Port-based telecloning of an unknown quantum state

Reiji Okada,* Kohtaro Kato,† and Francesco Buscemi‡
Graduate School of Informatics, Nagoya University, Furo-cho, Chikusa-ku, Nagoya 464-8601, Japan

(Received 13 February 2025; accepted 21 April 2025; published 6 May 2025)

Telecloning is a protocol introduced by Murao *et al.* [Phys. Rev. A **59**, 156 (1999)] to distribute copies of an unknown quantum state to many receivers in a way that beats the trivial "clone-and-teleport" protocol. In the last decade, a new type of teleportation called *port-based teleportation*, in which the receiver can recover the state simply by looking at the correct port without having to actively perform correction operations, has been widely studied. In this paper, we consider the analog of telecloning, in which conventional teleportation is replaced by the port-based variant. To achieve this, we generalize the optimal measurement used in port-based teleportation and develop a new one that achieves port-based telecloning. Numerical results show that, in certain cases, the proposed protocol is strictly better than the trivial clone-and-teleport approach.

DOI: 10.1103/PhysRevA.111.052408

I. INTRODUCTION

Quantum teleportation [1] is one of the basic protocols in quantum communication, allowing the transmission of quantum information from one location to another without physically moving the particles carrying the quantum state and instead using only local operations and classical communications with preshared quantum entanglement. Quantum teleportation is used in quantum repeaters [2] and is essential for the realization of long-distance quantum communication. The standard version of teleportation (ST) requires the receiver to actively perform a unitary correction on its system, depending on the classical information received from the sender.

Port-based teleportation (PBT) is an alternative type of quantum teleportation proposed by Ishizaka and Hiroshima [3,4] that uses a multipartite entangled state whose subsystems are called ports. Unlike ST, PBT does not require the receiver to actively perform a unitary transformation; instead, the teleportation process is completed simply by selecting one of the multiple ports depending on the sender's measurement result and discarding the others. This feature enables PBT to be applied to universal programmable quantum processors [3]. However, the no-programming theorem [5] shows that faithful and deterministic universal programmable quantum processors cannot be realized in a finite-dimensional system. Therefore, PBT succeeds only approximately or probabilistically. Despite these limitations, PBT has also been applied in areas such as instantaneous nonlocal quantum computation [6] and communication complexity and Bell nonlocality [7]. There has been extensive research on the performance [8–12] and algorithms [13–16] of PBT.

Telecloning, proposed by Murao *et al.* [17,18], is a protocol that generalizes teleportation with the goal of distributing a single unknown input state to many distant receivers. Since perfect copying of an unknown quantum state is forbidden by the no-cloning theorem [19–21], telecloning aims to transfer optimal clones instead [22,23].

Existing telecloning protocols are based on ST and thus require receivers to actively perform unitary transformations to complete the protocol. In this paper, we introduce port-based telecloning (PBTC), which combines telecloning with (multi-)PBT and allows the transmission of copies of an unknown quantum state without requiring active corrections by the receivers. To this end, we generalize the measurement used in PBT and propose a new one that, when used on maximally entangled resource states, asymptotically achieves the fidelity of the optimal universal cloning protocol [23]. Interestingly, numerical results show that when the number of ports is small, PBTC achieves a transmission fidelity that is *strictly higher* than that achievable by the naive method of simply performing optimal cloning and PBT sequentially. Throughout the study, we consider deterministic protocols using maximally entangled resource states. Room to investigate optimal resource states and a probabilistic variant of PBTC remains. See Sec. II A for details.

The structure of this paper is as follows. In Sec. II, we summarize the necessary concepts of PBT and telecloning. In Sec. III, we introduce PBTC and explain its protocol. After discussing the generalization of the positive operator-valued measure (POVM) and its asymptotic optimality, we compare the performance with the trivial protocol. In Sec. IV, we provide a summary and discuss open questions.

II. PRELIMINARIES

A. Port-based teleportation

For a finite-dimensional Hilbert space $\mathcal{H}$, $\mathcal{L}(\mathcal{H})$ denotes the space of linear operators on $\mathcal{H}$. In PBT, Alice (the sender)

*Contact author: reiji.okada@nagoya-u.jp
†Contact author: kokato@i.nagoya-u.ac.jp
‡Contact author: buscemi@nagoya-u.jp

and Bob (the receiver) share an entangled state $\Phi_{A^N B^N} \in \mathcal{L}(\mathcal{H}^{\otimes N} \otimes \mathcal{H}^{\otimes N})$ on $2N$ qudits, and Alice has the input pure state $\sigma_X \in \mathcal{L}(\mathcal{H}_X)$. Here, system $A^N \equiv A_1 \cdots A_N$ ($B^N \equiv B_1 \cdots B_N$) is on Alice's (Bob's) side. Each system A is associated with a finite-dimensional Hilbert space $\mathcal{H}_A \cong \mathbb{C}^d$. The shared entangled state $\Phi_{A^N B^N}$ is called a *resource state*, and each of systems $A_1, \ldots, A_N$ and $B_1, \ldots, B_N$ is referred to as a *port*.

PBT is mainly classified into *deterministic* PBT (dPBT) and *probabilistic* PBT (pPBT). Although dPBT always succeeds, faithful transfer can be achieved only asymptotically. On the other hand, pPBT always achieves faithful transmission, but the unit success probability of the protocol is only asymptotically achieved. In this work, we focus on only the deterministic version, so we refer to dPBT simply as PBT. The protocol of PBT is as follows:

(1) Alice jointly measures the input system X and all her ports A^N with a POVM $\{E^i_{XA^N}\}_{i=1}^N$.

(2) Alice relays the outcome $i \in \{1, \ldots, N\}$ to Bob via classical communication.

(3) Bob selects the port B_i and discards all other ports $B^N \setminus B_i$.

This completes the protocol, and the state is transferred to the remaining port B_i. The PBT channel $\mathcal{E}_N : \mathcal{L}(\mathcal{H}_X) \to \mathcal{L}(\mathcal{H}_B)$ is then expressed as follows:

$$\mathcal{E}_N(\sigma_X) = \sum_{i=1}^{N} \mathrm{Tr}_{XA^N B_i^c}\left[E^i_{XA^N}(\sigma_X \otimes \Phi_{A^N B^N})\right], \tag{1}$$

where $B_i^c \equiv B^N \setminus B_i = B_1 \cdots B_{i-1} B_{i+1} \cdots B_N$ and the remaining system B_i is relabeled as output system B. The left side of Fig. 1 represents PBT [3].

The performance of PBT is evaluated by entanglement fidelity. The entanglement fidelity F of a quantum channel $\mathcal{N} : \mathcal{L}(\mathcal{H}) \to \mathcal{L}(\mathcal{H})$ is defined as follows:

$$F(\mathcal{N}) := \langle \Phi^+ | (\mathcal{N} \otimes \mathrm{id})(\Phi^+) | \Phi^+ \rangle, \tag{2}$$

where $\Phi^+ = |\Phi^+\rangle \langle \Phi^+|$ is the maximally entangled state, defined by $|\Phi^+\rangle = \frac{1}{\sqrt{d}} \sum_{i=1}^d |i\rangle |i\rangle$ for the orthonormal basis $\{|i\rangle\}_{i=1}^d$, and id is the identity channel. Entanglement fidelity is related to average output fidelity f, which is defined as follows:

$$f(\mathcal{N}) := \int \mathrm{d}\phi \langle \phi | \mathcal{N}(\phi) | \phi \rangle, \tag{3}$$

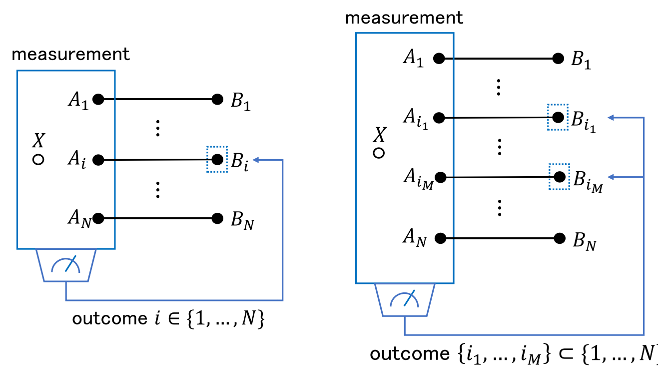
where the integral is performed with respect to the uniform distribution $\mathrm{d}\phi$ over all input pure state. These two quantities are connected by the following relationship [24]:

$$f(\mathcal{N}) = \frac{F(\mathcal{N})d + 1}{d + 1}. \tag{4}$$

An important class of POVMs in PBT is the pretty good measurement (PGM; also known as a square-root measurement) [25,26]. The PGM $\{E^i\}_i$ for the state ensemble $\{(p_i, \sigma^i)\}_{i \in \mathcal{I}}$ is given by

$$E^i = \bar{\sigma}^{-\frac{1}{2}} p_i \sigma^i \bar{\sigma}^{-\frac{1}{2}}, \tag{5}$$

where $\bar{\sigma} = \sum_{i \in \mathcal{I}} p_i \sigma^i$ and $\bar{\sigma}^{-1}$ is defined on the support of $\bar{\sigma}$, which can always be assumed to be invertible, without loss of generality. Note that the sum of E^i defined by (5) is the projection onto the support of $\bar{\sigma}$, which generally does not coincide with the identity operator. One way to make them POVMs in the full Hilbert space is to add



