Optimality of the pretty good measurement for port-based teleportation

Felix Leditzky1,2,3

Received: 1 September 2020 / Revised: 6 September 2022 / Accepted: 16 September 2022 / Published online: 27 September 2022 © The Author(s), under exclusive licence to Springer Nature B.V. 2022

Abstract
Port-based teleportation (PBT) is a protocol in which Alice teleports an unknown quantum state to Bob using measurements on a shared entangled multipartite state called the port state and forward classical communication. In this paper, we give an explicit proof that the so-called pretty good measurement, or square-root measurement, is optimal for the PBT protocol with independent copies of maximally entangled states as the port state. We then show that the very same measurement remains optimal even when the port state is optimized to yield the best possible PBT protocol. Hence, there is one particular pretty good measurement achieving the optimal performance in both cases. The following well-known facts are key ingredients in the proofs of these results: (i) the natural symmetries of PBT, leading to a description in terms of representation-theoretic data; (ii) the operational equivalence of PBT with certain state discrimination problems, which allows us to employ duality of the associated semidefinite programs. Along the way, we rederive the representation-theoretic formulas for the performance of PBT protocols proved in Studziński et al. (Sci Rep 7(1):1–11, 2017) and Mozrzymas et al. (N J Phys 20(5):053006, 2018) using only standard techniques from the representation theory of the unitary and symmetric groups. Providing a simplified derivation of these beautiful formulas is one of the main goals of this paper.

Keywords Quantum information theory · Quantum teleportation · Quantum state discrimination · Representation theory · Semidefinite programming

Mathematics Subject Classification 81P45
1 Introduction

Quantum teleportation [3] is arguably one of the most fundamental quantum information-processing tasks. Its basic setup consists of two spatially separated parties Alice and Bob with access to the following two resources: a classical communication link, and a shared entangled quantum state. The goal of teleportation is to use these two resources to teleport an unknown quantum state from Alice to Bob. In the original protocol by Bennett et al. [3], Alice measures the unknown quantum state together with her half of the shared entangled state, and sends the classical outcome to Bob through the classical communication link. Bob then applies a suitable correction operation to his half of the shared entangled state, thereby transforming it into the desired target state that is now in his possession. Provided that both the shared entanglement and the classical communication link are noiseless, the quantum teleportation protocol of [3] is perfect: it always works, and it faithfully teleports the unknown quantum state from Alice to Bob.

In certain (e.g., cryptographic) applications, one may be interested in simplifying the correction step of the teleportation protocol described above, at the expense of other features or resources. We focus here on a variant of teleportation called port-based teleportation (PBT), which was introduced by Ishizaka and Hiroshima [15, 16] as a modification of a linear optics teleportation scheme by Knill et al. [18]. In PBT, Alice and Bob share a multipartite entangled state on a collection of quantum systems called ports that are distributed evenly between them. To teleport an unknown quantum state, Alice again performs a joint measurement on the quantum systems in her possession, consisting of the quantum state to be teleported and her half of the ports. Alice’s measurement results in the teleportation of the target state into one of Bob’s ports, which is identified by the measurement outcome. Once Alice communicates the location of the correct port to Bob, he simply discards the other systems. A general PBT protocol is completely determined by the multipartite entangled state on the ports as well as Alice’s measurement.

The crucial property of a PBT protocol as described above is that it works equally well if Bob applies the same unitary operation to each of his port systems before the protocol starts. As a result, PBT allows for the teleportation of an unknown quantum state processed by a unitary operation, a property called unitary covariance. Unfortunately, in the case of finite resources such unitarily covariant protocols cannot be perfect [27], and hence PBT can only achieve approximate teleportation. Nevertheless, there are PBT protocols that become faithful in the limit of a large number of port systems [5, 8, 15, 16, 24]. The unitary covariance property of PBT enables interesting applications for universal programmable quantum processors [15], instantaneous non-local quantum computation [5], linking quantum communication complexity and non-locality [6], quantum channel discrimination [29, 31], channel simulation [28], and high-energy physics [10, 22, 23]. Furthermore, PBT has been generalized to a “multi-port” version where multiple systems are teleported at once [19, 26, 36]. The resource requirements of PBT have been further investigated in [33, 34].

Port-based teleportation enjoys an equivalent description in terms of a certain state discrimination problem ([5, 15, 16], see Sect. 3 for details). This useful equivalence enables the study of PBT using semidefinite programming [38, Sect. 1.2.3], and it
furthermore suggests the use of a special measurement called the pretty good measurement or square-root measurement ([2, 13, 14], see Sect. 4.1 for the definition). In a generic state discrimination problem, this measurement always achieves a success probability no worse than the square of the optimal success probability [4]. In this paper, we will employ the connection to state discrimination and semidefinite programming to show that the pretty good measurement is in fact optimal for certain PBT protocols of interest.

1.1 Main results, purpose, and structure of this paper

The main result of this paper is an explicit proof of optimality of the pretty good measurement for the port-based teleportation (PBT) protocol using \( N \) maximally entangled states. In addition, we show that somewhat surprisingly, the same pretty good measurement used in the previous result also achieves the optimal entanglement fidelity for a PBT protocol with an optimized port state. Both results are derived by exploiting the natural symmetries of PBT and using its operational equivalence to state discrimination. The former leads to the known representation-theoretic formulas for the performance of PBT protocols in the two settings based on \( N \) maximally entangled states and an optimized port state, derived by Studziński et al. [35] and Mozrzymas et al. [24], respectively. The equivalence of PBT to state discrimination along with the latter’s semidefinite programming formulation then allows us to prove that in both cases above the pretty good measurement is in fact the optimal measurement.

Optimality of the pretty good measurement for \( N \) maximally entangled states is implied by the results in [24]. These results can furthermore be used to show that the optimal measurement in the case of an optimized port state has the form of a pretty good measurement [37]. The present paper provides explicit proofs of both results. Along the way, based on the insights of our prior work [8], we also present an (almost) self-contained derivation of the beautiful formulas of [24, 35] mentioned above. One of this paper’s main goals is a streamlined presentation of these results that is intended to be accessible to a wide audience. Our approach is similar in spirit to the original proof method based on so-called partially transposed permutation operators [25] employed in [24, 35]; however, here we only use well-known results about the representation theory of the symmetric and unitary groups such as Schur–Weyl duality (see Sect. 2.2), as well as the results from [8].

This paper is structured as follows. In Sect. 2, we introduce some notation and basic definitions, and we review the necessary facts about Schur–Weyl duality. Section 3 introduces PBT and explains the operational equivalence to a certain state discrimination problem. We then prove our main results: optimality of the pretty good measurement for the PBT protocol using \( N \) maximally entangled states in Sect. 4, and optimality of the same measurement for the protocol using an optimized port state in Sect. 5. We conclude in Sect. 6 with a discussion of our results and open questions.
2 Preliminaries

2.1 Notation and definitions

Quantum systems are associated with finite-dimensional Hilbert spaces $\mathcal{H}_A$, labeled by capital letters $A_1$, etc. A multipartite system $AB$ is associated with the tensor product $\mathcal{H}_A \otimes \mathcal{H}_B$. Given $N$ quantum systems $A^N \equiv A_1 \ldots A_N$, we use the shortcut $A_i^c \equiv A_1 \ldots A_{i-1} A_{i+1} \ldots A_N$.

A quantum state $\rho_A$ on a quantum system $A$ is a linear positive semidefinite operator on $\mathcal{H}_A$ with unit trace, $\operatorname{tr} \rho_A = 1$. A pure state $\psi_A$ on a quantum system $A$ is a state of rank 1, which can be identified with a normalized vector $|\psi_A\rangle \in \mathcal{H}_A$ such that $\psi_A = |\psi_A\rangle \langle \psi_A|$. Given a $d$-dimensional quantum system $A$, we use the symbol $\pi_A = \frac{1}{d} \mathbb{1}_A$ for the completely mixed state, where $\mathbb{1}_A$ denotes the identity operator on $\mathcal{H}_A$. For a given orthonormal basis $\{|i\rangle\}_{i=1}^d$ of a $d$-dimensional quantum system $A$ and an isomorphic system $A' \cong A$, the maximally entangled state $|\Phi^+\rangle_{AA'}$ is defined as

$$|\Phi^+\rangle_{AA'} = \frac{1}{\sqrt{d}} \sum_{i=1}^d |i\rangle_A \otimes |i\rangle_{A'},$$

and satisfies $\operatorname{tr}_{A'} \Phi^+_{AA'} = \pi_A$ (and similarly for $\operatorname{tr}_A \Phi^+_{AA'}$).

A quantum measurement of a quantum system $A$ is described by a positive operator-valued measure (POVM) $E = \{E^i_i\}_{i=1}^N$, which consists of positive semidefinite operators $E^i_i$ satisfying $\sum_{i=1}^N E^i_i = \mathbb{1}_A$. When measuring the quantum system $A$ in the state $\rho_A$ with the POVM $E$, the outcome $i$ is obtained with probability $\operatorname{tr}(\rho_A E^i_i)$.

We denote by $[X, Y] = XY - YX$ the commutator of two operators $X$ and $Y$. We will often omit identity operators in expressions involving multiple quantum systems, e.g., $X_{AB} Y_A \equiv X_{AB}(Y_A \otimes \mathbb{1}_B)$, whenever this does not cause confusion. A partition of $N \in \mathbb{N}$ into $d$ parts is a vector $\mu = (\mu_1, \ldots, \mu_d)$ with $\mu_1 \geq \cdots \geq \mu_d \geq 0$ and $\sum_{i=1}^d \mu_i = N$, and denoted by $\mu \vdash_d N$. Alternatively, $\mu \vdash_d N$ can be interpreted as a Young diagram whose $i$-th row has $\mu_i$ boxes. For a given Young diagram $\alpha \vdash_d N - 1$, we denote by $\alpha + \square$ a Young diagram obtained by adding a single box to $\alpha$ such that the result is still a Young diagram, i.e., a box may be added to the $i$-th row of $\alpha$ if $\alpha_i < \alpha_{i-1}$.

We denote by $S_N$ the symmetric group of degree $N$, and by $U_d$ the group of unitary operators acting on a $d$-dimensional Hilbert space. For a positive semidefinite operator $X$ with spectral decomposition $X = \sum_i \lambda_i |\psi_i\rangle \langle \psi_i|$, the generalized inverse $X^{-1}$ is defined as $X^{-1} := \sum_{i: \lambda_i > 0} \lambda_i^{-1} |\psi_i\rangle \langle \psi_i|$. With this definition, $XX^{-1} = X^{-1}X = \Pi_X$, where $\Pi_X := \sum_{i: \lambda_i > 0} |\psi_i\rangle \langle \psi_i|$ denotes the orthogonal projection onto the support $\operatorname{supp}(X) := (\ker X)^\perp$ of $X$.

