Optimal lower bound for quantum channel tomography in away-from-boundary regime

Kean Chen * Zhicheng Zhang † Nengkun Yu ‡

Abstract

Consider quantum channels with input dimension d_1, output dimension d_2 and Kraus rank at most r. Such channels exist only when the constraint $rd_2 \geq d_1$ holds, and we refer to the parameter regime $rd_2 = d_1$ as the boundary regime. In this paper, we show an optimal query lower bound $\Omega(rd_1 d_2/\varepsilon^2)$ for quantum channel tomography to within diamond norm error ε in the away-from-boundary regime $rd_2 \geq 2d_1$, matching the existing upper bound $O(rd_1 d_2/\varepsilon^2)$. In particular, this lower bound fully settles the query complexity for the commonly studied case of equal input and output dimensions $d_1 = d_2 = d$ with $r \geq 2$, in sharp contrast to the unitary case $r = 1$ where Heisenberg scaling $\Theta(d^2/\varepsilon)$ is achievable.

1 Introduction

Estimating an unknown quantum physical process from experimental data is a foundational task in quantum computing and quantum information. A central question is to quantify the informational resources required for such estimation when the unknown process is given as a black-box quantum channel. In this paper, we study *quantum channel tomography*: given query access to an unknown quantum channel $\mathcal{E}$, the goal is to learn a full classical description of $\mathcal{E}$ using as few queries as possible (to a prescribed accuracy, e.g., in diamond norm).

Research on quantum channel tomography traces back to the more basic problem of quantum state tomography, which aims to learn a full classical description of an unknown quantum state from samples. Quantum state tomography can be viewed as a special case of quantum channel tomography in which the input dimension is 1. The optimal tomography of pure states has been well understood since the seminal works [Hay98, BM99, KW99]. Optimal tomography of mixed states was developed later in [HHJ+17, OW16] and subsequently refined and extended in [OW17, GKKT20, Yue23, SSW25, PSW25, PSTW25].

Compared with quantum state tomography, general quantum channel tomography involves a richer set of considerations. One may design the input states arbitrarily (including entanglement with ancillas), apply the unknown channel sequentially and adaptively, and perform collective measurements across multiple uses, which leads to more subtle analyses. Despite this difficulty, extensive work [CN97, PCZ97, Leu00, DP01, MRL08, KKEG19, BHK+19, SSKKG22, Ouf23b, Ouf23a, HCP23, FFGO23, Car24, RAS+24, ZLK+24, ZRCK25, YMM25] has been devoted to quantum channel tomography over the last thirty years. Notably, for tomography of unitary channels, Haah, Kothari, O'Donnell, and Tang [HKOT23] settled the optimal query complexity $\Theta(d^2/\varepsilon)$, where d is the channel dimension and ε is the target error in diamond norm. For tomography of general

*University of Pennsylvania, Philadelphia, USA. Email: keanchen.gan@gmail.com

†University of Technology Sydney, Sydney, Australia. Email: iszczhang@gmail.com

‡Stony Brook University, NY, USA. Email: nengkunyu@gmail.com

channels using only non-adaptive incoherent measurements, Oufkir [Ouf23b, Ouf23a] established a near-optimal query complexity $\widetilde{\Theta}(d_1^3 d_2^3/\varepsilon^2)$, generalizing the algorithm in [SSKKG22], where d_1 and d_2 are the input and output dimensions and ε is the diamond norm error. For isometry channel tomography, Yoshida, Miyazaki, and Murao [YMM25] established a query lower bound of $\Omega((d_2 - d_1)d_1/(\varepsilon^2 \log 1/\varepsilon))$[1].

In the most general setting, the unknown channel has input dimension d_1, output dimension d_2, and Kraus rank at most r, and the tomography algorithm can make coherent queries to the unknown channel. Recent work has substantially improved our understanding of the optimal scalings. On the upper-bound side, Mele and Bittel [MB25] and Chen, Yu, and Zhang [CYZ25] showed that $O\big(rd_1d_2/\varepsilon^2\big)$ queries suffice for channel tomography with diamond norm error ε. Moreover, in the boundary regime $rd_2 = d_1$, [CYZ25] showed that $O(rd_1d_2/\varepsilon)$ queries suffice for channel tomography with Choi-state trace norm error ε, achieving the Heisenberg scaling.

Girardi, Mele, Zhao, Fanizza, and Lami [GMZ+25] and Yoshida, Niwa, and Murao [YNM25] then algorithmically strengthened the local test technique in [CYZ25] by explicitly constructing the random Stinespring dilation superchannels with efficient circuit complexity. Intuitively, local test and random dilation for channels can be viewed as dual concepts in the Heisenberg and Schrödinger pictures, respectively. The underlying ideas trace back to local test and random purification for quantum states [TWZ25, CWZ24, SW22]. More developments can be found in [PSTW25, GML25, MGC+25, WW25].

On the lower-bound side, it was shown in [GMZ+25] that $\Omega(rd_1d_2)$ queries are required for channel tomography at constant error, improving the prior lower bound $\Omega(d_1^2d_2^2/\log(d_1d_2))$ for full Kraus-rank (i.e., $r = d_1d_2$) tomography due to Rosenthal, Aaronson, Subramanian, Datta, and Gur [RAS+24]. More recently, Oufkir and Girardi [OG26] incorporated the ε-dependence and proved a lower bound of $\Omega\big(rd_1d_2/(\varepsilon^2\log(d_2r/\varepsilon))\big)$[2] in the away-from-boundary regime $rd_2 \geq 2d_1$, matching the upper bound in [MB25, CYZ25] up to a logarithmic factor. They also showed a lower bound $\Omega(rd_1d_2/(\varepsilon\log(d_2r/\varepsilon)))$ in the boundary regime $rd_2 = d_1$, where ε can be either Choi-state trace norm or diamond norm error, matching the upper bound in [CYZ25] up to a logarithmic factor.

A remaining open question is whether a matching query lower bound $\Omega(rd_1d_2/\varepsilon^2)$ for general quantum channel tomography can be proved without logarithmic factors. In this paper, we resolve this question by establishing such a lower bound in the away-from-boundary regime $rd_2 \geq 2d_1$. In particular, this settles the most commonly studied case of equal input and output dimensions $d_1 = d_2$ with $r \geq 2$.

1.1 Main results

Our main result is as follows.

Theorem 1.1 (Optimal lower bound in away-from-boundary regime, Theorem 4.2 restated)**.** *Let d_1, d_2, r be positive integers such that $rd_2 \geq 2d_1$. Tomography of quantum channels with input dimension d_1, output dimension d_2 and Kraus rank at most r, and to within diamond norm error ε, requires $\Omega(rd_1d_2/\varepsilon^2)$ queries.*

This lower bound matches the existing upper bound $O(rd_1d_2/\varepsilon^2)$ [MB25, CYZ25], and fully settles the query complexity of quantum channel tomography in the away-from-boundary regime

[1] Since we consider the tomography with success probability at least 2/3, the lower bound in [YMM25] applies to our setting if the success probability is amplified to $1 - O(\varepsilon^2)$, which incurs an additional logarithmic factor on ε.

[2] During the preparation of this manuscript, we became aware of a very recent update (arXiv v3) of [OG26], in which their lower bound in the away-from-boundary regime $rd_2 \geq 2d_1$ is improved to $\Omega\big(rd_1d_2/(\varepsilon^2\log(d_2r/\varepsilon))\big)$. See Section 1.2 for further discussion.

$rd_2 \geq 2d_1$. Theorem 1.1 is based on a tight analysis on sets of isometries with a specific structure (which we call the "hard" isometry set), using the formalism of quantum combs and testers. Recent work [OG26] provides an instantiation of such a "hard" isometry set with sufficiently large cardinality and the desired separation properties, allowing our analysis to apply to their construction and yield the optimal lower bound.

As a special case of our main result, we consider quantum channels with equal input and output dimensions, i.e., $d_1 = d_2 = d$, which are simply called d-dimensional quantum channels. Combined with known results on unitary tomography [HKOT23] and upper bound on quantum channel tomography [MB25, CYZ25], we can fully settle the query complexity for the tomography task of d-dimensional quantum channels.

