The Existence of Quantum Entanglement Catalysts

Xiaoming Sun, Runyao Duan, and Mingsheng Ying

***Abstract*—Without additional resources, it is often impossible to transform one entangled quantum state into another with local quantum operations and classical communication. Jonathan and Plenio (*Phys. Rev. Lett.*, vol. 83, p. 3566, 1999) presented an interesting example showing that the presence of another state, called a catalyst, enables such a transformation without changing the catalyst. They also pointed out that in general it is very hard to find an analytical condition under which a catalyst exists. In this paper, we study the existence of catalysts for two incomparable quantum states. For the simplest case of 2×2 catalysts for transformations from one 4×4 state to another, a necessary and sufficient condition for existence is found. For the general case, we give an efficient polynomial time algorithm to decide whether a $k \times k$ catalyst exists for two $n \times n$ incomparable states, where k is treated as a constant.**

***Index Terms*—Entanglement catalysts, entanglement states, entanglement transformation, quantum information.**

I. Introduction

ENTANGLEMENT is a fundamental quantum-mechanical resource that can be shared among spatially separated parties. The existence of entanglement is a distinguishing feature of quantum mechanics that does not exist in classical mechanics. It plays a central role in some striking applications of quantum computation and quantum information, such as quantum teleportation [1], quantum superdense coding [2], and quantum cryptography [3]. As a result, entanglement has been recognized as a useful physical resource [4]. However, many fundamental problems concerning quantum entanglement are still unsolved. An important such problem concerns the existence of entanglement transformation. Suppose that Alice and Bob each have one part of a bipartite state. The question then is what other states can the entangled state be transformed into? Since an entangled state is separated spatially, it is natural to require that Alice and Bob can only make use of local operations and classical communication (LOCC). Significant progress in the study of entanglement was made by Bennett, Bernstein, Popescu, and Schumacher [5] in 1996. They proposed an entanglement concentration protocol which solved the entanglement transformation problem in the asymptotic case. In 1999, Nielsen [6] made another important advance as follows. Suppose there is a bipartite state

$$|\psi_1\rangle = \sum_{i=1}^{n} \sqrt{\alpha_i}|i\rangle_A|i\rangle_B$$

Manuscript received November 19, 2003; revised May 4, 2004. This work was supported in part by the National Foundation of Natural Sciences of China under Grants 60223004, 60496321, 60321002, and 60305005.

The authors are with the State Key Laboratory of Intelligent Technology and Systems, Department of Computer Science and Technology, Tsinghua University, Beijing, 100084, China (e-mail: sun_xm97@mails.tsinghua.edu.cn; dry02@mails.tsinghua.edu.cn; yingmsh@mail.tsinghua.edu.cn).

Communicated by E. Knill, Associate Editor for Quantum Information Theory.

Digital Object Identifier 10.1109/TIT.2004.839477

shared between Alice and Bob, with ordered Schmidt coefficients (OSCs for short) $\alpha_1 \geq \alpha_2 \geq \cdots \geq \alpha_n \geq 0$, and they want to transform $|\psi_1\rangle$ into another bipartite state

$$|\psi_2\rangle = \sum_{i=1}^{n} \sqrt{\beta_i}|i\rangle_A|i\rangle_B$$

with OSCs $\beta_1 \geq \beta_2 \geq \cdots \geq \beta_n \geq 0$. It was proved that $|\psi_1\rangle \rightarrow |\psi_2\rangle$ is possible under LOCC if and only if $\lambda_{\psi_1} \prec \lambda_{\psi_2}$, where λ_{ψ_1} and λ_{ψ_2} are the vectors of OSCs of $|\psi_1\rangle$ and $|\psi_2\rangle$, respectively, i.e., $\lambda_{\psi_1} = (\alpha_1, \ldots, \alpha_n)$, $\lambda_{\psi_2} = (\beta_1, \ldots, \beta_n)$, and $\prec$ denotes the majorization relation [7], [8], i.e., for $1 \leq l \leq n$

$$\sum_{i=1}^{l} \alpha_i \leq \sum_{i=1}^{l} \beta_i$$

with equality when $l = n$. This fundamental contribution by Nielsen provides us with an extremely useful mathematical tool for studying entanglement transformation. A simple but significant fact implied by Nielsen's theorem is that there exist incomparable states $|\psi_1\rangle$ and $|\psi_2\rangle$ with both transformations $|\psi_1\rangle \rightarrow |\psi_2\rangle$ and $|\psi_2\rangle \rightarrow |\psi_1\rangle$ impossible. Shortly after Nielsen's work, a quite surprising phenomenon of entanglement, namely, entanglement catalysis, was discovered by Jonathan and Plenio [9]. They gave an example showing that one may use another entangled state $|c\rangle$, known as a catalyst, to make an impossible transformation $|\psi\rangle \rightarrow |\phi\rangle$ possible. To be more precise, the transformation is in the form of $|\psi\rangle \otimes |c\rangle \rightarrow |\phi\rangle \otimes |c\rangle$, where the catalyst $|c\rangle$ is not modified in the process.

