No-Cloning Theorem of Entangled States

Masato Koashi and Nobuyuki Imoto
NTT Basic Research Laboratories, 3-1 Morinosato Wakamiya, Atsugi, Kanagawa 243-0198, Japan
(Received 1 May 1998)

We derive a necessary and sufficient condition for two pure states, each entangled in two remote systems, to be clonable by the sequential access to the two systems. The result shows to what extent the correlation to other systems can be read out from a subsystem without altering its marginal density operators. This extends the standard no-cloning theorem to the case of a subsystem correlated to others. [S0031-9007(98)07596-6]

PACS numbers: 03.67.Dd, 03.65.Bz, 89.70.+c

A striking feature of quantum mechanics is that one cannot freely read out the information of a system without affecting the state of the system. This property is clearly stated in the form of the no-cloning theorem that an unknown state cannot be cloned by any physical means. The pure-state no-cloning theorems state that linearity of quantum mechanics forbids cloning of three arbitrary pure states [1,2], and that cloning of two nonorthogonal pure states violates unitarity [3]. Recently, the no-cloning theorem is extended to the case of mixed states, and it was shown that the broadcasting of two noncommuting mixed states is impossible [4]. Since a pure state in a Hilbert space behaves in general as a mixed state in a subspace of the whole space, the above extension can be viewed as a step toward the no-cloning theorem of subsystems. The information contained in a subsystem is not represented entirely by its marginal density operator, but also by the correlation to the rest of the whole system. The next step will thus be to find out how quantum mechanics poses the restriction on reading out such information.

The no-cloning theorem also has a direct application to secret communication, known as quantum cryptography. For the simplest protocols using the minimal number (two) of states, general requirements for security for the pure-state [5] and for the mixed-state [6] cases have already been derived. For the case of two orthogonal entangled states, only a specific example is proposed [7] and a general condition is not known.

In this Letter, we derive the condition for two pure states, each entangled in two subsystems, to be clonable by the sequential access to the two subsystems. This directly gives the requirement for the two states used in the protocol of quantum cryptography via split sending [7,8]. In the access to the first system, one must extract the correlation to the second system without altering the marginal state of the first system. Our proof reveals what types of correlation can be extracted, and thus completes the extension of the no-cloning theorem to the case of a subsystem correlated to others.

The problem is formally posed as follows. A quantum system to be cloned is composed of two parts, A and B. In addition, we have a working system C, part of which is assigned as target spaces A' and B'. Initially the composite system AB is secretly prepared in either of two pure states, $|\Phi^{(0)}\rangle$ and $|\Phi^{(1)}\rangle$, and C in a standard quantum state $E = |u\rangle\langle u|$. We operate a unitary operation U on AC and, subsequently, another unitary operation U_2 on BC. We require that after these operations, AB is still in the pure state $|\Phi^{(s)}\rangle$ initially chosen, and $A'B'$ is also in $|\Phi^{(s)}\rangle$. We seek a necessary and sufficient condition for $|\Phi^{(0)}\rangle$ and $|\Phi^{(1)}\rangle$ in order that such unitary operations exist.

In order to derive the necessary condition [Eq. (30), below], let us suppose that the cloning operation $\{U, U_2\}$ exists. Since U_2 does not act on the space A, the first unitary operation U should preserve the marginal density operator in A, defined as $\rho^{(s)} \equiv \mathrm{Tr}_B(|\Phi^{(s)}\rangle\langle\Phi^{(s)}|)$. This is written as

$$\mathrm{Tr}_C(\tilde{\rho}^{(s)}) \equiv \mathrm{Tr}_C[U(\rho^{(s)} \otimes E)U^\dagger] = \rho^{(s)}. \qquad (1)$$

Most of our derivation of the cloning condition is devoted to finding a decomposition of space A into a direct sum of subspaces $\{H_i\}$ such that U affects each subspace independently, namely,

$$(P_i \otimes \mathbf{1})U(P_j \otimes E) = \mathbf{0} \quad \text{for any } i \neq j, \qquad (2)$$

where P_i is the projection operator onto H_i. Note that (2) is equivalent to

$$[P_i \otimes \mathbf{1}, U](\mathbf{1} \otimes E) = \mathbf{0} \quad \text{for any } i, \qquad (3)$$

which states that U and P_i "commute" in the relevant case.

