome m. The modified protocol creates the correct state with the correct probability if $\mathbf{b} = p_m \rho_{\phi m}$. We will prove this using a few lemmas (a proof by direct evaluation of $\mathbf{b}$ can be found in [12]).

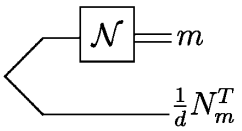
Lemma 1a: $(\mathrm{Tr}_1 AB)^T = \mathrm{Tr}_1 B^T A^T$.

Lemma 1b: $A(\mathrm{Tr}_1 B)C = \mathrm{Tr}_1(I \otimes A)B(I \otimes C)$.

These can be readily verified for square matrices A, B, C of compatible dimensions (proof omitted). We

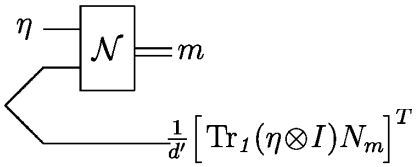
call the density matrix of a state, normalized by its probability of occurring, its *unnormalized density matrix*.

Lemma 2a: [13] $\mathrm{Tr}_1(N_m \otimes I)|\Phi_d\rangle\langle\Phi_d| = \frac{1}{d} N_m^T$ for any d-dimensional square matrix N_m. Thus, if a measurement $\mathcal{N}$ with POVM $\{N_m\}$ is applied to half of $|\Phi_d\rangle$ and the outcome is m, the unmeasured half has unnormalized density matrix $\frac{1}{d} N_m^T$.



(9)

Lemma 2b: $\mathrm{Tr}_{12}[(N_{m12} \otimes I_3)(\eta \otimes |\Phi_{d'}\rangle\langle\Phi_{d'}|)] = (1/d') \times [\mathrm{Tr}_1(\eta \otimes I) N_m]^T$ for square matrices N_m and η of dd' and d dimensions. Thus, if a measurement $\mathcal{N}$ with POVM $\{N_m\}$ is applied jointly on a state η and half of $|\Phi_{d'}\rangle$ and the outcome is m, the unmeasured half has unnormalized density matrix $(1/d')\,\mathrm{Tr}_1[(\eta \otimes I) N_m]^T$.



(10)

Proof:

$$\mathrm{Tr}_{12}(N_{m12} \otimes I_3)(\eta_1 \otimes |\Phi_{d'}\rangle\langle\Phi_{d'}|_{23})$$
$$= \mathrm{Tr}_2\,\mathrm{Tr}_1[N_{m12}(\eta_1 \otimes I_2) \otimes I_3](I_1 \otimes |\Phi_{d'}\rangle\langle\Phi_{d'}|_{23})$$
$$= \mathrm{Tr}_1\{[\mathrm{Tr}_1 N_{m12}(\eta_1 \otimes I_2) \otimes I_3]|\Phi_{d'}\rangle\langle\Phi_{d'}|_{12}\} \quad (11)$$

$$= \mathrm{Tr}_1(\{[\mathrm{Tr}_1 N_m(\eta \otimes I)] \otimes I\}|\Phi_{d'}\rangle\langle\Phi_{d'}|)$$
$$= \frac{1}{d'}[\mathrm{Tr}_1 N_m(\eta \otimes I)]^T, \quad (12)$$

where we have used Lemmas 1b and 2a to obtain Eqs. (11) and (12). In Eq. (11), the inner Tr_1 changes the indices outside of it, for instance, Tr_2 becomes Tr_1.

