Remote state preparation with unit success probability

Ba An Nguyen\textsuperscript{1,3}, Thi Bich Cao\textsuperscript{1}, Van Don Nung\textsuperscript{2} and Jaewan Kim\textsuperscript{3}

\textsuperscript{1} Center for Theoretical Physics, Institute of Physics, 10 Dao Tan, Thu Le, Ba Dinh, Hanoi, Vietnam
\textsuperscript{2} Department of Physics, Hanoi National University, 334 Nguyen Trai, Thanh Xuan, Hanoi, Vietnam
\textsuperscript{3} School of Computational Sciences, Korea Institute for Advanced Study, 207-43 Cheongryangni 2-dong, Dongdaemun-gu, Seoul 130-722, Korea

E-mail: nban@iop.vast.ac.vn

Received 27 May 2011
Accepted for publication 14 June 2011
Published 8 July 2011
Online at stacks.iop.org/ANSN/2/035009

Abstract
Remote state preparation is a secure and faithful method for transmitting known quantum states by means of local operation and classical communication. Existing protocols in the general case succeed just with probabilities of less than 100\%. In this paper, we design a protocol to remotely prepare the most general single-qubit state that always succeeds. To achieve unit success probability, the preparer is allowed to use additional local resources and implement adaptive measurements. Our protocol is meaningful because the most expensive resource, i.e. the quantum channel previously shared between the preparer and the receiver, remains the same as in the original protocol (Pati 2000 Phys. Rev. A \textbf{63} 014302), which, however, succeeds only half the time.

Keywords: remote state preparation, adaptive measurements, unit probability

Classification numbers: 1.00, 3.01

1. Introduction
Quantum information science (QIS) emerged recently as a fascinating engagement between quantum physics and information theory. It is among the top-ten topics over all the branches of science. The revolutionary feature of QIS is that information is stored, transmitted and processed in a quantum way. And, a vital ingredient in a quantum protocol to be superior to a classical one is purely quantum, the so-called quantum entanglement. In other words, by sharing a sufficient amount of quantum entanglement, remote parties are able to execute various interesting tasks only by local operation and classical communication (LOCC). One such task is remote state preparation (RSP) \cite{1-3} in which a party, Alice, needs securely and faithfully to prepare a quantum state $|\Psi\rangle$, known to her, for a remote party, Bob, who has absolutely no knowledge about $|\Psi\rangle$. The first original protocol for RSP of a single-qubit state was proposed explicitly in \cite{2}. Since then it has been extended to various more involved scenarios, such as RSP of multiquubit states \cite{4}, an ensemble of states \cite{5} and states in higher dimensions \cite{6}. Experiments on RSP have also been reported in \cite{7}. In general, all of the existing RSP protocols succeed only with probabilities of less than 100\%, i.e. they are probabilistic.

In this paper, we are concerned with the question ‘can one make a general RSP successful with unit probability?’ For that purpose, we reconsider the original probabilistic protocol in \cite{2} and try to make it deterministic. To achieve this goal, some additional resource/operation will be needed. However, as we shall show, such additional ingredients are just local ones (e.g. ancillary qubits, local operations) or of a classical nature (e.g., the conventional media), which are commonly regarded as low cost. The greatest cost is due to the shared quantum resource, which in our protocol is the same as in the probabilistic one \cite{2}. Therefore, the net benefit is the possibility of achieving unit success probability at the expense of cheap additional ingredients. In section 2, we represent the original protocol of \cite{2} for RSP of the most general single-qubit state to see that it is just probabilistic. Then, in section 3, we design our deterministic protocol. Finally, we draw our conclusion in section 4.
2. Probabilistic protocol

Let the most general single-qubit state that Alice needs, only by means of LOCC, to prepare for a remote Bob be

$$|\psi\rangle = \alpha |0\rangle + \beta |1\rangle,$$  \hspace{1cm} (1)

with \(|\{0\}, |1\}\rangle\) the two orthonormal states of a qubit in the computational basis and \(\alpha, \beta \in \mathbb{C}\) satisfying the normalization condition \(|\alpha|^2 + |\beta|^2 = 1\). Since the quantum measurement postulate does not allow for distinguishing quantum states that differ only by a global phase factor, we can, without any loss of generality, set \(\alpha = a\) and \(\beta = b e^{i\varphi}\) with \(a, b \in \mathbb{R}\) and \(a^2 + b^2 = 1\). Then the state (1) is rewritten as

$$|\psi\rangle = a |0\rangle + b e^{i\varphi} |1\rangle.$$  \hspace{1cm} (2)