Entanglement catalysis is another useful protocol that quantum mechanics provides. Therefore, to exploit the full power of quantum information processing, we would like a better understanding of the following basic problem: given a pair of incomparable states $|\psi_1\rangle$ and $|\psi_2\rangle$ with $|\psi_1\rangle \not\rightarrow |\psi_2\rangle$ and $|\psi_2\rangle \not\rightarrow |\psi_1\rangle$, determine whether there exists a catalyst $|c\rangle$ such that $|\psi_1\rangle \otimes |c\rangle \rightarrow |\psi_2\rangle \otimes |c\rangle$. According to Nielsen's theorem, solving the problem requires determining whether there is a state $|c\rangle$ for which the majorization relation $\lambda_{\psi_1 \otimes c} \prec \lambda_{\psi_2 \otimes c}$ holds. As pointed out by Jonathan and Plenio [9], it is very difficult to find an analytical and both necessary and sufficient condition for the existence of a catalyst. The difficulty is mainly due to lack of suitable mathematical tools to deal with majorization of tensor product states, and especially the flexible ordering of the OSCs of tensor products. In [9], Jonathan and Plenio only gave some simple necessary conditions for the existence of catalysts, but no sufficient condition was found. Those necessary conditions enabled them to show that entanglement catalysis can happen in the transformation between two $n \times n$ states with $n \geq 4$. One of the main aims of this paper is to give a necessary and sufficient conditions for entanglement

catalysis in the simplest case of entanglement transformations between 4×4 states with a 2×2 catalyst. For the general case, it seems not easy to find an analytical condition under which incomparable states are catalyzable. We thus follow an alternative approach: that is, to seek some efficient algorithm to decide catalyzability of entanglement transformation. Indeed, an algorithm to decide the existence of catalysts has been presented by Bandyopadhyay and Roychowdhury [10]. Unfortunately, for two $n \times n$ incomparable states, their algorithm to determine whether there exists a $k \times k$ catalyst for them runs in exponential time with complexity $O([(nk)!]^2)$, and so is intractable in practice. The intractability of Bandyopadhyay and Roychowdhury's algorithm stimulated us to find a more efficient algorithm for the same purpose, and this is exactly the second aim of this paper.

This paper is organized as follows. In Section II, we deal with entanglement catalysis in the simplest case of $n = 4$ and $k = 2$. A necessary and sufficient condition under which a 2×2 catalyst exists for an entanglement transformation between 4×4 states is presented. This condition is analytically expressed in terms of the OSCs of the states involved in the transformation, and thus it is easily checkable. Also, some interesting examples are given to illustrate the use of this condition. Section III considers the general case. We propose a polynomial-time algorithm to decide the existence of catalysts. Suppose $|\psi_1\rangle$ and $|\psi_2\rangle$ are two given $n \times n$ incomparable states, and k is any fixed natural number. With the aid of our algorithm, one can quickly find all $k \times k$ catalysts for the transformation $|\psi_1\rangle \rightarrow |\psi_2\rangle$ using only $O(n^{2k+3.5})$ time. Comparing to the time complexity $O([(nk)!]^2)$ of the algorithm given in [10], for constant k, our algorithm improves the complexity from superexponential to polynomial. We draw conclusions in Section IV, and some open problem are also discussed.

To simplify the presentation, in the rest of the paper, we identify the state $|\psi\rangle = \sum_{i=1}^{n} \sqrt{\gamma_i}|i\rangle|i\rangle$ with the vector of its Schmidt coefficients $(\gamma_1, \gamma_2, \ldots, \gamma_n)$, if the meaning is clear from the context.

II. A Necessary and Sufficient Condition of Entanglement Catalysis in the Simplest Case $(n = 4, k = 2)$

Jonathan and Plenio [9] have shown that entanglement catalysis only occurs in transformations between $n \times n$ states with $n \geq 4$. In this section, we consider the simplest case: when does there exist a 2×2 catalyst for transforming one 4×4 state to another? Assume

$$|\psi_1\rangle = (\alpha_1, \alpha_2, \alpha_3, \alpha_4) \quad \text{and} \quad |\psi_2\rangle = (\beta_1, \beta_2, \beta_3, \beta_4)$$

are two 4×4 states, where $\alpha_1 \geq \alpha_2 \geq \alpha_3 \geq \alpha_4 \geq 0$, $\sum_{i=1}^{4} \alpha_i = 1$, $\beta_1 \geq \beta_2 \geq \beta_3 \geq \beta_4 \geq 0$, and $\sum_{i=1}^{4} \beta_i = 1$. The potential catalyst is a 2×2 state, denoted by $|\phi\rangle = (c, 1-c)$, where $c \in [0.5, 1]$.

It was proved in [9] that if $|\psi_1\rangle \not\rightarrow |\psi_2\rangle$, but $|\psi_1\rangle|\phi\rangle \rightarrow |\psi_2\rangle|\phi\rangle$ then

$$\alpha_1 \leq \beta_1, \ \ \alpha_1+\alpha_2 > \beta_1+\beta_2, \alpha_1+\alpha_2+\alpha_3 \leq \beta_1+\beta_2+\beta_3 \quad (1)$$

or equivalently

$$\alpha_2+\alpha_3+\alpha_4 \geq \beta_2+\beta_3+\beta_4, \ \ \alpha_3+\alpha_4 < \beta_3+\beta_4, \ \ \alpha_4 \geq \beta_4. \quad (2)$$

Note that $\{\alpha_i\}$ and $\{\beta_i\}$ are arranged in decreasing order, so we have

$$\beta_1 \geq \alpha_1 \geq \alpha_2 > \beta_2 \geq \beta_3 > \alpha_3 \geq \alpha_4 \geq \beta_4. \quad (3)$$

These inequalities are necessary conditions for the existence of catalyst $|\phi\rangle$, and it is easy to see that they are not sufficient. In the following theorem, we give a condition which is both necessary and sufficient.

