Entanglement-changing power of two-qubit unitary operations

Ming-Yong Ye,* Dong Sun, Yong-Sheng Zhang,† and Guang-Can Guo‡
Key Laboratory of Quantum Information, Department of Physics, University of Science and Technology of China (CAS), Hefei 230026, People's Republic of China
(Received 31 March 2004; published 30 August 2004)

Entanglement-changing power of an arbitrary two-qubit operation, including increasing and decreasing power, is investigated in this paper. We consider the maximal entanglement $C_{\max}$ and the minimal entanglement $C_{\min}$ of the states obtained by a given two-qubit unitary operation U_d acting on arbitrary pure states with fixed entanglement C_0. We give the condition that the maximal entanglement $C_{\max}$ of the obtained states can be 1 and the minimal entanglement $C_{\min}$ can be 0. When the maximal entanglement $C_{\max}$ cannot be 1, we give the maximal value it can reach. When the minimal entanglement $C_{\min}$ cannot be 0, we give the minimal value it can reach. We think $C_{\max}$ and $C_{\min}$ represent the entanglement-changing power of two-qubit unitary operations.

DOI: 10.1103/PhysRevA.70.022326 PACS number(s): 03.67.Mn, 03.65.Ta

I. INTRODUCTION

Entanglement is a fundamental resource in quantum information, which is used in quantum key distribution [1], dense coding [2], teleportation [3], and so on. Entanglement has a close relation with nonlocal operations. On the one hand, entanglement can be used to implement nonlocal operations if local operations and classical communication are permitted [4–6]. On the other hand, nonlocal operations can be used to generate entanglement. This close relation stimulates many researchers to investigate nonlocal operations [7–11]. Now nonlocal operations, similar to entanglement, have been considered as a physical resource by Nielsen *et al.* [10].

Since nonlocal operations can generate entanglement, it is important to investigate the entangling capacity of nonlocal operations. Some results have been derived [8,12,13]. In particular, Kraus and Cirac [14] calculate the maximal entanglement of the states obtained by a given two-qubit unitary operation acting on arbitrary product pure states. Leifer *et al.* [16] consider a similar question. Their efforts are devoted to maximize the entanglement of the obtained state minus the entanglement of the initial state. They think this quantity represents the entanglement-generating ability of a nonlocal gate. In this paper, we consider a general question. We consider the maximal entanglement $C_{\max}$ of the states obtained by a given two-qubit unitary operation U_d acting on arbitrary pure states with fixed entanglement C_0. Obviously, Kraus and Cirac [14] solved the question of where C_0 is zero. We solve the question for a general C_0. We also consider the minimal entanglement $C_{\min}$ of the states obtained by a given two-qubit unitary operation U_d acting on arbitrary pure states with fixed entanglement C_0. The minimal entanglement can be zero if measurements are permitted, but we still calculate it for mathematical interest and some practical use. We think $C_{\max}$ and $C_{\min}$ represent the entanglement-changing power of a two-qubit gate. The entanglement of the obtained state can be any value between them due to continuity.

The structure of the paper is as follows. In Sec. II, we introduce concurrence [17] and canonical decomposition of two-qubit gates [14,15]. We use concurrence to quantify two-qubit entanglement and we use canonical decomposition to classify two-qubit gates. In Sec. III, we give the condition that the maximal entanglement of the obtained states can be 1, and the condition that the minimal entanglement of the obtained states can be 0. In Sec. IV, we calculate the maximal and minimal entanglement of the obtained states for a general initial-state entanglement. Finally, we conclude this paper in Sec. V. The proof of our results is given in the Appendixes.

II. CONCURRENCE AND CANONICAL DECOMPOSITION

Concurrence [17] is defined to quantify entanglement of formation of mixed two-qubit states. For pure states it has a simple form. We write two-qubit states in the magic basis $|\Psi\rangle=\Sigma_{k=1}^4 b_k|\Phi_k\rangle$. Then the concurrence is $C(|\Psi\rangle)=|\Sigma_{k=1}^4 b_k^2|$, where $\{|\Phi_k\rangle\}_{k=1}^4$ is defined as follows:

$$|\Phi_1\rangle = \frac{-i}{\sqrt{2}}(|00\rangle - |11\rangle), \tag{1}$$

$$|\Phi_2\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), \tag{2}$$

$$|\Phi_3\rangle = \frac{-i}{\sqrt{2}}(|01\rangle + |10\rangle), \tag{3}$$

$$|\Phi_4\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle). \tag{4}$$

The concurrence C is zero iff the two-qubit state is a product state. When the state is maximally entangled the concurrence is 1, which requires the coefficients $\{b_k\}_{k=1}^4$ to be real, except for a global phase.