We are now ready to verify $\mathbf{b} = p_m \rho_{\phi m}$. Using Eq. (7) to express M_m, and applying Lemma 2b:

$$\mathbf{b} = dp_m\,\mathrm{Tr}_1\{(\phi_1 \otimes I_2)\mathrm{Tr}_3[(I_1 \otimes U_{m23}^T) \times (|\Phi_d\rangle\langle\Phi_d|_{12} \otimes b_{m3}^{(\mathrm{out})\,T}) \times (I_1 \otimes U_{m23}^*)]\}^T.$$

Applying Lemma 1a to Tr_1 and then to Tr_3,

$$\mathbf{b} = dp_m\,\mathrm{Tr}_1\{\mathrm{Tr}_3[(I_1 \otimes U_{m23}^\dagger)(|\Phi_d\rangle\langle\Phi_d|_{12} \otimes b_{m3}^{(\mathrm{out})}) \times (I_1 \otimes U_{m23})](\phi_1^T \otimes I_2)\},$$

and applying Lemma 1b to Tr_3,

$$\mathbf{b} = dp_m\,\mathrm{Tr}_1\,\mathrm{Tr}_3[(I_1 \otimes U_{m23}^\dagger)(|\Phi_d\rangle\langle\Phi_d|_{12} \otimes b_{m3}^{(\mathrm{out})}) \times (\phi_1^T \otimes I_{23})(I_1 \otimes U_{m23})].$$

Exchanging the order of Tr_3 and Tr_1 (3 is reindexed as 2 outside of Tr_1), and applying Lemma 1b to Tr_1,

$$\mathbf{b} = dp_m\,\mathrm{Tr}_2\{U_m^\dagger \mathrm{Tr}_1[(|\Phi_d\rangle\langle\Phi_d|_{12} \otimes b_{m3}^{(\mathrm{out})})(\phi_1^T \otimes I_{23})]U_m\}.$$

Finally, using Lemma 2a on Tr_1,

$$\mathbf{b} = p_m\,\mathrm{Tr}_2[U_m^\dagger(\phi \otimes b_m^{(\mathrm{out})})U_m] = p_m \rho_{\phi m},$$

completing the proof of our major claim.

This result has several consequences. First, even though entanglement between the transmitted system and other systems may not be preserved by the original protocol, it is preserved by the modified one. Thus, the latter can be used for superdense coding and requires at least $2\log d$ cbits. Furthermore, the modification leaves p_m and therefore the classical communication cost unchanged. Altogether, the original RSP protocol must require at least $2\log d$ cbits, proving Lo's conjecture under the conditions imposed on the RSP protocol. Note that the original protocol works only for pure states; we have modified the protocol to be more versatile at no extra classical communication cost.

Second, a faithful RSP protocol may use a probabilistic amount of resources. As an example, take an RSP protocol that sometimes fails and use teleportation in case of failure. Our proof still applies when the resources are probabilistic because, in the general description of RSP in Eq. (1), the message m may have variable length and the outputs $a_{\phi m}^{(\mathrm{out})}$, $b_{\phi m}^{(\mathrm{out})}$ may contain unused entanglement. Since the modification preserves the probability distribution $\{p_m\}$ of the classical messages, the original and modified protocols require the same amount of classical communication under all measures, including the worst and the average costs.

Third, Eq. (2) is equivalent to Eq. (1) except for losing entanglement and shared classical randomness at the end of the protocol when $a_{\phi m}^{(\mathrm{out})}$ is traced out. The modified protocol can be used to establish $\log d$ ebits, which is a lower bound for the initial amount of entanglement required for the original protocol, though not for the net average amount of entanglement consumed.

Finally, we have derived Eq. (4) or (5) as a necessary condition for our class of RSP protocols. Equation (4) or (5) is also sufficient for an RSP protocol depicted in Eq. (2) to exist: Following Lemma 2a, Alice only needs to apply a measurement with POVM $\{p_m d' \rho_{\phi m}^T\}$.