In our optimality proofs, we will make use of the following fact, a version of which appeared in [20] (see also [15]). We give a proof in Appendix A for the convenience of the reader.
Lemma 1 Let $X$ be a positive semidefinite operator on a Hilbert space $\mathcal{H}$. For some $K \in \mathbb{N}$ and $c \in \mathbb{R}$ let $\{|\xi_k\rangle\}_{k=1}^K \subset \text{im}(X)$ be a collection of nonzero vectors such that $\langle \xi_j | X^{-1} | \xi_k \rangle = \delta_{j,k}$ for $1 \leq j, k \leq K$. Then, $c > 0$ and

$$X \geq \frac{1}{c} \sum_{k=1}^K |\xi_k\rangle \langle \xi_k|.$$ (2.2)

2.2 Representation theory of the symmetric and unitary groups

We consider the representations of $S_N$ and $U_d$ on $(\mathbb{C}^d)^{\otimes N}$ by permuting tensor factors and acting diagonally, respectively. More precisely, the representations are defined by the linear extension of the following actions on product states $|\psi_i\rangle \in \mathbb{C}^d$:

$$S_N \ni \pi : \bigotimes_{i=1}^N |\psi_i\rangle \longmapsto \bigotimes_{i=1}^N |\psi_{\pi^{-1}(i)}\rangle,$$ (2.3)

$$U_d \ni U : \bigotimes_{i=1}^N |\psi_i\rangle \longmapsto \bigotimes_{i=1}^N U |\psi_i\rangle.$$ (2.4)

It is easy to check that these two actions commute, i.e., $\pi U^{\otimes N} |\phi\rangle = U^{\otimes N} \pi |\phi\rangle$ for all $\pi \in S_N$, $U \in U_d$, and $|\phi\rangle \in (\mathbb{C}^d)^{\otimes N}$. Furthermore, Schur–Weyl duality states that these representations span each other’s commutant ([11, 32]; see also the PhD theses of Harrow [12] and Christandl [9]). This fact gives rise to a useful decomposition of $(\mathbb{C}^d)^{\otimes N}$ when considering the actions of the representations of $S_N$ in (2.3) and $U_d$ in (2.4) together:

$$(\mathbb{C}^d)^{\otimes N} = \bigoplus_{\mu \vdash d \mid N} V^d_\mu \otimes W_\mu.$$ (2.5)

Here, for a given Young diagram $\mu \vdash d \mid N$, each direct summand is the tensor product of the Weyl module $V^d_\mu$ carrying an irreducible representation of the unitary group $U_d$ labeled by $\mu$, and the Specht module $W_\mu$ carrying an irreducible representation of the symmetric group $S_N$, again labeled by $\mu$. Note that (2.5) only includes all irreducible representations of $S_N$ if $N \leq d$. We denote the dimensions of the Weyl and Specht modules by $m_{d,\mu} = \dim V^d_\mu$ and $d_\mu = \dim W_\mu$, respectively. Throughout the paper, $P_\mu$ denotes the projection onto the direct summand $V^d_\mu \otimes W_\mu$ in (2.5). The following result will be useful for us:

Lemma 2 (Partial trace of Young projectors, [7]) Let $\mu \vdash d \mid N$ be a Young diagram with $N$ boxes and at most $d$ rows, and let $P_\mu$ be the corresponding isotypical projection. Then,

$$\text{tr}_1 P_\mu = m_{d,\mu} \sum_{i : \mu_i > \mu_i+1} \frac{1}{m_{d,\mu-\varepsilon_i}} P_{\mu-\varepsilon_i},$$ (2.6)

where $\text{tr}_1$ denotes the partial trace over the first factor in $(\mathbb{C}^d)^{\otimes N}$, and $\varepsilon_i$ is the vector of length $d$ with a 1 in the $i$-th component and zeros elsewhere.
3 Port-based teleportation

In a general PBT protocol \([15, 16]\), Alice and Bob share an entangled state \(\phi_{ANB^N}\) defined on Alice’s port systems \(A^N\) and Bob’s ports \(B^N\), where \(A_i\) and \(B_i\) for \(i = 1, \ldots, N\) are \(d\)-dimensional quantum systems. Alice holds an additional \(d\)-dimensional quantum system \(A_0\) that she wishes to teleport to Bob. To achieve this task, she chooses a POVM \(\{E_i\}_{i=1}^N\) to measure the systems \(A_0A^N\), and communicates the outcome \(1 \leq i \leq N\) to Bob. Upon receiving this message, Bob discards all but the \(i\)-th port, which should now hold an approximate copy \(B_0\) of Alice’s initial system \(A_0\).\(^1\) Bob’s part of the protocol is equivalent to applying the “correction operation” \(\text{tr}_{B_i}^B\) to his ports. This operation commutes with any local unitary \(U \otimes \mathbb{I}_d\) for \(U \in \mathcal{U}_d\), and thus leads to the unitary covariance property of PBT mentioned in the introduction [8, 15, 16, 21].

A PBT protocol \((\phi_{ANB^N}, E)\) as introduced above can be described via a teleportation channel \(\Lambda: A_0 \to B_0\). The output state of the above protocol is given by

\[
\Lambda(\sigma_{A_0}) = \sum_{i=1}^N \text{tr}_{A_0A^N B_i^i} \left[ E_i^{A_0A^N} \left( \sigma_{A_0} \otimes \phi_{ANB^N} \right) \right], \quad (3.1)
\]

where in each summand, the final port \(B_i^i\) is relabeled as \(B_0\). The quality of a PBT protocol is determined by how close the teleportation channel \(\Lambda\) is to the identity channel \(\mathbb{I}_{A_0} \to B_0\). We quantify this by means of the entanglement fidelity, which measures how well \(\Lambda\) preserves correlations with an inaccessible reference system \(R \cong A_0 \cong B_0\). The entanglement fidelity is defined as

\[
F(\Lambda) = \text{tr} \left[ \Phi_{B_0R}^+ (\Lambda \otimes \mathbb{I}_R)(\Phi_{A_0R}^+) \right], \quad (3.2)
\]

and we have \(F(\Lambda) = 1\) if and only if \(\Lambda\) is the identity channel. In general, the entanglement fidelity represents an average error criterion, whereas the worst-case error is quantified by the so-called diamond norm distance on the set of quantum channels. However, the unitary covariance of PBT \([8, 15, 21]\) renders the two error criteria equivalent \([29]\), and hence the entanglement fidelity \((3.2)\) quantifies the worst-case error as well.

Ishizaka and Hiroshima \([15]\) (see also [5]) showed that the entanglement fidelity in \((3.2)\) can be written as

\[
F(\Lambda) = \frac{1}{d^2} \sum_{i=1}^N \text{tr} \left( E_i^{A^N B} \sigma_{A^N B}^{\dagger} \right), \quad (3.3)
\]

\(^1\) In this paper, we are only concerned with so-called deterministic PBT as described above. There is another variant of the protocol called probabilistic PBT, in which the protocol teleports the target state perfectly, but may abort with a certain probability. Both variants were introduced in the original papers \([15, 16]\), and we refer to [8] for a more detailed comparison of the two variants.
where the POVM $E = \{E^i_{A_0 A^N}\}_{i=1}^N$ from above is now interpreted as a measurement on $A^N B$ with $B \equiv B_0 \cong A_0$. The states $\sigma^i_{A^N B}$ are obtained from the port state $\phi_{A^N B^N}$ as

$$\sigma^i_{A^N B} = \text{tr}_{B^c} \phi_{A^N B^N}.$$  (3.4)

Equation 3.3 shows that the entanglement fidelity $F(\Lambda)$ is in fact proportional to the success probability of distinguishing the states $\sigma^i_{A^N B}$ for $i = 1, \ldots, N$ drawn uniformly at random. The (general) state discrimination problem of distinguishing $N$ states $\rho_i$ drawn with (not necessarily uniform) probability $p_i$ for $i = 1, \ldots, N$ admits the following semidefinite program formulation:

$$p_{\text{succ}} = \max \left\{ \sum_{i=1}^N p_i \text{tr}(\rho_i E_i) : E_i \geq 0 \text{ for } i = 1, \ldots, N, \sum_{i=1}^N E_i = 1 \right\}.$$  (3.5)

We refer to [38, Sect. 1.2.3] for an introduction to semidefinite programs. The dual program of (3.5) can be derived using standard methods, and is given by the following minimization problem:

$$p^*_{\text{succ}} = \min \{ \text{tr} K : K \geq p_i \rho_i \text{ for } i = 1, \ldots, N \}.$$  (3.6)

It has the same value as the primal problem (3.5) by strong duality, $p_{\text{succ}} = p^*_{\text{succ}}$, which follows for example from Slater’s Theorem [38, Sect. 1.2.3].

Using (3.3) and (3.5), it is now clear that the entanglement fidelity of a PBT protocol with teleportation channel $\Lambda$ can be expressed as [5, 15]

$$F(\Lambda) = \frac{N}{d^2} p_{\text{succ}},$$  (3.7)

where $p_{\text{succ}}$ is defined in terms of the $N$ states $\sigma^i_{A^N B}$ in (3.4) drawn uniformly at random. Figure 1 shows a schematic description of these states when the port state $\phi_{A^N B^N}$ is comprised of $N$ maximally entangled states, as discussed in Sect. 4. Equation 3.7 forges a useful operational equivalence between PBT and state discrimination. We will make use of this equivalence, in particular the semidefinite programming formulation and duality, to derive our main results. Throughout the discussion, the local port dimension $d$ and the number of ports $N$ are fixed but arbitrary.

### 4 Independent maximally entangled states

We first consider a special case of PBT where the port state is comprised of $N$ independent maximally entangled states,

$$\phi_{A^N B^N} = (\Phi^+_{A B})^\otimes N.$$  (4.1)
According to Sect. 3, we can equivalently consider the state discrimination problem of distinguishing the $N$ states

$$\rho_i = \Phi^+_{A_i B} \otimes \pi_{A_i^c} \quad (4.2)$$

on $A^N B$ drawn uniformly at random, i.e., with probability $\frac{1}{N}$ each. A graphical representation of these states is shown in Fig. 1.

