Sept. 2006, Vol.21, No.5, pp.776–789 *J. Comput. Sci. & Technol.*

Some Issues in Quantum Information Theory

Run-Yao Duan (段润尧), Zheng-Feng Ji (季铮锋), Yuan Feng (冯　元), and Ming-Sheng Ying (应明生)

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

E-mail: {dry02, jizhengfeng98}@mails.tsinghua.edu.cn; {feng-y, yingmsh}@mail.tsinghua.edu.cn

Received March 31, 2006; revised June 13, 2006.

Abstract Quantum information theory is a new interdisciplinary research field related to quantum mechanics, computer science, information theory, and applied mathematics. It provides completely new paradigms to do information processing tasks by employing the principles of quantum mechanics. In this review, we first survey some of the significant advances in quantum information theory in the last twenty years. We then focus mainly on two special subjects: discrimination of quantum objects and transformations between entanglements. More specifically, we first discuss discrimination of quantum states and quantum apparatus in both global and local settings. Secondly, we present systematical characterizations and equivalence relations of several interesting entanglement transformation phenomena, namely entanglement catalysis, multiple-copy entanglement transformation, and partial entanglement recovery.

Keywords discrimination, entanglement transformation, quantum computing, quantum information

1 Introduction

In 1982, when Elk Cloner—the first known computer virus that has been spread "in the wild"—was slowly copying itself from floppy to floppy, physicists announced confidently that quantum information *cannot* be cloned[1,2]. Again in 1982, Feynman noticed that simulation of general quantum systems might be computationally expensive on traditional computing machines and proposed the original idea of simulating quantum systems using quantum computers[3]. From then on, information science, benefited from its successful marriage with quantum physics, embraces an extraordinary new era of ongoing development. Numerous amazing discoveries exploiting the power of quantum mechanics not only contribute to the field of quantum information processing itself, but also impact the classical areas like computation, communication and cryptography by causing rethinking of fundamental problems in these areas—"What is computation?" "How powerful is it?" and "Is information physical?"

To tackle the problems listed above in the quantum context, exciting progress has been made constantly in quantum information theory. However, as it is nowadays impossible to have a comprehensive review of all these great achievements in such a short article, we will only introduce some of the most important ideas and will focus on the results that the authors are more familiar with. To get a more complete picture of quantum computation and quantum information, the readers are referred to [4–6].

Feynman's observation[3] inspired the inquiry of the computational power of quantum mechanics. Many different models of quantum computation are hence proposed. In 1985, Deutsch reexamined the Church–Turing thesis and argued that there is a physical assertion underlying it[7]. He then rigorously formalized quantum Turing machine model (QTM)[7], the counterpart of the classical Turing machine[8], and introduced in 1989 the quantum circuit model in terms of quantum networks[9]. Yao proved that any function that is polynomial-time computable by a QTM has a polynomial-size quantum circuit[10]. This alleviates the burden of dealing with abstract QTMs. Highly related to the circuit model is the one-way quantum computation model proposed by Raussendorf and Briegel[11,12]. It encodes a quantum circuit as simple measurements performed on a so called cluster state[13] which has possible advantage in physical realization[14]. Recently, adiabatic quantum computation model, proposed by Farhi *et al.*[15], is shown to be equivalent to the standard quantum computation model[16]. The strength of adiabatic model—its unified methods in both designing and analyzing algorithms—makes it a more promising new model of quantum computation. Quantum systems are especially susceptible; therefore it is also necessary to consider models that take the effect of noise into account. The first quantum error correction code[17] designed by Shor stimulates a whole theory of how to fight against quantum noises[18–21].

At the same time of developing quantum computation models, many fancy quantum algorithms are also found. It is Deutsch who devised the first quantum algorithm[7] which is generalized later and is now known as the Deutsch–Jozsa algorithm[22]. Though the problem it solves is a little bit artificial, the algorithm sheds light on the principles of quantum algorithms. Evidences of the quantum advantage of computation are further shown by Bernstein, Vazirani[23] and Simon[24] in an oracle model. In 1994, the first "killer application", Shor's algorithm, eventually emerged: Shor re-

Regular Paper

This work was partly supported by the National Natural Science Foundation of China (Grant Nos. 60503001, 60321002, 60305005, and 60496321), and by Tsinghua Basic Research Foundation (Grant No. 052220204). The first author was partly supported by Tsinghua University (Grant No. 052420003).

ported his ingenious way of efficiently factoring large numbers using a quantum computer[25]. Although quantum computers cannot be built today, this algorithm theoretically threats the RSA public cryptosystem[26] and popularizes the area of quantum computation and quantum information largely. Another important quantum algorithm, Grover's algorithm[27,28], uses the quantum tricks to quadratically speed up the searching of a specific datum out of an unsorted database. It is also found that Grover's construction is optimal[29] and many generalizations are made to investigate the power of quantum computation in the oracle model[30−33]. Recent development of quantum algorithm includes the introduction and applications of quantum walks[34−36], and algorithms for "Hidden Subgroup Problem" (see, for example, [37]).

Quantum algorithms, though superior to their classical counterparts in many ways, are infamous for their counter-intuitive nature. It is thus quite necessary to develop systematic methodologies that can accelerate the development of quantum algorithms. One attempt, motivated by the success of classical programming languages in developing classical programs, is to develop and study quantum programming languages. Knill moved the first step by outlining a set of basic principles for writing quantum pseudo-code[38]; while the first actual quantum programming language is due to Ömer[39]. Sanders and Zuliani extended the probabilistic version of Dijkstra's guarded command language (pGCL) to include quantum primitives[40]. The most distinguishing feature of their language is the support for stepwise refinement which can be used in program derivation and program verification. Recently, Bettelli *et al.* presented a quantum language extending the well-known language C++[41] and the first functional quantum programming language, which admits a denotational semantics assigning a super-operator to each quantum program fragment, was later proposed by Selinger[42].

It is worth noting that the notion of "Quantum Software Engineering" has already been proposed in the UK Grand Challenge Proposal, *Journeys in Non-Classical Computation*[43,44]. It is conducted by the UK Computing Research Committee (UKCRC) with the hope to seek "long-term, large-scale international research project with clearly defined deliverables, mile-stones, and plans for development, evaluation, and validation of its research results".

From the perspective of information theory[45], the source and channel coding theorems have been generalized to their quantum counterparts[46−48] although it still remains open whether entangled input can further increase the classical capacity of a quantum channel. For a detailed discussion on this topic, we refer to a survey article[49].

What is more interesting in quantum information theory is that it encounters many issues different from their classical counterparts. The non-cloning theorem[1,2], for example, says that we cannot create an identical copy of an arbitrary unknown quantum state with certainty though we are used to copy and backup data on classical computers. The theorem has profound implications in quantum information theory. Namely, it invalidates the classical way of doing quantum error correction, breaks the semantics of assignment in programming languages, and makes it impossible to backup quantum data. On the other hand, however, the theorem insures the security of some quantum cryptography protocols against eavesdropping[50], protects the uncertainty principle, and more surprisingly, prevents superluminal communication. There are in fact a series of "no-go" theorems in the same spirit of non-cloning: non-discrimination theorem[51], non-deleting theorem[52], and non-programmable theorem[53]. Although we cannot clone, discriminate or delete perfectly, it is still possible to perform these tasks in an imperfect approach[54,55] and we will discuss these problems in detail below.

Another specific topic lying at the heart of quantum information is the study of quantum entanglement. Entanglement is a quantum state of multiple particles among which there are strong, non-classical, correlations. The discussions of entanglement date as far back as the early days when quantum mechanics itself is in its infancy. In 1935, Einstein, Podolsky, and Rosen pointed out the weirdness of entanglement and argued that the quantum theory is incomplete[56]. However, researchers are now focusing on how to harness the weirdness to assist information processing. In 1992, Bennett and Wiesner discovered that entanglement can assist a noiseless quantum channel by doubling its classical capacity[57]. The protocol they proposed is now referred to as superdense coding. A year later, there came forth the famous quantum teleportation protocol[58] that can transfer quantum state between any two parties with the cost of consuming a shared entangled state and transmission of some classical information. Teleportation, formerly the imagination of science fiction writers, has now been realized by experimentalists[59].

Superdense coding and teleportation have stimulated broad interests of understanding the nature of quantum entanglement. It is nowadays widely accepted that entanglement is a new type of physical resource, like energy, which is indispensable in many information processing procedures. Therefore, a lot of effort has been made trying to measure[60], transform[61], and purify[62,63] the new resource. The structure and properties of pure (noiseless), bipartite (shared between two parties) entanglement are best understood while the characters of both the mixed (noisy) entanglement and multipartite entanglement are much lesser known. We will present detailed results in the context of transformation of pure entanglement later.

Before finishing this brief introduction to quantum computation and quantum information, we would like to mention some more interesting issues that have not been referred to so far: quantum cryptography (more

precisely, quantum key distribution[50,64,65]), the quantum version of communication complexity[10,66], quantum game theory[67,68], logical approach to quantum computation[69], and probably more that the authors have neglected.

The rest of the paper is organized as follows. In Section 2, the problem of discriminating pure states is first discussed. Next, we analyze more general problems where mixed states are under consideration. Section 3 devotes to the topics of discriminating operations, including unitary evolutions, measurement apparatus and general quantum operations. In the last part of the paper, we present, in order, numerous results concerning local manipulation of entanglements: local transformation of entanglement, entanglement catalysts, multiple-copy transformation, and partial recovery of entanglement.

2 Discrimination Between Quantum States

The general state discrimination problem is as follows: suppose a quantum system is prepared secretly in one of a set of states, and we hope to determine what quantum state the system is actually in. Precise quantum discrimination among any state set is forbidden by the laws of quantum mechanics. It is easy to prove that only orthogonal states can be perfectly discriminated. For discrimination among nonorthogonal state, there are two strategies we can use. The first strategy is the so-called "quantum hypothesis testing". The goal of discrimination under this strategy is to guess, with the minimum probability of error, which state the system is in depending on the outcome of some measurement applied on the target state. The second strategy is unambiguous discrimination, in which one must identify the state with certainty, but leaving a possibility of undecidability. Our aim then is to minimize the probability of inconclusive answer. In this section, we restrict our attention only on unambiguous discrimination between pure or mixed states.

