Remote extraction and destruction of spread qubit information

Yoshiko Ogata  
Graduate School of Mathematical Sciences, The University of Tokyo, Tokyo, 153-8914 Japan  
Department of Physics, The University of Tokyo, Tokyo 113-0033, Japan

Mio Murao  
Department of Physics, The University of Tokyo, Tokyo 113-0033, Japan  
PRESTO, JST, Kawaguchi, Saitama 332-0012, Japan  
The Collaborative Institute for Nano Quantum Information Electronics,  
The University of Tokyo, Tokyo 113-0033, Japan  
(Dated: February 2, 2008)

Necessary and sufficient conditions for deterministic remote extraction and destruction of qubit information encoded in bipartite states using only local operations and classical communications (LOCC) are presented. The conditions indicate that there is a way to asymmetrically spread qubit information between two parties such that it can be remotely extracted with unit probability at one of the parties but not at the other as long as they are using LOCC. Remote destruction can also be asymmetric between the two parties, but the conditions are incompatible with those for remote extraction.

PACS numbers: PACS numbers: 03.67.-a, 03.67.Hk, 03.65.Ud

I. INTRODUCTION

Quantum information processing seeks to perform tasks which are impossible or not efficient with the use of conventional classical information processing, by using systems described by quantum mechanics. We can consider two kinds of quantum information tasks based on the types input states: the classical input tasks and the quantum input tasks. Whereas input states of the classical input tasks are quantum states but encode just classical information, input states of the quantum input tasks encodes quantum information, of which unit is described by a qubit $|e_0\rangle + \beta|e_1\rangle$ where $\alpha$ and $\beta$ are unknown complex parameters satisfying $|\alpha|^2 + |\beta|^2 = 1$ and $|e_0\rangle$ and $|e_1\rangle$ are a fixed basis of a qubit. For example, quantum algorithms [1] are classical input tasks and quantum error correcting codes [2] and quantum universal optimal cloning [3] are quantum input tasks. To investigate yet unveiled full quantum potential of quantum information processing, it is necessary to understand properties of quantum input tasks.

In many quantum input tasks, how quantum information is encoded in the larger Hilbert space of composite systems determines the main functionality of the tasks. For example, in quantum error correcting codes, qubit information is encoded in a subspace of a larger Hilbert space such that it can be still recovered after being influenced by certain errors (or noises) which map input qubit information into the whole Hilbert space. The encoding process can be described by a transformation of a computational basis $\{|i\rangle\}$ where the original quantum information is given into a set of orthogonal states in the larger Hilbert space $\{|\psi_i\rangle\}$. In this picture, the properties of encoding for a task are captured by the choice of a set of states $\{|\psi_i\rangle\}$, which represents how original quantum information is spread across the Hilbert spaces of subsystems.

Entanglement, or a non-local quantum correlation, of an individual state is an essential resource for performing quantum input tasks such as quantum teleportation [4], namely, the existence of entanglement is necessary for performing teleportation beyond the classical limit. To analyze non-local properties of spread quantum information described by the set of states is a way to characterize how quantum information is spread by encoding. Here, we use the word non-local to represent properties which are not fully accessible by just using local operations on the subspaces and classical communications (LOCC) but global operations on the whole systems. For individual states, the existence of this kind of non-locality is accompanied by the existence of entanglement.

However, it is also known that such non-local properties of a set of states can be essentially different from non-locality of individual states. An important example is a set of nine product states which cannot be locally discriminated by using LOCC presented in [5] (the “non-locality without entanglement” paper by Bennet et al.). In this example, there is no entanglement in the quantum states where classical information is encoded, therefore, no entanglement resource required for encoding classical information, but it is not possible to decode (i.e., identify encoded classical information) deterministically LOCC, without using entanglement resources. Entanglement properties of each encoded state does not fully capture the non-local property appearing in the decoding process. As it had been also pointed out in the context of local copy and local state discrimination in [6], impossibility of tasks involving LOCC transformation of a set of states implies non-locality beyond individual entanglement.

For characterizing non-locality of the spread of quantum information, non-local resources required for decod-
Two we have to investigate simultaneous transformations of extreme case of spreading quantum information that does not consume non-local resources for decoding. We study a simple but fundamental case of spreading qubit information into two-party states. We present necessary and sufficient conditions for this task. Spread quantum information can only be irreversibly destroyed by Alice’s measurement on her qubit, in a way such that the state after the measurement does not contain quantum information (α and β). Note that some classical information represented by Cα,β can be retrieved from the outcome of Alice’s measurement i.

From the viewpoint of controlling transmission of quantum information, it is also useful to spread quantum information into two parties such that Alice’s local operation can irreversibly destroy quantum information such that the state of Bob’s qubit after Alice’s operation is set to a pure state which does not contain quantum information, i.e. the parameters α and β. Note that this process is not a randomizing process to transform Bob’s qubit to be in a completely mixed state. In this task, a part of classical information of the parameter α and β can be retrieved. We call this task remote destruction. Such a way for spreading quantum information can be used another kind of “switch” for controlling quantum information transmission. Using a similar technique for proving conditions of remote extraction, we also present necessary and sufficient conditions for this task. Spreading quantum information for remote destruction can also be asymmetric between two parties, but we show that the conditions for remote destruction are incompatible for those of remote extraction.

This paper is organized as the following: In Section II the definitions and precise statements of remote extraction and destruction are given. In Section III we show the proof of sufficiency for remote extraction. The preparations and outline of the proof of necessity are given in Section IV. The proof of necessity consists of seven steps and they are presented in Section V. The proof of conditions for remote destruction is presented in Section VI and the summary and discussions are given in Section VII.

II. STATEMENTS OF REMOTE EXTRACTION AND DESTRUCTION

A. Remote extraction

We take two orthonormal vectors |ψ0⟩AB, |ψ1⟩AB in two qubit Hilbert space $\mathcal{H}_{AB} = \mathbb{C}^2 \otimes \mathbb{C}^2$, which we will call basis states, and encode qubit information into a two-qubit state represented by $|\psi⟩ = \alpha |\psi_0⟩_{AB} + \beta |\psi_1⟩_{AB}$. The

![FIG. 1: Asymmetric remote extraction: We can encode single qubit information into two parties where information can be extracted only by using LOCC at Bob but not at Alice.](image1)

![FIG. 2: Asymmetric remote destruction: Spread quantum information can only be irreversibly destroyed by Alice’s measurement on her qubit, in a way such that the state after the measurement does not contain quantum information (α and β). Note that some classical information represented by Cα,β can be retrieved from the outcome of Alice’s measurement i.](image2)
We consider two qubits are spatially separated and one of the qubit is at Alice’s side and the other qubit is at Bob’s side. The task of remote extraction is to extract qubit information at Bob’s side from the two-qubit state $|\psi\rangle_{AB}$ by using finite rounds of LOCC. That is, we look for a finite round LOCC procedure $\Lambda$ such that

$$\Lambda(\alpha|\psi\rangle + \beta|\psi\rangle) = \langle \xi | \alpha e_0 + \beta e_1 \rangle_B$$

for arbitrary $\alpha, \beta \in \mathbb{C}$ satisfying $|\alpha|^2 + |\beta|^2 = 1$. Here, $\{|e_0\rangle_B, |e_1\rangle_B\}$ is a fixed orthonormal basis in $\mathcal{H}_B$, and $\langle \xi |$ is an arbitrary vector in $\mathcal{H}_A$. Throughout this paper, we use a notation $\langle \alpha| \psi\rangle + \beta|\psi\rangle \equiv \alpha|\psi\rangle + \beta|\psi\rangle$, and $\langle \alpha| + \beta|\psi\rangle \equiv \alpha|\psi\rangle + \beta|\psi\rangle$ where $\alpha$ and $\beta$ are complex conjugates of $\alpha$ and $\beta$, respectively. We also denote the conjugation of a single qubit state $|\phi\rangle = \alpha|e_0\rangle + \beta|e_1\rangle$ with respect to an orthonormal basis $\{|e_i\rangle\}$ of the qubit by $\overline{\langle \phi |} = \overline{\alpha|e_0\rangle + \beta|e_1\rangle}$.

The finite round LOCC procedure $\Lambda$ is given by a sequence of Alice’s measurements $\{M_{i_1,j_1}^{k_1}, \ldots, J_{k_1}^{k_1} \otimes I\}$ and Bob’s $\{I \otimes N_{i_2,j_2}^{k_2} \cdots J_{k_2}^{k_2} \}$, where $i_k$ is an index for Alice’s $k$-th round measurement and $j_k$ is an index for Bob’s $k$-the round measurement $(k = 1, \ldots, N)$, satisfying the normalization conditions

$$\sum_{i_k} M_{i_1,j_1}^{k_1} \cdots J_{k_1}^{k_1} = 1,$$

$$\sum_{j_k} N_{i_2,j_2}^{k_2} \cdots J_{k_2}^{k_2} = 1$$

for each $k$. We use the notation $I_k = (i_1, \ldots, i_k), J_k = (j_1, \ldots, j_k)$. It is easy to see that Eq. (1) is equivalent to

$$|\psi\rangle_{AB} = \frac{1}{\sqrt{N}} \sum_{\{t_i\}} \left( \sum_{i=0}^{N} \left( M_i^{J_i} \otimes I \right) \left( |e_i\rangle_B \right) \right)$$

for $i = 0, 1$ and all $(J_i, N_i)$. When there exists a LOCC procedure satisfying the condition of Eq. (1), we say that qubit information on the basis states $|\psi\rangle_{AB}, |\psi\rangle_{AB}$ can be deterministically extracted by LOCC at Bob’s side. We call the pair of the state by the right hand side of Eq. (1) $\{|\xi\rangle_B |e_0\rangle_B, |\xi\rangle_B |e_1\rangle_B\}$ as the extracted form, and $\{|e_i| |e_i\rangle_B, |\xi\rangle_B |e_i\rangle_B\}$ with some unitary operator $v$ is said to be locally equivalent to the extracted form to Bob. We use these notations in our proof of remote extraction.