Since $(U \otimes \bar{U})|\Phi^+\rangle = |\Phi^+\rangle$ for every unitary $U \in U_d$, the states $\rho_i$ have the symmetries

$$\left[ U^{\otimes N} \otimes \bar{U}, \rho_i \right] = 0 \quad \text{for all } U \in U_d, \quad (4.3)$$
$$\left[ \varphi \otimes 1_{A_i B}, \rho_i \right] = 0 \quad \text{for all } \varphi \in S_{N-1}, \quad (4.4)$$

where in the first line $U^{\otimes N} \otimes \bar{U} \equiv U^{\otimes N}_A \otimes \bar{U}_B$, and in the second line we consider the action of $S_{N-1}$ on $A_i^c$ by permuting tensor factors. Moreover,

$$\pi \rho_i \pi^\dagger = \rho_{\pi(i)} \quad \text{for all } \pi \in S_N. \quad (4.5)$$

It follows from eqs. (4.3) to (4.5) that the (unnormalized) average state $\tilde{\rho} = \sum_{i=1}^{N} \rho_i$ on $A^N B$ has the symmetries

$$\left[ U^{\otimes N} \otimes \bar{U}, \tilde{\rho} \right] = 0 \quad \text{for all } U \in U_d, \quad (4.6)$$
$$\left[ \pi \otimes 1_{B}, \tilde{\rho} \right] = 0 \quad \text{for all } \pi \in S_N. \quad (4.7)$$

---

Fig. 1 Schematic depiction of the state discrimination problem that is equivalent to PBT as explained in Sect. 3. Shown here is the state $\rho_2$ from the family $\{\rho_i\}_{i=1}^{N}$ defined in (4.2) that appears in a PBT protocol using $N$ maximally entangled states $\Phi^+_{AB}$. The latter are represented by wavy lines.

---

2 Here, $\bar{X}$ denotes complex conjugation with respect to the basis used to define $|\Phi^+\rangle$. 
The symmetries in eqs. (4.7) and (4.6) together with Schur’s Lemma imply that \( \bar{\rho} \) is diagonal with respect to the following decomposition of \( (\mathbb{C}^d)^{\otimes N+1} \) derived from Schur–Weyl duality (2.5) using the so-called dual Pieri rule:

\[
(\mathbb{C}^d)^{\otimes N+1} = \bigoplus_{\mu \vdash d N} \bigoplus_{i: \mu_i > \mu_{i+1}} V^d_{\mu - \varepsilon_i} \otimes W_{\mu}.
\]  

(4.8)

As in Lemma 2, \( \varepsilon_i \) is the vector of length \( d \) with a 1 in the \( i \)-th component and zeros elsewhere.\(^3\) We refer to Appendix A of [8] for details of the derivation of (4.8). In the present paper, we will make use of this result in the following way:

**Lemma 3** [8, 35] The (unnormalized) average state \( \bar{\rho} = \sum_{i=1}^N \rho_i \) of the ensemble \( \{(\frac{1}{N}, \rho_i)\}_{i=1}^N \) with \( \rho_i \) as in (4.2) can be written as

\[
\bar{\rho} = \bigoplus_{\alpha = \delta N - 1}^{\delta N} \bigoplus_{\mu = \alpha + \square} r_{\mu, \alpha} \mathbb{1}_{d} \otimes \mathbb{1}_{W_{\mu}},
\]

(4.9)

where the eigenvalues \( r_{\mu, \alpha} \) are given by

\[
r_{\mu, \alpha} = \frac{N m_{d, \mu} d_{\alpha}}{d^N m_{d, \alpha} d_{\mu}}.
\]

(4.10)

### 4.1 Performance of the pretty good measurement

For a given state ensemble \( \{(p_i, \sigma_i)\}_{i=1}^N \), the pretty good measurement [2, 13, 14] is defined as the measurement \( E = \{E_i\}_{i=1}^N \) with operators

\[
E_i = \bar{\sigma}^{-1/2} p_i \sigma_i \bar{\sigma}^{-1/2}.
\]

(4.11)

Here, \( \bar{\sigma} = \sum_{i=1}^N p_i \sigma_i \) is the ensemble average state. The measurement operators \( E_i \) satisfy \( E_i \geq 0 \) for all \( i = 1, \ldots, N \), and \( \sum_{i=1}^N E_i = \Pi_{\bar{\sigma}} \). The pretty good measurement thus forms a valid POVM once the Hilbert space is restricted to \( \text{supp} \bar{\sigma} \), which we will always assume.

The success probability of discriminating the states \( \{(\frac{1}{N}, \rho_i)\}_{i=1}^N \) with \( \rho_i \) as in (4.2) using the pretty good measurement \( E = \{E_i\}_{i=1}^N \) is thus given by the expression

\[
p_{\text{succ}} = \frac{1}{N} \sum_{i=1}^N \text{tr} \left( \rho_i \bar{\rho}^{-1/2} \rho_i \bar{\rho}^{-1/2} \right),
\]

(4.12)

where as before \( \bar{\rho} = \sum_{i=1}^N \rho_i \) is the unnormalized ensemble average state. It follows from the results of Studziński et al. [35] that this success probability can be expressed in terms of representation-theoretic quantities:

\(^3\) Note that we set \( \mu_{d+1} = -\infty \) in (4.8), and hence the summand for \( i = d \) always appears in the sum. For a Young diagram \( \mu \vdash d N \) with \( \mu_d = 0 \), the resulting \( \mu - \varepsilon_d \) is not a Young diagram anymore.
\[ p_{\text{succ}} = \frac{1}{Nd^N} \sum_{\alpha \vdash d N - 1} \left( \sum_{\mu = \alpha + \square} \sqrt{m_{\mu} d_{\mu}} \right)^2. \] (4.13)

The goal of this section is to rederive this formula.

To this end, we define the operator

\[ X = \sum_{i=1}^{N} \rho_i \tilde{\rho}^{-1/2} \rho_i \tilde{\rho}^{-1/2}, \] (4.14)

such that \( \frac{1}{N} \text{tr} \ X = p_{\text{succ}} \) for the success probability defined in (4.12). Since \( x \mapsto x^{-1/2} \) is a real-analytic function on \((0, \infty)\), the operator \( \tilde{\rho}^{-1/2} \) inherits the \( U \otimes \tilde{U} \) and \( S_N \) symmetries (eqs. (4.6) and (4.7)) from \( \tilde{\rho} \). Furthermore, for any \( \pi \in S_N \),

\[ \pi \rho_i \tilde{\rho}^{-1/2} \rho_i \tilde{\rho}^{-1/2} \pi^\dagger = \pi \rho_i \pi^\dagger \rho \tilde{\rho}^{-1/2} \pi \rho_i \pi^\dagger \tilde{\rho}^{-1/2} \pi^\dagger = \rho \rho_i \tilde{\rho}^{-1/2} \rho \rho_i \tilde{\rho}^{-1/2}, \] (4.15)

where we used (4.5) and (4.7).

The operator \( X \) in (4.14) thus has the same \( U \otimes \tilde{U} \) and \( S_N \) symmetries as \( \tilde{\rho} \) above,

\[ \left[ U^{\otimes N} \otimes \tilde{U}, X \right] = 0 \quad \text{for all} \ U \in \mathcal{U}_d, \] (4.17)

\[ [\pi \otimes 1_B, X] = 0 \quad \text{for all} \ \pi \in S_N. \] (4.18)

With respect to the decomposition (4.8), the operator \( X \) can hence be written as

\[ X = \bigoplus_{\mu \vdash d N} \bigoplus_{i: \mu_i > \mu_{i+1}} x_{\mu,i} \mathbb{1}_{V_{\mu - \varepsilon_i}^d} \otimes W_{\mu}. \] (4.19)

The coefficients \( x_{\mu,i} \) in (4.19) can be determined using a similar strategy as in Appendix A of [8]. Since \( d \) is fixed throughout the discussion, we abbreviate \( m_{\mu} \equiv m_{d,\mu} \) for the dimension of the Weyl modules \( V_{\mu}^d \) in the following. Recall that \( P_{\mu} \) denotes the projection onto the summand \( V_{\mu}^d \otimes W_{\mu} \) in the Schur–Weyl decomposition (2.5). We further denote by \( Q_{\alpha} \) the isotypical projections for the \( \mathcal{U}_d \) action by \( U^{\otimes N} \otimes \tilde{U} \) as defined via decomposition (4.8). Note that here \( \alpha \) can have negative entries and is thus not necessarily a valid Young diagram (see Footnote 3).

However, the coefficients \( x_{\mu,i} \) in (4.19) are only nonzero when \( \mu - \varepsilon_i \) is indeed a valid Young diagram, \( \mu - \varepsilon_i = \alpha \vdash d N - 1 \). To see this, we recall the following argument from [8, App. A]: Since \( (U \otimes \tilde{U}) \Phi_{A_1B}^+ \) for every \( U \in \mathcal{U}_d \), the actions of \( U^{\otimes N} \otimes \tilde{U} \) and \( \mathbb{1}_{A_1B} \otimes U^{\otimes N-1} \) agree on the range of \( \Phi_{A_1B}^+ \), and hence,

\[ \Phi_{A_1B}^+ Q_{\mu - \varepsilon_i} = \begin{cases} \Phi_{A_1B}^+ (\mathbb{1}_{A_1B} \otimes P_{\alpha}^d) & \text{if } \alpha = \mu - \varepsilon_i \text{ is a Young diagram}, \\ 0 & \text{otherwise}. \end{cases} \] (4.20)
Here, \( P^\prime_\alpha \) denotes the isotypical projection with respect to the action of \( U_d \) on \( A^c_i \) by \( U \otimes N^{-1} \). The operator \( X \) is proportional to a sum of terms of the form \( \Phi^+_A B \tilde{\rho}^{-1/2} \Phi^+_A B \tilde{\rho}^{-1/2} \), so we can apply the above argument to the coefficients \( x_{\mu,i} \) appearing in (4.19) to infer that \( x_{\mu,i} \neq 0 \) only when \( \mu - \varepsilon_i = \alpha \) is a Young diagram. We denote these coefficients by \( x_{\mu,\alpha} \) henceforth, and write \( X \) as

\[
X = \bigoplus_{\alpha + \square = N-1} \bigoplus_{\mu = \alpha + \square} x_{\mu,\alpha} \mathbb{I}_{V_d} \otimes \mathbb{I}_{W_\mu}. \tag{4.21}
\]

In the remainder of this subsection, we first compute the trace of this operator, and then derive a formula for the coefficients \( x_{\mu,\alpha} \).

