Commun. Theor. Phys. (Beijing, China) **49** (2008) pp. 1211–1216

Vol. 49, No. 5, May 15, 2008

Necessary and Sufficient Conditions of Separability for Multipartite Pure States*

LI Da-Fa,[1] LI Xiang-Rong,[2] HUANG Hong-Tao,[3] and LI Xin-Xin[4]

[1]Department of Mathematical Sciences, Tsinghua University, Beijing 100084, China

[2]Department of Mathematics, University of California, Irvine, CA 92697-3875, USA

[3]Electrical Engineering and Computer Science Department, University of Michigan, Ann Arbor, MI 48109, USA

[4]Department of Computer Science, Wayne State University, Detroit, MI 48202, USA

(Received May 25, 2007)

Abstract *In this paper we present a necessary and sufficient condition of separability for multipartite pure states and variants of it. These conditions are very simple and calculable, and they do not require Schmidt decomposition (for two subsystems) or tracing out operations. We also give a necessary condition for a local unitary equivalence class for a bipartite system in terms of the determinant of the matrix of amplitudes.*

PACS numbers: 03.67.Lx, 03.67.Hk
Key words: entanglement, quantum computing, separability

1 Introduction

A pure state is separable if and only if it can be written as a tensor product of states of different subsystems. It is also known that a state $|\psi\rangle$ of a bipartite system is separable if and only if it has Schmidt number 1.[1] Let $|\psi\rangle$ and $|\phi\rangle$ be two pure states of a composite system AB possessed by both Alice and Bob, where system A (B) is called Alice's (Bob's) system. To obtain a Schmidt decomposition of a pure state $|\psi\rangle$, we need to compute (i) the density operator $\rho_\psi^{\rm AB}$; (ii) the reduced density operator $\rho_\psi^{\rm A}$ for system A; (iii) the eigenvalues of $\rho_\psi^{\rm A}$. However it is hard to compute roots of a characteristic polynomial of high degree.

Peres[2] presented a necessary condition for separability by means of positivity of the partial transposition of the density matrix. The positivity was shown by Horodecki *et al.*[3] to be also sufficient for 2×2 and 2×3 dimensions. A reduction criterion of separability for bipartite systems was given.[4,5] Wu *et al.* gave a necessary and sufficient criterion for multipartite separable states by solving a set of equations. However, as the authors claimed, in general it is hard to solve the equations unless the density matrix of the given state has few nonzero eigenvalues. After Chen *et al.*[7] proposed a necessary and sufficient condition of separability of any system, Eggeling *et al.*[8] showed immediately that "it is nothing but a reformulation of the definition of separability, which is naturally a necessary and sufficient criterion for itself." Hence, "it is a reformulation of the problem rather than a practical criterion," said Eggeling *et al.*[8] Therefore, as Eggeling *et al.*[8] indicated, beyond the above special cases, no such calculable criterion is known. Recently, Meyer and Wallach[9] proposed a necessary and sufficient condition for n-qubit system in terms of wedge product. Raymer[10] developed a sufficient condition for bipartite systems. Thus, so far a simple, necessary and sufficient condition of separability for multipartite systems is still open.

For a multi n-partite system, in this paper we give a necessary and sufficient condition of separability for multipartite pure states and variants of it. This paper was adapted from the version in Ref. [11]. In Sec. 2, we present a necessary and sufficient condition for separability for a bipartite system in terms of 2×2 minor determinants of the matrix of the amplitudes. Section 3 contains three versions of a necessary and sufficient separability criterion for an n-qubit system. Section 4 is devoted to study the separability of multipartite pure states, and two versions of a necessary and sufficient separability criterion are proposed. Section 5 gives a simple necessary criterion for $|\psi\rangle \sim |\phi\rangle$ for a bipartite system, where $|\psi\rangle \sim |\phi\rangle$ means that $|\psi\rangle$ is equivalent to $|\phi\rangle$ under local unitary operators.

2 Separability for a Bipartite System with the Same-Dimensional n Subsystems

Let $|\psi\rangle$ be a pure state of a composite system AB possessed by both Alice and Bob. In this section we give a simple and intuitive criterion for the separability. Let $|i\rangle$ ($|j\rangle$) be the orthonormal basis for system A (B). Then we can write $|\psi\rangle = \sum_{i,j} a_{ij}|i\rangle|j\rangle$, where $\sum_{ij=0}^{n-1} |a_{ij}|^2 = 1$. Let $M = (a_{ij})_{n\times n}$ be the matrix of the amplitudes of $|\psi\rangle$. Then the criterion for the separability is as follows.

*The project supported by National Natural Science Foundation of China under Grant No. 60433050, the Fundamental Research Fund of Tsinghua University under Grant No. JC2003043 and partially by the State Key Lab. of Intelligence Technology and System

$|\psi\rangle$ is separable if and only if all 2×2 minor determinants of M are zero.