It is worth noting that the particular one we actually adopt in reality depends upon the type of information about the state we wish to obtain, and also on the prior information we have about the system.

2.1 Pure State Case

Suppose the quantum system we are concerned with is prepared in one of the n states $|\psi_1\rangle, |\psi_2\rangle, \ldots, |\psi_n\rangle$ in a d-dimensional Hilbert space with probabilities $p_1, p_2, \ldots, p_n$ respectively, where $d \geqslant n$. What we wish to do is to identify which state the system is prepared in with no errors. The most general unambiguous discrimination strategy is carried by constructing a positive operator-valued measurement, or POVM for short, $\{\Pi_j, j = 0, 1, \ldots, n\}$, such that $\sum_{j=0}^{n} \Pi_j = I$ and

$$\langle\psi_i|\Pi_j|\psi_i\rangle = P_j\delta_{i,j} \tag{1}$$

for any $i, j > 0$. The requirement in (1) ensures that if the outcome of the measurement is j, we can definitely say that the system is in the state $|\psi_j\rangle$. Here P_j is the success probability of $|\psi_j\rangle$ being identified. The optimal unambiguous discrimination is then the one which maximize the success discrimination probability

$$P_{suc} = \sum_{i=1}^{n} p_i P_i. \tag{2}$$

For the simplest case of discriminating two states $|\psi_1\rangle, |\psi_2\rangle$ with equal *a priori* probabilities, it was established by Ivanovic[70], Dieks[71], and Peres[51] that the optimal success probability reads $1 - |\langle\psi_1|\psi_2\rangle|$. Jaeger and Shimony[54] further extended the result to the case of unequal priori probabilities p_1 and p_2 with $p_1 \leqslant p_2$, and get the result as

$$P_{suc}^{opt} = \begin{cases} 1 - 2\sqrt{p_1 p_2}|\langle\psi_1|\psi_2\rangle|, & |\langle\psi_1|\psi_2\rangle| < \sqrt{\dfrac{p_1}{p_2}}, \\ p_2(1 - |\langle\psi_1|\psi_2\rangle|^2), & \text{otherwise.} \end{cases} \tag{3}$$

This result is also discussed by Ban in [72] in the context of quantum communications.

In the case of discriminating between more than two states, Chefles[73] first find that such an unambiguous strategy can exist if and only if the states $|\psi_1\rangle, |\psi_2\rangle, \ldots, |\psi_n\rangle$ are linearly independent. Furthermore, when the independency requirement is satisfied, the form of the POVM satisfying (1) can be restated by

$$\Pi_j = \frac{P_i}{|\langle\psi_j^{\perp}|\psi_j\rangle|^2}|\psi_j^{\perp}\rangle\langle\psi_j^{\perp}| \tag{4}$$

for $1 \leqslant j \leqslant n$, and $\Pi_0 = I - \sum_{j=1}^{n} \Pi_j$, where the normalized state $|\psi_j^{\perp}\rangle$ is defined as that which is orthogonal to all $|\psi_i\rangle$ for $i \neq j$.

When we try to decide the optimal unambiguous discrimination between n quantum states for $n > 2$, things become more complicated. In fact, we can easily transform the optimal unambiguous discrimination problem to the problem of solving the following semi-definite programming[74]

$$\begin{aligned} \text{Maximize} \quad & \sum_{i=1}^{n} p_i P_i \\ \text{subject to} \quad & \boldsymbol{X} - \Gamma \geqslant 0, \quad \Gamma \geqslant 0 \end{aligned} \tag{5}$$

where $\boldsymbol{X} = [\langle\psi_i|\psi_j\rangle]_{n\times n}$ is the matrix with the (i, j)-th entry being $\langle\psi_i|\psi_j\rangle$ and $\Gamma = \mathrm{diag}(P_1, P_2, \ldots, P_n)$. Unfortunately, semi-definite programming problems are mathematically very hard to find analytic solutions, and only numerical methods are known up to now[75].

Although the *explicit expression* of optimal success probability for unambiguous discrimination among n *general* quantum states are hard or, be more pessimistic, impossible to obtain, we can simplify the most general problem to consider two easier questions instead. One

question is, for some *special* quantum states and priori probabilities, how to derive the optimal discrimination strategies. Chefles and Barnett[76] considered the case of n symmetric independent quantum states with equal *a priori* probabilities and obtained the maximum probability to unambiguously discriminate them. A set of states is symmetric if there exists a unitary operator U such that $U^n = I$ and

$$|\psi_i\rangle = U|\psi_{i-1}\rangle = U^{i-1}|\psi_1\rangle. \tag{6}$$

The other question is that we can derive upper bounds on the optimal success probability of discrimination. By using a series of proper inequalities, Zhang *et al.*[77] derived an upper bound on success probability of unambiguous discrimination as follows

$$P_{suc} \leqslant 1 - \frac{1}{n-1}\sum_{i\neq j}\sqrt{p_i p_j}|\langle\psi_i|\psi_j\rangle|. \tag{7}$$

The above bound was further improved by Feng *et al.*[78] to

$$P_{suc} \leqslant \sqrt{\frac{n}{n-1}\sum_{i\neq j} p_i p_j |\langle\psi_i|\psi_j\rangle|^2}. \tag{8}$$

Suppose the unknown state to be discriminated is shared by spatially separated parties, and the operations allowed are restricted to local operation and classical communication (LOCC). It is obvious that this restriction limits the ability to discriminate between quantum states. Indeed, there exist a set of globally distinguishable product states that cannot be identified locally[79].

Surprisingly, however, for the special case of discriminating between two pure state, it seems that LOCC is strong enough to perform optimal discrimination. Walgate *et al.*[80] first proved that any two orthogonal multipartite states, entangled or not, can be distinguished perfectly using only LOCC. Later, Virmani *et al.* proved in [81] that the minimum probability of error can be achieved by LOCC discrimination in the setting of quantum hypothesis testing. For unambiguous discrimination, Chen *et al.*[82,83] and Ji *et al.*[84] considered the problem of unambiguous discrimination between any two *product* pure states with arbitrary a priori probability, any two pure states with *equal* prior probability, and any two pure states with *arbitrary* prior probability, respectively. It was shown that in all these cases, a local operation and classical communication protocol exists that achieves the optimal success probability of global unambiguous discrimination.

2.2 Mixed State Case

Unambiguous discrimination among pure states has attracted considerable research efforts for a long time. Somewhat surprisingly, it is only recently that the problem of unambiguous discrimination between mixed states is considered.

The aim of mixed state discrimination is to identify a quantum system which is prepared secretly in the states $\rho_1, \rho_2, \ldots, \rho_n$ with probabilities $p_1, p_2, \ldots, p_n$ respectively. The POVM $\{\Pi_j\}$ which can be used to unambiguously discriminate among these states then must satisfy the following condition:

$$\mathrm{tr}(\Pi_j \rho_i) = P_j \delta_{i,j}, \tag{9}$$

for any $i, j > 0$. Rudolph *et al.*[85] first considered the special case of discriminating between two mixed states with the kernels both being one-dimensional. Denoting by $|k_i\rangle\langle k_i|$ the projector onto the kernel of ρ_i, $A_1 = p_1\langle k_2|\rho_1|k_2\rangle$, and $A_2 = p_2\langle k_1|\rho_2|k_1\rangle$, the optimal success probability P_{suc}^{opt} is then given by

$$\begin{cases} \dfrac{A_1 + A_2 - 2\cos\theta\sqrt{A_1 A_2}}{\sin^2\theta}, & \text{if } \cos\theta < \sqrt{\dfrac{A_{\min}}{A_{\max}}}, \\ A_{\max}, & \text{otherwise,} \end{cases} \tag{10}$$

where θ is the angle between the kernels, i.e.,

$$\cos\theta = |\langle k_1|k_2\rangle|, \tag{11}$$

$A_{\min} = \min\{A_1, A_2\}$, $A_{\max} = \max\{A_1, A_2\}$. This extended the result of Jaeger and Shimony[54] for two pure states. They also derived a lower bound and an upper bound on the maximal probability of successful discrimination of two mixed states.

Raynal *et al.*[86] presented two reduction theorems to reduce the optimal unambiguous discrimination of two mixed states to that of other two mixed states which have the same rank. For the general case of n mixed state discrimination, Fiurasek and Jezek[87] and Eldar[88] gave some sufficient and necessary conditions on the optimal unambiguous discrimination and some numerical methods were discussed. We found in [89] (see also [90]) that the mixed quantum states $\rho_1, \ldots, \rho_n$ can be perfectly discriminated if and only if they are orthogonal, that is, for any $i, j = 1, \ldots, n$,

$$\rho_i \rho_j = \delta_{ij}\rho_i^2 \tag{12}$$

while they can be unambiguously discriminated if and only if for any $i = 1, \ldots, n$,

$$\mathrm{supp}(\rho_i) \not\subseteq \sum_{j\neq i}\mathrm{supp}(\rho_j). \tag{13}$$

Here $\mathrm{supp}(\rho)$ denotes the support space of ρ, i.e., the space spanned by the eigenvectors with nonzero eigenvalues. Furthermore, an upper bound on success probability of unambiguous discrimination which extends the result in (8) can be derived:

$$P_{suc} \leqslant \sqrt{\frac{n}{n-1}\sum_{i\neq j} p_i p_j F(\rho_i, \rho_j)^2} \tag{14}$$

where $F(\rho_i, \rho_j)$ is the fidelity of ρ_i and ρ_j.

For the case of discriminating between multipartite mixed states, it was found by Chefles[91] that N-particle

states $\rho_1, \ldots, \rho_n$ can be LOCC discriminated if and only if for any $i = 1, \ldots, n$, there exists an N-particle product state $|\psi_1\rangle \otimes \cdots \otimes |\psi_N\rangle$ such that

$$|\psi_1\rangle \otimes \cdots \otimes |\psi_N\rangle \in \Big(\sum_{j\neq i} \mathrm{supp}(\rho_j)\Big)^{\perp} - \mathrm{supp}(\rho_i)^{\perp} \quad (15)$$

where the notation $S^{\perp}$ represents the orthogonal complement of S.