Theorem 2.1: There exists a catalyst $|\phi\rangle$ for two states $(|\psi_1\rangle, |\psi_2\rangle)$ with $|\psi_1\rangle \not\rightarrow |\psi_2\rangle$, if and only if

$$\max\left\{\frac{\alpha_1+\alpha_2-\beta_1}{\beta_2+\beta_3}, 1-\frac{\alpha_4-\beta_4}{\beta_3-\alpha_3}\right\} \leq \min\left\{\frac{\beta_1}{\alpha_1+\alpha_2}, \frac{\beta_1-\alpha_1}{\alpha_2-\beta_2}, 1-\frac{\beta_4}{\alpha_3+\alpha_4}\right\} \quad (4)$$

and (1) hold. In addition, for any $c \in [0.5, 1]$ such that

$$\max\left\{\frac{\alpha_1+\alpha_2-\beta_1}{\beta_2+\beta_3}, 1-\frac{\alpha_4-\beta_4}{\beta_3-\alpha_3}\right\} \leq c \leq \min\left\{\frac{\beta_1}{\alpha_1+\alpha_2}, \frac{\beta_1-\alpha_1}{\alpha_2-\beta_2}, 1-\frac{\beta_4}{\alpha_3+\alpha_4}\right\}$$

$|\phi\rangle = (c, 1-c)$ is a catalyst for $(|\psi_1\rangle, |\psi_2\rangle)$.

Proof: Assume $|\psi_1\rangle \not\rightarrow |\psi_2\rangle$ but $|\psi_1\rangle|\phi\rangle \rightarrow |\psi_2\rangle|\phi\rangle$ under LOCC. From [9, eq. (8)] we know (1) holds. So (2) and (3) hold as well.

A routine calculation shows that the Schmidt coefficients of $|\psi_1\rangle|\phi\rangle$ and $|\psi_2\rangle|\phi\rangle$ are

$$A = \{\alpha_1 c, \alpha_2 c, \alpha_3 c, \alpha_4 c; \alpha_1(1-c), \alpha_2(1-c), \alpha_3(1-c), \alpha_4(1-c)\}$$

and

$$B = \{\beta_1 c, \beta_2 c, \beta_3 c, \beta_4 c; \beta_1(1-c), \beta_2(1-c), \beta_3(1-c), \beta_4(1-c)\}$$

respectively. Sort the elements in A and B in decreasing order and denote the resulting sequences by $a^{(1)} \geq a^{(2)} \geq \cdots \geq a^{(8)}$ and $b^{(1)} \geq b^{(2)} \geq \cdots \geq b^{(8)}$. It is clear that $a^{(1)} = \alpha_1 c$, $a^{(8)} = \alpha_4(1-c)$, $b^{(1)} = \beta_1 c$, and $b^{(8)} = \beta_4(1-c)$. Since $|\psi_1\rangle|\phi\rangle \rightarrow |\psi_2\rangle|\phi\rangle$, Nielsen's theorem tells us that

$$\sum_{i=1}^{l} a^{(i)} \leq \sum_{i=1}^{l} b^{(i)} \qquad (\forall\, 1 \leq l \leq 8).$$

Since $\{\beta_i\}$ is ordered, and $c \geq 0.5$

$$\begin{aligned} \beta_1 c \geq \beta_2 c \geq \beta_3 c \geq \beta_4 c \\ \beta_1(1-c) \geq \beta_2(1-c) \geq \beta_3(1-c) \geq \beta_4(1-c) \\ \beta_i c \geq \beta_i(1-c). \end{aligned} \quad (5)$$

Now we demonstrate that

$$\beta_1 c \geq \beta_1(1-c) > \beta_2 c \geq \beta_3 c > \beta_2(1-c) \geq \beta_3(1-c) > \beta_4 c \geq \beta_4(1-c) \quad (6)$$

and, consequently, fix the ordering of B. The key idea is that the sum of the biggest l numbers in a set is greater than or equal to the sum of any l numbers in this set.

First, by definition of $\{a^{(i)}\}$ we have $a^{(1)}+a^{(2)} \geq \alpha_1 c+\alpha_2 c$. So Nielsen's theorem leads to

$$b^{(1)} + b^{(2)} \geq a^{(1)} + a^{(2)} \geq \alpha_1 c + \alpha_2 c.$$

From inequality (1), we have $\alpha_1+\alpha_2 > \beta_1+\beta_2$, so $b^{(1)}+b^{(2)} > \beta_1 c + \beta_2 c$, i.e., $b^{(2)} > \beta_2 c$. Combining this with inequality (5), we see that the only case is $b^{(2)} = \beta_1(1-c)$, $b^{(3)} = \beta_2 c$, and $\beta_1(1-c) > \beta_2 c$.

