Remote state preparation without oblivious conditions

A. Hayashi, T. Hashimoto, and M. Horibe
Department of Applied Physics, Fukui University, Fukui 910, Japan
(Received 2 May 2002; published 13 May 2003)

In quantum teleportation, neither Alice nor Bob acquires any classical knowledge on teleported states. The teleportation protocol is said to be oblivious to both parties. In remote state preparation (RSP), it is assumed that Alice is given complete classical knowledge on the state that is to be prepared by Bob. Recently, Leung and Shor [e-print quant-ph/0201008] showed that the same amount of classical information as that in teleportation needs to be transmitted in any exact and deterministic RSP protocol that is oblivious to Bob. Assuming that the dimension of subsystems in the prior-entangled state is the same as the dimension of the input space, we study similar RSP protocols, but not necessarily oblivious to Bob. We show that in this case Bob's quantum operation can be safely assumed to be a unitary transformation. We then derive an equation that is a necessary and sufficient condition for such a protocol to exist. By studying this equation, we show that one-qubit RSP requires two classical bits of communication, which is the same amount as in teleportation, even if the protocol is not assumed oblivious to Bob. For higher dimensions, it is still an open question whether the amount of classical communication can be reduced by abandoning oblivious conditions.

DOI: 10.1103/PhysRevA.67.052302 PACS number(s): 03.67.Hk

I. INTRODUCTION

Interplay between classical information and a quantum state shows nontrivial and remarkable aspects where quantum entanglement is involved. In quantum teleportation [1], one qubit in an unknown quantum state can be transmitted from a sender (Alice) to a receiver (Bob) by a maximally entangled quantum channel and two classical bit (cbit) communication. In order to teleport a quantum state in a d-dimensional space, $\log_2 d$ qubits, Alice needs to transmit $2\log_2 d$ cbits of information to Bob. This is actually the minimum amount of classical communication, which can be shown by combining a teleportation protocol with another striking scheme utilizing quantum entanglement, superdense coding [2].

In teleportation, neither Alice nor Bob acquires any classical knowledge on teleported states. The teleportation protocol is said to be oblivious to Alice and Bob. In remote state preparation (RSP), however, it is assumed that Alice has complete classical knowledge on the state that is to be prepared by Bob [3–6]. The central concern has been whether quantum and classical resources can be reduced by Alice's knowledge on the state. In this respect, Lo has conjectured that RSP for a general state requires at least as much as classical communication as teleportation [3]. An experimental implementation of RSP scheme has also been reported [7].

Recently, Leung and Shor [8] showed that the same amount of classical information as in teleportation needs to be transmitted from Alice to Bob in any deterministic and exact RSP protocol that is oblivious to Bob. Here, the assumption that a protocol is oblivious to Bob means specifically two things: First, the probability that Alice sends a particular classical message to Bob does not depend on the state to be transmitted. Second, no extra information about the transmitted state is contained in Bob's quantum state.

In this paper, we will study exact and deterministic RSP protocols for a general state, in the case that the dimension of subsystems in the prior-entangled state is the same as the dimension of input space, but not necessarily oblivious to Bob. First, we will show that Bob's quantum operation can be assumed to be a unitary transformation. We then derive an equation that is a necessary and sufficient condition for such a protocol to exist. By studying this equation, we show that in order to remotely prepare one qubit in a general state, Alice needs to transmit two cbits of classical information to Bob, which is of the same amount as in teleportation, even if the protocol is not assumed oblivious to Bob. For a general dimensional case, it is still an open question whether the amount of classical communication can be reduced by abandoning oblivious conditions.

II. RSP PROTOCOL WITHOUT OBLIVIOUS CONDITIONS

In this paper, we only consider RSP protocols that are exact and deterministic. The diagram of protocol is depicted in Fig. 1.

