| | |
|---|---|
| Title | Conditions for degradability of tripartite quantum states |
| Author(s) | Fung, FCH; Li, CK; Sze, NS; Chau, HF |
| Citation | Journal of Physics A: Mathematical and Theoretical, 2014, v. 47 n. 11, p. article no. 115306 |
| Issued Date | 2014 |
| URL | http://hdl.handle.net/10722/195692 |
| Rights | Journal of Physics A: Mathematical and Theoretical. Copyright © Institute of Physics Publishing Ltd. |

# Conditions for degradability of tripartite quantum states

Chi-Hang Fred Fung
*Department of Physics and Center of Theoretical and Computational Physics, University of Hong Kong, Pokfulam Road, Hong Kong*

Chi-Kwong Li
*Department of Mathematics, College of William & Mary, Williamsburg, Virginia 23187-8795, USA*

Nung-Sing Sze
*Department of Applied Mathematics, The Hong Kong Polytechnic University, Hung Hom, Hong Kong*

H. F. Chau
*Department of Physics and Center of Theoretical and Computational Physics, University of Hong Kong, Pokfulam Road, Hong Kong*

**Abstract**

Alice, Bob, and Eve share a pure quantum state. We introduce the notion of state degradability by asking whether the joint density of Alice and Eve can be transformed to the joint density of Alice and Bob by processing Eve's part through a quantum channel, in order words, degrading Eve. We prove necessary and sufficient conditions for state degradability and provide an efficient method to quickly rule out degradability for a given state. The problem of determining degradability of states is different from that of quantum channels, although the notion is similar. One application of state degradability is that it can be used to test channel degradability. In particular, the degradability of the output state of a channel obtained from the maximally entangled input state gives information about the degradability of the channel.

## 1 Introduction

In quantum information processing, information is often encoded in quantum states which are transformed under quantum computation in order to carry out tasks such as the generation of secret keys [1, 2], encoding of error correcting codes [3, 4, 5, 6], and secret sharing [7, 8]. The general quantum state transformation problem concerns whether a state can be transformed via a quantum process to another state, possibly with some constraint on the quantum process. In as early as 1980's, Alberti and Uhlmann [9] studied the conditions for transforming two qubit mixed states. Subsequently, conditions for the transformations between two sets of pure states without any restriction on the number of states were found [10, 11, 12, 13]. The transformation of entangled

states under the condition that the two parties perform local operations has also been studied for a single bipartite state [14, 15, 16, 17, 18, 19] and for multiple bipartite states [20]. Extension to transformations for more than two parties has also been considered [21].

In this paper, we introduce the notion of state degradability, which is based on a transformation problem where we ask whether a subsystem can be degraded to another subsystem. More precisely, consider a quantum state in $|\psi\rangle \in H_A \otimes H_B$ shared by Alice and Bob. Assume that this state is processed by Eve and becomes an entangled state $|\tilde{\psi}\rangle \in H_A \otimes H_B \otimes H_E$. (In the context of quantum key distribution (QKD), such processing corresponds to eavesdropping by Eve or the noisy effect of the channel.) We are interested in constructing a quantum process $T : H_A \otimes H_E \to H_A \otimes H_B$ of the form

$$T(X) = \sum_{j=1}^{r} (I_A \otimes F_j) X (I_A \otimes F_j)^* \quad \text{with} \quad F_j : H_E \to H_B \quad \text{satisfying} \quad \sum_{j=1}^{r} F_j^* F_j = I_E \tag{1}$$

such that $T(\rho_{AE}) = \rho_{AB}$ for

$$\rho_{AE} = \mathrm{tr}_B(\rho) \in \mathcal{B}(H_A \otimes H_E), \ \rho_{AB} = \mathrm{tr}_E(\rho) \in \mathcal{B}(H_A \otimes H_B) \ \text{ with } \rho = |\tilde{\psi}\rangle\langle\tilde{\psi}|,$$

where $\mathcal{B}(H)$ is the set of bounded, positive-semidefinite operators acting on $H$, and $r$ is the number of Kraus operators of the quantum channel $T$ which can be arbitrary. If such a map $T$ exists, we call the state $|\tilde{\psi}\rangle$ $E \to B$ degradable. Similarly, if there exists a quantum channel $T' : H_A \otimes H_B \to H_A \otimes H_E$ such that $T'(\rho_{AB}) = \rho_{AE}$, we call the state $B \to E$ degradable. A state may be $E \to B$ and $B \to E$ degradable.

It is interesting to know whether a state is degradable. For example, in QKD if the joint state between Alice and Bob can be shown to be the same as the joint state between Alice and Eve via some processing of Eve's part, then no secret key can be generated with one-way postprocessing [22, 23, 24]. Also, state degradability is related to asymmetric quantum cloning [25, 26, 27], in which the two output subsystems are not necessarily copies of each other, but one subsystem can be transformed to be a clone of the other. If a given state is degradable, it means it could have been produced by asymmetric cloning of some other state.

Degradability has been studied in the context of quantum channels [28, 29]. Let us consider a channel in system $B$ which is described as a unitary transformation with ancillary system $E$ prepared in a standard state:

$$\Phi_B(\rho_B) = \mathrm{tr}_E[U_{BE}(\rho_B \otimes |0\rangle_E\langle 0|)U_{BE}^*].$$

Note that this system $A$ does not appear in this definition of degradable channel. This induces the complementary channel

$$\Phi_E(\rho_B) = \mathrm{tr}_B[U_{BE}(\rho_B \otimes |0\rangle_E\langle 0|)U_{BE}^*].$$

The channel $\Phi_B$ is called degradable when it may be degraded to $\Phi_E$, that is, there exists a quantum channel $\hat{T} : H_B \to H_E$ such that $\hat{T} \circ \Phi_B = \Phi_E$. Similarly, $\Phi_B$ is called anti-degradable when there exists a quantum channel $\hat{T} : H_E \to H_B$ such that $\hat{T} \circ \Phi_E = \Phi_B$.

It is clear that a degradable (anti-degradable) channel always output a state that is $B \to E$ ($E \to B$) degradable for any input. On the other hand, there are channels that output a degradable state for some input and a non-degradable state for another input. For example, consider this channel:

$$\begin{aligned} |0\rangle_B|0\rangle_E &\to |00\rangle_{BE} \\ |1\rangle_B|0\rangle_E &\to |11\rangle_{BE} \\ |2\rangle_B|0\rangle_E &\to |10\rangle_{BE}. \end{aligned}$$

For the input $|00\rangle_{AB}+|11\rangle_{AB}$, we get the output $|000\rangle_{ABE}+|111\rangle_{ABE}$ which is $B \to E$ and $E \to B$ degradable. But for the input $|00\rangle_{AB}+|11\rangle_{AB}+|22\rangle_{AB}$, we get $|000\rangle_{ABE}+|111\rangle_{ABE}+|210\rangle_{ABE}$. For this state, since to degrade $E$ to $B$, $|0\rangle_E$ has to change to $|0\rangle_B$ and $|1\rangle_B$, which is not possible without knowing $A$. Thus, the output state is not $E \to B$ degradable. With a similar argument, it is also not $B \to E$ degradable. This shows that a channel may output both degradable and non-degradable states. Therefore, it is a new problem to study degradable states without reference to whether the channel generating that state is degradable or not.

As one application of state degradability, we prove in Sec. 5 that state degradability can be used to test channel degradability. In particular, the degradability of the output state of a channel obtained from the maximally entangled input state gives information about the degradability of the channel. We show that if the channel output state of the maximally entangled input state is degradable, then the corresponding output state of the channel is degradable for any input state. Also, if the channel output state of the maximally entangled input state is not degradable, then the corresponding output state is not degradable for any input state in a special class.

In some applications, the issue of state degradability arises naturally in that Alice, Bob, and Eve are initially given a tripartite state, without regard to the details of how it is given. This may occur due to, for example, an entanglement source generating a tripartite state, or an unknown quantum channel processing one part of a bipartite input. As a specific example, in entanglement distillation [30], the problem is often cast as that given a noisy state in $AB$, which is purified to a tripartite state in $ABE$, the goal is to transform it (through, e.g., local operations and classical communications) to a maximally entangled state. This can be viewed as a problem of a given initial state. A similar situation occurs in QKD [1, 2]. After the quantum state transmission step, Alice and Bob are given bipartite states which they would like to transform to a secret key. They first learn about their states by error testing and then choose the appropriate procedures to correct bit errors and amplify privacy. This is also a problem centered on a given state. And as mentioned before, if the state is degradable, no secret key can be generated with one-way postprocessing [22, 23, 24]; and thus no maximal entanglement can be distilled.

We formulate the mathematical problem as follows.

