PHYSICAL REVIEW A **70**, 062306 (2004)

Resources required for exact remote state preparation

Dominic W. Berry

Department of Physics, The University of Queensland, Brisbane, Queensland 4072, Australia
and Centre of Excellence for Quantum Computer Technology, Macquarie University,
Sydney, New South Wales 2109, Australia
and Institute for Quantum Information Science, University of Calgary, Alberta, Canada T2N 1N4

(Received 8 April 2004; published 6 December 2004)

It has been shown [M.-Y. Ye, Y.-S. Zhang, and G.-C. Guo, Phys. Rev. A. **69**, 022310 (2004)] that it is possible to perform exactly faithful remote state preparation using finite classical communication and any entangled state with maximal Schmidt number. Here we give an explicit procedure for performing this remote state preparation. We show that the classical communication required for this scheme is close to optimal for remote state preparation schemes of this type. In addition we prove that it is necessary that the resource state have maximal Schmidt number.

DOI: 10.1103/PhysRevA.70.062306 PACS number(s): 03.67.−a, 03.65.Ud

I. INTRODUCTION

Remote state preparation (RSP) is the preparation of a state at a remote location using entanglement and classical communication [1–7]. In general, one may perform exactly faithful RSP [2,3,7], producing exactly the desired state, or asymptotically faithful RSP, where the fidelity approaches one as the number of states prepared approaches infinity [1,3–6].

It is well known that it is not possible to perform exactly faithful RSP without entanglement. An infinite amount of classical information is required to exactly represent an arbitrary state, and therefore exact RSP would require an infinite amount of classical communication if there were no entangled resource. A method for exact RSP of a restricted ensemble of states is given in Ref. [2], and an alternative method for exact RSP of arbitrary states is given in Ref. [3]. Recently Ye *et al.* [7] showed that it is possible to perform exact RSP using any pure entangled state, provided the Schmidt number is equal to the system dimension. However, the proof given in Ref. [7] does not give a complete technique for performing this remote state preparation.

Here we give an explicit technique that is based upon an approximate technique without entanglement, and quantify how much classical communication is required for this scheme. Similarly to the proof in Ref. [7], this technique has three steps: an entanglement transformation, followed by a disentangling measurement, and a final unitary transformation. In Sec. II we describe these steps, giving a technique for achieving the required entanglement transformation which improves upon that given in Ref. [7].

The final unitary transformation is based upon an approximation of the state. We give a simple method for approximating the state in Sec. II, then consider alternative methods in Sec. III. We give an explicit method that is more efficient for large system dimension, and also derive a nonconstructive method that requires less communication. In addition, we derive a lower bound on the communication required for this step. This lower bound provides a lower bound on the communication required for RSP schemes of this type, although it does not rule out the possibility of some more general method requiring less communication. However, it can be shown that it is necessary for the initial entangled state to have maximal Schmidt number, even for arbitrary RSP schemes. We give this proof in Sec. IV. Lastly we conclude in Sec. V.

II. EXPLICIT SCHEME

As in Ref. [7], the initial state is an entangled state of the form

$$|\mathrm{A}\rangle = \sum_{k=0}^{d-1} \alpha_k |k\rangle|k\rangle, \qquad (1)$$

where the α_k are positive real numbers, and each subsystem is of dimension d. Any entangled state with maximal Schmidt number may be brought to this form via local operations. The state we wish to prepare is

$$|\beta\rangle = \sum_{k=0}^{d-1} \beta_k |k\rangle, \qquad (2)$$

where the β_k may be complex.

To explain this remote state preparation scheme, we first explain a simple approximate scheme that one would use if no entangled resource state were available. In this case, one would communicate an approximation of the coefficients β_k, and prepare a state based on that approximation. To approximate β_k, note that the real and imaginary parts of β_k will be numbers in the interval $[-1, 1]$. We can approximate β_k by dividing the interval $[-1, 1]$ into D subintervals of length $2/D$

$$[-1,2/D-1),\ [2/D-1,4/D-1),\ \ldots,\ [1-2/D,1]. \qquad (3)$$

We then denote the numbers of the subintervals that the real and imaginary parts of β_k lie in as n_k^r and n_k^c, respectively. That is,

$$n_k^r = \min\{D, \lfloor D(\mathrm{Re}\beta_k + 1)/2 \rfloor + 1\}, \qquad (4)$$

$$n_k^c = \min\{D, \lfloor D(\mathrm{Im}\beta_k + 1)/2 \rfloor + 1\}.$$

We use the notation convention that $\lfloor\ \rfloor$ and $\lceil\ \rceil$ are the floor and ceiling functions, respectively. The min takes account of the fact that the last subinterval is closed, so 1 lies in subinterval D. We may then approximate the real and imaginary parts of β_k as

$$\mathrm{Re}\beta_k \approx (2n_k^r - 1)/D - 1, \quad \mathrm{Im}\beta_k \approx (2n_k^c - 1)/D - 1. \quad (5)$$