We assume that the dimension of subsystems in the prior-entangled state is the same as the dimension of the input space. Following Ref. [8], RSP protocols are formulated in the following way. The prior-entangled state shared by Alice

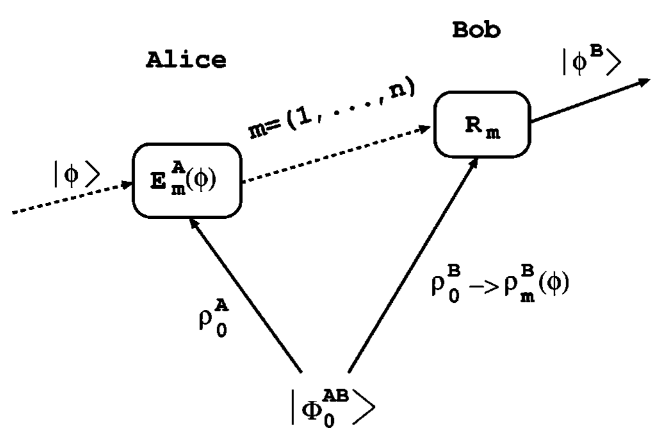

FIG. 1. Remote state preparation diagram.

and Bob is assumed to be a maximally entangled state in space AB, defined by

$$|\Phi_0^{\mathrm{AB}}\rangle = \frac{1}{\sqrt{d}} \sum_{k=1}^{d} |k^{\mathrm{A}}\rangle \otimes |k^{\mathrm{B}}\rangle, \tag{1}$$

where systems A and B are d-dimensional Hilbert spaces, with an orthonormal basis $|k\rangle$ $(k=1,\ldots,d)$. Writing $\rho_0^{\mathrm{AB}} = |\Phi_0^{\mathrm{AB}}\rangle\langle\Phi_0^{\mathrm{AB}}|$, we note that $\rho_0^{\mathrm{A}} \equiv \mathrm{tr}_{\mathrm{B}}\rho_0^{\mathrm{AB}} = \mathbf{1}^{\mathrm{A}}/d$ and $\rho_0^{\mathrm{B}} \equiv \mathrm{tr}_{\mathrm{A}}\rho_0^{\mathrm{AB}} = \mathbf{1}^{\mathrm{B}}/d$. Given a pure state $|\phi\rangle$ randomly chosen from an input state space of d dimension, Alice performs a POVM (positive operator-valued measure) measurement on system A with n possible outcomes:

$$\sum_{m=1}^{n} E_m^{\mathrm{A}}(\phi) = \mathbf{1}^{\mathrm{A}}. \tag{2}$$

Remember that since Alice is assumed to have a complete knowledge of state $|\phi\rangle$, the dependence of POVM elements $E_m^A(\phi)$ on ϕ is not limited. The probability for Alice to obtain outcome m is given by

$$p_m(\phi) = \mathrm{tr}_{\mathrm{A}}\rho_0^{\mathrm{A}} E_m^{\mathrm{A}}(\phi). \tag{3}$$

In this paper, we do not assume that the probability $p_m(\phi)$ is independent of ϕ, implying that the protocol may not be oblivious to Bob. With outcome m, Bob's system B is given by

$$\rho_m^{\mathrm{B}}(\phi) = \frac{\mathrm{tr}_{\mathrm{A}}\rho_0^{\mathrm{AB}} E_m^{\mathrm{A}}(\phi)}{p_m(\phi)}. \tag{4}$$

Receiving a classical message m $(m=1,\ldots,n)$ from Alice, Bob performs a trace-preserving quantum operation $\mathcal{R}_m$ on his subsystem B to restore the state $|\phi\rangle$:

$$\mathcal{R}_m(\rho_m^{\mathrm{B}}(\phi)) = |\phi^{\mathrm{B}}\rangle\langle\phi^{\mathrm{B}}|. \tag{5}$$

III. IT SUFFICES FOR BOB TO PERFORM A UNITARY OPERATION

In this section, we will show that Bob's quantum operation $\mathcal{R}_m$ is actually a unitary operation $\mathcal{R}_m(\rho) = u_m \rho u_m^+$, if the RSP protocol, considered in this paper, works for any state $|\phi\rangle$. First we observe the following theorem.

Theorem. Let $\mathcal{E}$ be a trace-preserving quantum operation with equal input and output space dimensions. If for any state $|\phi\rangle$, there exists a density operator ρ_ϕ such that $\mathcal{E}(\rho_\phi) = |\phi\rangle\langle\phi|$, then the quantum operation $\mathcal{E}$ is a unitary operation $\mathcal{E}(\rho) = u\rho u^+$, where u is a unitary operator.