(a) port-based teleportation (b) port-based telecloning

FIG. 1. (a) The setting of port-based teleportation (PBT). Alice and Bob share entangled states in ports $A_1, \ldots, A_N$ and $B_1, \ldots, B_N$, with Alice also holding the input state in the system X. In the protocol, Alice first measures systems $XA_1 \cdots A_N$ and sends the outcome $i \in \{1, \ldots, N\}$ to Bob, who then selects port B_i. This completes the protocol. (b) The setting of port-based telecloning (PBTC). PBTC is best thought of as having N receivers, where the ith receiver has port B_i ($i = 1, \ldots, N$), and the goal of the protocol is to have M receivers get approximate copies of the state of system X. In the protocol, Alice performs a measurement with a multi-index outcome, i.e., a subset $\{i_1, \ldots, i_M\} \subset \{1, \ldots, N\}$, and sends the outcome to all receivers. Each receiver keeps their port if their port number is contained in Alice's outcome. This completes the protocol, and an approximate copy of the input state of X is transferred to M receivers.

$$\Delta = \frac{1}{|\mathcal{I}|}\left(\mathbb{1} - \sum_{i \in \mathcal{I}} E^i\right) \tag{6}$$

to each E^i. This does not change the argument in PBT since $\mathrm{Tr}[\Delta \sigma^i] = 0$.

References [4,12] showed that the POVM that maximizes the fidelity of PBT is the PGM constructed from the ensemble $\{(1/N,\ \rho^i_{XA^N})\}_{i=1}^N$, where

$$\rho^i_{XA^N} := \Phi^+_{XA_i} \otimes \frac{1}{d^{N-1}} \mathbb{1}_{A_i^c}. \tag{7}$$

A PBT protocol that uses N pairs of maximally entangled states as ports and the PGM for $\{(1/N,\ \rho^i_{XA^N})\}_{i=1}^N$ as a measurement is called *standard* PBT. The entanglement fidelity of the standard PBT channel $\mathcal{E}_N^{\mathrm{std}}$ is computed as follows [11]:

$$F\left(\mathcal{E}_N^{\mathrm{std}}\right) = 1 - \frac{d^2 - 1}{4N} + O(N^{-\frac{3}{2}+\delta}), \tag{8}$$

where $\delta > 0$. In addition, we can consider using any resource state and are not limited to maximally entangled states. Even in this case, it is known that the PGM that is the same as the POVM used in standard PBT is optimal (i.e., maximizing entanglement fidelity) [12]. If we denote a PBT channel using the PGM and optimal resource states as $\mathcal{E}_N^{\mathrm{opt}}$, the performance of such a channel can be expressed as follows [11]:

$$F\left(\mathcal{E}_N^{\mathrm{opt}}\right) = 1 - \Theta(N^{-2}). \tag{9}$$

B. Telecloning

Telecloning [17,18] is a generalization of ST to the case of many receivers. The objective of telecloning is to distribute one input state to many distant receivers. However, the no-cloning theorem [20] prohibits making multiple perfect copies of a single unknown state. The best a sender can do is to transfer an *optimal clone* that is the closest to the original state allowed by quantum mechanics. In the following, we will focus on symmetric cloning, i.e., the situation where there is no difference between the copies that each recipient receives.

The $K \to M$ optimal cloning map $\mathcal{C} : \mathcal{L}(\mathcal{H}^{\otimes K}) \to \mathcal{L}(\mathcal{H}^{\otimes M})$ given by Werner [23] is obtained by projecting K input copies and $M-K$ completely mixed states onto a symmetric subspace:

$$\mathcal{C}(|\phi\rangle\langle\phi|^{\otimes K}) = \frac{d[K]}{d[M]}\Pi_M(|\phi\rangle\langle\phi|^{\otimes K} \otimes \mathbb{1}^{\otimes M-K})\Pi_M, \quad (10)$$

where $d[K] = \binom{d+K-1}{K}$ and Π_M is the projection onto the totally symmetric subspace of $\mathcal{H}^{\otimes M}$. The state in (10) also optimizes the fidelity of each clone [27], which is written as follows:

$$\mathcal{R} \circ \mathcal{C}(|\phi\rangle\langle\phi|^{\otimes K}) = \gamma_{K,M}|\phi\rangle\langle\phi| + (1-\gamma_{K,M})\frac{1}{d}\mathbb{1}, \quad (11)$$

where $\gamma_{K,M} = \frac{K}{M}\frac{M+d}{K+d}$ and $\mathcal{R}$ represents the trace over all subsystems except the first one (due to exchange symmetry all clones are equal). Furthermore, since $\mathcal{C}$ is *universal* (i.e., the fidelity does not depend on the input pure states), the fidelity for $K = 1$ is given as follows:

$$\begin{aligned} f(\mathcal{R} \circ \mathcal{C}) &= \gamma_{1,M} + (1-\gamma_{1,M})\frac{1}{d} \\ &= \frac{d+2M-1}{M(d+1)}. \end{aligned} \quad (12)$$

There is a straightforward protocol to transfer optimal clones to many receivers. That is, Alice applies the optimal cloning map locally and transfers its output to each receiver by ST. If the number of clones is M, this protocol requires $M \log_2 d$ ebits. Unlike this "clone-and-teleport" protocol, the protocol introduced in [17,18] performs cloning and teleportation simultaneously. An advantage of this protocol is that it requires only $(\log_2 d)$-ebit entanglement between the sender and the receivers. This is achieved by using the $2M$-qudit entangled state, called a *telecloning state*, which is shared between Alice and the $2M-1$ receivers (each participant has one qudit). The protocol is as follows:

(1) Alice performs a complete d-dimensional Bell measurement on the input state and her entangled state.

(2) Alice relays the outcome to all receivers via classical communication.

(3) Each receiver applies an appropriate unitary transformation based on Alice's measurement outcome.

This completes the protocol, and M receivers obtain the optimal clone of the input state. This is possible because the universal cloning is covariant under the action of the unitary group.

III. PORT-BASED TELECLONING

A. The protocol

In this section, we introduce PBTC, which performs telecloning using PBT. The goal of PBTC is to distribute M copies of the state of the input system across N ports in one go. In particular, we consider a symmetric cloning scenario, i.e., all copies should look the same locally.

In PBTC, we use a POVM whose outcomes specify a subset of all ports available: The ports contained in such a subset will receive a copy of the input state, whereas the remaining ports will be discarded. The set of measurement outcomes is defined as follows.

Definition 1. For fixed N and M ($N \geqslant M$), we define the set

$$\begin{aligned} \mathcal{I}_N^M := \{\{i_1, \dots, i_M\} \mid i_k \in \{1, \dots, N\} \text{ for } k \in \{1, \dots, M\}, \\ \text{and } i_1 < \dots < i_M\}. \end{aligned} \quad (13)$$

Here, $|\mathcal{I}_N^M| = \binom{N}{M}$. For $I = \{i_1, \dots, i_M\} \in \mathcal{I}_N^M$, we write the composite system $A_I \equiv A_{i_1} \cdots A_{i_M}$ and $A_I^c \equiv A^N \setminus A_I$.

The right side of Fig. 1 represents PBTC. In PBTC, Alice and N receivers share a resource state $\Phi_{A^N B^N}$. We consider Alice to have ports $A_1, \dots, A_N$, and the ith receiver has port B_i ($i = 1, \dots, N$). Additionally, Alice holds the input state σ_X. The protocol of PBTC is as follows:

(1) Alice measures the input system X and all her ports A^N with a POVM $\{E^I_{XA^N}\}_{I\in\mathcal{I}_N^M}$.

(2) Alice relays the outcome $I \in \mathcal{I}_N^M$ to all receivers via classical communication.

(3) The ith receiver discards their port B_i if $i \notin I$ and does nothing if $i \in I$ ($i = 1, \dots, N$).

This completes the protocol, and the clones are transferred to the M receivers. The PBTC channel $\mathcal{D}_{N,M} : \mathcal{L}(\mathcal{H}_X) \to \mathcal{L}(\mathcal{H}^{\otimes M})$ is expressed as follows:

$$\mathcal{D}_{N,M}(\sigma_X) = \sum_{I\in\mathcal{I}_N^M} \mathrm{Tr}_{XA^N B_I^c}\big[E^I_{XA^N}(\sigma_X \otimes \Phi_{A^N B^N})\big], \quad (14)$$

and the remaining system B_{i_k} ($k = 1, \dots, M$) is relabeled as output system B_k.

