

Entanglement transformation between sets of bipartite pure quantum states using local operations

H. F. Chau,¹ Chi-Hang Fred Fung,¹ Chi-Kwong Li,² Edward Poon,³ and Nung-Sing Sze⁴

¹*Department of Physics and Center of Computational and Theoretical Physics,
University of Hong Kong, Pokfulam Road, Hong Kong*

²*Department of Mathematics, College of William & Mary, Williamsburg,
Virginia 23187-8795, USA*

³*Department of Mathematics, Embry-Riddle Aeronautical University,
3700 Willow Creek Road, Prescott, Arizona 86301, USA*

⁴*Department of Applied Mathematics, The Hong Kong Polytechnic University,
Hung Hom, Hong Kong*

(Dated: 25 September 2012)

Alice and Bob are given an unknown initial state chosen from a set of pure quantum states. Their task is to transform the initial state to a corresponding final pure state using local operations only. We prove necessary and sufficient conditions on the existence of such a transformation. We also provide efficient algorithms that can quickly rule out the possibility of transforming a set of initial states to a set of final states.

PACS numbers: 03.67.-a, 03.67.Bg, 03.67.Lx, 03.65.Aa

I. INTRODUCTION

Entanglement is a useful resource in quantum information processing. Entanglement enables two parties to share non-classical correlation and is the basis for unconditional security in quantum key distribution¹⁻³, exponential speedup in quantum computing⁴⁻⁷, and error tolerance in computing with quantum error correction codes⁸⁻¹⁰. In this paper, we study a simple problem of transformation of entangled states, which is perhaps the simplest non-trivial case of studying the state transformation problem in the multi-partite setting. Alice and Bob are initially given an unknown bipartite pure state from the set $\{|x_i\rangle_{AB} \in \mathcal{H}_A \otimes \mathcal{H}_B, i = 1, \dots, N\}$, where \mathcal{H}_A (\mathcal{H}_B) denotes the Hilbert space of Alice's (Bob's) quantum system with dimension m (n). Their task is to transform the initial state to a corresponding state in the set $\{|y_i\rangle_{AB} \in \mathcal{H}_A \otimes \mathcal{H}_B, i = 1, \dots, N\}$ by performing local quantum operations only without any communication with each other. Any quantum operation on a density matrix ρ can be represented by a trace preserving completely positive (TPCP) map which can be expressed in the operator-sum form $\mathcal{F}(\rho) = \sum_i F_i \rho F_i^\dagger$ where $\sum_i F_i^\dagger F_i = I$. We prove necessary and sufficient conditions for the existence of a transformation $(\mathcal{F} \otimes \mathcal{G})(|x_i\rangle_{AB}\langle x_i|) = |y_i\rangle_{AB}\langle y_i|$ for all $i = 1, \dots, N$, where Alice (Bob) performs physical process \mathcal{F} (\mathcal{G}) on \mathcal{H}_A (\mathcal{H}_B). In other words, we are interested in the existence of a local operation (LO) transformation T of the form

$$T(\rho_{AB}) = \sum_{1 \leq i \leq p, 1 \leq j \leq q} (F_i \otimes G_j) \rho_{AB} (F_i^\dagger \otimes G_j^\dagger) \quad (1)$$

such that

$$T(|x_i\rangle_{AB}\langle x_i|) = |y_i\rangle_{AB}\langle y_i| \text{ for all } i = 1, \dots, N,$$

where $F_1, \dots, F_p \in M_m$ and $G_1, \dots, G_q \in M_n$ are Kraus operators satisfying $\sum F_i^\dagger F_i = I$ and $\sum G_j^\dagger G_j = I$. Here, p and q are the dimensions of the ancillas for the channels \mathcal{F} and \mathcal{G} . Figure 1(a) depicts the bipartite state transformation problem that we consider in this paper.

The state transformation problem has been studied since the early 1980s. Alberti and Uhlmann¹¹ proved necessary and sufficient conditions for the existence of a physical process that transforms two qubit (mixed) states to two other qubit (mixed) states. Subsequent works found necessary and sufficient conditions for transformations between two sets of pure states without any restriction on the number of states^{12–15}. Note that these previous results assume that the physical process acts on the entire Hilbert space the states live in (i.e., they do not impose a bipartite structure on the transformation as we do here). The pure-state single-party result^{12–15} states that a TPCP map T exists such that $T(|x_i\rangle_{AB}\langle x_i|) = |y_i\rangle_{AB}\langle y_i|$ for $i = 1, \dots, N$ if and only if there is a correlation matrix (positive semidefinite matrix with all diagonal entries equal to one) $M \in M_N$ such that the Gram matrix ($\langle x_i|x_j\rangle$) equals the Schur (entrywise) product $M \circ (\langle y_i|y_j\rangle)$.

Along a different line of research, transformation from one bipartite entangled pure state to another using local operations and classical communications (LOCC) has been studied for a long time. In particular, Bennett *et al.*¹⁶ as well as Lo and Popescu¹⁷ studied the transformation of a bipartite state to a maximally entangled state using LOCC. In fact, Lo and Popescu¹⁷ showed that any general transformation between bipartite pure states using LOCC can be performed with one-way classical communications only. Along a similar line, Nielsen¹⁸ studied the transformation problem between two general bipartite states and proved that $|x\rangle_{AB}$ transforms to $|y\rangle_{AB}$ using LOCC if and only if the eigenvalues of $\text{tr}_B(|x\rangle_{AB}\langle x|)$ are majorized by those of $\text{tr}_B(|y\rangle_{AB}\langle y|)$. Jonathan and Plenio¹⁹ extended this result to the case where the transformation is allowed to output one of many final states with a certain probability. Again, a majorization condition has been proven for this case. He and Bergou²⁰ further proposed a scheme to transform one bipartite state to another probabilistically. Gheorghiu and Griffiths²¹ considered transformation using separable operations (of which LOCC is a subset) and proved the same majorization condition for transformability as that in Ref. 19. Note that these results concern the transformation of only one bipartite state to another bipartite state.