This criterion for the separability avoids Schmidt decomposition. To compute the determinants, it needs $n^2(n-1)^2/2$ multiplication operations and $n^2(n-1)^2/4$ minus operations.

Proof Suppose that systems A and B have the same dimension n. By definition, $|\psi\rangle$ is separable if and only if we can write $|\psi\rangle = (\sum_{i=0}^{n-1} x_i|i\rangle)\otimes(\sum_{j=0}^{n-1} y_j|j\rangle)$, where $\sum_{i=0}^{n-1}|x_i|^2 = 1$ and $= \sum_{j=0}^{n-1}|y_j|^2 = 1$. By tensor product $|\psi\rangle = \sum_{i,j=0}^{n-1} x_i y_j|i\rangle|j\rangle$. It means that $|\psi\rangle$ is separable if and only if

$$x_i y_j = a_{ij}, \quad i,j = 0,1,\ldots,(n-1)\,. \tag{1}$$

Let $m = \left(\begin{smallmatrix} a_{il} & a_{ik} \\ a_{jl} & a_{jk}\end{smallmatrix}\right)$ be any 2×2 submatrix of M. It is easy to check

$$\det(m) = a_{il}a_{jk} - a_{ik}a_{jl} = x_i y_l x_j y_k - x_i y_k x_j y_l = 0\,.$$

Therefore if $|\psi\rangle$ is separable then all the 2×2 minor determinants of M are zero.

Conversely, suppose that all the 2×2 minor determinants of M are zero. We can write M in the block form, $M = \begin{pmatrix} A_0 \\ A_1 \\ \vdots \\ A_{n-1}\end{pmatrix} = (B_0, B_1, \ldots, B_{n-1})$, where A_i is the i-th row and B_i is the i-th column of M, respectively, $i = 0,1,\ldots,(n-1)$. Let

$$|x_i|^2 = A_i A_i^\dagger\,, \tag{2}$$

$$|y_j|^2 = B_j^\dagger B_j\,, \tag{3}$$

$$i,j = 0,1,\ldots,(n-1)\,,$$

respectively. Note that $A_i^\dagger$ is the complex conjugate of transpose of A_i. Under the supposition we can show that the above x_i in Eq. (2) and y_j in Eq. (3) satisfy Eq. (1). Let us consider the case in which all the a_{ij} are real. It is not hard to extend the result to the case in which all the a_{ij} are complex. We only show $|x_0 y_0|^2 = |a_{00}|^2$ and omit the others. From Eq. (2) and Eq. (3),

$$\begin{aligned}|x_0 y_0|^2 &= A_0 A_0^\dagger B_0^\dagger B_0 \\ &= \left(\sum_{j=0}^{n-1}|a_{0j}|^2\right)\left(\sum_{i=0}^{n-1}|a_{i0}|^2\right) \\ &= \sum_{i,j=0}^{n-1}|a_{0j}|^2\,|a_{i0}|^2 \\ &= \sum_{i,j=0}^{n-1}|a_{00}|^2\,|a_{ij}|^2 = |a_{00}|^2\,.\end{aligned}$$

In the last but one step we use the equality $|a_{0j}|^2|a_{i0}|^2 = |a_{00}|^2|a_{ij}|^2$, which holds since $\left(\begin{smallmatrix} a_{00} & a_{0j} \\ a_{i0} & a_{ij}\end{smallmatrix}\right)$ is a 2×2 submatrix of M. This completes the proof.

Corollary

If $|\psi\rangle$ is separable then $\det(M) = 0$.

3 The Separability for an n-qubit System

Let $|\psi\rangle$ be a pure state of an n-qubit system. Then we can write $|\psi\rangle = \sum_{i_1,i_2,\ldots,i_n\in\{0,1\}} a_{i_1 i_2\ldots i_n}|i_1 i_2\ldots i_n\rangle$. Let M_i be $2^{n-1}\times 2$ matrices of which each row is of the form $(a_{b_1 b_2\ldots b_{i-1}0 b_{i+1}\ldots b_n}, a_{b_1 b_2\ldots b_{i-1}1 b_{i+1}\ldots b_n})$, where b_1, b_2, …, $b_n \in \{0,1\}$, and $i = 1,2,\ldots,n$.[11] Note that M_i are not the usual matrices of the amplitudes of state $|\psi\rangle$. Later, M_i will be used for SLOCC classification and called the partition.[12,13]

For example, let $|\psi\rangle$ be a state of a three-qubit system. Then $|\psi\rangle$ can be written as $|\psi\rangle = \sum_{i=0}^{7} a_i|i\rangle$.

$$M_1 = \begin{pmatrix} a_0 & a_4 \\ a_1 & a_5 \\ a_2 & a_6 \\ a_3 & a_7\end{pmatrix}, \quad M_2 = \begin{pmatrix} a_0 & a_2 \\ a_1 & a_3 \\ a_4 & a_6 \\ a_5 & a_7\end{pmatrix},$$

$$M_3 = \begin{pmatrix} a_0 & a_1 \\ a_2 & a_3 \\ a_4 & a_5 \\ a_6 & a_7\end{pmatrix}.$$

There are three versions of the separability.