**State-Degradability Problem** Let $x \in \mathbf{C}^n \otimes \mathbf{C}^p \otimes \mathbf{C}^q$. Let $X_i = \mathrm{tr}_i(xx^*)$ with $i = 1, 2, 3$, be the partial traces of $xx^*$ in the three subsystems: $\mathbf{C}^p \otimes \mathbf{C}^q$, $\mathbf{C}^n \otimes \mathbf{C}^q$, and $\mathbf{C}^n \otimes \mathbf{C}^p$. Determine conditions on $x$ (or a class of $x$) such that there is $T$ of the form (1) such that $T(X_2) = X_3$. Here,

we adopt the mathematical notation: $X_1 = \rho_{BE}$, $X_2 = \rho_{AE}$, and $X_3 = \rho_{AB}$. It turns out that this notation allows our mathematical results in the following sections to be concisely described. We will however switch back to the physicist notation of $A, B, E$ when we discuss examples of physical relevance. Also, we use the notations $M_p$ to denote the set of $p \times p$ matrices and $M_{p,q}$ the set of $p \times q$ matrices. In this paper, we consider systems of finite dimensions.

The problem of determining whether a state is degradable is similar to the problem of finding a symmetric extension of a state [23] in that both problems are characterized by the generation of Alice and Bob's state by processing Eve's part of Alice and Eve's state. However, in the latter problem, we are given Alice and Bob's state and we seek an extension that adds Eve to the overall state, while in our state degradability problem, a tripartite state is given initially.

We first give low dimension examples in Sec. 2 which helps to understand the nature of the problem. Then, in Sec. 3, we prove necessary and sufficient conditions for our state-degradability problem as stated above. We discuss the physical interpretation of the transformability conditions in Sec. 4. Sec. 5 discusses state degradability when a quantum channel is used to generate the overall state. The transformability conditions might be difficult to verify in general, and thus we propose an easily computable method that can quickly rule out degradability of a given state in Sec. 6. We discuss some additional problems and observations in Sec. 7. Finally, we conclude in Sec. 8.

## 2 Low dimension examples

**Example 1.** Suppose $x = (x_1, \ldots, x_8)^t \in \mathbf{C}^8 \equiv \otimes^3(\mathbf{C}^2)$. Let $xx^* \in M_8$ and $\mathrm{tr}_1, \mathrm{tr}_2, \mathrm{tr}_3$ be the partial trace on the three systems. Then

$$X_1 = \mathrm{tr}_1(xx^*) = (x_1x_2x_3x_4)^t(\bar{x}_1\bar{x}_2\bar{x}_3\bar{x}_4) + (x_5x_6x_7x_8)^t(\bar{x}_5\bar{x}_6\bar{x}_7\bar{x}_8),$$

$$X_2 = \mathrm{tr}_2(xx^*) = (x_1x_2x_5x_6)^t(\bar{x}_1\bar{x}_2\bar{x}_5\bar{x}_6) + (x_3x_4x_7x_8)^t(\bar{x}_3\bar{x}_4\bar{x}_7\bar{x}_8),$$

$$X_3 = \mathrm{tr}_3(xx^*) = (x_1x_3x_5x_7)^t(\bar{x}_1\bar{x}_3\bar{x}_5\bar{x}_7) + (x_2x_4x_6x_8)^t(\bar{x}_2\bar{x}_4\bar{x}_6\bar{x}_8),$$

where for ease of notations, we omitted the commas in the vectors such as $(x_1, x_2, x_3, x_4)$. We would like to know whether there is $T : M_4 \to M_4$ of the form

$$T(X) = \sum_j (I_2 \otimes F_j) X (I_2 \otimes F_j)^*$$

with $\sum_j F_j^* F_j = I_2$ such that $T(X_2) = X_3$.

**Example 2.** Let $x = (a, 0, b, 0, 0, a, 0, -b)^t$ with $2(a^2 + b^2) = 1$. This state is non-trivial since it is not symmetric in 2 and 3. Then

$$X_2 = \begin{pmatrix} a^2+b^2 & 0 & 0 & a^2-b^2 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ a^2-b^2 & 0 & 0 & a^2+b^2 \end{pmatrix} \qquad \text{and} \qquad X_3 = \begin{pmatrix} a^2 & ab & 0 & 0 \\ ab & b^2 & 0 & 0 \\ 0 & 0 & a^2 & -ab \\ 0 & 0 & -ab & b^2 \end{pmatrix}.$$

Let

$$F_1 = \begin{pmatrix} a & a \\ b & -b \end{pmatrix} \qquad \text{and} \qquad F_2 = \begin{pmatrix} a & -a \\ b & b \end{pmatrix}.$$

Then $F_1^*F_1 + F_2^*F_2 = I_2$, and $T(X_2) = X_3$ if

$$T(X) = (I_2 \otimes F_1)X_2(I_2 \otimes F_1)^* + (I_2 \otimes F_2)X_2(I_2 \otimes F_2)^*.$$

**Proposition 2.1.** *In Examples 1 and 2, the desired map exists if and only if there are $F_1, \ldots, F_r$ with $\sum_{j=1}^r F_j^*F_j = I_2$ such that the map $L : M_2 \to M_2$ defined by*

$$L(X) = \sum_{j=1}^r F_j X F_j^*$$

*satisfies $L(R_iR_j^*) = S_iS_j^*$ for $1 \le i, j \le 2$, where*

$$R_1 = \begin{pmatrix} x_1 & x_3 \\ x_2 & x_4 \end{pmatrix},\ R_2 = \begin{pmatrix} x_5 & x_7 \\ x_6 & x_8 \end{pmatrix},\ S_1 = \begin{pmatrix} x_1 & x_2 \\ x_3 & x_4 \end{pmatrix},\ S_2 = \begin{pmatrix} x_5 & x_6 \\ x_7 & x_8 \end{pmatrix}.$$

**Remark** Alternatively, we can check whether there is a TPCP map $T$ sending $R_1R_1^*, R_2R_2^*, (R_1 + R_2)(R_1 + R_2)^*, (R_1 + iR_2)(R_1 + iR_2)^*$ to $S_1S_1^*, S_2S_2^*, (S_1 + S_2)(S_1 + S_2)^*, (S_1 + iS_2)(S_1 + iS_2)^*$. This can be checked readily.

**Example 3.** Suppose $x = (x_1, \ldots, x_{16}) \in \mathbf{C}^2 \otimes \mathbf{C}^2 \otimes \mathbf{C}^4$. Let $xx^* \in M_{16}$ and $\mathrm{tr}_1, \mathrm{tr}_2, \mathrm{tr}_3$ be the partial trace on the three systems. Then

$$X_1 = \mathrm{tr}_1(xx^*) = (x_1 \cdots x_8)^t(\bar{x}_1 \cdots \bar{x}_8) + (x_9 \cdots x_{16})^t(\bar{x}_9 \cdots \bar{x}_{16}),$$

$$X_2 = \mathrm{tr}_2(xx^*) = u_1u_1^* + u_2u_2^* = [u_1u_2][u_1u_2]^*,$$

with

$$u_1 = (x_1x_2x_3x_4x_9x_{10}x_{11}x_{12})^t,\ u_2 = (x_5x_6x_7x_8x_{13}x_{14}x_{15}x_{16})^t,$$

and

$$X_3 = \mathrm{tr}_3(xx^*) = v_1v_1^* + \cdots + v_4v_4^* = [v_1 \cdots v_4][v_1 \cdots v_4]^*$$

$$v_1 = (x_1x_5x_9x_{13})^t,\ v_2 = (x_2x_6x_{10}x_{14})^t,\ v_3 = (x_3x_7x_{11}x_{15})^t,\ v_4 = (x_4x_8x_{12}x_{16})^t.$$

We would like to know whether there is $T : M_8 \to M_4$ of the form

$$T(X) = \sum_j (I_2 \otimes F_j)X(I_2 \otimes F_j)^*$$

with $\sum_j F_j^*F_j = I_4$ such that $T(X_2) = X_3$.

**Proposition 2.2.** *Using the notation of Example 3, let*

$$R_1 = \begin{pmatrix} x_1 & x_5 \\ x_2 & x_6 \\ x_3 & x_7 \\ x_4 & x_8 \end{pmatrix}, \quad R_2 = \begin{pmatrix} x_9 & x_{13} \\ x_{10} & x_{14} \\ x_{11} & x_{15} \\ x_{12} & x_{16} \end{pmatrix},$$

$$S_1 = \begin{pmatrix} x_1 & x_2 & x_3 & x_4 \\ x_5 & x_6 & x_7 & x_8 \end{pmatrix} = R_1^t, \quad S_2 = \begin{pmatrix} x_9 & x_{10} & x_{11} & x_{12} \\ x_{13} & x_{14} & x_{15} & x_{16} \end{pmatrix} = R_2^t.$$

*Then, in Example 3, the desired map exists if and only if there exists a TPCP map sending*

$$R_1R_1^*, R_2R_2^*, (R_1+R_2)(R_1+R_2)^*, (R_1+iR_2)(R_1+iR_2)^*$$

*to*

$$S_1S_1^*, S_2S_2^*, (S_1+S_2)(S_1+S_2)^*, (S_1+iS_2)(S_1+iS_2)^*.$$

We remark that Propositions 2.1 and 2.2 are special cases of Theorem 3.1 below.

