

Probabilistic Nonlocal Gate Operation Via Imperfect Entanglement

Jingak JANG

National Security Research Institute, Electronics and Telecommunications Research Institute, Daejeon 305-350

Jinhyoung LEE and M. S. KIM*

School of Mathematics and Physics, The Queen's University, Belfast, BT7 1NN, U.K.

E. B. PARK and Y.-J. PARK

Department of Physics, Sogang University, Seoul 121-742

(Received 4 November 2002)

Nonlocal gate operation is based on sharing an ancillary pair of qubits in perfect entanglement. When the ancillary pair is partially entangled, the efficiency of gate operation drops. Using general transformations, we devise probabilistic nonlocal gates, which perform the nonlocal operation conclusively when the ancillary pair is only partially entangled. We show that a controlled purification protocol can be implemented by the probabilistic nonlocal operation.

PACS numbers: 03.67, 03.67.H, 03.67.L

Keywords: Nonlocal gate, Quantum computer

I. INTRODUCTION

Research in quantum computation tries to understand how quantum mechanics can improve acquisition, transmission, and processing of information. The design of any quantum computing device includes prescriptions on how to prepare quantum memories, how to realize quantum gate operation, and how to read out. In a quantum computation, any quantum logic operation can be performed in a combination of controlled-NOT (C-NOT) gates and single-bit unitary gates [1].

As a possible route toward a scalable quantum computation, nonlocal quantum gates have been suggested by Eisert *et al.* [2] and by Collins *et al.* [3]. Through a nonlocal quantum operation, the phase of a qubit can be changed depending on the state of a remote qubit. This nonlocal operation is based on sharing an ancillary pair of qubits in perfect entanglement. In realizable experiments for quantum computations, it is not easy to produce maximally entangled qubits (e-bit), so it is worth studying nonlocal gate operation when the ancillary e-bit is only partially entangled.

In this paper, we devise nonlocal C-NOT gates, which perform the operation *conclusively with a finite probability* when the ancillary e-bit is *pure* but partially entangled. We show that the nonlocal gate of Eisert *et al.* [2] can be decomposed into two smaller units. After sharing a maximally entangled ancillary e-bit, the first

unit of operation prepares a *control e-bit* which carries the information on the control qubit. The second unit then performs a NOT operation controlled by the control e-bit. When the ancillary e-bit is only partially entangled, the operation of the first unit becomes imperfect as the required preparation is impossible. We, thus, add an auxiliary unit of operation between the two operations to correct the error which occurs in the first unit. The auxiliary unit, called the *corrector unit*, works conclusively by using a general transformation. In our protocol, the general transformation is implemented after adding an ancillary qubit either by a two-body unitary interaction and an orthogonal measurement or by a positive operator-valued measurement (POVM) [4,5]. A POVM was recently accomplished in a quantum optical experiment [6]. A probabilistic computation [7] may be performed using such a probabilistic nonlocal gate.

It is well-known that a C-NOT gate can maximally entangle two product states. When performing the probabilistic nonlocal C-NOT operation for a partially entangled e-bit, a maximally entangled e-bit is conclusively produced, which implies that the present protocol concentrates entanglement from an ensemble of partially entangled particles to a sub-ensemble of maximally entangled ones.

II. NONLOCAL C-NOT GATE

*E-mail: m.s.kim@qub.ac.uk

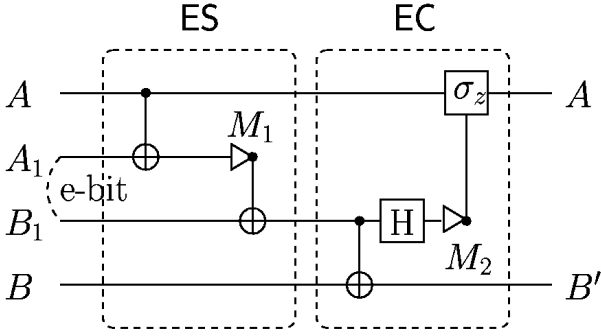


Fig. 1. Nonlocal C-NOT gate for the control qubit A and the target qubit B , assisted by a maximally entangled ancillary pair A_1 and B_1 . It can be decomposed into two small units: ES and EC. The ES unit prepares the control e-bit of A and B_1 , and the EC unit performs a C-NOT-like operation between the control e-bit and the target bit B . M_1 , M_2 are orthogonal measurements, and H is the Hadamard operator.

