Vol 13 No 1, January 2004
1009-1963/2004/13(01)/0014-05

Chinese Physics

© 2004 Chin. Phys. Soc.
and IOP Publishing Ltd

Implementation of non-local multiple qubits controlled-not operation via partially entangled channels*

Chen Li-Bing(陈立冰) and Lu Hong(路 洪)†

Department of Physics, Foshan University, Foshan 528000, *China*

(Received 9 April 2003; revised manuscript received 27 May 2003)

We propose two different schemes for probabilistic implementing a non-local multiple qubits controlled-not operation via partially entangled quantum channels. The overall physical resources required for accomplishing these schemes are different, and the successful implementation probabilities are also different.

Keywords: non-local multiple qubits CNOT gate, implementation, partially entangled
PACC: 0365, 4250

1. Introduction

The quantum non-locality plays a central role in quantum information processing. In recent years, much attention has been paid to the issue of non-locality of quantum states.[1−8] In fact, an equally important issue is that of non-locality of quantum operations. This situation arises, for example, in the context of distributed quantum computation,[9] in which two or more spatially separated computation units are available to solve a computational problem. Other examples are quantum network communication [10] and production of multi-particle entangled states.[11] For the alluring potential application, some fundamental research on non-local quantum operations has been presented.[10,12−15]

"If A is true, then do B". This is one of the most useful types of controlled operations in quantum computation and quantum information. The prototypical controlled operation is the two-qubit controlled-not (CNOT) gate, which acts on two qubits, a control and a target qubit, and flips the target whenever the control qubit is a $|1\rangle$. What about conditioning on multiple qubits? The familiar Toffoli gate is a particularly important special case of the multiple qubits controlled-not operation. We define the $(N+1)$-qubit $(N \geq 1)$ controlled-not operation $U(c_1, c_2, \ldots, c_N; t)$ by the equation

$$\begin{aligned} &U(c_1, c_2, \ldots, c_N; t)|c_1\rangle|c_2\rangle \ldots |c_N\rangle|t\rangle \\ &=|c_1\rangle|c_2\rangle \ldots |c_N\rangle|t \oplus c_1 c_2 \ldots c_N\rangle, \end{aligned} \tag{1}$$

which flips the target "t", conditioned on the N control qubits "$c_1, c_2, \ldots, c_N$" being set one. Note that $U(c; t)$ is the CNOT gate (N=1), and $U(c_1, c_2; t)$ is the Toffoli gate (N=2).

It is proved [16] that the Hadamard gate H $\left(H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\right)$, phase gate S $\left(S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}\right)$, CNOT gate and Toffoli gate form a universal set in terms of which any quantum computation may be expressed. Replacing the Toffoli gate in this list with the $\pi/8$ gate T $\left(T = \begin{pmatrix} 1 & 0 \\ 0 & \mathrm{e}^{\mathrm{i}\pi/4} \end{pmatrix}\right)$ also gives a universal family. This implies that the operation $U(c_1, c_2, \ldots, c_N; t)$ is an especially important essential operation when N=1,2, and the resource requirement for implementing the operation is one of the limiting factors in the construction of general unitary transformation in quantum information processing. On the other hand, when $N > 1$, the operation $U(c_1, c_2, \ldots, c_N; t)$ that can achieve the implementation of more other essential operations simultaneously