# 3 General result

Suppose $x = (x_{ijk}) \in \mathbf{C}^n \otimes \mathbf{C}^p \otimes \mathbf{C}^q$. We always assume that the entries of $x$ are arranged in lexicographic (dictionary) order of the indexes $(ijk)$, i.e., $x_{111}$ is the first entry and $x_{npq}$ is the last entry.

**Theorem 3.1.** *Suppose $x = (x_{ijk}) \in \mathbf{C}^n \otimes \mathbf{C}^p \otimes \mathbf{C}^q$. Then $\operatorname{tr}_1(xx^*) = \sum_{i=1}^n (x_{ijk})(x_{ijk})^* \in M_{p,q}$,*

$$X_2 = \operatorname{tr}_2(xx^*) = \sum_{j=1}^p (x_{ijk})(x_{ijk})^* \in M_{n,q}, \quad X_3 = \operatorname{tr}_3(xx^*) = \sum_{k=1}^q (x_{ijk})(x_{ijk})^* \in M_{n,q}.$$

*Let*

$$S_i = (x_{ijk})_{1\le j\le p, 1\le k\le q} \in M_{p,q} \quad \text{and} \quad R_i = S_i^t \in M_{q,p} \quad \text{for } i = 1, \dots, n.$$

*Suppose $R_i$ has rank $k_i$ for $i = 1, \dots, n$. Set $R_i = U_iD_iV_i^t$ such that $D_i \in M_{k_i}$ is a diagonal matrix with positive diagonal entries arranged in descending order, $U_i$ and $V_i$ have orthonormal columns. Then the following conditions are equivalent.*

(a) *There is a TPCP map $T : M_n \otimes M_q \to M_n \otimes M_p$ of the form*

$$X \mapsto \sum_{j=1}^r (I_n \otimes F_j)X(I_n \otimes F_j)^* \quad \text{with} \quad F_1, \dots, F_r \in M_{p,q} \tag{2}$$

*satisfying $T(X_2) = X_3$.*

(b) *There is a TPCP map sending*

$$\{R_uR_v^* : 1 \le u, v \le n\} \qquad \text{to} \qquad \{S_uS_v^* : 1 \le u, v \le n\}.$$

(c) *There are $p \times q$ matrices $F_1, \ldots, F_r$ with $\sum_{j=1}^r F_j^* F_j = I_q$ and $k_i \times p$ matrices $W_{i1}, \ldots, W_{ir}$ such that for all $i, j = 1, \ldots, n$,*

$$[F_1 R_i \cdots F_r R_i] = V_i D_i [W_{i1} \cdots W_{ir}] \quad \text{and} \quad [W_{i1} \cdots W_{ir}][W_{j1} \cdots W_{jr}]^* = U_i^t \overline{U}_j.$$

*Proof.* Direct checking shows that $X_2 = (R_u R_v^*)_{1 \le u,v \le n}$ and $X_3 = (S_u S_v^*)_{1 \le u,v \le n}$. The map in the form (2) will send $X_2$ to $X_3$ if and only if $\sum_{j=1}^r (F_j R_u R_v^* F_j) = (S_u S_v^*)_{1 \le u,v \le n}$. Equivalently, the TPCP map $Y \mapsto \sum_{j=1}^r F_j Y F_j^*$ will send $R_u R_v^*$ to $S_u S_v^*$ for $1 \le u, v \le n$. Thus, (a) and (b) are equivalent.

Suppose (b) holds. Then for any $1 \le i, j \le n$,

$$\sum_\ell F_\ell R_i R_j^* F_\ell^* = V_i D_i U_i^t \overline{U}_j D_j V_j^*.$$

Considering $i = j$, we see that $\mathrm{col}(F_\ell U_i D_i) \subseteq \mathrm{col}(V_i D_i)$, where $\mathrm{col}(X)$ denotes the column space of $X$. Thus, $F_\ell R_i = V_i D_i W_{i\ell}$ for a suitable $k_i \times p$ matrix $W_{i\ell}$. Now,

$$\sum_\ell F_\ell R_i R_j^* F_\ell^* = V_i D_i [W_{i1} \cdots W_{ir}][W_{j1} \cdots W_{jr}]^* D_j V_j^* = V_i D_i U_i^t \overline{U}_j D_j V_j^*.$$

Multiplying $D_i^{-1} V_i^*$ to the left and multiplying $V_j D_j$ to the right, see that

$$[W_{i1} \cdots W_{ir}][W_{j1} \cdots W_{jr}]^* = U_i^t \overline{U}_j$$

as asserted in (c). The converse can be checked directly. □

**Theorem 3.2.** *Use the notation in Theorem 3.1. Suppose $R_i = u_i d_i v_i^t$ is rank one for $i = 1, \ldots, n$. Then conditions* (a) - (c) *in Theorem 3.1 are equivalent to the following.*

(d) *There are unit vectors $\gamma_1, \ldots, \gamma_n \in \mathbf{C}^r$ and a unitary $U$ such that*

$$U[e_1 \otimes u_1 \ldots e_1 \otimes u_n] = [\gamma_1 \otimes v_1 \cdots \gamma_n \otimes v_n].$$

(e) *There is a correlation matrix $C$ such that $(u_i^* u_j) = (v_i^* v_j) \circ C$.*

(f) *There exists a TPCP map sending $u_i u_i^*$ to $v_i v_i^*$ for $i = 1, \ldots, n$.*

*Here, we abuse the notation of $e_1 \otimes u_i$ to represent a vector in $\mathbf{C}^{pr}$ with the first $q$ elements being $u_i$ and the remaining elements being zero.*

*Proof.* Using condition (c) and focusing on the column space and row space of $F_\ell u_j d_j v_j^t = v_j w_{j\ell}^t$, we see that $w_{j\ell} = d_j \gamma_{j\ell} v_j$ for some $\gamma_{j\ell} \in \mathbf{C}$ for $j = 1, \ldots, n$, and

$$(u_i^t \overline{u}_j) = ((\gamma_i \otimes v_i)^t (\overline{\gamma}_j \otimes \overline{v}_j)) = (\gamma_i^t \overline{\gamma_j}) \circ (v_i^t \overline{v}_j),$$

where $\gamma_i = (\gamma_{i1}, \ldots, \gamma_{ir})^t$ is a unit vector for $i = 1, \ldots, n$. Thus, there is a unitary $U \in M_{pr}$ such that $U[e_1 \otimes u_1 \ldots e_1 \otimes u_n] = [\gamma_1 \otimes v_1 \cdots \gamma_n \otimes v_n]$. If (d) holds, one can check condition (c) readily.

The equivalence of (d), (e), (f) follow from the results in Ref. [31]. □

**Corollary 3.3.** *Use the notation in Theorem 3.2. The following are equivalent.*

(a) *There are TPCP maps* $T = I_n \otimes T_1$ *and* $L = I_n \otimes L_1$ *such that* $T(X_2) = X_3$ *and* $L(X_3) = X_2$.

(b) *There is a diagonal unitary matrix* $E \in M_n$ *such that* $(u_i^* u_j) = E^*(v_i^* v_j)E$.

(c) *We may enlarge* $[u_1 \cdots u_n]$ *and* $[v_1 \ldots v_n]$ *by adding zero rows to get* $m \times n$ *matrices* $\tilde{U}$ *and* $\tilde{V}$ *with* $m = \max\{p, q\}$ *such that* $W\tilde{U} = \tilde{V}E$ *for a unitary* $W \in M_m$ *and a diagonal unitary* $E \in M_n$.

In Example 2, we have $R_1 = aE_{11} + bE_{22}$ and $R_2 = aE_{21} - bE_{22}$. There is TPCP map sending $X_3$ to $X_2$ if and only if $a^2 - b^2 = 0$. In such a case, we can set $L(X) = (I_2 \otimes G)X(I_2 \otimes G)^*$ with $G = (a^2 + b^2)^{-1/2} \begin{pmatrix} a & b \\ a & -b \end{pmatrix} = \sqrt{2} \begin{pmatrix} a & b \\ a & -b \end{pmatrix}$. By the fact that $a^2 + b^2 = 1/2$ and $a^2 - b^2 = 0$, we see that $L(X_3) = X_2$.

# 4 Physical interpretation of the transformability conditions

Using the physics notation, Alice, Bob, and Eve share a tripartite pure state $|\Psi\rangle_{ABE}$ which corresponds to $x$ in Sec. 3 with $x_{ijk} = \langle ijk|\Psi\rangle_{ABE}$ where $|ijk\rangle_{ABE}$ is an eigenstate in the computational basis (note that the indexes start at 1 instead of the usual 0). Define $|\Psi_i\rangle_{BE} \triangleq (\langle i|_A \otimes I_{BE})|\Psi\rangle_{ABE}$, which is a state conditional on $A$ being $|i\rangle_A$. Thus, we have

$$|\Psi\rangle_{ABE} = \sum_{i=1}^{n} |i\rangle_A |\Psi_i\rangle_{BE}.$$

According to the definitions of $R_i$ and $S_i$,

$$\begin{aligned} R_i R_i^* &= \mathrm{tr}_B(|\Psi_i\rangle_{BE}\langle\Psi_i|) \triangleq \rho_E^{(i)} \qquad \text{and} \\ S_i S_i^* &= \mathrm{tr}_E(|\Psi_i\rangle_{BE}\langle\Psi_i|) \triangleq \rho_B^{(i)} \qquad \text{for } i = 1, \ldots, n. \end{aligned}$$

In other words, $\rho_E^{(i)}$ is the reduced density matrix of $E$ conditioned on $A$ being $|i\rangle_A$; similarly for $\rho_B^{(i)}$. Note that for the rest of this section, we use the physics notation of $A, B, E$ to label states.