In this paper, we study the combination of the previous two research directions by considering the transformation of sets of bipartite states. Our result shares some characteristic with the single-state bipartite result¹⁸ in that singular (or eigen) values of the initial and final states play an important role. In particular, we can immediately rule out the existence of the desired transformation by looking at the singular (or eigen) values in both cases. On the other hand, while the eigenvalues alone are sufficient to determine whether a LOCC map exists to transform one bipartite state to another¹⁸, the eigenvalues alone are not sufficient when we consider the LO transformation of a set of bipartite states to another. In summary, we consider in this paper the transformability problem in a new context that was only partially considered by previous results, and as discussed our necessary and sufficient conditions are different from those in the other contexts studied previously.

We remark that, along a different direction, some of us have studied the problem of transforming between two sets of *mixed* states (with a single-party TPCP map, instead of a two-party map using LO or LOCC), and obtained necessary and sufficient conditions for the existence of such a transformation²².

A. State representation

We always work in some fixed orthonormal bases $\{|i\rangle_A : i = 1, \dots, m\}$ and $\{|j\rangle_B : j = 1, \dots, n\}$ on Alice's and Bob's systems respectively throughout the paper. Thus, a joint state of Alice and Bob $|x\rangle_{AB} = \sum_{i=1, \dots, m; j=1, \dots, n} \lambda_{ij} |i\rangle_A |j\rangle_B$ (where $\sum_{ij} |\lambda_{ij}|^2 = 1$) can be expressed as a column vector

$$x = \begin{bmatrix} \lambda_{11} \\ \lambda_{12} \\ \vdots \\ \lambda_{mn} \end{bmatrix} \in \mathbb{C}^{mn}. \quad (2)$$

For any state $|x\rangle_{AB} = \sum_{i=1, \dots, m; j=1, \dots, n} \lambda_{ij} |i\rangle_A |j\rangle_B$, we define an associated linear operator $X = \sum_{i=1, \dots, m; j=1, \dots, n} \lambda_{ij} |i\rangle\langle j|$, which is conveniently represented as an $m \times n$ matrix with

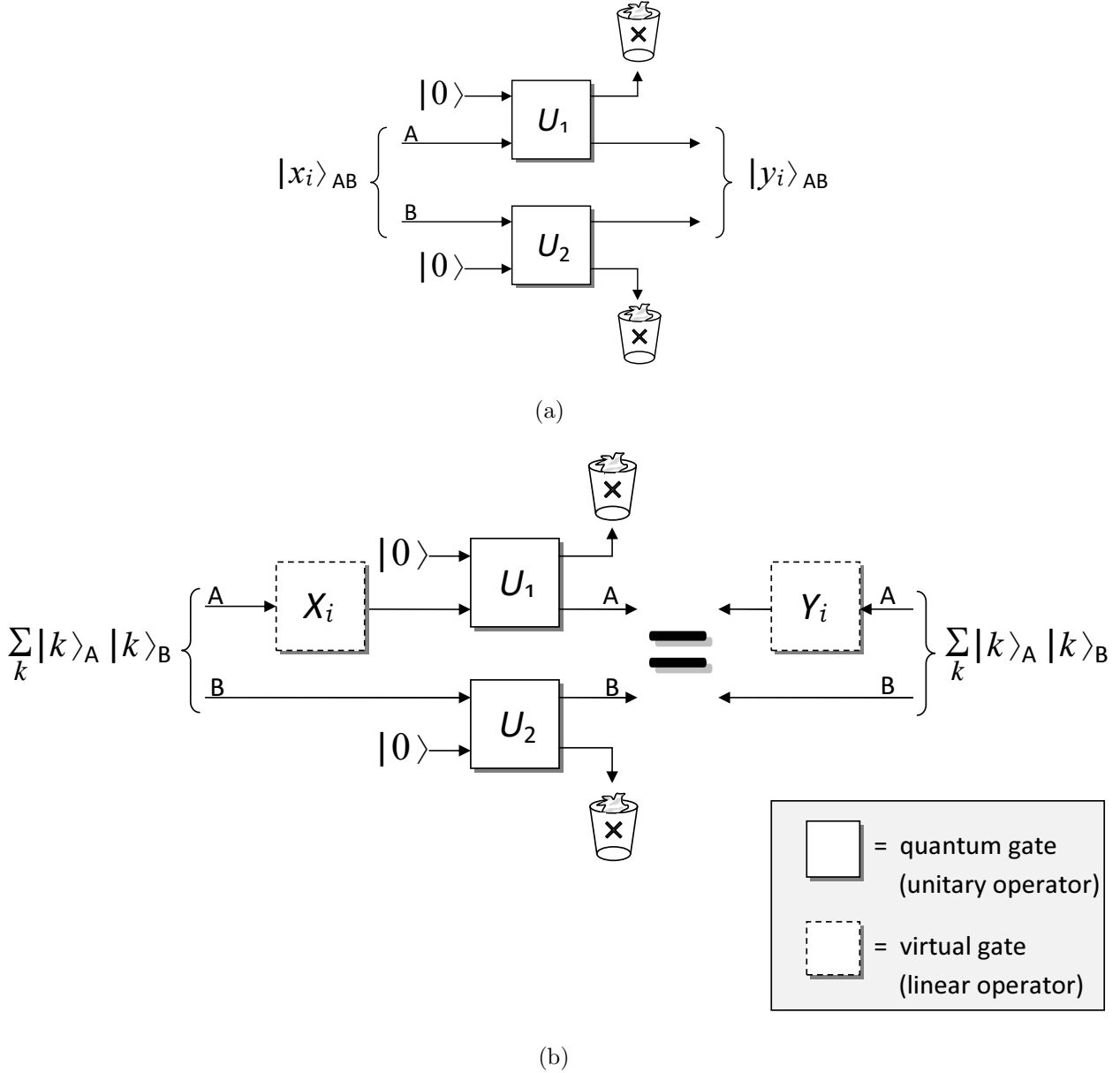


FIG. 1. The bipartite state transformation problem. (a) State representation of the problem: The input states $|x_i\rangle_{AB}$ are transformed to the corresponding output states $|y_i\rangle_{AB}$ for all $i = 1, \dots, N$ through a LO transformation $U_1 \otimes U_2$. The ancillas are prepared in the standard states and are discarded after the transformation. (b) Gate representation of the problem: The input states $|x_i\rangle_{AB}$ (output states $|y_i\rangle_{AB}$) are mapped to linear operators X_i (Y_i). The LO transformation $U_1 \otimes U_2$ maps the input “gate” X_i to the output “gate” Y_i for all i . This gate representation is useful as it can succinctly capture our necessary and sufficient conditions for the existence of the LO transformation.

