A simple proof of monogamy of entanglement

Dong Yang

1Hefei National Laboratory for Physical Sciences at Microscale & Department of Modern Physics, University of Science and Technology of China, Hefei, Anhui 230026, Peoples Republic of China

(Dated: November 3, 2006)

Monogamy of entanglement means that an entangled state cannot be shared with many parties. The more parties, the less entanglement between them. In this paper, we give a simple proof of this property and provide an upper bound of the number of parties.

PACS numbers: 03.67.Mn, 03.65.Ud

Monogamy is one of crucial properties of entanglement. It is essential in quantum cryptography. A simple example is the Bell state $|\Phi\rangle_{AB} = 1/\sqrt{2}(|00\rangle + |11\rangle)$ shared between Alice and Bob. Monogamy of the pure entangled state $|\Phi\rangle_{AB}$ excludes any possibility that another party including the potential eavesdropper Eve could correlate. The monogamous property of the pure entangled state is extended to the un-sharable property for the mixed state $\rho$. In a recent paper [4], the monogamous property is employed to prove asymptotic quantum cloning state estimation, which has been identified as one of the open problems in quantum information theory. In this paper, we give a simple proof of the monogamy of entanglement and provide an upper bound of the number of parties.

Definition 1 A bipartite state $\rho_{AB}$ is said to be $n$-shareable when it is possible to find a quantum state $\rho_{A_1B_2...B_n}$ such that $\rho_{A_1} = \rho_{A_2} = \cdots = \rho_{A_n} = \rho_{AB}$ where $\rho_{A_n} = tr_{B_n}\rho_{A_1B_2...B_n}$. If such state exists, $\rho_{A_1B_2...B_n}$ is called as an $n$-extension of $\rho_{AB}$.

Theorem 1 [2, 3, 4] A bipartite state is $n$-shareable for any $n$ if and only if it is separable.

Proof. For a separable state $\rho_{AB}$, there always exists a separable decomposition

$$\rho_{AB} = \sum_i p_i (|\phi_i\rangle_A \langle \phi_i|_A \otimes |\psi_i\rangle_B \langle \psi_i|_B).$$

(1)

It is explicit that

$$\rho_{A_1B_2...B_n} = \sum_i p_i (|\phi_i\rangle_A \langle \phi_i|_A \otimes |\psi_i\rangle_B \langle \psi_i|_B)$$

(2)

is a valid $n$-extension of $\rho_{AB}$ for any $n$.

Next we prove that for any entangled state $\rho_{AB}$, there always exists a finite $N$ such that no valid $n$-extension can be found for any $n > N$. Recall that the duality relation of a pure tripartite state $\phi_{ABC}$ is [5]

$$S(\rho_A) = E_f(\rho_{AB}) + C_-(\rho_{AC}).$$

(3)

Here $S(\rho_A) = -tr \rho_A \log \rho_A$ is the von Neumann entropy of $\rho_A$. $E_f(\rho_{AB}) = \min \sum_i p_i E(\phi^i_{AB})$ is the entanglement of formation (EoF) [7], where the minimum is taken over all pure ensembles $\{p_i, |\phi^i\rangle_{AB}\}$ satisfying $\rho_{AB} = \sum_i p_i (|\phi^i\rangle \langle \phi^i|)_{AB}$, and entanglement for pure state $\phi_{AB}$ is $E(\phi_{AB}) = S(tr_B(|\phi\rangle \langle \phi|)_{AB})$. $C_-(\rho_{AC}) = \max_{C_i} S(\rho_A) - \sum_i p_i S(\rho_A^i)$ is the classical correlation of bipartite state $\rho_{AC}$ [8], where $\{C_i\}$ is a positive operator-valued measurement (POVM) performed on subsystem $C$, $\rho_A^i = tr_C(I \otimes C_i \rho_{AC} I \otimes C_i)$ is the remaining state of $A$ after obtaining the outcome $i$ on $C$, and $p_i = tr_{AC} (I \otimes C_i \rho_{AC} I \otimes C_i)$ is the probability to obtain outcome $i$.

Suppose the optimal decomposition of EoF for a mixed tripartite state $\rho_{ABC}$ is $\{p_i, |\phi^i\rangle_{ABC}\}$, we have

$$E_f(\rho_{A:BC}) = \sum_i p_i S(\rho_A^i)$$

(4)

$$= \sum_i p_i (E_f(\rho_{A:B}) + C_-(\rho_{A:C}^i))$$

(5)

$$\geq E_f(\rho_{A:B}) + G_-(\rho_{A:C}).$$

(6)

The inequality (6) comes from the convexity of EoF $\sum_i p_i E_f(\rho_{A:B}) \geq E_f(\sum_i p_i \rho_{A:B}^i)$ [9] and $G_-(\rho_{A:C}) = \min \sum_i p_i C_-(\rho_{A:C}^i)$ [8], where the minimum is taken over all mixed ensembles $\{p_i, \rho_{AC}^i\}$ satisfying $\rho_{AC} = \sum_i p_i \rho_{AC}^i$. 

Now iteratively applying the inequality \( (6) \) to the n-extension state \( \rho_{AB_1B_2\ldots B_n} \) of an entangled state \( \rho_{AB} \) and further noticing \( E_f(\rho_{A:B}) \geq G_{\rho} \) by definition of \( G_{\rho} \) [8], we obtain

\[
E_f(\rho_{A:B_1B_2\ldots B_n}) \geq E_f(\rho_{A:B_2\ldots B_n}) + G_{\rho}(\rho_{A:B_1}) \\
\geq E_f(\rho_{A:B_3\ldots B_n}) + G_{\rho}(\rho_{A:B_2}) + G_{\rho}(\rho_{A:B_1}) \\
= E_f(\rho_{A:B_3\ldots B_n}) + 2G_{\rho}(\rho_{A:B}) \\
\geq \ldots \ldots \\
\geq E_f(\rho_{A:B}) + (n-1)G_{\rho}(\rho_{A:B}) \\
\geq nG_{\rho}(\rho_{A:B}). \tag{7}
\]

Employing the explicit relation \( S(\rho_A) \geq E_f(\rho_{A:B_1B_2\ldots B_n}) \) and an important property of \( G_{\rho} \) asserting that \( G_{\rho}(\rho_{A:B}) > 0 \) if and only if \( \rho_{AB} \) is entangled [8], we get the upper bound of n-extension of an entangled state \( \rho_{AB} \),

\[
n \leq N = \left[ \frac{S(\rho_A)}{G_{\rho}(\rho_{AB})} \right], \tag{8}
\]

where \([x]\) is the maximal integer not larger than \( x \). Thus we proved that for entangled state, there exists a finite number \( N \) such that no n-extension can be found for \( n > N \). Physically, entanglement in a given state can not be sharable in arbitrarily many parties.

For the system of many identical particles, the state \( \rho_{A_1A_2\ldots A_n} \) has the symmetry of permutation. It holds for any state that entanglement between any pair particles tends to zero as \( n \to \infty \).

In summary, we give a simple proof of monogamy of entanglement and provide an upper bound of the number of parties beyond which entanglement cannot be shared.

Acknowledgement D. Yang would like to thank M. Horodecki for helpful comment.