If Eve can imitate Bob using quantum channel $\mathcal{E}$ (i.e., $\mathcal{E}(\rho_{AE}) = \rho_{AB}$), then

$$\langle\phi|_A \mathcal{E}(\rho_{AE})|\phi\rangle_A = \langle\phi|_A \rho_{AB}|\phi\rangle_A \tag{3}$$

for any $|\phi\rangle_A$. Thus, when the projections are on the computational basis for $A$, the quantum channel is able to transform $\rho_E^{(i)}$ to $\rho_B^{(i)}$, i.e.,

$$\mathcal{E}(R_i R_i^*) = S_i S_i^*, \tag{4}$$

for $i = 1, \ldots, n$. On the other hand, the transformability condition of Theorem 3.1 (b) includes additional cross terms (i.e., $R_u R_v^* \to S_u S_v^*$ for $u \neq v$). Essentially, the transformability of the cross terms guarantees the transformability of $E$ to $B$ in other bases. To see this, consider the $\{+, -\}$ complementary basis for $A$ where we define $|\pm\rangle_A = (|1\rangle_A \pm |2\rangle_A)/\sqrt{2}$. If Eve is able to pretend to be

Bob, (3) means that the transformation $\rho_E^{(\pm)} \to \rho_B^{(\pm)}$ is possible, where $\rho_E^{(\pm)} \triangleq \mathrm{tr}_B(|\Psi_\pm\rangle_{BE}\langle\Psi_\pm|)$, $\rho_B^{(\pm)} \triangleq \mathrm{tr}_E(|\Psi_\pm\rangle_{BE}\langle\Psi_\pm|)$, and $|\Psi_\pm\rangle_{BE} = (|\Psi_1\rangle_{BE} \pm |\Psi_2\rangle_{BE})/\sqrt{2}$. In other words, (3) becomes

$$\mathcal{E}(\rho_E^{(\pm)}) = \rho_B^{(\pm)} \tag{5}$$

$$\Leftrightarrow$$

$$\mathcal{E}(R_1R_1^* + R_2R_2^* \pm R_1R_2^* \pm R_2R_1^*) = S_1S_1^* + S_2S_2^* \pm S_1S_2^* \pm S_2S_1^*. \tag{6}$$

Here, the reduced density matrix of $E$ conditioned on $A$ being $|\pm\rangle_A$ is $\rho_E^{(\pm)} = R_\pm R_\pm^*$. According to the definition of $R_i$ which is a rearragement of the elements of $|\Psi_i\rangle_{BE}$ for $i = +, -, 1, 2$, $R_\pm = (R_1 \pm R_2)/\sqrt{2}$. We have similar expressions for $B$. Given (4), (6) is true if and only if

$$\mathcal{E}(R_1R_2^* + R_2R_1^*) = S_1S_2^* + S_2S_1^*.$$

This shows that the transformability of the cross terms $R_uR_v^* \to S_uS_v^*$ for $u \neq v$ guarantees the transformability of $E$ to $B$ in other bases. Therefore, one cannot simplify the condition checking of Theorem 3.1 (b) by ignoring the cross terms. The following example illustrates this point by showing that there exists a state for which $R_uR_v^* \to S_uS_v^*$ for $u = v$ but not $u \neq v$.

**Example 4.** The initial state is a $3 \times 2 \times 2$ system in $A$, $B$, and $E$:

$$\begin{aligned}
|\Psi\rangle_{ABE} &= |1\rangle_A \otimes \left[ \begin{pmatrix} \alpha \\ \beta \end{pmatrix}_B \otimes \begin{pmatrix} a \\ b \end{pmatrix}_E + \begin{pmatrix} \alpha \\ -\beta \end{pmatrix}_B \otimes \begin{pmatrix} a \\ -b \end{pmatrix}_E \right] + \\
&\quad |2\rangle_A \otimes \begin{pmatrix} \alpha \\ \imath\beta \end{pmatrix}_B \otimes \begin{pmatrix} a \\ b \end{pmatrix}_E + |3\rangle_A \otimes \begin{pmatrix} \alpha \\ -\imath\beta \end{pmatrix}_B \otimes \begin{pmatrix} a \\ -b \end{pmatrix}_E \qquad (7) \\
&\triangleq |1\rangle_A \otimes \Big[ |p_+\rangle_B \otimes |\phi_+\rangle_E + |p_-\rangle_B \otimes |\phi_-\rangle_E \Big] + \\
&\quad |2\rangle_A \otimes |q_+\rangle_B \otimes |\phi_+\rangle_E + |3\rangle_A \otimes |q_-\rangle_B \otimes |\phi_-\rangle_E \qquad (8)
\end{aligned}$$

where $\alpha, \beta = \sqrt{1-\alpha^2}, a, b = \sqrt{1-a^2} \in \mathcal{R}$, and $\imath = \sqrt{-1}$.

Our goal is to show that there exists a quantum channel $\mathcal{E}$ such that (i) $\mathcal{E}(\rho_E^{(j)}) = \rho_B^{(j)}, j = 1, 2, 3$, i.e.,

$$\mathcal{E}(R_jR_j^*) = S_jS_j^*, \;\; j = 1, 2, 3, \tag{9}$$

and (ii) there does not exist a quantum channel $\mathcal{E}$ such that

$$\mathcal{E}(R_jR_k^*) = S_jS_k^*, \;\; j, k = 1, 2, 3. \tag{10}$$

This means that (9) does not imply (10).

We show that (9) holds but (5) does not hold for the state in (7).

**Proof of the validity of (9)**

First, we show that (9) holds. Assume that $\langle\phi_+|\phi_-\rangle < \langle q_+|q_-\rangle$ and so there exists a quantum channel $\mathcal{E}$ that transforms $|\phi_\pm\rangle \longrightarrow |q_\pm\rangle$. This can be verified by comparing the Gram matrices of the initial set of states and the final one [10, 11, 12, 13].

The quantum channel $\mathcal{E}$ is equivalent to a unitary transformation $U_{EE'}$ using an extended Hilbert space $E'$:

$$\begin{aligned} |\Psi'\rangle_{ABEE'} &= U_{EE'}|\Psi\rangle_{ABE}|0\rangle_{E'} && (11)\\ &= |1\rangle_A \otimes |\Psi'_1\rangle_{BEE'} + |2\rangle_A \otimes |\Psi'_2\rangle_{BEE'} + |3\rangle_A \otimes |\Psi'_3\rangle_{BEE'} && (12)\end{aligned}$$

where $\left|\Psi'_j\right\rangle_{BEE'} = U_{EE'}|\Psi_j\rangle_{BE}|0\rangle_{E'}, j = 1, 2, 3.$

Note that $\mathcal{E}(R_j R_j^*) = \mathrm{tr}_{BE'}(\left|\Psi'_j\right\rangle_{BEE'}\left\langle\Psi'_j\right|) = \mathcal{E}(\rho_E^{(j)})$.

In order that $\mathcal{E}(\rho_E^{(2)}) = \rho_B^{(2)} = |q_+\rangle\langle q_+|$, $U_{EE'}$ must transform as

$$\begin{aligned} & U_{EE'}|\Psi_2\rangle_{BE}|0\rangle_{E'} \\ = \; & U_{EE'}|q_+\rangle_B|\phi_+\rangle_E|0\rangle_{E'} \\ = \; & |q_+\rangle_B|q_+\rangle_E|x_+\rangle_{E'}, \end{aligned}$$

where $|x_+\rangle_{E'}$ is some normalized vector. Similarly, $\mathcal{E}(\rho_E^{(3)}) = \rho_B^{(3)}$ implies that

$$U_{EE'}|\Psi_3\rangle_{BE}|0\rangle_{E'} = |q_-\rangle_B|q_-\rangle_E|x_-\rangle_{E'},$$

where $|x_-\rangle_{E'}$ is some normalized vector. Then, we have

$$\begin{aligned} |\Psi'\rangle_{ABEE'} &= |1\rangle_A\Big[|p_+\rangle_B|q_+\rangle_E|x_+\rangle_{E'} + |p_-\rangle_B|q_-\rangle_E|x_-\rangle_{E'}\Big] + \\ & \quad |2\rangle_A|q_+\rangle_B|q_+\rangle_E|x_+\rangle_{E'} + |3\rangle_A|q_-\rangle_B|q_-\rangle_E|x_-\rangle_{E'} && (13)\end{aligned}$$