Similarly, we have

$$\begin{aligned} a^{(1)}+a^{(2)}+a^{(3)}+a^{(4)} &\geq \alpha_1 c+\alpha_2 c+\alpha_1(1-c)+\alpha_2(1-c) \\ &= \alpha_1+\alpha_2. \end{aligned}$$

So it holds that

$$\begin{aligned} b^{(1)} + b^{(2)} + b^{(3)} + b^{(4)} &\geq a^{(1)} + a^{(2)} + a^{(3)} + a^{(4)} \\ &\geq \alpha_1 + \alpha_2 > \beta_1 + \beta_2. \end{aligned}$$

This implies $b^{(4)} > \beta_2(1-c)$. Then it must be that $b^{(4)} = \beta_3 c$, and $\beta_3 c > \beta_2(1-c)$.

Now what remains is to determine the order between $b^{(5)}$ and $b^{(7)}$. We consider $b^{(7)}$ first. Nielsen's theorem yields $b^{(7)} + b^{(8)} \leq a^{(7)} + a^{(8)}$. By definition, we know that $a^{(7)} + a^{(8)} \leq \alpha_3(1-c) + \alpha_4(1-c)$. Therefore,

$$\begin{aligned} b^{(7)} + b^{(8)} &\leq \alpha_3(1-c) + \alpha_4(1-c) \\ &= (\alpha_3+\alpha_4)(1-c) < (\beta_3+\beta_4)(1-c) \end{aligned}$$

the last inequality is due to (2). Since $b^{(8)} = \beta_4(1-c)$, it follows that $b^{(7)} < \beta_3(1-c)$. Furthermore, we obtain $b^{(7)} = \beta_4 c$, $b^{(6)} = \beta_3(1-c)$, and $\beta_3(1-c) > \beta_4 c$.

Finally, only $\beta_2(1-c)$ is left, so $b^{(5)} = \beta_2(1-c)$. Combining the above arguments, we finish the proof of inequality (6).

Clearly, inequality (6) implies that

$$\frac{\beta_2}{\beta_2+\beta_3} < c < \left\{\frac{\beta_1}{\beta_1+\beta_2}, \frac{\beta_3}{\beta_3+\beta_4}\right\}. \tag{7}$$

This is needed in the remainder of the proof.

Since the order of B has been established, it enables us to calculate $\sum_{i=1}^{l} b^{(i)}$ for each l. The only remaining problem is how to calculate $\sum_{i=1}^{l} a^{(i)}$. To this end, we need the following lemma.

Lemma 2.1: Assume $A = \{a_1, \ldots, a_n\}$, $B = \{b_1, \ldots, b_n\}$. Sort B in decreasing order and denote the resulted sequence by $b^{(1)} \geq b^{(2)} \geq \cdots \geq b^{(n)}$. Then $A \prec B$ if and only if for $1 \leq l \leq n$

$$\max_{A' \subseteq A, |A'|=l} \sum_{a_i \in A'} a_i \leq \sum_{i=1}^{l} b^{(i)} \tag{8}$$

with equality when $l = n$.

Proof of Lemma 2.1: The "if" part is obvious. For the "only if " part, we sort A in decreasing order and denote the resulted sequence by $a^{(1)} \geq a^{(2)} \geq \cdots \geq a^{(n)}$. Then $A \prec B$ if and only if for $1 \leq l \leq n$

$$\sum_{i=1}^{l} a^{(i)} \leq \sum_{i=1}^{l} b^{(i)}.$$

It is easy to see that

$$\sum_{i=1}^{l} a^{(i)} = \max_{A' \subseteq A, |A'|=l} \sum_{a_i \in A'} a_i$$

so the lemma holds.

Proof of Theorem 2.1 (continued): The above lemma guarantees a way to deal with $\sum_{i=1}^{l} a^{(i)}$, namely by enumerating simply all the possible cases. For example, $a^{(1)} + a^{(2)} = \alpha_1 c + \alpha_1(1-c)$ or $\alpha_1 c + \alpha_2 c$, i.e.,

$$a^{(1)} + a^{(2)} = \max\{\alpha_1 c + \alpha_1(1-c), \alpha_1 c + \alpha_2 c\}.$$

The treatments for $\sum_{i=1}^{3} a^{(i)}, \ldots, \sum_{i=1}^{8} a^{(i)}$ are the same. What we still need to do is to solve systematically the inequalities of

$$\sum_{i=1}^{l} a^{(i)} \leq \sum_{i=1}^{l} b^{(i)} \qquad (1 \leq l \leq 8).$$

We move this daunting but routine part to the Appendix. □

The above theorem presents a necessary and sufficient condition for the case when a 2×2 catalyst exists for a transformation from one 4×4 state to another. Moreover, it is also worth noting that the theorem is indeed constructive. The second part of it gives all 2×2 catalysts (if any) for such a transformation. To illustrate the utility of the above theorem, we present some simple examples.

Example 2.1: This example is exactly the original example that Jonathan and Plenio [9] used to demonstrate entanglement catalysis. Let $|\psi_1\rangle = (0.4, 0.4, 0.1, 0.1)$ and $|\psi_2\rangle = (0.5, 0.25, 0.25, 0)$. Then

$$\begin{aligned} &\max\left\{\frac{\alpha_1+\alpha_2-\beta_1}{\beta_2+\beta_3}, 1-\frac{\alpha_4-\beta_4}{\beta_3-\alpha_3}\right\} \\ &\qquad = \max\{0.6, 1-2/3\} = 0.6 \\ &\min\left\{\frac{\beta_1}{\alpha_1+\alpha_2}, \frac{\beta_1-\alpha_1}{\alpha_2-\beta_2}, 1-\frac{\beta_4}{\alpha_3+\alpha_4}\right\} \\ &\qquad = \min\{5/8, 2/3, 1\} = 0.625. \end{aligned}$$

Since $0.6 < 0.625$, Theorem 2.1 gives us a continuous spectrum $|\phi\rangle = (c, 1-c)$ of catalysts for $|\psi_1\rangle$ and $|\psi_2\rangle$, where c ranges over the interval $[0.6, 0.625]$. In particular, when choosing $c = 0.6$, we get the catalyst $|\phi\rangle = (0.6, 0.4)$, which is the one given in [9].