Version 1 *$|\psi\rangle$ is separable if and only if all the 2×2 minor determinants of M_i, $i = 1,2,\ldots,n$, are zero.*

The proof of Version 1 is similar to the one for a bipartite system in Sec. 2.

Version 2 *$|\psi\rangle$ is separable if and only if $a_i a_j = a_k a_l$, where $i+j = k+l$ and $i\oplus j = k\oplus l$, where $0\le i,j,k,l\le 2^n-1$ are n-bit strings and $\oplus$ indicates addition modulo 2.*

For example, 2, 7, 5, and 4 can be written in binary numbers as 010, 111, 101, and 100, respectively. Clearly, $010 + 111(\text{modulo } 2) = 101$, $101 + 100 = 001(\text{modulo } 2)$.

Using this condition it is easy to verify that states $|W\rangle = (1/\sqrt{n})(|2^0\rangle + |2^1\rangle + \cdots + |2^{n-1}\rangle)$ and $|GHZ\rangle = (1/\sqrt{2})(|0^{(n)}\rangle + |1^{(n)}\rangle)$ for an n-qubit system[14] are entangled.

Let $i_1 i_2\cdots i_n$, $j_1 j_2\cdots j_n$, $k_1 k_2\cdots k_n$, and $l_1 l_2\cdots l_n$ be n-bit strings of i, j, k, and l, respectively. Then version 3 is phrased below.

Version 3 *$|\psi\rangle$ is separable if and only if $a_i a_j = a_k a_l$, where $\{i_t, j_t\} = \{k_t, l_t\}$, $t = 1,2,\ldots,n$.*

The following Lemma 1 shows that versions 2 and 3 are equivalent to each other.

Lemma 1 *$i+j = k+l$ and $i\oplus j = k\oplus l$ if and only if $\{i_t, j_t\} = \{k_t, l_t\}$, $t = 1,2,\ldots,n$.*

The proof of Lemma 1 is put in Appendix A.

We argue Version 3 next.

Assume that $|\psi\rangle = (x_0^{(1)}|0\rangle + x_1^{(1)}|1\rangle) \otimes (x_0^{(2)}|0\rangle + x_1^{(2)}|1\rangle) \otimes \ldots \otimes (x_0^{(n)}|0\rangle + x_1^{(n)}|1\rangle)$. By tensor product $x_{i_1}^{(1)} x_{i_2}^{(2)} \cdots x_{i_n}^{(n)} = a_{i_1 i_2 \cdots i_n}$, where $i_t = 0, 1$, $t = 1, 2, \ldots, n$. Then $a_i a_j = x_{i_1}^{(1)} x_{j_1}^{(1)} x_{i_2}^{(2)} x_{j_2}^{(2)} \cdots x_{i_n}^{(n)} x_{j_n}^{(n)}$ and $a_k a_l = x_{k_1}^{(1)} x_{l_1}^{(1)} x_{k_2}^{(2)} x_{l_2}^{(2)} \cdots x_{k_n}^{(n)} x_{l_n}^{(n)}$. Explicitly, $a_i a_j = a_k a_l$ whenever $\{i_t, j_t\} = \{k_t, l_t\}$, $t = 1, 2 \ldots, n$.

Conversely, suppose that $a_i a_j = a_k a_l$ whenever $\{i_t, j_t\} = \{k_t, l_t\}$, $t = 1, 2, \ldots, n$. Let $\left|x_{i_t}^{(t)}\right|^2 = \sum_{i_1, \ldots, i_{t-1}, i_{t+1}, \ldots, i_n \in \{0,1\}} |a_{i_1 i_2, \ldots, i_n}|^2$, where $t = 1, 2, \ldots, n$. We can show $|x_{i_1}^{(1)} x_{i_2}^{(2)} \cdots x_{i_n}^{(n)}|^2 = |a_{i_1 i_2 \cdots i_n}|^2$. We only demonstrate the cases of $n = 2$ and 3 to give the essential ideas of the general case.

When $n = 2$, see section 2. When $n = 3$, see appendix B. The two cases suggest that it be simpler to prove $|x_{i_1}^{(1)} x_{i_2}^{(2)} \cdots x_{i_n}^{(n)}|^2 = |a_{i_1 i_2 \cdots i_n}|^2 \left(\sum |a_{i_1 i_2 \cdots i_n}|^2\right)^{n-1}$. Now we finish the argument for the real number case. It is not hard to extend the result to the complex number case.

