The Existence of Quantum Entanglement Catalysts*

Xiaoming Sun† Runyao Duan‡ Mingsheng Ying§

State Key Laboratory of Intelligent Technology and Systems,
Department of Computer Science and Technology, Tsinghua Univ., Beijing, 100084, China.

Abstract

A direct transformation between two quantum states through local quantum operations and classical communication is often impossible. Jonathan and Plenio [Phys. Rev. Lett. 86, 3566(1999)] presented an interesting example showing that the presence of another state, called a catalyst, can make such a transformation becoming possible. They also pointed out that in general it is very hard to find an analytical condition when a catalyst exists. We study the existence of catalysts for two incomparable quantum states. For the simplest case of 2×2 catalysts for transformations between 4×4 states, a necessary and sufficient condition for existence is found. For 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 — Quantum information, entanglement states, entanglement transformation, entanglement catalysts.

1 Introduction

Entanglement is a fundamental quantum mechanical device shared among spatially separated parties. It is unique in quantum mechanics, not existing in classical mechanics, and it plays a central role in some striking applications of quantum computation and quantum information such as quantum teleportation [1], quantum superdense coding [2], quantum cryptography [3]. More and more researchers have come to realize that quantum entanglement, in fact, is a kind of useful physical resource [4]. On the other hand, many fundamental problems concerning quantum entanglement are still to be solved. A simple but very important one among them is related to entanglement transformation. Suppose that Alice and Bob share a bi-partite state. The question is then what kind of state can they transform the entangled state into. Since an entangled state is separated

*This work was partly supported by the National Foundation of Natural Sciences of China (Grant No: 60223004 and 60273003).

†Email: sun_xm97@mails.tsinghua.edu.cn
‡Email: dry02@mails.tsinghua.edu.cn
§Email: yingmsh@mail.tsinghua.edu.cn

spatially, it is naturally to require that any entanglement transformation must be carried out with the constraint that the entangled two parts can only do local operations on their own subsystems respectively and only classical communication is permitted (for simplicity, in the sequel we will use LOCC to stand for *local operations and classical communication*). A significant progress in the study of entanglement was made by Bennett, Bernstein, Popescu and Schumacher [5] in 1996. They proposed an entanglement concentration protocol and solved the entanglement transformation problem in asymptotic case. In 1999, Nielsen [6] made another important advance step for the deterministic case. Suppose there is a bi-partite state $|\psi_1\rangle = \sum_{i=1}^{n} \sqrt{\alpha_i}|i\rangle_A|i\rangle_B$ 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 bi-partite 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 eigenvalue vectors of ψ_1 and ψ_2, respectively, 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 a extremely useful mathematical too for studying entanglement transformation. A simple but significant fact implied by Nielsen's theorem is that there exists incomparable states $|\psi_2\rangle$ and $\psi_1\rangle$ with both $|\psi_1\rangle \rightarrow |\psi_2\rangle$ 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 $|\psi\rangle \rightarrow |\phi\rangle$ becoming possible, and in the catalyzed transformation $|\psi\rangle \otimes |c\rangle \rightarrow |\phi\rangle \otimes |c\rangle$ the catalyst $|c\rangle$ needs not be consumed at all.

It is certain that entanglement catalysis are another useful resource that quantum mechanics provides. This highly suggests us to exploit its full power in quantum information processing. To this end, we first have to solve the following basic problem: given a pair of incomparable states $|\psi_2\rangle$ and $\psi_1\rangle$ with $|\psi_1\rangle \not\rightarrow |\psi_2\rangle$ and $|\psi_2\rangle \not\rightarrow |\psi_1\rangle$, how to determine whether there exists a catalyst for them? According to Nielsen's theorem, it requires us to decide when the majorization relation $\lambda_{\psi_1 \otimes c} \prec \lambda_{\psi_2 \otimes c}$ for a entangled state $|c\rangle$. 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 difficult 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 a catalysts, but no sufficient condition was found. Those necessary conditions enable them to assert that entanglement catalysis can only happen in the transformation between two $n \times n$ states with $n \geq 4$. One of the main aims of the present paper is then to give a necessary and sufficient condition for entanglement catalysis in the simplest case of entanglement transformation between 4×4 states with a 2×2 catalyst. For general case, the fact that an analytical condition under which incomparable states are catalyzable is not easy to find leads us naturally to 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 was already presented by Bandyopadhyay and Roychowdhury [10]. Unfortunately, for two $n\times n$ incomparable states, to determine whether there exists a $k\times k$ catalyst for them, their algorithm runs in exponential time with complexity $O([(nk)!]^2)$, and so it is intractable in the practice use. The intractability of Bandyopadhyay and Roychowdhury's algorithm stimulates us to find a more efficient algorithm for the same purpose, and this is exactly the second aim of the present paper.