*Electronic address: myye@mail.ustc.edu.cn
†Electronic address: yshzhang@ustc.edu.cn
‡Electronic address: gcguo@ustc.edu.cn

 ©2004 The American Physical Society

Now we introduce canonical decomposition of two-qubit unitary operations [14]. Any unitary operation acting on two qubits has 16 parameters, but it can be locally equivalent to an operation which only has three parameters. According to the canonical decomposition given by Kraus and Cirac [14], we can decompose $U_{AB}=(U_A\otimes U_B)U_d(V_A\otimes V_B)$, where U_A, U_B, V_A, and V_B are local unitary operations and U_d has a special form

$$U_d=\exp\left(i\sum_{j=1}^{3}\alpha_j\sigma_j^A\otimes\sigma_j^B\right), \tag{5}$$

where $\pi/4\geqslant\alpha_1\geqslant\alpha_2\geqslant|\alpha_3|\geqslant 0$ and $\sigma_{1,2,3}$ are the Pauli matrix. Because local unitary operations do not change the entanglement, we only discuss the entanglement-changing power of U_d instead of U_{AB} in the following. In fact, we can always take $\alpha_3\geqslant 0$ when we discuss entanglement-changing power [14,16]. And because entanglement is invariant under conjugation, the entanglement-changing power of U_d is the same as U_d^* $(U_d^\dagger)$. This means if U_d can change the states of entanglement C_1 to the states of entanglement C_2, conversely it can change the states of entanglement C_2 to the states of entanglement C_1. This result will be used in the following. A very important characteristic of U_d is that the magic basis states are its eigenstates, $U_d|\Phi_j\rangle=e^{i\lambda_j}|\Phi_j\rangle$, where

$$\lambda_1=-\alpha_1+\alpha_2+\alpha_3, \tag{6}$$

$$\lambda_2=+\alpha_1-\alpha_2+\alpha_3, \tag{7}$$

$$\lambda_3=+\alpha_1+\alpha_2-\alpha_3, \tag{8}$$

$$\lambda_4=-\alpha_1-\alpha_2-\alpha_3. \tag{9}$$

III. THE CONDITIONS THAT $C_{\max}$ CAN BE 1 AND THAT $C_{\min}$ CAN BE 0

When a two-qubit unitary operation U_d is applied on the pure states with fixed entanglement C_0, first we want to know whether the maximal entanglement $C_{\max}$ of the obtained states can be 1 and the minimal entanglement $C_{\min}$ can be 0. In this section, we give the answer to this question, and we present it in the following theorem.

Theorem 1. Suppose $C_{0\max}$ denotes the maximal entanglement of the states obtained by a given unitary operation U_d acting on arbitrary product pure states, and $C_{1\min}$ denotes the minimal entanglement of the states obtained by the operation U_d acting on arbitrary maximally entangled pure states. If $C_0\geqslant C_{1\min}$, the maximal entanglement $C_{\max}$ of the states, obtained by the operation U_d acting on arbitrary pure states with fixed entanglement C_0, can be 1. If $C_0\leqslant C_{0\max}$, the minimal entanglement $C_{\min}$ of the states, obtained by the operation U_d acting on arbitrary pure states with fixed entanglement C_0, can be 0.

Proof. Since the Bell states are the eigenstates of the two-qubit unitary operation U_d, the entanglement of the states, obtained by the operation U_d acting on arbitrary maximally entangled pure states, can be any value between $C_{1\min}$ and 1 due to continuity. When $C_0\geqslant C_{1\min}$, the operation U_d can transform some maximally entangled state to a pure state with entanglement C_0. So the operation U_d^{-1} can transform some pure state with entanglement C_0 to a maximally entangled state. Since the operation U_d^{-1}, which is U_d^*, has the same entanglement-changing power as the operation U_d, the operation U_d can transform some pure state with entanglement C_0 to a maximally entangled state. It is not hard to see that the operation U_d can transform some product pure state to another product pure state. So the entanglement of the states, obtained by the operation U_d acting on arbitrary product pure states, can be any value between 0 and $C_{0\max}$ due to continuity. Using the same deduction, we can find that the operation U_d can transform some pure state with entanglement C_0 $(\leqslant C_{0\max})$ to a nonentangled state. So we can end our proof.