Example 2.2: We also consider the example in [10]. Let $|\psi_1\rangle = (0.4, 0.36, 0.14, 0.1)$ and $|\psi_2\rangle = (0.5, 0.25, 0.25, 0)$. The catalyst for $|\psi_1\rangle$ and $|\psi_2\rangle$ given there is $\phi \geq (0.65, 0.35)$. Note that

$$\begin{aligned} &\max\left\{\frac{\alpha_1+\alpha_2-\beta_1}{\beta_2+\beta_3}, 1-\frac{\alpha_4-\beta_4}{\beta_3-\alpha_3}\right\} \\ &\qquad = \max\{0.52, 1-10/11\} = 0.52 \\ &\min\left\{\frac{\beta_1}{\alpha_1+\alpha_2}, \frac{\beta_1-\alpha_1}{\alpha_2-\beta_2}, 1-\frac{\beta_4}{\alpha_3+\alpha_4}\right\} \\ &\qquad = \min\{25/38, 10/11, 1-0\} = 25/38 \end{aligned}$$

and $0.52 < 0.65 < 25/38$, Theorem 2.1 guarantees that $|\phi\rangle$ is really a catalyst; and it allows us to find many more catalysts $|\phi\rangle = (c, 1-c)$ with $c \in [0.52, 25/38]$.

III. An Efficient Algorithm for Deciding Existence of Catalysts

In Section II, we give a necessary and sufficient condition under which a 2×2 catalyst exists for an transformation between 4×4 states. The key idea enabling us to obtain such a condition is that the order among the Schmidt coefficients of the tensor product of the catalyst and the target state in the transformation is uniquely determined by Nielsen's theorem. However, the same idea does not work for higher dimensional states, and it seems very hard to find an analytical condition for existence of catalysts in the case of higher dimensions. On the other hand, existence of catalysts is a dominant problem in exploiting the power of entanglement catalysis in quantum information processing. This leads us to explore the possibility of finding an efficient algorithm for deciding existence of catalysts. The main goal of this section is to give a polynomial time algorithm to decide whether there is a $k \times k$ catalyst for two incomparable $n \times n$ states $|\psi_1\rangle$, $|\psi_2\rangle$, where $k \geq 2$ is a fixed natural number.

To explain the intuition behind our algorithm more clearly, we first consider the case of $k = 2$. Assume $|\psi_1\rangle = (\alpha_1, \ldots, \alpha_n)$, and $|\psi_2\rangle = (\beta_1, \ldots, \beta_n)$ are two $n \times n$ states, and assume that the potential catalyst for them is a 2×2 state $\phi \geq (x, 1-x)$. The Schmidt coefficients of $|\psi_1\rangle|\phi\rangle$ and $|\psi_2\rangle|\phi\rangle$ are then given as

$$A_x = \{\alpha_1 x, \alpha_2 x, \ldots, \alpha_n x; \alpha_1(1-x), \ldots, \alpha_n(1-x)\}$$

and

$$B_x = \{\beta_1 x, \beta_2 x, \ldots, \beta_n x; \beta_1(1-x), \ldots, \beta_n(1-x)\}$$

respectively. Sort them in decreasing order and denote the resulting sequences by

$$a^{(1)}(x) \geq a^{(2)}(x) \geq \cdots \geq a^{(2n)}(x)$$

and

$$b^{(1)}(x) \geq b^{(2)}(x) \geq \cdots \geq b^{(2n)}(x).$$

By Nielsen's theorem, we know that a necessary and sufficient condition for $|\psi_1\rangle|\phi\rangle \to |\psi_2\rangle|\phi\rangle$ is

$$\sum_{i=1}^{l} a^{(i)}(x) \leq \sum_{i=1}^{l} b^{(i)}(x) \qquad (l = 1, \ldots, 2n).$$

However we do not know the exact order of elements in A and B. Let us now consider this problem in a different way. If we fix x to some constant x_0, we can calculate the elements in A, B and sort them. Then if we moves x slightly from x_0 to $x_0 + \epsilon$, the order of the elements in A (or B) does not change, except in the case that x goes through a point x^* with $\alpha_i(1-x^*) = \alpha_j x^*$ (or $\beta_i(1-x^*) = \beta_j x^*$), i.e., $x^* = \frac{\alpha_i}{\alpha_i+\alpha_j}$ (resp., $x^* = \frac{\beta_i}{\beta_i+\beta_j}$) for some $i < j$. This observation leads us to the following algorithm.