This paper is organized as follows. The remainder of this introduction is used to fix some notations. In the second section 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 usage of this condition. The third section is devoted to consider 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 $|\psi_1\rangle\rightarrow|\psi_2\rangle$ only using $O(n^{2k})$ steps, where each step can be easily implemented by linear programming. Comparing to the time complexity $O([(nk)!]^2)$ of the algorithm given in [10], the algorithm we presented here is much more efficient. We make conclusions in section 4, and some open problem are also discussed.

To simplify the presentation, in the rest of the paper, an $n\times n$ state $|\psi\rangle=\sum_{i=1}^n\sqrt{\gamma_i}|i\rangle|i\rangle$ is always represented by the probabilistic vector of its Schmidt coefficients, $|\psi\rangle=(\gamma_1,\gamma_2,\ldots,\gamma_n)$.

2 A necessary and sufficient condition of entanglement catalysis in the simplest case $(n = 4, k = 2)$

Jonathan and Plenio [9] showed that entanglement catalysis only occurs in transformations between $n\times n$ states with $n\geq 4$. In this section, we consider the simplest case that a transformation between two 4×4 states possesses a 2×2 catalyst. Assume $|\psi_1\rangle = (\alpha_1,\alpha_2,\alpha_3,\alpha_4)$ and $|\psi_2\rangle=(\beta_1,\beta_2,\beta_3,\beta_4)$, be 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 supposed to be a 2×2 state, and it is denoted by $|\phi\rangle=(c,1-c)$ with $c\in[1/2,1]$.

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

$$\alpha_1\leq\beta_1,\quad \alpha_1+\alpha_2>\beta_1+\beta_2,\quad \alpha_1+\alpha_2+\alpha_3\leq\beta_1+\beta_2+\beta_3, \tag{1}$$

or equivalently,

$$\alpha_2+\alpha_3+\alpha_4\geq\beta_2+\beta_3+\beta_4,\quad \alpha_3+\alpha_4<\beta_3+\beta_4,\quad \alpha_4\geq\beta_4. \tag{2}$$

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

$$\beta_1\geq\alpha_1\geq\alpha_2>\beta_2\geq\beta_3>\alpha_3\geq\alpha_4\geq\beta_4 \tag{3}$$

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

Theorem 2.1 *There exists a catalysts $|\phi\rangle$ for two states $(|\psi_1\rangle, |\psi_2\rangle)$ with $|\psi_1\rangle \not\to |\psi_2\rangle$, if and only if*

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

and Eq. (1) hold. In addition, for any $c \in [1/2, 1]$ 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 $|\psi_1\rangle \not\to |\psi_2\rangle$ but $|\psi_1\rangle|\phi\rangle \to |\psi_2\rangle|\phi\rangle$ under LOCC. From Eq. (8) in [9] we know Eq. (1) holds. So Eq. (2) and Eq. (3) hold too.

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. We sort them in decreasing order and denote the resulted 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 $|\psi_1\rangle|\phi\rangle \to |\psi_2\rangle|\phi\rangle$, Nielsen's theorem tells us that

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

We already know that

$$\beta_1 c \geq \beta_2 c \geq \beta_3 c \geq \beta_4 c, \quad \beta_1(1-c) \geq \beta_2(1-c) \geq \beta_3(1-c) \geq \beta_4(1-c), \quad \beta_i c \geq \beta_i(1-c) \tag{5}$$

Now we are going to demonstrate that

$$\beta_1 c \geq \beta_1(1-c) > \beta_2 c \geq \beta_3 c > \beta_2(1-c) \geq \beta_3(1-c) > \beta_4 c \geq \beta_4(1-c). \tag{6}$$

and consequently fix the ordering of B. The key idea here is that the sum of the biggest l numbers in a set is greater than or equal 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), it follows that $\alpha_1+\alpha_2 > \beta_1+\beta_2$. 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

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

So it holds that

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

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 decide 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,

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

where 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 $\beta_2(1-c)$ leaves, 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.

We now remember that the ordering of B has been found out. This enables us to calculate easily $\sum_{i=1}^{l} b^{(i)}$ for each l. The only rest thing is how to calculate $\sum_{i=1}^{l} a^{(i)}$. To this end, we need the following simple 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: 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): Now the above lemma guarantees that there is a quite easy way to deal with $\sum_{i=1}^{l} a^{(i)}$: 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 now is to solve systematically the inequalities of $\sum_{i=1}^{l} a^{(i)} \leq \sum_{i=1}^{l} b^{(i)}$ $(1 \leq l \leq 8)$. We put this daunting but routine part in the Appendix. $\square$