Clone-and-teleport protocol

In Sec. II B, we described a trivial "clone-and-teleport" protocol for telecloning, and we can consider a similar protocol for PBTC. The protocol is that Alice creates an optimal M clone locally and transfers it by *multiport-based teleportation* (MPBT) [28]. For simplicity, we consider only $1 \to M$ cloning.

MPBT is the protocol that transfers M qudit states to M ports in one go. The POVM for MPBT using N pairs of maximally entangled states is given by the PGM for $\{(|\mathcal{J}_N^M|^{-1}, \rho^J_{X^M A^N})\}_{J\in\mathcal{J}_N^M}$, where

$$\begin{aligned} \mathcal{J}_N^M := \{(j_1, \dots, j_M) \mid j_k \in \{1, \dots, N\} \text{ for } k \in \{1, \dots, M\}, \\ \text{and } j_k \neq j_l \text{ for } k \neq l\} \end{aligned} \quad (15)$$

is the ordered version of $\mathcal{I}_N^M$, and for $J = (j_1, \ldots, j_M) \in \mathcal{J}_N^M$,

$$\rho^J_{X^M A^N} := \bigotimes_{k=1}^{M} \Phi^+_{X_k A_{j_k}} \otimes \frac{1}{d^{N-M}} \mathbb{1}_{A^c_J}. \tag{16}$$

We refer to the protocol that performs optimal cloning and MPBT successively as the *clone-and-MPBT protocol*. The clone-and-MPBT protocol can be considered in the framework of PBTC. The clone-and-MPBT protocol is equivalent to PBTC using the POVM

$$\left\{(\mathcal{C}^\dagger_{X^M\to X} \otimes \mathrm{id}_{A^N})\left(E^J_{X^M A^N}\right)\right\}_{J\in\mathcal{J}_N^M}, \tag{17}$$

where $\mathcal{C}^\dagger_{X^M\to X} : \mathcal{L}(\mathcal{H}^{\otimes M}_{X^M}) \to \mathcal{L}(\mathcal{H}_X)$ is the adjoint of the optimal cloning map given by (10) and $\{E^J_{X^M A^N}\}_{J\in\mathcal{J}_N^M}$ is the PGM for $\{(|\mathcal{J}_N^M|^{-1}, \rho^J_{X^M A^N})\}_{J\in\mathcal{J}_N^M}$. The set of measurement outcomes in (17) is not $\mathcal{I}_N^M$, but that poses no issue because it can be made equivalent to $\mathcal{I}_N^M$ by summing the POVM elements for outcomes that are identical when reordered. Note that since the figure of merit for (17) differs from the original PGM, it is essential to make (17) a proper POVM in the full Hilbert space. Thus, we take into account Δ, given by (6), in the clone-and-MPBT protocol.

The clone-and-MPBT protocol can transfer optimal clones in the limit of the number of ports $N \to \infty$. However, optimality for finite N is not guaranteed. In fact, the POVM we introduce in the next section achieves higher fidelity than the clone-and-MPBT protocol when N is small.

B. Generalization of POVM

As we have noted, in this work, we consider only symmetric cloning. We first introduce an ensemble for a PGM by partially symmetrizing the state $\rho^i_{XA^N}$ that constitutes the optimal POVM of PBT.

Definition 2. For $I = \{i_1, \ldots, i_M\} \in \mathcal{I}_N^M$, let

$$\eta^I_{XA^N} := \frac{d^M}{d[M]} \Pi_{A_I} \rho^{i_1}_{XA^N} \Pi_{A_I}, \tag{18}$$

where $\rho^{i_1}_{XA^N}$ is the state given by (7) and Π_{A_I} is the projection onto the symmetric subspace of $\mathcal{H}^{\otimes M}_{A_I}$.

In Eq. (18), although we formally use i_1 as the index of $\rho^{i_1}_{XA^N}$, note that $\eta^I_{XA^N}$ remains in the same state regardless of whether i_1 is replaced by any element of $I = \{i_1, \ldots, i_M\}$.

We refer to PBTC that uses N pairs of maximally entangled states and the PGM for $\{(|\mathcal{I}_N^M|^{-1}, \eta^I_{XA^N})\}_{I\in\mathcal{I}_N^M}$ as *standard* PBTC. Since standard PBTC is symmetric cloning, we evaluate its performance using an average fidelity of a single clone for all input pure states.

The asymptotic fidelity of standard PBTC is given by the following theorem.

Theorem 1. Let us consider the standard PBTC channel $\mathcal{D}^{\mathrm{std}}_{N,M}$ and the channel $\mathcal{R}$ that represents the trace over all subsystems except the first one. In the limit of the number of ports $N \to \infty$, the following equality holds:

$$\lim_{N\to\infty} f\left(\mathcal{R} \circ \mathcal{D}^{\mathrm{std}}_{N,M}\right) = \frac{d + 2M - 1}{M(d+1)}, \tag{19}$$

where d is the dimension of the local Hilbert space and M is the number of clones to be transferred.

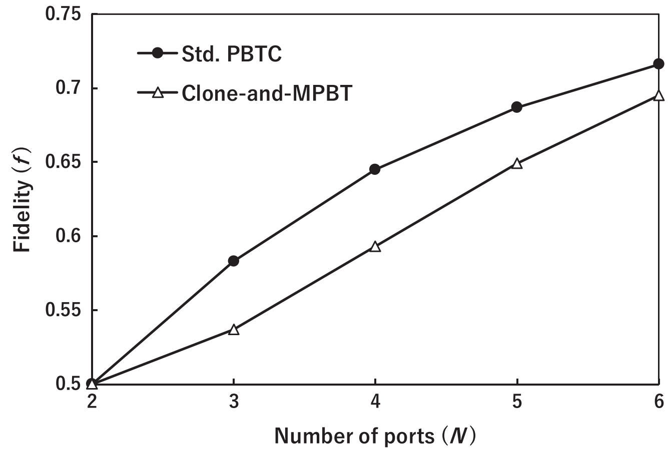


FIG. 2. The fidelity of the PBTC protocol proposed here (circles) and the trivial clone-and-MPBT protocol (triangles). The plotted values were obtained by numerical calculation for $d = 2$ and $M = 2$. Fidelity is the average over the input pure state and is calculated for a single clone.

The proof is given in Sec. III C. The value of (19) coincides with the fidelity of $1 \to M$ optimal cloning given by (12). Therefore, standard PBTC can transfer optimal clones asymptotically.

Finally, we numerically compare the performance of standard PBTC with the clone-and-MPBT protocol described in the previous section. Figure 2 shows the fidelity of each protocol obtained by numerical calculation. Fidelity is calculated for a single clone. Namely, it represents $f(\mathcal{R} \circ \mathcal{D}^{\mathrm{std}}_{N,M})$ and $f(\mathcal{R} \circ \mathcal{T}_{N,M})$, where $\mathcal{D}^{\mathrm{std}}_{N,M}$ is the standard PBTC channel and $\mathcal{T}_{N,M}$ is the quantum channel corresponding to the clone-and-MPBT protocol. Figure 2 shows that standard PBTC achieves higher fidelity than the clone-and-MPBT protocol when $d = 2$, $M = 2$, and $2 \leqslant N \leqslant 6$. Due to the increasing complexity of the calculation we were not able to go to higher values of M and N, but we conjecture that a finite gap exists for all finite values. This problem could potentially be gotten rid of by exploiting the proper representation theory approach given in [14,28].

C. Proof of Theorem 1

In this section, we prove Theorem 1. Within this section, we use the same notation for operators in systems $A^N B$ as we did for operators in systems XA^N in the previous sections via the isomorphism $X \cong B$. For example, for $\rho^i_{XA^N} = \Phi^+_{XA_i} \otimes \frac{1}{d^{N-1}} \mathbb{1}_{A^c_i}$ defined in (7), we have $\rho^i_{A^N B} = \Phi^+_{A_i B} \otimes \frac{1}{d^{N-1}} \mathbb{1}_{A^c_i}$.

We start by showing the properties related to the symmetric group.

Definition 3. Let S_N be the symmetric group in $\{1, \ldots, N\}$, and for $I \in \mathcal{I}_N^M$, let S_I be the subgroup of S_N consisting of all permutations of $I = \{i_1, \ldots, i_M\}$. For $\sigma \in S_N$, the action of the unitary representation $V_\sigma \in \mathcal{L}(\mathcal{H}^{\otimes N})$ is defined follows:

$$V_\sigma \left|k_1 \cdots k_N\right\rangle := \left|k_{\sigma^{-1}(1)} \cdots k_{\sigma^{-1}(N)}\right\rangle. \tag{20}$$

In addition, for $I \in \mathcal{I}_N^M$, let Π_{A_I} be the projection onto the symmetric subspace of $\mathcal{H}_{A_I}^{\otimes M}$ as follows:

$$\Pi_{A_I} := \frac{1}{M!} \sum_{\sigma \in S_I} V_\sigma. \tag{21}$$

Note that although Π_{A_I} defined in (21) is an operator on $\mathcal{H}_{A^N}^{\otimes N}$, it acts nontrivially only on $\mathcal{H}_{A_I}^{\otimes M}$.