4 Separability for a Multi(n)-Partite System with the Same-Dimensional d Subsystems

Assume that each subsystem has the same dimension d. Let $|i_t\rangle$ be the orthonormal basis $|0\rangle$,$|1\rangle$,...,$|(d-1)\rangle$ for the t-th subsystem. Then any pure state $|\psi\rangle$ can be written as $|\psi\rangle = \sum_{i_1, i_2, \ldots, i_n = 0}^{d-1} a_{i_1 i_2 \cdots i_n} |i_1 i_2 \cdots i_n\rangle$. Assume that $|\psi\rangle$ is separable. Then we can write $|\psi\rangle = \left(\sum_{i_1=0}^{d-1} x_{i_1}^{(1)} |i_1\rangle\right) \otimes \left(\sum_{i_2=0}^{d-1} x_{i_2}^{(2)} |i_2\rangle\right) \otimes \cdots \otimes \left(\sum_{i_n=0}^{d-1} x_{i_n}^{(n)} |i_n\rangle\right)$. By tensor product $x_{i_1}^{(1)} x_{i_2}^{(2)} \cdots x_{i_n}^{(n)} = a_{i_1 i_2 \cdots i_n}$, where $i_1, i_2, \ldots, i_n \in \{0, 1, \ldots, (d-1)\}$. Let M_i be $d^{n-1} \times d$ matrices of which each row is of the following form:

$$\left(a_{k_1 k_2 \cdots k_{i-1} 0 k_{i+1} \cdots k_n}, a_{k_1 k_2 \cdots k_{i-1} 1 k_{i+1} \cdots k_n}, \ldots, a_{k_1 k_2 \cdots k_{i-1} (d-1) k_{i+1} \cdots k_n}\right) ,$$

where $k_1, k_2, \ldots, k_n \in \{0, 1, \ldots, (d-1)\}$, and $i = 1, 2, \ldots, n$. Note that M_i are not the usual matrices of the amplitudes of state $|\psi\rangle$.

There are two versions of the separability.

Version 1 *$|\psi\rangle$ is separable if and only if all the 2×2 minor determinants of M_i, $i = 1, 2, \ldots, n$, are zero.*

Version 2 *$|\psi\rangle$ is separable if and only if $a_{i_1 i_2 \cdots i_n} a_{j_1 j_2 \cdots j_n} = a_{k_1 k_2 \cdots k_n} a_{l_1 l_2 \cdots l_n}$, where $\{i_t, j_t\} = \{k_t, l_t\}$, $\rfloor$ $t = 1, 2, \ldots, n$.*

The proof of Version 1 is similar to the one for a bipartite system. The proof of Version 2 is similar to the one for an n-qubit system.

When $n = 2$, the criterion is reduced to the one for a bipartite system. When $d = 2$, the criterion is reduced to the one for an n-qubit system.

Apparently,

$$|a_{i_1 i_2 \cdots i_n} a_{j_1 j_2 \cdots j_n} - a_{k_1 k_2 \cdots k_n} a_{l_1 l_2 \cdots l_n}| ,$$

where $\{i_t, j_t\} = \{k_t, l_t\}$, $t = 1, 2, \ldots, n.$, is just a deviation from a product state. Let

$$D_E(|\psi\rangle) = \sum |a_{i_1 i_2 \cdots i_n} a_{j_1 j_2 \cdots j_n} - a_{k_1 k_2 \cdots k_n} a_{l_1 l_2 \cdots l_n}|^2 , \tag{4}$$

where $\{i_t, j_t\} = \{k_t, l_t\}$, $t = 1, 2, \ldots, n$. Then $D_E(|\psi\rangle)$ has the following properties.

Property 1 $D_E(|\psi\rangle) = 0$ if and only if $|\psi\rangle$ is separable.

For a two-qubit system, let $|\psi\rangle = a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle$. Then $D_E(|\psi\rangle) = |ad - bc|^2$ and the following Properties 2 and 3 hold.

Property 2 The maximum of

$$D_E(|\psi\rangle) = |ad - bc|^2 \leq (|ad| + |bc|)^2 \leq \left(\frac{|a|^2 + |d|^2}{2} + \frac{|b|^2 + |c|^2}{2}\right)^2 = \frac{1}{4} .$$

When a, b, c, and d are real, by computing extremum it is derived that $D_E(|\psi\rangle)$ has the maximum at states of the forms: $x|00\rangle + y|01\rangle - y|10\rangle + x|11\rangle$ or $x|00\rangle + y|01\rangle + y|10\rangle - x|11\rangle$.

Property 3 $|\psi\rangle \sim |\psi'\rangle$ if and only if $D_E(|\psi\rangle) = D_E(|\psi'\rangle)$.