The entanglement $C_{0\max}$ for a given two-qubit unitary operation $U_d=\exp(i\Sigma_{j=1}^3\alpha_j\sigma_j^A\otimes\sigma_j^B)$ with $\pi/4\geqslant\alpha_1\geqslant\alpha_2\geqslant\alpha_3\geqslant 0$ has been calculated by Kraus and Cirac [14]. The detailed calculation of the entanglement $C_{1\min}$ for the operation U_d is given in Appendix A. Here we only give the results. (1) When $\alpha_1+\alpha_2\geqslant\pi/4$ and $\alpha_2+\alpha_3\leqslant\pi/4$, $C_{0\max}=1$ and $C_{1\min}=0$. (2) Otherwise, $C_{0\max}=\max_{k,l}|\sin(\lambda_k-\lambda_l)|$ and $C_{1\min}=\min_{k,l}|\cos(\lambda_k-\lambda_l)|$. More precisely, (i) when $\alpha_1+\alpha_2<\pi/4$ and $\alpha_2+\alpha_3\leqslant\pi/4$, $C_{0\max}=\sin[2(\alpha_1+\alpha_2)]$ and $C_{1\min}=\cos[2(\alpha_1+\alpha_2)]$; and (ii) when $\alpha_1+\alpha_2\geqslant\pi/4$ and $\alpha_2+\alpha_3>\pi/4$, $C_{0\max}=-\sin[2(\alpha_2+\alpha_3)]$ and $C_{1\min}=-\cos[2(\alpha_2+\alpha_3)]$.

The entanglement $C_{1\min}$ calculated in Appendix A can be applied in gate simulation. A maximal entangled state can be used to implement deterministic controlled unitary operations if local operations and classical communication (LOCC) are permitted [4,5]. If a two-qubit unitary gate can change some product initial state into a maximal entangled state, then it can be used to simulate controlled unitary operations under LOCC. If the nonlocal operation cannot change some product state into a maximal entangled one, we can let it act on an initially entangled state to get a maximally entangled one. Then what is the minimal entanglement of the initial state? It is $C_{1\min}$, which we calculate in Appendix A. We emphasize that if we can use ancillas, the situation will be different. For example, the swap gate cannot change a nonmaximally entangled state into a maximal one without ancillas, but it can produce two maximally entangled states from product states when ancillas are permitted.

IV. ENTANGLEMENT-CHANGING POWER

In Sec. III, we give the condition that the maximal entanglement $C_{\max}$ of the obtained states can be 1 and the minimal entanglement $C_{\min}$ of the obtained states can be 0. When $C_0<C_{1\min}$, the maximal entanglement $C_{\max}$ of the states, obtained by the given two-qubit unitary operation U_d acting on arbitrary pure states with fixed entanglement C_0, cannot be 1. Then what is the maximal value it can reach? When $C_0>C_{0\max}$, the minimal entanglement $C_{\min}$ of the states, obtained by the given two-qubit unitary operation U_d acting on arbitrary pure states with fixed entanglement C_0, cannot be 0. Then what is the minimal value it can reach? In this section, we give the answers to these two questions. The reachable maximal entanglement $C_{\max}$ and the reachable minimal entanglement $C_{\min}$ are calculated in Appendix B. Here we only give the results in the following theorem.

Theorem 2. When $C_0 < C_{1\,\min}$, the maximal entanglement of the states, obtained by the given two-qubit unitary operation U_d acting on arbitrary pure states with fixed entanglement C_0, is $C_{\max}=\max_{j,k}|\cos[\arccos C_0+(\lambda_j-\lambda_k)]|$. When $C_0 > C_{0\,\max}$, the minimal entanglement of the states, obtained by the given two-qubit unitary operation U_d acting on arbitrary pure states with fixed entanglement C_0, is $C_{\min} = \min_{j,k}|\cos[\arccos C_0+(\lambda_j-\lambda_k)]|$.

From theorem 1 and theorem 2, we can give a precise description of the entanglement-changing power of the two-qubit unitary operation $U_d=\exp(i\Sigma_{j=1}^{3}\alpha_j\sigma_j^A\otimes\sigma_j^B)$ with $\pi/4 \geqslant \alpha_1 \geqslant \alpha_2 \geqslant \alpha_3 \geqslant 0$.