Lemma 1. For any $\sigma \in S_N$ and $I \in \mathcal{I}_N^M$, $\sigma S_I \sigma^{-1} = S_{\sigma(I)}$.

Proof. First, if $\tau \in \sigma S_I \sigma^{-1}$, a $\pi \in S_I$ such that $\tau = \sigma\pi\sigma^{-1}$ exists. Since $\sigma\pi\sigma^{-1}$ is a bijection on $\sigma(I)$, τ is a permutation of $\sigma(I)$. Thus, $\sigma S_I \sigma^{-1} \subset S_{\sigma(I)}$. Next, suppose $\tau \in S_{\sigma(I)}$. In this case, $\sigma^{-1}\tau\sigma$ is a bijection on I. Therefore, a $\pi \in S_I$ such that $\sigma^{-1}\tau\sigma = \pi$ exists. Since $\tau = \sigma\pi\sigma^{-1}$ and $\sigma\pi\sigma^{-1} \in \sigma S_I \sigma^{-1}$, we have $\tau \in \sigma S_I \sigma^{-1}$. Therefore, $S_{\sigma(I)} \subset \sigma S_I \sigma^{-1}$. ■

Corollary 1. For any $\sigma \in S_N$ and $I \in \mathcal{I}_N^M$, $V_\sigma \Pi_{A_I} V_\sigma^\dagger = \Pi_{A_{\sigma(I)}}$.

Proof. From Lemma 1, we have

$$\sum_{\tau \in S_I} V_{\sigma\tau\sigma^{-1}} = \sum_{\pi \in S_{\sigma(I)}} V_\pi. \tag{22}$$

Since $V_{\sigma\pi} = V_\sigma V_\pi$ and $V_{\sigma^{-1}} = V_\sigma^\dagger$ for any $\sigma, \pi \in S_N$, the lemma holds. ■

Proposition 1. Let $\{E_{A^N B}^I\}_{I \in \mathcal{I}_N^M}$ be the PGM for $\{(|\mathcal{I}_N^M|^{-1}, \eta_{A^N B}^I)\}_{I \in \mathcal{I}_N^M}$. For any $I = \{i_1, \ldots, i_M\} \in \mathcal{I}_N^M$, it holds that $\Pi_{A_I} E_{A^N B}^I \Pi_{A_I} = E_{A^N B}^I$.

Proof. Let us denote

$$\bar{\eta}_{A^N B} = \binom{N}{M}^{-1} \sum_{I \in \mathcal{I}_N^M} \eta_{A^N B}^I. \tag{23}$$

For any $\sigma \in S_N$, we have

$$\begin{aligned} V_\sigma \bar{\eta}_{A^N B} &= \binom{N}{M}^{-1} \frac{d^M}{d[M]} \sum_{I \in \mathcal{I}_N^M} V_\sigma \Pi_{A_I} \rho_{A^N B}^{i_1} \Pi_{A_I} \\ &= \binom{N}{M}^{-1} \frac{d^M}{d[M]} \sum_{I \in \mathcal{I}_N^M} V_\sigma \Pi_{A_I} V_\sigma^\dagger V_\sigma \rho_{A^N B}^{i_1} V_\sigma^\dagger V_\sigma \Pi_{A_I} V_\sigma^\dagger V_\sigma \\ &= \binom{N}{M}^{-1} \frac{d^M}{d[M]} \sum_{I \in \mathcal{I}_N^M} \Pi_{A_{\sigma(I)}} \rho_{A^N B}^{\sigma(i_1)} \Pi_{A_{\sigma(I)}} V_\sigma \\ &= \bar{\eta}_{A^N B} V_\sigma. \end{aligned} \tag{24}$$

The second equality uses $V_\sigma^{-1} = V_\sigma^\dagger$, and the third equality uses $V_\sigma \rho_{A^N B}^{i_1} V_\sigma^\dagger = \rho_{A^N B}^{\sigma(i_1)}$ and Corollary 1. Note that from the symmetry $\binom{N}{M}^{-1} \frac{d^M}{d[M]} \sum_{I \in \mathcal{I}_N^M} \Pi_{A_{\sigma(I)}} \rho_{A^N B}^{\sigma(i_1)} \Pi_{A_{\sigma(I)}} = \bar{\eta}_{A^N B}$ holds. By summing both sides with respect to $\sigma \in S_I$ and dividing by $M!$, we obtain

$$\Pi_{A_I} \bar{\eta}_{A^N B} = \bar{\eta}_{A^N B} \Pi_{A_I}. \tag{25}$$

Since $\bar{\eta}_{A^N B}^{-1}$ is defined on the support of $\bar{\eta}_{A^N B}$, $[\Pi_{A_I}, \bar{\eta}_{A^N B}^{-\frac{1}{2}}] = 0$ also holds. Therefore,

$$\begin{aligned} \Pi_{A_I} E_{A^N B}^I \Pi_{A_I} &= \Pi_{A_I} \bar{\eta}_{A^N B}^{-\frac{1}{2}} \left(\frac{d^M}{d[M]} \Pi_{A_I} \rho_{A^N B}^{i_1} \Pi_{A_I} \right) \bar{\eta}_{A^N B}^{-\frac{1}{2}} \Pi_{A_I} \\ &= \bar{\eta}_{A^N B}^{-\frac{1}{2}} \left(\frac{d^M}{d[M]} \Pi_{A_I} \rho_{A^N B}^{i_1} \Pi_{A_I} \right) \bar{\eta}_{A^N B}^{-\frac{1}{2}} \\ &= E_{A^N B}^I. \end{aligned} \tag{26}$$

■

We then calculate the entanglement fidelity. The following lemma connects the entanglement fidelity of PBT with the state-discrimination problem.

Lemma 2. Let us fix the resource state to be N pairs of maximally entangled states [4,6]. The entanglement fidelity of the PBT channel $\mathcal{E}_N$ using the POVM $\{E_{XA^N}^i\}_{i=1}^N$ is given by

$$F(\mathcal{E}_N) = \frac{1}{d^2} \sum_{i=1}^N \mathrm{Tr}\big[E_{A^N B}^i \rho_{A^N B}^i\big]. \tag{27}$$

By applying this lemma for standard PBTC, we obtain the following corollary.

Corollary 2. Let us consider the standard PBTC channel $\mathcal{D}_{N,M}^{\mathrm{std}}$ and quantum channel $\mathcal{R}$ that traces over all subsystems except the first one. The entanglement fidelity of the quantum channel $\mathcal{R} \circ \mathcal{D}_{N,M}^{\mathrm{std}}$ is given by

$$F\big(\mathcal{R} \circ \mathcal{D}_{N,M}^{\mathrm{std}}\big) = \frac{1}{d^2} \sum_{I \in \mathcal{I}_N^M} \mathrm{Tr}\big[E_{A^N B}^I \rho_{A^N B}^{i_1}\big], \tag{28}$$

where i_1 is the smallest number of I and $\{E_{XA^N}^I\}_{I \in \mathcal{I}_N^M}$ is the PGM for $\{(|\mathcal{I}_N^M|^{-1}, \eta_{A^N B}^I)\}_{I \in \mathcal{I}_N^M}$.

The following lemma provides the lower bound of the success probability for the state-discrimination problem of PGM. It is proportional to the entanglement fidelity, as expressed by Lemma 2.

Lemma 3. [6] Let $\{E^i\}_{i=1}^N$ be the PGM for any state ensemble $\{(1/N, \sigma^i)\}_{i=1}^N$. Then, the success probability for the state-discrimination problem

$$p_{\mathrm{succ}} = \frac{1}{N} \sum_{i=1}^N \mathrm{Tr}[E^i \sigma^i] \tag{29}$$

satisfies the following inequality:

$$p_{\mathrm{succ}} \geqslant \frac{1}{N \bar{r} \mathrm{Tr} \bar{\sigma}^2}, \tag{30}$$

where

$$\bar{r} = \frac{1}{N} \sum_{i=1}^N \mathrm{rank} \sigma^i, \quad \bar{\sigma} = \frac{1}{N} \sum_{i=1}^N \sigma^i. \tag{31}$$

To utilize Lemma 3, we calculate the values of (31) for the state ensemble $\{(|\mathcal{I}_N^M|^{-1}, \eta_{XA^N}^I)\}_{I \in \mathcal{I}_N^M}$. The average rank is given by the following proposition.

