Vol 17 No 9, September 2008
1674-1056/2008/17(09)/3194-04

Chinese Physics B

© 2008 Chin. Phys. Soc.
and IOP Publishing Ltd

Indistinguishability of orthogonal time-separated bell states*

Tan Yong-Gang(谭勇刚)[a)b)], Cai Qing-Yu(蔡庆宇)[a)†], and Shi Ting-Yun(史庭云)[a)]

[a)] *State Key Laboratory of Magnetic Resonances and Atomic and Molecular Physics, Wuhan Institute of Physics and Mathematics, Chinese Academy of Sciences, Wuhan* 430071, *China*
[b)] *Graduate University of the Chinese Academy of Sciences, Beijing* 100049, *China*

(Received 5 November 2007; revised manuscript received 10 December 2007)

This paper proves that it is impossible to identify orthogonally time-separated Bell states. If two qubits of a Bell state interact with the measurement apparatus at different time, any attempt to identify this state will disturb it.

Keywords: Bell states, time-separated, indistinguishability
PACC: 0365, 0367

1. Introduction

A quantum state contains hidden information which may be accessible to measurement, therefore distinguishing a quantum state plays a key role in quantum computation and quantum cryptography. In quantum information theory, the indistinguishability of non-orthogonal quantum states is the foundation of quantum cryptography.[1] As is well known, nonorthogonal states cannot be distinguished,[2] which is equivalent to the description of the famous no-cloning theorem.[3] On the other hand, we can exactly distinguish orthogonal states with projective measurement. However, for multisystems which are spatially separated, local information of the density matrices, and even local operations and classical communication (LOCC), are not sufficient to distinguish among orthogonal states. It has been proven that all the four orthogonal Bell states, which are in canonical form, can be identified with LOCC if and only if two copies of each of the states are provided.[4] In general, an orthogonal multisystem state with a single copy can never be identified if only LOCC are permitted.

Here we consider that two qubits of a Bell state interact with the measurement apparatus one after the other, i.e. the two qubits are measured at different time, which we call it time-separated Bell state (this time-separated Bell states may be more general than the spatially separated Bell states, since time-separated Bell states also implies two qubits are in different positions at the same time, while time-separated two qubits can be measured by one measurement apparatus at different time). Is it possible to distinguish orthogonally time-separated Bell states? In this paper, we prove that it is impossible to distinguish orthogonally time-separated Bell states without disturbing them.

2. Indistinguishability of time-separated Bell states

As is well known, the four Bell states $|\Psi^{\pm}\rangle$, $|\Phi^{\pm}\rangle$ are mutually orthogonal to each other, where $|\Psi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|0\rangle|1\rangle \pm |1\rangle|0\rangle)$, and $|\Phi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|0\rangle|0\rangle \pm |1\rangle|1\rangle)$. Anyone who only accesses one qubit cannot distinguish the Bell state since $\rho_{\rm A}^{\pm} := {\rm tr_B}\{|\Psi^{\pm}\rangle\langle\Psi^{\pm}|\} = {\rm tr_B}\{|\Phi^{\pm}\rangle\langle\Phi^{\pm}|\} = \frac{1}{2}(|0\rangle\langle 0| + |1\rangle\langle 1|)_{\rm A}$. Suppose Alice wants to send a Bell state to Bob and Eve wants to identify Alice's state. And Alice sends her two qubits to Bob at different time slots. That is to say, Eve is not allowed to achieve Alice's two qubits simultaneously. Can Eve identify Alice's state without disturbing it?

In practice, Alice will select her Bell states randomly, i.e. the states are maximally mixed for anyone who is outside Alice's laboratory,

$$\rho = \frac{1}{4}(|\Psi^{+}\rangle\langle\Psi^{+}| + |\Psi^{-}\rangle\langle\Psi^{-}| + |\Phi^{+}\rangle\langle\Phi^{+}| + |\Phi^{-}\rangle\langle\Phi^{-}|).$$

*Project supported by the National Natural Science Foundation of China (Grant No 10504039) and the Youth Chenguang Project of Science and Technology of Wuhan City of China.
†E-mail: qycai@wipm.ac.cn