Now our problem is to find the condition of the basis states $|\psi\rangle_{AB}, |\psi\rangle_{AB}$ satisfying Eq. (1). In this paper, we prove the following Theorem:

**Theorem II.1** Qubit information spread between Alice and Bob $|\psi\rangle_{AB} = \alpha|\psi\rangle_{AB} + \beta|\psi\rangle_{AB}$ can be deterministically extracted using only LOCC at Bob’s side $|\phi\rangle_B = \alpha|e_0\rangle_B + \beta|e_1\rangle_B$ if and only if the Schmidt decompositions of the basis states $|\psi\rangle_{AB}, |\psi\rangle_{AB}$ are given by

$$|\psi\rangle_{AB} = \sqrt{\lambda_0} |a_0\rangle_A |b_0\rangle_B + \sqrt{\lambda_1} |a_1\rangle_A |b_1\rangle_B$$

$$|\psi\rangle_{AB} = \sqrt{\lambda_0} |a_0\rangle_A |b_1\rangle_B + \sqrt{\lambda_1} |a_1\rangle_A |b_0\rangle_B$$

where $\lambda_0$ and $\lambda_1$ are the Schmidt coefficients satisfying $0 \leq \lambda_0 \leq \lambda_0 + \lambda_1 = 1$, and $\{|a_i\rangle\}$ are the Schmidt basis of Alice’s qubit and $\{|b_i\rangle\}$ is the Schmidt basis of Bob’s qubit. If the conditions of Eq. (5) and (6) are satisfied, then $|a_0\rangle_A, |a_1\rangle_A$ are of the form

$$|a_0\rangle_A = e^{-i\theta} \cos \theta |a_0\rangle_A + \sin \theta |a_1\rangle_A,$$

$$|a_1\rangle_A = e^{i\phi} \left( -\sin \theta |a_0\rangle_A + e^{i\theta} \cos \theta |a_1\rangle_A \right)$$

using three real parameters $\phi, \theta$ and $\Theta$.

We define a family of orthonormal basis $\{e_i^n\}_i$ labeled by a positive real number $t_i$ by

$$|e_i^n\rangle_A = \left( F_{t_i, \theta} |a_0\rangle_A - i e^{i\theta} F_{t_i, \theta} |a_1\rangle_A \right) / N_i$$

where $F_{t_i, \theta} = 1 + ie^{i\theta}$ and $N_i = \sqrt{2(t_i^2 + 1)}$. Then if the pair of vectors $\{I \otimes N_{i_k}^{J_i} \cdots (M_i \otimes I) |\psi_{AB}\rangle, (I \otimes N_{i_k}^{J_i} \cdots (M_i \otimes I) |\psi_{AB}\rangle\}$ is not locally unitary equivalent to the extracted form, all the measurements by Alice on it are of the form

$$M_{i_k}^{J_i} = u_{i_k}^{J_i} \left( \tau_{i_k,J_k}^0 |e_i^n\rangle_B |e_i^n\rangle_B \right) + \sqrt{\tau_{i_k,J_k}^0} |e_i^n\rangle_B |e_i^n\rangle_B \left( u_{i_k}^{J_i} \right)^\dagger$$

where $u_{i_k}^{J_i}$ is an unitary operator, $0 \leq \tau_{i_k,J_k}^0, \tau_{i_k,J_k}^1 \leq 1$ and $i_k,J_k \geq 0$. On the other hand, all the measurements that Bob carries out $\{N_{i_k}\}$ are scalar multiplications of unitary operators.
From the theorem, we see that the Schmidt coefficients of the basis states have to be identical for remote extraction, therefore the basis states should have, at least, same entanglement for remote extraction. On the other hand, the Schmidt base of Alice’s qubit of the basis states are not necessary to be same. Although the orthogonality condition of the basis states $\langle \psi_0 | \psi_1 \rangle = \sqrt{\lambda_0 \lambda_1} ((a_1 | a_1^\dagger) + (a_0 | a_1^\dagger)) = 0$ fixes one of the parameters to be $\varphi = 0$, $\Theta = 0$ or $\Theta = \pi$ for $\lambda_1 \neq 0$, we can choose $\theta$ and one of $\varphi$ and $\Theta$ in Eq. (8) arbitrary. This property allows asymmetry of remote extraction: we can encode qubit information such that the conditions for remote extraction at Bob are satisfied but the conditions for remote extraction at Alice are not satisfied.

We can also obtain necessary and sufficient conditions of the basis states for symmetric remote extraction, where the deterministic remote extraction at either Alice or Bob is possible depending on the choice of LOCC procedures from the Theorem I.

**Corollary II.1** Extraction to either Alice or Bob is possible if and only if the Schmidt decompositions of the basis states are given by

$$|\psi_0\rangle_{AB} = \sqrt{\lambda_0} |a_0\rangle_{A} |b_0\rangle_{B} + \sqrt{\lambda_1} |a_1\rangle_{A} |b_1\rangle_{B}, \quad (12)$$

$$|\psi_1\rangle_{AB} = -\sqrt{\lambda_0} |a_1\rangle_{A} |b_1\rangle_{B} + \sqrt{\lambda_1} |a_0\rangle_{A} |b_0\rangle_{B} \quad (13)$$

Thus, if a set of the basis states $\{|\psi_0\rangle_{AB}, |\psi_1\rangle_{AB}\}$ satisfies the conditions of remote extraction Eqs. (4) and (5), but does not satisfy the conditions for the symmetric ones Eqs. (12) and (13), it gives an asymmetric way of spreading qubit information, where deterministic remote extraction is only possible at Bob, not at Alice. For $\lambda_0 = \lambda_1 = 1/\sqrt{2}$, any choice of two orthogonal (maximally entangled) states can be transformed into the forms of Eqs. (4) and (5), therefore there is no asymmetric remote extraction. However, for $\lambda_0 \neq \lambda_1$ where the Schmidt base are determined uniquely, asymmetry of (perfect) remote extraction is guaranteed as long as $\Theta \neq \pi/2$ in Eq. (5). The case of $\lambda_0 = 1$ presents an interesting picture how qubit information is spread between two parties in terms of symmetry and asymmetry; for $\Theta = 0$, qubit information is already extracted at Bob from the beginning, and no qubit information can be extracted at Alice by LOCC, for $\Theta = \pi/2$, qubit information is symmetrically shared between Alice and Bob, and for $0 < \Theta < \pi/2$, qubit information is shared but asymmetrically.

We note that Bob’s operation is restricted to scalar multiplication of unitary operators for extracting qubit information at Bob. Therefore, once one of the party performs an extraction measurement of the form of Eq. (11), qubit information can be only extracted to the party who has not performed the extraction measurement, even with the basis states allowing symmetric remote extraction. The measurement condition also implies that one-way LOCC, where Alice performs a projective measurement on her qubit in the $\{|\psi_0\rangle_A, |\psi_1\rangle_A\}$ basis and Bob performs a conditional unitary operation depending on Alice’s measurement outcome is sufficient for remote extraction of qubit information.

**B. Remote destruction**

The task of remote destruction is to irreversibly destroy spread qubit information by acting one of the party (Alice) and to prevent extracting quantum information at the other party (Bob). We assume that Bob would not cooperate to destroy information, and also we would like to prevent recovery of quantum information even if classical information about Alice’ measurement is known. We look for Alice’s measurement $\{M_i\}$ such that for arbitrary $\alpha, \beta \in \mathbb{C}$ satisfying $|\alpha|^2 + |\beta|^2 = 1$,

$$(M_i \otimes 1) |\alpha \psi_0 + \beta \psi_1\rangle_{AB} = C_{\alpha,\beta} |\chi_i\rangle_{A} |\xi_i\rangle_{B}, \quad (14)$$

for each $i$. Here, $C_{\alpha,\beta}$ is some scalar which depends on $\alpha, \beta$, and $|\chi_i\rangle_{A}, |\xi_i\rangle_{B}$ are vectors that do not depend on $\alpha, \beta$.

In this paper, we show the following:

**Theorem II.2** Deterministic remote destruction by Alice is possible if and only if the Schmidt decompositions of the basis states are given by

$$|\psi_0\rangle_{AB} = \sqrt{\lambda_0} |a_0\rangle_{A} |b_0\rangle_{B} + \sqrt{\lambda_1} |a_1\rangle_{A} |b_1\rangle_{B}, \quad (15)$$

$$|\psi_1\rangle_{AB} = -\sqrt{\lambda_0} |a_1\rangle_{A} |b_1\rangle_{B} + \sqrt{\lambda_1} |a_0\rangle_{A} |b_0\rangle_{B} \quad (16)$$

where $0 \leq \lambda_0 \leq \lambda_1 \leq 1$, $\lambda_0 + \lambda_1 = 1$ and $\{|a_i\rangle\}$ is the Schmidt base of Alice’s qubit and $\{|b_i\rangle\}$ and $\{|b_i\rangle\}$ are the Schmidt basis of Bob’s qubit. If the Schmidt rank of $|\psi_0\rangle_{AB}$ (resp. $|\psi_1\rangle_{AB}$) is 2, then the measurement operators for deterministic remote destruction $\{M_i\}$ are of the form

$$M_i = |\chi_i\rangle \langle f_{k_i}|, \quad (17)$$

where $|\chi_i\rangle$ is an arbitrary vector, $k_i = 0, 1$, and $\{|f_0\rangle, |f_1\rangle\}$ is an orthonormal basis diagonalizing a matrix.
If the Schmidt rank of both of $|\psi\rangle_{AB}$ and $|\psi\rangle_{AB}$ are 1, then the measurement operators $\{M_i\}$ are of the form

$$M_i = |\chi_i\rangle \langle \eta_i|.$$ 

Here, the vector $|\eta_i\rangle$ have to be $|a_0\rangle$ or $|a_1\rangle$ if $|b_0\rangle_B$ and $|b_0\rangle_B$ are not parallel to each other, while it can be an arbitrary vector if $|b_0\rangle_B$ and $|b_0\rangle_B$ are parallel to each other.

We see that the conditions given by Eq. (16) is identical for the conditions for deterministic remote extraction at Alice, instead of Bob. Therefore, the conditions for remote destruction by Alice’s measurement are incompatible for those of remote extraction by Alice’s measurement. The conditions for symmetric remote destruction are also given by Eqs. (12) and (13), therefore, in the symmetric case, Alice can determine whether destructing qubit information or letting Bob to extract full qubit information by the choice of her measurement, but Bob is also in the same position.