the (i, j) element being λ_{ij} :

$$X = \begin{bmatrix} \lambda_{11} & \lambda_{12} & \dots & \lambda_{1n} \\ \lambda_{21} & \dots & \dots & \lambda_{2n} \\ \vdots & & & \vdots \\ \lambda_{m1} & & \dots & \lambda_{mn} \end{bmatrix}. \quad (3)$$

Note that here we are using the well known correspondence between vectors and matrices: $x = \text{vec}(X^t)$ (see, e.g., Ref. 23). The vec operator has a property that relates multiplication and tensor product: $\text{vec}(AXB) = (B^t \otimes A) \text{vec}(X)$. This property will be useful in Theorem II.1 later. In order to simplify notations in the rest of this paper, whenever we refer to the correspondence between a vector and a matrix, they are related by Eqs. (2) and (3), with a lower-case (upper-case) letter representing the vector (matrix).

We slightly abuse the notation by calling X a virtual quantum gate that changes the space of the state it acts on from n -dimensional to m -dimensional. It turns out that our main results and proofs can be conveniently expressed in terms of X_i and Y_i in addition to the original states $|x_i\rangle_{AB}$ and $|y_i\rangle_{AB}$, where $i = 1, \dots, N$. First note that $(X \otimes I_B) \sum_{j=1, \dots, n} |j\rangle_A |j\rangle_B = |x\rangle_{AB}$ for any $|x\rangle_{AB}$. This means that the same input state $\sum_j |j\rangle |j\rangle$ (which is an unnormalized maximally entangled state) can always be transformed to any given state using its associated linear operator. Then the state transformation problem can be visualized as finding a quantum circuit (U_1 and U_2) that preserves the state $\sum_j |j\rangle |j\rangle$ processed by virtual gates X_i and Y_i where $i = 1, \dots, N$ (see Fig. 1(b)). Even though X_i and Y_i are not ordinary quantum gates because they are not unitary, they still transform states as linear operators and so we can still capture them in a quantum-circuit-like diagram. As we show below, the gate representation with X_i and Y_i is useful as it can capture our main results succinctly.

Using these notations, we have $\text{tr}_B |x\rangle_{AB} \langle x| = XX^\dagger$.

B. Notations

In what follows, we adopt the mathematicians' notation that the superscript $*$ denotes conjugate transpose and t denotes transpose. Thus, xx^* denotes $|x\rangle\langle x|$.

II. MAIN RESULTS

Theorem II.1. *Given pure states $x_1x_1^*, \dots, x_kx_k^*, y_1y_1^*, \dots, y_ky_k^* \in H_{mn}$, let X_i and Y_i be the $m \times n$ matrix forms of x_i and y_i for $i = 1, \dots, k$. Let E_{11} be the $p \times q$ matrix with 1 at the $(1, 1)$ position and 0 elsewhere. The following conditions are equivalent.*

(a) *There is a TPCP map T of the form (1) on tensor states such that $T(x_ix_i^*) = y_iy_i^*$ for $i = 1, \dots, k$.*

(b) *There is a unitary $U = U_1 \otimes U_2 \in M_{mp} \otimes M_{nq}$ such that*

$$U \begin{bmatrix} \tilde{x}_1 & \cdots & \tilde{x}_k \end{bmatrix} = \begin{bmatrix} \tilde{y}_1 & \cdots & \tilde{y}_k \end{bmatrix},$$

where \tilde{x}_i is the vector form of $E_{11} \otimes X_i$, \tilde{y}_i is the vector form of $R_i \otimes Y_i$ and $R_1, \dots, R_k \in M_{pq}$ have Frobenius norm one.

(c) *There are unitary $U \in M_{mp}$, $V \in M_{nq}$, and matrices $R_1, \dots, R_k \in M_{pq}$ such that*

$$\text{tr}R_iR_i^* = 1 \quad \text{and} \quad U(E_{11} \otimes X_i)V = R_i \otimes Y_i, \quad i = 1, \dots, k.$$

Proof. Note that, if we express $z \in \mathbb{C}^{mn}$ as an $m \times n$ matrix Z , then for any $F \in M_m$ and $G \in M_n$, the matrix form of $(F \otimes G)z$ is FZG^t . Thus, there exist $F_1, \dots, F_p \in M_m$ and $G_1, \dots, G_q \in M_n$ with $\sum F_i^*F_i = I_m$ and $\sum G_j^*G_j = I_n$ such that

$$\sum_{1 \leq i \leq p, 1 \leq j \leq q} (F_i \otimes G_j)x_lx_l^*(F_i \otimes G_j)^* = y_ly_l^* \quad \forall l = 1, \dots, k$$

if and only if

$$(F_i \otimes G_j)x_l = r_{ij}^l y_l \text{ for some scalars } r_{ij}^l \text{ satisfying } \sum_{1 \leq i \leq p, 1 \leq j \leq q} |r_{ij}^l|^2 = 1$$

$$(\text{and } \sum F_i^* F_i = I_m, \sum G_j^* G_j = I_n)$$

$$\iff F_i X_l G_j^t = r_{ij}^l Y_l \text{ with above constraints on } r_{ij}^l, F_i, G_j$$

$$\iff \begin{bmatrix} F_1 & * & * & * \\ F_2 & * & * & * \\ \vdots & * & * & * \\ F_p & * & * & * \end{bmatrix} \begin{bmatrix} X_l & 0 & \dots & 0 \\ 0 & 0 & & \\ \vdots & & \ddots & \\ 0 & \dots & \dots & 0 \end{bmatrix} \begin{bmatrix} G_1^t & G_2^t & \dots & G_q^t \\ * & * & * & * \\ * & * & * & * \\ * & * & * & * \end{bmatrix} = \begin{bmatrix} r_{11}^l Y_l & r_{12}^l Y_l & \dots & r_{1q}^l Y_l \\ r_{21}^l Y_l & r_{22}^l Y_l & & \\ \vdots & & \ddots & \\ r_{p1}^l Y_l & \dots & \dots & r_{pq}^l Y_l \end{bmatrix}$$

with previous constraints

$$\iff \exists \text{ unitary } U \in M_{pm}, V \in M_{qn} \text{ such that } U(E_{11} \otimes X_l)V = R_l \otimes Y_l \quad \forall l = 1, \dots, k$$

where $R_l \in M_{pq}$ has Frobenius norm one.