Proposition 2. $\binom{N}{M}^{-1} \sum_{I \in \mathcal{I}_N^M} \mathrm{rank} \eta_{A^N B}^I = d[M-1] d^{N-M}$.

Proof. For any $I = \{i_1, \ldots, i_M\} \in \mathcal{I}_N^M$, we have

$$\eta_{A^N B}^I = \frac{d^{M-N+1}}{d[M]} \Pi_{A_I} (\Phi_{A_{i_1} B}^+ \otimes \mathbb{1}_{A_I \setminus A_{i_1}}) \Pi_{A_I} \otimes \mathbb{1}_{A_I^c}. \tag{32}$$

The set W of eigenvectors corresponding to the nonzero eigenvalues of $\Pi_{A_I}(\Phi^+_{A_{i_1}B}\otimes \mathbb{1}_{A_I\setminus A_{i_1}})\Pi_{A_I}$ is

$$W=\{\Pi_{A_I}|\Phi^+\rangle_{A_{i_1}B}|k_1\cdots k_{M-1}\rangle_{A_I\setminus A_{i_1}}\}^d_{k_1,\dots,k_{M-1}=1},\tag{33}$$

where $\{|k\rangle\}_{k=1}^d$ is the orthonormal basis of $\mathcal{H}$. Since $\operatorname{rank}\mathbb{1}_{A_I^c}=d^{N-M}$, it is sufficient to show $|W|=d[M-1]$. Here,

$$\begin{aligned}\Pi_{A_I}&|\Phi^+\rangle_{A_{i_1}B}|k_1\cdots k_{M-1}\rangle_{A_I\setminus A_{i_1}}\\&=\frac{1}{\sqrt{d}}\sum_{i=1}^d\Pi_{A_I}|i\,k_1\cdots k_{M-1}\rangle_{A_I}|i\rangle_B.\end{aligned}\tag{34}$$

Thus,

$$\begin{aligned}\Pi_{A_I}&|\Phi^+\rangle_{A_{i_1}B}|k_1\cdots k_{M-1}\rangle_{A_I\setminus A_{i_1}}\\&=\Pi_{A_I}|\Phi^+\rangle_{A_{i_1}B}|l_1\cdots l_{M-1}\rangle_{A_I\setminus A_{i_1}}\end{aligned}\tag{35}$$

holds for $k_1,\dots,k_{M-1},l_1,\dots,l_{M-1}\in\{1,\dots d\}$ if and only if

$$\Pi_{A_I}|i\,k_1\cdots k_{M-1}\rangle_{A_I}=\Pi_{A_I}|i\,l_1\cdots l_{M-1}\rangle_{A_I}\tag{36}$$

holds for each $i\in\{1,\dots,d\}$. Equation (36) holds if and only if $k_1,\dots,k_{M-1}$ and $l_1,\dots,l_{M-1}$ match after permutation. Thus, $|W|$ equals the number of combinations with repetition of selecting $M-1$ elements from $\{1,\dots,d\}$. Hence, $|W|=d[M-1]$. ■

Next, we estimate $\operatorname{Tr}\bar{\eta}^2_{A^NB}$.

Lemma 4. Let $I,J,K,L\in\mathcal{I}_N^M$. If $|I\cap J|=|K\cap L|$, then $\operatorname{Tr}[\eta^I_{A^NB}\eta^J_{A^NB}]=\operatorname{Tr}[\eta^K_{A^NB}\eta^L_{A^NB}]$.

Proof. For any $\sigma\in S_N$ and $I=\{i_1,\dots,i_M\}\in\mathcal{I}_N^M$, we have

$$\begin{aligned}\eta^I_{A^NB}&=\frac{d^M}{d[M]}\Pi_{A_I}\rho^{i_1}_{A^NB}\Pi_{A_I}\\&=\frac{d^M}{d[M]}V_\sigma^\dagger V_\sigma\Pi_{A_I}V_\sigma^\dagger V_\sigma\rho^{i_1}_{A^NB}V_\sigma^\dagger V_\sigma\Pi_{A_I}V_\sigma^\dagger V_\sigma\\&=\frac{d^M}{d[M]}V_\sigma^\dagger\Pi_{A_{\sigma(I)}}\rho^{\sigma(i_1)}_{A^NB}\Pi_{A_{\sigma(I)}}V_\sigma\\&=V_\sigma^\dagger\eta^{\sigma(I)}_{A^NB}V_\sigma.\end{aligned}\tag{37}$$

The second equality uses $V_\sigma^{-1}=V_\sigma^\dagger$, and the third equality uses $V_\sigma\rho^{i_1}_{A^NB}V_\sigma^\dagger=\rho^{\sigma(i_1)}_{A^NB}$ and Corollary 1. Therefore, for any $\sigma\in S_N$ and $I,J\in\mathcal{I}_N^M$, we obtain

$$\begin{aligned}\operatorname{Tr}\big[\eta^I_{A^NB}\eta^J_{A^NB}\big]&=\operatorname{Tr}\big[\big(V_\sigma^\dagger\eta^{\sigma(I)}_{A^NB}V_\sigma\big)\big(V_\sigma^\dagger\eta^{\sigma(J)}_{A^NB}V_\sigma\big)\big]\\&=\operatorname{Tr}\big[\eta^{\sigma(I)}_{A^NB}\eta^{\sigma(J)}_{A^NB}\big].\end{aligned}\tag{38}$$

Note that $|I\cap J|=|\sigma(I)\cap\sigma(J)|$. Moreover, for any $K,L\in\mathcal{I}_N^M$ satisfying $|I\cap J|=|K\cap L|$, a $\sigma\in S_N$ such that $\sigma(I)=K$ and $\sigma(J)=L$ exists. Thus, the proposition is proved. ■

Lemma 5. For any $I,J\in\mathcal{I}_N^M$, it holds that $\operatorname{Tr}[\eta^I_{A^NB}\eta^J_{A^NB}]\leqslant\operatorname{Tr}[(\eta^I_{A^NB})^2]$.

Proof. Applying the Cauchy-Schwarz inequality to the Hilbert-Schmidt inner product, we have

$$\big|\operatorname{Tr}[A^\dagger B]\big|\leqslant\sqrt{\operatorname{Tr}[A^\dagger A]}\sqrt{\operatorname{Tr}[B^\dagger B]}\tag{39}$$

for any $A,B\in\mathcal{L}(\mathcal{H}^{\otimes N+1})$. By setting $A=\eta^I_{A^NB}$ and $B=V_\sigma\eta^I_{A^NB}V_\sigma^\dagger=\eta^{\sigma(I)}_{A^NB}$ for $\sigma\in S_N$, the left-hand side can be written as

$$\big|\operatorname{Tr}\big[\eta^I_{A^NB}\eta^{\sigma(I)}_{A^NB}\big]\big|=\operatorname{Tr}\big[\eta^I_{A^NB}\eta^{\sigma(I)}_{A^NB}\big],\tag{40}$$

while the right-hand side becomes

$$\begin{aligned}&\sqrt{\operatorname{Tr}\big[\eta^I_{A^NB}\eta^I_{A^NB}\big]}\sqrt{\operatorname{Tr}\big[\big(V_\sigma\eta^I_{A^NB}V_\sigma^\dagger\big)\big(V_\sigma\eta^I_{A^NB}V_\sigma^\dagger\big)\big]}\\&\quad=\operatorname{Tr}\Big[\big(\eta^I_{A^NB}\big)^2\Big].\end{aligned}\tag{41}$$

Since $\sigma\in S_N$ is arbitrary, $J=\sigma(I)$ is arbitrary. ■

Lemma 6. For any $I\in\mathcal{I}_N^M$, the following inequality holds:

$$\operatorname{Tr}\Big[\big(\eta^I_{A^NB}\big)^2\Big]\leqslant\frac{d^{M-N+2}}{d[M]}\frac{M!(M-1)!}{d+M-1}.\tag{42}$$

Proof. From the arguments made in the proof of Proposition 2, $\eta^I_{A^NB}$ has $d[M-1]d^{N-M}$ nonzero eigenvalues, and its eigenvectors are given in the form

$$\Pi_{A_I}|\Phi^+\rangle_{A_{i_1}B}|k_1\cdots k_{M-1}\rangle_{A_I\setminus A_{i_1}}|k_M\cdots k_{N-1}\rangle_{A_I^c},\tag{43}$$

where $k_1,\dots,k_{N-1}\in\{1,\dots,d\}$ and $\{|k\rangle\}_{k=1}^d$ is the orthonormal basis of $\mathcal{H}$. If there are n different permutations to rearrange $k_1,\dots,k_{M-1}$ without distinguishing the same numbers, the eigenvalue corresponding to (43) is $n\frac{d^{M-N+1}}{d[M]}$. Since $n\leqslant(M-1)!$ always holds, all $d[M-1]d^{N-M}$ nonzero eigenvalues are less than or equal to $(M-1)!\frac{d^{M-N+1}}{d[M]}$. Hence,

$$\begin{aligned}\operatorname{Tr}\Big[\big(\eta^I_{A^NB}\big)^2\Big]&\leqslant d[M-1]d^{N-M}\bigg((M-1)!\frac{d^{M-N+1}}{d[M]}\bigg)^2\\&=\frac{d^{M-N+2}}{d[M]}\frac{M!(M-1)!}{d+M-1}.\end{aligned}\tag{44}$$

■

Lemma 7. Let $I,J\in\mathcal{I}_N^M$. If $I\cap J=\emptyset$, then $\operatorname{Tr}[\eta^I_{A^NB}\eta^J_{A^NB}]=1/d^{N+1}$.