III. PROOF OF SUFFICIENCY FOR REMOTE EXTRACTION

We first observe that if the conditions given by Eqs. (5) and (6) are satisfied, then the representation of the base of Alice’s qubit (Eq. (8)) is obtained. The case of $\lambda_0 = 0$ or $\lambda_1 = 1$ is trivial. Let us assume $\lambda_0, \lambda_1 \neq 0$. Since $|\psi\rangle_{AB}$ and $|\psi\rangle_{AB}$ are orthogonal, the two base of Alice’s qubit appearing in Eqs. (5) and (6) have to satisfy

$$\langle a_0'| a_1 \rangle + \langle a_1'| a_0 \rangle = 0. \quad (18)$$

If we represent the basis state $|a_0\rangle_A$ by $|a_0\rangle_A = c_0 |a_0\rangle_A + c_1 |a_1\rangle_A$ and another basis state $|a_1\rangle_A$ by $|a_1\rangle_A = e^{i\varphi} (-c_1^* |a_0\rangle_A + c_0 |a_1\rangle_A)$ with complex parameters $c_0$ and $c_1$ satisfying $|c_0|^2 + |c_1|^2 = 1$, and a real parameter $\varphi$, the condition of Eq. (16) implies $c_1 = c_1^* e^{i\varphi}$. By introducing two real parameters $\theta$ and $\phi$, we can represent $c_0 = \cos \Theta e^{i(\varphi-\theta)}$ and $c_1 = \sin \Theta e^{i\varphi}$, respectively. Thus, we obtain the representation of the basis of Alice’s qubit in Eq. (8).

Now we choose another basis of Alice’s qubit $\{|0\rangle_A, |1\rangle_A\}$ given by

$$|0\rangle_A = \frac{1}{\sqrt{2}} (|a_0\rangle_A - ie^{i\theta} |a_1\rangle_A)$$

$$|1\rangle_A = \frac{1}{\sqrt{2}} (-ie^{-i\theta} |a_0\rangle_A + |a_1\rangle_A). \quad (19)$$

We will check that qubit information can be extracted to Bob’s qubit by Alice’s projective measurement described by $\{|0\rangle |0\rangle, |1\rangle |1\rangle\}$ followed by an appropriate unitary operation performed by Bob depending on the measurement outcome of Alice. If Alice obtains the measurement result corresponding to $|0\rangle_A$, the basis states are transformed to

$$|\psi\rangle_{AB} \rightarrow \frac{1}{\sqrt{2}} |0\rangle_A \left(\sqrt{\lambda_0} |b_0\rangle_B + ie^{-i\theta} \sqrt{\lambda_1} |b_1\rangle_B\right)$$

$$|\psi\rangle_{AB} \rightarrow \frac{1}{\sqrt{2}} |1\rangle_A \left(|\lambda_0, b_0\rangle_B + ie^{i\theta} \lambda_1 |b_1\rangle_B\right).$$

If Alice obtains the measurement result $|1\rangle_A$, the basis states are transformed to

$$|\psi\rangle_{AB} \rightarrow \frac{1}{\sqrt{2}} |0\rangle_A \left(\sqrt{\lambda_0} |b_0\rangle_B + \sqrt{\lambda_1} |b_1\rangle_B\right),$$

$$|\psi\rangle_{AB} \rightarrow \frac{1}{\sqrt{2}} |1\rangle_A \left(|\lambda_0, b_0\rangle_B + \sqrt{\lambda_1} |b_1\rangle_B\right).$$

Note that the resulting pairs are locally equivalent to the extracted form to Bob. Hence, by choosing a suitable unitary operation transforming the basis of Bob’s qubit back to $\{|0\rangle, |1\rangle\}$, spread qubit information can be faithfully extracted to Bob’s side by only using LOCC.

IV. PREPARATIONS AND OUTLINE FOR PROOF OF NECESSITY

In our proof, we employ matrix representations of states. In this section, we first describe the matrix representation, and then introduce the key notion in our proof: extraction measurements (E-measurements). We also present the outline of our proof of necessity for remote extraction consisting of seven steps.

A. Matrix representation

Let $\mathcal{H}$ be a $n$-dimensional Hilbert space, and let $\{|f_i\rangle\}_{i=1}^n$ be an orthonormal basis of $\mathcal{H}$. We consider a bipartite system $\mathcal{H} \otimes \mathcal{H}$. Let $\Omega_{AB} = \sum_{i=1}^n \sqrt{\alpha_i} |f_i\rangle_A |f_i\rangle_B$ be a maximal entangled state in $\mathcal{H} \otimes \mathcal{H}$. The conjugation of a state $|\xi\rangle = \sum_i \alpha_i |f_i\rangle \in \mathcal{H}$ with respect to $\{|f_i\rangle\}$ is represented by $|\bar{\xi}\rangle = \sum_i \bar{\alpha_i} |f_i\rangle \in \mathcal{H}$. The conjugation of
an operator $X \in B(\mathcal{H})$ with respect to a basis $\{|f_i\rangle\}_{i=1}^n$ is denoted by $\tilde{X}$, i.e.,

$$X = \sum_{ij} \beta_{ij} |f_i\rangle \langle f_j| \rightarrow \tilde{X} = \sum_{ij} \tilde{\beta}_{ij} |f_i\rangle \langle f_j|.$$ 

One can easily check that the useful relations $\tilde{X} |\xi\rangle = |\overline{X}\xi\rangle$, $(|\eta\rangle \langle \xi| \otimes 1) |\Omega\rangle_{AB} = \frac{1}{\sqrt{\tau_0}} |\eta\rangle_A |\xi B\rangle$ and $\langle \xi|\eta\rangle = \langle \overline{\eta}|\xi\rangle = \langle \overline{\xi}|\eta\rangle$. These relations are extensively used in our proof.

By straightforward calculation, we can check the following properties:

**Proposition IV.1**

1. For all $|\psi\rangle_{AB} \in \mathcal{H} \otimes \mathcal{H}$, there exists unique $X \in B(\mathcal{H})$ such that $|\psi\rangle = (X \otimes 1) |\Omega\rangle_{AB}$.
2. $\langle \Omega, (X \otimes 1) \Omega \rangle = \frac{1}{n} Tr X$.
3. $(X \otimes 1) |\Omega\rangle_{AB} = (1 \otimes \tilde{X}^\dagger) |\Omega\rangle_{AB}$

**B. Extraction measurements**

An E-measurement performed by Alice on a pair of orthonormal states $\{|\psi_0\rangle_{AB}, |\psi_1\rangle_{AB}\}$ is a measurement described by a set of measurement operators $\{M_i \otimes \mathbb{I}\}$ satisfying $\sum_i M_i^\dagger M_i = I$, which preserve orthogonality of the states $\langle \psi_0| (M_i^\dagger \otimes \mathbb{I})(M_i \otimes \mathbb{I}) |\psi_1\rangle = 0$ for all $i$ and also equi-probability, namely, equal probability for measuring each basis state $\| (M_i \otimes \mathbb{I}) |\psi_0\rangle_{AB} \| = \| (M_i \otimes \mathbb{I}) |\psi_1\rangle_{AB} \|$, while there exists $i$ such that $M_i^\dagger M_i \neq \mathbb{R}_+ \mathbb{I}$. An E-measurement performed by Bob is defined in the same manner.

An E-measurement is not always possible and the existence of the E-measurement restricts the form of $\{|\psi_0\rangle_{AB}, |\psi_1\rangle_{AB}\}$. Note that the final pair of extraction $\{|\xi_A\rangle_{A}, |\psi_0\rangle_{B}, |\xi_A\rangle_{A}, |\psi_1\rangle_{B}\}$ is measurable by E-measurement (E-measurable) of Alice given by $\{ |\xi\rangle |\xi\rangle, |\xi^+\rangle |\xi^-\rangle \}$. On the other hand, we call another type of measurement such that $M_i^\dagger M_i \in \mathbb{R}_+ \mathbb{I}$ for all $i$, a C-measurement. Note that if extraction to Bob is possible, Alice should be able to perform the E-measurement on the last pair, otherwise extraction to Bob at the next round is not possible.

Now, we introduce a set of orthonormal base of Alice’s qubit, $S_A(|\psi_0\rangle_{AB}, |\psi_1\rangle_{AB})$. We define $S_A(|\psi_0\rangle_{AB}, |\psi_1\rangle_{AB})$ by a set of all orthogonal basis $\{|0\rangle_A, |1\rangle_A\}$ such that the decompositions

$$|\psi_0\rangle_{AB} = |0\rangle_A |\xi B\rangle + |1\rangle_A |\eta B\rangle,$$
$$|\psi_1\rangle_{AB} = |0\rangle_A |\xi^+ B\rangle + |1\rangle_A |\eta^+ B\rangle,$$  

satisfy

$$\|\xi\| = \|\xi^+\|, \|\eta\| = \|\eta^+\|, \langle \xi |\xi^-\rangle = \langle \eta |\eta^-\rangle = 0.$$  

(20)

Of course, $S_A(|\psi_0\rangle_{AB}, |\psi_1\rangle_{AB})$ can be an empty set, depending on $\{|\psi_0\rangle_{AB}, |\psi_1\rangle_{AB}\}$. We call an element in $S_A(|\psi_0\rangle_{AB}, |\psi_1\rangle_{AB})$, an orthonormal basis on which Alice can perform an E-measurement. In fact, we will see that if Alice can operate an E-measurement $\{M_i\}$ on $\{|\psi_0\rangle_{AB}, |\psi_1\rangle_{AB}\}$, then each $M_i$ have to be of the form

$$M_i = \sqrt{\tau_i^0} u_i |0\rangle_A \langle 0| + \sqrt{\tau_i^1} u_i |1\rangle_A \langle 1|,$$  

(22)

where $u_i$ is a single qubit unitary, $\{|0\rangle_A, |1\rangle_A\} \in S_A(|\psi_0\rangle_{AB}, |\psi_1\rangle_{AB})$, and $0 \leq \tau_i^0, \tau_i^1 \leq 1$. We also define $S_B(|\psi_0\rangle_{AB}, |\psi_1\rangle_{AB})$ in the same manner. Then it is obvious that for arbitrary single qubit unitary operators $u, v$ and a complex number $c \neq 0$, we have

$$S_A ((cu \otimes v) |\psi_0\rangle_{AB}, (cu \otimes v) |\psi_1\rangle_{AB}) = uS_A (|\psi_0\rangle_{AB}, |\psi_1\rangle_{AB}).$$

**C. Outline of proof**

We prove the necessary conditions for remote extraction in the following seven steps:

**Step 1:** We prove that the orthogonality and equi-probability conditions should be satisfied for all rounds of LOCC. From this, we show that the local operations in the LOCC procedure have to be E-measurements or C-measurements.

