NEW DETERMINISTIC PROTOCOL FOR JOINT REMOTE PREPARATION OF TWO-QUBIT STATES

NUNG VAN DON, CAO THI BICH, NGUYEN BA AN
Center for Theoretical Physics, Institute of Physics, VAST

Abstract. Designing quantum protocols with unit success probability is highly desirable from a viewpoint of the overall resource cost. In this work, we propose a new deterministic protocol for joint remote preparation of the most general two-qubit state using the same quantum/classical resource as in [An et al., Phys. Lett. A 375 (2011) 3570] and, at the same time, retaining the passive role of the receiver as in [Xiao et al., J. Phys. B: At. Mol. Opt. Phys. 44 (2011) 075501], which employs a different kind of nonlocal resource. From a practical point of view, this protocol proves most suitable in situations when only Einstein-Podolsky-Rosen pairs are supplied and the receiver is not capable of performing any measurements nor controlled-NOT gates.

I. INTRODUCTION

Absolutely different from classical communication, in quantum communication information is encoded in qubits [1] which may be in terms of superposed multiqubit states. Security of communication is provided by fundamental laws of nature according to which the qubits cannot be cloned [2] nor learned without traces left behind. Yet, sending informative qubits themselves through space is not a good idea, since the arrived information may be unfaithful due to tampering en route of unauthorized parties. In 1993 a milestone quantum protocol [3] was designed enabling one to teleport an unknown qubit securely and faithfully by means of local operation and classical communication (LOCC). This appears possible thanks to a special kind of resource named entanglement [4] which must a priori be shared between the communicating parties. In case the state is known, its transmission can be done simpler by what is called remote state preparation (RSP) [5], using the same shared amount of entanglement as in teleportation. In RSP, however, the complete information encoded in the quantum state is disclosed to the transmitter (or the preparer, to suit the terminology RSP). To circumvent such leakage of full information joint remote state preparation (JRSP) protocols [6, 7, 8, 9, 10, 11, 12, 13, 14] have been proposed with participation of more than one preparer. Neither preparer is able to identify the to-be-prepared state since the state’s information is secretly split among them. JRSP has also been approached from an experimental architecture point of view [15].

The first JRSP was proposed in [6], which, however, contained some errors. These errors were then corrected in [7] in which a new way to perform JRSP was also put forward. It is in [7] the terminology “JRSP” was introduced for the first time and is now widely used in the community. Originally, single-qubit states were dealt with. In this work we
are concerned with two qubits in the most general state of the form

\[ |\Psi\rangle_{XY} = \sum_{j=0}^{3} \alpha_j |j\rangle_{XY}, \tag{1} \]

where \( \alpha_j \in \mathbb{C} \), \( \sum_{j=0}^{3} |\alpha_j|^2 = 1 \) and \( \{|0\rangle_{XY}, |1\rangle_{XY}, |2\rangle_{XY}, |3\rangle_{XY} \} \) are shorthands for \( \{|00\rangle_{XY}, |01\rangle_{XY}, |10\rangle_{XY}, |11\rangle_{XY} \} \), respectively. Probabilistic JRSP of \( |\Psi\rangle \) was studied in Refs. [10, 11, 12, 13, 14] using typical entangled states such as Greenberger-Horne-Zeilinger (GHZ) trios [16], W states [17] or Einstein-Podolsky-Rosen (EPR) pairs [18] as the shared quantum resource. Of particular interest are two recent protocols in Refs. [13, 14], where JRSP of \( |\Psi\rangle \) can be performed deterministically, i.e., with the success probability \( P = 1 \). Achieving \( P = 1 \) is very important from a viewpoint of the overall cost because the actually consumed resource scales with \( P^{-1} \). The key idea for deterministic JRSP is the adopting of the feed-forward measurement strategy. More precisely, the preparers should not carry out their measurements independently (as in Refs. [6, 7, 8, 9, 10, 11, 12]), but do them sequentially in such a way that the outcome of the first measurement decides the basis for the second measurement. Note that such a strategy does not violate the requirement of LOCC at all.