Corollary 1.2 (Tomography of d-dimensional quantum channels)**.** *The query complexity for tomography of d-dimensional quantum channels $\mathcal{E}$ with Kraus rank at most r, and to within diamond-norm error ε, is*

$$\Theta\left(\frac{rd^2}{\varepsilon^{\min\{r,2\}}}\right).$$

Note that this reveals a sharp phase transition in the dependence on ε: it exhibits Heisenberg scaling $1/\varepsilon$ when $r = 1$ and classical scaling $1/\varepsilon^2$ when $r \geq 2$.

As another special case, we consider tomography of quantum channels with input dimension 1, which reduces to quantum state tomography. Then, we can reproduce the recent development of the optimal sample lower bound for quantum state tomography [SSW25], which matches the known upper bound [OW16].

Corollary 1.3 (State tomography)**.** *Tomography of a d-dimensional mixed state with rank at most r, to within trace norm error ε, requires $\Omega(dr/\varepsilon^2)$ samples.*

Our method for this lower bound is quite different from that in [SSW25], which may be of independent interest.

Then, we summarize the current best upper and lower bounds for quantum channel tomography in different parameter regimes in Table 1.

	Boundary* $rd_2 = d_1$	Near-boundary $d_1 < rd_2 < 2d_1$	Away-from-boundary $rd_2 \geq 2d_1$
Upper bounds	$O\left(\frac{rd_1d_2}{\varepsilon}\right)$ [CYZ25]	$O\left(\frac{rd_1d_2}{\varepsilon^2}\right)$ [MB25, CYZ25]	
Lower bounds	$\Omega\left(\frac{rd_1d_2}{\varepsilon\log(d_2r/\varepsilon)}\right)$ [OG26]	$\Omega(rd_1d_2)$ [GMZ+25]	$\Omega\left(\frac{rd_1d_2}{\varepsilon^2}\right)$ **This work**

Table 1: Upper and lower bounds for quantum channel tomography in different parameter regimes. Note that $rd_2 \geq d_1$ holds for any quantum channels. There is a phase transition from the boundary regime to away-from-boundary regime: the Heisenberg scaling $1/\varepsilon$ becomes the classical scaling $1/\varepsilon^2$.

$*$: In the boundary regime of this table, the upper bound holds for Choi-state trace norm error and the lower bound hold for both Choi-state trace norm and diamond norm errors. All other bounds hold for diamond-norm error.

1.2 Related work

During the preparation of this manuscript, we became aware of a very recent update (arXiv v3) of [OG26], in which their lower bound in the away-from-boundary regime $rd_2 \geq 2d_1$ is improved from $\Omega(rd_1d_2/(\varepsilon \log(d_2r/\varepsilon)))$ to $\Omega\big(rd_1d_2/(\varepsilon^2 \log(d_2r/\varepsilon))\big)$, which also achieves classical scaling $1/\varepsilon^2$ and matches the upper bound up to a logarithmic factor $\log(d_2r/\varepsilon)$. Their proof relies on an information-theoretic approach, which is different from our approach for proving the lower bound. Specifically, in our proof of Theorem 1.1, we provide a tight analysis for the hardness of discriminating isometries with a specific structure (see Theorem 3.2), then we combine the isometry net instantiation provided in [OG26, arXiv v1] with our hardness result (i.e., Theorem 3.2), to obtain the optimal lower bound without logarithmic factors. In contrast to approaches using information-theoretic tools, our analysis is based on the formalism of quantum combs and testers.

1.3 Discussion

This work establishes a matching lower bound of $\Omega(rd_1d_2/\varepsilon^2)$ on the number of queries needed for quantum channel tomography in the away-from-boundary regime $rd_2 \geq 2d_1$. Combined with the prior upper bound $O\big(rd_1d_2/\varepsilon^2\big)$ [MB25, CYZ25], our new query lower bound fully settles the most commonly studied case of equal input and output dimensions $d_1 = d_2 = d$ with $r \geq 2$. This optimal scaling is in sharp contrast to the Heisenberg scaling $\Theta(d^2/\varepsilon)$ in unitary channel tomography.

An important open question is whether one can further settle the query complexity for quantum channel tomography beyond the away-from-boundary regime $rd_2 \geq 2d_1$.

2 Preliminaries

2.1 Notation

We use $\mathcal{L}(\mathcal{H})$ to denote the set of linear operators on the Hilbert space $\mathcal{H}$. Given two orthonormal bases for $\mathcal{H}_0$ and $\mathcal{H}_1$ respectively, we can represent each linear operator from $\mathcal{H}_0$ to $\mathcal{H}_1$ by a $\dim(\mathcal{H}_1) \times \dim(\mathcal{H}_0)$ matrix and for such a matrix X, we use $|X\rangle\!\rangle \in \mathcal{H}_1 \otimes \mathcal{H}_0$ to denote the vector obtained by flattening the matrix X. It is easy to see the following facts:

$$||\psi\rangle\langle\phi|\rangle\!\rangle = |\psi\rangle|\phi^*\rangle, \qquad |XYZ\rangle\!\rangle = X \otimes Z^{\mathrm{T}}|Y\rangle\!\rangle,$$

where $|\phi^*\rangle$ is the entry-wise complex conjugate of $|\phi\rangle$ w.r.t. to a given orthonormal basis, and Z^{T} is the transpose of the matrix Z. The inner product can be denoted by $\langle\!\langle X|Y\rangle\!\rangle = \mathrm{tr}(X^\dagger Y)$. For two linear operators X, Y, we use $X \sqsubseteq Y$ to denote that $Y - X$ is positive semidefinite.

Let n, m, d be positive integers such that $n \geq m$. Let $\mathcal{H}_1 \cong \cdots \cong \mathcal{H}_n \cong \mathbb{C}^d$ be n copies of the d-dimensional Hilbert space. Let $S \subseteq [n] = \{1, 2, \ldots, n\}$ be a set of integers and $|\psi\rangle \in \mathbb{C}^d$ be a state. We use the following notation

$$|\psi\rangle^{\otimes S}$$

to denote the state $|\psi\rangle^{\otimes|S|}$ on $\bigotimes_{i\in S} \mathcal{H}_i$. Therefore, if $|\varphi\rangle \in \mathbb{C}^d$ is another state, then

$$|\psi\rangle^{\otimes S} \otimes |\varphi\rangle^{\otimes[n]\setminus S}$$

denotes the state $\bigotimes_{i=1}^n |x_i\rangle$ on $\bigotimes_{i=1}^n \mathcal{H}_i$ where $|x_i\rangle = |\psi\rangle$ for $i \in S$, and $|x_i\rangle = |\varphi\rangle$ otherwise.

2.2 Quantum channels

A quantum channel with input dimension d_1 and output dimension d_2 is described by a linear map $\mathcal{E} : \mathcal{L}(\mathbb{C}^{d_1}) \to \mathcal{L}(\mathbb{C}^{d_2})$ such that $\mathcal{E}$ is completely positive and trace-preserving (see, e.g., [NC10, Wat18, Hay17]).

In the Kraus representation [Kra83], a quantum channel $\mathcal{E}$ is written as

$$\mathcal{E}(\rho) = \sum_{i=1}^{r} E_i \rho E_i^\dagger,$$

where $E_i : \mathbb{C}^{d_1} \to \mathbb{C}^{d_2}$ are non-zero linear operators that satisfy $\sum_{i=1}^{r} E_i^\dagger E_i = I$, which are called Kraus operators. We can always find a set of E_i such that $\operatorname{tr}(E_i^\dagger E_j) = 0$ for $i \neq j$, then those E_i are called orthogonal Kraus operators and r is called the *Kraus rank*. Note that r must satisfy the constraint $d_1/d_2 \leq r \leq d_1 d_2$. A quantum channel that has Kraus rank $r = 1$ is an isometry channels $\mathcal{V} = V(\cdot)V^\dagger$, where $V : \mathbb{C}^{d_1} \to \mathbb{C}^{d_2}$ is an isometry operator, i.e., $V^\dagger V = I_{d_1}$, and it must hold that $d_2 \geq d_1$.