One can suppose that Alice selects $|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|0\rangle_a|1\rangle_b - |1\rangle_a|0\rangle_b)$ this time, here a and b denote qubit a and qubit b respectively. Eve's most general operations can be represented by an unitary operation together with a measurement:[5] when the qubits a and b pass through Eve's area one after the other, the qubit a will interact with Eve's ancilla $|\Sigma\rangle_a$, and the qubit b will interact with Eve's ancilla $|\Sigma\rangle_b$, respectively. After the interactions, Eve measures her ancilla $|\Sigma\rangle_a$ and $|\Sigma\rangle_b$ to identify Alice's state. The initial state of the joint systems, including the EPR pair and Eve's ancilla, is

$$|\Psi^-\rangle \otimes |\Sigma\rangle_a \otimes |\Sigma\rangle_b.$$

The interaction between Alice's qubit a and Eve's ancilla $|\Sigma\rangle_a$ may be described as

$$\begin{aligned} U_a|0\rangle_a|\Sigma\rangle_a &= |0\rangle_a|\Sigma_{00}\rangle_a + |1\rangle_a|\Sigma_{01}\rangle_a, \\ U_a|1\rangle_a|\Sigma\rangle_a &= |1\rangle_a|\Sigma_{10}\rangle_a + |0\rangle_a|\Sigma_{11}\rangle_a, \end{aligned}$$

and the interaction between qubit b and $|\Sigma\rangle_b$ is

$$\begin{aligned} U_b|0\rangle_b|\Sigma\rangle_b &= |0\rangle_b|\Sigma_{00}\rangle_b + |1\rangle_b|\Sigma_{01}\rangle_b, \\ U_b|1\rangle_b|\Sigma\rangle_b &= |1\rangle_b|\Sigma_{10}\rangle_b + |0\rangle_b|\Sigma_{11}\rangle_b. \end{aligned}$$

Without loss of generality, we can assume ${}_i\langle\Sigma_{00}|\Sigma_{01}\rangle_i = 0$, ${}_i\langle\Sigma_{10}|\Sigma_{11}\rangle_i = 0$, where $i = a, b$. (In fact, the evolution of Alice's qubit can be completely described by using an ancilla no more than 4 dimensions together with a jointly unitary operation. If the ancilla is in the state $|\Sigma\rangle$ initially. With the jointly unitary operation, we can obtain $U|0\rangle|\Sigma\rangle = |0\rangle|\Sigma_{00}\rangle + |1\rangle|\Sigma_{01}\rangle$ and $U|1\rangle|\Sigma\rangle = |1\rangle|\Sigma_{10}\rangle + |0\rangle|\Sigma_{11}\rangle$. After the unitary evolution, Eve will perform a measurement on the ancilla to gain the information about the qubit. Her measurement may be a projective measurement or a more general positive operator value measurement (POVM). However, no matter what measurement Eve performs, she cannot distinguish the nonorthogonal states. Then she has to make $|\Sigma_{00}\rangle$, $|\Sigma_{01}\rangle$, $|\Sigma_{10}\rangle$ and $|\Sigma_{11}\rangle$ different, at least one of them should be different from the others. Otherwise, she cannot gain any information from the ancilla. So, it is reasonable to assume that $\langle\Sigma_{00}|\Sigma_{01}\rangle = 0$. Considering the symmetry, we can also assume that $\langle\Sigma_{10}|\Sigma_{11}\rangle = 0$. On the other hand, even if Eve has set $\langle\Sigma_{00}|\Sigma_{01}\rangle = 0$ and $\langle\Sigma_{10}|\Sigma_{11}\rangle = 0$ before unitary operation, she can still control the states of the ancilla freely by modifying the four parameters $\langle\Sigma_{00}|\Sigma_{00}\rangle$, $\langle\Sigma_{10}|\Sigma_{10}\rangle$, $\langle\Sigma_{00}|\Sigma_{10}\rangle$ and $\langle\Sigma_{01}|\Sigma_{11}\rangle$ since they are still open for Eve.) Taking the inner products of the equations above, we can obtain that