The error in this approximation will be no more than $1/D$. We may define a state corresponding to this approximation by

$$|\widetilde{\beta}'\rangle = \sum_{k=0}^{d-1} \{(2n_k^r - 1)/D - 1 + i[(2n_k^c - 1)/D - 1]\}|k\rangle. \quad (6)$$

This state will satisfy

$$\| |\beta\rangle - |\widetilde{\beta}'\rangle \| \leqslant \frac{\sqrt{2d}}{D}. \quad (7)$$

However, the state $|\widetilde{\beta}'\rangle$ is not necessarily normalized; the state that is prepared will be the corresponding normalized state, $|\beta'\rangle$. This state may be a slightly poorer approximation, but will still satisfy (see Appendix A)

$$|\langle\beta|\beta'\rangle|^2 \geqslant 1 - \frac{2d}{D^2}. \quad (8)$$

Without an entangled state, one would communicate the $2d$ numbers n_k^r and n_k^c using $2d \log D$ bits. Here we use the convention that log indicates logarithms base 2. We also use the convention that the number of "bits" is the logarithm base 2 of the number of messages, and need not be an integer. The preparer would intialize the system in the state $|0\rangle$, then apply a unitary operation U such that the final state is $|\beta'\rangle$.

In the case where an entangled state is available, one may initialize the system in an alternative state $|\psi\rangle$ that is close to $|0\rangle$, such that the operation U takes the system to the exact state $|\beta\rangle$. We express the required initial state $|\psi\rangle$ as

$$|\psi\rangle = \sum_{k=0}^{d-1} \psi_k e^{i\varphi_k}|k\rangle. \quad (9)$$

In order to prepare this state, we first apply an entanglement transformation scheme to transform the entangled state $|\mathrm{A}\rangle$ to a second state

$$|\Psi\rangle = \sum_{k=0}^{d-1} \psi_k |k\rangle|k\rangle. \quad (10)$$

The communication that is required depends on the entanglement transformation method that is used. There are a number of different methods of performing entanglement transformations [8–10], but there is the problem that most of these methods require local operations in subsystem 2 that are dependent on the state to be prepared.

It is possible to use the entanglement transformation scheme in Ref. [9], though this method requires communication of $\log d!$ bits to communicate the permutation used. Via Caratheodory's theorem one may restrict the number of possible permutations to $d^2 - 2d + 2$, indicating that the communication required is approximately $2 \log d$. However, the set of $d^2 - 2d + 2$ permutations is dependent on the state to be prepared, so it is still necessary to communicate $\log d!$ bits.

Here we describe a straightforward method of determining a set of permutations that is independent of the state to be prepared. In general, in order to perform the entanglement transformation, it is necessary that $\vec{\alpha}^2 \prec \vec{\psi}^2$. Here we apply the slightly stronger condition that $\psi_0^2 \geqslant 1 - r^2(d-1)$, where $r = \min\{\alpha_i\}$. This condition implies that the majorization relation holds (see Appendix B).

The entanglement transformation may be achieved via a two step process. First the state is transformed from $|\mathrm{A}\rangle$ to the intermediate state

$$|\Phi\rangle = \sum_{k=0}^{d-1} \phi_k |k\rangle|k\rangle, \quad (11)$$

where $\phi_0 = \psi_0$ and $\phi_k = \sqrt{(1-\psi_0^2)/(d-1)}$ for $k > 0$. This entanglement transformation may be achieved using the measurement operators

$$A_k = \sqrt{p_k}\left(\sum_{l=1;l\neq k}^{d-1} \frac{\phi_l}{\alpha_l}|l\rangle\langle l| + \frac{\phi_k}{\alpha_0}|0\rangle\langle 0| + \frac{\phi_0}{\alpha_k}|k\rangle\langle k| \right), \quad (12)$$

for $d-1 \geqslant k > 0$, and

$$A_0 = \sqrt{p_0}\sum_{l=0}^{d-1} \frac{\phi_l}{\alpha_l}|l\rangle\langle l|. \quad (13)$$

The probabilities $p_k = (|\alpha_k|^2 - \phi_k^2)/(\phi_0^2 - \phi_k^2)$ for $k > 0$ and $p_0 = 1 - \Sigma_{k>0} p_k$. On obtaining measurement result k, if $k > 0$ it is necessary to swap states $|0\rangle$ and $|k\rangle$. The total number of measurement results is d, so the communication required is $\log d$.

This entanglement transformation is followed by an entanglement transformation to take the state from $|\Phi\rangle$ to $|\Psi\rangle$. In this case the measurement operators required are

$$B_k = \frac{1}{\sqrt{d-1}}\left(|0\rangle\langle 0| + \sum_{l=1}^{d-1} \frac{\psi_{l\oplus k}}{\phi_l}|l\rangle\langle l| \right), \quad (14)$$

where $d-1 \geqslant k > 0$ (there is no measurement operator for $k = 0$). The notation $\oplus$ is used to indicate addition modulo $d - 1$ but excluding 0 (i.e., $1 + [(l+k-1) \bmod (d-1)]$). On obtaining measurement result k, it is necessary to perform a cyclic permutation of the states $|1\rangle$ to $|d-1\rangle$. The total number of possible measurement results is $d-1$, so the communication required is $\log(d-1)$. Thus this method allows one to transform $|\mathrm{A}\rangle$ to $|\Psi\rangle$ with communication of only $\log(d^2 - d)$.

