Faithful remote state preparation using finite classical bits and a nonmaximally entangled state

Ming-Yong Ye, Yong-Sheng Zhang,* and Guang-Can Guo†
Key Laboratory of Quantum Information, University of Science and Technology of China, CAS, Hefei 230026, People's Republic of China
(Received 4 July 2003; published 20 February 2004)

We present many ensembles of states that can be remotely prepared by using minimum classical bits from Alice to Bob and their previously shared entangled state and prove that we have found all the ensembles in two-dimensional case. Furthermore we show that any pure quantum state can be remotely and faithfully prepared by using finite classical bits from Alice to Bob and their previously shared nonmaximally entangled state though no faithful quantum teleportation protocols can be achieved by using a nonmaximally entangled state.

DOI: 10.1103/PhysRevA.69.022310 PACS number(s): 03.67.Hk, 03.65.Ud

I. INTRODUCTION

The question ''What tasks may be accomplished using a given physical resource?'' is of fundamental importance in many areas of physics [1,2]. Remote state preparation (RSP) [3] and quantum teleportation [4] answer partly this question. Both protocols use classical communication and the previously shared entangled state to prepare a quantum state in a remote place. The differences between them are as follows. First, in RSP the sender (Alice) knows the state she wants Bob to prepare while in quantum teleportation Alice need not know the state she wants to send. Second, in RSP, the required resource can be traded off between classical communication cost and entanglement cost while in quantum teleportation, two bits of forward classical communication and one ebit of entanglement (a maximally entangled pair of qubits) per teleported qubit are both necessary and sufficient, and neither resource can be traded off against the other [5]. Lo has shown that for some special ensembles of states, RSP requires less asymptotic classical communication than quantum teleportation [3]. Bennett *et al.* have shown that in the high-entanglement limit the asymptotic classical communication cost of remotely preparing a general qubit is one bit, which is also necessary by causality [5]. Recently, Berry *et al.* have shown it is possible to remotely prepare an ensemble of noncommutative mixed states by using communication that is equal to the Holevo information for this ensemble [6]. Bennett *et al.* [5] and Devetak *et al.* [7] have also investigated low-entanglement remote state preparation which uses more classical bits but less entanglement bits. The results were achieved asymptotically.

Different from the above mentioned researchers, some others investigated faithful and nonasymptotic remote state preparation [8–11]. Pati has shown that a qubit chosen from equatorial or polar great circles on a Bloch sphere can be remotely prepared with one classical bit from Alice to Bob if they share one ebit of entanglement [8]. Leung and Shor have proved that if faithful RSP protocols without back communicating can transmit generic ensembles and are oblivious to Bob, they can be modified to become protocols oblivious to Alice. This indicates that they use at least as much classical communication as that in quantum teleportation [9].

In this paper we generalize Pati's RSP protocol [8] to nonmaximally entanglement and higher-dimensional case. In Sec. II, we present a necessary and sufficient condition of a general RSP protocol, similar to that proposed by Leung and Shor [9] and that by Hayashi *et al.* [12]. Then, we investigate RSP protocols using minimum classical bits. In Sec. III, we investigate RSP protocols that do not use minimum classical bits, and prove that any pure quantum state can be remotely prepared by using finite classical bits and the previously shared nonmaximally entangled state. In Sec. IV, we shall summarize and draw some conclusions.

II. RSP ACHIEVED BY USING MINIMUM CLASSICAL BITS

A general Pati RSP protocol is characterized as follows. Alice and Bob share an entangled state in two d-dimensional systems

$$|\Psi_{AB}\rangle=\sum_{i=0}^{d-1}\alpha_i|i\rangle|i\rangle,\quad \alpha_i>0,\quad \sum_{i=0}^{d-1}\alpha_i^2=1, \tag{1}$$