This shows that (a) and (c) are equivalent. By taking the vector form of the last equation we obtain equivalence with (b). \square

Example II.2. Clearly, the existence of unitaries $U \in M_m$ and $V \in M_n$ (in other words, $p = q = 1$, the case without ancilla) such that $UX_iV = Y_i$ for all $i = 1, \dots, k$ is a sufficient condition for a TPCP map of the desired form. It is not, however, necessary. Fix $s_1 > s_2 > 0$.

Let $X_1 = Y_1 = \begin{bmatrix} s_1 & 0 & 0 & 0 \\ 0 & s_2 & 0 & 0 \end{bmatrix}$. Let $X_2 = \begin{bmatrix} I_2 & I_2 \end{bmatrix}$ and $Y_2 = \begin{bmatrix} \frac{1}{c}I_2 & \frac{r}{c}I_2 \end{bmatrix}$, where $r, c \in \mathbb{R}$ satisfy

$1 + r^2 = 2c^2$ and $|c| < 1$. (For example, $c = 1/\sqrt{2}$ and $r = 0$ will suffice.)

Let $\gamma = \sqrt{1 - c^2}/c$ and define

$$U = I_2 \quad \text{and} \quad V = \begin{bmatrix} I_2 & 0 & 0 & 0 \\ 0 & rI_2 & \gamma I_2 & r\gamma I_2 \\ 0 & * & * & * \\ 0 & * & * & * \end{bmatrix} \in M_8,$$

where we can complete V to be a unitary matrix (since the first four rows are orthonormal). Then $U(E_{11} \otimes X_1)V = E_{11} \otimes Y_1$ and $U(E_{11} \otimes X_2)V = R \otimes Y$ where $R = \begin{bmatrix} c & \gamma c \end{bmatrix}$, so there is a tensor TPCP map that will interpolate. (Note $\text{tr}R^*R = 1$.)

However, if $U \in M_2$ and $V \in M_4$ are unitary matrices such that $UX_1V = Y_1$, then U must be a diagonal unitary and V must have the form $V = \begin{bmatrix} U^* & 0 \\ 0 & W \end{bmatrix}$ for some unitary $W \in M_2$.

But then $UX_2V = \begin{bmatrix} I_2 & UW \end{bmatrix} \neq Y_2$.

To be more specific, in the above example, let $s_1 = 2s_2 = 2/3$, $c = 1/\sqrt{2}$, and $r = 0$. If $\{e_1, \dots, e_{16}\}$ is the standard basis for \mathbb{C}^{16} , then for any choice of unitary $W \in M_{16}$ with the first, third, sixth, and eighth columns equal to e_1, e_9, e_6 , and e_{14} , respectively, we have $W[x_1 x_2] = [y_1 y_2]$, where $x_1 = y_1 = s_1 e_1 + s_2 e_6$, $x_2 = e_1 + e_3 + e_6 + e_8$, $y_2 = (e_1 + e_6)/c$ are the vector form of the matrices $X_1 = Y_1, X_2, Y_2$. Clearly, there are many choices of W and not every choice will yield a matrix of the form $U_1 \otimes U_2$ with $U_1 \in M_2$ and $U_2 \in M_8$.

Condition (c) of Theorem II.1 shows that it is very difficult to have an LO operation to transform the states. For example, one needs to have R_i such that $E_{11} \otimes X_i$ and $R_i \otimes Y_i$ are unitarily equivalent via the same U, V pair. In particular, $E_{11} \otimes X_i$ and $R_i \otimes Y_i$ have the same singular values. Thus, the rank of X_i must be a multiple of that of Y_i . For an individual pair of matrices X and Y , this condition is easy to check as shown in the following proposition.

Proposition II.3. *Let $x, y \in \mathbb{C}^{mn}$ be unit vectors and let $X, Y \in M_{mn}$ be their corresponding matrix forms. There is a tensor TPCP map sending xx^* to yy^* if and only if X and $R \otimes Y$ have the same nonzero singular values for some matrix R with Frobenius norm one.*

Furthermore, suppose X has nonzero singular values $\alpha_1 \geq \dots \geq \alpha_p > 0$ and Y has nonzero singular values $\beta_1 \geq \dots \geq \beta_q > 0$. Then the existence of R can be determined by the following algorithm:

Set $A_1 = \{\alpha_1, \dots, \alpha_p\}$. If $r = p/q$ is not an integer, no map exists. Otherwise, perform

the following.

For $i = 1, \dots, r$

Set $\gamma_i = (\max A_i)/\beta_1$;

If $\mathcal{S}_i = \{\beta_1\gamma_i, \beta_2\gamma_i, \dots, \beta_q\gamma_i\} \subset A_i$ then set $A_{i+1} = A_i \setminus \mathcal{S}_i$;

otherwise stop: no map exists.

If this program finishes with $A_{r+1} = \emptyset$, then take R to be any matrix with nonzero singular values $\gamma_1, \dots, \gamma_r$, and a map exists. (Note that R will automatically have Frobenius norm one.)

Proof. The first assertion follows from Theorem II.1. One readily verifies the algorithm. \square

We illustrate the algorithm in the following.

Example II.4. For simplicity, we ignore normalization in the following. Suppose $A_1 = \{4, 2, 2, 1\}$. If $\{\beta_i\} = \{2, 1\}$, then we can find $\{\gamma_i\} = \{2, 1\}$ to produce A_1 . If $\{\beta_i\} = \{4, 2\}$, then we can find $\{\gamma_i\} = \{1, 1/2\}$ to produce A_1 . On the other hand, if $\{\beta_i\} = \{2, 1, 1\}, \{2, 1/2\}$, or $\{1, 1\}$, then no $\{\gamma_i\}$ exists to produce A_1 .

One easily deduces more necessary conditions for the existence of LO map in Theorem II.1.