One may then use the method applied in the proof of Theorem 1 of Ref. [7] to obtain the state $|\psi\rangle$. That is, one may apply the projection operators

$$P_k = \frac{1}{d}|\chi_k\rangle\langle\chi_k|, \quad (15)$$

where

$$|\chi_k\rangle = \sum_l e^{i[(2\pi/d)kl-\varphi_l]}|l\rangle. \qquad (16)$$

Upon obtaining measurement result k one performs the local operation

$$C_k = \sum_l e^{i(2\pi/d)kl}|l\rangle\langle l|. \qquad (17)$$

This step requires an additional $\log d$ bits of classical communication.

The final step is to perform the local operation in subsystem 1 to take the state from $|\psi\rangle$ to $|\beta\rangle$. Communication of the numbers n_k^r and n_k^c that specify this operation requires communication of $2d\log D$. To determine the value of D necessary, note that we have required $\psi_0^2 \geqslant 1-r^2(d-1)$ in order to perform the entanglement transformation. As $\psi_0^2 = |\langle 0|\psi\rangle|^2 = |\langle\beta'|\beta\rangle|^2$, ψ_0^2 is equal to the fidelity between the state to be prepared, $|\beta\rangle$, and the approximate state $|\beta'\rangle$. From Eq. (8), the condition $\psi_0^2 \geqslant 1-r^2(d-1)$ will be satisfied for D equal to

$$D_1 = \left\lceil \sqrt{\frac{2d}{r^2(d-1)}} \right\rceil. \qquad (18)$$

To summarize, the RSP scheme with entanglement is a three step process.

Step 1. Transform $|\mathrm{A}\rangle$ to $|\Psi\rangle$ using the measurement operators (12), (13), and (14). The communication required is $\log(d^2-d)$.

Step 2. Apply the method given in the proof of Theorem 1 of Ref. [7] to prepare the unentangled state $|\psi\rangle$. This step requires $\log d$ bits of communication.

Step 3. Perform the unitary operation U to transform $|\psi\rangle$ to $|\beta\rangle$. This step requires communication of the numbers n_k^r and n_k^c to determine the operation U, and therefore requires communication of $2d\log D_1$ bits.

III. CLASSICAL COMMUNICATION REQUIRED

The total classical communication for this scheme is approximately $3\log d + 2d\log D_1$. The classical communication required for this scheme is least when the entangled state used is close to a maximally entangled state. The amount of classical communication required goes to infinity as the entanglement approaches zero; there is, therefore, a tradeoff, just as in the asymptotic schemes considered by Refs. [3,4].

The classical communication required is shown in Fig. 1 for the case of a qubit. Comparing with the figure given in Refs. [3,4], we can see that the classical communication is significantly larger than for asymptotically faithful RSP. In contrast to the asymptotic case, it is also possible for the classical communication to approach infinity even if the entanglement is not approaching zero. This is possible because one of the Schmidt coefficients can become arbitrarily small even if the entanglement does not.

One question that naturally arises is whether it is possible to perform this RSP scheme with less classical communication. The total classical communication required for steps 1 and 2 only scales as $\log d$. This communication is already small, and it is unlikely that it can be improved upon. However, the communication for the final step is $2d\log D_1$, which is much larger.

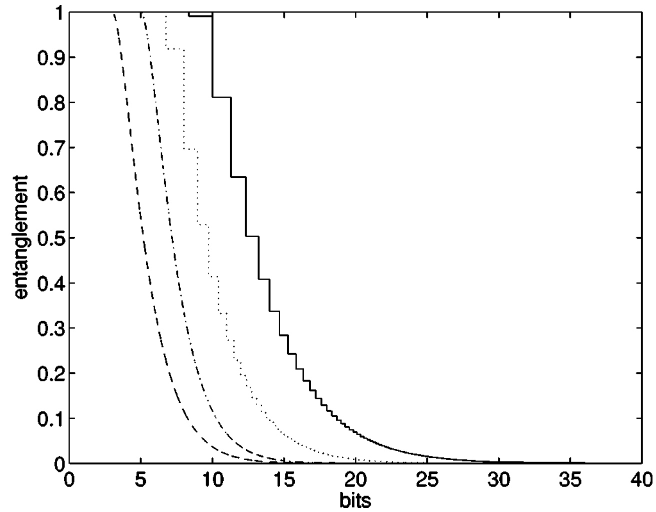

FIG. 1. The entanglement versus classical communication for the exact RSP of qubit states using a partially entangled state. The solid curve is that based on the first scheme given, and the dotted line gives the communication required when β_0 is taken to be real. The dashed-dotted line is the upper bound on the communication for the nonconstructive scheme, and the dashed line is a lower bound on the communication.

In the following we discuss ways of reducing the communication for this final step. First we give an explicit method that reduces the communication required, then give a more efficient, but nonconstructive method, and lastly give a lower bound on the communication required for this step.