**Step 2:** We show that if Alice can perform an E-measurement $\{M_i\}$ on a pair $\{|\psi_0\rangle_{AB}, |\psi_1\rangle_{AB}\}$, then $S_A(|\psi_0\rangle_{AB}, |\psi_1\rangle_{AB})$ is non-empty. Furthermore, we see that each $M_i$ has to be of the form given by Eq. (22).

**Step 3:** We derive the explicit form of the set $S_A(|\psi_0\rangle_{AB}, |\psi_1\rangle_{AB})$ when it is not empty. We see that it is parameterized by a positive scalar $t \geq 0$.

**Step 4:** We derive the necessity conditions for both of Alice and Bob to be able to perform an E-measurement on a pair of states $\{|\psi_0\rangle_{AB}, |\psi_1\rangle_{AB}\}$.

**Step 5:** Using the result of Step 4, we prove that the following situation is impossible: Alice performs some E-measurement $\{M_i\}$ on $\{|\psi_0\rangle_{AB}, |\psi_1\rangle_{AB}\}$, and for all the results of her measurement $\{|M_i \otimes \mathbb{I}|\psi_0\rangle_{AB}, (M_i \otimes \mathbb{I}) |\psi_1\rangle_{AB}\}$, Bob can sequently perform an E-measurement.

**Step 6:** We show that if deterministic remote extraction is possible, $S_A(|\psi_0\rangle_{AB}, |\psi_1\rangle_{AB})$ is not empty.

**Step 7:** We show that Eqs. (20) and (21) imply that the Schmidt forms of $|\psi_0\rangle_{AB}, |\psi_1\rangle_{AB}$ to be given by Eqs. (5) and (6).
V. PROOF FOR NECESSITY OF REMOTE EXTRACTION

A. Step 1: Orthogonality and equi-probability

We show that deterministic remote extraction requires that the two vectors (unnormalized basis states) have to be orthogonal to each other and have the same norm at every step in LOCC. Let us consider a LOCC described by a sequence of conditional local measurements of Alice \( \{M_{j_1,\cdots,j_k} \otimes I \} \) and Bob \( \{I \otimes N_{j_1,\cdots,j_k} \} \), for \( k = 1, \cdots, N \). Each set of measurement operators \( \{M_{j_1,\cdots,j_k} \} \), \( \{N_{j_1,\cdots,j_k} \} \) satisfies

\[
\sum_{k+1} \left( M_{j_1,\cdots,j_k} \right)^\dagger M_{j_1,\cdots,j_k} = I,
\]

\[
\sum_{k} \left( N_{j_1,\cdots,j_k} \right)^\dagger N_{j_1,\cdots,j_k} = I.
\]

(23)

We use a notation \( I_k = (i_1, \cdots, i_k) \), \( J_k = (j_1, \cdots, j_k) \), as introduced in Section II and denote the vectors at each step by

\[
\begin{align*}
|\psi_{I_k}^{m_1}\rangle_{AB} &= \left( M_{I_k}^{J_k} \cdots M_{I_1}^{J_1} \otimes N_{I_m}^{J_m} \cdots N_{I_1}^{J_1} \right) |\psi_0\rangle_{AB}, \\
|\psi_{J_k}^{m_1}\rangle_{AB} &= \left( M_{J_k}^{I_k} \cdots M_{J_1}^{I_1} \otimes N_{J_m}^{I_m} \cdots N_{J_1}^{I_1} \right) |\psi_1\rangle_{AB},
\end{align*}
\]

where \( m = k - 1 \) or \( m = k \). As seen in Section II at the last turn (\( k = N \)), the two vectors are orthogonal \( \langle \psi_1^{J_{N},N} | \psi_1^{I_{N},N} \rangle = 0 \) and they have the same length \( |||\psi_1^{I_{N},N}\rangle|| = |||\psi_1^{J_{N},N}\rangle|| \). By summing up with respect to \( J_k \), using the relation (22), we have \( \langle \psi_1^{I_{N},N-1} | \psi_1^{I_{N},N-1} \rangle = 0 \) and \( ||\psi_1^{I_{N},N-1}\rangle|| = ||\psi_1^{J_{N},N-1}\rangle|| \). Repeating this summation procedure, we obtain \( \langle \psi_0^{I_k,J_k} | \psi_0^{I_k,J_k} \rangle = 0 \) and \( ||\psi_0^{I_{k-1},J_{k-1}}\rangle|| = ||\psi_0^{I_{k-1},J_{k-1}}\rangle|| \) for all \( k = 1, \cdots, N \) and \( m = k-1, k \), i.e., the orthogonality and equi-probability conditions should be satisfied for all rounds in LOCC. Therefore, the local operations in the LOCC procedure have to be E-measurements or C-measurements. As the C-measurements cannot extract information on its own, we need the E-measurements.

B. Step 2: E-measurement by Alice

We derive the necessity and sufficient conditions for Alice to be able to carry out the E-measurement.

Lemma V.1 If Alice can carry out an E-measurement on a pair of orthonormal states \( \{ |\psi_0\rangle_{AB}, |\psi_1\rangle_{AB} \} \) in \( \mathcal{H}_{AB} \), then, \( S_A(|\psi_0\rangle_{AB}, |\psi_1\rangle_{AB}) \) is not empty. Furthermore, the E-measurement have to be of the form (22).

Proof: Let \( \{M_i \otimes I\}_i \) be an E-measurement by Alice on \( \{ |\psi_0\rangle_{AB}, |\psi_1\rangle_{AB} \} \). As it is the E-measurement, there exists \( i \) such that \( M_i^\dagger M_i \neq \mathbb{R}_+^+ \). As \( M_i^\dagger M_i \) is positive, it can be diagonalized in a suitable basis \( \{ |0\rangle_A, |1\rangle_A \} \). We will show that \( \{ |0\rangle_A, |1\rangle_A \} \in S_A(|\psi_0\rangle_{AB}, |\psi_1\rangle_{AB}) \). In the basis \( \{ |0\rangle_A, |1\rangle_A \} \), we have

\[
M_i^\dagger M_i = \begin{pmatrix} \tau_0 & 0 \\ 0 & \tau_1 \end{pmatrix},
\]

where \( 0 \leq \tau_0 < \tau_1 \leq 1 \). We define two matrices \( X_0 \) and \( X_1 \) for the matrix representation of the basis states \( |\psi_0\rangle_{AB} = (X_0 \otimes 1) |\Omega\rangle_{AB} \) and \( |\psi_1\rangle_{AB} = (X_1 \otimes 1) |\Omega\rangle_{AB} \). Let us represent \( X_0, X_1 \) in this basis \( \{ |0\rangle_A, |1\rangle_A \} \) as

\[
X_0 = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \quad X_1 = \begin{pmatrix} x & y \\ z & w \end{pmatrix}.
\]

As \( |\psi_0\rangle_{AB}, |\psi_1\rangle_{AB} \) are orthogonal unit vectors satisfying \( \langle \psi_0 | \psi_1 \rangle = 0 \) and \( ||\psi_0|| = ||\psi_1|| \), we have

\[
\begin{align*}
|a|^2 + |b|^2 &= |x|^2 + |y|^2 \quad (24) \\
|c|^2 + |d|^2 &= |z|^2 + |w|^2 \quad (25) \\
a\bar{x} + b\bar{y} &= c\bar{z} + d\bar{w} = 0.
\end{align*}
\]

These conditions are rewritten in term of \( \{ |0\rangle_A, |1\rangle_A \} \) as follows: We have

\[
\begin{align*}
X_0 |\Omega\rangle &= (|0\rangle \langle 0| + |1\rangle \langle 1|) X_0 |\Omega\rangle = |0\rangle |\xi\rangle + |1\rangle |\eta\rangle, \\
X_1 |\Omega\rangle &= (|0\rangle \langle 0| + |1\rangle \langle 1|) X_1 |\Omega\rangle = |0\rangle |\xi^\perp\rangle + |1\rangle |\eta^\perp\rangle.
\end{align*}
\]

where

\[
\begin{align*}
\xi &= \frac{1}{\sqrt{2}} X_0 |0\rangle, \quad \xi^\perp &= \frac{1}{\sqrt{2}} X_1 |0\rangle, \\
\eta &= \frac{1}{\sqrt{2}} X_0 |1\rangle, \quad \eta^\perp &= \frac{1}{\sqrt{2}} X_1 |1\rangle.
\end{align*}
\]

It is easy to check that Eq. (26) is equivalent to

\[
\langle \xi | \xi^\perp \rangle = \langle \eta | \eta^\perp \rangle = 0, \quad ||\xi|| = ||\xi^\perp||, ||\eta|| = ||\eta^\perp|| \quad (27)
\]

and we conclude the basis \( \{ |0\rangle_A, |1\rangle_A \} \) is in \( S_A(|\psi_0\rangle_{AB}, |\psi_1\rangle_{AB}) \). As \( \{ |0\rangle_A, |1\rangle_A \} \) was defined as a basis that diagonalizes \( M_i^\dagger M_i \), \( M_i \) has to be of the form given by Eq. (22), i.e., the E-measurement have to be of the form of Eq. (22). \( \square \)

C. Step 3: The set \( S_A(|\psi_0\rangle_{AB}, |\psi_1\rangle_{AB}) \)

We derive the explicit form of vectors in the set \( S_A(|\psi_0\rangle_{AB}, |\psi_1\rangle_{AB}) \).
Lemma V.2 Suppose that \(|\psi_0\rangle_A, |\psi_1\rangle_A\) is not local unitary equivalent to the extracted form, and \(S_A(|\psi_0\rangle_A, |\psi_1\rangle_A)\) is not empty. Let us fix one element \(|0\rangle_A, |1\rangle_A\) in \(S_A(|\psi_0\rangle_A, |\psi_1\rangle_A)\). Then

\[
S_A(|\psi_0\rangle_A, |\psi_1\rangle_A) = \{ |e^0\rangle_A, |e^1\rangle_A | \geq 0, \]

where \(|e^0\rangle_A, |e^1\rangle_A\) is an orthonormal basis of \(\mathcal{H}_A\), labeled by a positive real number \(t\):

\[
|e^0\rangle_A = \frac{1}{\sqrt{t^2 + 1}} (|0\rangle_A + te^{i\xi} |1\rangle_A),
\]

\[
|e^1\rangle_A = \frac{1}{\sqrt{t^2 + 1}} (-te^{-i\xi} |0\rangle_A + |1\rangle_A).
\]

Here, the phase factor \(e^{i\xi}\) is determined as follows: If the Schmidt rank of \(|\psi_0\rangle_A\) is 2, then we have \(|\xi|\xi^\perp\neq 0\), \(|\xi|\xi^\perp = 1\), and we define a phase factor \(e^{2i\xi}\) by \(e^{2i\xi} = -\frac{\xi}{\xi^\perp}\). If the Schmidt rank of \(|\psi_0\rangle_A\) is 1 and \(|\psi_0\rangle_A, |\psi_1\rangle_A\) is not local unitary equivalent to the extracted form, then we have \(|\xi|\xi^\perp \neq |\xi^\perp|\xi^\perp\), and we define the phase \(e^{2i\xi} = -\frac{|\xi| - (e^{i\xi} + e^{-i\xi})}{|\xi^\perp| - |\xi^\perp|}\).