3 Discrimination Between Quantum Operations

We considered unambiguous discrimination between quantum states in the last section. In this section, let us turn to examine the problem of unambiguous discrimination between quantum operations. Suppose we are given a quantum mechanical black box that performs one of the operations $\mathcal{E}_1, \ldots, \mathcal{E}_n$, how can we identify which one it really performs? A natural idea is to input a probe state to the black box and then discriminate between the possible outputs. Then the results obtained in the last section can be used to derive the ability of discriminating quantum operations. Indeed, we found many similarities between discriminating quantum states and quantum operations. There are, however, also many distinctions, especially when multiple copies of the states are provided or multiple uses of the operations are allowed.

3.1 Discriminating Unitary Operations

The simplest quantum operations are unitary operations which preserve the inner product of any two states. Recall that perfect discrimination is impossible for nonorthogonal states unless the number of copies of the unknown states goes infinite. To one's surprise, it is always possible to completely tell apart different unitary operations by only finite number of uses of the unknown devices[92,93]. To be specific, given any finite set of unitary operations, $U_1, \ldots, U_n$, there always exists a finite number N such that $U_1^{\otimes N}, \ldots, U_n^{\otimes N}$ are perfectly distinguishable, although they were not in the single-copy case.

It is worth noting that in the protocol of discriminating unitary operations in [92] and [93], a suitable entangled state is used as input. As we know, creation of entanglement needs to perform joint quantum operations on composite systems, which are generally difficult and expensive. So a natural question arises here is: Can we achieve the task without use of entanglement? Duan *et al.*[94] gave the question a positive answer by allowing the ability to perform any known unitary operations and projective measurements on single quantum systems. To be specific, suppose we are given an unknown quantum black box which can perform unitary operations U or V. To determine which case it really is, we first apply this box to a state prepared in state $|\psi\rangle$. If the possible resulting states $U|\psi\rangle$ and $V|\psi\rangle$ are orthogonal, then a perfect discrimination is achieved and the task is complete. Otherwise we apply a known unitary operation, say X_1, on the resulting state and then apply the unknown box once more. Then the orthogonality of the new possible resulting states is tested. It was proven in [94] that there always exist a finite N, a sequence of unitary operations $X_1, \ldots, X_{N-1}$, and a suitable input state $|\psi\rangle$ such that the final states $UX_{N-1}U \ldots X_1U|\psi\rangle$ and $VX_{N-1}V \cdots X_1V|\psi\rangle$ are orthogonal. Such a discrimination strategy is illustrated in Fig.1.

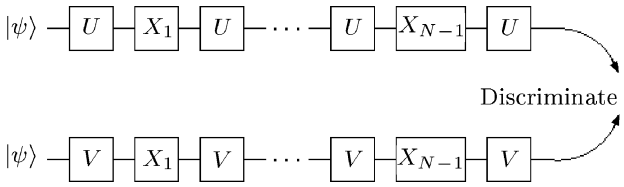

Fig.1. Discriminating two unitary operations without use of entanglement.

A more delicate analysis shows that the number N of uses of the unknown box is not more than that in the protocol where entanglement is used.

In the same paper, the authors also considered the problem of discrimination between nonlocal unitary operations in LOCC setting. Surprisingly, for almost all unitary operations perfect discriminations can always be achieved if multiple use is allowed. To be specific, let U and V be two multipartite unitary operations such that $U^{\dagger}V$ is not Hermitian. Then there exists a finite integer N such that $U^{\otimes N}$ and $V^{\otimes N}$ are perfectly distinguishable using only LOCC. In the special case where U and V act on the composite Hilbert space $\mathcal{H}_2 \otimes \mathcal{H}_n$ for any $n \geqslant 2$ or $\mathcal{H}_3 \otimes \mathcal{H}_3$, U and V can always be perfectly LOCC discriminated when multiple use is allowed.

3.2 Discriminating Projective Measurements

If the quantum mechanics black box we want to identify is actually an unknown measurement device, a more direct strategy without resorting to state discrimination can be used to realize the discrimination task[95]. The idea can be best illustrated by the following examples. Suppose the projective measurements to be discriminated are presented by observables $\boldsymbol{\sigma}_z$ and $\boldsymbol{\sigma}_x$, where

$$\boldsymbol{\sigma}_z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \text{ and } \boldsymbol{\sigma}_x = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}. \quad (16)$$

To achieve this task, we prepare first an entangled state $(|00\rangle - |11\rangle)/\sqrt{2}$ and then measure both qubits with the unknown apparatus. It is easy to see that if the two results coincide, the apparatus is $\boldsymbol{\sigma}_z$, otherwise $\boldsymbol{\sigma}_x$. A more complicated example needs the help of other unitary operations. Let $M = \sum_{i=1}^{3} |i\rangle\langle i|$ and $N = \sum_{i=1}^{3} |\psi_i\rangle\langle\psi_i|$ be two projective measurements

where

$$|\psi_1\rangle = \frac{|1\rangle - 2|2\rangle + |3\rangle}{\sqrt{6}},\ |\psi_2\rangle = \frac{|1\rangle + |2\rangle + |3\rangle}{\sqrt{3}}, \quad (17)$$

and

$$|\psi_3\rangle = \frac{|1\rangle - |3\rangle}{\sqrt{2}}. \quad (18)$$

To discriminate between M and N, we prepare a maximal entangled state $(|11\rangle + |22\rangle + |33\rangle)/\sqrt{3}$ and measure the first qutrit. If the outcome is 1, then the state of the second qutrit is now either $|1\rangle$ or $|\psi_1\rangle$ depending on the unknown apparatus. Apply to it a unitary operation which keeps $|1\rangle$ unchanged and rotates $|\psi_1\rangle$ to a state orthogonal to itself. Such a unitary can be

$$\boldsymbol{U}_1 = \frac{1}{5}\begin{bmatrix} 5 & 0 & 0 \\ 0 & -1 & \sqrt{24} \\ 0 & -\sqrt{24} & -1 \end{bmatrix}. \quad (19)$$

If the second measurement still outputs 1, the unknown device is definitely M else it is N. The case when the first outcome is other than 1 can be solved similarly by choosing proper $\boldsymbol{U}_2$ or $\boldsymbol{U}_3$. Such a discrimination strategy, called M-U-M scheme, is illustrated in Fig.2.

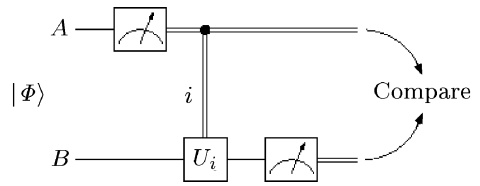

Fig.2. Illustration of the M-U-M scheme.

By using this strategy, the authors[95] proved that all projective measurements can be perfectly discriminated provided that multiple use is allowed. The optimal protocol for discriminating qubit observables was also proposed.

3.3 Discriminating General Quantum Operations

Now we turn to the discrimination between general quantum operations $\mathcal{E}_1, \ldots, \mathcal{E}_n$. Recall that for any trace-preserving quantum operation $\mathcal{E}$, there exist some set of matrices, called Kraus operators, $\{E_i, i = 1, \ldots, d\}$ with $\sum_i E_i^\dagger E_i = I$, such that

$$\mathcal{E}(\rho) = \sum_{i=1}^{d} E_i \rho E_i^\dagger. \quad (20)$$

It was proved by Wang and Ying[96] that the operations $\mathcal{E}_1, \ldots, \mathcal{E}_n$ can be unambiguous discriminated by a single use if and only if for any $i = 1, \ldots, n$,

$$\mathrm{supp}(\mathcal{E}_i) \not\subseteq \sum_{j \neq i} \mathrm{supp}(\mathcal{E}_j). \quad (21)$$

Here for any quantum operation $\mathcal{E}$, $\mathrm{supp}(\mathcal{E})$ denotes the span of its Kraus operators $\{E_k\}$, i.e.,

$$\mathrm{supp}(\mathcal{E}) = \Big\{ \sum_k \lambda_k E_k : \lambda_k \in \mathcal{C} \Big\}. \quad (22)$$

4 Entanglement Transformation Under LOCC

Quantum entanglement is a valuable resource in quantum information processing. It can implement some information processing tasks that cannot be accomplished classically. As a consequence, entanglement has been widely used in quantum cryptography[50], quantum superdense coding[57], and quantum teleportation[58]; see [4] for an excellent exposition. Due to the great importance of quantum entanglement, a fruitful branch of quantum information theory named quantum entanglement theory is currently being developed.

Since quantum entanglement exists between different subsystems of a composite system shared by spatially separated parties, a natural constraint on the manipulation of entanglement is that the separated parties are only allowed to perform local quantum operations on their own subsystems and to communicate to each other classically (LOCC). Using this restricted set of transformations, the parties are often required to optimally manipulate the entangled state. One of the central problems of quantum entanglement theory is thus to find the conditions for when an entangled state can be transformed into another one using LOCC. This problem can be approached in two different, but complementary, contexts: the finite regime and the asymptotic regime. In the asymptotic regime Bennett and his collaborators proposed a reversible protocol which shows that any two bipartite entangled pure states with infinite copies can be converted into each other without any loss of entropy of entanglement[60]. Since in practice one can only have finitely many copies of an entangled state, it is of great interest to consider the problem of entanglement transformation in a finite (non-asymptotic) setting[61,97−124].

Arguably, the most important step in the finite regime was made by Nielsen in [61], where he reported a necessary and sufficient condition for a bipartite entangled pure state to be transformed into another pure one deterministically using LOCC. Let $|\psi\rangle$ and $|\varphi\rangle$ be two bipartite entangled states, and let ψ and φ be their respective Schmidt coefficient vectors. Then the transformation of $|\psi\rangle$ to $|\varphi\rangle$ can be realized with certainty using LOCC, written $|\psi\rangle \to |\varphi\rangle$, if and only if ψ is majorized by φ, i.e., $\psi \prec \varphi$. Here two n-dimensional vectors ψ and φ satisfy $\psi \prec \varphi$ if and only if

$$E_l(\psi) \geqslant E_l(\varphi), \quad \text{for all } \ 2 \leqslant l \leqslant n$$

and $E_1(\psi) = E_1(\varphi)$, where $E_l(\psi)$ denotes the sum of the least $n - l + 1$ components of ψ. If all inequalities in the above equation hold strictly and $E_1(\psi) = E_1(\varphi)$, then we say that ψ is strictly majorized by φ.