1. $\rho_{i,j} \leftarrow \frac{\alpha_i}{\alpha_i+\alpha_j}$, $\delta_{i,j} \leftarrow \frac{\beta_i}{\beta_i+\beta_j}$, $1 \leq i < j \leq n$
2. Sort $\{\rho_{i,j}\} \cup \{\delta_{i,j}\}$ in nondecreasing order, and denote the resulting sequence by $\gamma^{(1)} \leq \gamma^{(2)} \leq \cdots \leq \gamma^{(n^2-n)}$
3. $\gamma^{(0)} \leftarrow 0.5$, $\gamma^{(n^2-n+1)} \leftarrow 1$
4. **For** $i = 0$ **to** $n^2 - n$ **do**
5. $\quad c \leftarrow \frac{\gamma^{(i)}+\gamma^{(i+1)}}{2}$
6. $\quad$ Determine the order of elements in A_c and B_c, respectively
7. $\quad$ Solve the system of inequalities:

$$\begin{cases} \sum_{i=1}^{l} a^{(i)}(x) \leq \sum_{i=1}^{l} b^{(i)}(x) & (l = 1, \ldots, 2n) \\ \gamma^{(i)} \leq x \leq \gamma^{(i+1)} \end{cases}$$

8. **OUTPUT**: Catalysts do not exist, if for all $i \in \{0, 1, \ldots, n^2 - n\}$, the solution set of the above inequalities is empty; catalyst $(x, 1-x)$, if for some i the inequalities has solution.

It is easy to see that this algorithm runs in $O(n^3)$ time. In [10], an algorithm for the same purpose was also given, but it runs in $O(n!)$ time.

By generalizing the idea explained above to the case of $k \times k$ catalyst, we obtain the following theorem.

Theorem 3.1: For any two $n \times n$ states $|\psi_1\rangle = (\alpha_1, \ldots, \alpha_n)$ and $|\psi_2\rangle = (\beta_1, \ldots, \beta_n)$, the problem of whether there exists a $k \times k$ catalyst $|\phi\rangle = (x_1, \ldots, x_k)$ for the transformation $|\psi_1\rangle \to |\psi_2\rangle$ can be decided in polynomial time in n. Furthermore, if there exists a $k \times k$ catalyst, our algorithm can find all the catalysts in $O(n^{2k+3.5})$ time.

Proof: The algorithm is similar to the one for the case $k = 2$. Now the Schmidt coefficients of $|\psi_1\rangle|\phi\rangle$ and $|\psi_2\rangle|\phi\rangle$ are

$$A_x = \{\alpha_1 x_1, \ldots, \alpha_n x_1; \alpha_1 x_2, \ldots, \alpha_n x_2; \ldots, \alpha_n x_k\}$$

and

$$B_x = \{\beta_1 x_1, \ldots, \beta_n x_1; \beta_1 x_2, \ldots, \beta_n x_2; \ldots, \beta_n x_k\}.$$

If we move x in the k-dimensional space $\mathbb{R}^k$, the order of the elements in A_x (or B_x) will change if and only if x goes through a hyperplane $\alpha_{i_1} x_{i_2} = \alpha_{j_1} x_{j_2}$ ($\beta_{i_1} x_{i_2} = \beta_{j_1} x_{j_2}$) for some $i_1 < j_1$ and $i_2 > j_2$. (Indeed, the area that x ranges over is $(k-1)$-dimensional because we have a constraint of $\sum_{i=1}^{k} x_i = 1$.) First, we can write down all the equations of these hyperplanes

$$\Gamma = \{\alpha_{i_1} x_{i_2} = \alpha_{j_1} x_{j_2} | i_1 < j_1, i_2 > j_2\} \cup \{\beta_{i_1} x_{i_2} = \beta_{j_1} x_{j_2} | i_1 < j_1, i_2 > j_2\},$$

where $|\Gamma| = 2\binom{k}{2}\binom{n}{2} = O(n^2)$. In the k-dimensional space $\mathbb{R}^k$, these $O(n^2)$ hyperplanes can at most divide the whole space into $O(O(n^2)^k) = O(n^{2k})$ different parts. Note that the number of parts generated by these hyperplanes is a polynomial of n. Now we enumerate all these possible parts. In each part, for different x, the elements in A_x (or B_x) have the same order. Then we can solve the inequalities

$$\sum_{i=1}^{l} a^{(i)}(x) \leq \sum_{i=1}^{l} b^{(i)}(x) \qquad (1 \leq l \leq nk)$$

and check the order constrains by linear programming. Following the well-known result that linear programming is solvable in $O(n^{3.5})$ time, our algorithm runs in $O(n^{2k+3.5})$ time, it is a polynomial time in n whenever k is a given constant. □

Theorem 3.1 is constructive, and its proof gives an algorithm which is able not only to decide whether a catalyst of a given dimension exists, but also to find all such catalysts when they do exist. The algorithm preceding Theorem 3.1 is just a more explicit presentation of the proof for the case of $k = 2$.

IV. Conclusion and Discussion

In this paper, we investigate the problem concerning the existence of catalysts for entanglement transformations. It is solved for the simplest case in an analytical way. We give a necessary and sufficient condition for the existence of a 2×2 catalyst for a pair of two incomparable 4×4 states. Although we fail to give an analytical condition, for the general case ($k \times k$ catalysts for $n \times n$ states), an efficient polynomial time algorithm is found when k is treated as a constant. However, if k is a variable, ranging over all positive integers, the problem of determining the existence of catalysts remains open. We believe that it is NP-hard, since the set $A_x = \{\alpha_1 x_1, \ldots, \alpha_n x_1; \alpha_1 x_2, \ldots, \alpha_n x_2; \ldots, \alpha_n x_k\}$ in the proof of Theorem 3.1 potentially has exponential kind of different orders.