*Project supported by the Natural Science Foundation of Guangdong Province, China (Grant No 020127), and the Natural Science Foundation from the Education Bureau of Guangdong Province, China (Grant No Z02069).
†E-mail: hlu@163.net

is also important for practical applications, because it would be useful in reducing operational time in circuits that require a large number of logical operations. So the multiple qubits controlled-not operation $U(c_1, c_2, \ldots, c_N; t)$ plays a central role in many proposed constructions of quantum computational and informational networks. Because of the great usefulness of the operation, the schemes of implementing a non-local two-qubit CNOT gate and three-qubit Toffoli gate have been proposed in Refs.[12,15], where some EPR pairs are used as the quantum channels. In the proposal of implementation, if the entangled states used as the quantum channels are not maximally entangled, the operation to be implemented will be distorted and the faithful implementation is not possible. In realistic conditions, instead of maximally entangled states, the users who are localized in different space domains may share non-maximally entangled states. So implementing a non-local quantum operation using partially entangled states is of practical importance. There are two strategies to implement the non-local operation $U(c_1, c_2, \ldots, c_N; t)$ via partially entangled channels: (1) purifying the partially entangled channels to maximally entangled channels before using them by entangled concentration [17,18] then implementing the operation; (2) implementing the operation through the partially entangled channels directly then rectifying the distorted operation. In this paper, we will use the second strategy to investigate how the non-local $(N+1)$-qubit $(N \geq 1)$ controlled-not operation $U(c_1, c_2, \ldots, c_N; t)$ can be probabilistically implemented by using partially entangled states as quantum channels.

2. Non-local multiple qubits controlled-not operation

Consider $(N+1)$ users C_1, C_2,..., C_{N-1}, C_N, T are localized in different space domains, who are able to perform local operations. They also have additional resources, namely they share entangled states, and they are able to communicate classically. Suppose each of them holds a message particle in an arbitrary state $|j\rangle = a_j|0\rangle_j + b_j|1\rangle_j$ $(j = c_1, c_2, \ldots, c_N, t)$. The control parties are enumerated from c_1 to c_N and each of them is carrying one ancilla numerated by a_1 to a_N. The target qubit is denoted by t and the target party possesses N further ancillary qubits numerated by b_1 to b_N. Without loss of generality, the quantum channels between T and $C_1, C_2, \ldots, C_N$ are N independent entangled pairs with the state $\prod_{i=1}^{N}(\alpha_i|00\rangle + \beta_i|11\rangle)_{a_i,b_i}$ (where $|\alpha_i|^2 + |\beta_i|^2 = 1$, $|\alpha_i| \geq |\beta_i|$). The state of $(N+1)$ message particles, which the operation $U(c_1, c_2, \ldots, c_N; t)$ will perform on, can be expended as

$$|\psi\rangle_{c_1,c_2,\ldots,c_N,t} = |c_1\rangle|c_2\rangle \cdots |c_N\rangle|t\rangle = \sum_{i=1}^{2^{N+1}} \lambda_i \prod_{j=1}^{N+1} |u_{ij}\rangle_j, \quad (2)$$

where

$$\prod_{j=1}^{N+1} |u_{ij}\rangle_j = |u_{i1}\rangle_1 |u_{i2}\rangle_2 \cdots |u_{iN}\rangle_N |u_{i(N+1)}\rangle_{N+1}$$

is the ith basis vector in the 2^{N+1} dimensional space; $u_{ij} \in \{0, 1\}$; $|0\rangle_j$ and $|1\rangle_j$ stand for two orthogonal states of the jth message particle. The initial state of the system composed of $(N+1)$ message particles $(c_1, c_2, \ldots, c_N, t)$ and independent entangled pairs (a_1, b_1), $(a_2, b_2), \ldots, (a_N, b_N)$ reads as

$$|\psi\rangle_1 = |\psi\rangle_{c_1,c_2,\ldots,c_N,t} \prod_{i=1}^{N}(\alpha_i|00\rangle + \beta_i|11\rangle)_{a_i,b_i}. \quad (3)$$