$$\begin{aligned} {}_a\langle\Sigma_{00}|\Sigma_{00}\rangle_a + {}_a\langle\Sigma_{01}|\Sigma_{01}\rangle_a &= 1, \\ {}_a\langle\Sigma_{10}|\Sigma_{10}\rangle_a + {}_a\langle\Sigma_{11}|\Sigma_{11}\rangle_a &= 1, \\ {}_b\langle\Sigma_{00}|\Sigma_{00}\rangle_b + {}_b\langle\Sigma_{01}|\Sigma_{01}\rangle_b &= 1, \\ {}_b\langle\Sigma_{10}|\Sigma_{10}\rangle_b + {}_b\langle\Sigma_{11}|\Sigma_{11}\rangle_b &= 1, \end{aligned}$$

and

$$\begin{aligned} {}_a\langle\Sigma_{00}|\Sigma_{11}\rangle_a + {}_a\langle\Sigma_{01}|\Sigma_{10}\rangle_a &= 0, \\ {}_b\langle\Sigma_{00}|\Sigma_{11}\rangle_b + {}_b\langle\Sigma_{01}|\Sigma_{10}\rangle_b &= 0. \end{aligned}$$

After both of the two qubits passed Eve's area, the joint states of the EPR pairs and the ancilla are

$$\rho_{ab\Sigma_{ab}} = U_aU_b|\Psi^-\rangle_{ab}|\Sigma\rangle_a|\Sigma\rangle_b{}_b\langle\Sigma|_a\langle\Sigma|_{ab}\langle\Psi^-|U_b^+U_a^+.$$

After the interaction can be obtained by tracing out Eve's ancilla, the density matrix of the EPR pairs is

$$\rho_{ab} = \mathrm{Tr}_{\Sigma_{ab}}\rho_{ab\Sigma_{ab}}.$$

And the density matrix of the associate probes $\rho_{\Sigma_{ab}}$ can be obtained by tracing out the EPR pair

$$\rho_{\Sigma_{ab}} = \mathrm{Tr}_{ab}\rho_{ab\Sigma_{ab}}.$$

The state of the EPR pair after the interaction are

$$\begin{aligned} \rho_{ab} &= \mathrm{Tr}_{\Sigma_a\Sigma_b}(U|\Psi^-\rangle_{ab}|\Sigma\rangle_a|\Sigma\rangle_b{}_b\langle\Sigma|_a\langle\Sigma|_{ab}\langle\Psi^-|U^+) \\ &= \frac{1}{2}|0\rangle_a|1\rangle_{ba}\langle 0|_b\langle 1|(g_{0a}^2g_{1b}^2 + g_{0a}^2u_b^2 + u_a^2g_{1b}^2 + u_a^2u_b^2) \\ &\quad -\frac{1}{2}|0\rangle_a|1\rangle_{ba}\langle 1|_b\langle 0|(g_{0a}u_ag_{1b}u_b + g_{0a}u_ag_{0b}u_b + g_{1a}u_ag_{1b}u_b + g_{1a}u_ag_{0b}u_b) \\ &\quad +\frac{1}{2}|0\rangle_a|0\rangle_{ba}\langle 0|_b\langle 0|(g_{0a}^2h_{1b}^2 + g_{1a}^2v_b^2 + u_a^2h_{1b}^2 + u_a^2v_b^2) \\ &\quad -\frac{1}{2}|0\rangle_a|0\rangle_{ba}\langle 1|_b\langle 1|(g_{0a}u_ah_{0b}v_b + g_{0a}u_ah_{1b}v_b + g_{1a}u_ah_{0b}v_b + g_{1a}u_ah_{1b}v_b) \end{aligned}$$