First, we show that the decomposition $\{P_i\} = \{\bar{P}^{(0)}, \mathbf{1} - \bar{P}^{(0)}\}$, where $\bar{P}^{(0)}$ is the projection onto the kernel of $\rho^{(0)}$, satisfies (2). Equation (1) implies that $\mathrm{Tr}_{AC}[(\bar{P}^{(0)} \otimes \mathbf{1}) \times \tilde{\rho}^{(0)}] = 0$, or equivalently, $(\bar{P}^{(0)} \otimes \mathbf{1})U(\rho^{(0)} \otimes E) = \mathbf{0}$. Since $\rho^{(0)}$ is invertible in its support, we have

$$(\bar{P}^{(0)} \otimes \mathbf{1})U[(\mathbf{1} - \bar{P}^{(0)}) \otimes E] = \mathbf{0}. \qquad (4)$$

Using this and Eq. (1), we obtain

$$\mathrm{Tr}_{AC}\{[(\mathbf{1} - \bar{P}^{(0)}) \otimes \mathbf{1}]U(\bar{P}^{(0)}\rho^{(1)}\bar{P}^{(0)} \otimes E)U^\dagger\} = \mathrm{Tr}_A(\bar{P}^{(0)}\rho^{(1)}) - \mathrm{Tr}_{AC}[(\bar{P}^{(0)} \otimes \mathbf{1})\tilde{\rho}^{(1)}] = 0. \qquad (5)$$

Since we can assume that $\rho^{(1)}$ is invertible in the kernel of $\rho^{(0)}$,

$$[(\mathbf{1} - \bar{P}^{(0)}) \otimes \mathbf{1}]U(\bar{P}^{(0)} \otimes E) = \mathbf{0}. \qquad (6)$$

 0031-9007/98/81(19)/4264(4)$15.00

Equation (1) means that the fidelity $F(\rho^{(0)},\rho^{(1)}) \equiv \mathrm{Tr}(\sqrt{\rho^{(0)(1/2)}\rho^{(1)}\rho^{(0)(1/2)}})$ between the two density operators in A is preserved under the operation U. This implies that the support of $\rho^{(0)}$ can be decomposed to its subspaces that satisfy (2), as shown in the following. From the operator polar decomposition theorem [9], there exists a unitary operator V such that

$$V\rho^{(1)(1/2)}\rho^{(0)(1/2)} = \sqrt{\rho^{(0)(1/2)}\rho^{(1)}\rho^{(0)(1/2)}}\,. \quad (7)$$

In the support of $\rho^{(0)}$, we define a positive Hermite operator M such that

$$M = \rho^{(0)(-1/2)}V\rho^{(1)(1/2)} = \rho^{(0)(-1/2)}\sqrt{\rho^{(0)(1/2)}\rho^{(1)}\rho^{(0)(1/2)}}\,\rho^{(0)(-1/2)}. \quad (8)$$

Let P_j be the projection operator onto the eigenspace of M with eigenvalue μ_j. Note that $\mu_j \geq 0$ and $\sum P_j = \mathbf{1} - \bar{P}^{(0)}$. Then, for these $\{P_j\}$ and V,

$$P_j\rho^{(1)}P_j = P_jM\rho^{(0)}MP_j = \mu_j^2P_j\rho^{(0)}P_j \quad (9)$$

and

$$\sum_j \sqrt{\mathrm{Tr}(\rho^{(1)}P_j)}\sqrt{\mathrm{Tr}(\rho^{(0)}P_j)} = \sum_j \mu_j\,\mathrm{Tr}(\rho^{(0)(1/2)}P_j\rho^{(0)(1/2)}) = \mathrm{Tr}(\sqrt{\rho^{(0)(1/2)}\rho^{(1)}\rho^{(0)(1/2)}}) = F(\rho^{(0)},\rho^{(1)}), \quad (10)$$