Proof

From the equivalence of Eqs. (26) and (27), the matrix forms of the basis states, \(X_0\) and \(X_1\), are represented by

\[
X_0 = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \quad X_1 = \begin{pmatrix} -\bar{b} & \bar{a} \\ -e^{2i\xi} \bar{d} & e^{2i\xi} \bar{c} \end{pmatrix}
\]

in the \(|0\rangle_A, |1\rangle_A\) basis. A general orthonormal basis can be written as \(|e^0\rangle = (|0\rangle_A + \kappa |1\rangle_A)/\sqrt{1 + |\kappa|^2}\) and \(|e^1\rangle = (-\bar{\kappa} |0\rangle_A + |1\rangle_A)/\sqrt{1 + |\kappa|^2}\) in terms of \(|0\rangle_A, |1\rangle_A\) using a parameter \(\kappa \in \mathbb{C}\). If \(|e^0\rangle_A, |e^1\rangle_A \in S_A(|\psi_0\rangle_A, |\psi_1\rangle_A)\), then the two basis states have to satisfy the condition \(|e^0\rangle_A, X_0 X_1^\dagger |e^0\rangle_A = 0\) and \(|X_1^\dagger |e^1\rangle_A\rangle = ||X_1^\dagger |e^1\rangle_A\rangle ||\), for \(i = 0, 1\). By Eq. (30), this condition is equivalent to

\[
|a + \bar{\kappa}|^2 + |b + d\bar{\kappa}|^2 = |b + e^{-2i\xi} d\bar{\kappa}|^2 + |a + e^{2i\xi} c\bar{\kappa}|^2
\]

\[
(a + c\bar{\kappa})(-b - e^{-2i\xi} d\bar{\kappa}) + (b + d\bar{\kappa})(a + e^{2i\xi} c\bar{\kappa}) = 0
\]

These conditions are also equivalent to the following conditions

\[
(\kappa - e^{2i\xi} \bar{\kappa})(a\bar{\kappa} + b d - bd\bar{\kappa} - ab\bar{\kappa} - a\bar{\kappa} c) = 0
\]

\[
(\kappa - e^{2i\xi} \bar{\kappa})(a\bar{\kappa} + b d - bd\bar{\kappa} - ab\bar{\kappa} - a\bar{\kappa} c) = 0
\]

If

\[
ad \neq bc \quad (31)
\]

or

\[
\bar{a} c + bd - bd\bar{\kappa} - a\bar{\kappa} c \neq 0, \quad (32)
\]

we have \(\kappa = te^{i\xi}\), hence we obtain \(\kappa = te^{i\xi}\) where \(t \in \mathbb{R}\). However, it is easy to see \(|e^0\rangle_A, |e^1\rangle_A\rangle = \{|e^0\_A\rangle_A, |e^1\_A\rangle_A\rangle \} \geq 0\).

D. Step 4 : E-operation from both sides

Suppose that both of Alice and Bob can perform an E-measurement on a pair of basis states \(|\psi_0\rangle_A, |\psi_1\rangle_A\rangle. This assumption excludes the possibility that \(|\psi_0\rangle_A, |\psi_1\rangle_A\rangle\) is local unitary equivalent to the extracted form at Alice or Bob from the beginning. Since Alice can perform an E-measurement, \(S_A(|\psi_0\rangle_A, |\psi_1\rangle_A\rangle)\) is non-empty and its elements are \(t\)-parameterized \(S_A(|\psi_0\rangle_A, |\psi_1\rangle_A\rangle) = \{|e^0\_A\rangle_A, |e^1\_A\rangle_A\rangle \} \geq 0\) as we have shown in Step 3. The vectors \(|\psi_0\rangle_A, |\psi_1\rangle_A\rangle\) can be decomposed with respect to the elements of \(S_A(|\psi_0\rangle_A, |\psi_1\rangle_A\rangle)\)

\[
|\psi_0\rangle_A = |e^0\rangle_A |\xi\rangle_B + |e^1\rangle_A |\eta\rangle_B, \quad (37)
\]

\[
|\psi_1\rangle_A = |e^0\rangle_A |\xi^\perp\rangle_B + |e^1\rangle_A |\eta^\perp\rangle_B, \quad (38)
\]

so that \(|\xi\rangle |\xi^\perp\rangle = \langle \eta^\perp |\eta\rangle = 0\) and \(||\xi\rangle = ||\xi^\perp\rangle ||\eta\rangle = ||\eta^\perp\rangle ||. Furthermore, every E-measurement by Alice on \(|\psi_0\rangle_A, |\psi_1\rangle_A\rangle\) is of the form

\[
M_i = \sum \tau_i u_i \langle e^0_i \_A | e^0\rangle_A \langle e^1_i \_A | e^1\rangle_A, \quad (39)
\]

where \(u_i\) is a unitary operator, \(0 \leq \tau_i, \tau_i^\perp \leq 1\) and \(i \in \mathbb{R}_+\). In Step 4, we show that under the assumption
that both Alice and Bob can perform an E-measurement on \( \{|\psi_0\rangle_{AB}, |\psi_1\rangle_{AB}\} \), the vectors \( |\xi_t\rangle_B, |\xi_t^+\rangle_B, |\eta_t\rangle_B \) and \( |\eta_t^+\rangle_B \) satisfy \( \langle \xi_t|\eta_t\rangle_B + \langle \xi_t^+|\eta_t^+\rangle_B = 0 \) and \( ||\xi_t|| = ||\eta_t|| \) for all \( t \geq 0 \).

To prove this, note that if Bob can perform an E-measurement, there exists a basis set \( \{|e_0^t\rangle_B, |e_1^t\rangle_B\} \in S_B(|\psi_0\rangle_{AB}, |\psi_1\rangle_{AB}) \) satisfying
\[
\langle e_i^t|X_0^tX_0^t|e_i^t\rangle = \langle e_i^t|X_1^tX_1^t|e_i^t\rangle = 0,
\]
for \( i = 0, 1, \) from Step 2. Note that \( X_0, X_1 \) can be represented as
\[
X_0 = \sqrt{2}(|e_0^t\rangle \langle e_0| + |e_1^t\rangle \langle e_1|),
\]
\[
X_1 = \sqrt{2}(|e_0^t\rangle \langle e_1| + |e_1^t\rangle \langle e_0|),
\]
because of Eq. (38). Let us represent the \( t \)-parameterized vectors in the \( \{|e_0^t\rangle_A, |e_1^t\rangle_A\} \) basis:
\[
|\xi_t\rangle = \alpha_0^t |e_0^t\rangle + \beta_0^t |e_1^t\rangle,
\]
\[
|\eta_t\rangle = \alpha_1^t |e_0^t\rangle + \beta_1^t |e_1^t\rangle,
\]
\[
|\xi_t^+\rangle = e^{i\epsilon_1^t}(\langle \bar{\xi}_t^+| \langle \bar{\eta}_t^+|) = \sqrt{c^t} e^{i\epsilon_0^t} + (\alpha_1^t |e_1^t\rangle + \alpha_1^t |e_1^t\rangle),
\]
\[
|\eta_t^+\rangle = e^{i\epsilon_1^t}(\langle \bar{\xi}_t^+| \langle \bar{\eta}_t^+|) = \sqrt{c^t} e^{i\epsilon_0^t} + (\alpha_1^t |e_1^t\rangle + \alpha_1^t |e_1^t\rangle).
\]

Then \( X_0^tX_0^t, X_1^tX_1^t, X_0^tX_1^t \) are represented in the \( \{|e_0^t\rangle_A, |e_1^t\rangle_A\} \) basis as
\[
X_0^tX_0^t = \sum_i \left| \alpha_i^t \right|^2\left| \beta_i^t \right|^2,
\]
\[
X_1^tX_1^t = \sum_i \left| \beta_i^t \right|^2\left| \alpha_i^t \right|^2,
\]
\[
X_0^tX_1^t = \sum_i \epsilon_i^t e^{i\epsilon_1^t}\left| -\bar{\beta}_i^t\alpha_i^t \right|^2\left| \bar{\alpha}_i^t\beta_i^t \right|^2
\]
where \( \ast \) represents irrelevant elements for our evaluation. Hence Eq. (39) implies
\[
\sum_i \left| \alpha_i^t \right|^2 = \sum_i \left| \beta_i^t \right|^2,
\]
\[
\sum_i \alpha_i^t\beta_i^t e^{-i\epsilon_1^t} = 0.
\]
It is easy to derive the relations \( \left| \beta_i^t \right| = \left| \alpha_0^t \right| \) and \( \left| \beta_i^t \right| = \left| \alpha_1^t \right| \) which imply \( ||\xi_t|| = ||\eta_t|| \) for all \( t \geq 0 \).