Notation 2.1. *We use* $\mathbf{QChan}_{d_1,d_2}^r$ *to denote the set of all quantum channels* $\mathcal{E} : \mathcal{L}(\mathbb{C}^{d_1}) \to \mathcal{L}(\mathbb{C}^{d_2})$ *that have Kraus rank at most* r*. In particular, we use* $\mathbf{ISO}_{d_1,d_2}$ *to denote the set of isometry channels with input dimension* d_1 *and output dimension* d_2*, which is equivalent to* $\mathbf{QChan}_{d_1,d_2}^1$*.*

In the Choi-Jamiołkowski representation [Cho75, Jam72, Jam72], $\mathcal{E}$ is represented by the Choi-Jamiołkowski operator

$$C_{\mathcal{E}} = (\mathcal{E} \otimes \mathcal{I})(|I\rangle\!\rangle\langle\!\langle I|) \in \mathcal{L}(\mathbb{C}^{d_2} \otimes \mathbb{C}^{d_1}),$$

where $|I\rangle\!\rangle = \sum_i |i\rangle|i\rangle \in \mathbb{C}^{d_1} \otimes \mathbb{C}^{d_1}$ is an unnormalized maximally entangled state. We may simply call it the Choi operator. Note that we can write $C_{\mathcal{E}} = \sum_{i=1}^{r} |E_i\rangle\!\rangle\langle\!\langle E_i|$, where E_i are orthogonal Kraus operators and thus $|E_i\rangle\!\rangle$ are pairwise orthogonal vectors. Therefore, the Kraus rank equals the rank of the Choi operator.

Stinespring dilation. Using the Stinespring dilation [Sti55], we can also write a quantum channel $\mathcal{E}$ with Kraus operators $\{E_i\}_{i=1}^r$ as

$$\mathcal{E}(\cdot) = \operatorname{tr}_{\mathcal{H}_{\mathrm{anc}}}(V(\cdot)V^\dagger), \tag{1}$$

where $\mathcal{H}_{\mathrm{anc}} \cong \mathbb{C}^r$ and $V = \sum_{i=1}^{r} |i\rangle_{\mathrm{anc}} \otimes E_i$ is an isometry operator. By this, one can notice that $rd_2 \geq d_1$ must hold. An isometry channel $\mathcal{V} = V(\cdot)V^\dagger$ that satisfies Equation (1) is called a dilation of $\mathcal{E}$. Suppose $\mathcal{V}_1$ is a dilation of $\mathcal{E}$, then $\mathcal{V}_2$ is a dilation of $\mathcal{E}$ if and only if they differ by a unitary on $\mathcal{H}_{\mathrm{anc}}$, i.e., $V_2 = (U \otimes I_{d_2})V_1$ for $U : \mathcal{H}_{\mathrm{anc}} \to \mathcal{H}_{\mathrm{anc}}$ a unitary. Conversely, given an isometry $V \in \mathbf{ISO}_{d_1,rd_2}$, the channel $\mathcal{E}(\cdot) = \operatorname{tr}_r(V(\cdot)V^\dagger)$ obtained from V by tracing out an r-dimensional subsystem has Kraus rank at most r.

2.3 Quantum combs and testers

The quantum comb [CDP08, CDP09] is a powerful tool to describe (higher) transformations of quantum processes. Specifically, the Choi-Jamiołkowski representation of quantum channels (i.e., transformations of quantum states) can be generalized to a higher-level concept (i.e., transformations of quantum processes), which is called *quantum comb*.

Definition 2.2 (Quantum comb [CDP09]). *For an integer $n \geq 1$, a quantum n-comb defined on a sequence of $2n$ Hilbert spaces $(\mathcal{H}_0, \mathcal{H}_1, \ldots, \mathcal{H}_{2n-1})$ is a positive semidefinite operator X on $\bigotimes_{j=0}^{2n-1} \mathcal{H}_j$ such that there exists a sequence of operators $X^{(n)}, X^{(n-1)}, \ldots, X^{(1)}, X^{(0)}$ such that*

$$\operatorname{tr}_{\mathcal{H}_{2j-1}}\left(X^{(j)}\right) = I_{\mathcal{H}_{2j-2}} \otimes X^{(j-1)}, \quad 1 \leq j \leq n, \tag{2}$$

where $X^{(n)} = X$ and $X^{(0)} = 1$.

We can easily see the following facts: A quantum 1-comb is simply the Choi-Jamiołkowski operator of a quantum channel. Any convex combination of quantum n-combs is also a quantum n-comb.

Then, we introduce the link product "$\star$".

Definition 2.3 (Link product "$\star$" [CDP08, CDP09]). *Suppose X is a linear operator on $\mathcal{H}_{\boldsymbol{i}} = \mathcal{H}_{i_1} \otimes \mathcal{H}_{i_2} \otimes \cdots \otimes \mathcal{H}_{i_n}$ and Y is a linear operator on $\mathcal{H}_{\boldsymbol{j}} = \mathcal{H}_{j_1} \otimes \mathcal{H}_{j_2} \otimes \cdots \otimes \mathcal{H}_{j_m}$, where $\boldsymbol{i} = (i_1, \ldots, i_n)$ is a sequence of pairwise distinct indices, and likewise for $\boldsymbol{j} = (j_1, \ldots, j_m)$. Let $\boldsymbol{a} = \boldsymbol{i} \cap \boldsymbol{j}$ be the set of indices in both $\boldsymbol{i}$ and $\boldsymbol{j}$ and $\boldsymbol{b} = \boldsymbol{i} \cup \boldsymbol{j}$ be the set of indices in either $\boldsymbol{i}$ or $\boldsymbol{j}$. Then, the combination of X and Y is defined by*

$$X \star Y = \operatorname{tr}_{\mathcal{H}_{\boldsymbol{a}}}\left(X^{\mathrm{T}_{\mathcal{H}_{\boldsymbol{a}}}} \cdot Y\right) = \operatorname{tr}_{\mathcal{H}_{\boldsymbol{a}}}\left(X \cdot Y^{\mathrm{T}_{\mathcal{H}_{\boldsymbol{a}}}}\right),$$

where $\mathcal{H}_{\boldsymbol{a}}$ means the tensor product of subsystems labeled by the indices in $\boldsymbol{a}$, $\mathrm{T}_{\mathcal{H}_{\boldsymbol{a}}}$ means the partial transpose on $\mathcal{H}_{\boldsymbol{a}}$, both X and Y are treated as linear operators on $\mathcal{H}_{\boldsymbol{b}}$, extended by tensoring with the identity operator as needed.

The link product describes the combination of quantum combs. For example, suppose X is an n-comb on $(\mathcal{H}_0, \mathcal{H}_1, \ldots, \mathcal{H}_{2n-1})$ and Y is an $(n-1)$-comb on $(\mathcal{H}_1, \mathcal{H}_2 \ldots, \mathcal{H}_{2n-2})$, then

$$X \star Y = \operatorname{tr}_{\mathcal{H}_{1:2n-2}}\left(X^{\mathrm{T}_{\mathcal{H}_{1:2n-2}}} \cdot (I_{\mathcal{H}_{2n-1}} \otimes Y \otimes I_{\mathcal{H}_0})\right) = \operatorname{tr}_{\mathcal{H}_{1:2n-2}}\left(X \cdot (I_{\mathcal{H}_{2n-1}} \otimes Y^{\mathrm{T}} \otimes I_{\mathcal{H}_0})\right)$$

turns out to be a 1-comb on $(\mathcal{H}_0, \mathcal{H}_{2n-1})$. The link product also has many good properties. It preserves the Löwner order: if $X, Y \sqsupseteq 0$ then $X \star Y \sqsupseteq 0$ [CDP09, Theorem 2]. It is commutative $X \star Y = Y \star X$, and associative $(X \star Y) \star Z = X \star (Y \star Z)$ whenever X, Y, Z do not share a common subsystem (i.e., there is no subsystem that is a subsystem of all three).