(1) When $\alpha_1+\alpha_2\geqslant\pi/4$ and $\alpha_2+\alpha_3\leqslant\pi/4$, $C_{0\,\max}=1$ and $C_{1\,\min}=0$. The inequalities $C_0\geqslant C_{1\,\min}$ and $C_0\leqslant C_{0\,\max}$ are true for any C_0, so the maximal entanglement of the obtained states is $C_{\max}=1$, and the minimal entanglement of the obtained states is $C_{\min}=0$.

(2) When $\alpha_1+\alpha_2<\pi/4$ and $\alpha_2+\alpha_3\leqslant\pi/4$, $C_{0\,\max} = \sin[2(\alpha_1+\alpha_2)]$ and $C_{1\,\min}=\cos[2(\alpha_1+\alpha_2)]$. When $C_0 \geqslant C_{1\,\min}$, that is, $\arccos C_0\leqslant 2(\alpha_1+\alpha_2)$, the maximal entanglement of the obtained states is $C_{\max}=1=\cos 0$. When $C_0<C_{1\,\min}$, that is, $\arccos C_0 > 2(\alpha_1+\alpha_2)$, the maximal entanglement of the obtained states is $C_{\max}=\max_{j,k}|\cos[\arccos C_0+(\lambda_j-\lambda_k)]|=\cos[\arccos C_0 -2(\alpha_1+\alpha_2)]$. When $C_0\leqslant C_{0\,\max}$, that is, $\arccos C_0\geqslant\pi/2 -2(\alpha_1+\alpha_2)$, the minimal entanglement of the obtained states is $C_{\min}=0=\cos(\pi/2)$. When $C_0\leqslant C_{0\,\max}$, that is, $\arccos C_0 \geqslant\pi/2-2(\alpha_1+\alpha_2)$, the minimal entanglement of the obtained states is $C_{\min}=0=\cos(\pi/2)$. When $C_0>C_{0\,\max}$, that is, $\arccos C_0<\pi/2-2(\alpha_1+\alpha_2)$, the minimal entanglement of the obtained states is $C_{\min}=\min_{j,k}|\cos[\arccos C_0+(\lambda_j-\lambda_k)]| =\cos[\arccos C_0+2(\alpha_1+\alpha_2)]$. In a unified form,

$$C_{\max} = \cos(\max[\arccos C_0 - 2(\alpha_1+\alpha_2),0]) \tag{10}$$

and

$$C_{\min} = \cos\left(\min\left[\arccos C_0 + 2(\alpha_1+\alpha_2), \frac{\pi}{2}\right]\right). \tag{11}$$

(3) When $\alpha_1+\alpha_2\geqslant\pi/4$ and $\alpha_2+\alpha_3>\pi/4$, $C_{0\,\max} =\sin[2(\alpha_2+\alpha_3)]=\cos[2(\alpha_2+\alpha_3)-\pi/2]$ and $C_{1\,\min}= -\cos[2(\alpha_2+\alpha_3)]=\cos[\pi-2(\alpha_2+\alpha_3)]$. When $C_0\geqslant C_{1\,\min}$, that is, $\arccos C_0\leqslant\pi-2(\alpha_2+\alpha_3)$, the maximal entanglement of the obtained states is $C_{\max}=1=\cos 0$. When $C_0<C_{1\,\min}$, that is, $\arccos C_0>\pi-2(\alpha_2+\alpha_3)$, the maximal entanglement of the obtained states is $C_{\max}=\max_{j,k}|\cos[\arccos C_0+(\lambda_j-\lambda_k)]| =\cos[\arccos C_0-\pi+2(\alpha_2+\alpha_3)]$. When $C_0\leqslant C_{0\,\max}$, that is, $\arccos C_0\geqslant 2(\alpha_2+\alpha_3)-\pi/2$, the minimal entanglement of the obtained states is $C_{\min}=0=\cos(\pi/2)$. When $C_0>C_{0\,\max}$, that is, $\arccos C_0<2(\alpha_2+\alpha_3)-\pi/2$, the minimal entanglement of the obtained states is $C_{\min}=\min_{j,k}|\cos[\arccos C_0 +(\lambda_j-\lambda_k)]|=\cos[\arccos C_0+\pi-2(\alpha_2+\alpha_3)]$. In a unified form,

$$C_{\max} = \cos(\max[\arccos C_0 - \pi + 2(\alpha_2+\alpha_3),0]) \tag{12}$$

and

$$C_{\min} = \cos(\min[\arccos C_0 + \pi - 2(\alpha_2+\alpha_3),\pi/2]). \tag{13}$$