Representing \( X_0, X_1 \) in the \( \{|0\rangle_A, |1\rangle_A\} \) basis, from the representation in Eq. (38), we see
\[
||\xi_t|| = ||\eta_t||
\]
\[
\Leftrightarrow t^2 (|c|^2 + |d|^2 - |a|^2 - |b|^2) + 2t \left( e^{-i\epsilon_c} c a + e^{-i\epsilon_c} c a + e^{-i\epsilon_c} d b + e^{-i\epsilon_c} d b \right) - (|c|^2 + |d|^2 - |a|^2 - |b|^2) = 0
\]
\[
\Leftrightarrow (t^2 - 1)(||\eta_t||^2 - ||\bar{\eta}_t||^2) + 2t e^{-i\epsilon_c}(\langle \xi_t|\eta_t\rangle + \langle \xi_t^+|\eta_t^+\rangle) = 0.
\]
(41)

for all \( t \). This implies \( \langle \xi_0|\eta_0\rangle + \langle \xi_0^+|\eta_0^+\rangle = 0 \). But as we have a freedom about the choice of the fixed basis \( \{|0\rangle_A, |1\rangle_A\} \) (we could take \( \{|0\rangle_A = |e_0^0\rangle_A, |1\rangle_A = |e_1^0\rangle_A\} \)), we obtain \( \langle \xi_t|\eta_t\rangle + \langle \xi_t^+|\eta_t^+\rangle = 0 \) for all \( t \geq 0 \). In the matrix representation in Eq. (30), we have
\[
\langle \xi_t|\eta_t\rangle + \langle \xi_t^+|\eta_t^+\rangle = 0
\]
\[
\Leftrightarrow (-t^2 + 1)(\bar{a}e^{2i\epsilon_c} + b\bar{d}e^{2i\epsilon_c} + \bar{d}b + \bar{a}c) + 2e^{t\epsilon_c}(|c|^2 + |d|^2 - |a|^2 - |b|^2) = 0.
\]
(42)

E. Step 5: Impossibility of sequent E-measurement

Let us consider the following situation: Alice performs some E-measurement \( \{M_t\} \) on \( \{|\psi_0\rangle_{AB}, |\psi_1\rangle_{AB}\} \), and for all the results of the measurements \( \{(M_t \otimes I)|\psi_0\rangle_{AB}, (M_t \otimes I)|\psi_1\rangle_{AB}\} \), Bob can sequentially perform another E-measurement. Can this situation occur? In this Step 5, we show this is not possible. By symmetry, the situation that interchanging Alice’s and Bob’s roles is also impossible.

If this situation occurs, the pair \( \{|\psi_0\rangle_{AB}, |\psi_1\rangle_{AB}\} \) is not local unitary equivalent to the extracted form at Bob. Therefore, \( S_B(|\psi_0\rangle_{AB}, |\psi_1\rangle_{AB}) \) should be \( t \)-parameterized and \( \{|\psi_0\rangle_{AB}, |\psi_1\rangle_{AB}\} \) is decomposed as in Eq. (38). Each \( M_t \) is of the form of Eq. (39).

As it is an E-measurement, there exists \( i \) such that \( \xi_0^i \neq \tau_0^i \). After Alice’s E-measurement, the two basis states are transformed as \( |\psi_0^0\rangle_{AB} = (M_t \otimes I)|\psi_0\rangle_{AB} = \sqrt{\tau_0^i}u_t^i |e_0^i\rangle_A \langle \xi_t| + \sqrt{\tau_0^i}u_t^i |e_0^i\rangle_A \langle \eta_t| B \rangle \) and \( |\psi_0^1\rangle_{AB} = (M_t \otimes I)|\psi_0\rangle_{AB} = \sqrt{\tau_0^i}u_t^i |e_0^i\rangle_A \langle \xi_t^+| + \sqrt{\tau_0^i}u_t^i |e_0^i\rangle_A \langle \eta_t^+| B \rangle \). Note that Alice still can perform an E-measurement on this pair, (with \( \{|e_0^i\rangle_A \langle e_0^i|, |e_0^i\rangle_A \langle e_0^i| \} \), for example.) Now assume that Bob can perform an E-measurement on \( |\psi_0^0\rangle_{AB}, |\psi_1^1\rangle_{AB} \) for all
Then, we have \( r_1^0 r_1^1 \neq 0 \), and the pair of basis states \(|\psi_0\rangle_{AB}, |\psi_1\rangle_{AB}\) have to satisfy
\[
\sqrt{r_1^0} \langle \xi_1 | \eta_1 \rangle = \sqrt{r_1^1} \langle \xi_1 | \eta_1 \rangle, \tag{43}
\]
\[
\langle \xi_1 | \eta_1 \rangle + \langle \xi_1^+ | \eta_1^+ \rangle = 0 \tag{44}
\]
by Step 4. As \(|M_1\rangle\) is an E-measurement, there exists i such that \( r_1^0 \neq r_1^1 \). In the following, we see that if there exists i such that \( r_1^0 \neq r_1^1 \), Eqs. (43) and (44) have at most one solution \( t_i = t' \) in \( \mathbb{R}^+ \).

Note that Eq. (41) is equivalent to Eq. (42). If
\[
a^2 c_2^2 + b d_2^2 + d b + a c = 0, \quad |c|^2 + |d|^2 - |a|^2 - |b|^2 = 0,
\]
we have \( \tau_1^0 \neq \tau_1^1 \). Eqs. (43) and (44) have at most one solution \( t \) from Eq. (41). From Eq. (43), this implies \( r_1^0 = r_1^1 \) for all i, which contradicts our assumption. Therefore, we have
\[
a^2 c_2^2 + b d_2^2 + d b + a c \neq 0, \quad |c|^2 + |d|^2 - |a|^2 - |b|^2 \neq 0.
\]
If \( a^2 c_2^2 + b d_2^2 + d b + a c = 0 \) and \( |c|^2 + |d|^2 - |a|^2 - |b|^2 = 0 \), then Eq. (41) has the only solution \( t = 0 \). If \( a^2 c_2^2 + b d_2^2 + d b + a c \neq 0 \), we have
\[
t^2 - 1 - 2e^{i\phi} (|c|^2 + |d|^2 - |a|^2 - |b|^2) (a^2 c_2^2 + b d_2^2 + d b + a c)^{-1} = 0.
\]
This equation has one negative solution and one positive solution. Hence in any case, Eqs. (43) and (44) have at most one solution in \( \mathbb{R}^+ \).

If Eqs. (43) and (44) have no solution, we can conclude that the situation is impossible. Let us consider the case that there exists a unique solution \( t \neq 0, \) where each i has to satisfy Eqs. (43) and (44), we have
\[
l_i = s + i \text{ for all } i. \quad \text{Then by Eq. (45), we obtain } \frac{\tau_i^0}{\tau_i^1} = \frac{|| \eta_i \rangle_{A} ||^2}{|| \xi_i \rangle_{A} ||^2} = r \text{ for all } i, \text{i.e., the ratio of } \tau_i^0 \text{ and } \tau_i^1 \text{ is independent of } i. \quad \text{Furthermore, there exists } i \text{ such that } \tau_i^0 \neq \tau_i^1, \text{ the ratio } r \text{ is not 1. Therefore, we have }
\]
\[
\sum_i M_i^0 M_i = \frac{r_1^0}{r_1^1} \langle e_i^0 | e_i^0 \rangle + \frac{r_1^1}{r_1^0} \langle e_i^1 | e_i^1 \rangle = \frac{1}{2s+1} \sum_i \left( \frac{r}{r_1} + \frac{s^2}{2s+1} \right)
\]
As for \( r \neq 1, \) this is not equal to \( I \). This contradicts the normalization condition of the measurement operator
\[
\sum_i M_i^0 M_i = I. \quad \text{Therefore, the situation we have considered cannot occur.}
\]

**F. Step 6: Necessary conditions for remote extraction**

Suppose that remote extraction to Bob’s qubit is possible somehow. If \(|\psi_0\rangle_{AB}, |\psi_1\rangle_{AB}\) is not local unitary equivalent to the extracted form, it should be possible to carry out the first E-measurement, for either Alice or Bob. If Alice can carry it out, \( S_A(|\psi_0\rangle_{AB}, |\psi_1\rangle_{AB}) \) is not empty. On the other hand, if Alice cannot perform the first E-measurement, Bob have to be able to do it. However, it is impossible from the following reason: Recall that the final pair Eq. (1) is a pair of the basis states that Alice can carry out an E-measurement. As we consider only finite rounds of LOCC, this means at some point of LOCC, Bob performs an E-measurement and after any result of Bob’s E-measurement, Alice should be able to perform an E-measurement i.e., the situation considered in Step 5 should occur. However, we have shown that it is impossible in Step 5. Therefore, the extraction to Bob’s qubit is only available for the case that Alice can perform the first E-measurement, i.e., the case that \( S_A(|\psi_0\rangle_{AB}, |\psi_1\rangle_{AB}) \) is not empty. Furthermore, as we have seen above, Bob can carry out only C-measurements in the extraction procedure.