where we used $MP_j = \mu_jP_j$. For the states after the unitary operation U, the following inequality holds for any sets of positive operators $\{\tilde{P}_j\}$ on AC such that $\sum_j \tilde{P}_j = \mathbf{1}\otimes\mathbf{1}$, and for any unitary operator $\tilde{V}$ on AC:

$$\begin{aligned}\sum_j \sqrt{\mathrm{Tr}(\tilde{\rho}^{(1)}\tilde{P}_j)}\sqrt{\mathrm{Tr}(\tilde{\rho}^{(0)}\tilde{P}_j)} &= \sum_j \sqrt{\mathrm{Tr}(\tilde{V}\tilde{\rho}^{(1)(1/2)}\tilde{P}_j\tilde{\rho}^{(1)(1/2)}\tilde{V}^\dagger)}\sqrt{\mathrm{Tr}(\tilde{\rho}^{(0)(1/2)}\tilde{P}_j\tilde{\rho}^{(0)(1/2)})} \\ &\geq \sum_j |\mathrm{Tr}(\tilde{V}\tilde{\rho}^{(1)(1/2)}\tilde{P}_j\tilde{\rho}^{(0)(1/2)})| \geq \left|\sum_j \mathrm{Tr}(\tilde{V}\tilde{\rho}^{(1)(1/2)}\tilde{P}_j\tilde{\rho}^{(0)(1/2)})\right| = |\mathrm{Tr}(\tilde{V}\tilde{\rho}^{(1)(1/2)}\tilde{\rho}^{(0)(1/2)})|\,. \end{aligned} \quad (11)$$

If we assume that the set $\{\tilde{P}_j\}$ consists of $\{P_j\otimes\mathbf{1}\}$ and $\bar{P}^{(0)}\otimes\mathbf{1}$, the left-hand side of the inequality is

$$\sum_j \sqrt{\mathrm{Tr}_{AC}(\tilde{\rho}^{(1)}\tilde{P}_j)}\sqrt{\mathrm{Tr}_{AC}(\tilde{\rho}^{(0)}\tilde{P}_j)} = \sum_j \sqrt{\mathrm{Tr}_A(\rho^{(1)}P_j)}\sqrt{\mathrm{Tr}_A(\rho^{(0)}P_j)} = F(\rho^{(0)},\rho^{(1)})\,. \quad (12)$$

For the choice of $\tilde{V} = U(V\otimes\mathbf{1})U^\dagger$, the right-hand side of the inequality is also

$$\begin{aligned}\mathrm{Tr}_{AC}(\tilde{V}\tilde{\rho}^{(1)(1/2)}\tilde{\rho}^{(0)(1/2)}) &= \mathrm{Tr}_A(V\rho^{(1)(1/2)}\rho^{(0)(1/2)}) \\ &= F(\rho^{(0)},\rho^{(1)})\,. \end{aligned} \quad (13)$$

This means the equalities in (11) hold for these choices. Therefore,

$$\tilde{V}\tilde{\rho}^{(1)(1/2)}\tilde{P}_j = \nu_j e^{i\phi}\tilde{\rho}^{(0)(1/2)}\tilde{P}_j, \qquad \nu_j \geq 0\,. \quad (14)$$

