Quantum Information and Computation, Vol. 3, No. 3 (2003) 203–210

LOCAL DISTINGUISHABLILITY OF QUANTUM STATES AND THE DISTILLATION OF ENTANGLEMENT

PING-XING CHEN[1,2a] and CHENG-ZU LI[1]

[1] *Department of Applied Physics, National University of Defense Technology*
Changsha, 410073, P. R. China

[2] *Key Laboratory of Quantum Information, University of Science and Technology of China*
Chinese Academy of Sciences, Hefei 230026, P. R. China

Received October 18, 2002
Revised March 23, 2003

This paper tries to probe the relation between the local distinguishability of orthogonal quantum states and the distillation of entanglement. An new interpretation for the distillation of entanglement and the distinguishability of orthogonal quantum states in terms of information is given, respectively. By constraining our discussion on a special protocol we give a necessary and sufficient condition for the local distinguishability of the orthogonal pure states, and gain the maximal yield of the distillable entanglement. It is shown that the information entropy, the locally distinguishability of quantum states and the distillation of entanglement are closely related.

Keywords: Distinguishability, distillation of entanglement, information entropy.

Communicated by: S Braunstein & R Laflamme

One of interesting topics in quantum mechanics is how to distinguish a set of quantum states by local operations and classical communication (LOCC). Alice and Bob share a quantum system, in one of a known set of possible orthogonal states $|\Psi_1\rangle, |\Psi_2\rangle, ..., |\Psi_i\rangle, ..., |\Psi_n\rangle$. They do not, however, know particular state they actually possesses.. To distinguish these possible states they should perform some sequence of LOCC. If these states are not orthogonal to each other, they cannot be distinguished deterministically. Further more, if these states are orthogonal to each other, when only a single copy is provided, they still cannot be distinguished by LOCC except for some special cases [1, 2, 3]. Some interesting works on locally distinguishability of quantum states have been presented [1, 2, 3, 4, 5]. For example, any three of the four Bell states

$$\begin{aligned} \left|\Phi^{\pm}\right\rangle &= \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle) \\ \left|\Psi^{\pm}\right\rangle &= \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle) \end{aligned} \qquad (1)$$

cannot be distinguished by LOCC if only a single copy is provided [2].

[a] E-mail: pxchen@nudt.edu.cn

Another interesting topic in quantum mechanics is the distillation of entanglement. Maximally entangled states may have many applications in quantum information, such as error correcting code[6], dense coding[7] and teleportation[8], etc. In the laboratory, however, a maximally entangled state always becomes a mixed state easily due to the interaction with environment. This results in poor applications. The idea of the distillation of entanglement is to get some maximally entangled states by LOCC from many [9] or infinite copies of a mixed state. A few of protocols for the distillation of entanglement were given[6, 10, 11]. But what is the most efficient distillation protocol and how to calculate the distillable entanglement (the maximal value of entanglement gained from per mixed state), E_D, are still open questions.

All protocols for the distillation of entanglement have a common feature: the distillable entanglement of a mixed state is not bigger than the entanglement of formation of the mixed state owing to the loss of information[12, 13]. In essence, indistinguishability of a set of orthogonal states is also owing to the loss of information. The transformation of information plays an important role in both the distillation of entanglement and the distinguishability of orthogonal quantum states. In this sense, the distillation of entanglement and the distinguishability of orthogonal quantum states should have some links. In this paper, we try to probe this question. Closely related to the present paper is the work of Vedral and Plenio et al [14, 15] who mentioned the link between the global distinguishability of quantum states and the distillation of entanglement, and the work in Refs.[12, 13] which discussed the relations of the classical information and the entanglement. But these paper did not look at the notion of local distinguishability.