Suppose that Alice knows all of the parameters \(a, b\) and \(\varphi\) precisely, but Bob knows nothing. According to the protocol in [2], Alice and Bob should share a pair of maximally entangled qubits of, say, the form

$$|q\rangle_{AB} = \frac{1}{\sqrt{2}} \left( |00\rangle + |11\rangle \right)_{AB},$$  \hspace{1cm} (3)

of which Alice possesses qubit A and Bob qubit B. Since Alice knows \(a, b\) and \(\varphi\), she is fully able to measure her qubit in any basis determined by those parameters. Let such a basis be

$$\begin{pmatrix} |\mu_0\rangle_A \\ |\mu_1\rangle_A \end{pmatrix} = M \begin{pmatrix} |0\rangle_A \\ |1\rangle_A \end{pmatrix},$$  \hspace{1cm} (4)

with

$$M = \begin{pmatrix} a & b e^{i\varphi} \\ b e^{-i\varphi} & -a \end{pmatrix}. \hspace{1cm} (5)$$

It is clear that the transformation \(M\) is unitary and \(|\mu_0\rangle_A, |\mu_1\rangle_A\) forms a complete orthonormal set of states of a qubit in Hilbert space of dimension 2. When Alice measures the qubit A in the basis \(|\mu_0\rangle_A, |\mu_1\rangle_A\), the outcome \(|\mu_0\rangle_A\) or \(|\mu_1\rangle_A\) occurs at random, but each of them has a probability of 1/2. If it is \(|\mu_0\rangle_A\), Bob’s qubit B collapses into

$$|\chi_0\rangle_B = (a |0\rangle + b e^{-i\varphi} |1\rangle)_B; \hspace{1cm} (6)$$

from which Bob cannot reconstruct \(|\psi\rangle\), equation (2), because of his lack of knowledge of the necessary parameters, implying a failure. However, if Alice obtains \(|\mu_1\rangle_A\), the collapsed state of the qubit B is

$$|\chi_1\rangle_B = (b e^{i\varphi} |0\rangle - a |1\rangle)_B; \hspace{1cm} (7)$$

from which Bob can reconstruct \(|\psi\rangle\), by applying on \(|\chi_1\rangle_B\) the operator \(\sigma_x, \sigma_y, \sigma_z\) \((\sigma_x = \{0, 1\}, \{1, 0\}\rangle\) is the Pauli bit-flip operator and \(\sigma_y = \{1, 0\}, \{0, -1\}\rangle\) the Pauli phase-flip one). Knowledge of the parameters \(a, b, \varphi\) does not matter at all. For Bob to perform the right action, Alice is required to announce her outcome, say, via a public classical communication channel. Since there are two possible outcomes, \(|\mu_0\rangle_A\) or \(|\mu_1\rangle_A\), the classical communication cost (CCC) is just 1 bit. As for the success probability, it is \(P = 50\%\). That is to say, this protocol is probabilistic.

3. Deterministic protocol

In this section, we aim to design a deterministic protocol based on the same shared quantum channel as in [2]. For the protocol to always succeed, an additional local quantum resource/operation and CCC must be consumed. Given the same shared quantum channel \(|q\rangle_{AB}\), equation (3), as a starting point like in [2], our protocol works as follows.

Firstly, Alice takes an ancillary qubit A’ in state \(|0\rangle_{A’}\).

Secondly, she performs a controlled-NOT gate (CNOT) on the qubits A and A’, with A the control qubit and A’ the target one (i.e. CNOT\(_{A\rightarrow A’}\)|i\rangle_{A’A} = |i\rangle_{A}(i \oplus j)_{A’}\), with \(i, j \in 0, 1\) and (an additional mod 2). As a result, the channel \(|q\rangle_{AB}\) and the state \(|0\rangle_{A}\) become an entangled state \(|Q\rangle_{AA’B} = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{AA’B}\). It is worth emphasizing that the state \(|Q\rangle_{AA’B}\) need not be shared beforehand at all; it is made locally by Alice from the quantum channel state \(|q\rangle_{AB}\).