Let \( \alpha \vdash_d N - 1 \) and \( \mu = \alpha + \square \). By symmetry and the form of \( \rho_1 \) in (4.2), we have

\[
\text{tr} \left[ X \left( P_\mu \otimes 1_B \right) Q_\alpha \right] = N \text{tr} \left[ \rho_1 \tilde{\rho}^{-1/2} \rho_1 \tilde{\rho}^{-1/2} \left( P_\mu \otimes 1_B \right) Q_\alpha \right] \tag{4.22}
\]

\[
= \frac{N}{d^{2N-2}} \text{tr} \left[ \Phi^+_A B \tilde{\rho}^{-1/2} \Phi^+_A B \tilde{\rho}^{-1/2} \left( P_\mu \otimes 1_B \right) Q_\alpha \right] \tag{4.23}
\]

\[
= \frac{N}{d^{2N-2}} \sum_{\alpha', \alpha'' \vdash_d N-1} \sum_{\mu = \alpha + \square} r_{\mu', \mu}^{-1/2} r_{\mu'', \mu}^{-1/2} \times \text{tr} \left[ \Phi^+_A B \left( P_{\mu'} \otimes 1_B \right) Q_{\alpha'} \Phi^+_A B \left( P_{\mu''} \otimes 1_B \right) Q_{\alpha''} \left( P_\mu \otimes 1_B \right) Q_\alpha \right], \tag{4.24}
\]

where we inserted the decomposition of \( \tilde{\rho} \) from Lemma 3 twice in (4.24). Let us take a closer look at the trace quantity in (4.24) for fixed \( \alpha \vdash_d N - 1 \) and \( \mu = \alpha + \square \). Using the fact that \( P_\alpha \otimes 1_B \) commutes with \( Q_\alpha \), we can apply the identity (4.20) to each of \( Q_\alpha \), \( Q_{\alpha'} \) and \( Q_{\alpha''} \) to obtain

\[
\text{tr} \left[ \Phi^+_A B \left( P_{\mu'} \otimes 1_B \right) Q_{\alpha'} \Phi^+_A B \left( P_{\mu''} \otimes 1_B \right) Q_{\alpha''} \left( P_\mu \otimes 1_B \right) Q_\alpha \right] = \text{tr} \left[ \Phi^+_A B \left( P_{\mu'} \otimes 1_B \right) \Phi^+_A B \left( P_{\mu''} \otimes 1_B \right) \right] \delta_{\mu, \mu'} \delta_{\alpha, \alpha'} \delta_{\alpha, \alpha''} \tag{4.25}
\]

\[
= \text{tr} \left[ \Phi^+_A B \left( P_{\mu'} \otimes 1_B \right) \Phi^+_A B \left( P_{\mu} \otimes 1_B \right) \right] \delta_{\mu, \mu'} \delta_{\alpha, \alpha'} \delta_{\alpha, \alpha''} \tag{4.26}
\]

where we used orthogonality among the projectors \( P_\alpha \) and among the \( P'_\alpha \) in the last line. Substituting (4.26) in (4.24) leads to

\[
\text{tr} \left[ X \left( P_\mu \otimes 1_B \right) Q_\alpha \right] = \frac{N}{d^{2N-2}} \sum_{\mu = \alpha + \square} r_{\mu', \mu}^{-1/2} \text{tr} \left[ \Phi^+_A B \left( P_{\mu'} \otimes 1_B \right) \Phi^+_A B \left( P_{\mu} \otimes 1_B \right) \right] \tag{4.27}
\]
where step (4.28) follows from the elementary identity \( \text{tr} \left[ \Phi_R^+ XST \Phi_R^+ YST \right] = \frac{1}{d^2} \text{tr} \left( X_T Y_T \right) \).

For the partial traces of the Young projectors \( P_\ast \), Lemma 2 gives

\[
\text{tr} A_1 (P_{\mu}) P'_\alpha = \frac{m_{\mu}}{m_\alpha} P'_\alpha, \tag{4.29}
\]

and similarly, \( \text{tr} A_1 (P_{\mu'}) P'_\alpha = \frac{m_{\mu'}}{m'_\alpha} P'_\alpha \). Substituting these two relations together with formula (4.10) for the coefficients \( r_{\mu,\alpha} \) in (4.28) yields

\[
\text{tr} \left[ X (P_{\mu} \otimes 1_B) Q_\alpha \right] = \frac{N}{d^2 N} \frac{m_\alpha \sqrt{d_{\mu}}}{\sqrt{m_{\mu}}} \frac{\sum_{\mu' = \alpha + \Box} \sqrt{d_{\mu'}} m_{\mu} m_{\mu'}}{m_{\alpha}^2} \text{tr} P'_\alpha \tag{4.30}
\]

\[
= \frac{1}{d^2 N} \frac{\sqrt{d_{\mu}} m_{\mu}}{m_{\alpha}} \sum_{\mu' = \alpha + \Box} \sqrt{d_{\mu'}} m_{\mu'}. \tag{4.31}
\]

Summing over \( \alpha \vdash d N - 1 \) and \( \mu = \alpha + \Box \) gives the trace of \( X \),

\[
\text{tr} X = \sum_{\alpha \vdash d N - 1} \sum_{\mu = \alpha + \Box} \text{tr} \left[ X (P_{\mu} \otimes 1_B) Q_\alpha \right] \tag{4.32}
\]

\[
= \frac{1}{d^2 N} \sum_{\alpha \vdash d N - 1} \left( \sum_{\mu = \alpha + \Box} \sqrt{d_{\mu}} m_{\mu} \right)^2, \tag{4.33}
\]

and thus we have proved (4.13) via \( p_{\text{succ}} = \frac{1}{N} \text{tr} X \).

It remains to derive a formula for the coefficients \( x_{\mu,\alpha} \) appearing in (4.21). By definition, for \( \alpha \vdash d N - 1 \) and \( \mu = \alpha + \Box \), we have

\[
\text{tr} \left[ X (P_{\mu} \otimes 1_B) Q_\alpha \right] = x_{\mu,\alpha} m_{\alpha} d_{\mu}, \tag{4.34}
\]

which is equal to (4.31) by the above calculation. Thus,

\[
x_{\mu,\alpha} = \frac{1}{d^2 N} \frac{\sqrt{m_{\mu}}}{\sqrt{d_{\mu}} m_{\alpha}} \frac{1}{m_{\alpha}} \sum_{\mu' = \alpha + \Box} \sqrt{d_{\mu'}} m_{\mu'}. \tag{4.35}
\]

### 4.2 Optimality of the pretty good measurement

To prove optimality of the pretty good measurement for distinguishing the states \( \rho_i \) defined in (4.2), we use the dual program (3.6) of the corresponding state discrimination problem. The proof idea is identical to the method used by Ishizaka and Hiroshima.
[15] to prove optimality of the pretty good measurement for qubit port systems. Recall from the previous section that \( p_{\text{succ}} = \frac{1}{N} \text{tr} X \) for the operator \( X \) defined in (4.14). If we can show that \( \frac{1}{N} X \) is feasible for the dual program (3.6), then optimality follows from the fact that any feasible solution to (3.6) is an upper bound on the optimal solution, given by either (3.5) or (3.6) because of strong duality. By construction, this upper bound is identical to the value of the success probability (4.13) calculated in Sect. 4.1, which establishes optimality of the pretty good measurement.

Feasibility of the operator \( \frac{1}{N} X \) for (3.6) is equivalent to showing that \( X \geq \rho_i \) for all \( i = 1, \ldots, N \); by symmetry, it is enough to prove this for \( \rho_1 = \Phi_{A_1B}^+ \otimes \pi A_i^\prime \). This will follow from Lemma 1 applied to the operator \( X \) and a set of vectors into which \( \rho_1 \) can be decomposed. First, we recall the expression \( X = \bigoplus_{\alpha = \alpha}^{N-1} \bigoplus_{\mu = \alpha + \square} x_{\mu, \alpha} \mathbb{1}_{V_{d_{\mu}}} \otimes \mathbb{1}_{W_{\mu}} \) derived in Sect. 4.1. Formula (4.35) for the coefficients \( x_{\mu, \alpha} \) shows that they are strictly positive for all \( \alpha \vdash d \ N - 1 \) and \( \mu = \alpha + \square \), so that \( X \) is manifestly positive definite. For the set of vectors in the statement of Lemma 1, we choose the following eigenvectors of \( \rho_1 = \Phi_{A_1B}^+ \otimes \pi A_i^\prime \),

\[
|\xi(\alpha, q_{\alpha}, p_{\alpha})\rangle := |\Phi^+\rangle_{A_1B} \otimes |\alpha, q_{\alpha}, p_{\alpha}\rangle_{A_i^\prime}
\]

(4.36)

for \( \alpha \vdash d \ N - 1, 1 \leq q_{\alpha} \leq m_{\alpha}, \) and \( 1 \leq p_{\alpha} \leq d_{\alpha} \). Here, \( \{|\alpha, q_{\alpha}, p_{\alpha}\rangle_{A_i^\prime}\}_{\alpha \vdash d \ N - 1, q_{\alpha}, p_{\alpha}} \)

is the Schur basis \([1, 12]\) adapted to the Schur–Weyl decomposition \((\mathbb{C}^d)^{\otimes N-1} = \bigoplus_{\alpha \vdash d \ N - 1} V_{d_{\alpha}} \otimes W_{\alpha}\). The indices \( 1 \leq q_{\alpha} \leq m_{\alpha} \) and \( 1 \leq p_{\alpha} \leq d_{\alpha} \) correspond to the Weyl module \( V_{d_{\alpha}} \) and the Specht module \( W_{\alpha} \), respectively. Since

\[
\rho_1 = \frac{1}{d^{N-1}} \Phi_{A_1B}^+ \otimes \mathbb{1}_{A_i^\prime} = \frac{1}{d^{N-1}} \sum_{\alpha \vdash d} \sum_{q_{\alpha}, p_{\alpha}} \Phi_{A_1B}^+ \otimes |\alpha, q_{\alpha}, p_{\alpha}\rangle_{A_i^\prime} \langle \alpha, q_{\alpha}, p_{\alpha}|_{A_i^\prime},
\]

(4.37)

the desired operator inequality \( X \geq \rho_1 \) follows from Lemma 1 once we establish that

\[
\langle \xi(\alpha, q_{\alpha}, p_{\alpha})| X^{-1}|\xi(\beta, q_{\beta}, p_{\beta})\rangle = \delta_{\alpha, \beta} \delta_{q_{\alpha}, q_{\beta}} \delta_{p_{\alpha}, p_{\beta}} \cdot d^{N-1}
\]

(4.38)

holds for all \( \alpha, \beta \vdash d \ N - 1, 1 \leq q_{\alpha} \leq m_{\alpha}, 1 \leq q_{\beta} \leq m_{\beta}, 1 \leq p_{\alpha} \leq d_{\alpha}, \) and \( 1 \leq p_{\beta} \leq d_{\beta} \).