We now verify that $\mathcal{E}(\rho_E^{(1)}) = \rho_B^{(1)}$. The LHS is

$$\begin{aligned} \mathcal{E}(\rho_E^{(1)}) &= \mathrm{tr}_{BE'}(|\Psi'_1\rangle_{BEE'}\langle\Psi'_1|) \\ &= \mathrm{tr}_{BE'}\Big[P(|p_+\rangle_B|q_+\rangle_E|x_+\rangle_{E'} + |p_-\rangle_B|q_-\rangle_E|x_-\rangle_{E'})\Big] \\ &= |q_+\rangle_E\langle q_+| + |q_-\rangle_E\langle q_-| + C|q_+\rangle_E\langle q_-| + C^*|q_-\rangle_E\langle q_+| \end{aligned}$$

where $P(|\varphi\rangle) \triangleq |\varphi\rangle\langle\varphi|$, and $C \triangleq \langle p_-|p_+\rangle_B\langle x_-|x_+\rangle_{E'}$. Substituting the various vectors using (7),

$$\mathcal{E}(\rho_E^{(0)}) = \begin{pmatrix} 2\alpha^2 & 0 \\ 0 & 2\beta^2 \end{pmatrix} + C\begin{pmatrix} \alpha^2 & \imath\alpha\beta \\ \imath\alpha\beta & -\beta^2 \end{pmatrix} + C^*\begin{pmatrix} \alpha^2 & -\imath\alpha\beta \\ -\imath\alpha\beta & -\beta^2 \end{pmatrix}. \quad (14)$$

The RHS is

$$\begin{aligned} \rho_B^{(1)} &= \mathrm{tr}_E(|\Psi_1\rangle_{BE}\langle\Psi_1|) \\ &= \mathrm{tr}_E\Big[P(|p_+\rangle_B|\phi_+\rangle_E + |p_-\rangle_B|\phi_-\rangle_E)\Big] \\ &= |p_+\rangle_B\langle p_+| + |p_-\rangle_B\langle p_-| + \langle\phi_-|\phi_+\rangle_E|p_+\rangle_B\langle p_-| + \langle\phi_+|\phi_-\rangle_E|p_-\rangle_B\langle p_+| \\ &= \begin{pmatrix} 2\alpha^2 & 0 \\ 0 & 2\beta^2 \end{pmatrix} + (a^2 - b^2)\begin{pmatrix} 2\alpha^2 & 0 \\ 0 & -2\beta^2 \end{pmatrix}. \end{aligned}$$

This means that $\mathcal{E}(\rho_E^{(1)}) = \rho_B^{(1)}$ if and only if $C = a^2 - b^2$. This is possible since we have assumed that $\langle\phi_+|\phi_-\rangle < \langle q_+|q_-\rangle = \langle p_+|p_-\rangle$. We impose that $|x_\pm\rangle$ be chosen such that $C = a^2 - b^2$, and thus $\mathcal{E}(\rho_E^{(j)}) = \rho_B^{(j)}$ for $j = 1, 2, 3$.

**Invalidity of (5) for the state in (7)**

We now show that (5) does not hold given that

$$C = (\alpha^2 - \beta^2)\langle x_-|x_+\rangle = a^2 - b^2. \tag{15}$$

Expressing (13) in the $\{+,-\}$ basis, we have

$$\begin{aligned}
|\Psi'\rangle_{ABEE'} &= U_{EE'}|\Psi\rangle_{ABE}|0\rangle_{E'} \\
&= \frac{1}{\sqrt{2}}|+\rangle_A\Big[(|p_+\rangle_B + |q_+\rangle_B)|q_+\rangle_E|x_+\rangle_{E'} + |p_-\rangle_B|q_-\rangle_E|x_-\rangle_{E'}\Big] + \\
&\quad \frac{1}{\sqrt{2}}|-\rangle_A\Big[(|p_+\rangle_B - |q_+\rangle_B)|q_+\rangle_E|x_+\rangle_{E'} + |p_-\rangle_B|q_-\rangle_E|x_-\rangle_{E'}\Big] + \\
&\quad |3\rangle_A|q_-\rangle_B|q_-\rangle_E|x_-\rangle_{E'} \\
&\triangleq |+\rangle_A \otimes \big|\Psi'_+\big\rangle_{BEE'} + |-\rangle_A \otimes \big|\Psi'_-\big\rangle_{BEE'} + |3\rangle_A \otimes |\Psi'_3\rangle_{BEE'}.
\end{aligned}$$

We show that $\mathcal{E}(\rho_E^{(-)}) \neq \rho_B^{(-)}$. The LHS is

$$\begin{aligned}
2\mathcal{E}(\rho_E^{(-)}) &= 2\mathrm{tr}_{BE'}(\big|\Psi'_-\big\rangle_{BEE'}\big\langle\Psi'_-\big|) \\
&= \mathrm{tr}_{BE'}\Big[P(\big|p'_+\big\rangle_B|q_+\rangle_E|x_+\rangle_{E'} + |p_-\rangle_B|q_-\rangle_E|x_-\rangle_{E'})\Big] \\
&= \big\langle p'_+|p'_+\big\rangle|q_+\rangle_E\langle q_+| + |q_-\rangle_E\langle q_-| + D|q_+\rangle_E\langle q_-| + D^*|q_-\rangle_E\langle q_+|
\end{aligned}$$

where $\big|p'_+\big\rangle_B = |p_+\rangle_B - |q_+\rangle_B$, and $D \triangleq \big\langle p_-|p'_+\big\rangle_B\langle x_-|x_+\rangle_{E'}$. Substituting the various vectors using (7),

$$\begin{aligned}
\big|p'_+\big\rangle_B &= \begin{pmatrix} 0 \\ (1-\imath)\beta \end{pmatrix}_B \text{ and} \\
2\mathcal{E}(\rho_E^{(-)}) &= 2\beta^2\begin{pmatrix} \alpha^2 & -\imath\alpha\beta \\ \imath\alpha\beta & \beta^2 \end{pmatrix} + \begin{pmatrix} \alpha^2 & \imath\alpha\beta \\ -\imath\alpha\beta & \beta^2 \end{pmatrix} + D\begin{pmatrix} \alpha^2 & \imath\alpha\beta \\ \imath\alpha\beta & -\beta^2 \end{pmatrix} + D^*\begin{pmatrix} \alpha^2 & -\imath\alpha\beta \\ -\imath\alpha\beta & -\beta^2 \end{pmatrix}
\end{aligned}$$

where $D = -(1-\imath)\beta^2\langle x_-|x_+\rangle$. The RHS is

$$\begin{aligned}
2\rho_B^{(-)} &= 2\mathrm{tr}_E(|\Psi_-\rangle_{BE}\langle\Psi_-|) \\
&= \mathrm{tr}_E\Big[P(\big|p'_+\big\rangle_B|\phi_+\rangle_E + |p_-\rangle_B|\phi_-\rangle_E)\Big] \\
&= \big|p'_+\big\rangle_B\big\langle p'_+\big| + |p_-\rangle_B\langle p_-| + \langle\phi_-|\phi_+\rangle_E\big|p'_+\big\rangle_B\langle p_-| + \langle\phi_+|\phi_-\rangle_E|p_-\rangle_B\big\langle p'_+\big| \\
&= \begin{pmatrix} 0 & 0 \\ 0 & 2\beta^2 \end{pmatrix} + \begin{pmatrix} \alpha^2 & -\alpha\beta \\ -\alpha\beta & \beta^2 \end{pmatrix} + (a^2 - b^2)\begin{pmatrix} 0 & (1+\imath)\alpha\beta \\ (1-\imath)\alpha\beta & -2\beta^2 \end{pmatrix}.
\end{aligned}$$

To show that $\mathcal{E}(\rho_E^{(-)}) \neq \rho_B^{(-)}$, we compare their $(1,1)$ elements. The RHS is $\alpha^2$, and the LHS is $\alpha^2(2\beta^2 + 1 + D + D^*) = \alpha^2(2\beta^2 + 1 - 2\beta^2\langle x_-|x_+\rangle_{E'})$. However, due to the assumption in (15), $\langle x_-|x_+\rangle_{E'} \neq 1$ in general. Therefore, $\mathcal{E}(\rho_E^{(-)}) \neq \rho_B^{(-)}$.

## 5 Degradability for a given quantum channel

We discuss state degradability when the overall state is generated by a given quantum channel. We show that if the channel output state of the maximally entangled input state is degradable, then the corresponding output state is degradable for any input state. Also, if the channel output state of the maximally entangled input state is not degradable, then the corresponding output state is not degradable for any input state in a special class.