In the asymptotic cases a protocol for the distillation of entanglement is to get pure entangled states by LOCC from $n(n \longrightarrow \infty)$ copies of a mixed state σ,

$$\sigma = \sum_{i=1}^{m} \lambda_i \left|\Phi_i\right\rangle \left\langle\Phi_i\right|, \quad \sum_{i=1}^{m} \lambda_i = 1, \tag{2}$$

where $\left|\Phi_i\right\rangle s$ are the eigenstates of σ with nonzero eigenvalues $\lambda_i s$. As shown in the paper by Bennett et al [10, 16] that $\sigma^{\otimes n}$ has $2^{nS(\sigma)}$ "likely" strings of orthogonal pure states. Because what is the most efficient distillation protocol and how to distinguish a general set of orthogonal states are still open questions, we first constrain our discussion on a special protocol (which we define as *one by one measurement* in the following). Under the special protocol we give the necessary and sufficient condition for the distinguishability of the $2^{nS(\sigma)}$ "likely" strings of orthogonal pure states, and gain the maximal yield of the distillable entanglement. It is shown that the information entropy, the locally distinguishability of orthogonal quantum states and the distillation of entanglement have close links. Finally, we consider the generalization of the links to general protocols briefly.

In this paper we will apply the following fact in many cases.

Fact: Suppose Alice and Bob share a pair particles whose state is σ. The n copies of $\sigma, \sigma^{\otimes n}$, is a mixture of m^n pure states-strings, but there are only $\prod_{i=1}^{m} C^{n\lambda_i}_{n-n\sum_{j=0}^{i-1}\lambda_j}$ "likely" strings of orthogonal pure states [10, 16], such as, one of the "likely" strings

$$\overbrace{\left|\Phi_1\right\rangle \cdots \left|\Phi_1\right\rangle}^{\lambda_1 n} \overbrace{\left|\Phi_2\right\rangle \cdots \left|\Phi_2\right\rangle}^{\lambda_2 n} \cdots \overbrace{\left|\Phi_m\right\rangle \cdots \left|\Phi_m\right\rangle}^{\lambda_m n}, \tag{3}$$

where we note $\lambda_0 = 0$. In each of "likely" strings there are $\lambda_i n$ pairs whose states are $|\Phi_i\rangle$. The probability that each "likely" string occurs is $\prod_{i=1}^{m} \lambda_i^{n\lambda_i}$. It can be proved that as $n \to \infty$ we have limits,

$$\prod_{i=1}^{m} C_{n-n\sum_{j=0}^{i-1}\lambda_j}^{n\lambda_i} = 2^{nS(\sigma)} \tag{4}$$

and

$$\prod_{i=1}^{m} \lambda_i^{n\lambda_i} \prod_{i=1}^{m} C_{n-n\sum_{j=0}^{i-1}\lambda_j}^{n\lambda_i} = 1, \tag{5}$$

where $S(\sigma)$ is the information entropy of σ

$$S(\sigma) = -\sum_{i=1} \lambda_i \ln \lambda_i \tag{6}$$

It is to say that the sum of probability of all "likely" strings tends to 1. So we only need consider the "likely" strings as $n \to \infty$.

Any protocol for distillation of entanglement from n copies of a mixed state $\sigma, \sigma^{\otimes n}$, can be conceived as successive rounds of measurements and communication by Alice and Bob. After N rounds of measurements and communication, there are many possible outcomes which correspond to many measurement operators $\{A_i \otimes B_i\}$ acting on the Alice and Bob's Hilbert space. Each of these operators is a product of the positive operators and unitary maps corresponding to Alice's and Bob's measurement and rotations, and represents the effect of the N measurements and communication. If the outcome i occurs, the given state $\sigma^{\otimes n}$ becomes:

$$A_i^+ \otimes B_i^+ \sigma^{\otimes n} A_i \otimes B_i \tag{7}$$

If the state σ is distillable, there must be at least an element $A_i \otimes B_i$ such that as $n \to \infty$

$$A_i^+ \otimes B_i^+ \sigma^{\otimes n} A_i \otimes B_i \to |\Psi_i\rangle \langle\Psi_i|, \tag{8}$$

where $|\Psi_i\rangle$ is a pure entangled state in subspace $V_i \otimes V_i$. The distillable entanglement of σ is the maximum numbers, $E_D(\sigma)$ such that there exists a set of operations as $n \to \infty$, we have limits [17]

$$E_D(\sigma) = \lim_{n\to\infty} \frac{1}{n} \sum_i p_i E(|\Psi_i\rangle), \tag{9}$$

where $E(|\Psi_i\rangle)$ is the entanglement of pure state $|\Psi_i\rangle$, p_i is the probability Alice and Bob carry out operation $A_i \otimes B_i$. One of the effects of $A_i \otimes B_i$ is to project out the subspace on which the projection of $\sigma^{\otimes n}$ is a pure entangled state. We define the subspace as *distillable subspace* (DSS) [9]. In general, there are many DSS in the Hilbert space of n pairs as $n \to \infty$.