2.3.1 Quantum channel testers

A *quantum channel tester* means a quantum algorithm that can make multiple queries to an unknown quantum channel and then produces a classical output. We adopt the quantum tester formalism based on Choi-Jamiołkowski representation (see, e.g., [CDP09, BMQ21, BMQ22]), which provides a practical framework for studying various classes of quantum testers, such as parallel and sequential ones.

Suppose a quantum channel tester uses n queries to an unknown quantum channel $\mathcal{E}$. We label the input and output systems of the i-th query to $\mathcal{E}$ as $\mathcal{H}_{\mathrm{A},i}$ and $\mathcal{H}_{\mathrm{B},i}$, i.e., the i-th copy of the unknown channel is a linear map from $\mathcal{L}(\mathcal{H}_{\mathrm{A},i})$ to $\mathcal{L}(\mathcal{H}_{\mathrm{B},i})$.

In a sequential tester, one sends a quantum system through the first use of the channel $\mathcal{E}$ and then feeds the resulting output into subsequent uses, potentially along with ancillary systems, while allowing arbitrary CPTP maps to act between uses of $\mathcal{E}$. After all n uses of the channel $\mathcal{E}$, a POVM is performed on the final output state. In other words, sequential testers can represent coherent and adaptive query-access algorithms.

Definition 2.4 (Sequential tester). *A sequential tester that uses n queries to an unknown channel is a set of linear operators $\{T_i\}_i$ for $T_i \in \mathcal{L}(\bigotimes_{j=1}^{n} \mathcal{H}_{\mathrm{A},j} \otimes \mathcal{H}_{\mathrm{B},j})$ such that $T_i \sqsupseteq 0$ and $\sum_i T_i$ is a quantum $(n+1)$-comb on $(\mathcal{H}_0, \mathcal{H}_{\mathrm{A},1}, \mathcal{H}_{\mathrm{B},1}, \ldots, \mathcal{H}_{\mathrm{A},n}, \mathcal{H}_{\mathrm{B},n}, \mathcal{H}_{n+1})$, where $\mathcal{H}_0 \cong \mathcal{H}_{n+1} \cong \mathbb{C}$ are one-dimensional.*

It is known that any sequential tester can be realized by a sequential query-access algorithm and any sequential query-access algorithm can be described by a sequential tester [CDP09, BMQ22]. When we apply a sequential tester $\{T_i\}_i$ to n queries to a quantum channel $\mathcal{E}$, we get the classical outcome i with probability

$$p_i = T_i \star C_{\mathcal{E}}^{\otimes n} = \mathrm{tr}(T_i (C_{\mathcal{E}}^{\otimes n})^{\mathrm{T}}) = \mathrm{tr}(T_i^{\mathrm{T}} C_{\mathcal{E}}^{\otimes n}),$$

where $C_{\mathcal{E}}^{\otimes n}$ is the Choi operator of all n queries to the channel $\mathcal{E}$ and $(\cdot)^{\mathrm{T}}$ denotes matrix transposition.

2.3.2 Discrimination of quantum channels

Suppose $\mathcal{N}$ is a finite set of quantum channels. Then, the discrimination problem for channels in $\mathcal{N}$ is defined as follows.

Problem 2.5. *Suppose $\mathcal{E}$ is uniformly randomly chosen from the set $\mathcal{N}$. The algorithm (or tester) can make n queries to the channel $\mathcal{E}$ and the goal is to identify $\mathcal{E}$.*

Suppose $\{T_{\mathcal{E}}\}_{\mathcal{E} \in \mathcal{N}}$ is a sequential tester for this discrimination task where $T_{\mathcal{E}}$ corresponds to outputting the label $\mathcal{E}$. Then, the success probability can be expressed as

$$\Pr[\text{success}] = \frac{1}{|\mathcal{N}|} \sum_{\mathcal{E} \in \mathcal{N}} T_{\mathcal{E}} \star C_{\mathcal{E}}^{\otimes n},$$

where $C_{\mathcal{E}}$ denotes the (unnormalized) Choi state of $\mathcal{E}$. We say an algorithm solves the discrimination problem if the success probability is higher than $2/3$.

3 Hardness of discriminating isometries

3.1 Hard instance

Suppose d_1, d_2 are positive integers such that $d_2 \geq 2d_1$ and $\varepsilon \in (0, 1)$. Define the Hilbert space $\mathcal{H}_{\mathrm{A}} \cong \mathbb{C}^{d_1}$ with an orthonormal basis $\{|1\rangle_{\mathrm{A}}, \ldots, |d_1\rangle_{\mathrm{A}}\}$ and $\mathcal{H}_{\mathrm{B}} \cong \mathbb{C}^{d_2}$ with an orthonormal basis $\{|1\rangle_{\mathrm{B}}, \ldots, |d_2\rangle_{\mathrm{B}}\}$. Define the isometries $V_0, \Delta : \mathcal{H}_{\mathrm{A}} \to \mathcal{H}_{\mathrm{B}}$ as follows

$$V_0 \coloneqq \sum_{i=1}^{d_1} |i\rangle_{\mathrm{B}} \langle i|_{\mathrm{A}}, \quad \text{and} \quad \Delta \coloneqq \sum_{i=1}^{d_1} |d_1 + i\rangle_{\mathrm{B}} \langle i|_{\mathrm{A}}.$$

Then, for any $U \in \mathbb{U}_{d_2 - d_1}$, we define the isometry $V_{\varepsilon,U} : \mathcal{H}_{\mathrm{A}} \to \mathcal{H}_{\mathrm{B}}$ as

$$\begin{aligned} V_{\varepsilon,U} &\coloneqq (I_{d_1} \oplus U) \left(\sqrt{1 - \varepsilon^2} V_0 + \varepsilon \Delta \right) \\ &= \sqrt{1 - \varepsilon^2} V_0 + \varepsilon U \Delta, \end{aligned} \tag{3}$$

where $I_{d_1} = \sum_{i=1}^{d_1} |i\rangle_{\mathrm{B}} \langle i|_{\mathrm{B}}$, and $U \in \mathbb{U}_{d_2 - d_1}$ acts on the subspace spanned by $\{|d_1 + 1\rangle_{\mathrm{B}}, \ldots, |d_2\rangle_{\mathrm{B}}\}$. Then, any subset of

$$\{V_{\varepsilon,U} \,|\, U \in \mathbb{U}_{d_2 - d_1}\}$$

is called a *"hard"* isometry set.

Note that in the above construction, the orthonormal bases of $\mathcal{H}_{\mathrm{A}}$ and $\mathcal{H}_{\mathrm{B}}$ are chosen arbitrarily. Therefore, this construction can also be described in an abstract way.

Definition 3.1. *Let $\mathcal{H}_{\mathrm{A}} \cong \mathbb{C}^{d_1}$, $\mathcal{H}_{\mathrm{B}} \cong \mathbb{C}^{d_2}$. Let $V_0 : \mathcal{H}_{\mathrm{A}} \to \mathcal{H}_{\mathrm{B}}$ be an arbitrary but fixed isometry and let $\mathcal{H}_0$ be the image of V_0. Then, any subset of*

$$\left\{ \sqrt{1-\varepsilon^2} V_0 + \varepsilon \Delta \;\middle|\; \Delta : \mathcal{H}_{\mathrm{A}} \to \mathcal{H}_0^{\perp} \text{ is an isometry} \right\}$$

is called a "hard" isometry set.

3.2 Hardness of the discrimination problem

Then, we have the following result.

Theorem 3.2. *Suppose $\mathcal{N}$ is a finite "hard" isometry set (see Section 3.1) with cardinality $|\mathcal{N}| \geq \exp(Cd_1d_2)$ for a universal constant C. Then, any algorithm that solves the discrimination problem for the isometries in $\mathcal{N}$ requires at least $n \geq \Omega(d_1d_2/\varepsilon^2)$ queries.*

Proof. Without loss of generality, we can assume $\mathcal{N}$ is a finite subset of $\{V_{\varepsilon,U} \,|\, U \in \mathbb{U}_{d_2-d_1}\}$ for $V_{\varepsilon,U}$ defined in Equation (3). Let $B = 2e^4$ be a constant. Suppose there is an algorithm that solves the discrimination problem using n queries. If $n > \frac{1}{B} d_1d_2/\varepsilon^2$, there is nothing to prove. Otherwise we assume $n \leq \frac{1}{B} d_1 d_2/\varepsilon^2$.