**Theorem 5.1.** *Suppose that a state $|\tilde{\psi}\rangle_{ABE}$ is generated by processing a state $|\psi\rangle_{AB}$ by a channel $\Phi_B$ acting on subsystem $B$ with an ancilla in subsystem $E$. The channel is implemented by a unitary extension $U_{BE}$ as follows:*

$$|\tilde{\psi}\rangle_{ABE} = (I_A \otimes U_{BE})|\psi\rangle_{AB}|0\rangle_E \triangleq U_{ABE}|\psi\rangle_{AB}|0\rangle_E,$$

*where $\Phi_B(\mathrm{tr}_A(P(|\psi\rangle_{AB}))) = \mathrm{tr}_{AE}(P(|\tilde{\psi}\rangle_{ABE}))$ with $P(|\cdot\rangle) = |\cdot\rangle\langle\cdot|$. We assume that the dimensions of subsystems $A$ and $B$ are the same, $n$, so that the maximally entangled state $|\psi_M\rangle_{AB} = \sum_{i=1}^{n}|ii\rangle_{AB}$ is defined. Using $|\psi_M\rangle_{AB}$ as the input state, if the output state $U_{ABE}|\psi_M\rangle_{AB}|0\rangle_E$ is $E \to B$ degradable with $T$ of the form (1) [i.e., $T$ satisfies $T(\rho_{AE}) = \rho_{AB}$ where $\rho_{AE} = \mathrm{tr}_B(\rho)$ and $\rho_{AB} = \mathrm{tr}_E(\rho)$ with $\rho = P(U_{ABE}|\psi_M\rangle_{AB}|0\rangle_E)$], then the output state $U_{ABE}|\psi\rangle_{AB}|0\rangle_E$ is $E \to B$ degradable with the same $T$ for any input state $|\psi\rangle_{AB}$.*

*Proof.* First, note that any state $|\psi\rangle_{AB}$ can be expressed as $|\psi\rangle_{AB} = (K_A \otimes I_B)|\psi_M\rangle_{AB}$ where $K_A = \sum_{i,j=1}^{n}|j\rangle_A\langle i|\,\langle ji|\psi\rangle_{AB}$. Note that $K_A$ is not necessarily invertible. Next, the condition for $E \to B$ degradability of the maximally entangled state means that

$$T(\rho_{AE}) = \rho_{AB} \tag{16}$$

$$\Rightarrow \quad T((K_A \otimes I)\rho_{AE}(K_A^* \otimes I)) = (K_A \otimes I)\rho_{AB}(K_A^* \otimes I) \text{ for any } K_A \tag{17}$$

where the last line is because $T$ acts only on subsystem $E$. Finally, the term on the LHS is

$$(K_A \otimes I)\rho_{AE}(K_A^* \otimes I) = \mathrm{tr}_B\left[P(U_{ABE}(K_A \otimes I_{BE})|\psi_M\rangle_{AB}|0\rangle_E)\right] \tag{18}$$

$$= \mathrm{tr}_B\left[P(U_{ABE}|\psi\rangle_{AB}|0\rangle_E)\right] \tag{19}$$

and we have an analogous term on the RHS. Thus, we have

$$T(\mathrm{tr}_B\left[P(U_{ABE}|\psi\rangle_{AB}|0\rangle_E)\right]) = \mathrm{tr}_E\left[P(U_{ABE}|\psi\rangle_{AB}|0\rangle_E)\right] \tag{20}$$

which means that the output state is $E \to B$ degradable for any input state $|\psi\rangle_{AB}$. □

**Corollary 5.2.** *For the channel $\Phi_B$, if the output state $U_{ABE}|\psi_M\rangle_{AB}|0\rangle_E$ is $E \to B$ degradable for the maximally entangled input state $|\psi_M\rangle_{AB}$, then the channel $\Phi_B$ is anti-degradable with respect to the complementary channel $\Phi_E$ [i.e., there exists a quantum channel $\hat{T} : H_E \to H_B$ such that $\hat{T} \circ \Phi_E = \Phi_B$]. Here, in terms of $U_{BE}$,*

$$\Phi_B(\rho_B) = \mathrm{tr}_E\left[U_{BE}(\rho_B \otimes |0\rangle_E\langle 0|)U_{BE}^*\right], \text{ and} \tag{21}$$

$$\Phi_E(\rho_B) = \mathrm{tr}_B\left[U_{BE}(\rho_B \otimes |0\rangle_E\langle 0|)U_{BE}^*\right]. \tag{22}$$

*Proof.* Since any state $\rho_B$ of dimension $n$ can be purified with a subsystem $A$ of dimension $n$ such that $\rho_B = \mathrm{tr}_A(P(|\psi\rangle_{AB}))$ for some $|\psi\rangle_{AB}$, we can trace out subsystem $A$ on both sides of Eq. (20) to get $\Phi_E$ processed by a channel acting on $E$ on the LHS and $\Phi_B$ on the RHS. □

**Remark 5.3.** *In the proof of Theorem 5.1, the operator $K_A$ performed on subsystem $A$ can have an operational interpretation related to entanglement transformation. It may be viewed as a local filtering operation that can be implemented probabilistically by a quantum measurement. This operation locally transforms a maximally entangled state to any other given state (entangled or unentangled) probabilistically.*

**Theorem 5.4.** *Following the notations in Theorem 5.1, for the input state $|\psi_M\rangle_{AB}$, if the output state $U_{ABE}|\psi_M\rangle_{AB}|0\rangle_E$ is not $E \to B$ degradable, then the output state $U_{ABE}|\psi\rangle_{AB}|0\rangle_E$ is not $E \to B$ degradable for any input state $|\psi\rangle_{AB} = (W_A \otimes I_B)|\psi_M\rangle_{AB}$ where $W_A$ is invertible.*

*Proof.* We prove by contradiction. Suppose that for some input state $|\psi\rangle_{AB}$, the output state $U_{ABE}|\psi\rangle_{AB}|0\rangle_E$ is $E \to B$ degradable. We repeat the arguments in the proof of Theorem 5.1 with $|\psi\rangle_{AB}$ and $|\psi_M\rangle_{AB}$ swapped and with $K_A = W_A^{-1}$. Then, Eqs. (16)-(20) follow, concluding that when the input state is $|\psi_M\rangle_{AB}$, the output state is $E \to B$ degradable. This contradicts the assumption and thus proves the theorem. □

# 6 Necessary condition for degradability

We provide an easily computable method to rule out the degradability of a given state. It is based on the expression of degradability in condition (b) of Theorem 3.1 and the contractivity of quantum channels under the trace distance.

**Definition 6.1.** *The trace norm of a matrix $\sigma \in M_q$ is $\mathrm{tr}\,|\sigma| = \sum_{j=1}^{q} \lambda_j$ where $\lambda_j$ are the singular values of $\sigma$.*

**Definition 6.2.** *The trace distance between two matrices $\rho, \sigma \in M_q$ is $d(\rho, \sigma) = \frac{1}{2}\mathrm{tr}\,|\rho - \sigma|$.*

Quantum channels are contractive under the trace distance for quantum states, i.e., $d(\rho, \sigma) \geq d(\mathcal{F}(\rho), \mathcal{F}(\sigma))$ for any density matrices $\rho$ and $\sigma$ and quantum channel $\mathcal{F}$ [32] (see also Theorem 9.2 of [33]). However, the matrices of concern in condition (b) of Theorem 3.1, $R_i R_j^*$ and $S_i S_j^*$, are general matrices and may not be Hermitian and positive semi-definite. Nevertheless, we prove in Appendix A that quantum channels are contractive under any unitarily invariant norm for general matrices, of which the following theorem for the trace norm is a special case.

**Theorem 6.3.** *Given a TPCP map (quantum channel) $\mathcal{F} : M_q \to M_p$ described by Kraus operators $F_1, \ldots, F_r \in M_{p,q}$ with $\sum_{j=1}^{r} F_j^* F_j = I_q$ acting on matrices $\sigma \in M_q$ (not necessarily quantum states),* $\mathrm{tr}|\mathcal{F}(\sigma)| \leq \mathrm{tr}|\sigma|$.

**Corollary 6.4.** *If*

$$d(R_iR_j^*, R_{i'}R_{j'}^*) < d(S_iS_j^*, S_{i'}S_{j'}^*)$$

*for some $i, j, i', j'$, then condition (b) of Theorem 3.1 does not hold.*

We prove by contradiction. If condition (b) holds, then there exists some quantum channel $\mathcal{F}$ satisfying the transformations, and

$$\begin{aligned} d(S_iS_j^*, S_{i'}S_{j'}^*) &= \frac{1}{2}\mathrm{tr}\,|\mathcal{F}(R_iR_j^*) - \mathcal{F}(R_{i'}R_{j'}^*)| \\ &= \frac{1}{2}\mathrm{tr}\,|\mathcal{F}(R_iR_j^* - R_{i'}R_{j'}^*)| \\ &\leq \frac{1}{2}\mathrm{tr}\,|R_iR_j^* - R_{i'}R_{j'}^*| \\ &= d(R_iR_j^*, R_{i'}R_{j'}^*) \end{aligned}$$

where the inequality is due to Theorem 6.3. □

Therefore, if we find the distance between the inputs of two transformations to be smaller than the distance between the outputs, the state is not degradable in the sense of Theorem 3.1.