From (13) and $F \geq 0$, the common phase factor is found to be $e^{i\phi} = 1$. Equation (14) implies that

$$\begin{aligned}\mathrm{Tr}_A(\rho^{(1)}P_j) &= \mathrm{Tr}_{AC}(\tilde{\rho}^{(1)}\tilde{P}_j) \\ &= \mathrm{Tr}_{AC}(\tilde{V}\tilde{\rho}^{(1)(1/2)}\tilde{P}_j\tilde{\rho}^{(1)(1/2)}\tilde{V}^\dagger) \\ &= \nu_j^2\,\mathrm{Tr}_{AC}(\tilde{\rho}^{(0)}\tilde{P}_j) = \nu_j^2\mathrm{Tr}_A(\rho^{(0)}P_j)\,. \end{aligned} \quad (15)$$

Substituting (9) gives $\mu_j = \nu_j$. Thus we can rewrite (14) as

$$(V\rho^{(1)(1/2)}\otimes E)U^\dagger(P_j\otimes\mathbf{1}) = \mu_j(\rho^{(0)(1/2)}\otimes E) \times U^\dagger(P_j\otimes\mathbf{1})\,. \quad (16)$$

Multiplying $P_i\rho^{(0)(-1/2)}\otimes\mathbf{1}$ from the left gives the relation corresponding to (2):

$$(P_j\otimes\mathbf{1})U(P_i\otimes E) = \mathbf{0} \quad \text{when } \mu_i \neq \mu_j\,. \quad (17)$$

At this point, we have a decomposition of the space A specified by $\bar{P}^{(0)}$ and P_j, satisfying (2). As shown below, the requirement of preserving an off-diagonal part $P_j\rho^{(s)}P_i$ reveals that U affects the two subspaces P_j and P_i in the same manner [see Eq. (24)]. This implies that each subspace may be further decomposed as a direct sum of its own subspaces on which U affects independently. We assume that repeating such procedures, we arrive at a form of decomposition $\sum_l\sum_{i=1}^{n_l} H_i^{(l)}$ in which each subspace cannot be decomposed further to satisfy (2). We denote the projection onto $H_i^{(l)}$ as $P_i^{(l)}$. We added the index l such that for any pair having the same index l, $H_i^{(l)}$, and $H_j^{(l)}$, there exists at least one nonzero operator of the form $P_i^{(l)}\rho^{(s)}P_{i'}^{(l)}\rho^{(s')}\cdots P_{i''}^{(l)}\rho^{(s'')}P_j^{(l)}$, and for the pair with different l there are no such operators.

Now let us see how the requirement of preserving $P_j^{(l)}\rho^{(s)}P_i^{(l)}$ poses restriction on the form of U. Suppose that $P_j^{(l)}\rho^{(s)}P_i^{(l)} \neq \mathbf{0}$, and that P is the projection onto the support $H(\subseteq H_i^{(l)})$ of the operator $P_j^{(l)}\rho^{(s)}P_i^{(l)}$. If we write a polar form of $P_j^{(l)}\rho^{(s)}P_i^{(l)}$ as VN, the Hermitian operator N is positive and invertible in H, and the unitary operator V [different from V used in Eq. (7)] transforms the bases of H to those of $H_j^{(l)}$. Using Eq. (1) and the fact that U commutes with $P_i^{(l)}$ and $P_j^{(l)}$ in the relevant space, we have

$$\begin{aligned}\mathrm{Tr}_A N &= \mathrm{Tr}_{AC}[(P_i^{(l)}PV^\dagger P_j^{(l)}\otimes\mathbf{1})\tilde{\rho}^{(s)}] \\ &= \mathrm{Tr}_{AC}[U^\dagger(PV^\dagger\otimes\mathbf{1})U(V\otimes\mathbf{1})(N\otimes E)]\,. \end{aligned} \quad (18)$$