where $\{|i\rangle\}_{i=0}^{d-1}$ forms an orthonormal basis of d-dimensional Hilbert space. Alice wants Bob to prepare a state $|\Phi\rangle$ which is known to her. She performs a positive operator valued measurement (POVM) measurement on her system A with measurement operators that depend on the state $|\Phi\rangle$. When Alice gets the result m with the probability $p_m(\Phi)$, Bob's system B will be in the state $\rho_m(\Phi)=|\Phi_m\rangle\langle\Phi_m|$. Alice sends the measurement result m to Bob and Bob performs the corresponding unitary operation u_m, which change his system into the state $|\Phi\rangle$ $(u_m|\Phi_m\rangle=|\Phi\rangle)$. It is necessary that u_m is independent of $|\Phi\rangle$ and that $\rho_m(\Phi)$ is a pure state. For Bob, before he receives the result m, his system is

$$\sum_{m=0}^{n-1}p_m(\Phi)|\Phi_m\rangle\langle\Phi_m|=\sum_{i=0}^{d-1}\alpha_i^2|i\rangle\langle i|. \tag{2}$$

Substituting $u_m|\Phi_m\rangle=|\Phi\rangle$ into Eq. (2), we can obtain

*Electronic address: yshzhang@ustc.edu.cn
†Electronic address: gcguo@ustc.edu.cn

 ©2004 The American Physical Society

$$\sum_{m=0}^{n-1} p_m(\Phi)u_m^{\dagger}|\Phi\rangle\langle\Phi|u_m=\sum_{i=0}^{d-1}\alpha_i^2|i\rangle\langle i|. \tag{3}$$

Equation (3) is a necessary condition for such RSP protocols. It is also a sufficient condition [9,12], because Alice only needs to apply a measurement on her system A with POVM operators

$$\left\{M_m=p_m(\Phi)\left(\sum_{i=0}^{d-1}\frac{1}{\alpha_i}|i\rangle\langle i|\right)\rho_m^T(\Phi)\left(\sum_{i=0}^{d-1}\frac{1}{\alpha_i}|i\rangle\langle i|\right)\right\}_{m=0}^{n-1},$$

where $\rho_m^T(\Phi)$ is the transposition of $\rho_m(\Phi)$. To prove this we need to verify three things. First, each M_m is a positive operator and $\Sigma_{m=0}^{n-1}M_m=I_d$. This is obvious from Eq. (3). Second, when Alice implements this POVM measurement the probability of an outcome m is $p_m(\Phi)$. This probability is calculated as follows. $\langle\Psi_{AB}|M_m|\Psi_{AB}\rangle=p_m(\Phi)\mathrm{tr}\rho_m^T(\Phi)=p_m(\Phi)$. Third, when the outcome is m the resultant state of system B is $\rho_m(\Phi)$. This state is calculated as follows. $1/p_m(\Phi)\mathrm{tr}_A(M_m|\Psi_{AB}\rangle\langle\Psi_{AB}|)=\rho_m(\Phi)$.

Given the unitary operations $\{u_m\}_{m=0}^{n-1}$, we can find an ensemble of states that satisfy Eq. (3). If the number of states in the ensemble is less than n the RSP protocol is useless. We are interested in what ensemble of states can be remotely prepared by using a given shared entanglement resource. When we say an ensemble of states can be remotely prepared, we mean that we can find a set of operators $\{u_m\}_{m=0}^{n-1}$ that satisfy Eq. (3) for any state in this ensemble.

In Eq. (3), it is obvious that $n\geqslant slantd$ must be satisfied. We have investigated RSP protocols with $n=d$. These are faithful RSP protocols using minimum classical bits.

Theorem 1. Suppose Alice and Bob have shared an entangled state in Eq. (1). The ensemble of states

$$\left\{|\Phi\rangle=\sum_{j=0}^{d-1}\alpha_j e^{i\varphi_j}|j\rangle,\quad \forall\ \varphi_j\right\} \tag{4}$$

can be remotely prepared by using $\ln d$ bits from Alice to Bob and their previously shared entangled state, where $\{\alpha_j\}_{j=0}^{d-1}$ and $\{\varphi_j\}_{j=0}^{d-1}$ are known to Alice. Particularly, if Alice and Bob share a maximally entangled state, we get the same results as those in Refs. [8,11].