To this end, we compute:

\[
\langle \xi(\alpha, q_{\alpha}, p_{\alpha})| X^{-1}|\xi(\beta, q_{\beta}, p_{\beta})\rangle = \sum_{\alpha' \vdash d} \sum_{\mu = \alpha' + \square} x^{-1}_{\mu, \alpha'} \text{tr} \left[ (P_{\mu} \otimes \mathbb{1}_{B}) \mathcal{Q}_{\alpha'} \left( \Phi_{A_1B}^+ \otimes |\beta, q_{\beta}, p_{\beta}\rangle \langle \alpha, q_{\alpha}, p_{\alpha}|_{A_i^\prime} \right) \right]
\]

(4.39)

\[
= \sum_{\alpha' \vdash d} \sum_{\mu = \alpha' + \square} x^{-1}_{\mu, \alpha'} \text{tr} \left[ (P_{\mu} \otimes \mathbb{1}_{B}) \left( \Phi_{A_1B}^+ \otimes P_{\alpha'} |\beta, q_{\beta}, p_{\beta}\rangle \langle \alpha, q_{\alpha}, p_{\alpha}|_{A_i^\prime} \right) \right]
\]

(4.40)
\begin{align}
\frac{1}{d} \sum_{\mu=\beta+1} x_{\mu,\beta}^{-1} \text{tr} \left[ P_{\mu} \left( \mathbb{1}_{A_1} \otimes |\beta, \tilde{q}_\beta, \tilde{p}_\beta\rangle \langle \alpha, q_\alpha, p_\alpha |A_1^c \right) \right] \\
= \frac{1}{d} \sum_{\mu=\beta+1} x_{\mu,\beta}^{-1} \text{tr} \left[ \text{tr}_{A_1} (P_{\mu}) |\beta, \tilde{q}_\beta, \tilde{p}_\beta\rangle \langle \alpha, q_\alpha, p_\alpha |A_1^c \right] \\
= d^{N-1} \left( \sum_{\mu'=\beta+1} \sqrt{m_{\mu'} d_{\mu'}} \right)^{-1} \sum_{\mu=\beta+1} \frac{\sqrt{d_{\mu} m_{\mu}}}{\sqrt{m_{\mu}}} \delta_{\alpha,\beta} \delta_{q_\alpha,\tilde{q}_\alpha} \delta_{p_\alpha,\tilde{p}_\alpha} \\
= d^{N-1} \delta_{\alpha,\beta} \delta_{q_\alpha,\tilde{q}_\alpha} \delta_{p_\alpha,\tilde{p}_\alpha},
\end{align}

where step (4.40) uses (4.20), step (4.41) uses the identity \( P_{\mu'} |\beta, \tilde{q}_\beta, \tilde{p}_\beta\rangle A_1^c = \delta_{\alpha',\beta} |\beta, \tilde{q}_\beta, \tilde{p}_\beta\rangle A_1^c \) and a partial trace over \( B \), and step (4.43) uses Lemma 2, the formula (4.35) for \( x_{\mu,\beta} \), and another application of \( P_{\mu'} |\beta, \tilde{q}_\beta, \tilde{p}_\beta\rangle A_1^c \).

The above calculation proves (4.38), and thus \( X \geq \rho_1 \) follows from Lemma 1. Hence, \( X \) is feasible in the dual program (3.6), which concludes the proof of optimality of the pretty good measurement for the PBT protocol with \( N \) maximally entangled states.

### 5 Fully optimized protocol

We now turn our attention to the fully optimized PBT protocol. In this case, we seek to find a port state \( \phi_{ANB_N} \) and POVM \( E = \{ E_i \}_{i=1}^N \) such that the entanglement fidelity \( F(\Lambda) \) for the corresponding teleportation channel \( \Lambda \) defined in (3.1) is maximized.

The port state \( \phi_{ANB_N} \) in a PBT protocol can always be assumed to be pure [8, 21]. Fixing the marginal \( \phi_{AN} \) on \( AN \), we further assume without loss of generality that \( |\phi\rangle_{ANB_N} \) is the "canonical" purification of \( \phi_{AN} \),

\begin{align}
|\phi\rangle_{ANB_N} = (O_{AN} \otimes I_{B^N}) |\Phi^+\rangle \otimes |AB\rangle,
\end{align}

where the positive semidefinite operator \( O_{AN} = \sqrt{d^N \phi_{AN}} \) satisfies \( \text{tr} O_{AN}^2 = d^N \). According to Sect. 3, PBT using the state \( \phi_{ANB_N} \) is equivalent to discriminating the states

\begin{align}
\eta_i = \text{tr}_{B_i^c} \phi_{ANB_N} = O_{AN} \left( \phi_{A_i B_i}^+ \otimes \pi_{A_i^c} \right) O_{AN}^\dagger,
\end{align}

each drawn uniformly at random with probability \( \frac{1}{N} \).

We saw in Sect. 4 that the states \( \rho_i = \text{tr}_{B_i^c} \left( \phi_{AB}^+ \right) \otimes |AB\rangle \) have \( U^\otimes N \otimes \tilde{U} \) and \( S_{N-1} \) symmetries, which facilitated the calculation of the entanglement fidelity of the corresponding PBT protocol. Majenz [21] showed that these symmetries can always be assumed in an arbitrary PBT protocol (see also the extended discussion in [8, 21]).

\[\text{Any two purifications of } \phi_{AN} \text{ on } A^N B^N \text{ are related by an isometry acting on } B^N, \text{ so we may assume that Bob applies a suitable isometry on } B^N \text{ to obtain the state in (5.1) before starting the protocol. The entanglement fidelity of the resulting protocol will be no worse than the original one.}\]
Sect. 3.3). More precisely, we may assume without loss of generality that $\phi_{AN}$ (or equivalently, $\phi_{BN}$) is a symmetric Werner state, which implies the following symmetries for $O_{AN} = \sqrt{d^N} \phi_{AN}$:

\[
\begin{align*}
\left[U^{\otimes N}, O_{AN}\right] &= 0 \quad \text{for all } U \in U_d, \\
\left[\pi, O_{AN}\right] &= 0 \quad \text{for all } \pi \in S_N.
\end{align*}
\]  

(5.3)  

(5.4)

We conclude that similar to Sect. 4, the states $\eta_i$ on $A^N B$ defined in (5.2) satisfy

\[
\begin{align*}
\left[U^{\otimes N} \otimes \bar{U}, \eta_i\right] &= 0 \quad \text{for all } U \in U_d, \\
\left[\varphi \otimes 1_{A_i B}, \eta_i\right] &= 0 \quad \text{for all } \varphi \in S_{N-1}, \\
\pi \eta_i \pi^\dagger &= \eta_{\pi(i)} \quad \text{for all } \pi \in S_N,
\end{align*}
\]  

(5.5)  

(5.6)  

(5.7)

where in (5.6), the action of $S_{N-1}$ is defined on $A_i^c$. Mozrzymas et al. [24] showed that the entanglement fidelity of the fully optimized PBT protocol is given by the expression

\[
F(A) = \frac{1}{d^{N+2}} \max_{\{c_\mu\}} \sum_{\alpha^d N - 1} \left( \sum_{\mu = \alpha + \Box} \sqrt{c_\mu d_\mu m_{d, \mu}} \right)^2,
\]  

(5.8)

where the non-negative coefficients $\{c_\mu\}_{\mu^d N}$ satisfy

\[
\sum_{\mu^d N} c_\mu d_\mu m_{d, \mu} = d^N.
\]  

(5.9)

We will rederive (5.8) in this section. Somewhat surprisingly, it will turn out that the same pretty good measurement as used in Sect. 4 maximizes the success probability of distinguishing the states $\eta_i$, and hence also achieves the optimal value (5.8) for the entanglement fidelity via (3.7).

### 5.1 Performance of the pretty good measurement

We consider again the pretty good measurement $E = \{E_i\}_{i=1}^N$ with $E_i = \tilde{\rho}^{-1/2} \rho_i \tilde{\rho}^{-1/2}$, defined in terms of the states $\rho_i$ given in (4.2). These states differ from the $\eta_i$ in (5.2) above by the conjugation with the operator $O_{AN}$. We stress that $E$ is not the pretty good measurement defined in terms of the states $\eta_i$, which would be a sub-optimal choice.

The success probability of distinguishing the state ensemble $\{(\frac{1}{N}, \eta_i)\}_{i=1}^N$ with the pretty good measurement $E = \{E_i\}_{i=1}^N$ is equal to

\[
p_{\text{succ}} = \frac{1}{N} \sum_{i=1}^N \text{tr} (\eta_i E_i) = \frac{1}{N} \sum_{i=1}^N \text{tr} \left( O_{AN} \rho_i \tilde{O}_{AN}^\dagger \tilde{\rho}^{-1/2} \rho_i \tilde{\rho}^{-1/2} \right),
\]  

(5.10)
where we inserted \( \eta_i = O_A \rho_i O_A^\dagger \). In analogy to Sect. 4, we define an operator

\[
Y = \sum_{i=1}^{N} O_A \rho_i O_A^\dagger \rho^{-1/2} \rho_i \rho^{-1/2},
\]

(5.11)
satisfying \( \frac{1}{N} \text{tr} \ Y = p_{\text{succ}} \). Due to the symmetries of the states \( \rho_i \) (eqs. (4.3) to (4.5)), the state \( \rho \) (eqs. (4.6) and (4.7)), the operator \( O_A \) (eqs. (5.3) and (5.4)), and the states \( \eta_i \) (eqs. (5.5) to (5.7)), we infer that \( Y \) has the following symmetries:

\[
\begin{align*}
\left[ U^\otimes N \otimes \tilde{U}, Y \right] & = 0 \quad \text{for all } U \in U_d, \quad (5.12) \\
\left[ \pi \otimes 1_B, Y \right] & = 0 \quad \text{for all } \pi \in S_N, \quad (5.13)
\end{align*}
\]
such that we can again write \( Y \) in the form

\[
Y = \bigoplus_{\alpha \vdash d N - 1} \bigoplus_{\mu = \alpha + \Box}^\mu y_{\mu, \alpha} \mathbf{1}_{V_{\alpha}^d} \otimes \mathbf{1}_{W_{\mu}}. \quad (5.14)
\]

In the following, we determine the value of \( \text{tr} \ Y \) and a formula for the coefficients \( y_{\mu, \alpha} \) appearing in (5.14). We again abbreviate \( m_{\mu} \equiv m_{d, \mu} \) for the dimension of the Weyl module \( V_{\mu}^d \). As before, we denote by \( P_{\mu} \) for \( \mu \vdash d N - 1 \) the isotypical projection for the \( U_d \) action by \( U \otimes N \otimes \tilde{U} \) as defined via decomposition (4.8), and by \( P_{\alpha}' \) for \( \alpha \vdash d N - 1 \) the isotypical projection with respect to the action of \( U_{d, 1} \) by \( U \otimes N - 1 \).