Thirdly, Alice measures the qubits A and A’ in different bases. For the qubit A, the measurement basis is defined as

$$\begin{pmatrix} |\mu_0\rangle_A \\ |\mu_1\rangle_A \end{pmatrix} = U \begin{pmatrix} |0\rangle_A \\ |1\rangle_A \end{pmatrix},$$  \hspace{1cm} (8)

with

$$U = \begin{pmatrix} a & b \\ b & -a \end{pmatrix}.$$  \hspace{1cm} (9)

while for the qubit A’ the basis is

$$\begin{pmatrix} |\upsilon_0\rangle_{A’} \\ |\upsilon_1\rangle_{A’} \end{pmatrix} = V \begin{pmatrix} |0\rangle_{A’} \\ |1\rangle_{A’} \end{pmatrix},$$  \hspace{1cm} (10)

with

$$V = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & e^{i\varphi} \\ e^{-i\varphi} & -1 \end{pmatrix}. \hspace{1cm} (11)$$

Note that Alice is in full manipulation of the bases (8) and (10) since she knows their determining parameters \((a, b)\) and \(\varphi\). A wise strategy Alice adopts is to measure the qubits A and A’ in sequence. In other words, she postpones measuring the qubit A’ until after she obtains the outcome of measuring the qubit A. When measuring the qubit A in the basis \(|\mu_0\rangle_A, |\upsilon_1\rangle_{A’}\), if \(|\mu_0\rangle_A\) is found, the unmeasured qubits A’ and B collapse into the (unnormalized) state,

$$|\phi’_{AB}\rangle = \frac{1}{\sqrt{2}} (a |00\rangle + b |11\rangle)_{AB}. \hspace{1cm} (12)$$

In this case, Alice does not measure the qubit A’ immediately but applies to it a unitary phase-shift operator,

$$\Pi = \begin{pmatrix} 1 & 0 \\ 0 & e^{2i\varphi} \end{pmatrix},$$  \hspace{1cm} (13)

thus transforming \(|\phi’_{AB}\rangle\) to

$$|\phi_{AB}\rangle = \frac{1}{\sqrt{2}} \left( a |00\rangle + b e^{2i\varphi} |11\rangle \right)_{AB}.$$  \hspace{1cm} (14)

Only after that operation does Alice measure the qubit A’ in the basis \(|\upsilon_0\rangle_{A’}, |\upsilon_1\rangle_{A’}\). Expressed in terms of \(|\upsilon_0\rangle_{A’}, |\upsilon_1\rangle_{A’}\), the state (14) reads

$$|\phi_{AB}\rangle = \frac{1}{\sqrt{2}} \left[ |\upsilon_0\rangle_{A’} (a |0\rangle + b e^{i\varphi} |1\rangle)_{B} + e^{i\varphi} |\upsilon_1\rangle_{A’} (a |0\rangle - b e^{i\varphi} |1\rangle)_{B} \right]. \hspace{1cm} (15)$$
With an equal probability, Alice may find $|u_1⟩_A$ when measuring the qubit A. This event projects the qubits A' and B onto the (unnormalized) state

$$|ϕ_i⟩_{AB} = \frac{1}{\sqrt{2}} (|b⟩_0 - a|1⟩)_{AB}. \quad (16)$$

In this case, Alice immediately proceeds to measuring the qubit A’ in the basis $\{|u_0⟩_{A'}, |u_1⟩_{A'}\}$, in terms of which the state (16) reads

$$|ϕ_i⟩_{AB} = \frac{1}{\sqrt{2}} \left[ e^{-iθ}|υ⟩_{A}⟨b|e^iθ|0⟩ - a|1⟩\right]_{B} + |u_1⟩_{A'} (b|e^iθ|0⟩ + a|1⟩). \quad (17)$$