Given $|\psi\rangle = a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle$ and $|\psi'\rangle = a'|00\rangle + b'|01\rangle + c'|10\rangle + d'|11\rangle$. Suppose that $|\psi\rangle \sim |\psi'\rangle$. By the necessary condition in Sec. 5, $D_E(|\psi\rangle) = D_E(|\psi'\rangle)$.

Conversely, suppose $D_E(|\psi\rangle) = D_E(|\psi'\rangle)$. Let us show $|\psi\rangle \sim |\psi'\rangle$. Using Schmidt decomposition, we can write $|\psi\rangle \sim \sqrt{\lambda_1}|00\rangle + \sqrt{\lambda_2}|11\rangle$, where $\lambda_1 + \lambda_2 = 1$. As discussed above, $|ad - bc| = \sqrt{\lambda_1}\sqrt{\lambda_2}$. As well using Schmidt decomposition we can write $|\psi'\rangle \sim \sqrt{\rho_1}|00\rangle + \sqrt{\rho_2}|11\rangle$, where $\rho_1 + \rho_2 = 1$, and $|a'd' - b'c'| = \sqrt{\rho_1}\sqrt{\rho_2}$. Thus $\lambda_1\lambda_2 = \rho_1\rho_2$. Then $\lambda_1(1-\lambda_1) = \rho_1(1-\rho_1)$. There are two cases. (i) $\lambda_1 = \rho_1$, then $\lambda_2 = \rho_2$. (ii) $\lambda_1 + \rho_1 + 1 = 0$. In the case $\lambda_2 = \rho_1$ and $\lambda_1 = \rho_2$. It means that $|\psi\rangle$ and $|\psi'\rangle$ have the same Schmidt coefficient for either of the two cases. By factor 5 in Ref. [5], $|\psi\rangle \sim |\psi'\rangle$.

Nielsen in Ref. [15] showed $|\psi'\rangle \sim |\psi''\rangle$ by calculating eigenvalue, where $|\psi'\rangle = \sqrt{\alpha_+}|00\rangle + \sqrt{\alpha_-}|11\rangle$, and $|\psi''\rangle = (|00\rangle + |1\rangle(\cos\gamma|0\rangle + \sin\gamma|1\rangle))/\sqrt{2}$. By Property 3 it only needs to check $\sqrt{\alpha_+}\sqrt{\alpha_-} = \sin\gamma/2$.

5 A Necessary Condition for a Local Unitary Equivalence Class for a Bipartite System

We use the following Lemma 2 to establish the necessary condition.

Lemma 2 Let $|\psi\rangle$ be a pure state of a composite system AB possessed by both Alice and Bob. Assume that each subsystem has the same dimension n. Let $M = (a_{jk})_{n\times n}$ be the matrix of the amplitudes of $|\psi\rangle$. Let $\rho^{\rm AB} = |\psi\rangle\langle\psi|$ and $\rho^{\rm A} = {\rm tr}_{\rm B}(\rho^{\rm AB})$. Then $|\det(M)|^2$ is just the product of the eigenvalues of $\rho^{\rm A}$.

The proof is put in Appendix C.

Lemma 2 reveals the relation between the determinant of the matrix of the amplitudes and the eigenvalues of $\rho^{\rm A}$ for a bipartite system.

The corollary of Lemma 2

Let M_ψ (M_ϕ) be the matrix of the amplitudes of a pure state $|\psi\rangle$ ($|\phi\rangle$) of a composite system AB. Assume that each subsystem has the same dimension n. Then $|\det(M_\psi)| = |\det(M_\phi)|$ whenever $|\psi\rangle \sim |\phi\rangle$. That is, $|\det(M_\psi)|$ is invariant under local unitary operators.

It is well known that it only needs $O(n^3)$ multiplication operations to compute $|\det(M)|$ instead of doing Schmidt decomposition in Refs. [2] and [15].

For a two-qubit system, let $|\psi\rangle = a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle$ and $\rho^{12} = |\psi\rangle\langle\psi|$. By lemma 2 $|ad-bc|^2$ is the product of the eigenvalues of ρ^1. Let $|ad - bc| = \epsilon$. We can show that ϵ satisfies $0 \le \epsilon \le 1/2$ and eigenvalues $\lambda_\pm = \frac{1\pm\sqrt{1-4\epsilon^2}}{2}$. Hence, $|\psi\rangle \sim \sqrt{\lambda_+}|00\rangle + \sqrt{\lambda_-}|11\rangle$ or $|\psi\rangle \sim \sqrt{\lambda_-}|00\rangle + \sqrt{\lambda_+}|11\rangle$.

6 Conclusion

In this paper we have presented the necessary and sufficient conditions of separability for multipartite pure states. These conditions do not require Schmidt decomposition (for two subsystems) or tracing out operations. By using the conditions it is easy to check whether or not a multipartite pure state is entangled.