We first use the \( U \otimes N \) and \( S_N \) symmetries of \( O_A \) (eqs. (5.3) and (5.4)) to write it as

\[
O_A \equiv \bigoplus_{\mu \vdash d N} \sqrt{c_{\mu}} \mathbf{1}_{V_{\mu}^d} \otimes \mathbf{1}_{W_{\mu}}, \quad (5.15)
\]

where \( \{ c_{\mu} \}_{\mu \vdash d N} \) are non-negative coefficients (recall that \( O_A \equiv \sqrt{d N \phi_{A N}} \) is positive semidefinite). Since \( \text{tr} \ O_A^2 = d^N \), we have \( \sum_{\mu \vdash d N} c_{\mu} d_{\mu} = d^N \), which is precisely the condition (5.9) for the coefficients \( c_{\mu} \) in the expression (5.8) for the entanglement fidelity.

We are now ready to compute the trace of \( Y \). By symmetry, and using the expressions for \( \rho \) from Lemma 3 and for \( O_A \) in (5.15), we have

\[
\text{tr} \left[ Y \left( P_{\mu} \otimes 1_B \right) Q_{\alpha} \right] = N \text{tr} \left[ O_A \rho_1 O_A^\dagger \rho^{-1/2} \rho_1 \rho^{-1/2} \left( P_{\mu} \otimes 1_B \right) Q_{\alpha} \right] \quad (5.16)
\]

\[
= \frac{N}{d^{2N - 2}} \sum_{\alpha', \alpha'' \vdash d N - 1} \sum_{\mu = \alpha' + \Box} \sum_{\mu = \alpha'' + \Box} \sum_{\mu = \alpha' + \Box} \frac{d_{\mu}}{d_{\mu, \alpha, \alpha''}} \frac{d_{\mu}}{d_{\mu, \alpha, \alpha''}} \sqrt{c_{\lambda_{\alpha'}} c_{\lambda_{\alpha''}}}
\]

5 In analogy to the discussion about the operator \( X \) in Sect. 4, one can show that the coefficients \( y_{\mu, i} \) defined with respect to the decomposition (4.8) vanish whenever \( \mu - \varepsilon_i \) does not correspond to a Young diagram \( \alpha \vdash d N - 1 \).
\( \times \text{tr} \left[ (P_{\alpha'} \otimes 1_B) \Phi_{A_1B}^+ (P_{\alpha'} \otimes 1_B) (P_{\mu'} \otimes 1_B) Q_{\alpha'} \Phi_{A_1B}^+ (P_{\mu'} \otimes 1_B) Q_{\alpha'} (P_{\mu} \otimes 1_B) Q_{\alpha} \right] \) 
\( = \frac{N}{d^{2N-2}} r_{\alpha,\alpha}^{1/2} \sqrt{c_{\mu}} \sum_{\mu' = \alpha + \square} r_{\mu',\alpha}^{1/2} \sqrt{c_{\mu'}} \text{tr} \left[ \Phi_{A_1B}^+ (P_{\mu'} \otimes 1_B) \Phi_{A_1B}^+ (P_{\mu'} \otimes 1_B) (I_{A_1B} \otimes P_{\alpha'}) \right] \) 
\( = \frac{N}{d^{2N-2}} r_{\alpha,\alpha}^{1/2} \sqrt{c_{\mu}} \sum_{\mu' = \alpha + \square} r_{\mu',\alpha}^{1/2} \sqrt{c_{\mu'}} \text{tr} \left[ \text{tr} A_1 (P_{\mu'}) \text{tr} A_1 (P_{\mu'}) P_{\alpha'} \right] \) 
\( = \frac{1}{d^N} \sqrt{c_{\mu} m_{\mu d_{\mu}}} \sum_{\mu' = \alpha + \square} \sqrt{c_{\mu'} m_{\mu' d_{\mu'}}} = \frac{1}{d^N} \sqrt{c_{\mu} m_{\mu d_{\mu}}} \sum_{\mu' = \alpha + \square} \sqrt{c_{\mu'} m_{\mu' d_{\mu'}}} \) 

In step (5.18), we used (4.20) for the terms \( \Phi_{A_1B}^+ Q_{\alpha} \) and orthogonality among the projectors \( P_{\alpha} \) and \( P_{\alpha'} \), respectively, and in step (5.20), we again used Lemma 2 in the same way as in Sect. 4.

The trace of \( Y \) is obtained by summing (5.21) over \( \alpha \vdash_d N - 1 \) and \( \mu = \alpha + \square \), giving 
\( \text{tr} Y = \sum_{\alpha \vdash_d N - 1} \sum_{\mu = \alpha + \square} \text{tr} \left[ Y (P_{\mu} \otimes 1_B) Q_{\alpha} \right] \) 
\( = \frac{1}{d^N} \sum_{\alpha \vdash_d N - 1} \left( \sum_{\mu = \alpha + \square} \sqrt{c_{\mu} m_{\mu d_{\mu}}} \right)^2 \) 

Maximizing (5.23) over all non-negative coefficients \( \{ c_{\mu} \}_{\mu \vdash_d N} \) satisfying \( \sum_{\mu \vdash_d N} c_{\mu} m_{\mu d_{\mu}} = d^N \) and using (3.7) together with \( p_{\text{succ}} = \frac{1}{N} \text{tr} Y \) now proves that the entanglement fidelity of the PBT protocol \( (\phi_{A_1B}^{N}, E) \) is given by formula (5.8) derived in [24]. Here, \( \phi_{A_1B}^{N} \) is defined via (5.1) and (5.15), and the pretty good measurement \( E = \{ E_i \}_{i=1}^N \) is defined in terms of the states \( \rho_i \) as given in (4.2).

It remains to determine the coefficients \( y_{\mu,\alpha} \) appearing in (5.14). By definition, for Young diagrams \( \alpha \vdash_d N - 1 \) and \( \mu = \alpha + \square \),
\( \text{tr} \left[ Y (P_{\mu} \otimes 1_B) Q_{\alpha} \right] = y_{\mu,\alpha} m_{\alpha d_{\mu}} \).
This is equal to (5.24) by the above calculation, leading to the following formula for the \( y_{\mu,\alpha} \):
\( y_{\mu,\alpha} = \frac{1}{d^N} \frac{1}{m_{\alpha d_{\mu}}} \sqrt{c_{\mu} m_{\mu d_{\mu}}} \sum_{\mu' = \alpha + \square} \sqrt{c_{\mu'} m_{\mu' d_{\mu'}}} \)

We stress that in expression (5.23) the port state \( \phi_{A_1B}^{N} \) is optimized over via the coefficients \( \{ c_{\mu} \}_{\mu \vdash_d N} \), while the POVM is fixed to be the pretty good measurement \( E \) discriminating the states \( \rho_i \) in (4.2). We show in the next section that this measurement
$E$ is in fact optimal for any given port state $\phi_{AN}B^N$ defined via (5.1), (5.15), and the coefficients $\{c_\mu\}_{\mu=dN}$, which also proves optimality of $E$ for the optimal such $\phi_{AN}B^N$.

### 5.2 Optimality of the pretty good measurement

It remains to show that the choice of the pretty good measurement $E$ associated with $\{(\frac{1}{N}, \rho_i)\}_{i=1}^N$ achieves the optimal success probability of discriminating the state ensemble $\{(\frac{1}{N}, \eta_i)\}_{i=1}^N$. To prove this, we follow a similar strategy as in Sect. 4: Once we establish that the operator $1_{AN}Y$ with $Y$ as defined in (5.11) is feasible for the dual program (3.6), optimality follows immediately from weak duality.

Feasibility of $1_{AN}Y$ is equivalent to $Y \geq \eta_i$ for all $i = 1, \ldots, N$, where $\eta_i = O_{AN} \rho_i O_{AN}$ with

$$O_{AN} = \bigoplus_{\mu=dN} \sqrt{c_\mu} 1_{V_\mu} \otimes 1_{W_\mu}. \quad (5.26)$$

By symmetry, it suffices to show that $Y \geq \eta_1$, for which we once more make use of Lemma 1. First, we recall the expression (5.14) for the operator $Y$, which together with formula (5.25) for the coefficients $y_{\mu,\alpha}$ shows that $Y$ is positive semidefinite (recall that $c_\mu \geq 0$ for all $\mu \vdash dN$). As the collection of vectors in Lemma 1, we choose

$$|\chi(\alpha, q_\alpha, p_\alpha)\rangle := (O_{AN} \otimes 1_{B}) (|\Phi^+\rangle_{A_1B} \otimes |\alpha, q_\alpha, p_\alpha\rangle_{A^c_1}) \quad (5.27)$$

for $\alpha \vdash dN - 1$, $1 \leq q_\alpha \leq m_\alpha$, and $1 \leq p_\alpha \leq d_\alpha$, where $|\alpha, q_\alpha, p_\alpha\rangle_{A^c_1}$ is the Schur basis on $A^c_1$ (see Sect. 4.2) and $O_{AN}$ is the operator in (5.26). Because of the spectral decomposition (4.37) of $\rho_1$ and (5.27), we have

$$\eta_1 = O_{AN} \rho_1 O_{AN} = \frac{1}{dN-1} \sum_{\alpha \vdash dN-1} \sum_{q_\alpha, p_\alpha} |\chi(\alpha, q_\alpha, p_\alpha)\rangle \langle \chi(\alpha, q_\alpha, p_\alpha)|, \quad (5.28)$$

so that $Y \geq \eta_1$ will follow from Lemma 1 once we establish that

$$\langle \chi(\alpha, q_\alpha, p_\alpha)|Y^{-1}\chi(\beta, \tilde{q}_\beta, \tilde{p}_\beta)\rangle$$

$$= \left(\langle \Phi^+\rangle_{A_1B} \otimes \langle \alpha, q_\alpha, p_\alpha|_{A^c_1}\right) O_{AN} Y^{-1} O_{AN} \left(\langle \Phi^+\rangle_{A_1B} \otimes |\beta, \tilde{q}_\beta, \tilde{p}_\beta\rangle_{A^c_1}\right)$$

$$= \delta_{\alpha,\beta} \delta_{q_\alpha, \tilde{q}_\beta} \delta_{p_\alpha, \tilde{p}_\beta} d^{N-1} \quad (5.29)$$

holds for all $\alpha, \beta \vdash dN - 1$, $1 \leq q_\alpha \leq m_\alpha$, $1 \leq \tilde{q}_\beta \leq m_\beta$, $1 \leq p_\alpha \leq d_\alpha$, and $1 \leq \tilde{p}_\beta \leq d_\beta$.