Notice that the operation $U_d(\pi/4-\alpha_3,\pi/4-\alpha_2,\pi/4-\alpha_1)$ can be obtained from the operation $U_d(-\alpha_3,-\alpha_2,-\alpha_1)$ followed by some single-qubit unitary operations and a swap operation. So it is not hard to find that the two-qubit unitary operations $U_d(\pi/4-\alpha_3,\pi/4-\alpha_2,\pi/4-\alpha_1)$ and $U_d(\alpha_1,\alpha_2,\alpha_3)$ have the same entanglement-changing power. Now we can easily get the maximal and minimal entanglement in Eqs. (12) and (13) from Eqs. (10) and (11), since $(\pi/4-\alpha_3)+(\pi/4-\alpha_2)<\pi/4$ and $(\pi/4-\alpha_2)+(\pi/4-\alpha_1) \leqslant\pi/4$.

The maximal and minimal entanglement of the obtained states is calculated when the input states are pure states. What happens if the input states can be mixed states but with fixed entanglement? It is still an open question to us. Notice that Kraus and Cirac's result [14] and Leifer *et al.*'s result [16] are still valid for mixed input states. We conjecture that the results in our paper are still valid for mixed input states.

V. CONCLUSION

In this paper, we consider the maximal and minimal entanglement of the states obtained by a given two-qubit unitary operation acting on arbitrary pure states with fixed entanglement. We think the maximal and minimal entanglement we get represents the entanglement-changing power of a two-qubit unitary operation. First we give the condition that the maximal entanglement of the obtained states can be 1 and the minimal entanglement of the obtained states can be 0. When the maximal entanglement of the obtained states cannot be 1, we give the maximal value it can reach. When the minimal entanglement of the obtained states cannot be 0, we give the minimal value it can reach.

ACKNOWLEDGMENTS

This work was funded by National Fundamental Research Program (Program No. 2001CB309300), National Natural Science Foundation of China, and Chinese Innovation Fund (Grant No. 60121503).

APPENDIX A

In this appendix, we calculate the entanglement $C_{1\,\min}$, which is the minimal entanglement of the states obtained by the operation U_d from arbitrary maximally entangled pure states. We write the initial state in the magic basis, $|\Psi_0\rangle =\Sigma_{j=1}^4 b_j|\Phi_j\rangle$. The coefficients $\{b_j\}_{j=1}^4$ are real and $\Sigma_{j=1}^4 b_j^2 =1$. The final state is

$$|\Psi\rangle = U_d|\Psi_0\rangle = \sum_{j=1}^{4} b_j e^{i\lambda_j}|\Phi_j\rangle. \tag{A1}$$

We want to minimize the concurrence C of the final state $|\Psi\rangle$. We define a Lagrangian function

$$L = C^2 - \mu\left(\sum_{k=1}^{4} b_k^2 - 1\right) = \left(\sum_{k=1}^{4} b_k^2 e^{2i\lambda_k}\right)\left(\sum_{l=1}^{4} b_l^2 e^{-2i\lambda_l}\right) - \mu\left(\sum_{k=1}^{4} b_k^2 - 1\right), \quad \text{(A2)}$$

where μ is a Lagrangian multiplier, which is real. Differentiating gives

$$\frac{\partial L}{\partial b_j} = 2b_j e^{2i\lambda_j}\left(\sum_{l=1}^{4} b_l^2 e^{-2i\lambda_l}\right) + 2b_j e^{-2i\lambda_j}\left(\sum_{k=1}^{4} b_k^2 e^{2i\lambda_k}\right) - 2\mu b_j = 0, \quad \text{(A3)}$$

multiplying b_j and summing over j gives

$$\mu = 2C^2. \quad \text{(A4)}$$

We write $(\Sigma_{k=1}^4 b_k^2 e^{2i\lambda_k}) = Ce^{i\eta}$. Then from Eq. (A3) we get