II. THE PROTOCOL

Consider the case with two preparers (Alice 1 and Alice 2) and one receiver (Bob). The full information of \( |\Psi\rangle \) is characterized by the parameter set \( S = \{\alpha_j\} \) which can be split into two subsets \( S_1 \) and \( S_2 \), with \( S_1 \) given only to Alice 1 and \( S_2 \) only to Alice 2. One can choose \( S_1 = \{\alpha_j^{(1)}\} \) with arbitrary \( \alpha_j^{(1)} \) and define \( S_2 = \{\alpha_j/\alpha_j^{(1)}\} \) (see Ref. [10]) or \( S_2 = \{f(\alpha_j^{(1)}, \alpha_j)\} \), where \( f \) is some function of \( \alpha_j^{(1)} \) and \( \alpha_j \) (see Ref. [11]). Nevertheless, to achieve \( P = 1 \), the proper information splitting, as used in Refs. [13, 14], should be \( S_1 = \{a_j\} \) and \( S_2 = \{\varphi_j\} \), with \( \{a_j, \varphi_j\} \in R, a_j e^{i\varphi_j} = \alpha_j \) and \( \sum_{j=0}^{3} a_j^2 = 1 \). In Ref. [13] two GHZ trios were served as the shared quantum resource (see Fig. 1a), but Ref. [14] used four EPR pairs (see Fig. 1b). Because of the different kinds of shared entanglement, the participants’ action sequels also differ. Namely, in Ref. [13] the sequel is Alice 1 \( \rightarrow \) Alice 2 \( \rightarrow \) Bob, while that in Ref. [14] is (Alice 1+ Bob) \( \rightarrow \) Alice 2 \( \rightarrow \) Bob, where (Alice 1+ Bob) implies independent actions of Alice 1 and Bob in the protocol’s first step. Note that the role of Bob is passive in Ref. [13] but active in Ref. [14]. More clearly, in Ref. [13] Bob participates only in the last step and his function is just to reconstruct \( |\Psi\rangle \), whereas in Ref. [14] he not only participates in the last step but also in the very first step, in which his contribution is as important as the preparers’. For full details the reader is referred to read Refs. [13] and [14]. Here we ask the question: “Whether can we achieve \( P = 1 \) for JRSP of the most general two-qubit state (1) using the same shared quantum resource as in Ref. [14], but retaining the passive role of Bob as in Ref. [13]?” Interestingly, it turns out possible with quite nontrivial modifications as we will describe in what follows.

Unlike in Ref. [14], here the qubits’ distribution is shown as in Fig. 1c. Thus, the shared entanglement state is

\[ |Q\rangle = |epr\rangle_{A_1B_1} |epr\rangle_{A_2B_2} |epr\rangle_{A'_1A'_2} |epr\rangle_{A'_1'A'_2}, \tag{2} \]
Fig. 1. The qubits’ distribution for JRSP of the most general two-qubit state via a) two GHZ trios as in Ref. [13], b) four EPR pairs as in Ref. [14] and c) four EPR pairs as in the present protocol.