Fourthly, Alice broadcasts 2 bits for identifying her four possible measurement outcomes in the following way: ‘00’, ‘01’, ‘10’ or ‘11’, if she found $|u_0⟩_{A}|υ⟩_{A}$. $|u_0⟩_{A}|υ⟩_{A}$, $|u_0⟩_{A'}|υ⟩_{A}$, or $|u_1⟩_{A'}|υ⟩_{A}$, respectively. If Alice’s announcement is ‘00’, Bob’s qubit B is left exactly in the desired state, equation (2). If it is ‘01’, Bob’s qubit B is, up to a global phase factor, in the state $(a|0⟩ - b|e^iθ|1⟩)B$, which he can easily transform to the desired one by applying a phase-flip operator $σ_z$. If ‘10’ is broadcast, Bob is sure that his qubit is, up to a global phase factor, in the state $(b|e^iθ|0⟩ - a|1⟩)B$, which requires application of both phase- and bit-flip operators $σ_zσ_x$. Finally, the outcome corresponding to ‘11’ projects Bob's qubit onto the state $(b|e^iθ|0⟩ + a|1⟩)B$, which is nothing else but the desired one, up to a bit-flip operator $σ_x$. As seen from equations (15) and (17), each of Alice’s outcome happens randomly but with an equal probability of $1/4$. Since Bob is always able to recover the desired state (2), the total success probability is $P = (1/4) \times 4 = 100\%$, rendering our protocol a deterministic one.

In other words, here the strategy of adaptive or feedforward measurements applies. ‘Adaptive’ or ‘feedforward’ means sequential measurements that should be performed one by one in such a way that the outcome of a given measurement decides the basis of the next measurement. If measurements of the qubit A in the basis $\{|υ⟩_{A}, |u⟩_{A}\}$ (see equation (8)) and of the qubit A’ in the basis $\{|υ⟩_{A'}, |u⟩_{A'}\}$ (see equation (10)) are carried out independently, then we can write

$$|Φ⟩_{AA'B} = \frac{1}{2} \left( |u⟩_{A'}|υ⟩_{A'} (a|0⟩ + b|e^iθ|1⟩)B + |u⟩_{A'}|υ⟩_{A'} (a|0⟩ + b|e^iθ|1⟩)B + |u⟩_{A'}|υ⟩_{A'} (b|0⟩ - a|e^iθ|1⟩)B + |u⟩_{A'}|υ⟩_{A'} (b|0⟩ - a|e^iθ|1⟩)B \right), \quad (18)$$

which implies success with a probability $P = 50\%$ when Alice’s measurement yields $|u⟩_{A'}$. However, with the strategy of adaptive measurements, the first measurement is to be done on the qubit A in the basis $\{|u⟩_{A}, |υ⟩_{A}\}$, whose outcome is specified by $m = 0$ (1) if $|u⟩_{A}$ ($|υ⟩_{A}$) is found. Then, the basis $\{|υ⟩_{0}⟩_{A}, |υ⟩_{1}⟩_{A}\}$ for the second measurement to be done on the qubit A’ depends on the outcome m in the following manner:

$$\begin{pmatrix} |υ⟩_{0}⟩_{A} \\ |υ⟩_{1}⟩_{A} \end{pmatrix} = W^{(m)} \begin{pmatrix} |0⟩_{A} \\ |1⟩_{A} \end{pmatrix}, \quad (19)$$

where $W^{(m)} = Π^{1-m}V(Π^m)^{1-m}$, with $V$ and $Π$ given by equations (11) and (13). If the outcome of the first measurement is $|υ⟩_{A}$ with $m = 0$ or 1, and that of the second corresponding measurement is $|υ⟩_{m}⟩_{A}$, with $n = 0$ or 1, then the eventually collapsed state of the three qubits A, A' and B is $|υ⟩_{A}|υ⟩_{m}⟩_{A} (σ_z^{m}σ_x^{m}|ψ⟩_{B})$, from which it follows that the outcome-dependent recovery operator is $R = σ_z^{m}σ_x^{m}$, for any $m, n \in [0, 1]$, implying $P = 100\%$.