Appendix A: The Proof of Lemma 1

Let $\alpha_1\alpha_2\cdots\alpha_n$, $\beta_1\beta_2\cdots\beta_n$, $\delta_1\delta_2\cdots\delta_n$, and $\gamma_1\gamma_2\cdots\gamma_n$ be the n-bit strings of α, β, δ, and γ, respectively.

Lemma 3 $\{\alpha_i, \beta_i\} = \{\delta_i, \gamma_i\}$, $i = 1, 2, \ldots, n$, if and only if $\alpha + \beta = \delta + \gamma$ and $\alpha \oplus \beta = \delta \oplus \gamma$, where $\oplus$ indicates addition modulo 2.

Proof Suppose $\{\alpha_i, \beta_i\} = \{\delta_i, \gamma_i\}$, $i = 1, 2, \ldots, n$. Since

$$\alpha + \beta = (\alpha_1 + \beta_1)2^{n-1} + (\alpha_2 + \beta_2)2^{n-2} + \cdots + (\alpha_n + \beta_n)$$

and

$$\delta + \gamma = (\delta_1 + \gamma_1)2^{n-1} + (\delta_2 + \gamma_2)2^{n-2} + \cdots + (\delta_n + \gamma_n)\,,$$

by the supposition it is easy to see $\alpha + \beta = \delta + \gamma$. It is straightforward to obtain

$$\alpha_1\alpha_2\cdots\alpha_n \oplus \beta_1\beta_2\cdots\beta_n = \delta_1\delta_2\cdots\delta_n \oplus \gamma_1\gamma_2\cdots\gamma_n\,.$$

Conversely, suppose $\alpha + \beta = \delta + \gamma$ and $\alpha \oplus \beta = \delta \oplus \gamma$. First let us consider the case where $n = 1$. There are three cases

(i) $\alpha_1 + \beta_1 = \delta_1 + \gamma_1 = 0$. This means $\alpha_1 = \beta_1 = \delta_1 = \gamma_1 = 0$.

(ii) $\alpha_1 + \beta_1 = \delta_1 + \gamma_1 = 1$. This implies $\{\alpha_1, \beta_1\} = \{\delta_1, \gamma_1\} = \{1, 0\}$.

(iii) $\alpha_1 + \beta_1 = \delta_1 + \gamma_1 = 2$. This says $\alpha_1 = \beta_1 = \delta_1 = \gamma_1 = 1$.

No matter which of the above three cases happens, it yields $\{\alpha_1, \beta_1\}$=$\{\delta_1, \gamma_1\}$.

Let us consider the case n. Since

$$\alpha+\beta=\delta+\gamma,\quad (\alpha_1+\beta_1)2^{n-1}+(\alpha_2+\beta_2)2^{n-2}+\cdots+(\alpha_n+\beta_n)=(\delta_1+\gamma_1)2^{n-1}+(\delta_2+\gamma_2)2^{n-2}+\cdots+(\delta_n+\gamma_n)\,.$$

Again since $\alpha\oplus\beta=\delta\oplus\gamma$, that is,

$$\alpha_1\alpha_2\cdots\alpha_n\oplus\beta_1\beta_2\cdots\beta_n=\delta_1\delta_2\cdots\delta_n\oplus\gamma_1\gamma_2\cdots\gamma_n\,,$$

we obtain $\alpha_i\oplus\beta_i=\delta_i\oplus\gamma_i$, $i=1,2,\ldots,n$. There are two cases.

(i) $\alpha_n\oplus\beta_n=\delta_n\oplus\gamma_n=1$. In the case $\{\alpha_n,\,\beta_n\}=\{\delta_n,\,\gamma_n\}=\{0,1\}$. Then

$$(\alpha_1+\beta_1)2^{n-2}+(\alpha_2+\beta_2)2^{n-3}+\cdots+(\alpha_{n-1}+\beta_{n-1})=(\delta_1+\gamma_1)2^{n-2}+(\delta_2+\gamma_2)2^{n-3}+\cdots+(\delta_{n-1}+\gamma_{n-1})$$

and $\alpha_i\oplus\beta_i=\delta_i\oplus\gamma_i$, $i=1,2,\ldots,n-1$. By induction hypothesis $\{\alpha_i,\beta_i\}=\{\delta_i,\gamma_i\}$, $i=1,2,\ldots,n-1$.

(ii) $\alpha_n\oplus\beta_n=\delta_n\oplus\gamma_n=0$. There are two subcases.

(iia) $\alpha_n=\beta_n=\delta_n=\gamma_n=0$ or $\alpha_n=\beta_n=\delta_n=\gamma_n=1$. As discussed in case (i), we can obtain $\{\alpha_i,\beta_i\}=\{\delta_i,\gamma_i\}$, $i=1,2,\ldots,n-1$ by induction hypothesis.