Nielsen's theorem establishes a connection between the theory of majorization[125,126] and entanglement transformation. It is of fundamental importance in studying entanglement transformation and has been extended in several ways to the case where deterministic local transformation cannot be achieved[97−99,102,111]. Notably, Vidal generalized Nielsen's result with a probabilistic manner and found an explicit expression of the maximal conversion probability between any two states under LOCC[97], say,

$$P(\psi \to \varphi) = \min_{1 \leqslant l \leqslant n} \frac{E_l(\psi)}{E_l(\varphi)}. \tag{23}$$

Since the fundamental properties of a bipartite pure state under LOCC are completely determined by its Schmidt coefficients, which can be treated as a probability vector, we always identify a probability vector with the quantum state represented by it. Let V^n denote the set of all n-dimensional probability vectors. For any $n \times n$ state $|\varphi\rangle$, let $S(\varphi)$ be the set of $n \times n$ states that can be directly transformed into $|\varphi\rangle$ by LOCC, by Nielsen's theorem,

$$S(\varphi) = \{\psi \in V^n : \psi \prec \varphi\}. \tag{24}$$

For any $|\varphi\rangle$, $S(\varphi)$ is a compact convex set with extreme points of the form $P\varphi$, where P is an arbitrary permutation over V^n. Thus the structure of deterministic entanglement transformations under LOCC has been completely understood.

It is straightforward to generalize $S(\varphi)$ to a probabilistic version. For any $\lambda \in [0, 1]$, let $S^\lambda(\varphi)$ be the set of $n \times n$ states that can be transformed into $|\varphi\rangle$ using LOCC with success probability at least λ, i.e.,

$$S^\lambda(\varphi) = \{\psi \in V^n : P(\psi \to \varphi) \geqslant \lambda\}. \tag{25}$$

In particular, $S^0(\varphi) = V^n$, $S^1(\varphi) = S(\varphi)$. Let

$$\varphi_\lambda = (1 - \lambda E_2(\varphi), \beta_2, \ldots, \beta_n), \tag{26}$$

then it holds that $S^\lambda(\varphi) = S(\varphi_\lambda)$[120], where $\varphi^\downarrow = (\beta_1, \ldots, \beta_n)$ is the vector that is obtained by rearranging the components of φ into non-increasing order. Hence $S^\lambda(\varphi)$ is also a convex compact set, with extreme points of the form $P\varphi_\lambda$, where P is arbitrary permutation over V^n.

In sum, the structure of transformations under LOCC in the single-copy scenario (that is, only one copy of source state and one copy of target state are under consideration) can be captured completely. However, when we introduce extra entangled states to help the original transformation or increase the number of copies of the source state, the transformations between bipartite pure states may get very complicated.

5 Catalyst-Assisted Entanglement Transformation

Unlike common resources, it was discovered by Jonathan and Plenio that quantum entanglement is truly a strange one: sometimes, it can help in becoming impossible entanglement transformations into possible without being consumed at all[99]. For a concrete example, let $|\psi\rangle$ and $|\varphi\rangle$ be two bipartite states such that

$$\psi = (0.4, 0.4, 0.1, 0.1) \tag{27}$$

and

$$\varphi = (0.5, 0.25, 0.25, 0). \tag{28}$$

We can easily check that the transformation of $|\psi\rangle$ to $|\varphi\rangle$ cannot be realized by LOCC as $\psi \not\prec \varphi$. Surprisingly, if someone lends the two parties another entangled state $|\phi\rangle$ with

$$\phi = (0.6, 0.4), \tag{29}$$

then the transformation of $|\psi\rangle \otimes |\phi\rangle$ of $|\varphi\rangle \otimes |\phi\rangle$ can be realized with certainty, as $\psi \otimes \phi \prec \varphi \otimes \phi$. The transformation can be represented as

$$|\psi\rangle \otimes |\phi\rangle \to |\varphi\rangle \otimes |\phi\rangle, \tag{30}$$

in which it is obvious that the state $|\phi\rangle$ is not consumed during the process. The effect of the state $|\phi\rangle$ in this transformation is just similar to that of a catalyst in a chemical process since it can help entanglement transformation process without being consumed. Thus it is termed a *catalyst* for the transformation of $|\psi\rangle$ to $|\varphi\rangle$. Such a transformation that uses intermediate entanglement without consuming it is called 'entanglement-assisted local transformation' in [99], abbreviated to ELOCC. Intuitively, it can also be called catalyst-assisted entanglement transformation. The mathematical structure of ELOCC has been carefully investigated in [109, 115, 117, 120]. It has also been shown that such an entanglement catalysis phenomenon exists in the manipulation of mixed states[100], and in the implementation of non-local quantum operations[127].

Let us now review some basic properties of ELOCC. For any $n \times n$ state $|\varphi\rangle$, the set

$$T(\varphi) = \{\psi \in V^n : \exists \phi \ \text{ s.t. } \psi \otimes \phi \prec \varphi \otimes \phi\} \tag{31}$$

denotes all the $n \times n$ states $|\psi\rangle$ which can be transformed into $|\varphi\rangle$ by LOCC with the help of some catalyst[109]. If $\psi \in T(\varphi)$, then we say that $|\psi\rangle$ can be transformed into $|\varphi\rangle$ using ELOCC. If we restrict the state $|\phi\rangle$ used as catalyst in $T(\varphi)$ to be $k \times k$-dimensional, then we can define $T_k(\varphi)$ similarly; namely,

$$T_k(\varphi) = \{\psi \in V^n : \exists \phi \in V^k \text{ s.t. } \psi \otimes \phi \prec \varphi \otimes \phi\}. \tag{32}$$

The fundamental problem concerning ELOCC is to determine when the transformation between two given states are possible using an appropriate catalyst. Let $|\psi\rangle$ and φ be the source and the target respectively, with dimensions $n \times n$. If $n = 4$, then analytical characterizations for the existence of 2×2 catalysts do exist[118]. For

general n, a polynomial time algorithm of time complexity $O(n^{2k+3.5})$ can be used to determine the existence of a $k \times k$ catalyst, where k is treated as a fixed integer[118]. When k is a variable, the above algorithm is of exponential time complexity and is not efficient any more. It remains an open problem to find a feasible characterization for the existence of catalysts.

Another important problem is to determine when ELOCC has advantages over than mere LOCC. More precisely, for a given state $|\varphi\rangle$, decide whether catalysis is useful in producing $|\varphi\rangle$, i.e., $S(\varphi) \neq T(\varphi)$. The condition is very simple: φ has at least two successive components that are distinct from both its smallest and largest components[109]. Moreover, for any given $k \geqslant 1$, whether $k \times k$ dimensional states can serve as catalysts in producing $|\varphi\rangle$ also has an analytical characterization[115]. Two consequences are of great interest. On the one hand, even in the case that catalysis is useful, increasing the dimension of catalysts does not mean a necessary improvement of the catalysis power. On the other hand, whenever ELOCC is useful the dimension of the potential catalysts are not bounded.

A somewhat surprising constraint on the power of ELOCC is that a maximally entangled state cannot serve as a catalyst[99]. Thus a necessary condition for being a catalyst is partially entangled. Interestingly, this partially entangled condition is also a sufficient one. Indeed, it has been shown that any partially entangled state can be used to catalyze certain transformation[109].

Similar catalysis effect exists for probabilistic transformations. In this scenario we say a catalyst is useful if it can increase the maximal conversion probability of a given transformation. That is, for a transformation of $|\psi\rangle$ to $|\varphi\rangle$ such that $P(\psi \to \varphi) < 1$, there may exist a catalyst $|\phi\rangle$ such that

$$P(\psi \otimes \phi \to \varphi \otimes \phi) > P(\psi \to \varphi). \tag{33}$$

An interesting question is when such an improvement is possible? Except for a special case, probabilistic catalysis is always possible[116,120]. To be concise, let $|\psi\rangle$ and $|\varphi\rangle$ be two $n \times n$ states with the respective least Schmidt coefficients α_n and β_n, then there exists a finite dimensional $|\phi\rangle$ such that (33) holds if and only if

$$P(\psi \to \varphi) < \min\left\{1, \frac{\alpha_n}{\beta_n}\right\}. \tag{34}$$

For any $\lambda \in (0,1)$, $T(\varphi)$ and $T_k(\varphi)$ can be generalized to probabilistic transformations directly[120]. To be specific, let

$$T^{\lambda}(\varphi) = \{\psi \in V^n : \exists \phi \text{ s.t. } P(\psi \otimes \phi \to \varphi \otimes \phi) \geqslant \lambda\} \tag{35}$$

be the set of all $n \times n$ states that can be transformed into $|\varphi\rangle$ with a success probability not less than λ with the help of a finite dimensional catalyst state. $T_k^{\lambda}(\varphi)$ has a similar meaning but the dimension of catalyst state is $k \times k$, i.e.,

$$T_k^{\lambda}(\varphi) = \{\psi \in V^n : \exists \phi \in V^k \text{ s.t. } P(\psi \otimes \phi \to \varphi \otimes \phi) \geqslant \lambda\}. \tag{36}$$

In contrast to the deterministic case, the condition, when probabilistic ELOCC has advantage over than mere LOCC, is rather simple, and the probabilistic threshold λ is not involved[120]. Furthermore, whenever probabilistic catalysis is useful, the dimension of the potential catalyst is unbounded.

One may naturally expect that the deterministic case ($\lambda = 1$) and the probabilistic case ($0 < \lambda < 1$) can be unified. Unfortunately, it is not the case. This strange phenomenon suggests there may exist some essential difference between deterministic transformations and probabilistic transformations[115].

6 Multiple-Copy Entanglement Transformation

Another interesting way of manipulating quantum entanglement was proposed by Bandyopadhyay *et al.*[111] Specifically, they found that sometimes multiple copies of a source state may be transformed into the same number of a target state although the transformation cannot happen for a single copy. Take $|\psi\rangle$ and $|\varphi\rangle$ in (27) and (28) as an example, it is a simple calculation to show that $\psi^{\otimes 3} \prec \varphi^{\otimes 3}$. Hence the transformation of $|\psi\rangle^{\otimes 3}$ to $|\varphi\rangle^{\otimes 3}$ can be achieved with certainty under LOCC. This kind of transformation that uses multiple copies of source state and then transforms all of them together into the same number of target state can be intuitively called "multiple-copy entanglement transformation", or MLOCC for short[121]. The mathematical structure of MLOCC has been extensively studied in [115, 122, 123].