Corollary II.5. *Use the notation in Theorem II.1. If any one (and hence all) of the conditions (a) – (c) hold, then for any $1 \leq i \leq j \leq k$,*

$$U(E_{11}E_{11}^* \otimes X_iX_j^*)U^* = R_iR_j^* \otimes Y_iY_j^* \quad \text{and} \quad V^*(E_{11}^*E_{11} \otimes X_i^*X_j)V = R_i^*R_j \otimes Y_i^*Y_j.$$

In particular, the eigenvalues of $X_iX_j^$ can be obtained from those of $Y_iY_j^*$ by taking their multiple with some $\gamma_1^{(ij)}, \dots, \gamma_{\ell_{ij}}^{(ij)} \in \mathbb{C}$.*

If X_1, \dots, X_k and Y_1, \dots, Y_k are all rank one matrices, we have the following.

Corollary II.6. *Suppose the matrices X_i, Y_i for $i = 1, \dots, k$ constructed in Theorem II.1 have rank one. Let $X_i = a_i b_i^*, Y_i = c_i d_i^*$ with unit vectors $a_i, c_i \in \mathbb{C}^m, b_i, d_i \in \mathbb{C}^n$ for $i = 1, \dots, k$. Then conditions (a) - (c) in Theorem II.1 are equivalent to:*

(d) *There are unitary matrices $U \in M_{mp}, V \in M_{nq}$, and unit vectors $\zeta_1, \dots, \zeta_k \in \mathbb{C}^p, \eta_1, \dots, \eta_k \in \mathbb{C}^q$ such that*

$$U \begin{bmatrix} a_1 & \cdots & a_k \\ 0 & \cdots & 0 \end{bmatrix} = \begin{bmatrix} \zeta_1 \otimes c_1 & \cdots & \zeta_k \otimes c_k \end{bmatrix} \quad \text{and} \quad V^* \begin{bmatrix} b_1 & \cdots & b_k \\ 0 & \cdots & 0 \end{bmatrix} = \begin{bmatrix} \eta_1 \otimes d_1 & \cdots & \eta_k \otimes d_k \end{bmatrix}.$$

The next theorem reduces the general problem to the situation described in Corollary II.6. The key idea is to use the fact that every $m \times n$ matrix X of rank r admits a Schmidt decomposition $X = \sum_{j=1}^r s_j(X) a_j b_j^*$, where $s_1(X) \geq \cdots \geq s_r(X) > 0$, and $\{a_1, \dots, a_r\} \subseteq \mathbb{C}^m$ and $\{b_1, \dots, b_r\} \subseteq \mathbb{C}^n$ are orthonormal sets.

Theorem II.7. *Use the notation in Theorem II.1. Then any of the conditions (a) - (c) in Theorem II.1 holds only if*

(e) *for each $i = 1, \dots, k$, the matrix Y_i has a Schmidt decomposition $Y_i = \sum_{v=1}^{\text{rank}(Y_i)} s_v(Y_i) Y_{iv}$ and there are positive numbers $\gamma_{i1}, \dots, \gamma_{i\ell_i}$ with $\ell_i = \text{rank}(X_i)/\text{rank}(Y_i)$ such that X_i has a Schmidt decomposition $X_i = \sum_{u,v} \gamma_{iu} s_v(Y_i) X_{iuv}$ with $X_{iuv} \in M_{m,n}$, and there is a tensor TPCP map sending X_{iuv} to Y_{iv} for all i, u, v .*

Proof. We only need to show that (c) implies (e). If (c) holds, then $E_{11} \otimes X_i = U^*(R_i \otimes Y_i)V^*$ for each $i = 1, \dots, k$. Taking a Schmidt decomposition for each of $R_i = \sum s_u(R_i) R_{iu}$ and $Y_i = \sum s_v(Y_i) Y_{iv}$, where R_{iu} and Y_{iv} have rank one and Frobenius norm one, we see that $E_{11} \otimes X_i$ has a Schmidt decomposition

$$E_{11} \otimes X_i = \sum_{u,v} s_u(R_i) s_v(Y_i) \tilde{X}_{iuv} \quad \text{with} \quad \tilde{X}_{iuv} = U^*(R_{iu} \otimes Y_{iv})V^*.$$

We claim that $\tilde{X}_{iuv} = E_{11} \otimes X_{iuv}$ with $X_{iuv} \in M_{m,n}$. To see this, note that $\tilde{X}_{iuv} = \tilde{a}_{iuv} \tilde{b}_{iuv}^*$ for some unit vectors $\tilde{a}_{iuv} \in \mathbb{C}^{mp}$ and $\tilde{b}_{iuv} \in \mathbb{C}^{nq}$ such that

$$(E_{11} \otimes X_i) \tilde{b}_{iuv} = s_u(R_i) s_v(Y_i) \tilde{a}_{iuv} \quad \text{and} \quad (E_{11} \otimes X_i)^* \tilde{a}_{iuv} = s_u(R_i) s_v(Y_i) \tilde{b}_{iuv}.$$

Thus,

$$\tilde{a}_{iuv} = \begin{bmatrix} a_{iuv} \\ 0 \end{bmatrix} \quad \text{and} \quad \tilde{b}_{iuv} = \begin{bmatrix} b_{iuv} \\ 0 \end{bmatrix}$$

with $a_{iuv} \in \mathbb{C}^m$ and $b_{iuv} \in \mathbb{C}^n$. Thus, $\tilde{X}_{iuv} = E_{11} \otimes X_{iuv}$ with $X_{iuv} = a_{iuv}b_{iuv}^*$. Consequently, the tensor TPCP map described in (c) will send X_{iuv} to Y_{iv} . \square

Note that the converse (e) \implies (c) does not hold in general. However, one can readily verify that the converse holds if one makes the additional stipulation that there exist $R_{iu} \in M_{pq}$ and unitary $U \in M_{mp}$, $V \in M_{nq}$ such that $U(E_{11} \otimes X_{iuv})V = R_{iu} \otimes Y_{iv}$ for all i, u, v .

By the result in Ref. 15, we can extend Theorem II.1 to the following.