Before proving the theorem, we note two general properties of the density operator, which will be used in the proof. The first one is that if $\mathrm{tr}(\rho\rho') = 1$, then ρ and ρ' are identical and pure, which can be shown by the Cauchy-Schwarz inequality. Next, let ρ^{QR} be a density operator of a system consisting of subsystems Q and R. Then, the second property used in the proof is that if $\rho^{\mathrm{Q}} \equiv \mathrm{tr}_{\mathrm{R}}\rho^{\mathrm{QR}}$ is pure, then $\rho^{\mathrm{QR}} = \rho^{\mathrm{Q}} \otimes \rho^{\mathrm{R}}$, where $\rho^{\mathrm{R}} = \mathrm{tr}_{\mathrm{Q}}\rho^{\mathrm{QR}}$. This can be seen by observing subadditivity and the triangle inequality of the von Neumann entropy S, by which we find

$$S(\rho^{\mathrm{R}}) = |S(\rho^{\mathrm{R}}) - S(\rho^{\mathrm{Q}})| \leqslant S(\rho^{\mathrm{QR}}), \tag{6}$$

$$S(\rho^{\mathrm{QR}}) \leqslant S(\rho^{\mathrm{R}}) + S(\rho^{\mathrm{Q}}) = S(\rho^{\mathrm{R}}). \tag{7}$$

This means that the equality in subadditivity holds since $S(\rho^{\mathrm{QR}}) = S(\rho^{\mathrm{R}}) + S(\rho^{\mathrm{Q}})$, which is true only if $\rho^{\mathrm{QR}} = \rho^{\mathrm{Q}} \otimes \rho^{\mathrm{R}}$.

Now we will prove the theorem given in the above.

Proof. In the unitary model of a quantum operation, the assumption in the theorem is stated as follows: For any $|\phi\rangle$ there exists a density operator ρ_ϕ such that

$$\mathrm{tr}_{\mathrm{E}} U(\rho_\phi \otimes |0^{\mathrm{E}}\rangle\langle 0^{\mathrm{E}}|) U^+ = |\phi\rangle\langle\phi|, \tag{8}$$

where $|0^{\mathrm{E}}\rangle$ is a standard pure state of the ancillary system E, and U is a unitary operator of the combined system. As we have noted, if a subsystem is pure after tracing out the ancilla system, it is already pure in the combined system and therefore we have

$$U(\rho_\phi \otimes |0^{\mathrm{E}}\rangle\langle 0^{\mathrm{E}}|) U^+ = |\phi\rangle\langle\phi| \otimes \rho_\phi^{\mathrm{E}}. \tag{9}$$

We will show that ρ_ϕ^{E} is actually pure and independent of ϕ. Introducing an orthonormal basis $|k\rangle$ $(k=1,\ldots,d)$, we write

$$U(\rho_k \otimes |0^{\mathrm{E}}\rangle\langle 0^{\mathrm{E}}|) U^+ = |k\rangle\langle k| \otimes \rho_k^{\mathrm{E}}. \tag{10}$$

Multiplying Eq. (10) of index k with the one of index l and taking trace of the product, we find

$$\mathrm{tr}\rho_k\rho_l = |\langle k|l\rangle|^2 \mathrm{tr}_{\mathrm{E}}\rho_k^{\mathrm{E}}\rho_l^{\mathrm{E}} = \delta_{k,l}\mathrm{tr}_{\mathrm{E}}\rho_k^{\mathrm{E}}\rho_k^{\mathrm{E}}, (k,l=1,\ldots,d). \tag{11}$$

This equation implies that the d density operators ρ_k's have orthogonal supports in the d-dimensional space. This is possible only if $\rho_k = |\psi_k\rangle\langle\psi_k|$, where the set $\{|\psi_k\rangle, k=1,\ldots,d\}$ is an orthonormal basis of the space. We also find that ρ_k^{E} is pure, since $\mathrm{tr}\rho_k^{\mathrm{E}}\rho_k^{\mathrm{E}} = 1$.