$$
\begin{aligned}
&+\frac{1}{2}|1\rangle_a|1\rangle_{ba}\langle 1|_b\langle 1|(h_{0a}^2g_{1b}^2+h_{0a}^2u_b^2+v_a^2g_{1b}^2+v_a^2u_b^2)\\
&-\frac{1}{2}|1\rangle_a|1\rangle_{ba}\langle 0|_b\langle 0|(h_{0a}v_ag_{0b}u_b+g_{0a}u_ah_{1b}v_b+g_{1a}u_ah_{0b}v_b+g_{1a}u_ah_{1b}v_b)\\
&+\frac{1}{2}|1\rangle_a|0\rangle_{ba}\langle 1|_b\langle 0|(h_{0a}^2h_{1b}^2+h_{0a}^2v_b^2+v_a^2h_{1b}^2+v_a^2v_b^2)\\
&-\frac{1}{2}|1\rangle_a|0\rangle_{ba}\langle 0|_b\langle 1|(h_{0a}v_ah_{0b}v_b+g_{0a}u_ah_{1b}v_b+g_{1a}u_ah_{0b}v_b+g_{1a}u_ah_{1b}v_b)\\
&-\frac{1}{2}|1\rangle_a|0\rangle_{ba}\langle 0|_b\langle 1|(g_{0a}u_ag_{0b}u_b+g_{0a}u_ag_{1b}u_b+g_{1a}u_ag_{0b}u_b+g_{1a}u_ag_{1b}u_b)\\
&+\frac{1}{2}|1\rangle_a|0\rangle_{ba}\langle 1|_b\langle 0|(g_{1a}^2g_{0b}^2+g_{1a}^2u_b^2+u_a^2g_{0b}^2+u_a^2u_b^2)\\
&-\frac{1}{2}|1\rangle_a|1\rangle_{ba}\langle 0|_b\langle 0|(g_{0a}u_ah_{0b}v_b+g_{0a}u_ah_{1b}v_b+g_{1a}u_ah_{0b}v_b+g_{1a}u_ah_{1b}v_b)\\
&+\frac{1}{2}|1\rangle_a|1\rangle_{ba}\langle 1|_b\langle 1|(g_{1a}^2h_{0b}^2+g_{1a}^2v_b^2+u_a^2h_{0b}^2+u_a^2v_b^2)\\
&-\frac{1}{2}|0\rangle_a|0\rangle_{ba}\langle 1|_b\langle 1|(h_{0a}v_ag_{0b}u_b+h_{0a}v_ag_{1b}u_b+h_{1a}v_ag_{0b}u_b+h_{1a}v_ag_{1b}u_b)\\
&+\frac{1}{2}|0\rangle_a|0\rangle_{ba}\langle 0|_b\langle 0|(h_{1a}^2g_{0b}^2+h_{1a}^2u_b^2+v_a^2g_{0b}^2+v_a^2u_b^2)\\
&-\frac{1}{2}|0\rangle_a|1\rangle_{ba}\langle 1|_b\langle 0|(h_{0a}v_ah_{0b}v_b+h_{0a}v_ah_{1b}v_b+h_{1a}v_ah_{0b}v_b+h_{1a}v_ah_{1b}v_b)\\
&+\frac{1}{2}|0\rangle_a|1\rangle_{ba}\langle 0|_b\langle 1|(h_{1a}^2h_{1b}^2+v_a^2h_{1b}^2+h_{1a}^2v_b^2+v_a^2v_b^2),
\end{aligned}
$$

where $g_{0i}={}_i\langle\Sigma_{00}|\Sigma_{00}\rangle_i$, $g_{1i}={}_i\langle\Sigma_{10}|\Sigma_{10}\rangle_i$, $h_{0i}={}_i\langle\Sigma_{01}|\Sigma_{01}\rangle_i$ and $h_{1i}={}_i\langle\Sigma_{11}|\Sigma_{11}\rangle_i$ are normalized factors, and $u_i={}_i\langle\Sigma_{00}|\Sigma_{10}\rangle_i$, $v_i={}_i\langle\Sigma_{01}|\Sigma_{11}\rangle_i$, $i=a,b$. The states of the Eve's two ancilla are