4. Conclusion

We have designed a protocol for RSP of the most general single-qubit state employing the same shared quantum channel, i.e. one maximally entangled state of two qubits, as in [2]. However, we let the preparer use one ancillary qubit and be capable of locally performing a CNOT on that qubit and the qubit belonging to the shared entangled state as well as measuring the ancillary qubit. These boost the success probability of our protocol to $P = 100\%$, as compared with $P = 50\%$ of that proposed in [2]. Our CCC is, however, 2 bits. The salient merit of our protocol is the achievement of unit success probability via the same nonlocal quantum resource previously shared between the preparer and the receiver. This matters significantly because the added ingredients are all local or of classical nature whose cost is much cheaper than the cost of the shared nonlocal entanglement and the value of success probability is of paramount importance to assess a quantum protocol. We conjecture that success probabilities of RSP in other more complicated situations could also be boosted considerably provided that additional local resources/operations are employed judiciously.

Before ending, a remark is in order. Of course, state (2) can be transmitted by means of teleportation [8] via the same previously shared quantum channel (3), with $P = 100\%$ and CCC = 2 bits, too. In other words, Alice first applies the operator $M$ defined in equation (5) on the state $|0⟩_{A'}$ to have $|ψ⟩_{A'}$. Then, she executes the standard teleportation protocol proposed for the first time in [8], which requires one CNOT$_{AA'}$, one Hadamard gate $H_A$ and two single-qubit measurements, $M_A$ and $M_{A'}$ on the qubits A and A’ in their computational bases. In total, the operations needed for teleportation are one CNOT$_{AA'}$, two unitary transformations ($M_A$ and $H_A$) plus two measurements $M_A$ and $M_{A'}$. As measuring an arbitrary single-qubit state $|Φ⟩$ in a basis $X(|0⟩, |1⟩)$ with any 2 x 2 unitary operator is tantamount to measuring the state $X^∗|Φ⟩$ in the computational basis $|0⟩, |1⟩$, the operations required for our deterministic RSP protocol, in comparison with those in teleportation, are one CNOT$_{AA'}$, two unitary transformations (U^*_A defined in equation (9) and W^{(m)} defined in equation (19)), and also plus two measurements in the computational bases ($M_A$ and $M_{A'}$). Therefore, our protocol is at least an alternative to teleportation from the operational point of view, but it proves to be interesting from the RSP conceptual point of view when the complete data set ($a, b, ψ$) of the state to be transmitted is known.

References

[1] Lo H K 2000 Phys. Rev. A 62 012313
[2] Pati A K 2000 Phys. Rev. A 63 014302
[3] Bennett C H, DiVincenzo D P, Shor P W, Smolin J A, Terhal B M and Wootters W K 2001 Phys. Rev. Lett. 87 077902
[4] Liu J M and Wang Y Z 2003 Phys. Lett. A 316 159
   Dai H Y, Chen P X, Liang L M and Li C Z 2006 Phys. Lett. A 355 285
   Xia Y, Song J and Song H S 2007 Opt. Commun. 277 219
   Wang D, Liu Y M and Zhang Z J 2008 Opt. Commun. 281 871
   Liu J M, Feng X L and Oh C H 2009 J. Phys. B: At. Mol. Opt. Phys. 42 055508
   Ma P C and Zhan Y B 2010 Opt. Commun. 283 2640
   Zha X W and Song H Y 2010 Opt. Commun. 284 1472
   Han L F and Yuan H 2011 Int. J. Quantum. Inf. 9 539
[5] Ye M Y, Zhang Y S and Guo G C 2004 Phys. Rev. A 69 022310
[6] Zeng B and Zhang P 2002 Phys. Rev. A 65 022316
   Yu C S, Song H S and Wang Y H 2006 Phys. Rev. A 73 022340
[7] Peng X, Zhu X, Fang X, Feng M, Liu M and Gao K 2003 Phys. Lett. A 306 271
   Peters N A, Barreiro J T, Goggin M E, Wei T C and Kwiat P G 2005 Phys. Rev. Lett. 94 150502
   Rosenfeld W, Berner S, Volz J, Weber M and Weinfurter H 2007 Phys. Rev. Lett. 98 050504
[8] Bennett C H, Brassard G, Crepeau C, Jozsa R, Peres A and Wootters W K 1993 Phys. Rev. Lett. 70 1895