Corollary II.8. *Suppose $A_1, \dots, A_k \in M_{mn}$ are mixed states, and $y_1y_1^*, \dots, y_ky_k^* \in M_{mn}$ are pure states such that $A_i = \sum_{j=1}^{\ell_i} x_{ij}x_{ij}^*$ for $i = 1, \dots, k$, where ℓ_1, \dots, ℓ_k are positive integers. Then there is a TPCP map in the tensor form (1) such that $T(A_i) = y_iy_i^*$ for all $i = 1, \dots, k$ if and only if there is a TPCP map of the tensor form (1) such that $T(x_{ij}x_{ij}^*) = (x_{ij}^*x_{ij})y_iy_i^*$ for all $i = 1, \dots, k$, and $j = 1, \dots, \ell_i$.*

Proof. By the result in Ref. 15, there is a TPCP map T sending the mixed states A_1, \dots, A_k to $y_1y_1^*, \dots, y_ky_k^*$ if and only if there is a TPCP map sending $x_{ij}x_{ij}^*$ to $(x_{ij}^*x_{ij})y_iy_i^*$ for all $i = 1, \dots, k$, and $j = 1, \dots, \ell_i$. Clearly, if T has the tensor form (1) and sends A_i to $y_iy_i^*$, then $y_iy_i^* = T(A_i) = \sum T(x_{ij}x_{ij}^*) \geq T(x_{ij}x_{ij}^*)$, where $P \geq Q$ means that $P - Q$ is positive semidefinite. Considering the range space and the trace of $T(x_{ij}x_{ij}^*)$, we see that $T(x_{ij}x_{ij}^*) = (x_{ij}^*x_{ij})y_iy_i^*$. The converse is clear. \square

We close this section with the following example.

Example II.9. Suppose

$$X_1 = \frac{1}{\sqrt{85}} \begin{bmatrix} 8 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 4 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \quad Y_1 = \frac{4}{\sqrt{20}}a_1b_1^* + \frac{2}{\sqrt{20}}a_2b_2^*, \quad (4)$$

$$X_2 = \begin{bmatrix} \frac{1}{\sqrt{2}} & 0 \\ \frac{1}{\sqrt{2}} & 0 \\ 0 & \frac{1}{\sqrt{2}} \\ 0 & \frac{1}{\sqrt{2}} \end{bmatrix} \begin{bmatrix} \frac{3}{\sqrt{10}} & 0 \\ 0 & \frac{1}{\sqrt{10}} \end{bmatrix} \begin{bmatrix} \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} \end{bmatrix}, Y_2 = \frac{3}{\sqrt{10}}a_1b_1^* + \frac{1}{\sqrt{10}}a_2b_2^*, \quad (5)$$

where $\{a_1, a_2\}$ and $\{b_1, b_2\}$ are orthonormal sets. We use Theorem II.7 and Corollary II.6 to check whether there is a desired TPCP map for these states. As required by condition (e) of Theorem II.7, we verify that the singular values of X_1 and Y_1 are related by $\{\gamma_{11}, \gamma_{12}\} = \sqrt{\frac{20}{85}}\{2, 1/2\}$, and those of X_2 and Y_2 are related by $\gamma_{21} = 1$. Next, we check whether there is a tensor TPCP map sending rank one X_{iuv} to rank one Y_{iv} . For the left singular vectors, we seek a transformation that maps

$$\begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} \rightarrow a_1, \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} \rightarrow a_1, \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} \rightarrow a_2, \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} \rightarrow a_2, \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \\ 0 \\ 0 \end{bmatrix} \rightarrow a_1, \begin{bmatrix} 0 \\ 0 \\ \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{bmatrix} \rightarrow a_2. \quad (6)$$

Using previous results¹²⁻¹⁵, we form the Gram matrices of the input and output states

$$G_X = \begin{bmatrix} 1 & 0 & 0 & 0 & \frac{1}{\sqrt{2}} & 0 \\ 0 & 1 & 0 & 0 & \frac{1}{\sqrt{2}} & 0 \\ 0 & 0 & 1 & 0 & 0 & \frac{1}{\sqrt{2}} \\ 0 & 0 & 0 & 1 & 0 & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 & 0 & 1 & 0 \\ 0 & 0 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 & 1 \end{bmatrix}, G_Y = \begin{bmatrix} 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix}, \quad (7)$$

and check whether there is a correlation matrix M that satisfies $G_X = M \circ G_Y$. Clearly, $M = G_X$ is a valid choice.

For the right singular vectors, we seek a transformation that maps

$$\begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} \rightarrow b_1, \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} \rightarrow b_1, \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} \rightarrow b_2, \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} \rightarrow b_2, \frac{1}{2} \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix} \rightarrow b_1, \frac{1}{2} \begin{bmatrix} 1 \\ 1 \\ -1 \\ -1 \end{bmatrix} \rightarrow b_2. \quad (8)$$

The Gram matrices are

$$G_X = \begin{bmatrix} 1 & 0 & 0 & 0 & \frac{1}{2} & \frac{1}{2} \\ 0 & 1 & 0 & 0 & \frac{1}{2} & \frac{1}{2} \\ 0 & 0 & 1 & 0 & \frac{1}{2} & -\frac{1}{2} \\ 0 & 0 & 0 & 1 & \frac{1}{2} & -\frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & 1 & 0 \\ \frac{1}{2} & \frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} & 0 & 1 \end{bmatrix}, G_Y = \begin{bmatrix} 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix}. \quad (9)$$

Clearly, no M exists that satisfies $G_X = M \circ G_Y$. Therefore, no tensor TPCP map exists that transforms X_1 to Y_1 and X_2 to Y_2 .

III. CONNECTION WITH OTHER TRANSFORMATIONS

The transformation considered in this paper can be viewed as a combination of the one-party multiple-state transformation¹²⁻¹⁵ and the two-party single-state transformation¹⁸. Let's consider an example of transforming $\{|x_1\rangle_{AB}, |x_2\rangle_{AB}\}$ to $\{|y_1\rangle_{AB}, |y_2\rangle_{AB}\}$ where a single channel acting on AB exists to transform the two inputs to the two outputs simultaneously and two bipartite transformations exist to separately transform $|x_i\rangle_{AB}$ to $|y_i\rangle_{AB}$. However, no bipartite LO transformation exists mapping $|x_i\rangle_{AB}$ to $|y_i\rangle_{AB}$ for $i = 1, 2$ simultaneously. We use Theorem II.1 to check.