1. Partially Entangled Ancillary Pair

Before considering the nonlocal C-NOT gate with a partially entangled e-bit, we discuss the main idea inherent in the protocol suggested by Eisert *et al.* [2]. The protocol is presented in Fig. 1. The control qubit is A , and the target qubit is B . The ancillary e-bit, A_1 and B_1 , shown in Fig. 1, plays a crucial role in the nonlocal gate operation. Any sub-indexed A (B) is local to the qubit A (B) throughout the paper. Suppose that the control qubit A is in the state $|A\rangle_A = a|0\rangle_A + b|1\rangle_A$ and that the target qubit B is in $|B\rangle_B = c|0\rangle_B + d|1\rangle_B$. A nonlocal C-NOT operation results in

$$|A\rangle_A |B\rangle_B \rightarrow (ac|00\rangle + ad|01\rangle + bc|11\rangle + bd|10\rangle)_{AB}. \quad (1)$$

The nonlocal C-NOT gate is composed of two smaller units. The first unit, shown in the box on the left side of Fig. 1, entangles the control qubit A to B_1 , one of the ancillary e-bit. The ancillary e-bit prepared in $|E\rangle_{A_1 B_1} = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{A_1 B_1}$ and the control qubit A are not entangled at the initial instance. The local C-NOT is applied on A and A_1 to give

$$(a|0\rangle + b|1\rangle)_A |E\rangle_{A_1 B_1} \rightarrow \frac{1}{\sqrt{2}} [a(|000\rangle + |011\rangle) + b(|110\rangle + |101\rangle)]_{AA_1 B_1}. \quad (2)$$

The state of A_1 is measured, and the result is transmitted to transform B_1 . If the measurement outcome is $|1\rangle$, the qubit B_1 is flipped. No operation is applied, otherwise. After the operation of the first unit, the entanglement of $|E\rangle_{A_1 B_1}$ is swapped to $|\Theta\rangle_{AB_1}$:

$$(a|0\rangle + b|1\rangle)_A |E\rangle_{A_1 B_1} \rightarrow |\Theta\rangle_{AB_1} = (a|00\rangle + b|11\rangle)_{AB_1}. \quad (3)$$

Thus, we call the first unit of the nonlocal gate an entanglement swap (ES) unit. The prepared e-bit $|\Theta\rangle_{AB_1}$

carries the quantum information of the control qubit A , so the e-bit $|\Theta\rangle_{AB_1}$ is called a control e-bit.

At the second unit, the NOT operation is performed on B controlled by the control e-bit. We, thus, call the second unit the entanglement-controlled operation (EC) unit. In the EC unit, a local C-NOT is applied on B_1 and B to give

$$(a|00\rangle + b|11\rangle)_{AB_1} (c|0\rangle + d|1\rangle)_B \rightarrow (ac|000\rangle + ad|001\rangle + bc|111\rangle + bd|110\rangle)_{AB_1 B}. \quad (4)$$

The B_1 qubit is measured after the Hadamard transformation H . When the measurement results is $|1\rangle$, the unitary $\hat{\sigma}_z$ is applied on the A qubit. Otherwise, no operation is done on it.

Now, we consider the situation that the ancillary e-bit is in the partially entangled pure state $|\tilde{E}\rangle_{A_1 B_1} = (\alpha|00\rangle + \beta|11\rangle)_{A_1 B_1}$ with $\alpha \neq \beta$, where α and β are assumed to be real numbers satisfying $\alpha > \beta$. For the partially entangled e-bit, the protocol present in Fig. 1 no longer work and needs some modification. The control e-bit produced in the ES unit depends on the measurement outcome m at the measuring device M_1 :

$$\begin{aligned} |\tilde{\Theta}_0\rangle_{AB_1} &= \frac{1}{\sqrt{p_0}} (a\alpha|00\rangle + b\beta|11\rangle)_{AB_1} \quad \text{for } m = 0, \\ |\tilde{\Theta}_1\rangle_{AB_1} &= \frac{1}{\sqrt{p_1}} (a\beta|00\rangle + b\alpha|11\rangle)_{AB_1} \quad \text{for } m = 1, \end{aligned} \quad (5)$$

where $p_0 = (a\alpha)^2 + (b\beta)^2$ and $p_1 = (a\beta)^2 + (b\alpha)^2$ are the probabilities for the output $m = 0$ and $m = 1$, respectively. The output state $|\tilde{\Theta}_m\rangle_{AB_1}$ has a channel dependence on α and β different from that for $|\Theta\rangle_{AB_1}$ in Eq. (3).