Since the operator $O \equiv U^\dagger(PV^\dagger\otimes\mathbf{1})U(V\otimes\mathbf{1})$ appeared above is a product of unitary operators and a projection, its norm satisfies $||O|| \leq 1$. If we rewrite $N\otimes E$ in (18) as $N\otimes E = \sum_k \lambda_k|b_k\rangle\langle b_k|$, where $\lambda_k > 0$ are its eigenvalues and $|b_k\rangle$ its eigenstates, we have

$$\sum_k \lambda_k = \sum_k \lambda_k\langle b_k|O|b_k\rangle\,. \quad (19)$$

Since $||O|| \leq 1$, we obtain $\langle b_k|O|b_k\rangle = 1$ and applying $||O|| \leq 1$ again gives $O|b_k\rangle = |b_k\rangle$. We thus have $O(P \otimes E) = P \otimes E$, namely,

$$(PV^\dagger \otimes \mathbf{1})U(V \otimes \mathbf{1})(P \otimes E) = U(P \otimes E). \quad (20)$$

Operating $(P_i^{(l)} - P) \otimes \mathbf{1}$ from the left gives

$$[(P_i^{(l)} - P) \otimes \mathbf{1}]U(P \otimes E) = \mathbf{0}. \quad (21)$$

Since $P_i^{(l)}\rho^{(s)}P_i^{(l)}$ is nonzero, this operator should be invertible in $H_i^{(l)}$ [see (9)]. Then, the discussion from (4) through (6) similarly applies here, and we obtain

$$(P \otimes \mathbf{1})U[(P_i^{(l)} - P) \otimes E] = \mathbf{0}. \quad (22)$$

Since we have assumed that $H_i^{(l)}$ cannot be decomposed further, $P_i^{(l)}$ must be equal to P. Similarly, the image of $P_j^{(l)}\rho^{(s)}P_i^{(l)}$ is $H_j^{(l)}$. These mean that $P_j^{(l)}\rho^{(s)}P_i^{(l)}{:}H_i^{(l)} \to H_j^{(l)}$ is bijective, and thus all $H_j^{(l)}$ with the same index l have the same dimension d_l. Now, operating $V \otimes \mathbf{1}$ from the left and replacing P by $P_i^{(l)}$ in (20), we have

$$(P_j^{(l)} \otimes \mathbf{1})U(V \otimes \mathbf{1})(P_i^{(l)} \otimes E) = (V \otimes \mathbf{1})U(P_i^{(l)} \otimes E), \quad (23)$$

where we have used $VP_i^{(l)}V^\dagger = P_j^{(l)}$. If we define $Q_{ji}^{(l)} \equiv VP_i^{(l)} = P_j^{(l)}VP_i^{(l)}$, we obtain a commutation relation

$$[Q_{ji}^{(l)} \otimes \mathbf{1}, U](\mathbf{1} \otimes E) = \mathbf{0}, \quad (24)$$

which states that U affects the two subspaces $H_j^{(l)}$ and $H_i^{(l)}$ in the same manner. If we further define the operators $Q_{jj}^{(l)} \equiv P_j^{(l)}$ and $Q_{ij}^{(l)} \equiv Q_{ji}^{(l)\dagger}$, the four operators in $H_j^{(l)}$ of the form $Q_{j\alpha}^{(l)}\rho^{(s)}Q_{\beta j}^{(l)}(\alpha, \beta = i, j)$ have the following property:

$$\mathrm{Tr}_C[U(Q_{j\alpha}^{(l)}\rho^{(s)}Q_{\beta j}^{(l)} \otimes E)U^\dagger] = Q_{j\alpha}^{(l)}\rho^{(s)}Q_{\beta j}^{(l)}. \quad (25)$$

Since $Q_{jj}^{(l)}\rho^{(s)}Q_{ij}^{(l)} = VNV^\dagger$, $Q_{j\alpha}^{(l)}\rho^{(s)}Q_{\beta j}^{(l)}$ is a positive self-adjoint operator even when $\alpha \neq \beta$. Then, the discussion from (7) through (17) can be applied to any two of $Q_{j\alpha}^{(l)}\rho^{(s)}Q_{\beta j}^{(l)}$, that is, to any two combinations of (α, β), and reveals conditions like (17). Under the assumption that $H_j^{(l)}$ cannot be decomposed further, $H_j^{(l)}$ must be an eigenspace of M with $\rho^{(0)}$ and $\rho^{(1)}$ replaced by any two of $Q_{j\alpha}^{(l)}\rho^{(s)}Q_{\beta j}^{(l)}$. This implies that the four operators $Q_{j\alpha}^{(l)}\rho^{(s)}Q_{\beta j}^{(l)}$ are all proportional [see (9)].