Our result can be extended in two interesting ways. First, it applies when the protocol is nondeterministic and when it fails (with some probability p_f) Alice knows, and when she tells Bob, his system is in a state ρ_f independent of ϕ. The protocol prepares an exact copy of ϕ otherwise. Our previous arguments hold almost exactly, except now $\sum_m p_m = 1 - p_f$ and Eqs. (1), (2), and (6) only occur with probability $1 - p_f$. Equations (4) and (5) are, respectively, replaced by $\sum_m p_m \rho_{\phi m} + p_f \rho_f = (I/d')$ and $\sum_m p_m[\mathrm{Tr}_2 U_m^\dagger(\phi \otimes b_m^{(\mathrm{out})})U_m] + p_f \rho_f = (I/d')$. The

measurement $\mathcal{M}$ in the modified protocol has an extra POVM element $I \otimes \rho_f^T$ besides those specified in Eq. (7).

Second, our result adapts to RSP in which Alice and Bob initially share a fixed but arbitrary pure state $|\Psi\rangle$ instead of $|\Phi_{d'}\rangle$. Without loss of generality, $|\Psi\rangle = \sum_{i=1}^{d'} \sqrt{q_i}|i\rangle|i\rangle$ for some $q_i > 0$ and $\sum_i q_i = 1$. Let $\psi = \sum_i q_i |i\rangle\langle i|$ be the reduced density matrix on either side. Each step in our original proof can be repeated, essentially replacing $(I/d')^{1/2}$ by $\psi^{1/2}$ whenever appropriate. Here, we outline all the changes. We replace $|\Phi_{d'}\rangle$ by $|\Psi\rangle$ in the circuits and I/d' by ψ in Eqs. (4) and (5). $\mathcal{F}$ is defined as before; now, following Eq. (5), $\mathcal{F}(\cdot) = \psi$. The POVM for $\mathcal{M}$ is now $\{[I \otimes (d'\psi)^{-(1/2)T}] \times M_m [I \otimes (d'\psi)^{-(1/2)T}]\}$, where M_m is still given by Eq. (7) with the $|\Phi_d\rangle\langle\Phi_d|$ factor. We use Lemma 2a$'$: $\mathrm{Tr}_1(N_m \otimes I)|\Psi\rangle\langle\Psi| = \psi^{1/2} N_m^T \psi^{1/2}$, and Lemma 2b$'$: $\mathrm{Tr}_{12}[(N_{m12} \otimes I_3)(\eta \otimes |\Psi\rangle\langle\Psi|)] = \psi^{1/2}[\mathrm{Tr}_1(\eta \otimes I)N_m]^T \psi^{1/2}$, with which the verification of $\mathbf{b} = p_m \rho_{\phi m}$ reduces to the previous argument.

We can establish a one-to-one correspondence between faithful oblivious RSP without back communication and private quantum channel (PQC) [8,9] based on the second extension. We generalize the definition in [8] slightly. The goal of PQC is to encrypt a quantum state ϕ to be transmitted from Alice to Bob, using a private classical key, m, with prior probability p_m. Alice encrypts by attaching an ancilla b_m [14], applying a unitary operation $U_m^\dagger$, and sends the resulting state. Here, U_m, p_m depend on m but not on ϕ since PQC is oblivious to Alice. Bob decrypts by applying U_m and discarding b_m. Information theoretic secrecy is achieved if and only if

$$\sum_m p_m U_m^\dagger (\phi \otimes b_m) U_m = \psi, \tag{13}$$

where ψ is a constant state seen by an eavesdropper who does not know m. Without loss of generality, ψ is diagonal. Given a PQC [$\{p_m\}$, $\{U_m\}$, $\{b_m\}$, and ψ satisfying Eq. (13)], an RSP protocol in Eq. (2) exists in which Alice and Bob share an initial pure state $|\Psi\rangle$ with reduced density matrix ψ and Alice's measurement has POVM $\{\psi^{-(1/2)T}[p_m U_m^\dagger(\phi \otimes b_m)U_m]^T \psi^{-(1/2)T}\}$. This is faithful, without back communication, and oblivious to Bob [$b_{\phi m}^{(\mathrm{out})} = b_m$ and $(p_\phi)_m = p_m$]. The classical communication cost in RSP is equal to the key size in the initial PQC. This RSP protocol can be made oblivious to Alice and requires at least $2 \log d$ cbits. Thus, the original PQC requires $2 \log d$ key bits, rederiving the result in [8] for our slightly more general definition. Conversely, given a faithful RSP protocol oblivious to Bob using initial entangled state $|\Psi\rangle$ and no back communication, an analogue of Eq. (5) (without the partial trace) necessarily holds:

$$\sum_m p_m [U_m^\dagger(\phi \otimes b_m^{(\mathrm{out})})U_m] = \psi \otimes |0\rangle\langle 0|. \tag{14}$$

This defines a PQC with key size equal to the classical communication cost of the RSP protocol.

We described in [12] a faithful RSP protocol using no back communication and oblivious to Bob that transmits a nongeneric ensemble and violates Lo's conjecture. Hence, a generic ensemble is generally needed for our result to hold.

The oblivious condition renders Bob's quantum state [after receiving the message, Eq. (3)] to be obtainable by applying a quantum operation on ϕ. This is necessary if the modified protocol is to be oblivious to Alice. Sufficiency is due to the generic ensemble transmitted, so that $\mathcal{F}$ randomizes *all* input states and $I \otimes \mathcal{F}$ randomizes half of a maximally entangled state. This ensures the POVM $\mathcal{M}$ exists for a protocol oblivious to Alice.

In summary, we characterize faithful RSP protocols without back communication and, for those oblivious to Bob and transmitting generic ensembles, we prescribe a modification to protocols oblivious to Alice and prove Lo's conjecture. We also draw a one-to-one correspondence between those RSP protocols and PQC and discuss the role of obliviousness in our result.

We thank Bennett, DiVincenzo, Hayden, Lo, Smolin, Terhal, and Winter for enlightening discussions. D. W. L. is supported in part by the NSA and ARDA under the US ARO, Grant No. DAAG55-98-C-0041.

[1] C. Bennett, G. Brassard, C. Crepeau, R. Jozsa, A. Peres, and W. Wootters, Phys. Rev. Lett. **70**, 1895 (1993).
[2] C. Bennett and S. Wiesner, Phys. Rev. Lett. **69**, 2881 (1992).
[3] H.-K. Lo, Phys. Rev. A **62**, 012313 (2000).
[4] An ensemble is a set of quantum states, endowed with a prior probability distribution, that the sender may send.
[5] C. Bennett, D. DiVincenzo, P. Shor, J. Smolin, B. Terhal, and W. Wootters, Phys. Rev. Lett. **87**, 077902 (2000).
[6] I. Devetak and T. Berger, Phys. Rev. Lett. **87**, 197901 (2001).
[7] A. Holevo, Probl. Inf. Transm. (USSR) **9**, 117 (1973).
[8] A. Ambainis, M. Mosca, A. Tapp, and R. de Wolf, in *Proceedings of the 41st Annual Symposium on Foundations of Computer Science* (IEEE Computer Society Press, Los Alamitos, CA, 2000), p. 547.
[9] P. Boykin and V. Roychowdhury, quant-ph/0003059.
[10] The $b_{\phi m}^{(\mathrm{out})}$ in Eq. (2) includes an extra system that can be traced out to obtain the original $b_{\phi m}^{(\mathrm{out})}$ in Eq. (1).
[11] C. Bennett, G. Brassard, R. Jozsa, D. Mayers, B. Schumacher, A. Peres, and W. Wootters, J. Mod. Opt. **41**, 2307 (1994).
[12] D. Leung and P. Shor, quant-ph/0201008.
[13] D. DiVincenzo, D. Leung, and B. Terhal, IEEE Trans. Inf. Theory **48**, 580 (2002).
[14] Two ancillae are equivalent if and only if they have the same spectrum. In [8], the ancilla b_m does not depend on m. Thus, our definition is strictly more general.