A. Explicit method

One may slightly reduce the communication required for step 3 by noting that the global phase is arbitrary, so we may take β_0 to be real. Then it is only necessary to approximate $2d-1$ numbers, and we obtain the fidelity

$$|\langle\beta|\beta'\rangle|^2 \geqslant 1 - \frac{2d-1}{D^2}. \qquad (19)$$

The slightly lower value of D may be taken

$$D_2 = \left\lceil \sqrt{\frac{2d-1}{r^2(d-1)}} \right\rceil, \qquad (20)$$

and the total communication for step 3 is $(2d-1)\log D_2$. This only gives a slight reduction in the communication required; an example for qubit states is given in Fig. 1.

For large system dimensions it is possible to use a more efficient coding of the state. One method is to record the signs of the real and imaginary parts of β_k, then use n_k^r and n_k^c to approximate the absolute values of $\mathrm{Re}\beta_k$ and $\mathrm{Im}\beta_k$. For large d most of the n_k^r and n_k^c will be small, so it is more efficient to record the numbers of digits in the binary representations of n_k^r and n_k^c, as well as those digits. The total communication required for step 3 is then no more than (see Appendix C)

$$(2d-1)\left[\log(1/r\sqrt{d-1}) + \log\lceil \log D_3\rceil + 2\right], \tag{21}$$

where

$$D_3 = \left\lceil \sqrt{\frac{2d-1}{4r^2(d-1)}} \right\rceil. \tag{22}$$

The first term is the communication required for the digits, and the second term is the communication required for the numbers of digits. The third term includes a correction for rounding, as well as the communication required for the signs.

In assessing the scaling of each of the terms with d it is necessary to assume a scaling for r. It is not possible to take r to be independent of d, because $r \le 1/\sqrt{d}$. If $r \propto 1/\sqrt{d}$, the first term in Eq. (21) scales approximately linearly with d, whereas the second term scales as $d \log\log d$, and therefore is dominant for large d. However, this situation is unlikely, because it would mean that the communication required for the numbers of digits in n_k^r and n_k^c is less than that for the digits themselves. It is more realistic to assume that r decreases more rapidly than $1/\sqrt{d}$ (for example, as $1/d$); this is because for a larger dimension, it is more likely that one of the Schmidt coefficients is exceptionally small. Under this assumption, the first term is dominant, as would be expected.

B. Nonconstructive method

It is possible to further improve the efficiency of the coding, although the proof is not constructive. In general, in order to approximate a state with fidelity $1-\epsilon^2$, it is necessary to have a set of states $\mathcal{M}=\{|\varphi_k\rangle\}$, such that for any state $|\beta\rangle$, the fidelity between $|\beta\rangle$ and some element of $\mathcal{M}$ is at least $1-\epsilon^2$. In the following discussion we refer to this condition as the fidelity condition. Given this set, to approximate $|\beta\rangle$, we communicate the index k such that $|\varphi_k\rangle$ has fidelity at least $1-\epsilon^2$ with $|\beta\rangle$. The communication required is then the logarithm (base 2) of the number of states in $\mathcal{M}$. It was shown in Ref. [6] that the number of states in $\mathcal{M}$ need be no greater than $(2.5/\epsilon)^{2d}$; here we apply a similar method to improve upon this bound.

In order to obtain a set that has a small number of elements, we introduce an additional condition. This condition, which we will call the spacing condition, is that for all $|\varphi_k\rangle$, $|\varphi_l\rangle \in \mathcal{M}$, if $k \neq l$ then $|\langle\varphi_k|\varphi_l\rangle|^2 < 1-\epsilon^2$. This condition means that no two elements of $\mathcal{M}$ have fidelity of $1-\epsilon^2$ or more with each other. We denote the largest set satisfying this condition by $\mathcal{M}_{\max}$; this set must also satisfy the fidelity condition. To show this result, note that if $\mathcal{M}_{\max}$ is the largest set satisfying the spacing condition, then there must be no state $|\beta\rangle$ such that $|\langle\varphi_k|\beta\rangle|^2 < 1-\epsilon^2$ for all $|\varphi_k\rangle \in \mathcal{M}_{\max}$. Otherwise $|\beta\rangle$ could be added to $\mathcal{M}_{\max}$ to obtain a larger set satisfying the spacing condition. Hence, for all $|\beta\rangle$, there must be a state $|\varphi_k\rangle \in \mathcal{M}_{\max}$ such that $|\langle\varphi_k|\beta\rangle|^2 \ge 1-\epsilon^2$, and $\mathcal{M}_{\max}$ therefore satisfies the fidelity condition.

Because no two states in $\mathcal{M}_{\max}$ have fidelity as large as $1-\epsilon^2$ with each other, no state can have fidelity as large as $1-(\epsilon/2)^2$ with more than one member of $\mathcal{M}_{\max}$.[1] Thus the regions of states with fidelity at least $1-(\epsilon/2)^2$ with different elements of $\mathcal{M}_{\max}$ do not intersect. Let us denote by $V(\epsilon)$ the volume of the region of states with fidelity at least $1-\epsilon^2$ with some state $|\varphi\rangle$. From Appendix D, this volume is independent of $|\varphi\rangle$, so we need not include it as an argument. One may therefore determine an upper limit on the number of states in $\mathcal{M}_{\max}$ by dividing the volume of the region of normalized states by $V(\epsilon/2)$. The region of normalized states is the surface of a hypersphere, and has volume $2\pi^d/(d-1)!$. In addition, from Appendix D, $V(\epsilon/2)=2\pi^d(\epsilon/2)^{2d-2}/(d-1)!$. Therefore the number of states in the set $\mathcal{M}_{\max}$ is no larger than $(2/\epsilon)^{2d-2}$.