Note that each element V in $\mathcal{N}$ is of the form

$$V = \sqrt{1-\varepsilon^2} V_0 + \varepsilon U \Delta,$$

where $U \in \mathbb{U}_{d_2-d_1}$.

Suppose the algorithm for distinguishing the isometry set is described by a tester $\{T_V\}_{V\in\mathcal{N}}$. Then, the success probability is

$$\begin{aligned} \Pr[\text{success}] &= \frac{1}{|\mathcal{N}|} \cdot \sum_{V\in\mathcal{N}} T_V \star |V\rangle\!\rangle\langle\!\langle V|^{\otimes n} \\ &\leq \exp(-Cd_1d_2) \cdot \sum_{V\in\mathcal{N}} T_V \star |V\rangle\!\rangle\langle\!\langle V|^{\otimes n}. \end{aligned}$$

Here, $|V\rangle\!\rangle\langle\!\langle V|^{\otimes n}$ is an n-comb on $(\mathcal{H}_{\mathrm{A},1}, \mathcal{H}_{\mathrm{B},1}, \ldots, \mathcal{H}_{\mathrm{A},n}, \mathcal{H}_{\mathrm{B},n})$, where $\mathcal{H}_{\mathrm{A},j}$ and $\mathcal{H}_{\mathrm{B},j}$ denote the input and output spaces of the j-th query to V, respectively. Note that for $V \in \mathcal{N}$,

$$|V\rangle\!\rangle^{\otimes n} = \sum_{i=0}^{n} \left(\sqrt{1-\varepsilon^2}\right)^{n-i} \varepsilon^i \sum_{\substack{S\subseteq[n] \\ |S|=i}} |V_0\rangle\!\rangle^{\otimes [n]\setminus S} \otimes |U\Delta\rangle\!\rangle^{\otimes S}.$$

For $i \in \{0, 1, \ldots, n\}$, we define the vector

$$|\gamma_i\rangle \coloneqq \frac{1}{\sqrt{\binom{n}{i}}} \sum_{\substack{S\subseteq[n] \\ |S|=i}} |V_0\rangle\!\rangle^{\otimes [n]\setminus S} \otimes |\Delta\rangle\!\rangle^{\otimes S}. \tag{4}$$

Note that $|\gamma_i\rangle$ are pairwise orthogonal since $\langle\!\langle V_0|\Delta\rangle\!\rangle = \operatorname{tr}(V_0^\dagger \Delta) = 0$. For any $V \in \mathcal{N}$, there exists a $U \in \mathbb{U}_{d_2-d_1}$ such that

$$|V\rangle\!\rangle^{\otimes n} = \sum_{i=0}^{n} \left(\sqrt{1-\varepsilon^2}\right)^{n-i} \varepsilon^i \sqrt{\binom{n}{i}} U^{\otimes n} |\gamma_i\rangle, \tag{5}$$

where $U^{\otimes n}$ acts as $(I_{d_1} \oplus U)^{\otimes n}$ on $\bigotimes_{i=1}^{n} \mathcal{H}_{\mathrm{B},i}$. Next, we define the operator Γ_i as

$$\Gamma_i \coloneqq \mathop{\mathbf{E}}_{U \sim \mathbb{U}_{d_2-d_1}} \left[U^{\otimes n} |\gamma_i\rangle\langle\gamma_i| U^{\dagger\otimes n} \right], \tag{6}$$

where $U^{\otimes n}$ acts as $(I_{d_1} \oplus U)^{\otimes n}$ on $\bigotimes_{i=1}^{n} \mathcal{H}_{\mathrm{B},i}$. Note that $\mathrm{supp}(\Gamma_i)$ are also pairwise orthogonal, which can be easily seen from the fact that $|\gamma_i\rangle$ contains different numbers of $|V_0\rangle\rangle$ and $|\Delta\rangle$ for different i, and any element in the orbit $\{U|\Delta\rangle\rangle \mid U \in \mathbb{U}_{d_2-d_1}\}$ is orthogonal to $|V_0\rangle\rangle$.

If we can find some positive numbers $\lambda_0, \ldots, \lambda_n$ such that, for any $V \in \mathcal{N}$,

$$|V\rangle\rangle\langle\langle V|^{\otimes n} \sqsubseteq \sum_{i=0}^{n} \lambda_i \Gamma_i, \tag{7}$$

then the success probability can be upper bounded as

$$\begin{aligned}
\Pr[\text{success}] &\leq \exp(-Cd_1d_2) \cdot \sum_{V \in \mathcal{N}} T_V \star |V\rangle\rangle\langle\langle V|^{\otimes n} \\
&\leq \exp(-Cd_1d_2) \cdot \sum_{V \in \mathcal{N}} T_V \star \sum_{j=0}^{n} \lambda_j \Gamma_j \\
&= \exp(-Cd_1d_2) \cdot \sum_{k=0}^{n} \lambda_k \cdot \sum_{V \in \mathcal{N}} T_V \star \sum_{j=0}^{n} \frac{\lambda_j}{\sum_{k=0}^{n} \lambda_k} \Gamma_j \\
&= \exp(-Cd_1d_2) \cdot \sum_{i=0}^{n} \lambda_i, \qquad (8)
\end{aligned}$$

where Equation (8) is because

- $\sum_{V \in \mathcal{N}} T_V$ is an (n+1)-comb with input and output dimensions 1, and
- $\sum_{j=0}^{n} \frac{\lambda_j}{\sum_{k=0}^{n} \lambda_k} \Gamma_j$ is an n-comb since Γ_i is an n-comb (due to Lemma 3.3) and convex combination of n-combs is also an n-comb,

so that their contraction evaluates to 1.

By Lemma 3.4, there are $\{\lambda_i\}_{i=0}^{n}$ with $\sum_{i=0}^{n} \lambda_i \leq 3d_1^2 d_2^2 \exp(\sqrt{8n\varepsilon^2 d_1 d_2})$. Therefore, we know that the success probability can be bounded by

$$\Pr[\text{success}] \leq \exp(-Cd_1d_2) \cdot 3d_1^2 d_2^2 \exp\left(\sqrt{8n\varepsilon^2 d_1 d_2}\right).$$

If we want the success probability being at least 2/3, we have

$$\sqrt{8n\varepsilon^2 d_1 d_2} \geq Cd_1d_2 - 2\ln(d_1d_2) + \ln(2/9),$$

which means

$$n \geq \Omega(d_1 d_2/\varepsilon^2).$$

$\square$

3.3 Technical lemmas

Lemma 3.3. *Let $|\gamma_i\rangle$ be the state defined in Equation (4). Then, $|\gamma_i\rangle\!\langle\gamma_i|$ is an n-comb. This further means Γ_i defined in Equation (6) is an n-comb.*

Proof. We use $|\gamma_i^n\rangle$ to denote the state $|\gamma_i\rangle$ defined in Equation (4) with parameter n. Then, we use induction on n to prove $|\gamma_i^n\rangle\!\langle\gamma_i^n|$ is an n-comb. First, we note that

$$\begin{aligned} \operatorname{tr}_{\mathcal{H}_{\mathrm{B}}}(|V_0\rangle\!\rangle\!\langle\!\langle\Delta|) = V_0^{\mathrm{T}}\Delta = 0, \qquad \operatorname{tr}_{\mathcal{H}_{\mathrm{B}}}(|\Delta\rangle\!\rangle\!\langle\!\langle V_0|) = \Delta^{\mathrm{T}} V_0 = 0, \\ \operatorname{tr}_{\mathcal{H}_{\mathrm{B}}}(|V_0\rangle\!\rangle\!\langle\!\langle V_0|) = I_{\mathrm{A}}, \qquad \operatorname{tr}_{\mathcal{H}_{\mathrm{B}}}(|\Delta\rangle\!\rangle\!\langle\!\langle\Delta|) = I_{\mathrm{A}}, \end{aligned} \tag{9}$$

where I_{A} denotes $\sum_{i=1}^{d_1} |i\rangle_{\mathrm{A}}\langle i|_{\mathrm{A}}$. Then, we note that

$$|\gamma_i^i\rangle = |\Delta\rangle\!\rangle^{\otimes i}.$$

Since $\operatorname{tr}_{\mathcal{H}_{\mathrm{B}}}(|\Delta\rangle\!\rangle\!\langle\!\langle\Delta|) = I_{\mathrm{A}}$, we know that $|\gamma_i^i\rangle\!\langle\gamma_i^i|$ is an i-comb, and the hypothesis holds for the case $n = i$. On the other hand, note that

$$|\gamma_i^n\rangle = \sqrt{\frac{\binom{n-1}{i}}{\binom{n}{i}}}|V_0\rangle\!\rangle \otimes |\gamma_i^{n-1}\rangle + \sqrt{\frac{\binom{n-1}{i-1}}{\binom{n}{i}}}|\Delta\rangle\!\rangle \otimes |\gamma_{i-1}^{n-1}\rangle.$$