Definition: one by one measurement, *the measurement is one by one measurement if Alice and Bob measure some pairs and only measure a pair particles at one time.*

Now we consider a protocol. The aim of the protocol is to distinguish deterministically the $2^{nS(\sigma)}$ "likely" strings by Alice's and Bob's *one by one measurements.* To distinguish deterministically the $2^{nS(\sigma)}$ "likely" strings, Alice and Bob should exclude the possibility of the other "likely" strings and keep only a string. In terms of information the procedure of distinguishing these "likely" strings is to clear up the uncertainty of the n pairs particles, or get the $nS(\sigma)$ bits information by rounds of local unitary operations (LUO) and measurements each of which will destroy some entanglement of each string. By measuring some pairs Alice and Bob can divide the $2^{nS(\sigma)}$ strings into many strings-groups and then get some information of the n pairs. Each of the strings-groups can be distinguished from others, since each of the groups can be "indicated" by the product vectors of the measured pairs [3]. For example, if σ is a Bell-diagonal states Alice and Bob can measure a pair with product bases $|00\rangle, |01\rangle, |10\rangle, |11\rangle$. Alice and Bob may get bases $|00\rangle$ and $|11\rangle$ with same probability $(\lambda_1 + \lambda_2)/2$. The bases both $|00\rangle$ and $|11\rangle$ indicate the strings in which the state of the measured pair is $|\Phi\rangle$; Or Alice and Bob may get bases $|01\rangle$ and $|10\rangle$ with same probability $(\lambda_3 + \lambda_4)/2$, and both $|01\rangle$ and $|10\rangle$ indicate the strings in which the state of the measured pair is $|\Psi\rangle$. After measuring some pairs each of the $2^{nS(\sigma)}$ strings may be indicated by the product vectors of the measured pairs and can be distinguished. If the $2^{nS(\sigma)}$ can be distinguished we say that Alice and Bob get the $nS(\sigma)$ bits information.

Obviously, Alice and Bob should measurement n pairs to get the $nS(\sigma)$ bits information by measurement directly on n copies without the help of any LUO. Fortunately, it is possible that Alice and Bob get the $nS(\sigma)$ bits information by measuring less than n pairs with the help of a set of LUO acting on the all copies $\sigma^{\otimes n}$ and classical communication. So, in essence, the above protocol is to distinguish the $2^{nS(\sigma)}$ strings by distinguishing the states of each measured pair with the help of LUO and classical communications.

Suppose Alice and Bob need at least to measure $(n - m)$ pairs particles to get $nS(\sigma)$ bits informations. After measuring $n - m$ pairs with the help of a set of local unitary transformations, Alice and Bob can distinguish the $2^{nS(\sigma)}$ strings and the entanglement of unmeasured pairs in each string is kept. So they get a yield of entanglement,

$$E_D' = \frac{mE(\sigma)}{n}, \tag{10}$$

where $mE(\sigma)$ is the entanglement of kept pairs in a string.