For an $n \times n$ state $|\varphi\rangle$, we denote $M(\varphi)$ by the set of all $n \times n$ states which, when provided with a finite (but large enough) number of copies, can be transformed into the same number of $|\varphi\rangle$ under LOCC[122], that is,

$$M(\varphi) = \{\psi \in V^n : \exists k \text{ s.t. } \psi^{\otimes k} \prec \varphi^{\otimes k}\}. \tag{37}$$

If we restrict the number of copies used in $M(\varphi)$ to be k, then we can define $M_k(\varphi)$ similarly; namely,

$$M_k(\varphi) = \{\psi \in V^n : \psi^{\otimes k} \prec \varphi^{\otimes k}\}. \tag{38}$$

The fundamental problem about MLOCC is to give a feasible characterization for when $\psi \in M(\varphi)$, where $|\psi\rangle$ and $|\varphi\rangle$ are any two given states. Such a characterization has not been found yet. So we are interested in determining whether $\psi \in M_k(\varphi)$ holds for a given integer k. In contrast to determining $\psi \in T_k(\varphi)$, the former can always be verified efficiently when one of n and k is a constant[122].

Similar to ELOCC case, a simple characterization for when MLOCC (or k-MLOCC) has an advantage over LOCC exists[122]. An interesting consequence is

in determining whether a transformation can occur by MLOCC, the number of the copies we should consider is unbounded.

We can also consider probabilistic transformations in the MLOCC scenario[115]. A careful investigation is needed to generalize the above results. For any $k \geqslant 1$, we define the average probability of k-copy transformation, namely, the transformation of $|\psi\rangle^{\otimes k}$ to $|\varphi\rangle^{\otimes k}$, as follows:

$$P^{(k)}(\psi \to \varphi) = [P(\psi^{\otimes k} \to \varphi^{\otimes k})]^{\frac{1}{k}}. \tag{39}$$

Intuitively, $P^{(k)}$ is the geometric average value of the probability of (single-copy) transformation $|\psi\rangle \to |\varphi\rangle$ when considering in the environment of k-copy transformation $|\psi\rangle^{\otimes k} \to |\varphi\rangle^{\otimes k}$. Now $M_k(\varphi)$ can be generalized to probabilistic transformations as follows:

$$M_k^{\lambda}(\varphi) = \{\psi \in V^n : P^{(k)}(\psi \to \varphi) \geqslant \lambda\}. \tag{40}$$

The intuition behind the above definition is that with the help of k-MLOCC, the geometric average value of the probability of a single-copy transformation is not less than λ. When the k is not fixed, we have the following

$$M^{\lambda}(\varphi) = \{\psi \in V^n : \exists k \text{ s.t. } P^{(k)}(\psi \to \varphi) \geqslant \lambda\}. \tag{41}$$

The physical meaning of $\psi \in M^{\lambda}(\varphi)$ is that with the help of MLOCC, the average probability of a single-copy transformation is not less than λ. With these notations, most properties of deterministic transformations under MLOCC can be easily generalized to probabilistic transformations. For details about probabilistic MLOCC we refer to [115].

7 Equivalence Between ELOCC and MLOCC

At first glance, entanglement-assisted transformation and multiple-copy entanglement transformation are two completely different extensions of ordinary LOCC. To achieve a specific transformation, the former needs to borrow extra entanglement as resource but is promised not to consume it during the transformation, while the latter realizes a similar purpose by accumulating a sufficiently large number of copies of source state and then transforms all these copies together into the same number of target state.

A surprising fact is that these two kinds of manipulations of entanglement are closely related to each other[113,115,122,123]. We will show some interesting connections between them.

The first interesting relation is that for any state $|\varphi\rangle$, $\lambda \in [0,1]$, and $k \geqslant 1$, k-copy transformation is useful in producing $|\varphi\rangle$ if and only if k-dimensional catalysis is useful in producing the same target[115]. That is,

$$S^{\lambda}(\varphi) = M_k^{\lambda}(\varphi) \Leftrightarrow S^{\lambda}(\varphi) = T_k^{\lambda}(\varphi). \tag{42}$$

In particular, when k tends to infinity, we obtain a nice equivalence between MLOCC and ELOCC: MLOCC is useful in producing a state if and only if ELOCC is useful in producing the same target[122], i.e.,

$$S^{\lambda}(\varphi) = M^{\lambda}(\varphi) \Leftrightarrow S^{\lambda}(\varphi) = T^{\lambda}(\varphi). \tag{43}$$

Furthermore, one can show that every multiple-copy entanglement transformation can be implemented by an appropriate entanglement-assisted one[121], i.e.,

$$M^{\lambda}(\varphi) \subseteq T^{\lambda}(\varphi). \tag{44}$$

Another interesting question is, whether we can help entanglement-assisted transformation by increasing the number of copies of the original state? To be concise, let us define

$$T^{\lambda M}(\varphi) = \{\psi \in V^n : \exists k,\ \exists \phi \text{ s.t. } P(\psi^{\otimes k} \otimes \phi \to \varphi^{\otimes k} \otimes \phi) \geqslant \lambda^k\}. \tag{45}$$

Then for any state $|\varphi\rangle$, we have

$$T^{\lambda M}(\varphi) = T^{\lambda}(\varphi). \tag{46}$$

Intuitively, the combination of MLOCC and ELOCC is still equivalent to pure ELOCC[122].

One may naturally hope that every catalyst-assisted transformation can also be simulated by a suitable multiple-copy one. This suggests a strong equivalence between ELOCC and MLOCC: $M^{\lambda}(\varphi) = T^{\lambda}(\varphi)$. Unfortunately, this is not always correct since sometimes an entanglement-assisted transformation is more powerful than a corresponding multiple-copy entanglement transformation[113]. Surprisingly, these two kinds of transformation are asymptotically equivalent although it is not the case when only a finite manner is allowed. To present this result, we need to introduce several notations. The optimal conversion probability of a multiple-copy entanglement transformation is given by

$$P_M(\psi \to \varphi) = \sup_k P^{(k)}(\psi \to \varphi), \tag{47}$$

where $P^{(k)}$ is the k-copy average transformation probability defined in (39) and k ranges over all positive integers. On the other hand, we define the optimal conversion probability of an entanglement-assisted transformation from $|\psi\rangle$ to $|\varphi\rangle$ by

$$P_E(\psi \to \varphi) = \sup_{\phi} P(\psi \otimes \phi \to \varphi \otimes \phi), \tag{48}$$

where $|\phi\rangle$ ranges over all finite dimensional bipartite pure states. Now the asymptotical equivalence of ELOCC and MLOCC can be exactly stated as[123]:

$$P_E(\psi \to \varphi) = P_M(\psi \to \varphi). \tag{49}$$

The above relation can be alternatively stated as follows:

$$\overline{T^{\lambda}(\varphi)} = \overline{M^{\lambda}(\varphi)},\ \lambda \in (0,1). \tag{50}$$

Note that for a subset $A \subseteq V^n$, $\overline{A}$ represents A's closure. It is unclear whether the above relation also holds for $\lambda = 1$.

The equivalence of ELOCC and MLOCC transformations is interesting in many ways, both theoretically and practically. In principle, it uncovers an essential connection between entanglement catalysis and multiple-copy entanglement transformation, and declares that they have almost the same effect. In practice, it provides a more feasible way to evaluate the optimal conversion probability of an ELOCC transformation by calculating the optimal conversion probability of the corresponding MLOCC one.

8 Efficiency of Deterministic Entanglement Transformation

Suppose that two parties share some copies of entangled pure state $|\psi_1\rangle$, and want to deterministically transform them into some copies of another state $|\psi_2\rangle$ by LOCC, the efficiency of such a transformation is characterized by the deterministic entanglement exchange rate from $|\psi_1\rangle$ to $|\psi_2\rangle$, which is defined as the supremum of ratios of n and m for any positive integers m and n such that m copies of $|\psi_1\rangle$ can be transformed into n copies of $|\psi_2\rangle$ by LOCC[119], i.e.,

$$D(\psi_1, \psi_2) = \sup\left\{\frac{n}{m} : |\psi_1\rangle^{\otimes m} \to |\psi_2\rangle^{\otimes n}\right\}. \tag{51}$$

Intuitively, for a sufficiently large m, we can transform m copies of $|\psi_1\rangle$ exactly into $mD(|\psi_1\rangle, |\psi_2\rangle)$ copies of $|\psi_2\rangle$ by LOCC.

It would be desirable to know the precise value of $D(\psi_1, \psi_2)$. However, we still do not know how to compute the deterministic entanglement exchange rate at present. Nevertheless, we can obtain a lower bound and an upper bound of $D(\psi_1, \psi_2)$ as follows[119]:

$$0 < D(\psi_1, \psi_2) \leqslant R(\psi_1, \psi_2), \tag{52}$$

where $R(\psi_1, \psi_2)$ is the entropy ratio of $|\psi_1\rangle$ and $|\psi_2\rangle$ and is defined to be the infimum of the ratios of Renyi's entropies of $|\psi_1\rangle$ and $|\psi_2\rangle$.

The relation $D(\psi_1, \psi_2) > 0$ reveals a fundamental property of entangled pure states. That is, any two entangled pure states are interconvertible in the sense that sufficiently many copies of one state can always be exactly transformed into some copies of another state by LOCC.

In general whether the upper bound $R(\psi_1, \psi_2)$ is tight or not is still unknown. In particular, if the target state is maximally entangled, the deterministic entanglement exchange rate can be calculated explicitly and coincides with the upper bound presented above.

It is also of great interest to consider the influence of catalysis on the deterministic entanglement exchange rate. Since an ELOCC transformation is always not less, and sometimes strictly more, powerful than an LOCC transformation, one may naturally expect that the deterministic entanglement exchange rate will be increased by introducing extra states to serve as catalysts. However, a rather surprising fact is that $D(\psi_1, \psi_2)$ cannot be enhanced even allowing extra entangled states to serve as catalysts. In other words, entanglement catalysis has no effect on the deterministic entanglement exchange rate[119]. It is interesting that this result also holds in the multipartite setting though the existence of multipartite catalyst is still unknown.