**G. Schmidt picture**

In this Step 7, we represent the conditions of Eq. (20) for \( S_A(|\psi_0\rangle_{AB}, |\psi_1\rangle_{AB}) \) in the Schmidt form given by Eqs. (5) and (6). Suppose that Eq. (20) is satisfied and let
\[
|\psi_0\rangle_{AB} = \sqrt{\lambda_0} |a_0\rangle_A |b_0\rangle_B + \sqrt{\lambda_1} |a_1\rangle_A |b_1\rangle_B
\]
\[
|\psi_1\rangle_{AB} = \sqrt{\lambda_0'} |a_0'\rangle_A |b_0'\rangle_B + \sqrt{\lambda_1'} |a_1'\rangle_A |b_1'\rangle_B
\]
be the Schmidt decompositions of \(|\psi_0\rangle_{AB}, |\psi_1\rangle_{AB}\), respectively. Then we have
\[
X_0/\sqrt{2} = \sqrt{\lambda_0} |a_0\rangle_B + \sqrt{\lambda_1} |a_1\rangle_B |b_0\rangle_B + |0\rangle\langle \bar{\xi}_0 | 1\rangle\langle 1 | \bar{\eta}_0 \rangle, \quad X_1/\sqrt{2} = \sqrt{\lambda_0'} |a_0'\rangle_B + \sqrt{\lambda_1'} |a_1'\rangle_B |b_0'\rangle_B + |0\rangle\langle \bar{\xi}_1 | 1\rangle\langle 1 | \bar{\eta}_1 \rangle.
\]
By the relations \( \langle \xi^+ | \rangle = \langle \eta | \eta^+ \rangle = 0 \) and \( || \xi \|| = || \xi^+ \||, \quad || \eta \|| = || \eta^+ \|| \), the vectors \( |\xi\rangle_B, |\xi^+\rangle_B, |\eta\rangle_B, |\eta^+\rangle_B \) are represented in the basis parallel to \( |\xi\rangle_B \) as
\[
|\xi\rangle_B = \begin{pmatrix} s \\ 0 \end{pmatrix}, \quad |\xi^+\rangle_B = \begin{pmatrix} 0 \\ s \end{pmatrix}, \quad |\eta\rangle_B = \begin{pmatrix} \alpha' \\ \beta' \end{pmatrix}, \quad |\eta^+\rangle_B = e^{i\alpha} \begin{pmatrix} -\beta' \\ \alpha' \end{pmatrix},
\]
for \( s \in \mathbb{R} \), \( \alpha', \beta' \in \mathbb{C} \). Therefore, we have
\[
|\xi\rangle\langle \xi | + |\eta\rangle\langle \eta | = \begin{pmatrix} s^2 + |\alpha'|^2 & \alpha' \beta' \\ \beta' \alpha' & |\beta'|^2 \end{pmatrix} = \lambda_0 |b_0\rangle_B \langle b_0 | + \lambda_1 |b_1\rangle_B \langle b_1 | + |\eta^+\rangle\langle \eta^+ | = \begin{pmatrix} \beta'^2 & -\alpha' \beta' \\ -\beta' \alpha' & s^2 + |\alpha'|^2 \end{pmatrix} = \lambda_0' |b_0'\rangle_B \langle b_0' | + \lambda_1' |b_1'\rangle_B \langle b_1' |
\]
From these relations, we derive that \( \lambda_0 = \lambda_0', \lambda_1 = \lambda_1', |b_0\rangle_B \) is parallel to \( |b_1\rangle_B \), and \( |b_0'\rangle_B \) is parallel to \( |b_0\rangle_B \). By modifying the phase of \( |a_0\rangle_A \) and \( |a_1\rangle_A \) appropriately, we can take \( |b_0'\rangle_B = |b_1\rangle_B \) and \( |b_1'\rangle_B = |b_0\rangle_B \).

**H. The form of LOCC**

Finally, we present the explicit form of LOCC. By Section 111 the basis \(|0\rangle_A, |1\rangle_A\) represented by \(|0\rangle_A =\)
Let $|\psi\rangle_{AB}, |\psi\rangle_B \in \mathcal{H}_{AB}$, $\langle \psi | \psi \rangle = 0$. We consider the basis states in the matrix representation: $|\psi\rangle_{AB} = (X_0 \otimes 1)|\Omega\rangle_{AB}, |\psi\rangle_{AB} = (X_1 \otimes 1)|\Omega\rangle_{AB}$. First we show the following lemma.

**Lemma VI.1** Suppose that there exists a matrix $M \neq 0$ and vectors $|\chi\rangle, |\xi\rangle$ satisfying the following property: for all $a, b \in \mathbb{C}$, there exists $C_{a,b} \in \mathbb{C}$ such that

$$(M \otimes 1)(a|\psi\rangle_{AB} + b|\psi\rangle_B) = C_{a,b}|\chi\rangle_{A} \otimes |\xi\rangle_{B}.$$  

Then if the Schmidt rank of $|\psi\rangle_{AB}$ (resp. $|\psi\rangle_B$) is 2, $M = |\chi\rangle \langle \eta |$, where $|\eta\rangle$ is an eigenvector of a matrix $(X_0^{-1})^{-1}X_1^{-1}$. If the Schmidt rank of both of $|\psi\rangle_{AB}$ and $|\psi\rangle_B$ are 1 and the basis states are represented by $|\psi\rangle_{AB} = |f\rangle_{A}|\xi\rangle_{B}, |\psi\rangle_{AB} = |f'\rangle_{A}|\xi'\rangle_{B}$, then one of the following occurs:

1. $M = |\chi\rangle \langle f^{-1} |$
2. $M = |\chi\rangle \langle f'^{-1} |$
3. $|\xi\rangle_{B}$ and $|\xi'\rangle_{B}$ are parallel to each other and $M = |\chi\rangle \langle \eta |$ for an arbitrary vector $|\eta\rangle$.

**Proof**

If the Schmidt rank of $|\psi\rangle_B$ is 2, and $(M \otimes 1)|\psi\rangle_{AB} = C_{1,0}|\chi\rangle_{A} \otimes |\xi\rangle_{B}, M$ has to be of rank 1. We represent it as $M = |\chi\rangle \langle \eta |$ by introducing a vector $|\eta\rangle$. Then we have

$$M = |\chi\rangle \langle \eta | = \frac{(M \otimes 1)|\psi\rangle_{AB} = \left( |\chi\rangle \langle X_0 \eta | \otimes 1 \right) \Omega}{\sqrt{2}}.$$  

By Step 5, Bob can carry out only a C-measurement for remote extraction at Bob, therefore, all $N'_{1,1}$ are scalar multiplications of unitary operators. On the other hand, the form of Alice’s measurement on the pair of the states $(|\psi\rangle_{AB}, |\psi\rangle_B)$ have to be $M_i = \sqrt{\tau_i} u_i |\epsilon_i\rangle \langle \epsilon_i | + \sqrt{\tau_i} u_i |\epsilon_i\rangle \langle \epsilon_i |$, with a unitary operation $u_i$, $0 \leq \tau_i \leq 1$ and $\{ |\epsilon_i\rangle, |\epsilon_i\rangle \} \in S_A(|\psi\rangle_{AB}, |\psi\rangle_B)$. For this $M_i$ and a nonzero scalar multiplication of a unitary operator $N_i$, we can see $S_A(M_i \otimes N_i |\psi\rangle_{AB}, M_i \otimes N_i |\psi\rangle_B)$ if $\tau_i \neq 0$, from the argument in Step 2. Note that if $\tau_i \neq 0$, the pair $M_i \otimes N_i |\psi\rangle_{AB}, M_i \otimes N_i |\psi\rangle_B$ is locally unitary equivalent to the transformed form at Bob. Thus, we obtain the form of Alice’s measurement given in the Theorem inductively.

**VI. PROOF FOR REMOTE DESTRUCTION**

As the Schmidt rank of $|\psi\rangle_{AB}$ is 2, the rank of $X_0$ is 2, i.e., $X_0$ is invertible. Therefore, $C_{1,0} \neq 0$, and

$$\sqrt{2} |\xi\rangle = \frac{1}{C_{1,0}} |X_0^{-1}X_1^{-1}\rangle.$$  

Then we obtain

$$|X_0^{-1}\rangle = \frac{C_{1,0}^{-1}}{C_{1,0}} |X_0^{-1}\rangle.$$  

As $X_0$ is invertible, we have

$$|X_0^{-1}\rangle = \frac{C_{1,0}}{C_{1,0}^{-1}} |\eta\rangle.$$  

Hence $|\eta\rangle$ is an eigenvector of $(X_0^{-1})^{-1}X_1^{-1}$. The result is also unchanged for the case that Schmidt rank of $|\psi\rangle_B$ is 1.

Next we present the following Lemma for the cases where the Schmidt the Schmidt rank of $|\psi\rangle_{AB}$ (resp. $|\psi\rangle_B$) is 2.

**Lemma VI.2** If the Schmidt rank of $|\psi\rangle_{AB}$ (resp. $|\psi\rangle_B$) is 2, deterministic remote destruction is possible if and only if the matrix $$(\sqrt{X_0} |a_0\rangle \langle b_0 | + \sqrt{X_1} |a_1\rangle \langle b_1 |)(\sqrt{X_0} |b_0\rangle \langle a_0 | + \sqrt{X_1} |b_1\rangle \langle a_1 |)$$

is diagonalized by some orthonormal basis $\{ |f_0\rangle, |f_1\rangle \}$ with eigenvalues $\omega_0, \omega_1 \in \mathbb{C}$. Furthermore, the measurement operators for deterministic remote destruction $\{ M_i \}$ are of the form

$$M_i = |\chi_i\rangle \langle f_k |,$$

where $|\chi_i\rangle$ is an arbitrary vector and $k_i = 0, 1$.

**Proof** Note that
\[(X_0^{-1})^\dagger X_1^{-1} = 2 \left( \frac{1}{\sqrt{\lambda_0}} |a_0\rangle \langle b_0| + \frac{1}{\sqrt{\lambda_1}} |a_1\rangle \langle b_1| \right) \left( \sqrt{\lambda_0} |b_0\rangle \langle a_0| + \sqrt{\lambda_1} |b_1\rangle \langle a_1| \right).\]

If \((X_0^{-1})^\dagger X_1^{-1}\) is diagonalized by an orthonormal basis \(\{|f_k\rangle\}\) with corresponding eigenvalues \(\{z_k\}\), then we have \(X_1^\dagger |f_k\rangle = z_k X_0^\dagger |f_k\rangle\), for \(k = 0, 1\). We set \(\xi^k = \sum_i M_i^\dagger M_i = I\). Therefore, \((X_0^{-1})^\dagger X_1^{-1}\) has two eigenvectors. However, we cannot take them orthogonal to each other, it is again impossible to have \(\sum_i M_i^\dagger M_i = I\). Therefore, \((X_0^{-1})^\dagger X_1^{-1}\) has two orthogonal eigenvectors, which means that it is diagonalized by the orthonormal basis, and \(M_i\) has to be given as in Eq. (46). The proof for the case that the Schmidt rank of \(|\psi\rangle_{AB}\) is 2 is identical.

Now we present a Lemma for the cases where both of the basis states \(|\psi\rangle_{AB}, |\psi\rangle_{AB}\) have the Schmidt rank 1.

**Lemma VI.3** If the Schmidt rank of both of \(|\psi\rangle_{AB}\) and \(|\psi\rangle_{AB}\) are 1, then deterministic remote destruction is possible if and only if \(|\psi\rangle_{AB}, |\psi\rangle_{AB}\) are of the form

\[|\psi\rangle_{AB} = |a_0\rangle_A |b_0\rangle_B, |\psi\rangle_{AB} = |a_0^\perp\rangle_A |b_0^\perp\rangle_B,\]  \hspace{1cm} (46)

where \(|a_0\rangle_A, |a_0^\perp\rangle_A\) are orthogonal. The measurement operators \(M_i\) are of the form

\[M_i = |\chi_i\rangle \langle \eta_i|.