where $|epr\rangle_{A_1B_1} = (|0\rangle + |3\rangle)_{A_1B_1}/\sqrt{2}$, ..., qubits $\{A_1, A'_1, A''_1\}$ are with Alice 1, qubits $\{A_2, A'_2, A''_2\}$ with Alice 2 and qubits $\{B_1, B_2\}$ belong to Bob. Yet, the splitting of information is the same as in Refs. [13] and [14], i.e., $S_1 = \{a_j\}$ and $S_2 = \{\varphi_j\}$. The protocol
begins with Alice 1 measuring qubits \( \{A_1, A'_1, A''_1\} \) in the basis
\[
\begin{pmatrix}
|u_0\rangle_{A_1 A'_1 A''_1} \\
|u_1\rangle_{A_1 A'_1 A''_1} \\
\vdots \\
|u_7\rangle_{A_1 A'_1 A''_1}
\end{pmatrix}
= U
\begin{pmatrix}
|0\rangle_{A_1 A'_1 A''_1} \\
|1\rangle_{A_1 A'_1 A''_1} \\
\vdots \\
|7\rangle_{A_1 A'_1 A''_1}
\end{pmatrix},
\]  
with \( U \) determined solely by \( \{a_j\} \) as
\[
U = \begin{pmatrix}
a_0 & a_1 & 0 & 0 & 0 & a_2 & a_3 \\
a_1 & -a_0 & 0 & 0 & 0 & a_3 & -a_2 \\
a_2 & -a_3 & 0 & 0 & 0 & -a_0 & a_1 \\
a_3 & a_2 & 0 & 0 & 0 & -a_1 & -a_0 \\
0 & 0 & a_0 & a_1 & a_2 & a_3 & 0 & 0 \\
0 & 0 & a_1 & -a_0 & a_3 & -a_2 & 0 & 0 \\
0 & 0 & a_2 & -a_3 & -a_0 & a_1 & 0 & 0 \\
0 & 0 & a_3 & a_2 & -a_1 & -a_0 & 0 & 0
\end{pmatrix}.
\]  
Note, in Eq. (3) \( |0\rangle_{XYZ} \equiv |000\rangle_{XYZ}, \ |1\rangle_{XYZ} \equiv |001\rangle_{XYZ}, \ldots \) and \( |7\rangle_{XYZ} \equiv |111\rangle_{XYZ} \) have been used for convenience. In terms of \( \{ |u_k\rangle_{A_1 A'_1 A''_1} \} \) the state (2) reads
\[
|Q\rangle = \frac{1}{4} \sum_{k=0}^{7} |u_k\rangle_{A_1 A'_1 A''_1} |L_k\rangle_{A_2 A'_2 A''_2 B_1 B_2},
\]  
where \( (|L_k\rangle \equiv |L_k\rangle_{A_2 A'_2 A''_2 B_1 B_2}) \)
\[
|L_0\rangle = (a_0 |0\rangle + a_1 |1\rangle)_{A_2 A'_2 A''_2} |0\rangle_{B_1 B_2} + (a_0 |4\rangle + a_1 |5\rangle)_{A_2 A'_2 A''_2} |1\rangle_{B_1 B_2} + (a_2 |2\rangle + a_3 |3\rangle)_{A_2 A'_2 A''_2} |2\rangle_{B_1 B_2} + (a_2 |6\rangle + a_3 |7\rangle)_{A_2 A'_2 A''_2} |3\rangle_{B_1 B_2},
\]  
\[
|L_1\rangle = (a_0 |0\rangle - a_0 |1\rangle)_{A_2 A'_2 A''_2} |0\rangle_{B_1 B_2} + (a_1 |4\rangle - a_0 |5\rangle)_{A_2 A'_2 A''_2} |1\rangle_{B_1 B_2} + (a_2 |2\rangle - a_3 |3\rangle)_{A_2 A'_2 A''_2} |2\rangle_{B_1 B_2} + (a_3 |6\rangle - a_2 |7\rangle)_{A_2 A'_2 A''_2} |3\rangle_{B_1 B_2},
\]  
\[
|L_2\rangle = (a_2 |0\rangle - a_3 |1\rangle)_{A_2 A'_2 A''_2} |0\rangle_{B_1 B_2} + (a_2 |4\rangle - a_3 |5\rangle)_{A_2 A'_2 A''_2} |1\rangle_{B_1 B_2} + (a_3 |6\rangle - a_2 |7\rangle)_{A_2 A'_2 A''_2} |3\rangle_{B_1 B_2},
\]  
\[
|L_3\rangle = (a_3 |0\rangle + a_2 |1\rangle)_{A_2 A'_2 A''_2} |0\rangle_{B_1 B_2} + (a_3 |4\rangle + a_2 |5\rangle)_{A_2 A'_2 A''_2} |1\rangle_{B_1 B_2} - (a_1 |2\rangle + a_0 |3\rangle)_{A_2 A'_2 A''_2} |2\rangle_{B_1 B_2} - (a_1 |6\rangle + a_0 |7\rangle)_{A_2 A'_2 A''_2} |3\rangle_{B_1 B_2},
\]  
\[
|L_4\rangle = (a_0 |2\rangle + a_1 |3\rangle)_{A_2 A'_2 A''_2} |0\rangle_{B_1 B_2} + (a_0 |6\rangle + a_1 |7\rangle)_{A_2 A'_2 A''_2} |1\rangle_{B_1 B_2} + (a_2 |0\rangle + a_3 |1\rangle)_{A_2 A'_2 A''_2} |2\rangle_{B_1 B_2} + (a_2 |4\rangle + a_3 |5\rangle)_{A_2 A'_2 A''_2} |3\rangle_{B_1 B_2},
\]  
\[
|L_5\rangle = (a_1 |2\rangle - a_0 |3\rangle)_{A_2 A'_2 A''_2} |0\rangle_{B_1 B_2} + (a_1 |6\rangle - a_0 |7\rangle)_{A_2 A'_2 A''_2} |1\rangle_{B_1 B_2} + (a_3 |0\rangle - a_2 |1\rangle)_{A_2 A'_2 A''_2} |2\rangle_{B_1 B_2} + (a_3 |4\rangle - a_2 |5\rangle)_{A_2 A'_2 A''_2} |3\rangle_{B_1 B_2},
\]
\[ |L_6\rangle = (a_2 |2\rangle - a_3 |3\rangle)_{A_2A'_2A''_2} |0\rangle_{B_1B_2} + (a_2 |6\rangle - a_3 |7\rangle)_{A_2A'_2A''_2} |1\rangle_{B_1B_2} - (a_0 |0\rangle - a_1 |1\rangle)_{A_2A'_2A''_2} |2\rangle_{B_1B_2} - (a_0 |4\rangle - a_1 |5\rangle)_{A_2A'_2A''_2} |3\rangle_{B_1B_2}, \]  
\[ |L_7\rangle = (a_3 |2\rangle + a_2 |3\rangle)_{A_2A'_2A''_2} |0\rangle_{B_1B_2} + (a_3 |6\rangle + a_2 |7\rangle)_{A_2A'_2A''_2} |1\rangle_{B_1B_2} - (a_1 |0\rangle + a_0 |1\rangle)_{A_2A'_2A''_2} |2\rangle_{B_1B_2} - (a_1 |4\rangle + a_0 |5\rangle)_{A_2A'_2A''_2} |3\rangle_{B_1B_2}. \]