2.1. Implementation scheme 1

The first N steps of the scheme are essentially analogous. In the ith step a local quantum CNOT gate is applied on c_i and a_i with c_i as control. Then this party measures particle a_i and the target party performs an X_{b_i} (here, and in what follows, we will write X and Z instead of σ_X and σ_Z) operation on his ancillary qubit b_i if the user C_i finds $|1\rangle_{a_i}$ and the identity if C_i finds $|0\rangle_{a_i}$. After the Nth time manipulation, the state (3) will be

$$\begin{aligned} |\psi\rangle_2 =& X_{b_N} \ldots X_{b_2} X_{b_1} \langle u_{a_N}| \ldots \langle u_{a_2}| \langle u_{a_1}| \\ & \times U_{\mathrm{CNOT}}(c_N; a_N) \ldots U_{\mathrm{CNOT}}(c_2; a_2) \\ & \times U_{\mathrm{CNOT}}(c_1; a_1)|\psi\rangle_1 \\ =& \prod_{i=1}^{N} X_{b_i} \prod_{i=1}^{N} \langle u_{a_i}| \prod_{i=1}^{N} U_{\mathrm{CNOT}}(c_i; a_i)|\psi\rangle_1, \end{aligned} \quad (4)$$

where $|u_{a_i}\rangle = |0\rangle_{a_i}$, $|1\rangle_{a_i}$ is the computation basis in which the particle a_i is measured.

In the $(N+1)$-th step, the user T applies a local operation $U(b_1, b_2, \ldots, b_N; t)$ on his particles, with the ancillas $b_1, b_2, \ldots, b_N$ being control qubits and t the target. Subsequently the control particles perform Hadamard gates on each of its ancillas.

This is then followed by N steps involving only measurements. In the ith step qubit b_i is measured in the computation basis. If the outcome is $|1\rangle_{b_i}$, then Z_{c_i} is applied to the qubit c_i, if the outcome is $|0\rangle_{b_i}$ then no action is taken on qubit c_i. After this, the state (4) collapses to

$$\begin{aligned}|\psi\rangle_3 =&Z_{c_N}\ldots Z_{c_2}Z_{c_1}\langle u_{b_N}|\ldots\langle u_{b_2}|\langle u_{b_1}|\\&\times H_{b_N}\ldots H_{b_2}H_{b_1}U(b_1,b_2,\ldots,b_N;t)|\psi\rangle_2\\=&\prod_{i=1}^{N}Z_{c_i}\prod_{i=1}^{N}\langle u_{b_i}|\prod_{i=1}^{N}H_{b_i}U(b_1,b_2,\ldots,b_N;t)|\psi\rangle_2.\end{aligned}\tag{5}$$

But the users $C_1, C_2, \ldots, C_N, T$ find they cannot evolve the state shown in Eq.(2) to the state (1) which they need, because the state given in Eq.(5) includes the parameters of the imperfect quantum channels, α_i and β_i $(i = 1, 2, \ldots, N)$. For example, when N=2, Eq.(5) will be

$$\begin{aligned}|\psi\rangle_3^{N=2} =&(1/\sqrt{2})^2(\alpha_1\alpha_2\lambda_1|000\rangle+\alpha_1\alpha_2\lambda_2|001\rangle\\&+\alpha_1\beta_2\lambda_3|010\rangle+\alpha_1\beta_2\lambda_4|011\rangle\\&+\beta_1\alpha_2\lambda_5|100\rangle+\beta_1\alpha_2\lambda_6|101\rangle\\&+\beta_1\beta_2\lambda_7|111\rangle+\beta_1\beta_2\lambda_8|110\rangle)_{c_1,c_2,t}.\end{aligned}\tag{5'}$$

In order to distill the state (1) from the state (5), the users who hold control qubits must give some general evolutions [3] to rectify the distorted state.