To illustrate the utility of the above theorem, let us see 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

$$\max\left\{\frac{\alpha_1+\alpha_2-\beta_1}{\beta_2+\beta_3}, 1-\frac{\alpha_4-\beta_4}{\beta_3-\alpha_3}\right\} = \max\{0.6, 1-2/3\} = 0.6,$$

$$\min\left\{\frac{\beta_1}{\alpha_1+\alpha_2}, \frac{\beta_1-\alpha_1}{\alpha_2-\beta_2}, 1-\frac{\beta_4}{\alpha_3+\alpha_4}\right\} = \min\{5/8, 2/3, 1-0\} = 5/8.$$

Since $0.6 < 5/8 = 0.625$, 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 $[0.6, 0.625]$. Especially, 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 $\phi = (0.65, 0.35)$. Note that

$$\max\left\{\frac{\alpha_1+\alpha_2-\beta_1}{\beta_2+\beta_3}, 1-\frac{\alpha_4-\beta_4}{\beta_3-\alpha_3}\right\} = \max\{0.52, 1-10/11\} = 0.52,$$

$$\min\left\{\frac{\beta_1}{\alpha_1+\alpha_2}, \frac{\beta_1-\alpha_1}{\alpha_2-\beta_2}, 1-\frac{\beta_4}{\alpha_3+\alpha_4}\right\} = \min\{25/38, 10/11, 1-0\} = 25/38,$$

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

3 An efficient algorithm for deciding existence of catalysts

In the last section, we was able to 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 the necessary conditions given in [9] and Nielsen's Theorem. However, the same idea does not work when we deal with higher dimensional states, and it seems very hard to find an analytical condition for existence of catalyst in the case of higher dimension. On the other hand, existence of catalysts is a dominant problem in exploiting the power of entanglement catalysis in quantum information processing. Such a dilemma forces us to explore alternatively the possibility of finding an efficient algorithm for deciding existence of catalysts. The main purpose 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 intuition behind our algorithm more clearly, we first cope with 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 $\phi = (x, 1-x)$. 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. We 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

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

Now the difficulty arise from the fact that 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, then we can calculate the elements in A, B and sort them. Thus if we moves x slightly from x_0 to $x_0 + \epsilon$, the order of A (or B) will not change, except 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. Calculate $\{\frac{\alpha_i}{\alpha_i+\alpha_j}, \frac{\beta_i}{\beta_i+\beta_j} : 1 \leq i < j \leq n\}$, and sort them in nondecreasing order. The resulted sequence is denoted by $\gamma^{(1)} \leq \gamma^{(2)} \leq \cdots \leq \gamma^{(n^2-n)}$, and let $\gamma^{(0)} = 1/2, \gamma^{(n^2-n+1)} = 1$).

2. For each interval $[\gamma^{(i)}, \gamma^{(i+1)}]$, select a constant $c \in [\gamma^{(i)}, \gamma^{(i+1)}]$ (for example, $c = \frac{\gamma^{(i)}+\gamma^{(i+1)}}{2}$), determine the order between A_x and B_x, and solve the system of inequalities:

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

Then there exists a catalyst for $|\psi_1\rangle$ and $|\psi_2\rangle$ if and only if there is a $i \in \{0, 1, \ldots, n^2-n\}$, the solution set of the above inequalities is not empty.

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

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 whether there exists a $k \times k$ catalyst $|\phi\rangle = (x_1, \ldots, x_k)$ for them can be decided in polynomial time about n.*

Proof. The idea is similar to the one for the case of 2×2 catalyst. 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 should be $(k-1)-$dimensional because we have a constrain of $\sum_{i=1}^{k} x_i = 1$.) So 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) has the same order. Then we can solve the inequalities

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

and check the order constrains by linear programming. Since linear programming is solvable in polynomial time, our algorithm runs in polynomial time of n too whenever k is a given constant. □

4 Conclusion and discussion

In this paper we consider the problem concerning existence of catalysts for entanglement transformations. It is solved for the simplest case. We give a necessary and sufficient condition for the existence of a 2×2 catalyst for a pair of two incomparable 4×4 states. For the general case of $k \times k$ catalysts for $n \times n$ states, we fail to find an analytical condition for existence of catalysts. An efficient polynomial time algorithm to decide whether a $k \times k$ catalyst exists for two incomparable $n \times n$ states is found when k is seen as a constant. However, problem of finding such an algorithm still remains open if the dimension k of catalyst is allowed to be a variable, ranging over all positive integers.

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 *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing*, pp. 175–179, IEEE, New York, 1984.

[4] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press, Cambridge, 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*, Academic Press, New York, 1979.

[8] P. Alberti and A. Uhlmann, *Stochasticity and Partial Order: Doubly Stochastic Maps and Unitary Mixing*, Dordrecht, Boston, 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(4), Art. No. 042306, Apr. 2002.