Should the outcome of Alice 1 be \( |u_k\rangle_{A_1A'_1A''_1} \), she publicly publishes \( k \). Due to entanglement swapping [19], after Alice 1 completed her measurement qubits \( A_2, A'_2, A''_2, B_1 \) and \( B_2 \) are disentangled from qubits \( A_1, A'_1 \) and \( A''_1 \), but become entangled among themselves, as seen from Eqs. (5)-(13). If Alice 2 independently measures qubits \( \{ A_2, A'_2, A''_2 \} \) in a basis determined solely by \( \{ \varphi_j \} \), then \( P = 1 \) cannot be achieved. Hence, Alice 2 must wait until after hearing the outcome of Alice 1. As a key strategy mentioned above, Alice 2 should make use of both \( \{ \varphi_j \} \) and \( k \) to properly determine her measurement basis. After a careful consideration, we find out that the measurement bases \( \{|v^{(k)}_l\rangle_{A_2A'_2A''_2}, l \in \{0, 7\} \} \) for Alice 2 must be chosen in the following manner

\[
V^{(k)} = \begin{pmatrix}
    x^{(k)} & 0 & y^{(k)} & 0 & 0 & z^{(k)} & 0 & \ell^{(k)} \\
    x^{(k)} & 0 & -y^{(k)} & 0 & 0 & z^{(k)} & 0 & -\ell^{(k)} \\
    x^{(k)} & 0 & y^{(k)} & 0 & 0 & -z^{(k)} & 0 & \ell^{(k)} \\
    0 & z^{(k)} & 0 & \ell^{(k)} & x^{(k)} & 0 & y^{(k)} & 0 \\
    0 & z^{(k)} & 0 & -\ell^{(k)} & x^{(k)} & 0 & -y^{(k)} & 0 \\
    0 & -z^{(k)} & 0 & \ell^{(k)} & x^{(k)} & 0 & -y^{(k)} & 0 \\
    0 & -z^{(k)} & 0 & -\ell^{(k)} & x^{(k)} & 0 & y^{(k)} & 0 
\end{pmatrix},
\]