To this end, we first observe that

$$O_{AN} Y^{-1} O_{AN} = \bigoplus_{\alpha \vdash dN-1} \bigoplus_{\mu = \alpha+\square} c_{\mu} y_{\mu,\alpha}^{-1} 1_{V_\mu} \otimes 1_{W_\mu}. \quad (5.31)$$
We then compute:

\[
\langle \chi(\alpha, q_\alpha, p_\alpha) | Y^{-1} | \chi(\beta, q_\beta, p_\beta) \rangle
= \sum_{\alpha' \vdash d N - 1} \sum_{\mu = \alpha' + \square} c_\mu^{-1} y_{\alpha, \alpha'}^{-1} \text{tr} \left[ (P_\mu \otimes 1_B) Q_{\alpha'} \left( \Phi_{A_1 B}^+ | \beta, q_\beta, p_\beta \rangle \langle \alpha, q_\alpha, p_\alpha | A_1^c \right) \right]
\]

(5.32)

\[
= \frac{1}{d} \sum_{\mu = \beta + \square} c_\mu^{-1} y_{\mu, \beta}^{-1} \text{tr} \left[ \text{tr}_{A_1} (P_\mu \beta, q_\beta, p_\beta \rangle \langle \alpha, q_\alpha, p_\alpha | A_1^c \right) \right]
\]

(5.33)

\[
= d^{N-1} \left( \sum_{\mu' = \beta + \square} \sqrt{c_\mu m_\mu d_\mu} \right)^{-1} \sum_{\mu' = \beta + \square} \frac{c_\mu m_\mu d_\mu}{\sqrt{c_\mu m_\mu d_\mu}} m_\mu \delta_{\alpha, \beta} \delta_{q_\alpha, q_\alpha} \delta_{p_\alpha, p_\alpha}
\]

(5.34)

\[
= d^{N-1} \delta_{\alpha, \beta} \delta_{q_\alpha, q_\alpha} \delta_{p_\alpha, p_\alpha}
\]

(5.35)

where we used similar arguments as in Sect. 4.2, and the expression (5.25) for the coefficients \( y_{\mu, \beta} \) in step (5.34).

This proves (5.30), so that \( Y \geq \eta_1 \) follows from Lemma 1. Hence, \( \frac{1}{N} Y \) is feasible in the dual program (3.6), which proves that the pretty good measurement from Sect. 4 optimally distinguishes the states \( \eta_i \) defined in (5.2) in terms of an arbitrary set of non-negative coefficients \( \{c_\mu\}_{\mu = d N} \) satisfying \( \sum_{\mu = d N} m_\mu d_\mu = d^N \). We showed above that the optimal success probability of this discrimination problem as a function of \( \{c_\mu\}_{\mu = d N} \) is equal to (5.23). Optimizing over the coefficients \( \{c_\mu\}_{\mu = d N} \) and using (3.7) then leads to the expression (5.8) for the entanglement fidelity of the fully optimized PBT protocol.

### 6 Discussion

In this paper, we proved that the pretty good measurement is optimal for PBT protocols using maximally entangled states. Furthermore, we showed that the very same measurement also achieves the optimal entanglement fidelity for arbitrary port states once the natural symmetries of PBT have been imposed without loss of generality. We stress once again that for the second result the pretty good measurement is not derived from the optimal port state (see Sect. 3 for how to obtain the state discrimination problem from a given port state), but instead from \( N \) maximally entangled states.

In the course of proving optimality of the pretty good measurement, we also re-derived the representation-theoretic formulas for the entanglement fidelity of PBT protocols using maximally entangled states [35] and using an optimized port state [24]. In order to better distinguish the two settings, we adopt the notation of [8] and write \( F^\text{std}_d(N) \) and \( F^*_d(N) \) for the entanglement fidelity in each case, respectively.\(^6\) This notation makes the dependence of \( F \) on the local dimension \( d \) and the number of ports \( N \) explicit, and it highlights the assumption of fixed but arbitrary \( d \) and varying \( N \) made in this paper as well as in [8].

\(^6\) In [8], the PBT protocol based on \( N \) maximally entangled states and the associated pretty good measurement is called the standard protocol.
In Sect. 4, we rederived the following result from [35]:

\[ F_{\text{std}}^d (N) = \frac{1}{d^{N+2}} \sum_{\alpha \vdash d N} \left( \sum_{\mu = \alpha + \Box} \sqrt{d_{\mu} m_{\mu}} \right)^2. \]  

(6.1)

Ishizaka and Hiroshima [15] (see also [5]) proved that \( F_{\text{std}}^d (N) \geq 1 - \frac{d^2 - 1}{4N} + O(N^{-3/2 + \delta}) \), which shows that the PBT protocol becomes perfect in the limit \( N \to \infty \) for fixed \( d \). One of the main goals of [8] was to determine the exact first-order coefficient of this convergence. We showed in [8] that for any \( \delta > 0 \),

\[ F_{\text{std}}^d (N) = 1 - \frac{d^2 - 1}{4N} + O(N^{-3/2 + \delta}). \]  

(6.2)

For optimal PBT, we rederived in Sect. 5 the following expression for the entanglement fidelity first proved in [24]:

\[ F_{\ast}^d (N) = \frac{1}{d^{N+2}} \max_{\{c_\mu\}_{\mu \vdash d N}} \sum_{\alpha \vdash d N-1} \left( \sum_{\mu = \alpha + \Box} \sqrt{c_\mu m_\mu d_\mu} \right)^2, \]  

(6.3)

where the non-negative coefficients \( \{c_\mu\}_{\mu \vdash d N} \) satisfy \( \sum_{\mu \vdash d N} c_\mu m_\mu d_\mu = d^N \). Equation (6.3) bears a striking resemblance with (6.1), and the additional optimization over coefficients \( \{c_\mu\}_{\mu \vdash d N} \) corresponds to the optimization over the port state (see Sect. 5 for details). Ishizaka [17] proved the upper bound \( F_{\ast}^d (N) \leq 1 - c_d N^{-2} + O(N^{-3}) \) with \( c_d = (4(d - 1))^{-1} \), which was improved by Majenz [21] (see also [8]) to \( c_d = (d^2 - 1)/8 \) whenever \( N > \frac{d^2}{2} \). However, prior to our work [8], it was not clear whether there are protocols achieving the \( N^{-2} \) scaling asymptotically. In [8], we exhibited a protocol with such a scaling in \( N \), albeit with non-matching coefficients in \( d \). This resulted in the asymptotic expansion

\[ F_{\ast}^d (N) = 1 - \Theta(N^{-2}), \]  

(6.4)

where \( f = \Theta(g) \) means that both \( f = O(g) \) and \( g = O(f) \). It remains a challenging open problem to determine the exact coefficient of \( N^{-2} \) as a function of \( d \) in (6.4). Moreover, an investigation of (6.3) in the interesting limit \( N, d \to \infty \) with \( N/d^2 \) fixed has yet to be carried out.

In this paper, we only discussed the “deterministic” variant of PBT, in which the protocol gives an output state that approximates the target state. In “probabilistic” PBT, the protocol yields an exact copy of the target state, but only succeeds with a certain success probability [15, 16]. A description of this probability in terms of representation-theoretic data was obtained in [24, 35], along with converse bounds [30] and asymptotic expansions [8, 24]. It should be a stimulating exercise to apply the techniques of [8] and the present paper to rederive the results on probabilistic PBT.
proved in [24, 35]. Moreover, a “multi-port” generalization of PBT was recently proposed in [19, 26, 36], and the methods employed here could potentially be applied to study this generalized setting as well. Finally, it would be interesting to derive expressions for the optimal entanglement fidelity in the case of noisy maximally entangled states, e.g., when each maximally entangled state is shared between Alice and Bob via a noisy quantum channel.

Acknowledgements I would like to thank Christian Majenz, Connor Paul-Paddock, and Michael Walter for valuable discussions and helpful feedback. I am also grateful to the anonymous referee for useful comments on an earlier version of this manuscript, and permission to reproduce their proof of Lemma 1. This research was partially funded through the Army Research Lab CDQI program.

Declarations

Conflict of interest. The corresponding author states that there is no conflict of interest.

A Proof of Lemma 1

In this appendix, we give a proof of Lemma 1, which is restated below for convenience. For a positive semidefinite operator $X$, the generalized inverse $X^{-1}$ and the orthogonal projection $\Pi_X$ onto $\text{supp} X$ are defined as in Sect. 2. Note that $\text{supp} X = (\ker X)^\perp = \text{im} X$ for positive semidefinite $X$.

**Lemma 1** (restated) Let $X$ be a positive semidefinite operator on a Hilbert space $\mathcal{H}$. For some $K \in \mathbb{N}$ and $c \in \mathbb{R}$ let $\{ |\xi_k\rangle \}_{k=1}^K \subset \text{im}(X)$ be a collection of nonzero vectors such that $\langle \xi_j | X^{-1} | \xi_k \rangle = \delta_{j,k} c$ for $1 \leq j, k \leq K$. Then, $c > 0$ and

$$X \geq \frac{1}{c} \sum_{k=1}^K |\xi_k\rangle \langle \xi_k|.$$  \hfill (A.1)

**Proof** We prove this lemma by induction on $K$.

Let first $K = 1$. Recall that $\Pi_X |\xi\rangle = |\xi\rangle$ by assumption, and $\Pi_X = \sqrt{X} \sqrt{X^{-1}}$ by the definitions of the square root and generalized inverse of $X$. For any $|\psi\rangle \in \mathcal{H}$,

$$\langle \psi | \xi \rangle \langle \xi | \psi \rangle = |\langle \psi | \xi \rangle|^2 = |\langle \psi | \Pi_X |\xi\rangle|^2 = |\langle \psi | \sqrt{X} \sqrt{X^{-1}} |\xi\rangle|^2 \leq \langle \psi | X |\psi\rangle \langle \xi | X^{-1} |\xi\rangle \leq \frac{1}{c} |\xi\rangle \langle \xi| \leq X$$

where (A.3) follows from the Cauchy-Schwarz inequality. Then $|\xi\rangle \langle \xi| \leq cX$ holds since $|\psi\rangle \in \mathcal{H}$ was arbitrary. Taking traces on both sides of this operator inequality and using $|\xi\rangle \neq 0$ and $X \geq 0$ shows $c > 0$, from which the induction base case follows.