Thus, we have

$$\begin{aligned} \operatorname{tr}_{\mathcal{H}_{\mathrm{B},n}}(|\gamma_i^n\rangle\!\langle\gamma_i^n|) &= \frac{\binom{n-1}{i}}{\binom{n}{i}} \operatorname{tr}_{\mathcal{H}_{\mathrm{B}}}(|V_0\rangle\!\rangle\!\langle\!\langle V_0|) \otimes |\gamma_i^{n-1}\rangle\!\langle\gamma_i^{n-1}| + \frac{\binom{n-1}{i-1}}{\binom{n}{i}} \operatorname{tr}_{\mathcal{H}_{\mathrm{B}}}(|\Delta\rangle\!\rangle\!\langle\!\langle\Delta|) \otimes |\gamma_{i-1}^{n-1}\rangle\!\langle\gamma_{i-1}^{n-1}| \\ &\quad + \frac{\sqrt{\binom{n-1}{i}\binom{n-1}{i-1}}}{\binom{n}{i}}\Big(\operatorname{tr}_{\mathcal{H}_{\mathrm{B}}}(|V_0\rangle\!\rangle\!\langle\!\langle\Delta|) \otimes |\gamma_i^{n-1}\rangle\!\langle\gamma_{i-1}^{n-1}| + \operatorname{tr}_{\mathcal{H}_{\mathrm{B}}}(|\Delta\rangle\!\rangle\!\langle\!\langle V_0|) \otimes |\gamma_{i-1}^{n-1}\rangle\!\langle\gamma_i^{n-1}| \Big) \\ &= \frac{\binom{n-1}{i}}{\binom{n}{i}} I_{\mathrm{A}} \otimes |\gamma_i^{n-1}\rangle\!\langle\gamma_i^{n-1}| + \frac{\binom{n-1}{i-1}}{\binom{n}{i}} I_{\mathrm{A}} \otimes |\gamma_{i-1}^{n-1}\rangle\!\langle\gamma_{i-1}^{n-1}|, \end{aligned} \tag{10}$$

where Equation (10) is due to Equation (9). By induction hypothesis, both $|\gamma_i^{n-1}\rangle\!\langle\gamma_i^{n-1}|$ and $|\gamma_{i-1}^{n-1}\rangle\!\langle\gamma_{i-1}^{n-1}|$ are $(n-1)$-combs. Note that $\binom{n-1}{i} + \binom{n-1}{i-1} = \binom{n}{i}$ and thus

$$\frac{\binom{n-1}{i}}{\binom{n}{i}}|\gamma_i^{n-1}\rangle\!\langle\gamma_i^{n-1}| + \frac{\binom{n-1}{i-1}}{\binom{n}{i}}|\gamma_{i-1}^{n-1}\rangle\!\langle\gamma_{i-1}^{n-1}|$$

is an $(n-1)$-comb. Therefore, $|\gamma_i^n\rangle\!\langle\gamma_i^n|$ is an n-comb.

Note that $U^{\otimes n}|\gamma_i\rangle\!\langle\gamma_i|U^{\dagger\otimes n}$ is also an n-comb because here U is applied only on the output system $\mathcal{H}_{\mathrm{B}}$. Then, Γ_i by definition is a convex combination of n-comb, thus Γ_i is also an n-comb. □

Lemma 3.4. *Suppose $B = 2e^4$, $d_1 d_2 \geq 2$ and $n \leq \frac{1}{B} d_1 d_2 / \varepsilon^2$. There exists positive numbers $\lambda_0, \ldots, \lambda_n$ such that Equation (7) holds and $\sum_{i=0}^n \lambda_i \leq 3 d_1^2 d_2^2 \exp\big(\sqrt{8n\varepsilon^2 d_1 d_2}\big)$.*

Proof. From Equation (5), it is easy to see that $|V\rangle\!\rangle^{\otimes n}$ is contained in $\bigoplus_{j=0}^n \operatorname{supp}(\Gamma_j)$. Then, by Fact 5.2, Equation (7) is equivalent to

$$\sum_{i=0}^n \frac{1}{\lambda_i} \operatorname{tr}\big(\Gamma_i^{-1} |V\rangle\!\rangle\!\langle\!\langle V|^{\otimes n}\big) \leq 1. \tag{11}$$

Note that the LHS of Equation (11) can be upper bounded as

$$\sum_{i=0}^{n} \frac{1}{\lambda_i} \operatorname{tr}\!\left(\Gamma_i^{-1} |V\rangle\!\rangle\!\langle\!\langle V|^{\otimes n}\right) = \sum_{i=0}^{n} \frac{1}{\lambda_i} \binom{n}{i} \left(1-\varepsilon^2\right)^{n-i} \varepsilon^{2i} \operatorname{tr}\!\left(\Gamma_i^{-1} U^{\otimes n} |\gamma_i\rangle\!\langle\gamma_i| U^{\dagger\otimes n}\right) \tag{12}$$

$$= \sum_{i=0}^{n} \frac{1}{\lambda_i} \binom{n}{i} \left(1-\varepsilon^2\right)^{n-i} \varepsilon^{2i} \operatorname{tr}\!\left(\Gamma_i^{-1} |\gamma_i\rangle\!\langle\gamma_i|\right) \tag{13}$$

$$\leq \sum_{i=0}^{n} \frac{1}{\lambda_i} \binom{n}{i} \left(1-\varepsilon^2\right)^{n-i} \varepsilon^{2i} \binom{d_1 d_2 + i - 2}{i}, \tag{14}$$

where Equation (12) is by using Equation (5) and the fact that $U^{\otimes n}|\gamma_i\rangle$ lies in $\operatorname{supp}(\Gamma_i)$, Equation (13) is because Γ_i commutes with $U^{\otimes n}$, Equation (14) by using Lemma 3.5 where we consider $|\gamma_i\rangle$ as a vector in the linear space:

$$\operatorname{span}\left(\left\{ \sum_{\substack{S\subseteq[n]\\ |S|=i}} |\psi\rangle^{\otimes S} \otimes |V_0\rangle\!\rangle^{\otimes [n]\setminus S} \;\middle|\; |\psi\rangle \in |V_0\rangle\!\rangle^{\perp} \right\}\right),$$

which has dimension $\binom{d_1 d_2+i-2}{i}$ by Lemma 3.6. Therefore, it suffices to find positive numbers $\lambda_0, \ldots, \lambda_n$ such that Equation (14) is upper bounded by 1.