In the same way as we obtained Eq. (11), we find

$$\mathrm{tr}\rho_\phi\rho_k = |\langle\phi|k\rangle|^2 \mathrm{tr}_{\mathrm{E}}\rho_\phi^{\mathrm{E}}\rho_k^{\mathrm{E}}, (k=1,\ldots,d). \tag{12}$$

Summing this equation over k and using $\Sigma_{k=1}^d \rho_k = \Sigma_{k=1}^d |\psi_k\rangle\langle\psi_k| = \mathbf{1}$, we obtain

$$1 = \sum_{k=1}^{d} |\langle\phi|k\rangle|^2 \mathrm{tr}_{\mathrm{E}}\rho_\phi^{\mathrm{E}}\rho_k^{\mathrm{E}}, \tag{13}$$

which implies that ρ_ϕ^E is pure and given by

$$\rho_\phi^{\mathrm{E}} = \sum_{k=1}^{d} |\langle\phi|k\rangle|^2 \rho_k^{\mathrm{E}}. \tag{14}$$

From this we conclude that ρ_k^{E} is independent of k and furthermore ρ_ϕ^E for a general $|\phi\rangle$ has no state dependence either. Writing $\rho_\phi^{\mathrm{E}} = |0'^{\mathrm{E}}\rangle\langle 0'^{\mathrm{E}}|$, we thus have

$$\rho_\phi \otimes |0^{\mathrm{E}}\rangle\langle 0^{\mathrm{E}}| = U^+(|\phi\rangle\langle\phi| \otimes |0'^{\mathrm{E}}\rangle\langle 0'^{\mathrm{E}}|)U. \tag{15}$$

Sandwiching this between $\langle 0^{\mathrm{E}}|$ and $|0^{\mathrm{E}}\rangle$ gives

$$\rho_\phi = u^+|\phi\rangle\langle\phi|u, \tag{16}$$

where $u=\langle 0'^{E}|U|0^{E}\rangle$ and $u^{+}=\langle 0^{E}|U^{+}|0'^{E}\rangle$. It is clear that the operator u must be a unitary operator since $u^{+}|\phi\rangle\langle\phi|u$ is a density operator for any state $|\phi\rangle$. Since Eq. (16) holds for any $|\phi\rangle$, we conclude that the quantum operation $\mathcal{R}$ is a unitary operation:

$$\mathcal{E}(\rho)=u\rho u^{+}. \tag{17}$$

□

Now remember that Bob receives a classical message $m \in \{1,2,\ldots,n\}$ from Alice and performs a quantum operation $\mathcal{R}_m$ on the state $\rho_m^{B}(\phi)$ to restore state $|\phi\rangle$ that Alice wants him to prepare:

$$\mathcal{R}_m(\rho_m^{B}(\phi))=|\phi^{B}\rangle\langle\phi^{B}|. \tag{18}$$

Since this should hold for any state $|\phi\rangle$, by the theorem we have just proved, $\mathcal{R}_m$ turns out to be a unitary operation,

$$\mathcal{R}_m(\rho)=u_m\rho u_m^{+}, \tag{19}$$

where u_m is unitary. We also note that we did not assume that ρ^{E}, the state of ancilla system E after Bob's quantum operation, is independent of $|\phi\rangle$ (oblivious condition); but it was shown that ρ^{E} should be independent of $|\phi\rangle$ in the proof of the theorem.

IV. NECESSARY AND SUFFICIENT CONDITION FOR RSP

Now that we have shown that Bob's quantum operation is a unitary operation, we can derive an equation that is a necessary and sufficient condition for RSP protocols considered in this paper.