Consider systems A and B where each has dimension 4. Let

$$|x_1\rangle_{AB} = (1.6|00\rangle + 1.2|11\rangle + 0.8|22\rangle + 0.6|33\rangle)/\sqrt{5} \quad (10)$$

$$|y_1\rangle_{AB} = 0.8|00\rangle + 0.6|11\rangle \quad (11)$$

$$|x_2\rangle_{AB} = (1.2|00\rangle - 1.6|11\rangle - 0.6|22\rangle + 0.8|33\rangle)/\sqrt{5} \quad (12)$$

$$|y_2\rangle_{AB} = (2|00\rangle + |11\rangle)/\sqrt{5}. \quad (13)$$

Using the pure-state single-party result¹²⁻¹⁵, we can verify that a TPCP map T acting on AB exists such that $T(|x_i\rangle\langle x_i|) = |y_i\rangle\langle y_i|$ for $i = 1, 2$. We need to check the existence of a

correlation matrix M such that $G_X = M \circ G_Y$ where the Gram matrices $G_X = (\langle x_i | x_j \rangle) = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ and $G_Y = (\langle y_i | y_j \rangle) = \begin{bmatrix} 1 & 0.98 \\ 0.98 & 1 \end{bmatrix}$. Clearly, we can take $M = G_X$.

Next, we consider whether each input state $|x_i\rangle_{AB}$ can individually be transformed to $|y_i\rangle_{AB}$ using a bipartite LO transformation. According to Proposition II.3, X_i can be mapped to Y_i using a bipartite LO transformation if and only if X_i and $R_i \otimes Y_i$ have the same singular values, in other words, $U_i(E_{11} \otimes X_i)V_i = R_i \otimes Y_i$. We can verify that this is satisfied for $i = 1, 2$ with

$$X_1 = \frac{1}{\sqrt{5}} \begin{bmatrix} 1.6 & 0 & 0 & 0 \\ 0 & 1.2 & 0 & 0 \\ 0 & 0 & 0.8 & 0 \\ 0 & 0 & 0 & 0.6 \end{bmatrix}, R_1 = \frac{1}{\sqrt{5}} \begin{bmatrix} 2 & 0 \\ 0 & 1 \end{bmatrix}, Y_1 = \begin{bmatrix} 0.8 & 0 & 0 & 0 \\ 0 & 0.6 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}, \quad (14)$$

$$U_1 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & * & * & * & * \\ 0 & 0 & 0 & 0 & * & * & * & * \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & * & * & * & * \\ 0 & 0 & 0 & 0 & * & * & * & * \end{bmatrix}, V_1 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & * & * & 0 & 0 & * & * \\ 0 & 0 & * & * & 0 & 0 & * & * \\ 0 & 0 & * & * & 0 & 0 & * & * \\ 0 & 0 & * & * & 0 & 0 & * & * \end{bmatrix}, \quad (15)$$

and

$$X_2 = \frac{1}{\sqrt{5}} \begin{bmatrix} 1.2 & 0 & 0 & 0 \\ 0 & -1.6 & 0 & 0 \\ 0 & 0 & -0.6 & 0 \\ 0 & 0 & 0 & 0.8 \end{bmatrix}, R_2 = \begin{bmatrix} 0.6 & 0 \\ 0 & 0.8 \end{bmatrix}, Y_2 = \frac{1}{\sqrt{5}} \begin{bmatrix} 2 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}, \quad (16)$$

$$U_2 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & * & * & * & * \\ 0 & 0 & 0 & 0 & * & * & * & * \\ 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & * & * & * & * \\ 0 & 0 & 0 & 0 & * & * & * & * \end{bmatrix}, V_2 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & * & * & 0 & 0 & * & * \\ 0 & 0 & * & * & 0 & 0 & * & * \\ 0 & 0 & * & * & 0 & 0 & * & * \\ 0 & 0 & * & * & 0 & 0 & * & * \end{bmatrix}. \quad (17)$$

Thus, individual transformations are possible. This is consistent with Nielsen's result¹⁸.

Since the eigenvalues of $\text{tr}_B |x_i\rangle_{AB}\langle x_i| = X_i X_i^*$ are majorized by the eigenvalues of $\text{tr}_B |y_i\rangle_{AB}\langle y_i| = Y_i Y_i^*$, Nielsen's result implies that $|x_i\rangle_{AB}$ can be transformed to $|y_i\rangle_{AB}$ individually using a two-way LOCC protocol (which can be a LO transformation as a special case).

On the other hand, it is obvious that no bipartite LO transformation exists to simultaneously map $|x_i\rangle_{AB}$ to $|y_i\rangle_{AB}$ for $i = 1, 2$, since according to Theorem II.1, we must have $U_1 = U_2$ and $V_1 = V_2$ for such a transformation to exist. It is easily seen that this is not possible even if we extend the dimensions of U_i , V_i , and R_i .

IV. ADDITIONAL REMARKS

Even in the classical case, finding a correlation matrix M such that $(x_i^* x_j) = M \circ (y_i^* y_j)$ is highly non-trivial. If $(y_i^* y_j)$ has no zero entries, then M is uniquely determined. Clearly, if M exists, then $x_i^* x_j = 0$ whenever $y_i^* y_j = 0$. However, in these zero positions, it is not easy to decide how to choose the corresponding (i, j) entry in M so that M is positive semi-definite. Such a problem is known as a completion problem in matrix theory, and is very

challenging unless the specified entries of M have some nice pattern (such as the chordal graph pattern²⁴). Nonetheless, one can use positive semi-definite programming software to search for a solution for a given partial matrix (i.e., a matrix for which only some of the entries are specified).

For our problem, one may search for unitary $U \in M_{mnpq}$ of the form $U_1 \otimes U_2$ with $U_1 \in M_{mp}$ and $U_2 \in M_{nq}$ such that

$$U \begin{bmatrix} \tilde{x}_1 & \cdots & \tilde{x}_k \\ 0 & \cdots & 0 \end{bmatrix} = \begin{bmatrix} \tilde{y}_1 & \cdots & \tilde{y}_k \end{bmatrix}$$

as done in the proof of Theorem II.1. Alternatively, one may ignore the structure of U and search for unit vectors ξ_1, \dots, ξ_k such that

$$(x_i^* x_j) = (\xi_i^* \xi_j) \otimes (y_i^* y_j)$$

and

$$U(E_{11} \otimes X_i)V = R_i \otimes Y_i, \quad i = 1, \dots, k$$

as in Theorem II.1(c). Of course, finding ξ_1, \dots, ξ_k in this way is not easy.