Proof. We present an explicit method in which Alice prepared the ensemble of states. Suppose the state Alice wants Bob to prepare is

$$|\Phi\rangle=\sum_{j=0}^{d-1}\alpha_j e^{i\varphi_j}|j\rangle, \tag{5}$$

where $\{\varphi_j\}_{j=0}^{d-1}$ is known to Alice. First, Alice transforms locally the shared entangled state into

$$|\Psi_{AB}\rangle=\sum_{i=0}^{d-1}\alpha_i e^{i\varphi_i}|i\rangle|i\rangle,\quad \alpha_i>0,\quad \sum_{i=0}^{d-1}\alpha_i^2=1, \tag{6}$$

and then she performs a projective measurement on her system A with the measurement operators

$$\left\{P_m=\frac{1}{d}\left(\sum_{j=0}^{d-1}e^{i(2\pi/d)mj}|j\rangle\right)\left(\sum_{j=0}^{d-1}e^{-i(2\pi/d)mj}\langle j|\right)\right\}_{m=0}^{d-1}. \tag{7}$$

The measurement result, (supposed to be m), will be sent to Bob. When Bob receives the message m, he performs the corresponding unitary operation

$$u_m=\sum_{j=0}^{d-1}e^{i(2\pi/d)mj}|j\rangle\langle j| \tag{8}$$

on his system B to transform the system B into state (5). Q.E.D.

Obviously we have the following corollary.

Corollary. Suppose Alice and Bob have shared an entangled state in Eq. (1). The ensemble of states

$$\left\{v|\Phi\rangle=v\left(\sum_{j=0}^{d-1}\alpha_j e^{i\varphi_j}|j\rangle\right),\quad \forall\varphi_j\right\}$$

can be remotely prepared by using $\log d$ bits from Alice to Bob and their previously shared entangled state, where v is an arbitrary unitary operators in d-dimensional Hilbert space.

In the two-dimensional case the corollary shows that qubits chosen from the same circle with radius $\sqrt{1-(\alpha_0^2-\alpha_1^2)^2}$ on a Bloch sphere can be remotely prepared by using one classical bit from Alice to Bob and their previously shared entangled state. Theorem 2 proves that we have found all the ensembles in the two-dimensional case.

Theorem 2. Suppose Alice and Bob have shared an entangled state

$$|\Psi_{AB}\rangle=\alpha_0|0\rangle|0\rangle+\alpha_1|1\rangle|1\rangle,\quad \alpha_0,\alpha_1>0,\quad \alpha_0^2+\alpha_1^2=1. \tag{9}$$

If there is an ensemble of states that can be remotely prepared by using one bit from Alice to Bob and their previously shared entangled state, this ensemble must be in the form

$$\{v|\Phi\rangle=v(\alpha_0|0\rangle+\alpha_1 e^{i\varphi}|1\rangle),\forall\ \varphi\}, \tag{10}$$

where v is a unitary operator in two-dimensional Hilbert space.

Proof. If a state $|\Phi\rangle$ can be remotely prepared, there should be unitary operators u_0 and u_1, and probabilities $p_0(\Phi)$ and $p_1(\Phi)$ which satisfy the necessary and sufficient condition of RSP. From Eq. (3) we have

$$\begin{aligned}&p_0(\Phi)u_0^{\dagger}|\Phi\rangle\langle\Phi|u_0+p_1(\Phi)u_1^{\dagger}|\Phi\rangle\langle\Phi|u_1\\&\quad=\alpha_0^2|0\rangle\langle 0|+\alpha_1^2|1\rangle\langle 1|.\end{aligned} \tag{11}$$