Let now $K > 1$. Applying the argument above to $|\xi_K\rangle$ shows that $Y := X - c^{-1} |\xi_K\rangle \langle \xi_K|$ is positive semidefinite. In order to use the induction hypothesis, we...
need to verify that (a) $|\xi_j\rangle \in \text{im}(Y)$ for $1 \leq j \leq K - 1$ and (b) $\langle \xi_j|Y^{-1}|\xi_k\rangle = \delta_{j,k}$ for $1 \leq j, k \leq K - 1$.

To show (a), observe that for any $1 \leq j \leq K - 1$,

$$YX^{-1}|\xi_j\rangle = \left(X - \frac{1}{c}|\xi_K\rangle\langle\xi_K|\right)X^{-1}|\xi_j\rangle = XX^{-1}|\xi_j\rangle - \frac{1}{c}|\xi_K\rangle\langle\xi_K|X^{-1}|\xi_j\rangle = \Pi_X|\xi_j\rangle = |\xi_j\rangle,$$

(A.5)

since $\langle\xi_K|X^{-1}|\xi_j\rangle = 0$ and $|\xi_j\rangle \in \text{im}(X)$ for $1 \leq j \leq K - 1$ by assumption.

To show (b), we apply $Y^{-1}$ to both sides of (A.5), giving

$$Y^{-1}|\xi_j\rangle = Y^{-1}YX^{-1}|\xi_j\rangle = \Pi_Y X^{-1}|\xi_j\rangle.$$

(A.6)

Taking the inner product with any $|\xi_k\rangle$ for $1 \leq k \leq K - 1$ and using (a) then shows that

$$\langle\xi_k|Y^{-1}|\xi_j\rangle = \langle\xi_k|\Pi_Y X^{-1}|\xi_j\rangle = \langle\xi_k|X^{-1}|\xi_j\rangle = \delta_{j,k}c.$$

(A.7)

We may therefore apply the induction hypothesis to $Y$ and the vectors $\{|\xi_j\rangle\}_{j=1}^{K-1}$, giving

$$Y = X - \frac{1}{c}|\xi_K\rangle\langle\xi_K| \geq \frac{1}{c} \sum_{j=1}^{K-1} |\xi_j\rangle\langle\xi_j|.$$

(A.8)

Rearranging this inequality yields the assertion of Lemma 1. □

References

1. Bacon, D., Chuang, I.L., Harrow, A.W.: Efficient quantum circuits for Schur and Clebsch-Gordan transforms. Phys. Rev. Lett. 97(17), 170502 (2006). arXiv:quant-ph/0407082
2. Belavkin, V.P.: Optimal multiple quantum statistical hypothesis testing. Stoch.: Int. J. Probab. Stoch. Process. 1(1–4), 315–345 (1975)
3. Bennett, C.H., Brassard, G., Crépeau, C., Jozsa, R., Peres, A., Wootters, W.K.: Teleporting an unknown quantum state via dual classical and Einstein–Podolsky–Rosen channels. Phys. Rev. Lett. 70(13), 1895–1899 (1993)
4. Barnum, H., Knill, E.: Reversing quantum dynamics with near-optimal quantum and classical fidelity. J. Math. Phys. 43(5), 2097–2106 (2002). arXiv:quant-ph/0004088
5. Beigi, S., König, R.: Simplified instantaneous non-local quantum computation with applications to position-based cryptography. N. J. Phys. 13(9), 093036 (2011). arXiv:1101.1065 [quant-ph]
6. Buhrman, H., et al.: Quantum communication complexity advantage implies violation of a Bell inequality. Proc. Natl. Acad. Sci. 113(12), 3191–3196 (2016). arXiv:1502.01058 [quant-ph]
7. Christandl, M., König, R., Mitchison, G., Renner, R.: One-and-a-half quantum de Finetti theorems. Commun. Math. Phys. 273(2), 473–498 (2007). arXiv:quant-ph/0602130
8. Christandl, M., Leditzky, F., Majenz, C., Smith, G., Speelman, F., Walter, M.: Asymptotic performance of port-based teleportation. Commun. Math. Phys. 381(1), 379–451 (2021). arXiv:1809.10751 [quant-ph]
9. Christandl, M.: The structure of bipartite quantum states—insights from group theory and cryptography. Ph.D. thesis. University of Cambridge (2006). arXiv:quant-ph/0604183
10. Dolev, K., Cree, S.: Non-local computation of quantum circuits with small light cones. arXiv preprint (2022). arXiv:2203.10106 [quant-ph]
11. Fulton, W.: Young Tableaux: With Applications to Representation Theory and Geometry, vol. 35. Cambridge University Press, Cambridge (1997)
12. Harrow, A.W.: Applications of coherent classical communication and the Schur transform to quantum information theory. Ph.D. thesis. Massachusetts Institute of Technology (2005). arXiv:quant-ph/0512255
13. Holevo, A.S.: On asymptotically optimal hypothesis testing in quantum statistics. Theory Probab. Appl. 23(2), 411–415 (1979)
14. Hausladen, P., Wootters, W.K.: A ‘pretty good’ measurement for distinguishing quantum states. J. Mod. Opt. 41(12), 2385–2390 (1994)
15. Ishizaka, S., Hiroshima, T.: Asymptotic teleportation scheme as a universal programmable quantum processor. Phys. Rev. Lett. 101(24), 240501 (2008). arXiv:0807.4568 [quant-ph]
16. Ishizaka, S., Hiroshima, T.: Quantum teleportation scheme by selecting one of multiple output ports. Phys. Rev. A. 79(4), 042306 (2009). arXiv:0901.2975 [quant-ph]
17. Ishizaka, S.: Some remarks on port-based teleportation. arXiv preprint (2015). arXiv:1506.01555 [quant-ph]
18. Knill, E., Laflamme, R., Milburn, G.J.: A scheme for efficient quantum computation with linear optics. Nature 409(6816), 46–52 (2001)
19. Kopszak, P., Mozrzymas, M., Studziński, M., Horodecki, M.: Multiport based teleportation-transmission of a large amount of quantum information. Quantum 5, 576 (2021). arXiv:2008.00856 [quant-ph]
20. Lewenstein, M., Sanpera, A.: Separability and entanglement of composite quantum systems. Phys. Rev. Lett. 80(11), 2261 (1998). arXiv:quant-ph/9707043
21. Majenz, C.: Entropy in Quantum Information Theory – Communication and Cryptography. Ph.D. thesis. University of Copenhagen (2018). arXiv:1810.10436 [quant-ph]
22. May, A.: Quantum tasks in holography. J. High Energy Phys. 2019(10), 1–39 (2019). arXiv:1902.06845 [hep-th]
23. May, A.: Complexity and entanglement in non-local computation and holography. arXiv preprint (2022). arXiv:2204.00908 [quant-ph]
24. Mozrzymas, M., Studziński, M., Strelchuk, S., Horodecki, M.: Optimal port-based teleportation. N. J.Phys. 20(5), 053006 (2018). arXiv:1707.08456 [quant-ph]
25. Mozrzymas, M., Studziński, M., Horodecki, M.: A simplified formalism of the algebra of partially transposed permutation operators with applications. J. Phys. A: Math. Theor. 51(12), 125202 (2018). arXiv:1708.02434 [quant-ph]
26. Mozrzymas, M., Studziński, M., Kopszak, P.: Optimal multi-port-based teleportation schemes. Quantum 5, 477 (2021). arXiv:2011.09256 [quant-ph]
27. Nielsen, M.A., Chuang, I.L.: Programmable quantum gate arrays. Phys. Rev. Lett. 79(2), 321 (1997). arXiv:quant-ph/9703032
28. Pereira, J., Banchi, L., Pirandola, S.: Characterising port-based teleportation as universal simulator of qubit channels. J. Phys. A: Math. Theor. 54(20), 205301 (2021). arXiv:1912.10374 [quant-ph]
29. Pirandola, S., Laurenza, R., Lupo, C., Pereira, J.L.: Fundamental limits to quantum channel discrimination. npj Quantum Inf. 5(1), 1–8 (2019). arXiv:1803.02834 [quant-ph]
30. Pitalúa-García, D.: Deduction of an upper bound on the success probability of port-based teleportation from the no-cloning theorem and the no-signaling principle. Phys. Rev. A. 87(4), 040303 (2013). arXiv:1206.4836 [quant-ph]
31. Pereira, J.L., Pirandola, S.: Bounds on amplitude-damping-channel discrimination. Phys. Rev. A. 103(2), 022610 (2021). arXiv:2009.04783 [quant-ph]
32. Simon, B.: Representations of finite and compact groups. Graduate studies in mathematics. 10. American Mathematical Society (1996)
33. Studziński, M., Mozrzymas, M., Kopszak, P.: Square-root measurements and degradation of the resource state in port-based teleportation scheme. J. Phys. A: Math. Theor. 55(37), 375302 (2022). arXiv:2105.14886 [quant-ph]
34. Strelchuk, S., Studziński, M.: Minimal Port-Based Teleportation. arXiv preprint (2021). arXiv:2111.05499 [quant-ph]
35. Studziński, M., Strelchuk, S., Mozrzymas, M., Horodecki, M.: Port-based teleportation in arbitrary dimension. Sci. Rep. 7(1), 1–11 (2017). arXiv:1612.09260 [quant-ph]
36. Studziński, M., Mozrzymas, M., Kopszak, P., Horodecki, M.: Efficient multi port-based teleportation schemes. IEEE Trans. Inf. Theory (2022). arXiv:2008.00984 [quant-ph]
37. Studziński, M.: Personal communication (2020)
38. Watrous, J.: The Theory of Quantum Information. Cambridge University Press, Available online. Cambridge (2018)

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Springer Nature or its licensor holds exclusive rights to this article under a publishing agreement with the author(s) or other rightsholder(s); author self-archiving of the accepted manuscript version of this article is solely governed by the terms of such publishing agreement and applicable law.