The above discussions have been generalized to multipartite scenario[114]. A state is genuinely entangled if it cannot be written in product form between any bipartite of the parties. Formally, let $\mathcal{P}$ be the set of all parties under consideration, say, $\mathcal{P} = \{P_i : 1 \leqslant i \leqslant m\}$. A state $|\psi\rangle$ shared by parties in $\mathcal{P}$ is called an m-partite entangled state if for any nonempty proper subset of $\mathcal{P}$, say $\mathcal{A}$, $|\psi\rangle$ is entangled according to any bipartite partition $\mathcal{A}$ and $\mathcal{P} - \mathcal{A}$. Let $|\psi_1\rangle$ and $|\psi_2\rangle$ be two m-partite entangled states, where $m \geqslant 3$. The definition of the deterministic entanglement exchange rate of $|\psi_1\rangle$ to $|\psi_2\rangle$ is the same as bipartite case. However, the entropy ratio needs a careful investigation, since different bipartite partition can cause different values. Let $R(\psi_1^{\mathcal{A}}, \psi_2^{\mathcal{A}})$ be the entropy ratio obtained through the bipartite partition $\{\mathcal{A}, \mathcal{P} - \mathcal{A}\}$, then the entropy ratio between $|\psi_1\rangle$ and $|\psi_2\rangle$ is defined by

$$R(\psi_1, \psi_2) = \min_{\mathcal{A}} R(\psi_1^{\mathcal{A}}, \psi_2^{\mathcal{A}}), \tag{53}$$

where $\mathcal{A}$ ranges over all nonempty proper subsets of $\mathcal{P}$. With these notations, (52) also holds for any m-partite entangled states[114].

9 Partial Recovery of Quantum Entanglement

Unlike the transformations in the asymptotic regime, a direct implication of Nielsen's theorem is that a certain amount of entanglement will be lost in an LOCC transformation[61]. It would be desirable to save some entanglement lost and reduce the net loss of entanglement in the transformation, since the saved entanglement can be used, for example, to increase the classical capacity of a quantum channel[128].

The possibility of recovering lost entanglement was first observed by Morikoshi[101]. Morikoshi's recovering scheme can be outlined as follows. Suppose Alice and Bob share an entangled state $|\psi\rangle$ and they can transform it into $|\varphi\rangle$ by LOCC. Suppose now an auxiliary state $|\chi\rangle$ is supplied to Alice and Bob. Instead of transforming $|\psi\rangle$ into $|\varphi\rangle$ directly, they perform collective operations on the joint state $|\psi\rangle \otimes |\chi\rangle$, and transform it into another joint state $|\varphi\rangle \otimes |\omega\rangle$. Of course, as required by Nielsen's theorem, entanglement of the whole system decreases too. But by choosing a suitable auxiliary state $|\chi\rangle$, sometimes a more entangled state $|\omega\rangle$ can be obtained. Intuitively, this process enables part of entanglement lost in the original transformation to be transferred to the auxiliary state, and it was termed

partial entanglement recovery. Morikoshi demonstrated that partial entanglement recovery for a transformation between 2×2 states is always possible by using a 2×2 auxiliary state. Partial entanglement recovery for transformations between higher dimensional states was considered by Bandyopadhyay *et al.*[107] They showed that for any states $|\psi\rangle$ and $|\varphi\rangle$ such that ψ is strictly majorized by φ and $n > 2$, it is always possible to use a 2×2-dimensional auxiliary state to achieve partial entanglement recovery.

Here we consider the possibility of partial entanglement recovery for general transformations[124]. More precisely, we consider the problem of whether a given entangled state can be used to recover some entanglement lost in a specified transformation. Let $|\psi\rangle$ and $|\varphi\rangle$ be the source state and the target state of the specified transformation, respectively, and let $|\chi\rangle$ be the given auxiliary state. Our goal is to determine whether there exists another state $|\omega\rangle$ satisfying (i) the transformation of $|\psi\rangle \otimes |\chi\rangle$ to $|\varphi\rangle \otimes |\omega\rangle$ can be implemented with certainty using LOCC, and (ii) $|\omega\rangle$ is more entangled than $|\chi\rangle$.

A somewhat interesting thing is when the given transformation satisfies strict majorization, i.e., ψ is strictly majorized by φ, the possibility of partial entanglement recovery can be determined analytically[124]. For the case where ψ is not strictly majorized by φ, a complete solution appears to be very difficult. Nevertheless, two sufficient conditions for partial entanglement recovery are presented.

We can also employ an algorithmic approach to studying the process of partial entanglement recovery. To be specific, let n and k be the dimensions of ψ (as well as φ) and χ (as well as ω), respectively. Then an algorithm of time complexity $O(n^2k^4)$ can be used to efficiently determine the possibility of partial entanglement recovery[124].

As an interesting application, one can generate maximally entangled states by using a scheme based on partial entanglement recovery[101,106,124]. Further investigations show that partial entanglement recovery also happens in situations such as entanglement catalysis[110], mutual catalysis[112], and multiple-copy transformation[122]. A close connection between partial entanglement recovery and ELOCC exists: if a transformation can be implemented by ELOCC, then the entanglement lost in the transformation can be partially recovered by a suitable auxiliary state[124]. Moreover, partial entanglement recovery is directly connected to mutual catalysis. As a consequence, a systematic construction of the instances with mutual catalysis effect based on partial entanglement recovery was obtained in [124]. When considering the possibility of partial entanglement recovery in multiple-copy transformations, we notice a very interesting phenomenon: although an auxiliary state cannot be used to do partial entanglement recovery for a single-copy transformation, it can recover some entanglement lost in certain multiple-copy transformations[124].

All the results obtained so far are only concerned with the possibility of partial entanglement recovery, while the efficiency of this process has not been touched yet. These results are of limited use in practice, where one needs to minimize entanglement lost in LOCC transformations. In other words, one requires the resulting state $|\omega\rangle$ to be not only more entangled than $|\chi\rangle$, but also an "optimal" one that can be achieved in this process. How to design efficient algorithms to find such an optimal state $|\omega\rangle$ would be a challenging and worthwhile problem.

References

[1] William K Wootters, W H Zurek. A single quantum cannot be cloned. *Nature*, 1982, 299: 802–803.

[2] Dennis Dieks. Communication by EPR devices. *Physics Letters A*, 1982, 92: 271–272.

[3] Richard P Feynman. Simulating physics with computers. *International Journal of Theoretical Physics*, 1982, 21(6/7): 467–488.

[4] Michael A Nielsen, Isaac L Chuang. Quantum Computation and Quantum Information. Cambridge University Press, 2000.

[5] John Preskill. Lecture Notes for Physics 219/Computer Science 219: Quantum Computation, 1997–2004. Available online: www.theory.caltech.edu/people/preskill/ph229/

[6] A Yu Kitaev, A H Shen, M N Vyalyi. Classical and Quantum Computation. American Mathematical Society, 2002.

[7] David Deutsch. Quantum theory, the Church-Turing principle and the universal quantum computer. In *Proc. the Royal Society of London A*, 1985, 400: 97–117.

[8] Alan M Turing. On computable numbers, with an application to the Entscheidungsproblem. In *Proc. the London Mathematical Society*, 1937, 42: 230–265.

[9] David Deutsch. Quantum computational networks. In *Proc. the Royal Society of London A*, 1989, 425: 73.

[10] Andrew Chi-Chih Yao. Quantum circuit complexity. In *the 34th Annual IEEE Symposium on Foundations of Computer Science* (*FOCS*), IEEE, New York, Nov. 1993, pp.352–360.

[11] Robert Raussendorf, Hans J Briegel. A one-way quantum computer. *Physical Review Letters*, 2001, 86(22): 5188–5191.

[12] Robert Raussendorf, Daniel E Browne, Hans J Briegel. Measurement-based quantum computation on cluster states. *Physical Review A* (*Atomic, Molecular, and Optical Physics*), 2003, 68(2): 022312,

[13] Hans J Briegel, Robert Raussendorf. Persistent entanglement in arrays of interacting particles. *Physical Review Letters*, 2001, 86(5): 910–913.

[14] Walther P, Resch K J, Rudolph T *et al.* Experimental one-way quantum computing. *Nature*, 2005, 434: 169–176.

[15] Edward Farhi, Jeffrey Goldstone, Sam Gutmann, Michael Sipser. Quantum computation by adiabatic evolution. Available online: http://arxiv.org/abs/quant-ph/0001106.

[16] Dorit Aharonov, Wim van Dam, Julia Kempe *et al.* Adiabatic quantum computation is equivalent to standard quantum computation. Available online: http://arxiv.org/abs/quant-ph/0405098.

[17] Peter W Shor. Scheme for reducing decoherence in quantum computer memory. *Physical Review A* (*Atomic, Molecular, and Optical Physics*), 1995, 52(4): R2493–R2496.

[18] Steane A M. Error correcting codes in quantum theory. *Physical Review Letters*, 1996, 77(5): 793-797.

[19] A R Calderbank, Peter W Shor. Good quantum error-correcting codes exist. *Physical Review A* (*Atomic, Molecular, and Optical Physics*), 1996, 54(2): 1098–1105.