From Eq. (11) we can find that

$$\sqrt{p_0(\Phi)}\left(\frac{1}{\alpha_0}|0\rangle\langle 0|+\frac{1}{\alpha_1}|1\rangle\langle 1|\right)u_0^{\dagger}|\Phi\rangle$$

and

$$\sqrt{p_1(\Phi)}\left(\frac{1}{\alpha_0}|0\rangle\langle 0|+\frac{1}{\alpha_1}|1\rangle\langle 1|\right)u_1^{\dagger}|\Phi\rangle$$

form an orthonormal basis. So we can get

$$\langle\Phi|u_0\left(\frac{1}{\alpha_0^2}|0\rangle\langle 0|+\frac{1}{\alpha_1^2}|1\rangle\langle 1|\right)u_1^{\dagger}|\Phi\rangle=0. \tag{12}$$

It is the same as

$$\mathrm{tr}\left[\left(\frac{1}{\alpha_0^2}|0\rangle\langle 0|+\frac{1}{\alpha_1^2}|1\rangle\langle 1|\right)u_1^{\dagger}u_0(u_0^{\dagger}|\Phi\rangle\langle\Phi|u_0)\right]=0. \tag{13}$$

We assume that

$$u_1^{\dagger}u_0=\cos\frac{\theta_0}{2}I_2-i\sin\frac{\theta_0}{2}(x_0\sigma_x+y_0\sigma_y+z_0\sigma_z) \tag{14}$$

and

$$u_0^{\dagger}|\Phi\rangle\langle\Phi|u_0=\tfrac{1}{2}(I_2+x\sigma_x+y\sigma_y+z\sigma_z), \tag{15}$$

where σ_x,σ_y, and σ_z are Pauli operators.

Substituting Eqs. (14) and (15) into Eq. (13), we get

$$\cos\frac{\theta_0}{2}+z(\alpha_1^2-\alpha_0^2)\cos\frac{\theta_0}{2}+(\alpha_1^2-\alpha_0^2)(x_0y-y_0x)\sin\frac{\theta_0}{2}=0, \tag{16}$$

$$\sin\frac{\theta_0}{2}[(\alpha_1^2-\alpha_0^2)z_0+x_0x+y_0y+z_0z]=0. \tag{17}$$

Because $|\Phi\rangle$ is a pure state, so

$$x^2+y^2+z^2=1. \tag{18}$$

The common solutions of Eqs. (16)–(18) represent the ensemble of states that can be remotely prepared. Generally, Eqs. (16) and (17) represent two planes and Eq. (18) represents a sphere. If Eqs. (16) and (17) represent two different planes there are at most two common solutions of Eqs. (16)–(18), which are trivial. So we should seek the appropriate $u_1^{\dagger}u_0$, which ensures that Eqs. (16) and (17) represent the same plane. The requirement that Eqs. (16) and (17) represent the same plane leads to the following results:

$$\theta_0=\pi,\quad x_0=y_0=0,\quad z=\alpha_0^2-\alpha_1^2,\quad \text{when}\quad \alpha_0\neq\alpha_1, \tag{19}$$

$$\theta_0=\pi,\quad x_0x+y_0y+z_0z=0,\quad \text{when}\quad \alpha_0=\alpha_1. \tag{20}$$

Equations (15), (19), and (20) show that qubits chosen from the same circle with radius $\sqrt{1-(\alpha_0^2-\alpha_1^2)^2}$ on a Bloch sphere can be remotely prepared by using one classical bit from Alice to Bob and their previously shared entangled state. This result is the same as the corollary in two-dimensional case. Q.E.D.

III. REMOTE PREPARATION OF A GENERAL PURE QUANTUM STATE

Now we turn to investigate RSP protocols which do not use minimum classical bits. We will show that any pure quantum state can be faithfully remotely prepared by using finite classical bits and a nonmaximally entangled state. To prove this result, we first prove the following lemma.

Lemma. Suppose Alice and Bob have shared an entangled state in Eq. (1). The ensemble of states

$$S=\left\{|\Phi\rangle=\sum_{j=0}^{d-1}\beta_j e^{i\varphi_j}|j\rangle,\quad \forall\ \varphi_j,(\alpha_j^2)_{j=0}^{d-1}\prec(\beta_j^2)_{j=0}^{d-1}\right\} \tag{21}$$

known to Alice can be remotely prepared by using $\log d+m$ bits from Alice to Bob and their previously shared entangled state, where m is equal to $\log d$ when they initially shared a maximal entangled state, otherwise m is equal to $\log d!$. The symbol $\prec$ has the same meaning as that in Ref. [1].