Here, the vector \(|\eta_i\rangle\) have to be \(|a_0\rangle\) or \(|a_0^\perp\rangle\) if \(|b_0\rangle_B, |b_0^\perp\rangle_B\) are not parallel to each other, while it can be an arbitrary vector if \(|b_0\rangle_B, |b_0^\perp\rangle_B\) are parallel to each other.

**Proof:** If \(|\psi\rangle_{AB}, |\psi\rangle_{AB}\) are of the forms given by Eq. (46), then we can take \([M_0 = |a_0\rangle \langle a_0|, M_1 = |a_0^\perp\rangle \langle a_0^\perp|]\) for destruction. Conversely, suppose that by performing a measurement represented by \(\{M_i\}_i\), deterministic remote destruction is possible. We represent the basis states as

\[|\psi\rangle_{AB} = |f\rangle_A \langle \xi|_B \cdot |\psi\rangle_{AB} = |f\rangle_A \langle \xi|_B.\]

Note that either \((f, f') ≠ 0\) or \((\xi, \xi') ≠ 0\) should hold. By Lemma VI.1, \(M_i\) has to be either of the form \(I-\theta\) in the Lemma. If \((f, f') ≠ 0\), we have \((\xi, \xi') = 0\) and the situation \(\theta\) cannot occur. However, if \((f, f') = 0\), we also have \((f^\perp, f'^\perp) ≠ 0\) and \(M_i\) can not satisfy \(\sum_i M_i^\dagger M_i = I\). Hence we obtain \((f, f') = 0\). Again by Lemma VI.1 if \((\xi|_B)\) and \((\xi'|_B)\) are not parallel, each \(M_i\) has to be of the form \(M_i = |\chi_i\rangle \langle f|, M_i = |\chi_i\rangle \langle f'|\) while they are parallel, then \(M_i = |\chi_i\rangle \langle \eta_i|\) for an arbitrary \(|\eta_i\rangle\).

Now, let us prove Theorem II.2 for remote destruction. From Lemma VI.2 if \(|\psi\rangle_{AB}\) has Schmidt rank 2, destruction is possible if and only if

\[(X_0^{-1})^\dagger X_1^{-1} = z_0 |f_0\rangle \langle f_0| + z_1 |f_1\rangle \langle f_1| \equiv Z^\dagger,

for some orthogonal basis \(f_0, f_1\). This is equivalent to

\[X_1 = Z X_0, Z^\dagger Z = ZZ^\dagger.\]  \hspace{1cm} (47)

Using orthogonality condition \((b_1, b_0') = (b_0, b_1') = 0\), one can easily check that Eq. (10) implies Eq. (17). Below, we show that Eq. (17) implies Eq. (14).

Now, using Schmidt decomposition, we have \(X_0 = \sqrt{\lambda_0} |a_0\rangle \langle b_0| + \sqrt{\lambda_1} |a_1\rangle \langle b_1|\). Representing \(Z\) in this basis as \(Z = a |a_0\rangle \langle a_0| + b |a_0\rangle \langle a_1| + c |a_1\rangle \langle a_0| + d |a_1\rangle \langle a_1|\), Eq. (17) can be written as \(X_1 = Z X_0 = \sqrt{\lambda_0} (a |a_0\rangle + c |a_1\rangle) \langle b_0| + \sqrt{\lambda_1} (b |a_0\rangle + d |a_1\rangle) \langle b_1|\). Using the conditions \(\text{Tr} X_1^\dagger X_1 = \text{Tr} X_0^\dagger X_0\), \(\text{Tr} X_1^\dagger X_1 = 0\)
we obtain
\[ \lambda_0(|a|^2 + |c|^2) + \lambda_1(|b|^2 + |d|^2) = \lambda_0 + \lambda_1, \] (48)
and
\[ \lambda_0a + \lambda_1d = 0. \] (49)
On the other hand, Eq. (17) requires
\[ |b| = |c|, \quad ab + cd = ca + db. \] (50)
Combining these relations, we see that \( a, b, c, d \) have to be of the form
\[ a = \sqrt{\frac{\lambda_1}{\lambda_0}} \cos \gamma e^{i\alpha}, \quad b = \sin \gamma e^{i\beta}, \]
\[ c = \sin \gamma e^{2i\alpha - i\beta}, \quad d = -\sqrt{\frac{\lambda_0}{\lambda_1}} \cos \gamma e^{i\alpha}. \]
Substituting these, \( X_1 \) is given by
\[
X_1 = |a_0\rangle \left\langle \sqrt{\lambda_1} \cos \gamma e^{-i\alpha} |b_0\rangle + \sqrt{\lambda_1} \sin \gamma e^{-i\beta} |b_1\rangle \right\rangle + |a_1\rangle \left\langle \sqrt{\lambda_0} \sin \gamma e^{-2i\alpha + i\beta} |b_0\rangle - \sqrt{\lambda_0} \cos \gamma e^{-i\alpha} |b_1\rangle \right\rangle. \]
Note that \( \sqrt{\lambda_1} \cos \gamma e^{-i\alpha} |b_0\rangle + \sqrt{\lambda_1} \sin \gamma e^{-i\beta} |b_1\rangle \) and \( \sqrt{\lambda_0} \sin \gamma e^{-2i\alpha + i\beta} |b_0\rangle - \sqrt{\lambda_0} \cos \gamma e^{-i\alpha} |b_1\rangle \) are orthogonal. Hence this decomposition in the matrix form gives the Schmidt decomposition of the vector \( |\psi_1\rangle_{AB} \), and we obtain Eq. (10).

VII. SUMMARY AND DISCUSSIONS

In this paper, we present necessary and sufficient conditions for remote extraction and destruction of single-qubit information encoded and spread in two-qubit states. The conditions show that there are ways to spread qubit information into a two-qubit Hilbert space in a less “non-local” manner, namely, the recovery (extraction) of qubit information at one of the qubits and irreversible erasure (destruction) of qubit information can be achieved by measurements on only one of the qubits and classical communications, even though the encoded two qubit states are entangled in general.

The main part of the paper is devoted to the proof of necessity for remote extraction shown in seven steps. By introducing the notation of extraction measurements (E-measurements), which are local measurements preserving orthogonality of the basis states for encoding and equal probability for measuring each basis state, we evaluate the conditions of the basis states for the existence of E-measurements. We have derived necessary and sufficient conditions for basis states for encoding and the explicit form of measurements.

Necessary and sufficient conditions for remote extraction indicate the possibility of sharing qubit information between two parties in an asymmetric manner, namely, we can spread qubit information such that it can be remotely extracted to only one of the parties by using LOCC but not to the other party. Since impossibility of LOCC tasks implies the existence of a kind of non-locality, the possibility of asymmetric qubit information sharing indicates that such non-locality can be asymmetric between two parties. The obtained necessary and sufficient conditions for remote destruction indicate that such asymmetric non-locality for irreversibly destroying qubit information can also be introduced, but the conditions for asymmetric cases are not compatible with those for remote extraction. Remote destruction by one of the parties is possible if and only if remote extraction at that party is possible.

If we consider Alice’s system in our model as an environment, it is a similar situation to quantum lost and found considered by Gregoretti and Werner in [8]. In their paper, they have obtained necessary and sufficient conditions for extracting quantum information spread over the system and environment due to the system-environment coupling, by measuring the environment and performing conditional operations on the system. By using quantum information theoretical analysis, they have proven that extraction is possible if and only if when a map \( \Lambda \) for the system state \( |\phi\rangle_S \) can be represented by the random unitary channel \( \Lambda(\phi)_S = \sum_k p_k \phi_k \langle \phi | u_k \rangle \), where \( \{ \phi_k \} \) is a set of random unitary operators acting on the system qubit, and \( p_k \) is probability satisfying \( \sum_k p_k = 1 \).

We note that our remote extraction can be regarded as a special case where both the system and environment consist of a single qubit, however we consider the conditions for general LOCC whereas they consider only one-way (from the environment to the system) LOCC for quantum information extraction. In the case of the single qubit system-environment, a purification of the map \( \Lambda \) gives a corresponding transformation describing the spread of qubit information to the two parties, the system and environment;
\[
|\alpha e_0 + \beta e_1\rangle_S \rightarrow \sqrt{p_0} |g_0\rangle_E \otimes u_0 |\alpha e_0 + \beta e_1\rangle_S + \sqrt{p_1} |g_1\rangle_E \otimes u_1 |\alpha e_0 + \beta e_1\rangle_S \] (51)
for arbitrary \( \alpha \) and \( \beta \), where \( \{|g_0\rangle_E, |g_1\rangle_E\} \) is an orthonormal basis of the environment. They are equivalent to our LOCC extraction conditions for basis states given by Eqs. (5) and (6). Therefore, the encoding conditions for remote extraction of qubit information spread into two-qubit states are same for both one-way LOCC and general LOCC, in spite of the inapplicability of the Lo-Popescu theorem to this task.

Acknowledgments

The authors are grateful to D. Markham for discussions. This work was supported by the Suntitomo Foundation, the Asahi Glass Foundation, and the Japan Society of the Promotion of Science. Y. O. was supported
by the COE21 program at Graduate School of Mathematical Sciences, the University of Tokyo. M. M. was partially supported by the Special Coordination Funds for Promoting Science and Technology.

[1] P.W. Shor, in *Proc., 35th Annual Symposium of Foundation of Computer Science*, IEEE Press (1994); L. Grover, in *Proc. 28th Annual ACM Symposium on the Theory of Computation*, 212, ACM Press (1996).
[2] P.W. Shor, Phys. Rev. A **52**, R2493 (1995); A.R. Calderbank and P.W. Shor, Phys. Rev. A **54**, 1098 (1996); A.M. Steane, Phys. Rev. Lett. **77**, 793 (1996).
[3] V. Bužek and M. Hillery, Phys. Rev. A **54**, 1844 (1996).
[4] C.H. Bennett et.al., Phys. Rev. Lett. **70**, 1895 (1993).
[5] C. H. Bennett, D. P. DiVincenzo, C. A. Fuchs, T. Mor, E. Rains, P. W. Shor, J. A. Smolin, and W. K. Wootters, Phys. Rev. A **59**, 1070 (1999).
[6] M. Owari and M. Hayashi, Phys. Rev. A **74**, 032108 (2006)
[7] H.-K. Lo and S. Popescu, Phys. Rev. A **63**, 022301 (2001).
[8] M. Gregoretti and R. F. Werner, J. Mod. Opt. **50**, 915 (2003).