[20] Steane A M. Multiple particle interference and quantum error correction. In *Proc. the Royal Society of London A*, 1996, 452: 2551–2577.
[21] Gottesman D. Stabilizer codes and quantum error correction [Dissertation]. California Institute of Technology, 1997.
[22] David Deutsch, Richard Jozsa. Rapid solution of problems by quantum computation. In *Proc. the Royal Society of London A*, 1992, 439: 553–558.
[23] Bernstein E, Vazirani U. Quantum complexity theory. In *the 25th Annual ACM Symposium on Theory of Computing* (*STOC*), ACM Press, 1993, pp.11–20.
[24] Daniel R Simon. On the power of quantum computation. In *the 35th Annual IEEE Symposium on Foundations of Computer Science*, IEEE, New York, 1994, p.116.
[25] Peter W Shor. Algorithms for quantum computation: Discrete log and factoring. In *the 35th Annuel Symp. Foundations of Computer Science* (*FOCS*), IEEE Press, 1994, pp.124–134.
[26] Ronald L Rivest, A Shamir, L Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 1978, 21(12): 120–126.
[27] Grover L K. A fast quantum mechanical algorithm for database search. In *the 28th Annual ACM Symposium on Theory of Computing* (*STOC*), ACM Press, 1996, pp.212–219.
[28] Lov K Grover. Quantum mechanics helps in searching for a needle in a haystack. *Physical Review Letters*, 1997, 79(2): 325–328.
[29] Charles H Bennett, Ethan Bernstein, G Brassard, Umesh Vazirani. Strengths and weaknesses of quantum computing. *SIAM Journal of Computing*, 1997, 26(5): 1510–1523.
[30] Michel Boyer, Gilles Brassard, Peter Hoeyer, Alain Tapp. Tight bounds on quantum searching. *Fortschritte der Physik*, 1998, 4–5(46): 493–505.
[31] Mosca M. Quantum computer algorithms [Dissertation]. University of Oxford, 1999.
[32] Andris Ambainis. Quantum lower bounds by quantum arguments. In *the 32nd Annual ACM Symposium on Theory of Computing* (*STOC*), ACM Press, 2000, pp.636–643.
[33] Gui-Lu Long. Grover algorithm with zero theoretical failure rate. *Physical Review A* (*Atomic, Molecular, and Optical Physics*), 2001, 64(2): 022307.
[34] Dorit Aharonov, Andris Ambainis, Julia Kempe, Umesh Vazirani. Quantum walks on graphs. In *the 33rd Annual ACM Symposium on Theory of Computing* (*STOC*), ACM Press, 2001, pp.50–59.
[35] Andris Ambainis. Quantum walk algorithm for element distinctness. In *the 45th Annual IEEE Symposium on Foundations of Computer Science* (*FOCS*), IEEE Press, New York, 2004, pp.22–31.
[36] Andris Ambainis. Quantum walks and their algorithmic applications. Available online: http://arxiv.org/abs/quant-ph/0403120.
[37] Chris Lomont. The hidden subgroup problem — Review and open problems. Available online: http://arxiv.org/abs/quant-ph/0411037.
[38] Knill E. Conventions for quantum pseudocode. Technical Report LAUR-96-2724, Los Alamos National Laboratory, 1996.
[39] Bernhard Ömer. A procedural formalism for quantum computing. Available online: http://tph.tuwien.ac.at/~oemer/qcl.html, 1998.
[40] Sanders J W, Zuliani P. Quantum programming. *Mathematics of Program Construction*, 2000, 1837: 80–99.
[41] Bettelli S, Calarco T, Serafini L. Toward an architecture for quantum programming. *European Physical Journal D*, 2003, 25(2): 181–200.
[42] Selinger P. Towards a quantum programming language. *Mathematical Structures in Computer Science*, 2004, 14(4): 527–586.
[43] Susan Stepney, Samuel L Braunstein, John A Clark *et al.* Journeys in non-classical computation I: A grand challenge for computing research. *International Journal of Parallel, Emergent and Distributed Systems*, 2005, 20(1): 5–19.
[44] Susan Stepney, Samuel L Braunstein, John A Clark *et al.* Journeys in non-classical computation II: Initial journeys and waypoints. *International Journal of Parallel, Emergent and Distributed Systems*, 2006, 21(2): 97–125.
[45] Claude E Shannon. A mathematical theory of communication. *Bell System Technical Journal*, 1948, 27: 379–423, 623–656.
[46] Benjamin Schumacher. Quantum coding. *Physical Review A* (*Atomic, Molecular, and Optical Physics*), 1995, 51(4): 2738–2747.
[47] Holevo A S. The capacity of the quantum channel with general signal states. *IEEE Trans. Information Theory*, IEEE Press, 1998, 44(1): 269–273.
[48] Benjamin Schumacher, Michael D Westmoreland. Sending classical information via noisy quantum channels. *Physical Review A* (*Atomic, Molecular, and Optical Physics*), 1997, 56(1): 131–138.
[49] Charles H Bennett, Peter W Shor. Quantum information theory. *IEEE Trans. Information Theory*, IEEE Press, 1998, 44(6): 2724–2742.
[50] Charles H Bennett, G Brassard. Quantum cryptography: Public key distribution and coin tossing. In *IEEE Int. Conf. Computers, Systems and Signal Processing*, IEEE, New York, Bangalore, India, December 1984, p.175.
[51] Peres A. How to differentiate between non-orthogonal states. *Physics Letters A*, 1988, 128(1–2): 19.
[52] Arun Kumar Pati, Samuel L Braunstein. Impossibility of deleting an unknown quantum state. *Nature*, 2000, 404: 164–165.
[53] Michael A Nielsen, Isaac L Chuang. Programmable quantum gate arrays. *Physical Review Letters*, 1997, 79(2): 321–324.
[54] Gregg Jaeger, Abner Shimony. Optimal distinction between two non-orthogonal quantum states. *Physics Letters A*, 1995, 197(2): 83–87.
[55] Lu-Ming Duan, Guang-Can Guo. Probabilistic cloning and identification of linearly independent quantum states. *Physical Review Letters*, 1998, 80(22): 4999–5002.
[56] Einstein A, Podolsky B, Rosen N. Can quantum-mechanical description of physical reality be considered complete? *Physical Review*, 1935, 47: 777–780.
[57] Charles H Bennett, Stephen J Wiesner. Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states. *Physical Review Letters*, 1992, 69(20): 2881–2884.
[58] Charles H Bennett, Gilles Brassard, Claude Crépeau *et al.* Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Physical Review Letters*, 1993, 70(13): 1895–1899.
[59] Bouwmeester D, Pan J-W, Mattle K *et al.* Experimental quantum teleportation. *Nature*, 1997, 390: 575–579.
[60] Charles H Bennett, Herbert J Bernstein, Sandu Popescu *et al.* Concentrating partial entanglement by local operations. *Physical Review A* (*Atomic, Molecular, and Optical Physics*), 1996, 53(4): 2046–2052.
[61] Nielsen M A. Conditions for a class of entanglement transformations. *Physical Review Letters*, 1999, 83(2): 436–439.
[62] Charles H Bennett, Gilles Brassard, Sandu Popescu *et al.* Purification of noisy entanglement and faithful teleportation via noisy channels. *Physical Review Letters*, 1996, 76(5): 722–725.
[63] Michal Horodecki, Pawel Horodecki, Ryszard Horodecki. Mixed-state entanglement and distillation: Is there a "bound" entanglement in nature? *Physical Review Letters*, 1998, 80(24): 5239–5242.
[64] Artur K Ekert. Quantum cryptography based on Bell's theorem. *Physical Review Letters*, 1991, 67(6): 661–663.
[65] Dominic Mayers. Unconditional security in quantum cryptography. *Journal of the ACM*, 2001, 48(3): 351–406.
[66] Andris Ambainis, Leonard J Schulman, Amnon Ta-Shma *et al.* Quantum communication complexity of sampling. In *the 39th Annual IEEE Symposium on Foundations of Computer Science* (*FOCS*), IEEE, New York, 1998, pp.342–351.

[67] Jens Eisert, Martin Wilkens, Maciej Lewenstein. Quantum games and quantum strategies. *Physical Review Letters*, 1999, 83(15): 3077–3080.

[68] Jiangfeng Du, Hui Li, Xiaodong Xu *et al.* Experimental realization of quantum games on a quantum computer. *Physical Review Letters*, 2002, 88(13): 137902.

[69] Mingsheng Ying. A theory of computation based on quantum logic (I). *Theoretical Computer Science*, 2005, 344(2–3): 134–207.

[70] Igor D Ivanovic. How to differentiate between non-orthogonal states. *Physics Letters A*, 1987, 123(6): 257–259.

[71] Dennis Dieks. Overlap and distinguishability of quantum states. *Physics Letters A*, 1988, 126(5-6): 303–306.

[72] Ban B. Error-free optimum quantum receiver for a binary pure quantum state signal. *Physics Letters A*, 1996, 213(5-6): 235–238.

[73] Chefles A. Unambiguous discrimination between linearly independent quantum states. *Physics Letters A*, 1998, 239(6): 339–347.

[74] Xiaoming Sun, Shengyu Zhang, Yuan Feng *et al.* Mathematical nature of and a family of lower bounds for the success probability of unambiguous discrimination. *Physical Review A (Atomic, Molecular, and Optical Physics)*, 2002, 65(4): 044306.

[75] Vandenberghe L, Boyd S. Semidefinite programming. *Siam Review*, 1996, 38(1): 49–95.

[76] Anthony Chefles, Stephen M Barnett. Quantum state separation, unambiguous discrimination and exact cloning. *Journal of Physics A: Mathematical and General*, 1998, 31: 10097.

[77] Shengyu Zhang, Yuan Feng, Xiaoming Sun *et al.* Upper bound for the success probability of unambiguous discrimination among quantum states. *Physical Review A (Atomic, Molecular, and Optical Physics)*, 2001, 6406(6): 062103.

[78] Yuan Feng, Shengyu Zhang, Runyao Duan *et al.* Lower bound on inconclusive probability of unambiguous discrimination. *Physical Review A (Atomic, Molecular, and Optical Physics)*, 2002, 66(6): 062313.

[79] Charles H Bennett, David P DiVincenzo, Christopher A Fuchs *et al.* Quantum nonlocality without entanglement. *Physical Review A (Atomic, Molecular, and Optical Physics)*, 1999, 59(2): 1070–1091.

[80] Jonathan Walgate, Anthony J Short, Lucien Hardy *et al.* Local distinguishability of multipartite orthogonal quantum states. *Physical Review Letters*, 2000, 85(23): 4972–4975.

[81] S Virmani, M F Sacchi, Martin B Plenio *et al.* Optimal local discrimination of two multipartite pure states. *Physics Letters A*, 2001, 288(2): 62–68.

[82] Yi-Xin Chen, Dong Yang. Optimal conclusive discrimination of two nonorthogonal pure product multipartite states through local operations. *Physical Review A (Atomic, Molecular, and Optical Physics)*, 2001, 64(6): 064303.

[83] Yi-Xin Chen, Dong Yang. Optimally conclusive discrimination of nonorthogonal entangled states by local operations and classical communications. *Physical Review A (Atomic, Molecular, and Optical Physics)*, 2002, 65(2): 022320.