(iib) $\alpha_n=\beta_n=1$ and $\delta_n=\gamma_n=0$ or $\alpha_n=\beta_n=0$ and $\delta_n=\gamma_n=1$. Let us consider the former case. In the case

$$\begin{aligned}&(\alpha_1+\beta_1)2^{n-2}+(\alpha_2+\beta_2)2^{n-3}+\cdots+(\alpha_{n-2}+\beta_{n-2})2+(\alpha_{n-1}+\beta_{n-1}+1)\\&\quad=(\delta_1+\gamma_1)2^{n-2}+(\delta_2+\gamma_2)2^{n-3}+\cdots+(\delta_{n-2}+\gamma_{n-2})2+(\delta_{n-1}+\gamma_{n-1})\,.\end{aligned}$$

Since $\alpha_{n-1}\oplus\beta_{n-1}=\delta_{n-1}\oplus\gamma_{n-1}$, either $\alpha_{n-1}\oplus\beta_{n-1}=\delta_{n-1}\oplus\gamma_{n-1}=0$ or 1 causes that one of $(\alpha_{n-1}+\beta_{n-1}+1)$ and $(\delta_{n-1}+\gamma_{n-1})$ is odd and the other is even. It contradicts $\alpha\oplus\beta=\delta\oplus\gamma$.

Appendix B: The Separability for an n-Qubit System

When $n=3$, let us show $|x_{i_1}^{(1)}x_{i_2}^{(2)}x_{i_3}^{(3)}|^2=|a_{i_1i_2i_3}|^2$, when $a_ia_j=a_ka_l$, where $\{i_t,j_t\}=\{k_t,l_t\}$, $t=1,2,3$. We only illustrate $|x_0^{(1)}x_0^{(2)}x_0^{(3)}|^2=|a_{000}|^2$. Other cases then follow readily. Experientially, it is simpler to prove

$$|x_0^{(1)}x_0^{(2)}x_0^{(3)}|^2=|a_{000}|^2\left(\sum_{i,j,k\in\{0,1\}}|a_{ijk}|^2\right)\left(\sum_{i,j,k\in\{0,1\}}|a_{ijk}|^2\right)\,,$$

where $|x_0^{(1)}|^2=\sum_{i,j\in\{0,1\}}|a_{0ij}|^2$, $|x_0^{(2)}|^2=\sum_{k,l\in\{0,1\}}|a_{k0l}|^2$, and $|x_0^{(3)}|^2=\sum_{p,q\in\{0,1\}}|a_{pq0}|^2$.

First we show that $a_{0ij}a_{k0l}a_{pq0}$ can be rewritten as $a_{000}a_{\alpha_1\alpha_2\alpha_3}a_{\delta_1\delta_2\delta_3}$. There are the following four cases.

(i) Consider $a_{0ij}a_{k0l}$ and the pairs $\{0,k\},\{i,0\}$ and $\{j,l\}$. If $j*l=0$, then $a_{0ij}a_{k0l}=a_{000}a_{ki(j+l)}$ since $\{j,l\}=\{0,j+l\}$.

(ii) Consider $a_{0ij}a_{pq0}$ and the pairs $\{0,p\},\{i,q\}$ and $\{j,0\}$. If $i*q=0$, then $a_{0ij}a_{pq0}=a_{000}a_{p(i+q)j}$ since $\{i,q\}=\{0,i+q\}$.

(iii) Consider $a_{k0l}a_{pq0}$ and the pairs $\{k,p\},\{0,q\}$ and $\{l,0\}$. If $k*p=0$, then $a_{k0l}a_{pq0}=a_{000}a_{(k+p)ql}$ since $\{k,p\}=\{0,k+p\}$.

(iv) Otherwise $i=j=l=k=p=q=1$. It is not hard to derive $a_3a_5a_6=a_1a_7a_6=a_0a_7^2$.

Second, let us show that $a_{000}a_{\alpha_1\alpha_2\alpha_3}a_{\delta_1\delta_2\delta_3}$ can be rewritten as $a_{0ij}a_{k0l}a_{pq0}$. If $a_{000}a_{\alpha_1\alpha_2\alpha_3}a_{\delta_1\delta_2\delta_3}$ is of the forms: $a_{000}a_{0ij}a_{k0l}$, $a_{000}a_{0ij}a_{pq0}$ or $a_{000}a_{k0l}a_{pq0}$, then these forms are desired. Otherwise $a_{000}a_{\alpha_1\alpha_2\alpha_3}a_{\delta_1\delta_2\delta_3}$ must be $a_0a_6a_6$, $a_0a_3a_3$, $a_0a_5a_5$ or of the form $a_0a_7a_{rst}$, which can be rewritten as $a_2a_4a_6$, $a_1a_2a_3$, $a_1a_4a_5$, $a_1a_6a_{rst}$, respectively. $a_2a_4a_6$, $a_1a_2a_3$ and $a_1a_4a_5$ are just desired and $a_1a_6a_{rst}$ is furthermore rewritten as follows. There are three cases.