$$
\begin{aligned}
\rho_{\Sigma_{ab}} &= \mathrm{Tr}_{ab}(U|\Psi^-\rangle_{ab}|\Sigma\rangle_a|\Sigma\rangle_{bb}\langle\Sigma|_a\langle\Sigma|_{ab}\langle\Psi^-|U^+)\\
&= \frac{1}{2}|\Sigma_{00}\rangle_a|\Sigma_{10}\rangle_{ba}\langle\Sigma_{00}|_b\langle\Sigma_{10}|-\frac{1}{2}|\Sigma_{00}\rangle_a|\Sigma_{10}\rangle_{ba}\langle\Sigma_{11}|_b\langle\Sigma_{01}|\\
&\quad+\frac{1}{2}|\Sigma_{00}\rangle_a|\Sigma_{11}\rangle_{ba}\langle\Sigma_{00}|_b\langle\Sigma_{11}|-\frac{1}{2}|\Sigma_{00}\rangle_a|\Sigma_{11}\rangle_{ba}\langle\Sigma_{11}|_b\langle\Sigma_{00}|\\
&\quad+\frac{1}{2}|\Sigma_{01}\rangle_a|\Sigma_{10}\rangle_{ba}\langle\Sigma_{01}|_b\langle\Sigma_{10}|-\frac{1}{2}|\Sigma_{01}\rangle_a|\Sigma_{10}\rangle_{ba}\langle\Sigma_{10}|_b\langle\Sigma_{01}|\\
&\quad+\frac{1}{2}|\Sigma_{01}\rangle_a|\Sigma_{11}\rangle_{ba}\langle\Sigma_{01}|_b\langle\Sigma_{11}|-\frac{1}{2}|\Sigma_{01}\rangle_a|\Sigma_{11}\rangle_{ba}\langle\Sigma_{10}|_b\langle\Sigma_{00}|\\
&\quad-\frac{1}{2}|\Sigma_{10}\rangle_a|\Sigma_{00}\rangle_{ba}\langle\Sigma_{01}|_b\langle\Sigma_{11}|+\frac{1}{2}|\Sigma_{10}\rangle_a|\Sigma_{00}\rangle_{ba}\langle\Sigma_{10}|_b\langle\Sigma_{00}|\\
&\quad-\frac{1}{2}|\Sigma_{10}\rangle_a|\Sigma_{01}\rangle_{ba}\langle\Sigma_{01}|_b\langle\Sigma_{10}|+\frac{1}{2}|\Sigma_{10}\rangle_a|\Sigma_{01}\rangle_{ba}\langle\Sigma_{10}|_b\langle\Sigma_{01}|\\
&\quad-\frac{1}{2}|\Sigma_{11}\rangle_a|\Sigma_{00}\rangle_{ba}\langle\Sigma_{00}|_b\langle\Sigma_{11}|+\frac{1}{2}|\Sigma_{11}\rangle_a|\Sigma_{00}\rangle_{ba}\langle\Sigma_{11}|_b\langle\Sigma_{00}|\\
&\quad-\frac{1}{2}|\Sigma_{11}\rangle_a|\Sigma_{01}\rangle_{ba}\langle\Sigma_{00}|_b\langle\Sigma_{10}|+\frac{1}{2}|\Sigma_{11}\rangle_a|\Sigma_{01}\rangle_{ba}\langle\Sigma_{11}|_b\langle\Sigma_{01}|.
\end{aligned}
$$

If the states have not been disturbed, then we necessarily and sufficiently have $\langle\Psi^-|\rho_{ab}|\Psi^-\rangle = 1$, $\langle\Psi^+|\rho_{ab}|\Psi^+\rangle = 0$, $\langle\Phi^-|\rho_{ab}|\Phi^-\rangle = 0$, and $\langle\Phi^+|\rho_{ab}|\Phi^+\rangle = 0$. A detailed calculation shows that

$$
\begin{aligned}
&u_a = u_b = \pm 1,\\
&v_a = v_b = 0,\\
&g_{0a} = g_{0b} = 1,\\
&g_{1a} = g_{1b} = 1,\\
&h_{0a} = h_{0b} = 0,\\
&h_{1a} = h_{1b} = 0.
\end{aligned}
$$

Consequently, if Alice's state has not been disturbed after the whole process, it requires

$$
\begin{aligned}
|\Sigma_{00}\rangle_i &= \pm|\Sigma_{10}\rangle_i,\\
|\Sigma_{01}\rangle_i &= |\Sigma_{11}\rangle_i = 0.
\end{aligned}
$$

Let us denote that $|\Sigma'\rangle_i = |\Sigma_{00}\rangle_i = \pm|\Sigma_{10}\rangle_i$. There-

fore, after the interaction, the state of the EPR pair is

$$\rho_{ab} = |\Psi^-\rangle_{ab}\langle\Psi^-|,$$

and the state of the ancilla is

$$\rho_{\Sigma_{ab}} = |\Sigma'\rangle_a|\Sigma'\rangle_{ba}\langle\Sigma'|_b\langle\Sigma'|.$$