Appendix
Proof of Theorem 2.1

Proof of Theorem 2.1 (Remaining Part)

We need to solve the system of inequalities

$$\sum_{i=1}^{l} a^{(i)} \le \sum_{i=1}^{l} b^{(i)} \qquad (1 \le l \le 8).$$

This is carried out by the following seven items.

(I) First, we have

$$a^{(1)} \le b^{(1)} \Longleftrightarrow \alpha_1 c \le \beta_1 c \Longleftrightarrow \alpha_1 \le \beta_1. \quad (9)$$

(II) The inequality $a^{(1)} + a^{(2)} \le b^{(1)} + b^{(2)}$ may be rewritten as

$$\max\{\alpha_1 c + \alpha_1(1-c), \alpha_1 c + \alpha_2 c\} \le \beta_1 c + \beta_1(1-c) \Longleftrightarrow \quad (10)$$

$$c \le \frac{\beta_1}{\alpha_1 + \alpha_2},\ \alpha_1 \le \beta_1. \quad (11)$$

(III) We now consider $a^{(1)} + a^{(2)} + a^{(3)} \le b^{(1)} + b^{(2)} + b^{(3)}$. It is equivalent to

$$\max\{\alpha_1 c + \alpha_1(1-c) + \alpha_2 c, \alpha_1 c + \alpha_2 c + \alpha_3 c\} \le \beta_1 c + \beta_1(1-c) + \beta_2 c \Longleftrightarrow$$
$$c \le \left\{ \frac{\beta_1}{\alpha_1 + \alpha_2 + \alpha_3 - \beta_2}, \frac{\beta_1 - \alpha_1}{\alpha_2 - \beta_2} \right\}. \quad (12)$$

(IV) Equation (13) at the bottom of the page holds.[1]

(V) See (14) at the bottom of the page.

(VI) See (15) at the bottom of the page.

(VII) We have

$$\sum_{i=1}^{7} a^{(i)} \le \sum_{i=1}^{7} b^{(i)} \Longleftrightarrow a^{(8)} \ge b^{(8)} \Longleftrightarrow \alpha_4 \ge \beta_4. \quad (16)$$

Combining (7), (9)–(16) we obtain

$$c \le \left\{ \frac{\beta_1}{\beta_1 + \beta_2}, \frac{\beta_3}{\beta_3 + \beta_4}; \frac{\beta_1}{\alpha_1 + \alpha_2}, \frac{\beta_1}{\alpha_1 + \alpha_2 + \alpha_3 - \beta_2}, \frac{\beta_1 - \alpha_1}{\alpha_2 - \beta_2}, \right.$$

[1]If $\alpha_2 + \alpha_3 - \beta_2 - \beta_3 \le 0$, this term is useless.

$$\begin{aligned} a^{(1)} + a^{(2)} + a^{(3)} + a^{(4)} \le b^{(1)} + b^{(2)} + b^{(3)} + b^{(4)} &\Longleftrightarrow \\ \max\{\alpha_1 c + \alpha_1(1-c) + \alpha_2 c + \alpha_2(1-c), \alpha_1 c + \alpha_2 c + \alpha_3 c + \alpha_1(1-c), & \\ \alpha_1 c + \alpha_2 c + \alpha_3 c + \alpha_4 c\} \le \beta_1 c + \beta_1(1-c) + \beta_2 c + \beta_3 c &\Longleftrightarrow \\ \frac{\alpha_1 + \alpha_2 - \beta_1}{\beta_2 + \beta_3} \le c \le \left\{ \frac{\beta_1}{1 - \beta_2 - \beta_3}, \frac{\beta_1 - \alpha_1}{\alpha_2 + \alpha_3 - \beta_2 - \beta_3} \right\}. & \end{aligned} \quad (13)$$

$$\begin{aligned} a^{(1)} + a^{(2)} + a^{(3)} + a^{(4)} + a^{(5)} \le b^{(1)} + b^{(2)} + b^{(3)} + b^{(4)} + b^{(5)} &\Longleftrightarrow \\ a^{(6)} + a^{(7)} + a^{(8)} \ge b^{(6)} + b^{(7)} + b^{(8)} &\Longleftrightarrow \\ \min\{\alpha_2(1-c) + \alpha_3(1-c) + \alpha_4(1-c), \alpha_3(1-c) + \alpha_4 c + \alpha_4(1-c)\} & \\ \ge \beta_3(1-c) + \beta_4 c + \beta_4(1-c) &\Longleftrightarrow \\ 1 - \frac{\alpha_4 - \beta_4}{\beta_3 - \alpha_3} \le c \le 1 - \frac{\beta_4}{\alpha_2 + \alpha_3 + \alpha_4 - \beta_3}. & \end{aligned} \quad (14)$$

$$\begin{aligned} \textstyle\sum_{i=1}^{6} a^{(i)} \le \sum_{i=1}^{6} b^{(i)} &\Longleftrightarrow \\ a^{(7)} + a^{(8)} \ge b^{(7)} + b^{(8)} &\Longleftrightarrow \\ \min\{\alpha_3(1-c) + \alpha_4(1-c), \alpha_4 c + \alpha_4(1-c)\} \ge \beta_4 c + \beta_4(1-c) &\Longleftrightarrow \\ c \le 1 - \frac{\beta_4}{\alpha_3 + \alpha_4}, \quad \alpha_4 \ge \beta 4. & \end{aligned} \quad (15)$$