Proof. Suppose $I=\{i_1,\dots,i_M\}$ and $J=\{j_1,\dots,j_M\}$. When $I\cap J=\emptyset$, we have

$$[\Pi_{A_I},\Pi_{A_J}]=\big[\Pi_{A_I},\rho^{j_1}_{A^NB}\big]=\big[\Pi_{A_J},\rho^{i_1}_{A^NB}\big]=0.\tag{45}$$

Thus,

$$\operatorname{Tr}\big[\eta^I_{A^NB}\eta^J_{A^NB}\big]=\frac{d^{2M}}{(d[M])^2}\operatorname{Tr}\big[\Pi_{A_I}\rho^{i_1}_{A^NB}\Pi_{A_J}\rho^{j_1}_{A^NB}\big].\tag{46}$$

Therefore, with some calculations we obtain

$$\begin{aligned}\operatorname{Tr}\big[\eta^I_{A^NB}\eta^J_{A^NB}\big]&=\frac{1}{(d[M]M!)^2d^N}\sum_{\sigma\in S_I}\sum_{\tau\in S_J}\sum_{k_{i_1},\dots,k_{i_M}=1}^d\sum_{l_{j_1},\dots,l_{j_M}=1}^d\\&\quad\times\delta_{l_{j_1},k_{\sigma^{-1}(i_1)}}\delta_{k_{i_1},l_{\tau^{-1}(j_1)}}\prod_{p=2}^M\delta_{k_{i_p},k_{\sigma^{-1}(i_p)}}\delta_{l_{j_p},l_{\tau^{-1}(j_p)}}.\end{aligned}\tag{47}$$

For a detailed derivation of (47), see the Appendix. To calculate (47), we decompose σ and τ into cycles. Suppose $\sigma\in S_I$ can be decomposed into $\sigma=C_1^\sigma C_2^\sigma\cdots C_{l(\sigma)}^\sigma$ (including cycles with a single element), and let c_m^σ represent the length of the cycle C_m^σ (with similar notation for $\tau \in S_J$). Then, by definition,

$$\sum_{m=1}^{l(\sigma)} c_m^\sigma = \sum_{m=1}^{l(\tau)} c_m^\tau = M. \tag{48}$$

Furthermore, we denote the elements of the cycle as $C_m^\sigma = (i_1^m \ \cdots \ i_{c_i^\sigma}^m)$ and $C_m^\tau = (j_1^m \ \cdots \ j_{c_j^\tau}^m)$. Without loss of generality, let $i_1 = i_1^1$ and $j_1 = j_1^1$. When $c_1^\sigma \neq 1$ and $c_1^\tau \neq 1$, each summand in (47) can be expressed as follows:

$$\begin{aligned}&\delta_{l_{j_1},k_{\sigma^{-1}(i_1)}}\delta_{k_{i_1},l_{\tau^{-1}(j_1)}}\prod_{p=2}^{M}\delta_{k_{i_p},k_{\sigma^{-1}(i_p)}}\delta_{l_{j_p},j_{\tau^{-1}(j_p)}}\\&=\left(\delta_{l_{j_1^1},k_{\sigma^{-1}(i_1^1)}}\delta_{k_{i_1^1},l_{\tau^{-1}(j_1^1)}}\prod_{p=2}^{c_1^\sigma}\delta_{k_{i_p^1},k_{\sigma^{-1}(i_p^1)}}\prod_{q=2}^{c_1^\tau}\delta_{l_{j_q^1},l_{\tau^{-1}(j_q^1)}}\right)\\&\quad\times\left(\prod_{m=2}^{l(\sigma)}\prod_{n=1}^{c_m^\sigma}\delta_{k_{i_n^m},k_{\sigma^{-1}(i_n^m)}}\right)\left(\prod_{s=2}^{l(\tau)}\prod_{t=1}^{c_s^\tau}\delta_{l_{j_t^s},l_{\tau^{-1}(j_t^s)}}\right).\end{aligned} \tag{49}$$

When $c_1^\sigma = 1$ or $c_1^\tau = 1$, $\prod_{p=2}^{c_1^\sigma}\delta_{k_{i_p^1},k_{\sigma^{-1}(i_p^1)}}$ or $\prod_{q=2}^{c_1^\tau}\delta_{l_{j_q^1},l_{\tau^{-1}(j_q^1)}}$ in (49) is disregarded, respectively. The right-hand side of (49) corresponds to cycles C_1^σ and C_1^τ in the first parentheses, $C_2^\sigma, \dots, C_{l(\sigma)}^\sigma$ in the second parentheses, and $C_2^\tau, \dots, C_{l(\tau)}^\tau$ in the third parentheses. When we sum (49) over $k_{i_1}, \dots, k_{i_M}$ and $l_{j_1}, \dots, l_{j_M}$, the first parentheses eliminate $c_1^\sigma + c_1^\tau - 1$ indices. The second parentheses eliminate $c_m^\sigma - 1$ indices for fixed $m \in \{2, \dots, l(\sigma)\}$, for a total of $\sum_{m=2}^{l(\sigma)}(c_m^\sigma - 1)$ indices. Similarly, the third parentheses eliminate $\sum_{s=2}^{l(\tau)}(c_s^\tau - 1)$ indices. Consequently, the total number of eliminated indices for fixed $\sigma \in S_I, \tau \in S_J$ is

$$\begin{aligned}&\left(c_1^\sigma + c_1^\tau - 1\right) + \sum_{m=2}^{l(\sigma)}\left(c_m^\sigma - 1\right) + \sum_{s=2}^{l(\tau)}\left(c_s^\tau - 1\right)\\&= \sum_{k=1}^{l(\sigma)} c_k^\sigma + \sum_{k=1}^{l(\tau)} c_k^\tau - 1 - [l(\sigma) - 1] - [l(\tau) - 1]\\&= 2M + 1 - l(\sigma) - l(\tau).\end{aligned} \tag{50}$$

Since there were $2M$ indices of $k_{i_1}, \dots, k_{i_M}$ and $l_{j_1}, \dots, l_{j_M}$ at the beginning, the remaining indices are

$$2M - [2M + 1 - l(\sigma) - l(\tau)] = l(\sigma) + l(\tau) - 1. \tag{51}$$

Hence,

$$\begin{aligned}&\sum_{k_{i_1},\dots,k_{i_M}=1}^{d}\ \sum_{l_{j_1},\dots,l_{j_M}=1}^{d}\delta_{l_{j_1},k_{\sigma^{-1}(i_1)}}\delta_{k_{i_1},l_{\tau^{-1}(j_1)}}\\&\quad\times\prod_{p=2}^{M}\delta_{k_{i_p},k_{\sigma^{-1}(i_p)}}\delta_{l_{j_p},l_{\tau^{-1}(j_p)}} = d^{l(\sigma)+l(\tau)-1}.\end{aligned} \tag{52}$$

Here, the number of $\sigma \in S_M$ satisfying $l(\sigma) = k$ is given by the first kind of Stirling number $\left[{M \atop k}\right]$ (see Remark 1 for details). Therefore,

$$\begin{aligned}\sum_{\sigma\in S_I}\sum_{\tau\in S_J} d^{l(\sigma)+l(\tau)-1} &= \left(\sum_{\sigma\in S_I} d^{l(\sigma)}\right)\left(\sum_{\tau\in S_J} d^{l(\tau)}\right)d^{-1}\\&= \left(\sum_{k=1}^{M}\left[{M \atop k}\right]d^k\right)^2 d^{-1}\\&= \frac{1}{d}\left(\frac{(M+d-1)!}{(d-1)!}\right)^2.\end{aligned} \tag{53}$$

Thus,

$$\begin{aligned}\mathrm{Tr}\left[\eta_{A^N B}^I \eta_{A^N B}^J\right] &= \frac{1}{(d[M]M!)^2 d^N}\frac{1}{d}\left(\frac{(M+d-1)!}{(d-1)!}\right)^2\\&= \frac{1}{d^{N+1}}.\end{aligned} \tag{54}$$