Proof. We can accomplish our remote state preparation by two steps.

Step 1. Alice and Bob transform their shared entangled state into

$$|\Psi_{AB}\rangle=\sum_{i=0}^{d-1}\beta_i|i\rangle|i\rangle,\quad \beta_i\geqslant 0,\quad \sum_{i=0}^{d-1}\beta_i^2=1 \tag{22}$$

by using m bits from Alice to Bob [1]. For the final entangled state has the same Schmidt basis as the original one, Bob can only perform permutative operation to accomplish the transformation, which indicates Bob need not know the final state [13]. The total number of such operation is $d!$, i.e., $m=\log d!$ will be enough. Especially when the initially shared entangled state in Eq. (1) is a maximal one, $m=\log d$ will be enough [3].

Step 2. According to Theorem 1, Alice and Bob use their new shared entangled state in Eq. (22) to prepare the state

$$|\Phi\rangle=\sum_{j=0}^{d-1}\beta_j e^{i\varphi_j}|j\rangle \tag{23}$$

by using $\log d$ bits from Alice to Bob. Note that Alice does not receive classical message from Bob, Alice can send $\log d+m$ bits together to Bob and Bob performs the corresponding unitary operation to accomplish the remote state preparation. Q.E.D.

In the above we have presented an ensemble of state S that can be remotely prepared by using finite classical bits communication. If we can find finite unitary operations $\{u_i\}_{i=1}^{m}$ such that $|\Phi\rangle\in\cup_{i=1}^{m}(u_iS)$ for any pure state $|\Phi\rangle$, then we can claim that any pure state can be remotely prepared by using finite classical bits communication from Alice to Bob. Fortunately there exist such finite unitary operations satisfying the condition. This result relies on Heine-Borel theorem [14].

Theorem 3. Suppose Alice and Bob have shared an entangled state in Eq. (1). Any pure state of dimension d can be

remotely prepared by using finite classical bits from Alice to Bob and their previously shared entangled state.

Proof. From Heine-Borel theorem [14] we can conclude that the set $A=\{x\in C^d|\|x\|=1\}$ is compact [15]. Because the set $F=\{B(x_0,r)|x_0\in A\}$ is an open cover of A, where $B(x_0,r)=\{x\in C^d|\|x-x_0\|<r\}$, so F admits a finite subcover. This means, for any $r>0$, there exists a finite $n_r\in N$ such that the set $G=\{B(x_i,r)\cap A|x_i\in A,i=1,\ldots,n_r\}$ is a cover of A. That is to say $\cup_{i=1}^{n_r}\{B(x_i,r)\cap A\}=A$. Since unitary operations preserve the norm, any two elements of G can be connected by a unitary operation. There is a bijective map between the set A and the set of all pure state of dimension d which maps the state $\Sigma_{i=0}^{d-1}\alpha_i e^{i\varphi_i}|i\rangle$ to the point $(\alpha_0 e^{i\varphi_0},\ldots,\alpha_{d-1}e^{i\varphi_{d-1}})$. So we can regard the state set S presented in the lemma as a subset of A. We assume that u_0 is the image of the state $|0\rangle$. It can be easily verified that when $0<r<\min(\alpha_0,\ldots,\alpha_{d-1})$, the set $B(u_0,r)\cap A$ is a subset of S. This means that there is a cover G of A which has finite element and each element can be generated by a unitary operation performed on the subset $B(u_0,r)\cap A$ of S. Note that A represent all pure states and S represent the state set we given in the lemma, we can finish our proof. Q.E.D.