$$\frac{\beta_1}{1-\beta_2-\beta_3}, \frac{\beta_1-\alpha_1}{\alpha_2+\alpha_3-\beta_2-\beta_3}, 1-\frac{\beta_4}{\alpha_2+\alpha_3+\alpha_4-\beta_3}, 1-\frac{\beta_4}{\alpha_3+\alpha_4}\Bigg\} \quad (17)$$

and

$$c \geq \left\{\frac{\alpha_1+\alpha_2-\beta_1}{\beta_2+\beta_3}, 1-\frac{\alpha_4-\beta_4}{\beta_3-\alpha_3}\right\}. \quad (18)$$

Since

$$\beta_1 \geq \alpha_1 \geq \alpha_2 > \beta_2 \geq \beta_3 > \alpha_3 \geq \alpha_4 \geq \beta_4, \alpha_1+\alpha_2 > \beta_1+\beta_2$$

it follows that

$$\frac{\beta_1}{\beta_1+\beta_2} > \frac{\beta_1}{\alpha_1+\alpha_2}$$
$$\frac{\beta_3}{\beta_3+\beta_4} = 1-\frac{\beta_4}{\beta_3+\beta_4} > 1-\frac{\beta_4}{\alpha_3+\alpha_4}$$
$$\frac{\beta_1}{\alpha_1+\alpha_2} < \frac{\beta_1}{\alpha_1+\alpha_2+(\alpha_3-\beta_2)}$$
$$\frac{\beta_1}{\alpha_1+\alpha_2} < \frac{\beta_1}{\beta_1+\beta_2} < \frac{\beta_1}{\beta_1+\beta_4} = \frac{\beta_1}{1-\beta_2-\beta_3}$$
$$1-\frac{\beta_4}{\alpha_2+\alpha_3+\alpha_4-\beta_3} > 1-\frac{\beta_4}{\alpha_3+\alpha_4}$$

and

$$\frac{\beta_1-\alpha_1}{\alpha_2+\alpha_3-\beta_2-\beta_3} \geq \frac{\beta_1-\alpha_1}{\alpha_2-\beta_2}.$$

This indicates that there are six useless terms in (17), so we can omit them. Now we get

$$\max\left\{\frac{\alpha_1+\alpha_2-\beta_1}{\beta_2+\beta_3}, 1-\frac{\alpha_4-\beta_4}{\beta_3-\alpha_3}\right\} \leq c \leq \min\left\{\frac{\beta_1}{\alpha_1+\alpha_2}, \frac{\beta_1-\alpha_1}{\alpha_2-\beta_2}, 1-\frac{\beta_4}{\alpha_3+\alpha_4}\right\}.$$

Therefore, (4) is a necessary condition for the existence of catalysts.

On the other hand, we claim that (1) and (4) are the sufficient conditions. Indeed, if we choose a c which satisfies (1), then c satisfies (17) and (18). From (9)–(16) we know that

$$\sum_{i=1}^{k} a^{(i)} \leq \sum_{i=1}^{k} b^{(i)}$$

i.e., $|\psi_1\rangle|\phi\rangle \rightarrow |\psi_2\rangle|\phi\rangle$ under LOCC. This completes the proof. □

ACKNOWLEDGMENT

The authors are very grateful to the anonymous referees for their invaluable comments and suggestions that helped to improve the presentation in this paper.

REFERENCES

[1] C. H. Bennett, G. Brassard, C. Crepeau, R. Josza, A. Peres, and W. K. Wooters, "Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels," *Phys. Rev. Lett.*, vol. 70, pp. 1895–1899, Mar. 1993.

[2] C. H. Bennett and S. J. Wiesner, "Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states," *Phys. Rev. Lett.*, vol. 69, pp. 2881–2884, Nov. 1992.

[3] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in *Proc. IEEE Int. Conf. Computers, Systems, and Signal Processing*, New York, 1984, pp. 175–179.

[4] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*. Cambridge, U.K.: Cambridge Univ. Press, 2000.

[5] C. H. Bennett, H. J. Bernstein, S. Popescu, and B. Schumacher, "Concentrating partial entanglement by local operations," *Phys.Rev. A*, vol. 53, pp. 2046–2052, Apr. 1996.

[6] M. A. Nielsen, "Conditions for a class of entanglement transformations," *Phys. Rev. Lett.*, vol. 83, pp. 436–439, Jul. 1999.

[7] A. W. Marshall and I. Olkin, *Inequalities: Theory of Majorization and Its Applications*. New York: Academic, 1979.

[8] P. Alberti and A. Uhlmann, *Stochasticity and Partial Order: Doubly Stochastic Maps and Unitary Mixing*. Berlin, Germany: VEB Deutcher Verlag, 1982.

[9] D. Jonathan and M. B. Plenio, "Entanglement-assisted local manipulation of pure quantum states," *Phys. Rev. Lett.*, vol. 83, pp. 3566–3569, Oct. 1999.

[10] S. Bandyopadhyay and V. Roychowdhury, "Efficient entanglement-assisted transformation for bipartite pure states," *Phys. Rev. A*, vol. 65, no. 4, Apr. 2002.