From Eqs. (3) and (4), we obtain

$$\sum_{m=1}^{n} p_m(\phi)\rho_m^{B}(\phi)=\rho_0^{B}=\frac{\mathbf{1}^{B}}{d}, \tag{20}$$

which means that the density operator of system B should not change by Alice's POVM measurement on system A as long as an outcome of the measurement is unspecified. Using the result from the preceding section, $\rho_m^{B}(\phi)=u_m^{+}|\phi^{B}\rangle\langle\phi^{B}|u_m$, we get

$$\sum_{m=1}^{n} p_m(\phi)u_m^{+}|\phi^{B}\rangle\langle\phi^{B}|u_m=\frac{\mathbf{1}^{B}}{d}. \tag{21}$$

Here, u_m's are unitary and $p_m(\phi)$ is the probability of an outcome m of Alice's POVM measurement; therefore $p_m(\phi)\geqslant 0$ and $\sum_{m=1}^{n}p_m(\phi)=1$. We also note that this should hold for any state $|\phi\rangle$. A similar equation has been discussed for a continuous variable teleportation in Ref. [9] and implicitly stated for oblivious RSP in Ref. [8].

It is important that Eq. (21) is also a sufficient condition for RSP protocols. Let us assume that Eq. (21) holds in space B for some unitary operators u_m's and for some probability distribution $p_m(\phi)$, then the same equation also holds in space A:

$$\sum_{m=1}^{n} p_m(\phi)|\phi_m^{A}\rangle\langle\phi_m^{A}|=\frac{\mathbf{1}^{A}}{d}, \tag{22}$$

since the dimension is the same for spaces A and B, where we wrote $|\phi_m\rangle=u_m^{+}|\phi\rangle$ for convenience. Here for a state $|\phi\rangle=\sum_{k=1}^{d}|k\rangle\langle k|\phi\rangle$, we introduce state $|\overline{\phi}\rangle$ defined as $|\overline{\phi}\rangle=\sum_{k=1}^{d}|k\rangle\langle\phi|k\rangle$. Then it is clear that the following relation also holds:

$$\sum_{m=1}^{n} p_m(\phi)|\overline{\phi}_m^{A}\rangle\langle\overline{\phi}_m^{A}|=\frac{\mathbf{1}^{A}}{d}. \tag{23}$$

From this relation, we can construct POVM elements as

$$E_m^{A}(\phi)=dp_m(\phi)|\overline{\phi}_m^{A}\rangle\langle\overline{\phi}_m^{A}| \quad (m=1,\ldots,n). \tag{24}$$

Evidently, each $E_m^{A}(\phi)$ is a positive operator and $\sum_{m=1}^{n}E_m^{A}(\phi)=\mathbf{1}^{A}$. Since Alice is assumed to be given complete classical knowledge on state $|\phi\rangle$, she can, in principle, implement this POVM measurement. The probability of an outcome m is calculated as $\mathrm{tr}_A\rho_0^{A}E_m^{A}(\phi)=(1/d)\mathrm{tr}_A E_m^{A}(\phi)=p_m(\phi)$, and with an outcome being given by m, the resultant state of B is given by

$$\begin{aligned}\rho_m^{B}(\phi)&=d\,\mathrm{tr}_A|\Phi_0^{AB}\rangle\langle\Phi_0^{AB}||\overline{\phi}_m^{A}\rangle\langle\overline{\phi}_m^{A}|\\&=d\langle\overline{\phi}_m^{A}|\Phi_0^{AB}\rangle\langle\Phi_0^{AB}|\overline{\phi}_m^{A}\rangle=|\phi_m^{B}\rangle\langle\phi_m^{B}|\\&=u_m^{+}|\phi^{B}\rangle\langle\phi^{B}|u_m.\end{aligned} \tag{25}$$

Receiving a classical message m from Alice, Bob can restore state $|\phi\rangle$ by a single unitary operation since $u_m\rho_m^{B}(\phi)u_m^{+}=|\phi^{B}\rangle\langle\phi^{B}|$.

Thus, Eq. (21) is a necessary and sufficient condition for the class of RSP protocols considered in this paper and will be called RSP equation hereafter.

V. RSP EQUATION

We will study the RSP equation (21), which is a necessary and sufficient condition for the class of RSP protocols considered in this paper:

$$\sum_{m=1}^{n} p_m(\phi)u_m^{+}|\phi\rangle\langle\phi|u_m=\frac{\mathbf{1}}{d}. \tag{26}$$

Here, superscripts A or B are omitted, since the equation should hold in either of the d-dimensional space.