5 Appendix: Proof of Theorem 2.1

Proof of Theorem 2.1 (remaining part): We need to solve the system of inequalities $\sum_{i=1}^{l} a^{(i)} \leq \sum_{i=1}^{l} b^{(i)}$ $(1 \leq l \leq 8)$. This is carried out by the following items:

(1) First, we have:

$$a^{(1)} \leq b^{(1)} \iff \alpha_1 c \leq \beta_1 c \iff \alpha_1 \leq \beta_1. \tag{9}$$

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

$$\max\{\alpha_1 c + \alpha_1(1-c), \alpha_1 c + \alpha_2 c\} \leq \beta_1 c + \beta_1(1-c) \iff \tag{10}$$

$$c \leq \frac{\beta_1}{\alpha_1 + \alpha_2}, \quad \alpha_1 \leq \beta_1. \tag{11}$$

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

$$\begin{aligned} \max\{\alpha_1 c + \alpha_1(1-c) + \alpha_2 c, \alpha_1 c + \alpha_2 c + \alpha_3 c\} &\leq \beta_1 c + \beta_1(1-c) + \beta_2 c \iff \\ c &\leq \left\{\frac{\beta_1}{\alpha_1 + \alpha_2 + \alpha_3 - \beta_2}, \frac{\beta_1 - \alpha_1}{\alpha_2 - \beta_2}\right\} \end{aligned} \tag{12}$$

(4) It holds that

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

(5)

$$\begin{aligned} a^{(1)} + a^{(2)} + a^{(3)} + a^{(4)} + a^{(5)} \leq b^{(1)} + b^{(2)} + b^{(3)} + b^{(4)} + b^{(5)} &\iff \\ a^{(6)} + a^{(7)} + a^{(8)} \geq b^{(6)} + b^{(7)} + b^{(8)} &\iff \\ \min\{\alpha_2(1-c) + \alpha_3(1-c) + \alpha_4(1-c), \alpha_3(1-c) + \alpha_4 c + \alpha_4(1-c)\} & \\ \geq \beta_3(1-c) + \beta_4 c + \beta_4(1-c) &\iff \\ 1 - \frac{\alpha_4 - \beta_4}{\beta_3 - \alpha_3} \leq c \leq 1 - \frac{\beta_4}{\alpha_2 + \alpha_3 + \alpha_4 - \beta_3} & \end{aligned} \tag{14}$$

(6)

$$\begin{aligned} \textstyle\sum_{i=1}^{6} a^{(i)} \leq \sum_{i=1}^{6} b^{(i)} &\iff \\ a^{(7)} + a^{(8)} \geq b^{(7)} + b^{(8)} &\iff \\ \min\{\alpha_3(1-c) + \alpha_4(1-c), \alpha_4 c + \alpha_4(1-c)\} \geq \beta_4 c + \beta_4(1-c) &\iff \\ c \leq 1 - \tfrac{\beta_4}{\alpha_3 + \alpha_4}, \quad \alpha_4 \geq \beta_4 & \end{aligned} \tag{15}$$

(7) We have

$$\sum_{i=1}^{7} a^{(i)} \leq \sum_{i=1}^{7} b^{(i)} \iff a^{(8)} \geq b^{(8)} \iff \alpha_4 \geq \beta_4 \tag{16}$$

Combining Eq. (7, 9-16) we obtain

$$\begin{aligned} c \leq \Bigg\{ & \frac{\beta_1}{\beta_1 + \beta_2}, \frac{\beta_3}{\beta_3 + \beta_4}; \frac{\beta_1}{\alpha_1 + \alpha_2}, \frac{\beta_1}{\alpha_1 + \alpha_2 + \alpha_3 - \beta_2}, \frac{\beta_1 - \alpha_1}{\alpha_2 - \beta_2}, \frac{\beta_1}{1 - \beta_2 - \beta_3}, \\ & \frac{\beta_1 - \alpha_1}{\alpha_2 + \alpha_3 - \beta_2 - \beta_3}^{1}, 1 - \frac{\beta_4}{\alpha_2 + \alpha_3 + \alpha_4 - \beta_3}, 1 - \frac{\beta_4}{\alpha_3 + \alpha_4} \Bigg\} \end{aligned} \tag{17}$$

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

and

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

Since

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

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 Eq. (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, Eq. (4) is a necessary condition for the existence of catalyst.

On the other hand, we claim that Eq. (1) and Eq. (4) are the sufficient conditions. Indeed, if we choose a c satisfies Eq. (2.1), then c satisfies Eq. (17) and (18). From Eq. (9-16) we know that $\sum_{i=1}^{k} a^{(i)} \leq \sum_{i=1}^{k} b^{(i)}$, i.e. $|\psi_1\rangle|\phi\rangle \to |\psi_2\rangle|\phi\rangle$ under LOCC. This completes the proof. □