Operations to distinguish the states of a pair particles can be achieved by measuring a pair with a set of product vectors [3]. Suppose that P_j is the probability of Alice and Bob getting the j'th product vector, and $P_j^{'}$ is the sum of the probability such that the j'th product vector indicates $P_j^{'} 2^{nS(\sigma)}$ "likely" strings. If Alice and Bob get the j'th product vector, they keep $P_j^{'} 2^{nS(\sigma)}$ strings and discard the others. In terms of information, they get $-\ln P_j'$ bit information. We define $-\ln P_j'$ as *distinguishable information* (DI) which reflects on the contribution to distinguish the "likely" strings when Alice and Bob get the j'th product vector. If the j'th vector indicates a few of the "likely" strings (or indicates a strings-group), not all the "likely" strings, it presents nonzero DI, $-\ln P_j^{'}$, and makes a contribution to distinguish these "likely" strings. If a vector indicates all the "likely" strings, it presents no DI, which corresponds to inability to distinguish the "likely" strings. Only when the DI gained by measuring some pairs is equal to the information entropy of the $2^{nS(\rho)}$ strings, $nS(\rho)$, can these "likely" strings be distinguished. Because all strings have same structure, by the symmetry when $n \to \infty$, Alice and Bob can get the same DI from each measured pair.

Suppose that Alice and Bob have measured M pairs, we consider a kind of outputs in which M_j pairs collapse the j'th basis. The probability that Alice and Bob get one of this kind of outputs is

$$\prod_j P_j^{M_j},$$

where $M = \sum_j M_j$. The number of these outputs is

$$\prod_j C^{\ M_j}_{\ M-\sum_{i=0}^{j-1} M_i},$$

where $M_0 = 0$. Each of these outputs results in $-\ln\prod_j P_j^{\prime M_j}$ bits informations. From the similar statement as the Fact it follows that the "likely" outputs are those in which MP_j pairs collapse the j'th vector, and the probability of all the "likely" outputs tends to 1 as $n \to \infty$. A "likely" output results in $-\ln\prod_j P_j^{\prime MP_j}$ bits DI. When DI is equal to the information entropy of n pairs, i.e.,

$$-\ln\prod_j P_j^{\prime MP_j} = -M\sum_j P_j \ln P_j^{'} = nS(\sigma), \tag{11}$$

Alice and Bob can distinguish the $2^{nS(\sigma)}$ strings, and get a yield

$$E_D^{''}(\sigma) = \frac{1}{n}(n - \frac{nS(\sigma)}{I_d(\sigma)})E(\sigma) = (1 - \frac{S(\sigma)}{I_d(\sigma)})E(\sigma), \tag{12}$$

where $I_d(\sigma) = -\sum_j P_j \ln P_j^{'}$, is a average DI by measuring a pair. If the maximal average DI is $I_{d\,\max}(\sigma)$, the yield is

$$E_D^{'''}(\sigma) = (1 - \frac{S(\sigma)}{I_{d\,\max}(\sigma)})E(\sigma). \tag{13}$$

The discussion above means that under one by one measurement protocol Alice and Bob should measure $\frac{nS(\sigma)}{I_{d\,\max}(\sigma)}$ pairs at least to get a yield in Eq. (13). By measuring $\frac{nS(\sigma)}{I_{d\,\max}(\sigma)}$ pairs Alice and Bob can get the all "likely" outputs, each of which results in a yield in Eq. (13). So the yield of entanglement in equation (13) is the maximal yield under one by one measurement protocol, and is a lower bound of the distillable entanglement. On the other hand, the above discussion shows that under the one by one measurement protocol Alice and Bob should measure $\frac{nS(\sigma)}{I_{d\,\max}(\sigma)}$ pairs at least to distinguish deterministically the $2^{nS(\rho)}$ "likely" strings, the $2^{nS(\rho)}$ "likely" strings are distinguishable if and only if the yield $E_D^{'''}(\sigma)$ in Eq. (13) is bigger than or equal to zero, i.e.,

$$I_{d\,\max}(\sigma) \geq S(\sigma). \tag{14}$$

So equation (13) shows a close link between the locally distinguishability of orthogonal quantum states and the distillation of entanglement. This link is fit to all multi-partite states.