where \( V^{(k)} \) are conditioned on both \( \{ \varphi_j \} \) and \( k \):

\[
x^{(0)} = z^{(1)} = y^{(2)} = \ell^{(3)} = y^{(4)} = \ell^{(5)} = x^{(6)} = z^{(7)} = \frac{1}{2} e^{-i \varphi_0},
\]
\[
z^{(0)} = x^{(1)} = \ell^{(2)} = y^{(3)} = \ell^{(4)} = y^{(5)} = z^{(6)} = x^{(7)} = \frac{1}{2} e^{-i \varphi_1},
\]
\[
y^{(0)} = \ell^{(1)} = x^{(2)} = z^{(3)} = x^{(4)} = z^{(5)} = y^{(6)} = \ell^{(7)} = \frac{1}{2} e^{-i \varphi_2},
\]
\[
\ell^{(0)} = y^{(1)} = z^{(2)} = x^{(3)} = z^{(4)} = x^{(5)} = \ell^{(6)} = y^{(7)} = \frac{1}{2} e^{-i \varphi_3}.
\]
Expressed through \(\{|u_k\rangle_{A_1A_1'}A''_1, \left|v^k_l\right\rangle_{A_2A_2'}A''_2\}\) the state (2) can be written as

\[
|Q\rangle = \frac{1}{8} \sum_{l=0}^{7} \sum_{k=0}^{7} |u_k\rangle_{A_1A_1'}A''_1 \left|v^k_l\right\rangle_{A_2A_2'}A''_2 R^{+}_{kl} |\Psi\rangle_{B_1B_2},
\]

with \(R_{kl}\) some unitary operators acting on Bob’s qubits \(B_1\) and \(B_2\). For a given outcome \(k\) of Alice 1, Alice 2 would find a state \(\left|v^k_l\right\rangle_{A_2A_2'}A''_2\) in which case she announces \(l\) via the public media. As for Bob, he just looks forward to hearing the outcomes \(k\) and \(l\) from the two preparers, then applies \(R_{kl}\) on qubits \(B_1\) and \(B_2\) to obtain the desired state \(|\Psi\rangle_{B_1B_2}\). For example, if \(k = l = 0\), qubits \(B_1\) and \(B_2\) are automatically collapsed into \(|\Psi\rangle_{B_1B_2}\), implying \(R_{00} = I \otimes I\), with \(I\) the identity operator. If \(k = 0\) and \(l = 1\), the two qubits collapse into \((\alpha_0 |0\rangle + \alpha_1 |1\rangle - \alpha_2 |2\rangle - \alpha_3 |3\rangle)_{B_1B_2} = Z \otimes I |\Psi\rangle_{B_1B_2}\), implying \(R_{01} = Z \otimes I\) (\(Z\) the phase-flip operator). The operators \(R_{kl}\) for all the possible values of \(k\) and \(l\) are tabulated in Table 1.

**Table 1.** Bob’s recovery operators \(R_{kl}\) in Eq. (20) and the corresponding probability \(P_{kl}\) associated with the outcomes \(k\) of Alice 1 and \(l\) of Alice 2. \(I, X\) and \(Z\) are the identity, bit-flip and phase-flip operators, respectively.