Our task is to remove the channel dependency in the control e-bit by adding a *corrector unit* in the protocol to recover the control e-bit in the form of $|\Theta\rangle_{AB_1}$ in Eq. (3). This requires a local resource to communicate between the ES and the corrector units, which can be implemented by either a local classical communication or an internal one-bit classical memory. We present two possible protocols for the corrector unit in the following.

2. Conditioned Unitary Operator

Consider a corrector unit based on a conditioned unitary operation (CU-CUO), as shown in Fig. 2. The CU-CUO needs an ancillary qubit B_2 initially prepared in the ground state $|0\rangle_{B_2}$. A two-qubit unitary transformation is performed over qubits B_1 and B_2 [8], conditioned by the measurement outcome m at M_1 . The unitary operators \hat{U}_1 and \hat{U}_2 are given in the basis

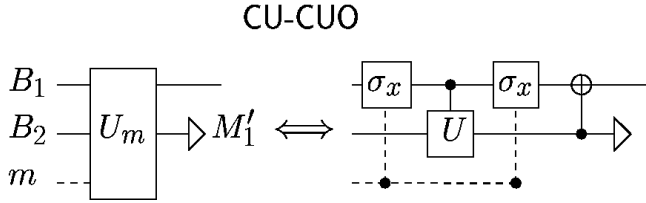


Fig. 2. Corrector unit based on the conditioned unitary operator (CU-CUO) to prepare the correct control e-bit when the ancillary e-bit is only partially entangled. The corrector unit is inserted between the ES and the EC units in Fig. 1. It works *conclusively* to make the operation free of errors. Its success is determined by the measurement outcome at M'_1 . The two-qubit unitary operation U_m can be decomposed into two conditioned- σ_x operations, a controlled-unitary U operation, and a C-NOT operations, as shown on the right side.

$\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}_{B_1 B_2}$ by

$$U_0 = \begin{pmatrix} \cos \theta & \sin \theta & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ -\sin \theta & \cos \theta & 0 & 0 \end{pmatrix} \text{ for } m = 0, \quad (6)$$

and

$$U_1 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & -\sin \theta & \cos \theta \\ 0 & 0 & \cos \theta & \sin \theta \\ 0 & 1 & 0 & 0 \end{pmatrix} \text{ for } m = 1, \quad (7)$$

where $\cos \theta = \beta/\alpha$. For $m = 0$, if \hat{U}_0 is applied on qubits B_1 and B_2 , the composite system of A , B_1 , and B_2 is in the state

$$|\tilde{\Theta}_0\rangle_{AB_1} |0\rangle_{B_2} \xrightarrow{\hat{U}_0} \frac{1}{\sqrt{p_0}} (\beta|\Theta\rangle_{AB_1} |0\rangle_{B_2} - a\alpha \sin \theta |01\rangle_{AB_1} |1\rangle_{B_2}). \quad (8)$$

Similarly, for $m = 1$, the composite system is in the state

$$|\tilde{\Theta}_1\rangle_{AB_1} |0\rangle_{B_2} \xrightarrow{\hat{U}_1} \frac{1}{\sqrt{p_1}} (\beta|\Theta\rangle_{AB_1} |0\rangle_{B_2} - b\alpha \sin \theta |10\rangle_{AB_1} |1\rangle_{B_2}). \quad (9)$$

After the unitary transformation, the state of qubit B_2 is orthogonally measured by the measuring device M'_1 . If the state $|0\rangle$ is measured with the probability β^2/p_m , the e-bit of A and B_1 is in the state $|\Theta\rangle_{AB_1}$ which is the state we want to prepare for the nonlocal C-NOT operation. If the measurement at M'_1 is $|1\rangle$, the preparation has failed and the whole process has to be restarted. Note that the probability to successfully prepare the control e-bit is $2\beta^2$.

It is important to assess the conditioned unitary operations \hat{U}_0 and \hat{U}_1 in Eqs. (6) and (7) to see what kind of basic units we need to perform such operations. We find that the two qubit unitary operators, \hat{U}_0 and \hat{U}_1 , can

Table 1. Controlled-unitary operation for the control qubit B_1 and the target qubit B_2 . $\cos \theta = \beta/\alpha$.

input		output	
B_1	B_2	B_1	B_2
$ 0\rangle$	$ 0\rangle$	$ 0\rangle$	$ 0\rangle$
$ 0\rangle$	$ 1\rangle$	$ 0\rangle$	$ 1\rangle$
$ 1\rangle$	$ 0\rangle$	$ 1\rangle$	$\cos \theta 0\rangle + \sin \theta 1\rangle$
$ 1\rangle$	$ 1\rangle$	$ 1\rangle$	$-\sin \theta 0\rangle + \cos \theta 1\rangle$