It is well known that there are a few of upper bound of the distillable entanglement, such as the relative entropy of entanglement [14]. Here we present a lower bound of the distillable entanglement as Eq. (13). If the mixed state σ is a Bell-diagonal state ρ, the maximal DI is not less than 1 as shown in the Ref.[6, 10], i.e.,

$$I_{d\max}(\rho) \geq 1. \tag{15}$$

Given that $E(\rho)$ in Eq. (13) is equal to 1, we can get a lower bound of the distillable entanglement of a Bell-diagonal state ρ,

$$E_D(\rho) \geq 1 - S(\rho)$$

Suppose that the mixed state σ is a multiple copies of four Bell states [18], i.e.,

$$\sigma = \rho^{(n)} = \frac{1}{4}\sum_{i=1}^{4}(|\Phi_i\rangle\langle\Phi_i|)^{\otimes n},$$

where $|\Phi_{1,2}\rangle = |\Phi^{\pm}\rangle\,;|\Phi_{3,4}\rangle = |\Psi^{\pm}\rangle$. Because a copy of four Bell states provides at least 1 bit DI, the following inequality should hold

$$I_{d\max}(\rho^{(n)}) \geq n. \tag{16}$$

Given that $E(\rho^{(n)})$ in Eq. (13) is equal to n, and $S(\rho^{(n)}) = 2$, we can get a lower bound of the distillable entanglement of a Bell-diagonal state $\rho^{(n)}$,

$$E_D(\rho^{(n)}) \geq n - 2. \tag{17}$$

On the other hand, the relative entropy of entanglement of $\rho^{(n)}$ is equal to $n-2$, as shown in the Ref. [18], so we follow that $E_D(\rho^{(n)}) = n - 2$.

The example above shows that the Eq. (13) may be useful to calculate the distillable entanglement or the lower bound of the distillable entanglement. But the novelty of the Eq. (13) is to show the close relation among the distillation of entanglement, the local distinguishability of orthogonal quantum states and the information entropy.

Now we would like to discuss the more general protocol briefly. To distinguish the $2^{nS(\rho)}$ "likely" strings, Alice and Bob should do rounds of measurements and classical communication. The effect of these measurements and classical communication can be represented as a set of operators $\{A_i \otimes B_i\}$. If the output is i Alice and Bob know they have got the $i'th$ string with certainty, i.e.,

$$\begin{aligned} A_i \otimes B_i\,|string_i\rangle &= |string_i'\rangle\,; \\ A_i \otimes B_i\,|string_j\rangle &= 0, \text{for} i \neq j, \end{aligned} \tag{18}$$

where $|string_i\rangle$ is the state of $i'th$ "likely" string; $|string_i'\rangle$ is the state after $A_i \otimes B_i$ acts on the $|string_i\rangle$. If the state $|string_i'\rangle\, s$ is an entangled state Alice and Bob get a yield of entanglement, so the operators $\{A_i \otimes B_i\}$ also work for the distillation of entanglement. On the other hand, if σ is distillable, as shown in equation (8) there must be elements $A_i \otimes B_i$ such that as $n \to \infty$, $A_i^{+} \otimes B_i^{+}\sigma^{\otimes n}A_i \otimes B_i \to |\Psi_i\rangle\langle\Psi_i|$. Each operator $A_i \otimes B_i$ projects out the pure entangled state $|\Psi_i\rangle$. If $|\Psi_i\rangle$ belongs to only a string, the operations $\{A_i \otimes B_i\}$ for the distillation of entanglement also work for the local distinguishability of the "likely" strings.

To discuss the generalization of the E.q (13) to more general cases, we should consider two questions: 1. Whether a general measure for the distillation of entanglement can be carried out by many *one by one measurements* or not; 2. It is possible for Alice and Bob to distill a pure entangled state $|\Psi_i\rangle$ from the $2^{nS(\rho)}$ strings but not to distinguish each string, so we should revise the E.q (13). How to revise it? Although the two questions are still open questions, we believe there are some states the distillable entanglement of these states can be gained from the E.q (13).

In summary, the transformation of information in the distillation of entanglement and the locally distinguishability of orthogonal quantum states plays an important role. In terms of information one can get a general link between the distillation of entanglement and the distinguishability of orthogonal quantum states. This link may be useful to calculate distillable entanglement or get a lower bound of distillable entanglement, and understand the essence of entanglement [19].