<table>
<thead>
<tr>
<th>#</th>
<th>(kl)</th>
<th>(R_{kl})</th>
<th>(P_{kl})</th>
</tr>
</thead>
<tbody>
<tr>
<td>1, 2, 3, 4</td>
<td>00, 17, 40, 57</td>
<td>(I \otimes I)</td>
<td>(1/16)</td>
</tr>
<tr>
<td>5, 6, 7, 8</td>
<td>01, 16, 41, 56</td>
<td>(Z \otimes I)</td>
<td>(1/16)</td>
</tr>
<tr>
<td>9, 10, 11, 12</td>
<td>02, 15, 42, 55</td>
<td>(Z \otimes Z)</td>
<td>(1/16)</td>
</tr>
<tr>
<td>13, 14, 15, 16</td>
<td>03, 14, 43, 54</td>
<td>(I \otimes Z)</td>
<td>(1/16)</td>
</tr>
<tr>
<td>17, 18, 19, 20</td>
<td>04, 13, 44, 53</td>
<td>(I \otimes X)</td>
<td>(1/16)</td>
</tr>
<tr>
<td>21, 22, 23, 24</td>
<td>05, 12, 45, 52</td>
<td>(Z \otimes X)</td>
<td>(1/16)</td>
</tr>
<tr>
<td>25, 26, 27, 28</td>
<td>06, 11, 46, 51</td>
<td>(Z \otimes ZX)</td>
<td>(1/16)</td>
</tr>
<tr>
<td>29, 30, 31, 32</td>
<td>07, 10, 47, 50</td>
<td>(I \otimes ZX)</td>
<td>(1/16)</td>
</tr>
<tr>
<td>33, 34, 35, 36</td>
<td>20, 37, 60, 77</td>
<td>(ZX \otimes Z)</td>
<td>(1/16)</td>
</tr>
<tr>
<td>37, 38, 39, 40</td>
<td>21, 36, 61, 76</td>
<td>(X \otimes Z)</td>
<td>(1/16)</td>
</tr>
<tr>
<td>41, 42, 43, 44</td>
<td>22, 35, 62, 75</td>
<td>(X \otimes I)</td>
<td>(1/16)</td>
</tr>
<tr>
<td>45, 46, 47, 48</td>
<td>23, 34, 63, 74</td>
<td>(ZX \otimes I)</td>
<td>(1/16)</td>
</tr>
<tr>
<td>49, 50, 51, 52</td>
<td>24, 33, 64, 73</td>
<td>(ZX \otimes ZX)</td>
<td>(1/16)</td>
</tr>
<tr>
<td>53, 54, 55, 56</td>
<td>25, 32, 65, 72</td>
<td>(X \otimes ZX)</td>
<td>(1/16)</td>
</tr>
<tr>
<td>57, 58, 59, 60</td>
<td>26, 31, 66, 71</td>
<td>(X \otimes X)</td>
<td>(1/16)</td>
</tr>
<tr>
<td>61, 62, 63, 64</td>
<td>27, 30, 67, 70</td>
<td>(ZX \otimes X)</td>
<td>(1/16)</td>
</tr>
</tbody>
</table>

As seen from the Table, each of the 64 possible situations corresponding to a pair of \(k, l \in \{0, 1, \ldots, 7\}\) occurs with an equal probability \(P_{kl} = 1/64\) and there always exists a corresponding recovery operator \(R_{kl}\). This means that the protocol succeeds all the time. In other words, it is deterministic because its total success probability is \(P = \sum_{l=0}^{7} \sum_{k=0}^{7} P_{kl} = 8 \times 8 \times \frac{1}{64} = 1\).
III. CONCLUSION

In conclusion, we have proposed a new deterministic protocol for JRSP of the most general two-qubit state. The presented protocol employs the same shared quantum resource as in Ref. [14], but with different qubits’ distribution. The total classical communication cost is 6 bits which is the same as that in Ref. [14]. However, here “6 bits = 3 bits + 3 bits” implying each of the two preparers communicating 3 bits, while in Ref. [14] “6 bits = 2 bits + 2 bits + 2 bits” implying each of the three participants communicating 2 bits. Another feature is that here the receiver just plays a passive role with a simple action as in Ref. [13], i.e., he needs to participate only in the very last step to reconstruct the target state. This, in comparison with the protocol in Ref. [14], is advantageous for the receiver in the sense that he is not required either to carry out any controlled-NOT gates or to perform some measurements or to communicate via public channels. The disadvantage, however, arises for the preparers who should be capable of performing three-qubit measurements that are technically more difficult than the two-qubit ones in Ref. [14]. From an application point of view, this work would shed some light on diversity and flexibility with respect to the ways to perform a quantum task with a given quantum/classical resource. From such a viewpoint, the present protocol proves to be uniquely suitable for the circumstance in which the receiver is not well-equipped, say, lacking controlled-NOT gates and/or measuring devices.

ACKNOWLEDGMENTS

N. B. An is supported by the Vietnam National Foundation for Science and Technology Development (NAFOSTED) under the project no. 103.99-2011.26.

REFERENCES


Received 26 April 2012.