■

Remark 1. The first kind of Stirling number $\left[{n \atop k}\right]$ is defined as the coefficient of x^k in the expansion of the rising factorial

$$x^{\bar{n}} := x(x+1)\cdots(x+n-1) \tag{55}$$

as a power series in x:

$$x^{\bar{n}} = \sum_{k=0}^{n}\left[{n \atop k}\right]x^k. \tag{56}$$

It is known that $\left[{n \atop k}\right]$ gives the number of ways to decompose a set of n elements into k cycles. The following relationship was used in (53):

$$\begin{aligned}\sum_{k=0}^{M}\left[{M \atop k}\right]d^k &= d^{\bar{M}} = d(d+1)\cdots(d+M-1)\\&= \frac{(M+d-1)!}{(d-1)!}.\end{aligned} \tag{57}$$

Proposition 3. For $\bar{\eta}_{A^N B} = \binom{N}{M}^{-1}\sum_{I\in\mathcal{I}_N^M}\eta_{A^N B}^I$, the following holds:

$$\lim_{N\to\infty} d^{N+1}\mathrm{Tr}\left[\bar{\eta}_{A^N B}^2\right] = 1. \tag{58}$$

Proof. Let $m(k)$ $(0 \leqslant k \leqslant M)$ be the number of pairs (I, J) $(I, J \in \mathcal{I}_N^M)$ that satisfy $|I \cap J| = k$, and let $f(k) = \mathrm{Tr}[\eta_{A^N B}^I \eta_{A^N B}^J]$ when $|I \cap J| = k$. Note from Lemma 4 that $f(k)$ depends only on k. Then,

$$\begin{aligned}&d^{N+1}\mathrm{Tr}\left[\bar{\eta}_{A^N B}^2\right]\\&= d^{N+1}\binom{N}{M}^{-2}\sum_{I,J\in\mathcal{I}_N^M}\mathrm{Tr}\left[\eta_{A^N B}^I\eta_{A^N B}^J\right]\\&= d^{N+1}\binom{N}{M}^{-2}\sum_{k=0}^{M} m(k)f(k)\\&\leqslant d^{N+1}\binom{N}{M}^{-2}\left[m(0)f(0) + \left(\sum_{k=1}^{M} m(k)\right)f(M)\right]\\&= d^{N+1}\left\{\binom{N-M}{M}\binom{N}{M}^{-1}f(0)\right.\\&\quad\left.+\left[1 - \binom{N-M}{M}\binom{N}{M}^{-1}\right]f(M)\right\}\end{aligned}$$

$$\leqslant d^{N+1}\left\{\binom{N-M}{M}\binom{N}{M}^{-1}\frac{1}{d^{N+1}} + \left[1-\binom{N-M}{M}\binom{N}{M}^{-1}\right]\frac{d^{M-N+2}}{d[M]}\frac{M!(M-1)!}{d+M-1}\right\}$$

$$= \binom{N-M}{M}\binom{N}{M}^{-1} + \left[1-\binom{N-M}{M}\binom{N}{M}^{-1}\right] \times \frac{d^{M+3}}{d[M]}\frac{M!(M-1)!}{d+M-1}. \tag{59}$$

The first inequality uses Lemma 5, and the second inequality uses Lemmas 6 and 7. Since

$$\lim_{N\to\infty}\binom{N-M}{M}\binom{N}{M}^{-1} = 1 \tag{60}$$

holds for finite M, we obtain

$$\lim_{N\to\infty}\left|d^{N+1}\mathrm{Tr}\left[\bar{\eta}_{A^N B}^2\right]-1\right| = 0. \tag{61}$$

■

Finally, we prove Theorem 1.

Proof of Theorem 1. Let $\{E^I_{XA^N}\}_{I\in\mathcal{I}_N^M}$ be the PGM for $\{(|\mathcal{I}_N^M|^{-1}, \eta^I_{A^N B})\}_{I\in\mathcal{I}_N^M}$. From Proposition 1, the following holds:

$$p_{\mathrm{succ}} := \binom{N}{M}^{-1}\sum_{I\in\mathcal{I}_N^M}\mathrm{Tr}\left[E^I_{A^N B}\eta^I_{A^N B}\right] = \binom{N}{M}^{-1}\frac{d^M}{d[M]}\sum_{I\in\mathcal{I}_N^M}\mathrm{Tr}\left[E^I_{A^N B}\rho^{i_1}_{A^N B}\right]. \tag{62}$$

Thus, we obtain

$$\sum_{I\in\mathcal{I}_N^M}\mathrm{Tr}\left[E^I_{A^N B}\rho^{i_1}_{A^N B}\right] = \frac{d[M]}{d^M}\binom{N}{M}p_{\mathrm{succ}}. \tag{63}$$

Therefore,

$$\begin{aligned} F\left(\mathcal{R}\circ\mathcal{D}^{\mathrm{std}}_{N,M}\right) &= \frac{1}{d^2}\sum_{I\in\mathcal{I}_N^M}\mathrm{Tr}\left[E^I_{A^N B}\rho^{i_1}_{A^N B}\right] \\ &= \frac{1}{d^2}\frac{d[M]}{d^M}\binom{N}{M}p_{\mathrm{succ}} \\ &\geqslant \frac{d[M]}{d^{M+2}}\binom{N}{M}\binom{N}{M}^{-1}\frac{1}{d[M-1]d^{N-M}}\frac{1}{\mathrm{Tr}\left[\bar{\eta}^2_{A^N B}\right]} \\ &= \frac{d+M-1}{dM}\frac{1}{d^{N+1}\mathrm{Tr}\left[\bar{\eta}^2_{A^N B}\right]}. \end{aligned} \tag{64}$$

The first equality uses Corollary 2, and the first inequality uses Lemma 3 and Proposition 2. From Proposition 3,

$$\lim_{N\to\infty}F\left(\mathcal{R}\circ\mathcal{D}^{\mathrm{std}}_{N,M}\right) \geqslant \frac{d+M-1}{dM}. \tag{65}$$

Thus, from (4),

$$\lim_{N\to\infty}f\left(\mathcal{R}\circ\mathcal{D}^{\mathrm{std}}_{N,M}\right) \geqslant \frac{d+2M-1}{M(d+1)}. \tag{66}$$

On the other hand, since the fidelity of symmetric cloning is upper bounded by (12), the equality holds. ■

IV. CONCLUSION

In this paper, we introduced port-based telecloning, a variant of telecloning that uses PBT instead of conventional teleportation. To achieve this, we constructed a new POVM by partially symmetrizing the state that constitutes the optimal POVM for PBT. We then demonstrated that the PBTC protocol we constructed can asymptotically distribute optimal clones to many receivers. Furthermore, numerical calculations showed that, at least in the case of few ports, PBTC outperforms the naive clone-and-teleport protocol.

There are several open questions about PBTC. The first is finding an optimal POVM for PBTC with finite N. We showed that the POVM we introduced achieves an optimal value in the limit $N \to \infty$, but its optimality for finite N has not been clarified. In previous research [9,10,12], the optimal POVM in PBT was derived using semidefinite programming and representation theory. Since PBTC additionally requires the condition to be a symmetric cloning, the proof done in PBT cannot be directly applied to PBTC, but it is expected that a similar method can be used. In addition, since the results of this study were obtained for the maximally entangled resource states, the optimization of a resource state can also be considered. It could increase the efficiency of PBTC since in the optimized PBT we have a square improvement of fidelity in N. Also, we considered only the deterministic PBTC, but the study of a probabilistic version presents an additional challenge. Regarding the numerical study, it would be interesting to verify whether the performance gap between our PBTC and the naive version persists for larger numbers of ports.

ACKNOWLEDGMENTS

We thank S. Strelchuk for helpful comments. K.K. acknowledges support from JSPS Grant-in-Aid for Early-Career Scientists No. 22K13972 and from MEXT-JSPS Grant-in-Aid for Transformative Research Areas (B) No. 24H00829. F.B. acknowledges support from MEXT Quantum Leap Flagship Program (MEXT QLEAP) Grant No. JPMXS0120319794, from MEXT-JSPS Grant-in-Aid for Transformative Research Areas (A) "Extreme Universe" Grant No. 21H05183, and from JSPS KAKENHI Grant No. 23K03230.

DATA AVAILABILITY

No data were created or analyzed in this study.