References

1. C. H. Bennett, D.P. DiVincenzo, C.A. Fuchs, T.Mor, E.Rains, P.W. Shor, J.A. Smolin, and W.K. Wootters (1999), Quantum nonlocality without entanglement,Phys. Rev. A 59,1070.
2. S.Ghosh, G.Kar, A.Roy, A.Sen and U.Sen (2001), Distinguishability of Bell states, Phys.Rev.Lett.87, 277902
3. J.Walgate, A.J.Short, L.Hardy and V.Vedral (2000), Local distinguishability of multipartite orthogonal quantum states, Phys.Rev.Lett.85,4972; J.Walgate and L.Hardy (2002), Nonlocality, Asymmetry, and distinguishing bipartite states, Phys.Rev.Lett 89, 127901; P.-X Chen and C.-Z Li (2002), Criterion for distinguishability of arbitrary orthogonal states, quant-ph/0209048.
4. Y.-X.Chen and D.Yang (2001), The distillable entanglement of multiple copies of Bell states, Phys.Rev.A 64, 064303
5. S. Virmani, M.F. Sacchi, M.B. Plenio and D. Markham (2001), Optimal local discrimination of two multipartite pure states, Physics Letters A 288, 62-68; M. Horodecki, P. Horodecki, and R. Horodecki (1998), Entanglement and thermodynamical analogies, Acta Physica Slovaca 48, 141-156.
6. C. H. Bennett, D. P. Divincenzo, J. A.Smolin, and W. K.Wootters (1996), Mixed-state entanglement and quantum error correction. Phys. Rev. A 54:3824˜3851.
7. C.H. Bennett and S.J. Wiesner (1992), Communication via one-and-two particle operators on Einstein-Podolsky-Rosen states. Phys. Rev. Lett 69, 2881˜2884.
8. C.H. Bennett, G.Brassard, C.Crepeau, R.Jozsa, A.Peres and W.K.Wootters (1993), Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels, Phys. Rev. Lett 70:1895˜1898.
9. P.-X.Chen, L.-M Liang, C.-Z Li and M.-Q Huang (2002), Imposibility criterion for obtaining pure entangled states from mixed states by purifying protocols, Phys.Rev.A 65, 012317; A necessary and sufficient condition of distillability with unite fidelity from finite copies of a mixed state: the most efficient purification protocol, Phys.Rev.A 66, 022309.
10. C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher and W. K. Wootters (1996), Purification of noisy entanglement and faithful teleportation via noisy channels, Phys. Rev. Lett 76 722
11. David P. Divincenzo, Peter W. Shor and John A. Smolin (1998), Quantum channel capacity of very noisy channels, Phys. Rev. A **57**, 830-839.
12. J. Eisert, T. Felbinger, P. Papadopoulos, M.B. Plenio and M. Wilkens (2000), Classical information and distillable entanglement, Phys. Rev. Lett 84, 1611; L.Henderson and V.Vedral (2000), Information, relative entropy of entanglement, and irreversibility. Phys. Rev. Lett 84, 2263˜2267.
13. G. Vidal and J. I. Cirac (2001), Irreversibility in asymptotic maniputations of entanglement,

Phys.Rev.Lett 86, 5803-5806.
14. V. Vedral and M. B. Plenio (1998), Entanglement measures and purification procedures, Phys. Rev. A 57: 1619˜1632.
15. V. Vedral M. B. Plenio, K. Jocobs and P. L. Knight (1997), Statistical inference, distinguishability of quantum states and quantum entanglement, Phys. Rew A 56, 4452-4455.
16. C. H. Bennett, G. Brassard, S. Popescu and B. Schumacher (1996), Concentrating partial entanglement by local operations, Phys. Rev. A **53** 2046.
17. E.M.Rains (1999), Rigorous treatment of distillable entanglement, Phys. Rev. A 60, 173-178.
18. Y.-X.Chen and D.Yang (2002), Distillable entanglement of multiple copies of Bell states, Phys.Rev.A 66, 014303
19. C.Brukner, M.Zukowski and A.Zeilinger (2001), The essence of entanglement, quant-ph/0106119.