$$b_j C \cos(2\lambda_j - \eta) = b_j C^2. \quad \text{(A5)}$$

If C is equal to 0, this means U_d can change the maximal entangled states to the product states. Actually this question has been solved by Kraus and Cirac [14], though they considered a different question. We write the result here: if

$$\alpha_1 + \alpha_2 \geqslant \pi/4 \text{ and } \alpha_2 + \alpha_3 \leqslant \pi/4, \quad \text{(A6)}$$

then the two-qubit unitary operation U_d can change maximally entangled pure qubit states to product states along with local unitary operations. In the following, we focus on the cases where C is not 0. Now Eq. (A5) becomes

$$b_j \cos(2\lambda_j - \eta) = b_j C. \quad \text{(A7)}$$

One possible solution of Eq. (A7) is $b_j = 0$, but there must be some nonzero coefficients. If there is only one nonzero coefficient, the initial state is the eigenstate of U_d and the final state is also a maximally entanglement state. So there are at least two nonzero coefficients. Suppose $b_k \neq 0$ and $b_l \neq 0$, then we have

$$\cos(2\lambda_k - \eta) = \cos(2\lambda_l - \eta) = C. \quad \text{(A8)}$$

This means

$$\lambda_k - \lambda_l = n\pi \quad \text{or} \quad \lambda_k + \lambda_l - \eta = n\pi, \quad \text{(A9)}$$

where n is an integer. Suppose no parameters λ_k are equal. From the value range of $\alpha_{1,2,3}$, we can find that $\lambda_k - \lambda_l = n\pi$ is impossible. If there is another coefficient b_m that is also nonzero, it will satisfy $\lambda_k + \lambda_m - \eta = n'\pi$ for some integer n'. Then we can easily find that $\lambda_l - \lambda_m = (n - n')\pi$, but this is impossible. So there is only one pair of indices (k, l) satisfying Eq. (A9). That means there are only two nonzero coefficients and we denote them as b_k and b_l. Now our purpose is to minimize the concurrence $C = |b_k^2 e^{2i\lambda_k} + b_l^2 e^{2i\lambda_l}|$ of the final state under the condition $b_k^2 + b_l^2 = 1$. Because

$$C^2 = b_k^4 + b_l^4 + 2b_k^2 b_l^2 \cos(2\lambda_k - 2\lambda_l) \geqslant |\cos(\lambda_k - \lambda_l)|^2, \quad \text{(A10)}$$

the minimal entanglement of the final state is $C_{1\,\min} = \min_{k,l}|\cos(\lambda_k - \lambda_l)|$, which is achieved when $b_k^2 = b_l^2 = 1/2$. This minimal entanglement $C_{\min}$ is calculated when we suppose no parameters λ_k are equal. The point $(\alpha_{10}, \alpha_{20}, \alpha_{30})$ in parameter space makes some parameters λ_k equal, but for arbitrary small positive number ξ, there always exists some point $(\alpha_1', \alpha_2', \alpha_3')$ which cannot make any two parameters λ_k equal, where $|\alpha_1' - \alpha_{10}| + |\alpha_2' - \alpha_{20}| + |\alpha_3' - \alpha_{30}| < \xi$. So this constraint can be removed by continuity.

APPENDIX B

In this appendix, we calculate the maximal entanglement $C_{\max}$ and the minimal entanglement $C_{\min}$ of the states obtained by a given unitary operation from arbitrary pure states with fixed entanglement C_0. Since we know the condition under which the final state can be maximally entangled and nonentangled, and we have discussed the cases in which C_0 is 0 and 1, we assume that the entanglement of the initial state C_0 and the entanglement of the final state C cannot be 0 or 1 in the following.

We write the initial state in the magic basis: $|\Psi_0\rangle = \Sigma_{j=1}^4 b_j |\Phi_j\rangle$. The coefficients satisfy two conditions: $\Sigma_{j=1}^4 |b_j|^2 = 1$ and $|\Sigma_{j=1}^4 b_j^2|^2 = C_0^2$. We want to calculate the possible maximal and minimal entanglement of the final state, $C = |\Sigma_{j=1}^4 b_j^2 e^{2i\lambda_j}|$. We define a Lagrangian function

$$L = \left|\sum_{j=1}^{4} b_j^2 e^{2i\lambda_j}\right|^2 - \mu_1\left(\sum_{j=1}^{4} |b_j|^2 - 1\right) - \mu_2\left(\left|\sum_{j=1}^{4} b_j^2\right|^2 - C_0^2\right), \quad \text{(B1)}$$

where μ_1 and μ_2 are real. Differentiating gives

$$2b_j e^{2i\lambda_j}\left(\sum_{j=1}^{4} (b_j^*)^2 e^{-2i\lambda_j}\right) - \mu_1 b_j^* - 2\mu_2 b_j \sum_{j=1}^{4} (b_j^*)^2 = 0. \quad \text{(B2)}$$