For the nonconstructive method, to approximate $|\beta\rangle$ we simply communicate the index k of a state $|\varphi_k\rangle \in \mathcal{M}_{\max}$ such that $|\langle\varphi_k|\beta\rangle|^2 \ge 1-\epsilon^2$. In order to be able to perform the entanglement transformation in step 1, we require the state to be approximated with fidelity at least $1-\epsilon^2$, where $\epsilon = r\sqrt{d-1}$. Therefore, the communication required for this nonconstructive scheme is no more than

$$(2d-2)\log(2/r\sqrt{d-1}). \tag{23}$$

C. Lower bound

We may place a lower bound on the communication required in a similar way. Let $\mathcal{M}$ be a set of states satisfying the fidelity condition. The volume of the set of states that may be approximated by $|\varphi_k\rangle \in \mathcal{M}$ with fidelity at least $1-\epsilon^2$ is equal to $V(\epsilon)$. If $\mathcal{M}$ satisfies the fidelity condition, $V(\epsilon)$ multiplied by the number of states in $\mathcal{M}$ must be at least as large as the total volume of normalized states. We may therefore place a lower bound on the number of states in $\mathcal{M}$ by dividing the total volume of normalized states by $V(\epsilon)$. The volume of normalized states is $2\pi^d/(d-1)!$, and $V(\epsilon)=2\pi^d\epsilon^{2d-2}/(d-1)!$. Thus the total number of states can be no less than $(1/\epsilon)^{2d-2}$.

Taking $\epsilon = r\sqrt{d-1}$, the classical communication can be no less than

$$(2d-2)\log(1/r\sqrt{d-1}). \tag{24}$$

The communication required for the nonconstructive method is close to this, as it is no more than $2d-2$ bits larger. In addition, the lower bound in Eq. (24) is similar to the first term in Eq. (21); therefore, provided the first term in Eq. (21) is dominant, the explicit method that we described in Sec. III A is close to optimal.

To summarize, the communication required for the various methods is as given in Table I. This is the communication required for step 3; that is, the communication required to obtain an approximation of the state with fidelity at least $1-r^2(d-1)$. The total communication for RSP schemes of this type is equal to these values plus $\log[d^2(d-1)]$, which is the communication required for the first two steps. There-

[1]If $|\beta\rangle$ had fidelity as large as $1-(\epsilon/2)^2$ with both $|\varphi_k\rangle$ and $|\varphi_l\rangle$, by the chain rule for fidelities, the fidelity between $|\varphi_k\rangle$ and $|\varphi_l\rangle$ would have to be at least $1-\epsilon^2$.

TABLE I. The communication required for step 3 using various methods, as well as the lower bound.

Method	Communication required
Simple method from Sec. II	$2d \log D_1$, where $D_1 = \left\lceil \sqrt{\frac{2d}{r^2(d-1)}} \right\rceil$.
Simple method taking β_0 real	$(2d-1) \log D_2$, where $D_2 = \left\lceil \sqrt{\frac{2d-1}{r^2(d-1)}} \right\rceil$.
More efficient explicit method	$(2d-1) [\log(1/r\sqrt{d-1}) + \log\lceil \log D_3 \rceil + 2]$, where $D_3 = \left\lceil \sqrt{\frac{2d-1}{4r^2(d-1)}} \right\rceil$.
Nonconstructive method	$(2d-2) \log(2/r\sqrt{d-1})$
Lower bound	$(2d-2) \log(1/r\sqrt{d-1})$

fore, for exact RSP schemes of this type, the total communication used cannot be less than

$$\log[d^2(d-1)] + (2d-2) \log(1/r\sqrt{d-1}), \qquad (25)$$

and there will be a scheme that uses communication of

$$\log[d^2(d-1)] + (2d-2) \log(2/r\sqrt{d-1}). \qquad (26)$$

These expressions are plotted for the case $d=2$ in Fig. 1. There is only a few bits difference between Eqs. (25) and (26), and the explicit scheme given before requires communication that is greater than both Eqs. (25) and (26).

It must be emphasized that the lower bound (25) is not a lower bound for arbitrary exact RSP schemes. One reason is that it was derived from the requirement that a state must be approximated with fidelity $1-r^2(d-1)$. In order for it to be possible to apply the entanglement transformation from $|\mathrm{A}\rangle$ to $|\Psi\rangle$, it is only necessary that $\vec{\alpha}^2 \prec \vec{\psi}^2$. The volume of states satisfying this condition will, in most cases, be larger, so it will be possible to specify the state with less communication (though more communication will be required for the state transformation). It is also possible that there may be some very different RSP scheme that uses less communication.