V. CONCLUSIONS

We proved necessary and sufficient conditions for the existence of a LO transformation between two sets of entangled states. We also reduced the general problem for checking the existence of such LO transformation to smaller problems. However, a general algorithm seems to be difficult to obtain. On the other hand, if a LO transformation is not possible, one can easily use our theorems to rule out its existence in a computationally efficient manner. In fact, from our theorems, one can see that it is a rather stringent condition for a LO transformation to exist, especially when the number of states to transform is large. We hope that our results can shed some light on entanglement transformation and stimulate further investigation. Open problems include (i) the transformability between sets of states

using LOCC and separable operations and between sets of mixed states, (ii) probabilistic transformations where the final states are produced only probabilistically, and (iii) allowing the initial states and final states to have different dimensions.

ACKNOWLEDGMENTS

We thank Hoi-Kwong Lo for enlightening discussion, especially on prior works and interpretation of our result.

This research evolved in a faculty seminar on quantum information science at the University of Hong Kong in the spring of 2012 co-ordinated by Chau and Li. The support of the Departments of Physics and Mathematics of the University of Hong Kong is greatly appreciated.

Chau and Fung were partially supported by the Hong Kong RGC grant No. 700709P. Li and Sze were partially supported by the Hong Kong RGC grant PolyU 502910; this grant supported the visit of Poon in the spring of 2012. Li was also supported by a USA NSF grant; he was a visiting professor of the University of Hong Kong in the spring of 2012, an honorary professor of Taiyuan University of Technology (100 Talent Program scholar), and an honorary professor of Shanghai University.

REFERENCES

- ¹A. K. Ekert, “Quantum cryptography based on bell’s theorem,” *Phys. Rev. Lett.*, **67**, 661–663 (1991).
- ²C. H. Bennett, G. Brassard, and N. D. Mermin, “Quantum cryptography without bell’s theorem,” *Phys. Rev. Lett.*, **68**, 557–559 (1992).
- ³H.-K. Lo and H. F. Chau, “Unconditional security of quantum key distribution over arbitrarily long distances,” *Science*, **283**, 2050 (1999).

- ⁴D. Deutsch, “Quantum theory, the church-turing principle and the universal quantum computer,” *Proc. Royal Soc. London Series A*, **400**, 97–117 (1985).
- ⁵P. Shor, “Algorithms for quantum computation: discrete logarithms and factoring,” in *Foundations of Computer Science, 1994 Proceedings., 35th Annual Symposium on* (1994) pp. 124–134.
- ⁶D. P. DiVincenzo, “Quantum computation,” *Science*, **270**, 255–261 (1995).
- ⁷S. Lloyd, “Universal quantum simulators,” *Science*, **273**, 1073–1078 (1996).
- ⁸P. Shor, “Fault-tolerant quantum computation,” in *Foundations of Computer Science, 1996. Proceedings., 37th Annual Symposium on* (1996) pp. 56–65.
- ⁹J. I. Cirac, T. Pellizzari, and P. Zoller, “Enforcing coherent evolution in dissipative quantum dynamics,” *Science*, **273**, 1207–1210 (1996).
- ¹⁰D. Gottesman, “Theory of fault-tolerant quantum computation,” *Phys. Rev. A*, **57**, 127–137 (1998).
- ¹¹P. Alberti and A. Uhlmann, “A problem relating to positive linear maps on matrix algebras,” *Rep. Math. Phys.*, **18**, 163 – 176 (1980), ISSN 0034-4877.
- ¹²A. Uhlmann, “Eine bemerkung ber vollstndig positive abbildungen von dichteoperatoren,” *Wiss. Z. Karl-Marx-Univ. Leipzig, Math.-Naturwiss. Reihe*, **34**, 580–582 (1985).
- ¹³A. Chefles, “Deterministic quantum state transformations,” *Phys. Lett. A*, **270**, 14 – 19 (2000), ISSN 0375-9601.
- ¹⁴A. Chefles, “Quantum operations, state transformations and probabilities,” *Phys. Rev. A*, **65**, 052314 (2002).
- ¹⁵A. Chefles, R. Jozsa, and A. Winter, “On the existence of physical transformations between sets of quantum states,” *Int. J. Quant. Inf.*, **2**, 11–21 (2004).
- ¹⁶C. H. Bennett, H. J. Bernstein, S. Popescu, and B. Schumacher, “Concentrating partial entanglement by local operations,” *Phys. Rev. A*, **53**, 2046–2052 (1996).
- ¹⁷H.-K. Lo and S. Popescu, “Concentrating entanglement by local actions: beyond mean values,” *Phys. Rev. A*, **63**, 022301 (2001).

- ¹⁸M. A. Nielsen, “Conditions for a class of entanglement transformations,” *Phys. Rev. Lett.*, **83**, 436–439 (1999).
- ¹⁹D. Jonathan and M. B. Plenio, “Minimal conditions for local pure-state entanglement manipulation,” *Phys. Rev. Lett.*, **83**, 1455–1458 (1999).
- ²⁰B. He and J. A. Bergou, “Entanglement transformation with no classical communication,” *Phys. Rev. A*, **78**, 062328 (2008).
- ²¹V. Gheorghiu and R. B. Griffiths, “Separable operations on pure states,” *Phys. Rev. A*, **78**, 020304 (2008).
- ²²Z. Huang, C.-K. Li, E. Poon, and N.-S. Sze, “Efficient quantum key distribution with practical sources and detectors,” (2012), to appear in *J. Math. Phys.*, e-print arXiv:1203.5547 [math-ph].
- ²³R. A. Horn and C. R. Johnson, *Topics in Matrix Analysis* (Cambridge University Press, 1994) Chap. 4.
- ²⁴M. Laurent, “Matrix completion problems,” in *The Encyclopedia of Optimization, vol. III (Interior - M)*, edited by C. Floudas and P. Pardalos (Kluwer, 2001) pp. 221–229.