CU-POVM

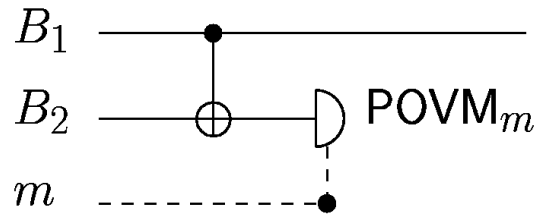


Fig. 3. Corrector unit based on a one-bit conditioned POVM (CU-POVM). POVM_m may or may not be performed, depending on the classical information of the measurement outcome m from the ES unit.

be decomposed into a C-NOT, a controlled-unitary operator, and two conditioned- $\hat{\sigma}_x$ operations, as shown in Fig. 2. The conditioned- $\hat{\sigma}_x$ operator performs either the $\hat{\sigma}_x$ operation when the measurement outcome is $m = 0$ and no operation when $m = 1$. The controlled-unitary operation is illustrated in Table. 1.

3. Positive Operator-valued Measurement

The corrector unit can also be implemented using a conditioned POVM and an ancillary qubit B_2 . The corrector unit based on the conditioned POVM (CU-POVM) is shown in Fig. 3. A set of POVM operators is determined such that a) the POVM operators depend on the measurement outcome m on the qubit A_1 , b) after the measurement, we should be able to tell whether the required control e-bit, $|\Theta\rangle_{AB_1}$, is recovered from $|\tilde{\Theta}_m\rangle_{AB_1}$ or the process has failed so that we have to start the whole operation again, and c) the probability of the success is maximized. We find the following POVM operators satisfy the requirements:

$$\hat{S}_m = \frac{1}{\alpha^2} |\psi_m\rangle \langle \psi_m|, \quad (10)$$

$$\hat{F}_m = \mathbb{1} - \hat{S}_m, \quad (11)$$

where

$$|\psi_0\rangle = \beta|0\rangle + \alpha|1\rangle \quad \text{and} \quad |\psi_1\rangle = \alpha|0\rangle + \beta|1\rangle. \quad (12)$$

Note that Eq. (11) implies the completeness relation. Straightforward algebra shows that both operators are positive with $\alpha > \beta$.

Suppose that the measurement outcome is $m = 0$ at M_1 and the operation of the ES unit puts the qubits A and B_1 in the state $|\Theta_0\rangle_{AB_1}$. An ancillary qubit B_2 is initially prepared in the ground state $|0\rangle$. Applying the C-NOT operation to B_2 controlled by B_1 , the composite system of A , B_1 , and B_2 is in

$$|\Psi_0\rangle = \frac{1}{\sqrt{p_0}}(a\alpha|000\rangle + b\beta|111\rangle)_{AB_1B_2}. \quad (13)$$

The qubit B_2 is measured using the POVM set $\{\hat{S}_0, \hat{F}_0\}$. When the outcome of \hat{S}_0 is obtained with a success probability of $p_s = \langle\Psi_0|\hat{S}_0|\Psi_0\rangle = \beta^2/p_0$, the qubits A and B_1 are in the state

$$\frac{1}{p_s}\text{Tr}_{B_2}\hat{S}_0|\Psi_0\rangle\langle\Psi_0| = |\Theta\rangle_{AB_1}\langle\Theta|, \quad (14)$$

which is the required control e-bit state for the nonlocal gate. On the other hand, if the outcome \hat{F}_0 is obtained, the correction has failed, and the whole operation must be restarted. A similar procedure is performed for the case of $m = 1$. The POVM set is now $\{\hat{S}_1, \hat{F}_1\}$. When the measurement outcome is due to \hat{S}_m , we get the required control e-bit. Note that the overall probability of the success is $2\beta^2$, which is the same as that for the CU-CUO.

It is notable that instead of the POVM, an orthogonal measurement may be employed to implement the corrector unit. In this case, the orthogonal measurement set is either $\{|\psi_0\rangle, |\phi_0\rangle\}$ or $\{|\psi_1\rangle, |\phi_1\rangle\}$, where $|\psi_m\rangle$ is defined in Eq. (12) and $|\phi_0\rangle = \alpha|0\rangle - \beta|1\rangle$ and $|\phi_1\rangle = \beta|0\rangle - \alpha|1\rangle$. For either set of the orthogonal measure, the corrector unit is successful when the state $|\psi_m\rangle$ is measured. In this case, the overall probability of success is $2\alpha^2\beta^2$, which is clearly less than $2\beta^2$ of the CU-POVM. Thus, for successful operation, the CU-POVM is better than the corrector unit based on the orthogonal measurement.