IV. SCHMIDT NUMBER REQUIRED

It is possible to obtain stronger results for the Schmidt number of the entangled state. For the RSP scheme outlined above the Schmidt number of the entangled state used must be maximal. It is possible to prove that this is necessary for arbitrary exact RSP schemes as follows. First, note that the above exact RSP scheme is equivalent to a local measurement performed in subsystem A, followed by a unitary transformation applied in subsystem B that is based on information communicated from subsystem A.

This is not the most arbitrary RSP scheme possible. In general, one may add local ancillas, perform local unitary transformations, local general measurements, and two-way communication. The POVMs used in each subspace may depend on the results of previous measurements. Let the initial state be

$$|\mathrm{A}\rangle = \sum_{k=0}^{d'-1} \alpha_k |k\rangle|k\rangle, \qquad (27)$$

where $d' < d$. Because the local unitary transformations and measurement operators on subsystem A commute with those on subsystem B, we may combine the operators on subsystem A into a single operator $M_A(\beta, \vec{\phi})$. This operator may depend on the state to be prepared, $|\beta\rangle$, as well as the results of measurements, $\vec{\phi}$. The vector $\vec{\phi}$ contains the results of measurements performed in both subsystems. We allow $\vec{\phi}$ to contain real numbers resulting from measurements in both subsystems (even though these results cannot be communicated with finite classical communication), as this does not make the RSP scheme less general. We also combine the operators on subsystem B into a single operator $M_B(\vec{n}, \vec{\phi})$. This operator also may depend on the results of measurements $\vec{\phi}$, as well as additional information $\vec{n}$ communicated from subsystem A.

After performing operation $M_A(\beta, \vec{\phi})$, the reduced density matrix in subsystem B is

$$\rho \otimes \rho_{\mathrm{anc}}, \qquad (28)$$

where ρ_{anc} is the state of the ancilla for subsystem B. As the ancilla for subsystem B is initially unentangled, it cannot be modified in any way by $M_A(\beta, \vec{\phi})$. In addition, although ρ will depend on $M_A(\beta, \vec{\phi})$, it must still be orthogonal to $|k\rangle$ for

$k > d' - 1$. Without loss of generality, we assume that it is possible to prepare any state ρ, provided it is orthogonal to $|k\rangle$ for $k > d' - 1$. In order to obtain perfect RSP, we require

$$|\beta\rangle\langle\beta| = \mathrm{Tr}_{\mathrm{anc}}\Big[M_B(\vec{n},\vec{\phi})(\rho \otimes \rho_{\mathrm{anc}})M_B^\dagger(\vec{n},\vec{\phi})\Big]. \tag{29}$$

If Eq. (29) holds for ρ and ρ_{anc}, there must be pure states for which it holds. Therefore we may take these states to be $|\psi\rangle$ and $|\psi_{\mathrm{anc}}\rangle$. Equation (29) then becomes

$$|\beta\rangle \otimes |\psi'_{\mathrm{anc}}\rangle = M_B(\vec{n},\vec{\phi})|\psi\rangle \otimes |\psi_{\mathrm{anc}}\rangle, \tag{30}$$

where $|\psi'_{\mathrm{anc}}\rangle$ is the final state of the ancilla.

In order to obtain $|\beta\rangle$, for any given measurement results $\vec{\phi}$, one may adjust $|\psi\rangle$ and the communicated information $\vec{n}$. An arbitrary pure d-dimensional state $|\beta\rangle$ is equivalent to a point on a $2d-1$ dimensional hypersphere (one dimension may be omitted because we may take β_0 to be real). Because $|\psi_{\mathrm{anc}}\rangle$ is fixed, and $|\psi\rangle$ is orthogonal to $|k\rangle$ for $k > d' - 1$, the state $|\psi\rangle \otimes |\psi_{\mathrm{anc}}\rangle$ is equivalent to a point on a $2d' - 1$ dimensional hypersphere. Since there is only a finite set of messages that may be communicated $\vec{n}$, the set of states obtained by varying $\vec{n}$ and $|\psi\rangle$ can only correspond to a $2d' - 2$ dimensional space, and cannot fill the $2d-2$ dimensional space corresponding to the set of states $|\beta\rangle$.

Therefore, even if it is possible to prepare an arbitrary d'-dimensional state and perform one of a finite number of operations, it is not possible to prepare an arbitrary d-dimensional state. Thus it is not possible to exactly prepare an arbitrary d-dimensional state if the resource state has a lower Schmidt number.

V. CONCLUSIONS

We have given an explicit scheme for performing exact RSP using an arbitrary entangled state with a maximal Schmidt number and classical communication that is close to optimal for schemes of this type. The scheme is a three-step process, involving an entanglement transformation, followed by a disentangling measurement, and a final unitary operation to obtain the exact state.

This method improves on that given in Ref. [7] in two main ways.

(1) The communication required for the entanglement transformation is less than $2 \log d$, as compared to $\log d!$ for Ref. [7].

(2) We have given an explicit method for determining the final unitary operation.