APPENDIX: DETAILED DERIVATION OF EQUATION (47)

In this Appendix, we give a detailed derivation of Eq. (47). At first, for $I \in \mathcal{I}_N^M = \{i_1, \dots, i_M\}$,

$$\begin{aligned}\Pi_{A_I}\rho^{i_1}_{A^N B} &= \frac{1}{M!d^N}\sum_{\sigma\in S_I}\sum_{k_{i_1},\dots,k_{i_M},k'_{i_1}=1}^{d} V_\sigma\, |k_{i_1}k_{i_2}\cdots k_{i_M}\rangle\langle k'_{i_1}k_{i_2}\cdots k_{i_M}|_{A_I}\otimes|k_{i_1}\rangle\langle k'_{i_1}|_B\otimes \mathbb{1}_{A^N\setminus A_I}\\ &= \frac{1}{M!d^N}\sum_{\sigma\in S_I}\sum_{k_{i_1},\dots,k_{i_M},k'_{i_1}=1}^{d} |k_{\sigma^{-1}(i_1)}k_{\sigma^{-1}(i_2)}\cdots k_{\sigma^{-1}(i_M)}\rangle\langle k'_{i_1}k_{i_2}\cdots k_{i_M}|_{A_I}\otimes|k_{i_1}\rangle\langle k'_{i_1}|_B\otimes \mathbb{1}_{A^N\setminus A_I}.\end{aligned} \tag{A1}$$

Likewise, for $J = \{j_1, \dots, j_M\} \in \mathcal{I}_N^M$,

$$\Pi_{A_J}\rho^{j_1}_{A^N B} = \frac{1}{M!d^N}\sum_{\tau\in S_J}\sum_{l_{j_1},\dots,l_{j_M},l'_{j_1}=1}^{d} |l_{\tau^{-1}(j_1)}l_{\tau^{-1}(j_2)}\cdots l_{\tau^{-1}(j_M)}\rangle\langle l'_{j_1}l_{j_2}\cdots l_{j_M}|_{A_J}\otimes|l_{j_1}\rangle\langle l'_{j_1}|_B\otimes \mathbb{1}_{A^N\setminus A_J}. \tag{A2}$$

Hence, when $I\cap J = \emptyset$,

$$\begin{aligned}\mathrm{Tr}\big[\Pi_{A_I}\rho^{i_1}_{A^N B}\Pi_{A_J}\rho^{j_1}_{A^N B}\big] &= \frac{1}{(M!)^2 d^{2N}}\sum_{\sigma\in S_I}\sum_{\tau\in S_J}\sum_{k_{i_1},\dots,k_{i_M},k'_{i_1}=1}^{d}\sum_{l_{j_1},\dots,l_{j_M},l'_{j_1}=1}^{d}\mathrm{Tr}[|k_{\sigma^{-1}(i_1)}k_{\sigma^{-1}(i_2)}\cdots k_{\sigma^{-1}(i_M)}\rangle\langle k'_{i_1}k_{i_2}\cdots k_{i_M}|_{A_I}\\ &\quad\otimes |l_{\tau^{-1}(j_1)}l_{\tau^{-1}(j_2)}\cdots l_{\tau^{-1}(j_M)}\rangle\langle l'_{j_1}l_{j_2}\cdots l_{j_M}|_{A_J}\otimes|k_{i_1}\rangle\langle k'_{i_1}|l_{j_1}\rangle\langle l'_{j_1}|_B\otimes\mathbb{1}_{A^N\setminus A_I A_J}]\\ &= \frac{1}{(M!)^2 d^{N+2M}}\sum_{\sigma\in S_I}\sum_{\tau\in S_J}\sum_{k_{i_1},\dots,k_{i_M},k'_{i_1}=1}^{d}\sum_{l_{j_1},\dots,l_{j_M},l'_{j_1}=1}^{d}\\ &\quad\times\delta_{k'_{i_1},k_{\sigma^{-1}(i_1)}}\delta_{k_{i_2},k_{\sigma^{-1}(i_2)}}\cdots\delta_{k_{i_M},k_{\sigma^{-1}(i_M)}}\delta_{l'_{j_1},l_{\tau^{-1}(j_1)}}\delta_{l_{j_2},l_{\tau^{-1}(j_2)}}\cdots\delta_{l_{j_M},l_{\tau^{-1}(j_M)}}\delta_{k_{i_1},l'_{j_1}}\delta_{k'_{i_1},l_{j_1}}\\ &= \frac{1}{(M!)^2 d^{N+2M}}\sum_{\sigma\in S_I}\sum_{\tau\in S_J}\sum_{k_{i_1},\dots,k_{i_M}=1}^{d}\sum_{l_{j_1},\dots,l_{j_M}=1}^{d}\delta_{l_{j_1},k_{\sigma^{-1}(i_1)}}\delta_{k_{i_1},l_{\tau^{-1}(j_1)}}\prod_{p=2}^{M}\delta_{k_{i_p},k_{\sigma^{-1}(i_p)}}\delta_{l_{j_p},l_{\tau^{-1}(j_p)}}.\end{aligned} \tag{A3}$$

Therefore, from (46), we obtain (47).

[1] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels, Phys. Rev. Lett. **70**, 1895 (1993).

[2] H. J. Briegel, W. Dür, J. I. Cirac, and P. Zoller, Quantum repeaters: The role of imperfect local operations in quantum communication, Phys. Rev. Lett. **81**, 5932 (1998).

[3] S. Ishizaka and T. Hiroshima, Asymptotic teleportation scheme as a universal programmable quantum processor, Phys. Rev. Lett. **101**, 240501 (2008).

[4] S. Ishizaka and T. Hiroshima, Quantum teleportation scheme by selecting one of multiple output ports, Phys. Rev. A **79**, 042306 (2009).

[5] M. A. Nielsen and I. L. Chuang, Programmable quantum gate arrays, Phys. Rev. Lett. **79**, 321 (1997).

[6] S. Beigi and R. König, Simplified instantaneous non-local quantum computation with applications to position-based cryptography, New J. Phys. **13**, 093036 (2011).

[7] H. Buhrman, Ł. Czekaj, A. Grudka, M. Horodecki, P. Horodecki, M. Markiewicz, F. Speelman, and S. Strelchuk, Quantum communication complexity advantage implies violation of a Bell inequality, Proc. Natl. Acad. Sci. USA **113**, 3191 (2016).

[8] Z.-W. Wang and S. L. Braunstein, Higher-dimensional performance of port-based teleportation, Sci. Rep. **6**, 33004 (2016).

[9] M. Studziński, S. Strelchuk, M. Mozrzymas, and M. Horodecki, Port-based teleportation in arbitrary dimension, Sci. Rep. **7**, 10871 (2017).

[10] M. Mozrzymas, M. Studziński, S. Strelchuk, and M. Horodecki, Optimal port-based teleportation, New J. Phys. **20**, 053006 (2018).

[11] M. Christandl, F. Leditzky, C. Majenz, G. Smith, F. Speelman, and M. Walter, Asymptotic performance of port-based teleportation, Commun. Math. Phys. **381**, 379 (2021).

[12] F. Leditzky, Optimality of the pretty good measurement for port-based teleportation, Lett. Math. Phys. **112**, 98 (2022).

[13] J. Fei, S. Timmerman, and P. Hayden, Efficient quantum algorithm for port-based teleportation, arXiv:2310.01637.

[14] D. Grinko, A. Burchardt, and M. Ozols, Gelfand-Tsetlin basis for partially transposed permutations, with applications to quantum information, arXiv:2310.02252.

[15] D. Grinko, A. Burchardt, and M. Ozols, Efficient quantum circuits for port-based teleportation, arXiv:2312.03188.

[16] A. Wills, M.-H. Hsieh, and S. Strelchuk, Efficient algorithms for all port-based teleportation protocols, PRX Quantum **5**, 030354 (2024).

[17] M. Murao, D. Jonathan, M. B. Plenio, and V. Vedral, Quantum telecloning and multiparticle entanglement, Phys. Rev. A **59**, 156 (1999).

[18] M. Murao, M. B. Plenio, and V. Vedral, Quantum-information distribution via entanglement, Phys. Rev. A **61**, 032311 (2000).

[19] J. L. Park, The concept of transition in quantum mechanics, Found. Phys. **1**, 23 (1970).

[20] W. K. Wootters and W. H. Zurek, A single quantum cannot be cloned, Nature (London) **299**, 802 (1982).

[21] D. Dieks, Communication by EPR devices, Phys. Lett. A **92**, 271 (1982).

[22] V. Bužek and M. Hillery, Quantum copying: Beyond the no-cloning theorem, Phys. Rev. A **54**, 1844 (1996).

[23] R. F. Werner, Optimal cloning of pure states, Phys. Rev. A **58**, 1827 (1998).

[24] M. Horodecki, P. Horodecki, and R. Horodecki, General teleportation channel, singlet fraction, and quasidistillation, Phys. Rev. A **60**, 1888 (1999).

[25] V. P. Belavkin, Optimal multiple quantum statistical hypothesis testing, Stochastics **1**, 315 (1975).

[26] P. Hausladen and W. K. Wootters, A 'pretty good' measurement for distinguishing quantum states, J. Mod. Opt. **41**, 2385 (1994).

[27] M. Keyl and R. F. Werner, Optimal cloning of pure states, testing single clones, J. Math. Phys. **40**, 3283 (1999).

[28] M. Studziński, M. Mozrzymas, P. Kopszak, and M. Horodecki, Efficient multi port-based teleportation schemes, IEEE Trans. Inf. Theory **68**, 7892 (2022).