4. Resources

We have proposed two protocols for a probabilistic nonlocal C-NOT gate. It is useful to check the resources used in these protocols. Here, we confine ourselves to assess the resources required by the corrector unit. Both protocols require a one-bit classical memory, an ancillary qubit, a measurement, and one-bit classical communication. The one-bit classical memory is required for communication between the ES and the corrector units because the corrector unit processes the output state of the ES unit, depending on its measurement result. Eisert *et al.* found that one bit of classical communication in each direction and one shared e-bit is necessary and sufficient for the nonlocal implementation of a quantum

C-NOT gate when the e-bit is maximally entangled [2]. When the probabilistic nonlocal C-NOT gate operation is implemented using a partially entangled e-bit, the operation has a probability to fail. We have to introduce a measurement to determine the success of the operation, and its measurement result has to be communicated. This requires an extra measurement, and one-bit classical communication.

Comparing the two protocols in terms of required resources, it is sufficient to consider the types of measurements in the CU-CUO and the CU-POVM. In the CU-CUO, a one-bit orthogonal measurement is performed. In the CU-POVM, on the other hand, a one-bit POVM is performed, so we need to expand the Hilbert space by adding at least one extra qubit, which enables the nonorthogonal states to be measured conclusively. Thus, the CU-POVM needs an additional qubit for optimal success probability. To achieve the same success probability $2\beta^2$, the CU-CUO employs fewer resources than the CU-POVM.

III. REMARKS

One of the important properties of the C-NOT operation is to generate or to remove the entanglement between two qubits. Let us assume that we initially prepare a control qubit A in $(|0\rangle \pm |1\rangle)/\sqrt{2}$, a target qubit B in $|0\rangle$ and a shared e-bit which is partially entangled. After performing the nonlocal C-NOT operation using an imperfect channel, we obtain a maximally entangled pair. We can, thus, say that the shared imperfect channel is purified to a perfectly entangled channel. The optimal probability of the purification scheme via entanglement swapping is $2\beta^2$ [9]. The probabilistic nonlocal C-NOT gate also gives the same optimal probability. The advantage of this method is that any kind of maximally entangled pure states can be generated by preparing appropriately the initial states of the qubits A and B .

Quantum entanglement lies at the heart of nonlocal operations. We have proposed probabilistic nonlocal C-NOT gates based on a general transformation. They have the same optimal probabilities of success, $2\beta^2$. If successful, the operation is faithfully done, and more importantly, we know whether or not it has been successful. We have compared the required resources. When the initial states are appropriately prepared, the probabilistic nonlocal C-NOT gate in effect refines a partially entangled state to a perfectly entangled state. This may, thus, serve as a purification protocol for generating maximally entangled states.

ACKNOWLEDGMENTS

This work was supported by the UK Engineering and Physical Sciences Research Council (EPSRC) through

GR/R33304 and by the Brain Korea 21 project (D-1099) of the Korean Ministry of Education.

REFERENCES

- [1] D. DiVincenzo, Phys. Rev. A **51**, 1015 (1995); A. Barenco, Proc. R. Soc. Lond. A **449**, 679 (1995).
- [2] J. Eisert, K. Jacobs, P. Papadopoulos and M. B. Plenio, Phys. Rev. A **62**, 052317 (2000).
- [3] D. Collins, N. Linden and S. Popescu, quant-ph/0005102 (2000).
- [4] J. M. Jauch and C. Piron, Helv. Phys. Acta **40**, 559 (1967).
- [5] A. Peres, *Quantum Theory: Concepts and Methods* (Kluwer, Amsterdam, 1993).
- [6] R. B. M. Clarke, V. M. Kendon, A. Chefles, S. M. Barnett, E. Riis and M. Sasaki, quant-ph/0008028 (2000); R. B. V. Clarke, A. Chefles, S. M. Barnett and E. Riis, quant-ph/0007063 (2000).
- [7] L. K. Grover, quant-ph/0011118 (2000).
- [8] W-L. Li, C-F. Li and G-C. Guo, Phys. Rev. A **61**, 034301 (2000); B-S. Shi, Y-K. Jiang and G-C. Guo, Phys. Lett. A **268**, 161 (2000).
- [9] S. Bose, V. Vedral and P. L. Knight, Phys. Rev. A **60**, 194 (1999).