The above calculations can be done in full analogy, and the obtained results are the same, when we assume that Alice sends $|\Psi^+\rangle$, and $|\Phi^\pm\rangle$ instead of $|\Psi^-\rangle$:

$$\begin{aligned}
\rho_{ab} &= |\Psi^+\rangle_{ab}\langle\Psi^+|, \quad \rho_{\Sigma_{ab}} = |\Sigma'\rangle_a|\Sigma'\rangle_{ba}\langle\Sigma'|_b\langle\Sigma'|,\\
\rho_{ab} &= |\Phi^+\rangle_{ab}\langle\Phi^+|, \quad \rho_{\Sigma_{ab}} = |\Sigma'\rangle_a|\Sigma'\rangle_{ba}\langle\Sigma'|_b\langle\Sigma'|,\\
\rho_{ab} &= |\Phi^-\rangle_{ab}\langle\Phi^-|, \quad \rho_{\Sigma_{ab}} = |\Sigma'\rangle_a|\Sigma'\rangle_{ba}\langle\Sigma'|_b\langle\Sigma'|.
\end{aligned}$$

That is to say, no matter which state Alice sends, Eve's ancilla will be in the same state $\rho_{\Sigma_{ab}}$. Then, we can conclude that time-separated Bell states cannot be distinguished without disturbing them.

3. Impersonation attack

It is interesting to know whether Eve can obtain the time-separated EPR pair at the same time without disturbing its states. It has been discussed above that Eve's any attempt to distinguish Bell states will disturb them when she cannot hold two qubits of the EPR pair at the same time. However, there is one way that Eve can hold two qubits of the time-separated EPR pair at the same time but without disturbing its states. Eve first prepares an EPR pair. She captures the first qubit of Alice's EPR pair and sends one qubit of her dummy EPR pair to Bob. She then captures the second qubit of Alice's EPR pair and performs a Bell basis measurement on the EPR pair to gain its states. Based on her measurement results, she performs an unitary operation on the second qubit of her dummy EPR pair and sends it to Bob. In this way, Eve can exactly distinguish Alice's Bell states with zero risk of disturbing them.

Eve's impersonation attack above does not challenge our proof, because we have assumed that Eve cannot hold the EPR pair at the same time in our proof. However, in the impersonation attack scheme, Eve can hold Alice's two qubits at the same time, so that, for Eve, Alice's EPR pair is not time-separated any longer. Consequently, our proof cannot be used in quantum communication directly since it is completely nonrobust against impersonation attack. In quantum communication, Alice and Bob should first check the fidelity of the EPR pair after Bob received the first qubit to detect the potential attacks, including Eve's impersonation attack. Similar quantum communication has already been presented and it is called as two-step quantum communication.[6]

4. Discussion and conclusion

Another equivalent description of indistinguishability of quantum state is the no-clone theorem. In Ref.[7], Mor has pointed out that orthogonal composite system made of two subsystems cannot be cloned if the subsystems are only available one after the other. In fact, our proof of indistinguishability of orthogonal time-separated Bell states implies that cloning of orthogonal time-separated Bell states is forbidden, vice versa.

Indistinguishability of time-separated Bell states may be generalized to the multipartite systems. In the future quantum computation, entangled qubits may be processed under remote logical gates or under the same gate at different times. However, all entangled qubits should be measured at the same time in order to read out the computing results correctly. And our proof may also provide theoretical support to many present protocols based on orthogonal Bell state.[8]

References

[1] Gisin N, Ribordy G, Tittel W and Zbinden H 2002 *Rev. Mod. Phys.* **74** 145

[2] Nielsen M A and Chuang I L 2000 *Quantum Computation and Quantum Information* (Cambridge: Cambridge University Press)

[3] Wooters W K and Zurek W H 1982 *Nature* **299** 802

[4] Ghosh S, Kar G, Roy A, de Sen A and Sen U 2001 *Phys. Rev. Lett.* **87** pp277902.1–277902.2

[5] Kraus K 1983 *States, Effects, and Operations* (Berlin: Springer)

[6] Deng F G, Long G L and Liu X S 2003 *Phys. Rev.* A **68** 042317

[7] Mor T 1998 *Phys. Rev. Lett.* **80** 3137

[8] Lü H, Chen A X and Yan X D 2007 *Chin. Phys.* **16** 2862
Man Z X and Xia Y J 2007 *Chin. Phys.* **16** 1197