**Example 5.** Consider the output state processed by the qubit depolarizing channel:

$$\mathcal{E}(\rho) = (1-\epsilon)\rho + \frac{\epsilon}{3}Z\rho Z + \frac{\epsilon}{3}Y\rho Y + \frac{\epsilon}{3}X\rho X \tag{23}$$

where $\rho \in M_2$ is the input density matrix, $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $Y = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, and $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. Suppose the input state is $(|00\rangle + |11\rangle)_{AB}$ and $\mathcal{E}$ is applied to system $B$. The output state purified with system $E$ is

$$\begin{aligned} |\Psi\rangle_{ABE} = \sqrt{1-\epsilon}\ (|00\rangle + |11\rangle)_{AB}|0\rangle_E &+ \sqrt{\frac{\epsilon}{3}}\ (|00\rangle - |11\rangle)_{AB}|1\rangle_E + \\ \sqrt{\frac{\epsilon}{3}}\ (|01\rangle - |10\rangle)_{AB}|2\rangle_E &+ \sqrt{\frac{\epsilon}{3}}\ (|01\rangle + |10\rangle)_{AB}|3\rangle_E. \end{aligned} \tag{24}$$

Note that this state is unnormalized, and normalization is not important in the following discussion.Denote the coefficient for $|ijk\rangle_{ABE}$ by $x_{ijk}$. Then, following Theorem 3.1,

$$S_0 = \begin{pmatrix} x_{000} & x_{001} & x_{002} & x_{003} \\ x_{010} & x_{011} & x_{012} & x_{013} \end{pmatrix} = \begin{pmatrix} \alpha & \beta & 0 & 0 \\ 0 & 0 & \beta & \beta \end{pmatrix} \tag{25}$$

$$S_1 = \begin{pmatrix} x_{100} & x_{101} & x_{102} & x_{103} \\ x_{110} & x_{111} & x_{112} & x_{113} \end{pmatrix} = \begin{pmatrix} 0 & 0 & -\beta & \beta \\ \alpha & -\beta & 0 & 0 \end{pmatrix} \tag{26}$$

where $\alpha = \sqrt{1-\epsilon}$ and $\beta = \sqrt{\frac{\epsilon}{3}}$, and

$$R_i = S_i^t. \tag{27}$$

We compute the trace distances as follows:

$$R_0R_0^* - R_1R_1^* = \begin{pmatrix} 0 & 2\alpha\beta & 0 & 0 \\ 2\alpha\beta & 0 & 0 & 0 \\ 0 & 0 & 0 & 2\beta^2 \\ 0 & 0 & 2\beta^2 & 0 \end{pmatrix} \tag{28}$$

$$S_0S_0^* - S_1S_1^* = \begin{pmatrix} \alpha^2-\beta^2 & 0 \\ 0 & -(\alpha^2-\beta^2) \end{pmatrix} \tag{29}$$

$$R_0R_1^* - R_1R_0^* = \begin{pmatrix} 0 & 0 & -2\alpha\beta & 0 \\ 0 & 0 & 0 & 2\beta^2 \\ 2\alpha\beta & 0 & 0 & 0 \\ 0 & -2\beta^2 & 0 & 0 \end{pmatrix} \tag{30}$$

$$S_0S_1^* - S_1S_0^* = \begin{pmatrix} 0 & \alpha^2-\beta^2 \\ -(\alpha^2-\beta^2) & 0 \end{pmatrix}. \tag{31}$$

It can be shown that $R_0R_0^* - R_1R_1^*$ and $R_0R_1^* - R_1R_0^*$ have singular values $2\alpha\beta, 2\alpha\beta, 2\beta^2, 2\beta^2$, and $S_0S_0^* - S_1S_1^*$ and $S_0S_1^* - S_1S_0^*$ have singular values $(\alpha+\beta)(\alpha-\beta), (\alpha+\beta)(\alpha-\beta)$. Here, we assume $\alpha > \beta$. Thus, $d_R \equiv d(R_0R_0^*, R_1R_1^*) = d(R_0R_1^*, R_1R_0^*) = 2\beta(\alpha+\beta)$ and $d_S \equiv d(S_0S_0^*, S_1S_1^*) = d(S_0S_1^*, S_1S_0^*) = (\alpha+\beta)(\alpha-\beta)$.

Therefore, we have the condition for the input distance being smaller than the output distance:

$$d_R < d_S \Rightarrow \epsilon < \frac{1}{4}. \tag{32}$$

Under this condition, there does not exist a quantum channel $T_E$ acting on system $E$ such that $T_E(\rho_{AE}) = \rho_{AB}$. Here, $\rho_{AE} = \mathrm{tr}_B(|\Psi\rangle_{ABE}\langle\Psi|)$ and $\rho_{AB} = \mathrm{tr}_E(|\Psi\rangle_{ABE}\langle\Psi|)$. By Theorem 5.4, the same conclusion holds for all other Bell states serving as the input state since all Bell states are unitarily transformable to each other. We can interpret the result in the context of quantum key distribution (QKD) [1, 2], in which two legitimate parties, conventionally named Alice and Bob (they correspond to systems $A$ and $B$ here), want to share a secret key against an eavesdropper Eve (system $E$ here), by exchanging quantum states. These states may be modified by Eve. In a typical QKD session, Alice and Bob learn about the quantum states by comparing measurement results in various measurement bases (such as $X$, $Y$, or $Z$). For each basis, we can compute the fraction of measurement mismatches, which is known as the quantum bit error rate (QBER). Note that the QKD protocol described here operates in a two-dimensional space, although the presentation of this paper treats arbitrary finite dimensions. Since the state in Eq. (23) is symmetric with respect to measurements in $X$, $Y$, and $Z$, the QBER for each of them is the same, $2\epsilon/3$. (This means that measurements in say the $X$ basis produce an error rate of $2\epsilon/3$ when the channel input is an $X$ eigenstate.) Combining with Eq. (32), it means that when the QBER is less than 1/6, Eve is not able to imitate Bob. Recall that if, on the other hand, Eve is able to imitate Bob, no key can be generated using one-way postprocessing [22, 23, 24]. Thus, our result here is consistent with the result that positive key rate is achievable when the QBER is less than 1/6 for the six-state protocol [34].

## 7 Additional remarks and questions

Direct application of Theorem 3.2 yields the following.

**Proposition 7.1.** *Use the notation in Theorem 3.1. The following are equivalent.*

(a) *There are TPCP maps* $T = I_n \otimes T_1$ *and* $L = I_n \otimes L_1$ *such that* $T(X_2) = X_3$ *and* $L(X_3) = X_2$.

(b) *There is a TPCP map sending* $\{R_u R_v^* : 1 \le u, v \le n\}$ *to* $\{S_u S_v^* : 1 \le u, v \le n\}$, *and a TPCP map sending* $\{S_u S_v^* : 1 \le u, v \le n\}$ *to* $\{R_u R_v^* : 1 \le u, v \le n\}$.

(c) *There are* $p \times q$ *matrices* $F_1, \ldots, F_r$ *with* $\sum_{j=1}^r F_j^* F_j = I_q$ *and* $k_i \times p$ *matrices* $W_{i1}, \ldots, W_{ir}$ *such that for all* $i, j = 1, \ldots, n$,

$$[F_1 R_i \cdots F_r R_i] = V_i D_i [W_{i1} \cdots W_{ir}] \quad \text{and} \quad [W_{i1} \cdots W_{ir}][W_{j1} \cdots W_{jr}]^* = U_i^t \overline{U}_j,$$

*and there are* $q \times p$ *matrices* $\tilde{F}_1, \ldots, \tilde{F}_s$ *with* $\sum_{j=1}^s \tilde{F}_j^* \tilde{F}_j = I_p$ *and* $k_i \times q$ *matrices* $\tilde{W}_{i1}, \ldots, \tilde{W}_{is}$ *such that for all* $i, j = 1, \ldots, n$,

$$[\tilde{F}_1 R_i^t \cdots \tilde{F}_s R_i^t] = U_i D_i [\tilde{W}_{i1} \cdots \tilde{W}_{is}] \quad \text{and} \quad [\tilde{W}_{i1} \cdots \tilde{W}_{is}][\tilde{W}_{j1} \cdots \tilde{W}_{js}]^* = V_i^t \overline{V}_j.$$

**Proposition 7.2.** *The following are equivalent.*

(a) *There is a TPCP map sending* $R_i R_j^*$ *to* $S_i S_j^*$.

(b) *There is a TPCP map sending* $(\sum c_i R_i)(\sum \tilde{c}_j R_j)^*$ *to* $(\sum c_i S_i)(\sum \tilde{c}_j S_j)^*$ *for any scalars* $c_1, \ldots, c_n, \tilde{c}_1, \ldots, \tilde{c}_n$.

(c) *There is a TPCP map sending* $(\sum c_i R_i)(\sum c_j R_j)^*$ *to* $(\sum c_i S_i)(\sum c_j S_j)^*$ *for any scalars* $c_1, \ldots, c_n$.

By the above proposition, we can focus on a maximal linearly independent subset set $\{R_1, \ldots, R_m\}$ and check whether there is a TPCP map sending $R_i R_j^*$ to $S_i S_j^*$ for matrices $R_i, R_j$ in this set. Note, however, that the above propositions are not very practical and it is desirable to have some more practical conditions.

**Problem** Can we extend Corollary 3.3 and determine the condition for the existence of TPCP maps $T = I_n \otimes T_1$ and $L = I_n \otimes L_1$ such that $T(X_2) = X_3$ and $L(X_3) = X_2$?