Using Fact 5.1, we can upper bound Equation (14) as

$$\begin{aligned}
(14) &\leq \sum_{i=0}^{n} \frac{1}{\lambda_i} \exp\!\left(-nD\!\left(\frac{i}{n} \,\middle\|\, \varepsilon^2\right) + (d_1 d_2 + i) H\!\left(\frac{i}{d_1 d_2 + i}\right)\right) \\
&= \sum_{i=0}^{n} \frac{1}{\lambda_i} \exp\!\left(-i \ln\!\left(\frac{i}{n\varepsilon^2}\right) - (n-i)\ln\!\left(\frac{n-i}{n(1-\varepsilon^2)}\right) + i\ln\!\left(1+\frac{d_1 d_2}{i}\right) + d_1 d_2 \ln\!\left(1 + \frac{i}{d_1 d_2}\right)\right) \\
&\leq \sum_{i=0}^{n} \frac{1}{\lambda_i} \exp\!\left(-i \ln\!\left(\frac{i}{n\varepsilon^2}\right) + i \ln\!\left(1 + \frac{d_1 d_2}{i}\right) + 2i\right),
\end{aligned} \tag{15}$$

where Equation (15) is because

$$(n-i)\ln\!\left(\frac{n(1-\varepsilon^2)}{n-i}\right) \leq (n-i)\left(\frac{n(1-\varepsilon^2)}{n-i} - 1\right) = i - n\varepsilon^2 \leq i,$$

and

$$d_1 d_2 \ln\!\left(1 + \frac{i}{d_1 d_2}\right) \leq d_1 d_2 \frac{i}{d_1 d_2} = i.$$

Now, we bound each summand in Equation (15) separately:

- For $i < d_1 d_2$, we use

$$\begin{aligned}
-i \ln\!\left(\frac{i}{n\varepsilon^2}\right) + i \ln\!\left(1 + \frac{d_1 d_2}{i}\right) + 2i &\leq -i \ln\!\left(\frac{i}{n\varepsilon^2}\right) + i \ln\!\left(\frac{2 d_1 d_2}{i}\right) + 2i \\
&= 2i \ln\!\left(\frac{\sqrt{2e^2 n\varepsilon^2 d_1 d_2}}{i}\right) \\
&\leq \sqrt{8 n\varepsilon^2 d_1 d_2},
\end{aligned} \tag{16}$$

  where Equation (16) is due to Fact 5.3.

- For $i \geq d_1 d_2$, then we have $i \geq Bn\varepsilon^2$ since $n \leq \frac{1}{B} d_1 d_2/\varepsilon^2$ by assumption, and

$$-i\ln\left(\frac{i}{n\varepsilon^2}\right) + i\ln\left(1 + \frac{d_1 d_2}{i}\right) + 2i \leq -i\ln(B) + i\ln(2) + 2i = -i\ln\big(B/2e^2\big) = -2i.$$

Therefore, taking $\lambda_i = 2d_1 d_2 \exp\big(\sqrt{8n\varepsilon^2 d_1 d_2}\big)$ for $i < d_1 d_2$ and $\lambda_i = \exp(-i)$ for $i \geq d_1 d_2$, we can see Equation (15) is upper bounded by

$$\begin{aligned}
(15) &\leq \sum_{i<d_1 d_2} \frac{1}{\lambda_i} \exp\left(\sqrt{8n\varepsilon^2 d_1 d_2}\right) + \sum_{i \geq d_1 d_2} \frac{1}{\lambda_i} \exp(-2i) \\
&\leq \frac{1}{2} + \sum_{i \geq d_1 d_2} \exp(-i) \\
&\leq \frac{1}{2} + \exp(-d_1 d_2) \frac{e}{e-1} \\
&< 1,
\end{aligned}$$

where in the last inequality we use that $d_1 d_2 \geq 2$, and we also have

$$\begin{aligned}
\sum_{i=0}^{n} \lambda_i &\leq 2d_1^2 d_2^2 \exp\left(\sqrt{8n\varepsilon^2 d_1 d_2}\right) + \exp(-d_1 d_2) \frac{e}{e-1} \\
&< 2d_1^2 d_2^2 \exp\left(\sqrt{8n\varepsilon^2 d_1 d_2}\right) + \frac{1}{2} \\
&< 3d_1^2 d_2^2 \exp\left(\sqrt{8n\varepsilon^2 d_1 d_2}\right),
\end{aligned}$$

as desired. □

Lemma 3.5. *Let G be a compact Lie group equipped with a unitary action $\rho(\cdot)$ on a finite-dimensional Hilbert space $\mathcal{H}$. Let $X \in \mathcal{L}(\mathcal{H})$ be a positive semidefinite operator. Then, we have*

$$\operatorname{tr}\left(\left(\mathop{\mathbf{E}}_{g\sim G}\left[\rho(g) X \rho(g)^{-1}\right]\right)^{-1} X\right) \leq \dim(\mathcal{H}),$$

where $(\cdot)^{-1}$ denotes the pseudo-inverse and $\mathbf{E}_{g\sim G}$ is the expectation over the Haar measure of G.

Proof. Since $\mathcal{H}$ is a unitary representation of G, it is completely reducible. This means we can write:

$$\mathcal{H} \overset{G}{\cong} \bigoplus_i \mathcal{V}_i \otimes \mathcal{W}_i,$$

where these $\mathcal{V}_i$ are pairwise non-isomorphic irreducible representations of G and $\mathcal{W}_i$ are corresponding multiplicity spaces. We can write $X = \bigoplus_{i,j} X_{i\to j}$ where $X_{i\to j} : \mathcal{V}_i \otimes \mathcal{W}_i \to \mathcal{V}_j \otimes \mathcal{W}_j$ is a linear operator. Then, by Schur's lemma, we have

$$\mathop{\mathbf{E}}_{g\sim G}\left[\rho(g) X \rho(g)^{-1}\right] = \bigoplus_i \frac{1}{\dim(\mathcal{V}_i)} I_{\mathcal{V}_i} \otimes \operatorname{tr}_{\mathcal{V}_i}(X_{i\to i}).$$

Therefore,

$$\operatorname{tr}\left(\left(\mathop{\mathbf{E}}_{g\sim G}\left[\rho(g) X \rho(g)^{-1}\right]\right)^{-1} X\right) = \sum_i \dim(\mathcal{V}_i) \operatorname{tr}\left(\left(I_{\mathcal{V}_i} \otimes \operatorname{tr}_{\mathcal{V}_i}(X_{i\to i})^{-1}\right) \cdot X_{i\to i}\right)$$

$$
\begin{aligned}
&= \sum_i \dim(\mathcal{V}_i) \operatorname{tr}\left(\operatorname{tr}_{\mathcal{V}_i}(X_{i\to i})^{-1} \cdot \operatorname{tr}_{\mathcal{V}_i}(X_{i\to i})\right) \\
&\leq \sum_i \dim(\mathcal{V}_i) \dim(\mathcal{W}_i) \\
&= \dim(\mathcal{H}).
\end{aligned}
$$

□

Lemma 3.6. *Consider the linear space $\mathbb{C}^{d+1}$ with the orthonormal basis $\{|0\rangle, |1\rangle, \ldots, |d\rangle\}$. Let $n \geq m$ be two positive integers and $\mathcal{H}_i \cong \mathbb{C}^{d+1}$ for $i \in [n]$. Consider the following subspace of $\bigotimes_{i=1}^n \mathcal{H}_i$:*

$$A = \operatorname{span}\left(\left\{ \sum_{\substack{S\subseteq[n] \\ |S|=m}} |\psi\rangle^{\otimes S} \otimes |0\rangle^{\otimes [n]\setminus S} \;\middle|\; |\psi\rangle \in |0\rangle^{\perp} \right\}\right),$$

where $|0\rangle^{\perp}$ denotes the subspace orthogonal to $|0\rangle$ (i.e., the subspace spanned by $\{|1\rangle, \ldots, |d\rangle\}$). Then, we have

$$\dim(A) = \binom{d+m-1}{m}.$$

Proof. Consider the linear operator

$$P = \sum_{\pi\in\mathfrak{S}_n} \mathtt{p}(\pi),$$

where $\mathtt{p}(\cdot)$ denotes the tensor permutation action of $\mathfrak{S}_n$ on $\bigotimes_{i=1}^n \mathcal{H}_i$, i.e., $\mathtt{p}(\pi)|\psi_1\rangle \otimes \cdots \otimes |\psi_n\rangle = |\psi_{\pi^{-1}(1)}\rangle \otimes \cdots \otimes |\psi_{\pi^{-1}(n)}\rangle$. One can easily check that P is injective when restricting on the subspace $\operatorname{span}(\{|\psi\rangle^{\otimes m} \otimes |0\rangle^{\otimes n-m} \mid |\psi\rangle \in |0\rangle^{\perp}\})$ and A is exactly the image of P on this subspace. Furthermore, we know that $\operatorname{span}(\{|\psi\rangle^{\otimes m} \mid |\psi\rangle \in |0\rangle^{\perp}\}) \cong \vee^m \mathbb{C}^d$ is the symmetric subspace of $(\mathbb{C}^d)^{\otimes m}$, and has dimension $\binom{d+m-1}{m}$ [Har13], and thus A has the same dimension. □

4 Instantiation

In Section 3, we showed that for a sufficiently large set $\mathcal{N}$ of isometries with specific structures, the discrimination problem for $\mathcal{N}$ is hard. In this section, we use the construction of the ε-net provided in [OG26] as an instantiation of $\mathcal{N}$. This, combined with our Theorem 3.2, provides the lower bound for quantum channel tomography.