When $P_j^{(l)}\rho^{(s)}P_i^{(l)} = \mathbf{0}$, we can also define $Q_{ji}^{(l)}$ that converts the bases of H_i to those of H_j and satisfies (24), by making a product of other $Q_{j'i'}^{(l)}$. This definition of $Q_{ji}^{(l)}$ is unique except for an overall phase. The reason is that if two such operators $Q_{ji}^{(l)}$ and $Q_{ji}^{(l)\prime}$ exist, $Q_{ji}^{(l)\dagger}Q_{ji}^{(l)\prime}$ is unitary in $H_i^{(l)}$ and commutes with U in the relevant case, so that it must be written as $e^{i\phi}P_i^{(l)}$, otherwise $H_i^{(l)}$ would be decomposed further. Thus, for a particular choice of $Q_{1i}^{(l)}$, all $2n_l^2$ operators in $H_1^{(l)}$ of the form $Q_{1i}^{(l)}\rho^{(s)}Q_{j1}^{(l)}$ with a fixed l are proportional and can be diagonalized simultaneously by choosing a basis $\{|a_k^{(l)}\rangle\}$. Then, if we define nonzero positive parameters

$$\eta_k^{(l)} \equiv \frac{\langle a_k^{(l)}|\rho^{(0)} + \rho^{(1)}|a_k^{(l)}\rangle}{\sum_k \langle a_k^{(l)}|\rho^{(0)} + \rho^{(1)}|a_k^{(l)}\rangle}, \quad (26)$$

the matrix elements of $\rho^{(s)}$ in the basis $\{|l, k, i\rangle \equiv Q_{i1}^{(l)}|a_k^{(l)}\rangle\}$ can be written as

$$\langle l, k, i|\rho^{(s)}|l', k', j\rangle = \delta_{l'l}\delta_{k'k}\xi_{ij}^{(s,l)}\eta_k^{(l)}, \quad (27)$$

where $\xi_{ij}^{(s,l)}$ are complex numbers which satisfy $\xi_{ij}^{(s,l)*} = \xi_{ji}^{(s,l)}$. This relation shows that $\rho^{(0)}$ and $\rho^{(1)}$ are simultaneously block diagonalized in this basis, where a subspace with fixed l and k holds one block. Blocks with the same indices l and s are proportional, and the weights $\eta_k^{(l)}$ are common to $\rho^{(0)}$ and $\rho^{(1)}$.

The simultaneous block-diagonalized form just derived is "irreducible," i.e., each block is never split into smaller blocks. This is seen from the fact that each base of a single block belongs to different $H_i^{(l)}$. If a different choice of basis gave smaller blocks, the projection measurement onto the new blocks would not change $\rho^{(s)}$. This leads to contradiction since the unitary operator of such interaction does not commute with some of $P_i^{(l)}$. This uniqueness allows a more convenient way of finding the basis $\{|l, k, i\rangle\}$, i.e., conducting block diagonalization first and examining the proportionality by comparing blocks with the same size.

Now using the operators $\{Q_{ij}^{(l)}\}$, a necessary and sufficient condition of the cloning is derived as follows. Consider a unitary operation U' acting on AC', where C' is a new auxiliary system initially in $|x\rangle$. Suppose that U' has the following property that does not contradict with the unitarity of U':

$$U'(\mathbf{1} \otimes |x\rangle\langle x|) = \sum_{l,i} Q_{1i}^{(l)} \otimes |x_{li}\rangle\langle x|, \quad (28)$$