## 8 Concluding remarks

In this paper, we introduced the notion of state degradability. The joint state of Alice and Eve is degradable if Eve's system can be processed by a quantum channel to produce a joint state that is the same as the joint state of Alice and Bob. We proved necessary and sufficient conditions for state degradability. The conditions are in general difficult to check, but we also provide an easily computable method to rule out degradability. This method is based on the fact that the trace distance between two states can only become smaller under the action of a quantum channel. One application of state degradability is that it can be used to test channel degradability. Analysis of the channel output state of the maximally entangled input state gives information about the

degradability of the channel. Another application of state degradability is in the analysis of QKD, in which no secret key can be generated by one-way postprocessing when the joint state between Alice and Eve can be degraded to a joint state between Alice and Bob. For future work, we hope to investigate more connections between degradability and other quantum information processing tasks, and extend our result to the case where Alice, Bob, and Eve share a mixed quantum state.

# A Proof of Theorem 6.3

A norm is unitarily invariant if $\|X\| = \|UXV\|$ for any unitary $U, V$. Note that the trace norm is one such norm.

**Proposition A.1.** *Suppose $B \in M_p$ and $A \in M_q$ such that $B = \sum_{j=1}^r F_j A F_j^*$ with $\sum F_j^* F_j = I_q$. Then, $\|I_r \otimes B\| \le r\|A \oplus O\|$ for any unitarily invariant norm $\|\cdot\|$ on $M_{pr}$.*

*Proof.* Let $U = (U_{ij})_{1\le i,j\le r}$ be unitary such that $U_{j1} = F_j$ for $j = 1, \dots, r$. Then $U(A\oplus O)U^* = (A_{ij})_{1\le i,j\le r}$ such that $A_{11} + ... + A_{rr} = B$. Take $P = \operatorname{diag}(1, w, .., w^{r-1}) \otimes I_p$ with $w = e^{i2\pi/r}$. Then $r^{-1}\sum_{1\le \ell\le r} P^\ell (A_{ij})(P^\ell)^* = A_{11} \oplus \cdots \oplus A_{rr}$. Now take $Q = (E_{12} + \cdots E_{r-1,r} + E_{r,1}) \otimes I_p$. Then $\sum_{1\le j\le r} Q^j (A_{11} \oplus \cdots \oplus A_{rr})(Q^j)^* = I_r \otimes B$. Thus, using the triangle inequality,

$$\|I_r \otimes B\| = \left\| \frac{1}{r} \sum_{\ell,k=1}^{r} Q^k P^\ell U (A \oplus O)(Q^k P^\ell U)^* \right\| \le \frac{1}{r} \sum_{\ell,k=1}^{r} \|A \oplus O\| = r\|A \oplus O\|.$$

□

To prove Theorem 6.3, we just take $\|\cdot\|$ to be the trace norm to get

$$\|B\| = \frac{1}{r}\|I_r \otimes B\| \le \|A \oplus O\| = \|A\|.$$

# Acknowledgments

We thank Zejun Huang and Edward Poon for enlightening discussion.

This research evolved in a faculty seminar on quantum information science at the University of Hong Kong in the spring of 2012 coordinated 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. 700712P. Sze was partially supported by the Hong Kong RGC grant PolyU 502512. Li was supported by a USA NSF grant and a Hong Kong RGC 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


[1] C. H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. In *Proc. of IEEE Int. Conference on Computers, Systems, and Signal Processing*, pages 175–179, IEEE Press, New York, December 1984.

[2] A. K. Ekert. Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.*, 67:661–663, 1991.

[3] P. W. Shor. Scheme for reducing decoherence in quantum computer memory. *Phys. Rev. A*, 52:R2493–R2496, Oct 1995.

[4] D. Gottesman. Class of quantum error-correcting codes saturating the quantum hamming bound. *Phys. Rev. A*, 54:1862–1868, Sep 1996.

[5] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane. Quantum error correction and orthogonal geometry. *Phys. Rev. Lett.*, 78:405–408, Jan 1997.

[6] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane. Quantum error correction via codes over GF(4). *IEEE Trans. Inform. Theory*, 44(4):1369–1387, 1998.

[7] M. Hillery, V. Bužek, and A. Berthiaume. Quantum secret sharing. *Phys. Rev. A*, 59:1829–1834, Mar 1999.

[8] A. Karlsson, M. Koashi, and N. Imoto. Quantum entanglement for secret sharing and secret splitting. *Phys. Rev. A*, 59:162–168, Jan 1999.

[9] P. Alberti and A. Uhlmann. A problem relating to positive linear maps on matrix algebras. *Rep. Math. Phys.*, 18(2):163 – 176, 1980.

[10] A. Uhlmann. Eine bemerkung er vollstdig positive abbildungen von dichteoperatoren. *Wiss. Z. Karl-Marx-Univ. Leipzig, Math.-Naturwiss. Reihe*, 34(6):580–582, 1985.

[11] A. Chefles. Deterministic quantum state transformations. *Phys. Lett. A*, 270(1):14 – 19, 2000.

[12] A. Chefles. Quantum operations, state transformations and probabilities. *Phys. Rev. A*, 65:052314, May 2002.

[13] A. Chefles, R. Jozsa, and A. Winter. On the existence of physical transformations between sets of quantum states. *Int. J. Quant. Inf.*, 2(1):11–21, 2004.

[14] C. H. Bennett, H. J. Bernstein, S. Popescu, and B. Schumacher. Concentrating partial entanglement by local operations. *Phys. Rev. A*, 53:2046–2052, Apr 1996.

[15] H.-K. Lo and S. Popescu. Concentrating entanglement by local actions: beyond mean values. *Phys. Rev. A*, 63:022301, Jan 2001.

[16] M. A. Nielsen. Conditions for a class of entanglement transformations. *Phys. Rev. Lett.*, 83:436–439, Jul 1999.

[17] D. Jonathan and M. B. Plenio. Minimal conditions for local pure-state entanglement manipulation. *Phys. Rev. Lett.*, 83:1455–1458, Aug 1999.

[18] B. He and J. A. Bergou. Entanglement transformation with no classical communication. *Phys. Rev. A*, 78:062328, Dec 2008.

[19] V. Gheorghiu and R. B. Griffiths. Separable operations on pure states. *Phys. Rev. A*, 78:020304, Aug 2008.

[20] H. F. Chau, C.-H. F. Fung, C.-K. Li, E. Poon, and N.-S. Sze. Entanglement transformation between sets of bipartite pure quantum states using local operations. *J. Math. Phys.*, 53(12):122201, 2012.

[21] G. Gour and N. R. Wallach. Necessary and sufficient conditions for local manipulation of multipartite pure quantum states. *New Journal of Physics*, 13(7):073013, 2011.

[22] D. Bruß, D. P. DiVincenzo, A. Ekert, C. A. Fuchs, C. Macchiavello, and J. A. Smolin. Optimal universal and state-dependent quantum cloning. *Phys. Rev. A*, 57:2368–2378, Apr 1998.

[23] M. L. Nowakowski and P. Horodecki. A simple test for quantum channel capacity. *Journal of Physics A: Mathematical and Theoretical*, 42(13):135306, 2009.

[24] T. Moroder, M. Curty, and N. Lütkenhaus. One-way quantum key distribution: Simple upper bound on the secret key rate. *Phys. Rev. A*, 74:052301, Nov 2006.

[25] N. J. Cerf. Asymmetric quantum cloning in any dimension. *J. Mod. Opt.*, 47:187–209, 2000.

[26] J. Fiurášek, R. Filip, and N. J. Cerf. Highly asymmetric quantum cloning in arbitrary dimension. *Quant. Inform. Comp.*, 5:583–592, 2005.

[27] S. Iblisdir, A. Acín, N. J. Cerf, R. Filip, J. Fiurášek, and N. Gisin. Multipartite asymmetric quantum cloning. *Phys. Rev. A*, 72:042328, Oct 2005.

[28] I. Devetak and P. W. Shor. The capacity of a quantum channel for simultaneous transmission of classical and quantum information. *Comm. Math. Phys.*, 256(2):287–303, 2005.

[29] T. S. Cubitt, M. B. Ruskai, and G. Smith. The structure of degradable quantum channels. *J. Math. Phys.*, 49(10):102104, 2008.

[30] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin, and W. K. Wootters. Purification of noisy entanglement and faithful teleportation via noisy channels. *Phys. Rev. Lett.*, 76:722–725, Jan 1996.

[31] Z. Huang, C.-K. Li, E. Poon, and N.-S. Sze. Physical transformations between quantum states. *J. Math. Phys.*, 53(10):102209, 2012.

[32] M. B. Ruskai. Beyond Strong Subadditivity? Improved Bounds on the Contraction of Generalized Relative Entropy. *Rev. Math. Phys.*, 6:1147–1161, 1994.

[33] M. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information*. CUP, 2000.

[34] R. Renner, N. Gisin, and B. Kraus. Information-theoretic security proof for quantum-key-distribution protocols. *Phys. Rev. A*, 72:012332, Jul 2005.