Note that the theorem in Sec. III implies that Bob's state does not carry extra information on the transmitted state. In the case where the probabilities $p_m(\phi)$ are independent of the transmitted state $|\phi\rangle$, we obtain the oblivious condition in Ref. [8] and therefore all the results in Ref. [8] (see also Ref. [10]). In particular, $2\log_2 d$ cbits are necessary, and that a teleportationlike protocol that is oblivious to Alice can be obtained without increasing the classical communication cost.

That remains to study is the case where the probability $p_m(\phi)$ may depend on the state $|\phi\rangle$ that is to be remotely prepared. The question is whether this dependence can reduce the minimum amount of classical communication. In the case of one-qubit RSP $(d=2)$, we will show that this is not the case: the minimum amount of classical information turns out to be $2=2\log_2 d$ cbits as in teleportation.

Unfortunately, for general dimension d, however, we have only limited results: The RSP equation (26) immediately tells us that $n \geqslant d$, which is known as Holevo's bound [11], since the equation requires that $\{u_m^{+}|\phi\rangle\ (m=1,\ldots,n)\}$ is complete in the d-dimensional space. We can also show that $n \geqslant d+1$. Assume that the RSP equation (26) holds for $n=d$. Generally, in a d-dimensional space, the relation $\Sigma_{m=1}^{d}|\chi_m\rangle\langle\chi_m|=\mathbf{1}$ is satisfied if and only if the states $|\chi_m\rangle$ are orthonormal. Therefore, when $m\neq m'$, the inner product $\langle\phi|u_m u_{m'}^{+}|\phi\rangle$ should vanish for any $|\phi\rangle$, implying $u_m u_{m'}^{+}=0$. This, however, contradicts unitarity of u_m's.

Now we return to the qubit case $(d=2)$. The Bloch sphere representation is convenient for a pure qubit state $|\phi\rangle\langle\phi|$,

$$|\phi\rangle\langle\phi|=\frac{\mathbf{1}+\boldsymbol{\chi}\cdot\boldsymbol{\sigma}}{2}, \tag{27}$$

where $\boldsymbol{\chi}$ is a three-dimensional unit vector, and σ_x, σ_y, and σ_z are the Pauli matrices. We also introduce a 3×3 rotation matrix R_m for each unitary operator u_m through

$$u_m^{+}\sigma_i u_m=\sum_{j=1}^{3}(R_m)_{ji}\sigma_j. \tag{28}$$

The RSP equation is then reduced to

$$\sum_{m=1}^{n} p_m(\boldsymbol{\chi})R_m\boldsymbol{\chi}=\mathbf{0}, \tag{29}$$

which should hold for any unit vector $\boldsymbol{\chi}$ and we emphasize again that the probability p_m may depend on $\boldsymbol{\chi}$.

It can be readily seen that if Eq. (29) holds for a set of rotation matrices R_m and some probability $p_m(\boldsymbol{\chi})$, it is also satisfied by a set of transformed rotations SR_mT, with S and T being any rotation matrices, and probability $p_m(T\boldsymbol{\chi})$. With this freedom, we can safely assume that R_1 is a unit matrix, R_2 is a rotation about the x axis, and R_3 is a rotation about an axis in the xy plane.

Now assume that Eq. (29) holds for $n=3$ and take $\boldsymbol{\chi}=\boldsymbol{e}_x$ (the unit vector along the x axis), then we find

$$[p_1(\boldsymbol{e}_x)+p_2(\boldsymbol{e}_x)]\boldsymbol{e}_x+p_3(\boldsymbol{e}_x)R_3\boldsymbol{e}_x=\mathbf{0}. \tag{30}$$

Since $p_m(\boldsymbol{e}_x)$ is a probability distribution, this equation is satisfied only when $R_3\boldsymbol{e}_x=-\boldsymbol{e}_x$, namely, R_3 is a rotation of 180° about the y axis. By a similar argument with $\boldsymbol{\chi}=\boldsymbol{e}_y$ (the unit vector along the y axis), R_2 turns out to be a rotation of 180° about the x axis. Therefore, for a general unit vector $\boldsymbol{\chi}=(\chi_x,\chi_y,\chi_z)$, Eq. (29) with $n=3$ takes the following matrix form:

$$\begin{pmatrix}\chi_x & \chi_x & -\chi_x\\ \chi_y & -\chi_y & \chi_y\\ \chi_z & -\chi_z & -\chi_z\end{pmatrix}\begin{pmatrix}p_1(\boldsymbol{\chi})\\ p_2(\boldsymbol{\chi})\\ p_3(\boldsymbol{\chi})\end{pmatrix}=\begin{pmatrix}0\\0\\0\end{pmatrix}. \tag{31}$$