where $|x_{li}\rangle$ are orthogonal states in C'. The condition (24) implies that the order of applying U and U' makes no difference, namely, if the cloning operation exists, the same operation still works even if U' is applied beforehand. Therefore, a necessary condition of the cloning is that the two states $|\Phi^{(0)}\rangle$ and $|\Phi^{(1)}\rangle$ are still orthogonal in AB even after the operation of U', i.e.,

$$\mathrm{Tr}_{AB}\left[\prod_{s=0,1} \mathrm{Tr}_{C'}[U'(|\Phi^{(s)}\rangle\langle\Phi^{(s)}| \otimes |x\rangle\langle x|)U'^\dagger]\right] = 0. \quad (29)$$

This is equivalent to

$$\langle\Phi^{(0)}|Q_{ij}^{(l)}|\Phi^{(1)}\rangle = 0 \quad \text{for any } l, i, j. \quad (30)$$

In order to show that this is also a sufficient condition, we directly introduce a particular form of U that enables cloning:

$$U(\mathbf{1}\otimes E)=\sum_{likk'}\sqrt{\eta_k^{(l)}}\,Q_{i1}^{(l)}|a_k^{(l)}\rangle\langle a_{k'}^{(l)}|Q_{1i}^{(l)}\otimes|u_{lkk'}\rangle\langle u|\,, \tag{31}$$

where $|u_{lkk'}\rangle$ are orthogonal states in C and the unitarity is not broken since $\sum_k \eta_k^{(l)}=1$. It is easy to verify that $\mathrm{Tr}_C[U(\rho^{(s)}\otimes E)U^\dagger]=\rho^{(s)}$. The state $\rho_{BC}^{(s)}$ in BC after the interaction is

$$\begin{aligned}\rho_{BC}^{(s)}&\equiv \mathrm{Tr}_A[U(|\Phi^{(s)}\rangle\langle\Phi^{(s)}|\otimes E)U^\dagger]\\&=\sum_{likk'k''}\eta_k\langle a_{k'}^{(l)}|Q_{1i}^{(l)}|\Phi^{(s)}\rangle\langle\Phi^{(s)}|Q_{i1}^{(l)}|a_{k''}^{(l)}\rangle\\&\qquad\otimes|u_{lkk'}\rangle\langle u_{lkk''}|\,.\end{aligned} \tag{32}$$

Then, under the condition (30),

$$\mathrm{Tr}_{BC}[\rho_{BC}^{(0)}\rho_{BC}^{(1)}]=\sum_{lijk}\eta_k^{(l)2}|\langle\Phi^{(0)}|Q_{ij}^{(l)}|\Phi^{(1)}\rangle|^2=0\,. \tag{33}$$

This means that the original state can be distinguished by projection measurement in BC, after system A is sent away. The rest of task is to reproduce the original state in AB, only by manipulating systems BC. Since the marginal density operator in A is unchanged, there exists a unitary operation U_2 in BC that converts the whole system ABC to $|\Phi^{(s)}\rangle|u_s\rangle$ [10]. Therefore, (30) is a necessary and sufficient condition so that two pure entangled states $|\Phi^{(0)}\rangle$ and $|\Phi^{(1)}\rangle$ be cloned by the sequential access to the two systems, A and B.

The argument above tells us what types of information on the correlation with the subsystem B can be extracted from the subsystem A without altering its marginal state. For this purpose, it will help to rewrite (33) as

$$\mathrm{Tr}_{BC}[\rho_{BC}^{(0)}\rho_{BC}^{(1)}]=\left(\sum_{k'}\eta_{k'}^{(l)2}\right)\sum_{ii'l}\left|\sum_k\langle\Phi^{(0)}|l,k,i\rangle\times\langle l,k,i'|\Phi^{(1)}\rangle\right|^2, \tag{34}$$