(i) In the case $r=0$ or $s=0$, this is desired.

(ii) In the case $r=s=t=1$, $a_1a_6a_7=a_3a_5a_6$, desired.

(iii) In the case $r=s=1$ and $t=0$, $a_1a_6a_6=a_2a_5a_6$, desired.

Appendix C: The Proof of Lemma 2

Proof Suppose that systems A and B have the same dimensions n. Let $|\psi\rangle=\sum_{i,j=0}^{n-1}a_{ij}|i\rangle|j\rangle$. Then $M=(a_{ij})_{n\times n}$. Let density operator $\rho^{\mathrm{AB}}=|\psi\rangle\langle\psi|$. Then

$$\rho^{\mathrm{AB}}=\left(\sum_{i,j=0}^{n-1}a_{ij}|i\rangle|j\rangle\right)\left(\sum_{l,k=0}^{n-1}a_{lk}^*\langle l|\langle k|\right)=\sum_{i,j=0}^{n-1}\sum_{l,k=0}^{n-1}a_{ij}a_{lk}^*|i\rangle|j\rangle\langle l|\langle k|=\sum_{i,l=0}^{n-1}\sum_{j,k=0}^{n-1}a_{ij}a_{lk}^*|i\rangle|j\rangle\langle l|\langle k|\,.$$

The reduced density operator for system A is defined by $\rho^{\rm A} = {\rm tr}_{\rm B}(\rho^{\rm AB})$. Let us compute $\rho^{\rm A}$.

$\rho^{\rm A} = \sum_{i,l=0}^{n-1}\sum_{j,k=0}^{n-1} a_{ij}a_{lk}^{*}|i\rangle\langle l|\delta_{kj}$ (where $\delta_{kj} = 1$ when $k = j$. Otherwise 0.) $= \sum_{i,l=0}^{n-1}\sum_{j=0}^{n-1} a_{ij}a_{lj}^{*}|i\rangle\langle l| = \sum_{i,l=0}^{n-1}(\sum_{j=0}^{n-1} a_{ij}a_{lj}^{*})|i\rangle\langle l|$. Let $A_i = (a_{i0}, a_{i1}, \ldots, a_{i(n-1)})$, that is, the i-th row of A. Then $\sum_{j=0}^{n-1} a_{ij}a_{lj}^{*} = A_i A_l^{\dagger}$. Finally

$$\rho^{\rm A} = \sum_{i,l=0}^{n-1} A_i A_l^{\dagger}|i\rangle\langle l| = \begin{pmatrix} A_0 \\ A_1 \\ \vdots \\ A_{n-1} \end{pmatrix} (A_0^{\dagger}, A_1^{\dagger}, \ldots, A_{n-1}^{\dagger}) = MM^{\dagger}\,.$$

Thus $\det(\rho^{A}) = |\det(M)|^2$. Hence $|\det(M)|^2$ is just the product of the eigenvalues of ρ^{A}. Q.E.D.

References

[1] M.A. Nielsen and I.L. Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press, Cambridge, England (2000) p. 109.

[2] A. Peres, Phys. Rev. Lett. **77** (1996) 1413.

[3] M. Horodecki, *et al.*, Phys. Lett. A **223** (1996)1.

[4] M. Horodecki, *et al.*, Phys. Rev. A **59** (1999) 4206.

[5] N.J. Cerf, *et al.*, Phys. Rev. A **60** (1999) 898.

[6] S. Wu, *et al.*, Phys. Lett. A **275** (2000) 244.

[7] Ping-Xing Chen, *et al.*, Phys. Rev. A **63** (2001) 052306.

[8] T. Eggeling, *et al.*, e-print quant-ph/0103003.

[9] D.A. Meyer and N. R. Wallach, J. Math. Phys. **43** (2002) 4273.

[10] M. Raymer, *et al.*, Phys. Rev. A **67** (2003) 052104.

[11] D. Li, *et al.*, quant-ph/0604147. This paper was submitted to PRL in September 2004. Paper No. is LV9637. Finally, it was not accepted by PRL.

[12] L. Lamata, *et al.*, Phys. Rev. A **74** (2006) 052336. Also see, quant-ph/0603243.

[13] L. Lamata, *et al.*, Phys. Rev. A **75** (2007) 022318.

[14] W. Dür, *et al.*, Phys. Rev. A **62** (2000) 062314.

[15] M.A. Nielsen, Phys. Rev. Lett. **83** (1999) 436.