This equation has only a trivial solution $p_m(\boldsymbol{\chi})=0$ for $\boldsymbol{\chi}$ with $\chi_x\chi_y\chi_z\neq 0$, since the determinant of the matrix in the equation is $4\chi_x\chi_y\chi_z$. Thus, we conclude that in order to remotely prepare a general qubit state $(d=2)$, Alice needs to transmit $2=\log_2 2^2$ cbits of information to Bob.

VI. SUMMARY AND DISCUSSION

In this paper, we studied exact and deterministic RSP schemes for a general state. Though the schemes were not assumed to be oblivious to Bob, we restricted ourselves to the case where the dimension of subsystems in the prior-entangled state is the same as the dimension of the input space. In this case Bob's quantum operation was shown to be just a unitary operation, if the protocol works for a general state.

Using this fact we have derived the RSP equation, which is a necessary and sufficient condition for an RSP protocol to exist in the class considered in this paper. By studying this equation, it was shown that in order to remotely prepare one qubit in a general state, Alice needs to transmit two cbits of information to Bob, which is the same amount as in teleportation, even if the protocol is not assumed oblivious to Bob. So, for one-qubit RSP, Lo's conjecture [3] has been proved without oblivious conditions. Leung and Shor investigated oblivious RSP without assuming that the two dimensions are the same [8]. Study on nonoblivious RSP in this general case is now in progress.

Unfortunately, generalization to higher dimensions is not straightforward. Though it is not yet clear as whether the amount of classical communication can be reduced by abandoning oblivious conditions in higher dimensions. We believe that the RSP equation will be a key to obtain some insights for further study in this direction.

In this paper, the input ensemble, from which state $|\phi\rangle$ is randomly chosen, is assumed to be the entire Hilbert space of d dimensions. We remark that if the state is chosen from a subensemble of the space, the RSP equation should still hold in the subensemble, as long as Bob's action can be assumed to be a unitary operation. In the case of qubits on the equatorial circle of the Bloch sphere [4,5], the RSP equation (29) with $n=2$ is satisfied as

$$\tfrac{1}{2}(R_1\boldsymbol{\chi}+R_2\boldsymbol{\chi})=\mathbf{0}, \tag{32}$$

where $\boldsymbol{\chi}$ is a unit vector on the equator, R_1 is a unit matrix, and R_2 is a rotation of 180° about the z axis. Generalizations of the equator and the polar great circle to higher dimensions have been discussed by Zeng and Zhang [6]. We can also verify that corresponding RSP equations with $n=d$ are satisfied for those ensembles.

[1] C.H. Bennett, G. Brassard, C. Crepeau, R. Jozsa, A. Peres, and W. Wootters, Phys. Rev. Lett. **70**, 1895 (1993).
[2] C.H. Bennett and S.J. Wiesner, Phys. Rev. Lett. **69**, 2881 (1992).
[3] H.K. Lo, Phys. Rev. A **62**, 012313 (2000).
[4] A.K. Pati, Phys. Rev. A **63**, 014302 (2000).
[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 (2000).
[6] Bei Zeng and Peng Zhang, Phys. Rev. A **65**, 022316 (2002).
[7] Xinhua Peng, Xiwen Zhu, Ximing Fang, Mang Feng, Maili Liu, and Kelin Gao, e-print quant-ph/0202004.
[8] D.W. Leung and P.H. Shor, e-print quant-ph/0201008.
[9] H. Rubin, Phys. Rev. A **61**, 022311 (2000).
[10] M. Mosca, A. Tapp, and R. de Wolf, e-print quant-ph/0003101.
[11] A.S. Holevo, Probl. Inf. Transm. **9**, 117 (1973).