and to compare it with the orthogonality of the original states in B,

$$\mathrm{Tr}_B\left[\prod_{s=0,1}\mathrm{Tr}_A(|\Phi^{(s)}\rangle\langle\Phi^{(s)}|)\right]=\sum_{ll'kk'ii'}|\langle\Phi^{(0)}\mid l,k,i\rangle\times\langle l',k',i'\mid\Phi^{(1)}\rangle|^2, \tag{35}$$

and with that in AB,

$$\mathrm{Tr}_{AB}\left[\prod_{s=0,1}|\Phi^{(s)}\rangle\langle\Phi^{(s)}|\right]=\left|\sum_{lki}\langle\Phi^{(0)}\mid l,k,i\rangle\times\langle l,k,i\mid\Phi^{(1)}\rangle\right|^2. \tag{36}$$

We notice that the summation on k in (34) is identical to that in the case (36) where system A is fully available, and the summations on ii' in (34) are identical to those in (35) where system A is not accessible at all. These show the following: (i) We can extract some correlation concerning the indices l and k, but not on i. (ii) The full quantum correlation can be extracted for the index k. For the index l, the phase information is not available and only the classical correlation can be extracted.

Although the marginal density operators in A are preserved by the operation U, the correlations between A and B are not necessarily preserved by U. This is seen by calculating the following quantity:

$$\mathrm{Tr}_{AB}\left\{\prod_{s=0,1}\mathrm{Tr}_C[U(|\Phi^{(s)}\rangle\langle\Phi^{(s)}|\otimes E)U^\dagger]\right\}=\left(\sum_{k''}\eta_{k''}^{(l)2}\right)\sum_{lkk'}\left|\sum_i\langle\Phi^{(0)}|lki\rangle\langle lk'i|\Phi^{(1)}\rangle\right|^2. \tag{37}$$

This implies that the original correlation for k and the phase information of the correlation for l are broken by the operation U.

To summarize, under the restriction that the two marginal density operators in A be preserved, we can copy the classical correlations with respect to the subspaces for which the two density operators are simultaneously block diagonalized. The copying classical correlations results in destroying the phase information for that correlation. If some of the blocks are identical except for factors common to the two states, we can transfer (thus destroy the original) the full quantum correlation for those blocks.

Finally, we consider slightly different problems. One is with a stronger requirement so that A' is not included in C. Here U acts on $AA'C$ first, and U_2 acts on BC after systems A and A' are sent away. In this case (*in situ* cloning), what U does is to clone (not to broadcast) the marginal density operator $\rho^{(s)}$ of A into A'. A necessary and sufficient condition for the *in situ* cloning is thus $F(\rho^{(0)},\rho^{(1)})=0,1$ [4]. Another problem is with a weaker requirement so that another operation U_3 is allowed to act on AC after the operations of U and U_2. In this case, U is allowed to transfer the contents of A into C because it is possible to return them to A by U_3. The argument thus reduces to the pure-state case, with the cloning condition $\langle\Phi^{(0)}\mid\Phi^{(1)}\rangle=0,1$.

[1] W. K. Wootters and W. H. Zurek, Nature (London) **299**, 802 (1982).
[2] D. Dieks, Phys. Lett. A **92**, 271 (1982).
[3] H. P. Yuen, Phys. Lett. A **113**, 405 (1986).
[4] H. Barnum, C. M. Caves, C. A. Fuchs, R. Jozsa, and B. Schumacher, Phys. Rev. Lett. **76**, 2818 (1996).
[5] C. H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992).
[6] M. Koashi and N. Imoto, Phys. Rev. Lett. **77**, 2137 (1996).
[7] M. Koashi and N. Imoto, Phys. Rev. Lett. **79**, 2383 (1997).
[8] L. Goldenberg and L. Vaidman, Phys. Rev. Lett. **75**, 1239 (1995).
[9] R. Schatten, *Norm Ideals of Completely Continuous Operators* (Springer, Berlin, 1960).
[10] H.-K. Lo and H. F. Chau, Phys. Rev. Lett. **78**, 3410 (1997); D. Mayers, Phys. Rev. Lett. **78**, 3414 (1997).