The last N steps of the scheme are also essentially analogous. In the last ith step, the user C_i introduces an auxiliary qubit A_i with the original $|0\rangle_{A_i}$ and operates a unitary transformation U_i under the basis $\{|00\rangle_{c_i,A_i}, |10\rangle_{c_i,A_i}, |01\rangle_{c_i,A_i}, |11\rangle_{c_i,A_i}\}$,

$$U_i=\begin{pmatrix}\beta_i/\alpha_i & 0 & \sqrt{1-(\beta_i/\alpha_i)^2} & 0\\ 0 & 1 & 0 & 0\\ \sqrt{1-(\beta_i/\alpha_i)^2} & 0 & -\beta_i/\alpha_i & 0\\ 0 & 0 & 0 & -1\end{pmatrix}.\tag{6}$$

Then C_i measures the state of particle A_i. If the measurement result is $|1\rangle_{A_i}$, the implementation fails. If all the measurement result is $|0\rangle_{A_i}$, the state of particles $c_1, c_2, \ldots, c_N$, and t collapses to

$$\begin{aligned}|\psi\rangle_4 =&\langle u_{A_N}|\ldots\langle u_{A_2}|\langle u_{A_1}|\\&\times U_N\ldots U_2U_1|\psi\rangle_3|0\rangle_{A_1}|0\rangle_{A_2}\ldots|0\rangle_{A_N}\\=&(1/\sqrt{2})^N\Big(\prod_{i=1}^{N}\beta_i\Big)U(c_1,c_2,\ldots,c_N;t)\\&\times|c_1\rangle|c_2\rangle\ldots|c_{N-1}\rangle|c_N\rangle|t\rangle,\end{aligned}\tag{7}$$

so C_1, C_2, ..., C_N and T have probability $2^{-N}\left|\prod_{j=1}^{N}\beta_j\right|^2$ to obtain the desired state $U(c_1, c_2, \ldots, c_N; t)|c_1\rangle|c_2\rangle\ldots|c_N\rangle|t\rangle$. Synthesizing all conditions (2^{2N} kinds), we obtain that the total probability of successful implementation is $P = 2^N\left|\prod_{j=1}^{N}\beta_j\right|^2$. If $|\alpha_i| = |\beta_i| = 1/\sqrt{2}$, complete implementation can be realized and the total required resources are N initially shared e-bits (maximally entangled pairs of qubits) and $2N$ c-bits (bits of classical communication). A teleportation-based protocol [19] in which the respective states of the qubits at different nodes are twice teleported would use $2N$ e-bits and $4N$ c-bits to finish the same task. One could also employ the simulation of the gate with the use of single qubit gates and CNOT gates as in Ref.[20], but such that each step is realized non-locally. In such a procedure both classical communication requirements and entanglement consumption exponentially increase with the number N of qubits in which the operation has been encoded. So this scheme is more economical in terms of physical resources. On the other hand, the scheme 1 can be implemented with linear optics, because the collective operations introduced in the scheme are unitary and any unitary operation can be realized with a sequence of beamsplitters and phaseshifters.[21] Furthermore, in terms of successful implementation probability, implementing the non-local operation $U(c_1, c_2, \ldots, c_N; t)$ directly through the partially entangled channels is always better than the strategy based on purification of the channels first. Because for a single copy, the best purification is the method shown in Ref.[18], which has optimal efficiency P=2min $\{|\alpha|^2, |\beta|^2\}$. If we restrict performance of purification to the use of linear devices, the efficiency will be less than P=2min $\{|\alpha|^2, |\beta|^2\}$. Hence the successful probability of implementation using the first strategy is always less than $P = 2^N\left|\prod_{j=1}^{N}\beta_j\right|^2$.

2.2. Implementation scheme 2

The initial state of the whole system is still in the state shown in Eq.(3). We will present in the following another scheme which allows $(N+1)$ distant users C_1, $C_2, \ldots, C_{N-1}$, C_N, T to finish the operation shown in Eq.(1) with probability $P = 2^N \prod_{i=1}^{N} |\alpha_i\beta_i|^2$.