Multiplying b_j and summing over j gives

$$\mu_1 = 2C^2 - 2\mu_2 C_0^2. \quad \text{(B3)}$$

We write $\Sigma_{j=1}^4 (b_j^*)^2 e^{-2i\lambda_j} = Ce^{2i\eta}$ and $\Sigma_{j=1}^4 (b_j^*)^2 = C_0 e^{2i\epsilon}$. Substituting them into Eq. (B2), we get

$$2b_j Ce^{2i(\lambda_j + \eta)} - \mu_1 b_j^* - 2\mu_2 b_j C_0 e^{2i\epsilon} = 0. \quad \text{(B4)}$$

One possible solution of Eq. (B4) is $b_j = 0$. To find nonzero b_j, we write $b_j = \beta_j e^{i\gamma_j}$. Then Eq. (B4) becomes

$$C^2 - \mu_2 C_0^2 - Ce^{2i(\lambda_j + \eta + \gamma_j)} + \mu_2 C_0 e^{2i(\gamma_j + \epsilon)} = 0. \quad \text{(B5)}$$

If $\mu_2 = 0$, then $C^2 - Ce^{2i(\lambda_j + \eta + \gamma_j)} = 0$. Because C is real, it will be 0 or 1. We have found the condition that the entanglement of the final state is 0 or 1. So we assume that μ_2 is nonzero in the following. If there is only one nonzero coefficient, the initial and final state will both be maximally entangled, which is trivial. So there are at least two nonzero coefficients. Assume b_j and b_k are nonzero. Similar to Eq. (B5), we have

$$C^2 - \mu_2 C_0^2 - Ce^{2i(\lambda_k + \eta + \gamma_k)} + \mu_2 C_0 e^{2i(\gamma_k + \epsilon)} = 0. \quad \text{(B6)}$$

Subtracting Eq. (B6) from Eq. (B5), we get

$$(e^{2i(\lambda_j+\eta+\gamma_j)} - e^{2i(\lambda_k+\eta+\gamma_k)})C = \mu_2 C_0 (e^{2i(\gamma_j+\epsilon)} - e^{2i(\gamma_k+\epsilon)}). \tag{B7}$$

Simplifying Eq. (B7), we get

$$\sin(\lambda_j - \lambda_k + \gamma_j - \gamma_k)C = e^{i(2\epsilon-2\eta-\lambda_j-\lambda_k)}\mu_2 C_0 \sin(\gamma_j - \gamma_k). \tag{B8}$$

We assume no parameters λ_j are equal. Because $\mu_2 C_0 C$ is nonzero and $\sin(\gamma_j - \gamma_k)$ cannot be 0, from Eq. (B8) we can get

$$2\epsilon - 2\eta - \lambda_j - \lambda_k = n\pi,\ n \in Z. \tag{B9}$$

Because no parameters λ_j are equal, there is only one pair of indices (j,k) satisfying Eq. (B9). So there is only one pair of nonzero coefficients. Now Eq. (B2) becomes

$$2b_j e^{2i\lambda_j}[(b_j^*)^2 e^{-2i\lambda_j} + (b_k^*)^2 e^{-2i\lambda_k}] - \mu_1 b_j^* - 2\mu_2 b_j[(b_j^*)^2 + (b_k^*)^2] = 0. \tag{B10}$$

Substituting $b_j = \beta_j e^{i\gamma_j}$ and $b_k = \beta_k e^{i\gamma_k}$ into Eq. (B10), we have

$$2\beta_j^2 + 2\beta_k^2 \cos(\alpha+\beta) - \mu_1 - 2\mu_2(\beta_j^2 + \beta_k^2 \cos\alpha) = 0, \tag{B11}$$

$$\sin(\alpha+\beta) = \mu_2 \sin\alpha, \tag{B12}$$

where $\alpha = 2(\gamma_j - \gamma_k)$, $\beta = 2(\lambda_j - \lambda_k)$. Similarly, we have

$$2\beta_k^2 + 2\beta_j^2 \cos(\alpha+\beta) - \mu_1 - 2\mu_2(\beta_k^2 + \beta_j^2 \cos\alpha) = 0. \tag{B13}$$