The majority of the communication is required for the final unitary operation. The communication required for this step is slightly superlinear in d, whereas the communication required for the first two steps is logarithmic in d. This communication is close to optimal, provided the RSP scheme is of this type; however, we have not eliminated the possibility that some more general RSP scheme may require less communication.

This remote state preparation scheme also requires that the Schmidt number of the initial entangled state be maximal. We have proven that this is necessary even for an arbitrary remote state preparation scheme.

ACKNOWLEDGMENTS

I am grateful for valuable discussions with Patrick Hayden, Barry C. Sanders, and Guifré Vidal. This work was supported by Alberta's informatics Circle of Research Excellence (iCORE), the Australian Research Council, and the National Science Foundation under Grant No. EIA-0086038 through the Institute for Quantum Information at the California Institute of Technology.

APPENDIX A: DISTANCE AND FIDELITY

Consider two states that satisfy

$$\||\beta\rangle - |\tilde{\beta}'\rangle\| \leq \epsilon, \tag{A1}$$

where $|\tilde{\beta}'\rangle$ is not necessarily normalized. The state $|\tilde{\beta}'\rangle$ may be expressed as $|\tilde{\beta}'\rangle = a|\beta\rangle + b|\beta^\perp\rangle$, where $|\beta^\perp\rangle$ is orthogonal to $|\beta\rangle$. Then Eq. (A1) is equivalent to $|1-a|^2 + |b|^2 \leq \epsilon^2$, which implies

$$|a| \geq 1 - \sqrt{\epsilon^2 - |b|^2}, \tag{A2}$$

and

$$\frac{|b|}{|a|} \leq \frac{|b|}{1 - \sqrt{\epsilon^2 - |b|^2}}. \tag{A3}$$

The right-hand side of this expression is minimized for $|b|^2 = \epsilon^2 - \epsilon^4$, giving

$$\frac{|b|^2}{|a|^2} \leq \frac{\epsilon^2}{1 - \epsilon^2}. \tag{A4}$$

In turn this implies

$$\frac{|a|^2}{|a|^2 + |b|^2} \geq 1 - \epsilon^2. \tag{A5}$$

If $|\beta'\rangle$ is the normalized state corresponding to $|\tilde{\beta}'\rangle$, then

$$|\langle\beta|\beta'\rangle|^2 = \frac{|a|^2}{|a|^2 + |b|^2}. \tag{A6}$$

Therefore $\||\beta\rangle - |\tilde{\beta}'\rangle\| \leq \epsilon$ implies that $|\langle\beta|\beta'\rangle|^2 \geq 1 - \epsilon^2$.

APPENDIX B: MAJORIZATION AND FIDELITY

In this appendix it is shown that $\vec{\alpha}^2 \prec \vec{\psi}^2$ is satisfied if $\psi_0^2 \geq 1 - (d-1)r^2$. The majorization condition $\vec{\alpha}^2 \prec \vec{\psi}^2$ is equivalent to

$$\sum_{k=0}^{p} {}^{\downarrow}\psi_k^2 \geq \sum_{k=0}^{p} {}^{\downarrow}\alpha_k^2, \tag{B1}$$

where the down arrow indicates that the coefficients are sorted into descending order. Because the ${}^{\downarrow}\psi_k^2$ are in descending order,

$$\frac{1}{p}\sum_{k=1}^{p} {}^{\downarrow}\psi_k^2 \geq \frac{1}{d-p-1}\sum_{k=p+1}^{d-1} {}^{\downarrow}\psi_k^2. \tag{B2}$$

Multiplying on both sides by $d-p-1$ and adding $\Sigma_{k=1}^{p} {}^{\downarrow}\psi_k^2$ gives

$$\frac{d-1}{p}\sum_{k=1}^{p} {}^{\downarrow}\psi_k^2 \geqslant (1-{}^{\downarrow}\psi_0^2). \tag{B3}$$

In turn this gives

$$\sum_{k=0}^{p} {}^{\downarrow}\psi_k^2 \geqslant {}^{\downarrow}\psi_0^2\frac{d-p-1}{d-1} + \frac{p}{d-1}. \tag{B4}$$

Then substituting the inequality $\psi_0^2 \geqslant 1-(d-1)r^2$ (and using ${}^{\downarrow}\psi_0^2 \geqslant \psi_0^2$) gives

$$\sum_{k=0}^{p} {}^{\downarrow}\psi_k^2 \geqslant 1-(d-p-1)r^2. \tag{B5}$$

Because $\alpha_k^2 \geqslant r^2$, it is also the case that

$$1-(d-p-1)r^2 \geqslant \sum_{k=0}^{p} {}^{\downarrow}\alpha_k^2, \tag{B6}$$

thus giving

$$\sum_{k=0}^{p} {}^{\downarrow}\psi_k^2 \geqslant \sum_{k=0}^{p} {}^{\downarrow}\alpha_k^2. \tag{B7}$$

Hence the inequality $\psi_0^2 \geqslant 1-(d-1)r^2$ is sufficient to imply the majorization relation $\vec{\alpha}^2 \prec \vec{\psi}^2$.