The first $(N+1)$ steps of the scheme 2 are the same as the scheme 1. After this, the state (3) will be

$$|\psi\rangle_2' = U(b_1, b_2, \ldots, b_N; t)|\psi\rangle_2. \tag{8}$$

For example, when $N=2$, Eq.(8) is

$$\begin{aligned}(|\psi\rangle_2')^{N=2} =& [\alpha_1\alpha_2(\lambda_1|00000\rangle + \lambda_2|00100\rangle) \\ &+ \alpha_1\beta_2(\lambda_3|01001\rangle + \lambda_4|01101\rangle) \\ &+ \beta_1\alpha_2(\lambda_5|10010\rangle + \lambda_6|10110\rangle) \\ &+ \beta_1\beta_2(\lambda_7|11111\rangle + \lambda_8|11011\rangle)]_{c_1,c_2,t,b_1,b_2}.\end{aligned} \tag{8'}$$

Subsequently, the user T performs N manipulations in the same manner. In the ith step, T sends the qubit b_i through an R_{Yb_i} gate

$$R_{Yb_i} = \begin{pmatrix} \beta_i & -\alpha_i \\ \alpha_i & \beta_i \end{pmatrix}, \tag{9}$$

where R_{Yb_i} is the rotation operation about the Y-axis. This is then followed by computation basis measurements on qubit b_i. If the outcome is $|0\rangle_{b_i}$, then Z_{c_i} is applied to the qubit c_i; if the outcome is $|1\rangle_{b_i}$ then no action is taken on qubit c_i. After the Nth time manipulation, the final state of the $(N+1)$ particles $(c_1, c_2, \ldots, c_N; t)$ belonging to $(N+1)$ distant users C_1, C_2, ..., C_{N-1}, C_N, T is given by

$$\begin{aligned}|\psi\rangle_3' =& Z_{c_N} \ldots Z_{c_2} Z_{c_1} \langle u_{b_N}| \ldots \langle u_{b_2}|\langle u_{b_1}| \\ &\times R_{Yb_N} \ldots R_{Yb_2} R_{Yb_1} |\psi\rangle_2' \\ =& \prod_{i=1}^{N} Z_{c_i} \prod_{i=1}^{N} \langle u_{b_i}| \prod_{i=1}^{N} R_{Yb_i} |\psi\rangle_2'.\end{aligned} \tag{10}$$

If $\alpha_i = \beta_i = 1/\sqrt{2}$, $R_{Yb_i} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix} = H_{b_i} Z_{b_i}$,

$$\begin{aligned}|\psi\rangle_3' = (1/\sqrt{2})^N U(c_1, c_2, \ldots, c_N; t) \\ \times |c_1\rangle|c_2\rangle \ldots |c_{N-1}\rangle|c_N\rangle|t\rangle,\end{aligned} \tag{10'}$$

the probability of successful implementation is $(1/\sqrt{2})^{2N}$. Synthesizing all conditions (2^{2N} kinds), the total successful probability is $P=1$; if $\alpha_i \neq \beta_i$,

$$\begin{aligned}|\psi\rangle_3' = \Big(\prod_{i=1}^{N} \alpha_i\beta_i\Big) U(c_1, c_2, \ldots, c_N; t) \\ \times |c_1\rangle|c_2\rangle \ldots |c_{N-1}\rangle|c_N\rangle|t\rangle,\end{aligned} \tag{10''}$$

the probability of successful implementation is $\prod_{i=1}^{N} |\alpha_i\beta_i|^2$, and the total successful probability is $P = 2^N \prod_{i=1}^{N} |\alpha_i\beta_i|^2$ (all 2^N kinds of conditions).