Subtracting Eq. (B13) from Eq. (B11), we get

$$(\beta_j^2 - \beta_k^2)\left[\sin^2\left(\frac{\alpha+\beta}{2}\right) - \mu_2 \sin^2\left(\frac{\alpha}{2}\right)\right] = 0. \tag{B14}$$

If $\beta_j^2 \neq \beta_k^2$, then we have

$$\left[\sin^2\left(\frac{\alpha+\beta}{2}\right) - \mu_2 \sin^2\left(\frac{\alpha}{2}\right)\right] = 0. \tag{B15}$$

From Eqs. (B12) and (B15), we have $\beta/2 = \lambda_j - \lambda_k = n\pi$, where n is an integer. This result contradicts with our assumption that no parameters λ_j are equal. So we have $\beta_j^2 = \beta_k^2 = 1/2$. Now we rewrite the concurrence of the initial state

$$C_0^2 = |\beta_j^2 e^{2i\gamma_j} + \beta_k^2 e^{2i\gamma_k}|^2 = \cos^2(\gamma_j - \gamma_k). \tag{B16}$$

So there will be

$$\gamma_j - \gamma_k = n\pi \pm \arccos C_0. \tag{B17}$$

The concurrence of the final state satisfies

$$C^2 = |\beta_j^2 e^{2i(\gamma_j+\lambda_j)} + \beta_k^2 e^{2i(\gamma_k+\lambda_k)}|^2 = \cos^2(\gamma_j - \gamma_k + \lambda_j - \lambda_k) = \cos^2[\arccos C_0 \pm (\lambda_j - \lambda_k)]. \tag{B18}$$

So the maximal possible concurrence of the final state is

$$C_{\max} = \max_{j,k} |\cos[\arccos C_0 + (\lambda_j - \lambda_k)]|. \tag{B19}$$

The minimal possible concurrence of the final state is

$$C_{\min} = \min_{j,k} |\cos[\arccos C_0 + (\lambda_j - \lambda_k)]|. \tag{B20}$$

These results are derived when we assume no parameters λ_k are equal. This constraint can be removed by continuity, and the reason is the same as explained in Appendix A.

[1] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
[2] C. H. Bennett and S. J. Wiesner, Phys. Rev. Lett. **69**, 2881 (1992).
[3] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, Phys. Rev. Lett. **70**, 1895 (1993).
[4] J. Eisert, K. Jacobs, P. Papadopoulos, and M. B. Plenio, Phys. Rev. A **62**, 052317 (2000).
[5] B. Reznik, Y. Aharonov, and B. Groisman, Phys. Rev. A **65**, 032312 (2002).
[6] J. I. Cirac, W. Dür, B. Kraus, and M. Lewenstein, Phys. Rev. Lett. **86**, 544 (2001).
[7] W. Dür, G. Vidal, and J. I. Cirac, Phys. Rev. Lett. **89**, 057901 (2002).
[8] W. Dür, G. Vidal, J. I. Cirac, N. Linden, and S. Popescu, Phys. Rev. Lett. **87**, 137901 (2001).
[9] G. Vidal and J. I. Cirac, Phys. Rev. Lett. **88**, 167903 (2002).
[10] M. A. Nielsen *et al.*, Phys. Rev. A **67**, 052301 (2003).
[11] J. Zhang, J. Vala, S. Sastry, and K. B. Whaley, Phys. Rev. A **67**, 042313 (2003).
[12] X. Wang and B. C. Sanders, Phys. Rev. A **68**, 014301 (2003).
[13] P. Zanardi, C. Zalka, and L. Faoro, Phys. Rev. A **62**, 030301 (2000).
[14] B. Kraus and J. I. Cirac, Phys. Rev. A **63**, 062309 (2001).
[15] N. Khaneja, R. Brockett, and S. J. Glaser, Phys. Rev. A **63**, 032308 (2001).
[16] M. S. Leifer, L. Henderson, and N. Linden, Phys. Rev. A **67**, 012306 (2003).
[17] S. Hill and W. K. Wootters, Phys. Rev. Lett. **78**, 5022 (1997).