APPENDIX C: EFFICIENT CODING

If the numbers n_k^r and n_k^c record the absolute values of the real and imaginary parts of β_k, and the interval [0,1] is divided into D subintervals, then the fidelity is

$$|\langle\beta|\beta'\rangle|^2 \geqslant 1-\frac{2d-1}{4D^2}. \tag{C1}$$

The number of subintervals D should therefore be taken to be equal to

$$D_3 = \left\lceil \sqrt{\frac{2d-1}{4r^2(d-1)}} \right\rceil. \tag{C2}$$

The number of bits required to encode the length of the bitstrings representing each of the numbers n_k^r and n_k^c is $\log\lceil \log D_3\rceil$. In addition β_0 is taken to be real, and we require $2d-1$ bits to record the signs of the real and imaginary parts of β_k. The total communication is therefore

$$\begin{aligned}
&(2d-1)\log\lceil\log D_3\rceil + \lceil\log(n_0^r-1)\rceil + \sum_{k=1}^{d-1}[\lceil\log(n_k^r-1)\rceil \\
&\quad + \lceil\log(n_k^c-1)\rceil] + (2d-1) \\
&\leqslant (2d-1)\log\lceil\log D_3\rceil + \lceil\log(D_3\beta_0)\rceil \\
&\quad + \sum_{k=1}^{d-1}[\lceil\log(D_3\mathrm{Re}\beta_k)\rceil + \lceil\log(D_3\mathrm{Im}\beta_k)\rceil] + (2d-1) \\
&\leqslant (2d-1)\left(\log\frac{D_3}{\sqrt{2d-1}} + \log\lceil\log D_3\rceil + 2\right) \\
&\leqslant (2d-1)\left[\log(1/r\sqrt{d-1}) + \log\lceil\log D_3\rceil + 2\right].
\end{aligned} \tag{C3}$$

APPENDIX D: VOLUME OF REGION OF STATES

Here we consider the problem of determining the volume of the region of states $|\beta\rangle$ for a given $|\varphi\rangle$ that satisfies $|\langle\varphi|\beta\rangle|^2 \geqslant 1-\epsilon^2$. To do this, we write the state $|\beta\rangle$ in the form

$$|\beta\rangle = e^{i\phi}\cos\theta|\varphi\rangle + \sin\theta|\varphi^{\perp}\rangle, \tag{D1}$$

where $|\varphi^{\perp}\rangle$ is a state perpendicular to $|\varphi\rangle$. Every state may be represented in this way when the ranges of ϕ and θ are $[-\pi,\pi]$ and $[0,\pi/2]$, respectively. The condition $|\langle\varphi|\beta\rangle|^2 \geqslant 1-\epsilon^2$ implies that $|\sin\theta| \leqslant \epsilon$. The volume of states is given by

$$V(\epsilon,\varphi) = \int_0^{\arcsin\epsilon} d\theta \int_{-\pi}^{\pi} d\phi (\cos\theta) S_{2d-2}(\sin\theta), \tag{D2}$$

where

$$S_n(r) = \frac{2\pi^{n/2}}{\Gamma(n/2)}r^{n-1} \tag{D3}$$

is the surface area of a hypersphere. It is evident that this expression for the volume is independent of $|\varphi\rangle$, and we therefore omit it as an argument from this point on. Integrating over ϕ and using Eq. (D3) gives

$$\begin{aligned}
V(\epsilon) &= \frac{4\pi^d}{(d-2)!}\int_0^{\arcsin\epsilon}\cos\theta\sin^{2d-3}\theta d\theta \\
&= \frac{4\pi^d}{(d-2)!}\left[\frac{\sin^{2d-2}\theta}{2d-2}\right]_0^{\arcsin\epsilon} = \frac{2\pi^d}{(d-1)!}\epsilon^{2d-2}.
\end{aligned} \tag{D4}$$

Note that using $\epsilon=1$ recovers the formula for the surface area of a $2d$-dimensional hypersphere, which gives the total volume of normalized states.

[1] H.-K. Lo, Phys. Rev. A **62**, 012313 (2000).
[2] A. K. Pati, Phys. Rev. A **63**, 014302 (2001).
[3] C. H. Bennett, D. P. DiVincenzo, P. W. Shor, J. A. Smolin, B. M. Terhal, and W. K. Wootters, Phys. Rev. Lett. **87**, 077902 (2001).
[4] I. Devetak and T. Berger, Phys. Rev. Lett. **87**, 197901 (2001).
[5] D. W. Berry and B. C. Sanders, Phys. Rev. Lett. **90**, 057901 (2003).
[6] C. H. Bennett, P. Hayden, D. W. Leung, P. W. Shor, and A. Winter, e-print quant-ph/0307100.
[7] M.-Y. Ye, Y.-S. Zhang, and G.-C. Guo, Phys. Rev. A **69**, 022310 (2004).
[8] M. A. Nielsen, Phys. Rev. Lett. **83**, 436 (1999).
[9] J. G. Jensen and R. Schack, Phys. Rev. A **63**, 062303 (2001).
[10] M. A. Nielsen and G. Vidal, Quantum Inf. Comput. **1**, 76 (2001).