[84] Zhengfeng Ji, Hongen Cao, Mingsheng Ying. Optimal conclusive discrimination of two states can be achieved locally. *Physical Review A (Atomic, Molecular, and Optical Physics)*, 2005, 71(3): 032323.

[85] Rudolph T, Spekkens R W, Turner P S. Unambiguous discrimination of mixed states. *Physical Review A (Atomic, Molecular, and Optical Physics)*, 2003, 68(1): 010301.

[86] Raynal P, Lutkenhaus N, van Enk S J. Reduction theorems for optimal unambiguous state discrimination of density matrices. *Physical Review A (Atomic, Molecular, and Optical Physics)*, 2003, 68(2): 022308.

[87] Fiurasek J, Jezek M. Optimal discrimination of mixed quantum states involving inconclusive results. *Physical Review A (Atomic, Molecular, and Optical Physics)*, 2003, 67(1): 012321.

[88] Eldar Y C. Mixed-quantum-state detection with inconclusive results. *Physical Review A (Atomic, Molecular, and Optical Physics)*, 2003, 67(4): 042309.

[89] Yuan Feng, Runyao Duan, Mingsheng Ying. Unambiguous discrimination between mixed quantum states. *Physical Review A (Atomic, Molecular, and Optical Physics)*, 2004, 70(1): 012308.

[90] Chi Zhang, Yuan Feng, Mingsheng Ying. Unambiguous discrimination of mixed quantum states. *Physics Letters A*, 2006, 353(4): 300–306.

[91] Chefles A. Condition for unambiguous state discrimination using local operations and classical communication. *Physical Review A (Atomic, Molecular, and Optical Physics)*, 2004, 69(5): 050307.

[92] Acin A. Statistical distinguishability between unitary operations. *Physical Review Letters*, 2001, 8717(17): 177901.

[93] G M D'Ariano, P Lo Presti, M G A Paris. Using entanglement improves the precision of quantum measurements. *Physical Review Letters*, 2001, 87(7): 270404.

[94] Runyao Duan, Yuan Feng, Mingsheng Ying. Entanglement is not necessary for perfect discrimination between unitary operations. Available online: http://arxiv.org/abs/quant-ph/0601150, 2006.

[95] Zhengfeng Ji, Yuan Feng, Runyao Duan *et al.* Identification and distance measures of measurement apparatus. *Physical Review Letters*, 2006, 96(20): 200401.

[96] Guoming Wang, Mingsheng Ying. Unambiguous discrimination between quantum operations. *Physical Review A (Atomic, Molecular, and Optical Physics)*, 2006, 73(4): 042301.

[97] Vidal G. Entanglement of pure states for a single copy. *Physical Review Letters*, 1999, 83(5): 1046–1049.

[98] Jonathan D, Plenio M B. Minimal conditions for local pure-state entanglement manipulation. *Physical Review Letters*, 1999, 83(7): 1455–1458.

[99] Jonathan D, Plenio M B. Entanglement-assisted local manipulation of pure quantum states. *Physical Review Letters*, 1999, 83(17): 3566–3569.

[100] Jens Eisert, Martin Wilkens. Catalysis of entanglement manipulation for mixed states. *Physical Review Letters*, 2000, 85(2): 437–440.

[101] Morikoshi F. Recovery of entanglement lost in entanglement manipulation. *Physical Review Letters*, 2000, 84(14): 3189–3192.

[102] Vidal G, Jonathan D, Nielsen M A. Approximate transformations and robust manipulation of bipartite pure state entanglement. *Physical Review A (Atomic, Molecular, and Optical Physics)*, 2000, 62(1): 012304.

[103] Zhengwei Zhou, Guangcan Guo. Basic limitations for entanglement catalysis. *Physics Letters A*, 2000, 277(2): 70–74.

[104] Lo H-K, Popescu S. Concentrating entanglement by local actions: Beyond mean values. *Physical Review A (Atomic, Molecular, and Optical Physics)*, 2001, 63(2): 022301.

[105] Bennett C H, Popescu S, Rohrlich D *et al.* Exact and asymptotic measures of multipartite pure state entanglement. *Physical Review A (Atomic, Molecular, and Optical Physics)*, 2001, 63(1): 012307.

[106] Morikoshi F, Koashi M. Deterministic entanglement concentration. *Physical Review A (Atomic, Molecular, and Optical Physics)*, 2001, 64(2): 022316.

[107] Bandyopadhyay S, Roychowdhury V, Vatan F. Partial recovery of entanglement in bipartite-entanglement transformations. *Physical Review A (Atomic, Molecular, and Optical Physics)*, 2001, 65(4): 040303 (Rapid Communications).

[108] Leung D W, Smolin J A. More is not necessarily easier. Available online: http://arxiv.org/abs/quant-ph/0103158, 2001.

[109] Daftuar S, Klimesh M. Mathematical structure of entanglement catalysis. *Physical Review A (Atomic, Molecular, and Optical Physics)*, 2001, 64(4): 042314.

[110] Bandyopadhyay S, Roychowdhury V. Efficient entanglement-assisted transformation for bipartite pure states. *Physical Review A (Atomic, Molecular, and Optical Physics)*, 2002, 65(4): 042303.

[111] Bandyopadhyay S, Roychowdhury V, Sen U. Classification of nonasymptotic bipartite pure-state entanglement transformations. *Physical Review A* (*Atomic, Molecular, and Optical Physics*), 2002, 65(5): 052315.
[112] Xunli Feng, Zhongyang Wang, Zhizhan Xu. Mutual catalysis of entanglement transformations for pure entangled states. *Physical Review A* (*Atomic, Molecular, and Optical Physics*), 2002, 65(2): 022307.
[113] Yuan Feng, Runyao Duan, Mingsheng Ying. The relation between catalyst-assisted entanglement transformation and multiple-copy transformation. Available online: http://arxiv.org/abs/quant-ph/0312110, 2003.
[114] Zhengfeng Ji, Runyao Duan, Mingsheng Ying. Comparability of multipartite entanglement. *Physics Letters A*, 2004, 330(3): 418–423.
[115] Runyao Duan, Yuan Feng, Mingsheng Ying. An equivalence of entanglement-assisted transformation and multiple-copy entanglement transformation. Available online: http://arxiv.org/abs/quant-ph/0404046, 2004.
[116] Yuan Feng, Runyao Duan, Mingsheng Ying. When catalysis is useful for probabilistic entanglement transformation. *Physical Review A* (*Atomic, Molecular, and Optical Physics*), 2004, 69(6): 062310.
[117] Sumit Kumar Daftuar. Eigenvalue inequalities in quantum information processing [Dissertation]. California Institute of Technology, 2004.
[118] Xiaoming Sun, Runyao Duan, Mingsheng Ying. The existence of quantum entanglement catalysts. *IEEE Trans. Information Theory*, 2005, 51(1): 75–80.
[119] Runyao Duan, Yuan Feng, Zhengfeng Ji *et al.* Efficiency of deterministic entanglement transformation. *Physical Review A* (*Atomic, Molecular, and Optical Physics*), 2004, 71(2): 022305.
[120] Yuan Feng, Runyao Duan, Mingsheng Ying. Catalyst-assisted probabilistic entanglement transformation. *IEEE Transanctions on Information Theory*, 2005, 51(3): 1090–1101.
[121] Runyao Duan, Yuan Feng, Xin Li *et al.* Trade-off between multiple-copy transformation and entanglement catalysis. *Physical Review A* (*Atomic, Molecular, and Optical Physics*), 2005, 71(6): 062306.
[122] Runyao Duan, Yuan Feng, Xin Li *et al.* Multiple-copy entanglement transformation and entanglement catalysis. *Physical Review A* (*Atomic, Molecular, and Optical Physics*), 2005, 71(4): 042319.
[123] Runyao Duan, Yuan Feng, Mingsheng Ying. Entanglement-assisted transformation is asympotically equivalent to multiple-copy transformation. *Physical Review A* (*Atomic, Molecular, and Optical Physics*), 2005, 72(2): 024306.
[124] Runyao Duan, Yuan Feng, Mingsheng Ying. Partial recovery of quantum entanglement. *IEEE Trans. Information Theory* (accepted, in press), Available online: http://arxiv.org/abs/quant-ph/0404047, 2006.
[125] Marshall A W, Olkin I. Inequalities: Theory of Majorization and Its Applications. Academic Press, New York, 1st Edition, 1979.
[126] Alberti P M, Uhlmann A. Stochasticity and Partial Order: Doubly Stochastic Maps and Unitary Mixing. Dordrecht, Boston, 1st Edition, 1982.
[127] Vidal G, Cirac J I. Catalysis in nonlocal quantum operations. *Physical Review Letters*, 2002, 88(16): 167903.
[128] Bennett C H, Shor P W, Smolin J A *et al.* Entanglement-assisted classical capacity of a quantum channel and the reverse Shannon theorem. *IEEE Trans. Information Theory*, 2002, 48(10): 2637–2655.

Run-Yao Duan received the B.S. degree from the Department of Computer Science and Technology, Tsinghua University, Beijing, China, in 2002. Now he is working towards the Ph.D. degree at the same department. His current research interests include quantum computation and quantum information theory.

Zheng-Feng Ji received B.S. degree from the Department of Computer Science and Technology, Tsinghua University, Beijing, China, in 2002. He is now a Ph.D. candidate at Tsinghua University under supervision of Prof. Mingsheng Ying. Currently, he works in the area of quantum computation and information.

Yuan Feng received the B.S. degree from the Department of Mathematics, Tsinghua University, Beijing, China, in 1999 and the Ph.D. degree in computer science from the Department of Computer Science and Technology, Tsinghua University, in 2004. His current research is focusing on quantum information and quantum computation.

Ming-Sheng Ying graduated from the Department of Mathematics, Fuzhou Teachers College, Jiangxi, China, in 1981. He is currently a Cheung Kong Professor at State Key Laboratory of Intelligent Technology and Systems, Department of Computer Science and Technology, Tsinghua University, Beijing China. His research interests include formal methods and semantics, logic in computer science and artificial intelligence, quantum information, and fuzzy logic. He has published more than 50 papers on the international referred journals, and he is also the author of the book *Topology in Process Calculus: Approximating Correctness and Infinite Evolution of Concurrent Programs* (New York: Springer-Verlag, 2001).