IV. DISCUSSION AND SUMMARY

In Sec. II, we have discussed the RSP protocols by using minimum classical bits and we have found many ensembles of states that can be remotely prepared by using minimum classical bits and the previously shared entangled state. Any two such ensembles are connected by a unitary operation. In some special cases, we can find more ensembles of states that can be remotely prepared by using the same resource and the connection between them is not necessarily a unitary operation. For example, when Alice and Bob share the entangled state

$$|\Psi_{AB}\rangle=\alpha|00\rangle+\beta|11\rangle+\alpha|22\rangle+\beta|33\rangle, \tag{24}$$

the ensemble of states

$$\{|\Phi\rangle=\alpha|0\rangle+e^{i\varphi_1}\beta|1\rangle+\alpha e^{i\varphi_2}|2\rangle+\beta e^{i\varphi_3}|3\rangle, \quad \forall\ \varphi_j,\quad j=1,2,3\} \tag{25}$$

and the ensemble of states

$$\{|\Phi\rangle=\alpha|0\rangle+e^{i\varphi}\beta|1\rangle,\quad \forall\ \varphi\} \tag{26}$$

can both be remotely prepared by using two classical bits from Alice to Bob and their previously shared entangled state. But these two ensemble of states can not be connected by a unitary operation. Actually we can get the ensemble of states in Eq. (26) by performing a quantum measurement [16] with measurement operators

$$E_0=|0\rangle\langle 0|+|1\rangle\langle 1|,\quad E_1=|0\rangle\langle 2|+|1\rangle\langle 3| \tag{27}$$

on the ensemble of states

$$\{|\Phi\rangle=\alpha|0\rangle+e^{i\varphi}\beta|1\rangle+e^{i\psi}(\alpha|2\rangle+\beta e^{i\varphi}|3\rangle),\quad \forall\ \varphi,\quad \forall\ \psi,\} \tag{28}$$

In Sec. III, we have proved that any pure quantum state can be remotely prepared by using finite classical bits and the previously shared nonmaximally entangled qubit states.

ACKNOWLEDGMENTS

We thank Z. W. Zhou, Y. C. Wu, Y. J. Han, and Y. Hu for their helpful advice. This work was funded by the National Fundamental Research Program (Program No. 2001CB309300), National Natural Science Foundation of China.

[1] M.A. Nielsen, Phys. Rev. Lett. **83**, 436 (1999).
[2] C.H. Bennett, A.W. Harrow, D.W. Leung, and J.A. Smolin, e-print quant-ph/0205057.
[3] H.K. Lo, Phys. Rev. A **62**, 012313 (2000).
[4] C.H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W.K. Wootters, Phys. Rev. Lett. **70**, 1895 (1993).
[5] 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).
[6] D.W. Berry and B.C. Sanders, Phys. Rev. Lett. **90**, 057901 (2003).
[7] I. Devetak and T. Berger, Phys. Rev. Lett. **87**, 197901 (2001).
[8] A.K. Pati, Phys. Rev. A **63**, 014302 (2000).
[9] D.W. Leung and P.W. Shor, Phys. Rev. Lett. **90**, 127905 (2003).
[10] X.H. Peng, X.W. Zhu, X.M. Fang, M. Feng, M.L. Liu, and K.L. Gao, Phys. Lett. A **306**, 271 (2003).
[11] B. Zeng and P. Zhang, Phys. Rev. A **65**, 022316 (2002).
[12] A. Hayashi, T. Hashimoto, and M. Horibe, Phys. Rev. A **67**, 052302 (2003).
[13] J.G. Jensen and R. Schack, Phys. Rev. A **63**, 062303 (2001).
[14] E. Hewitt and K. Stromberg, *Real and Abstract Analysis* (Springer-Verlag, New York, 1965). Heine-Borel theorem: Let $n\in N$ and let $A\subset R^n$ (or C^n). Then A is compact if and only if A is closed and bound. A topological space X is said to be compact if each open cover of X admits a finite subcover.
[15] Let $x=(x_1,\ldots,x_d)\in C^d$, we define the norm $\|x\|=\sqrt{|x_1|^2+\ldots+|x_d|^2}$.
[16] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, England, 2000).