3. Conclusion

In conclusion, we have investigated the problem of implementation of a non-local $(N+1)$-qubit controlled-not operation $U(c_1, c_2, \ldots, c_N; t)$ via partially entangled quantum channels. Two schemes have been considered to complete the task. Comparing the two schemes, we have found the total physical resources (such as the local unitary operations, prior entanglement, projective measurement in the computation basis, auxiliary qubits, and so on) required for accomplishing these schemes are different, and the successful implementation probabilities are also different. In the first one, we have found that by using some auxiliary qubits and performing some collective unitary transformations on the control qubits and auxiliary qubits, the $(N+1)$ distant users $C_1, C_2, \ldots, C_N$ and T are able to complete the non-local operation with successful probability $P = 2^N \Big|\prod_{j=1}^{N} \beta_j\Big|^2$. The probability of success is determined by the smaller Schmidt coefficient of the entangled states that are used as quantum channels. The second one gains an advantage over the first one in the simplicity of manipulation, and consumes far fewer overall resources at the expense of the much smaller successful probability $P = 2^N \prod_{i=1}^{N} |\alpha_i\beta_i|^2$, which is determined by both Schmidt coefficients of the entangled pair. This is of no great advantage to the situation where the N is large. The probabilistic implementation of quantum gates may not be so useful in the context of quantum computation, as probabilistic operations may change the complexity class of the problem and may thus destroy the (exponential) speed up of the quantum

algorithm in question. However, probabilistic gates are useful for processes such as entanglement distillation,[17] which by itself is already a probabilistic process. For example, this may help in the implementation of quantum repeaters [22] using photons only. Due to the fact that photons are ideal candidates for quantum information processing, it is highly desirable to manipulate them directly rather than by mapping their states on the states of another physical system, e.g. of an ion or an atom, and vice versa.

References

[1] Bennett C H *et al* 1993 *Phys. Rev. Lett.* **70** 1895
[2] Bouwmeester D *et al* 1997 *Nature* **390** 575
[3] Li W L, Li C F and Guo G C 2000 *Phys. Rev.* A **61** 34301
[4] Lu H 2001 *Chin. Phys. Lett.* **18** 1004
[5] Lu H and Guo G C 2000 *Phys. Lett.* A **276** 209
[6] Ye L, Yao C M and Guo G C 2001 *Chin. Phys.* **10** 1001
[7] Lin X 2001 *Acta Phys. Sin.* **50** 686 (in Chinese)
[8] Chen L B 2002 *Chin. Phys.* **11** 999
[9] Grover L K 1996 *Preprint* quant-ph/9607024
Cirac J I, Ekert A, Huelga S F and Macchiavello C 1999 *Phys. Rev.* A **59** 64294
[10] Chefles A, Gilson C R and Barnett S M 2001 *Phys. Rev.* A **63** 32314
[11] Bose S, Vedral V and Knight P L 1998 *Phys. Rev.* A **57** 822
[12] Eisert J *et al* 2000 *Phys. Rev.* A **62** 52317
[13] Collins D, Linden N and Popescu S 2001 *Phys. Rev.* A **64** 32302
[14] Zheng Y Z, Gu Y J, Chen L B and Guo G C 2002 *Chin. Phys.* **11** 529
[15] Chen L B 2002 *Chin. Phys.* **11** 881
[16] Nielsen M A and Chuang I L 2000 *Quantum Computation and Quantum Information* (Cambridge: Cambridge University Press) p213
[17] Bennett C H, Popescu S, Schumacher B, Smolin J A and Wootters W K 1996 *Phys. Rev. Lett.* **76** 722
Bennet C H *et al* 1996 *Phys. Rev.* A **54** 3824
[18] Bennett C H, Bernstein H J, Popescu S and Schumacher B 1996 *Phys. Rev.* A **53** 2046
[19] Chefles A, Gilson C R and Barnett S M 2000 *Preprint* quant-ph/0003062
[20] Barenco A *et al* 1995 *Phys. Rev.* A **52** 3457
[21] Reck M, Zeilinger A, Bernstein H J and Bertani P 1994 *Phys. Rev. Lett.* **73** 58
[22] Briegel H J, Dür W, Cirac J I and Zoller P 1998 *Phys. Rev. Lett.* **81** 5932
Dür W, Briegel H J, Cirac J I and Zoller P 1999 *Phys. Rev.* A **59** 169