Suppose r, d_1, d_2 are positive integers such that $rd_2 \geq d_1$ and $\varepsilon \in (0,1)$. Define the Hilbert spaces $\mathcal{H}_{\mathrm{A}} \cong \mathbb{C}^{d_1}$ and $\mathcal{H}_{\mathrm{B}} \cong \mathbb{C}^{d_2}$, and $\mathcal{H}_{\mathrm{anc}} \cong \mathbb{C}^{r}$. Define the isometries $\Delta : \mathcal{H}_{\mathrm{A}} \to \mathcal{H}_{\mathrm{B}} \otimes \mathcal{H}_{\mathrm{anc}}$ as

$$\Delta \coloneqq \sum_{i=1}^{d_1} |i\rangle_{\mathrm{B,anc}} \langle i|_{\mathrm{A}}.$$

Then, for $U \in \mathbb{U}_{rd_2}$, define the isometries $V_{\varepsilon,U} : \mathcal{H}_{\mathrm{A}} \to \mathbb{C}^2 \otimes \mathcal{H}_{\mathrm{B}} \otimes \mathcal{H}_{\mathrm{anc}}$ as

$$V_{\varepsilon,U} \coloneqq \sqrt{1-\varepsilon^2}|0\rangle \otimes V_0 + \varepsilon|1\rangle \otimes (U\Delta), \tag{17}$$

where $V_0 = \sum_{i=1}^{r} |i\rangle_{\mathrm{anc}} \otimes K_i : \mathcal{H}_{\mathrm{A}} \to \mathcal{H}_{\mathrm{B}} \otimes \mathcal{H}_{\mathrm{anc}}$ is an isometry such that

$$\left|\operatorname{tr}\left(K_i^{\dagger} K_j\right)\right| \leq \frac{2d_1}{r} \cdot \mathbb{1}_{i=j}, \quad \forall i, j \in [r].$$

Then, define the quantum channels $\mathcal{E}_{\varepsilon,U} : \mathcal{L}(\mathcal{H}_{\mathrm{A}}) \to \mathcal{L}(\mathbb{C}^2 \otimes \mathcal{H}_{\mathrm{B}})$ as

$$\mathcal{E}_{\varepsilon,U}(\cdot) \coloneqq \mathrm{tr}_{\mathcal{H}_{\mathrm{anc}}}\left(V_{\varepsilon,U}(\cdot)V_{\varepsilon,U}^{\dagger}\right). \tag{18}$$

The following result is adapted from [OG26].

Lemma 4.1. *Let d_1, d_2, r be positive integers such that $d_1/d_2 \le r \le d_1 d_2$, and $\varepsilon \in (0, 10^{-4})$. There exists a subset $\mathcal{M} \subseteq \mathbb{U}_{rd_2}$ with cardinality $|\mathcal{M}| \ge \exp(rd_1d_2/1201)$ such that for any $U_1, U_2 \in \mathcal{M}$ and $U_1 \ne U_2$, we have*

$$\|\mathcal{E}_{\varepsilon,U_1} - \mathcal{E}_{\varepsilon,U_2}\|_{\diamond} \ge 0.07\varepsilon,$$

where $\mathcal{E}_{\varepsilon,U} \in \mathbf{QChan}^r_{d_1,2d_2}$ is defined in Equation (18). For convenience, we will denote the set of isometries $\{V_{\varepsilon,U} \,|\, U \in \mathcal{M}\} \subseteq \mathbf{ISO}_{d_1,2rd_2}$ as $\mathcal{N}$.

Then, we can prove the lower bound for quantum channel tomography.

Theorem 4.2. *Let d_1, d_2, r be positive integers such that $2d_1/d_2 \le r \le d_1d_2/2$. Suppose $\mathcal{E} \in \mathbf{QChan}^r_{d_1,d_2}$ is an unknown quantum channel. Any algorithm that can output an estimate for $\mathcal{E}$ to within diamond norm error ε with high probability must use at least $n = \Omega(rd_1d_2/\varepsilon^2)$ queries to $\mathcal{E}$.*

Proof. If d_2 is an even number, we call Lemma 4.1 with parameters $(d_1, d_2/2, r)$, and we can find a set of isometries $\mathcal{N} \subseteq \mathbf{ISO}_{d_1,rd_2}$ with cardinality $|\mathcal{N}| \ge \exp(rd_1d_2/C)$ for a universal constant C such that for any $V_1, V_2 \in \mathcal{N}$, the channels $\mathcal{E}_1(\cdot) = \mathrm{tr}_r\left(V_1(\cdot)V_1^{\dagger}\right)$ and $\mathcal{E}_2(\cdot) = \mathrm{tr}_r\left(V_2(\cdot)V_2^{\dagger}\right)$ satisfy

$$\|\mathcal{E}_1 - \mathcal{E}_2\|_{\diamond} \ge 0.07\varepsilon.$$

Suppose $\mathcal{A}$ is an algorithm that can output an estimate of an unknown channel in $\mathbf{QChan}^r_{d_1,d_2}$ to within diamond norm error 0.03ε using n queries to the unknown channel. Then, $\mathcal{A}$ can also solve the discrimination task for the isometries in $\mathcal{N}$ using n queries to the unknown isometry by simply discarding the r-dimensional ancilla system.

On the other hand, note that the set $\mathcal{N}$ (c.f. Lemma 4.1 and Equation (17)) is a "hard" isometry set (see Definition 3.1). Thus, Theorem 3.2 applies, which means $\mathcal{A}$ must use at least $n \ge \Omega(rd_1d_2/\varepsilon^2)$ queries.

If d_2 is an odd number and $r(d_2-1) \ge 2d_1$, then we can simply work with a (d_2-1)-dimensional subspace of the output space and find the set $\mathcal{N}$ by calling Lemma 4.1 with parameters $(d_1, (d_2 - 1)/2, r)$, and everything remains the same as those for the even output dimension case. For the case d_2 is an odd number and $r(d_2 - 1) < 2d_1$, we show a modified construction of $\mathcal{N}$ that works for this case in Appendix A. $\square$

5 Auxiliary facts

We will also use the following well-known facts.

Fact 5.1. *Let $n \ge k$ be positive integers and $p \in [0, 1]$, then*

$$\binom{n}{k} \le \exp(nH(k/n)),$$

and thus

$$\binom{n}{k} p^k (1-p)^{n-k} \le \exp(-nD(k/n\|p)).$$

Proof. Note that $\binom{n}{k} \le \frac{n^n}{k^k(n-k)^{n-k}}$ since

$$\binom{n}{k}\left(\frac{k}{n}\right)^k\left(1-\frac{k}{n}\right)^{n-k} \le \left(\frac{k}{n}+1-\frac{k}{n}\right)^n = 1.$$

$\square$

Fact 5.2. *Suppose M is a positive semidefinite matrix and $|\psi\rangle$ is a vector such that $|\psi\rangle \in \mathrm{supp}(M)$. Then, we have*

$$M \sqsupseteq |\psi\rangle\langle\psi| \iff 1 \ge \langle\psi|M^{-1}|\psi\rangle,$$

where M^{-1} is the pseudo-inverse of M.

Proof.

$$M \sqsupseteq |\psi\rangle\langle\psi| \iff I_{\mathrm{supp}(M)} \sqsupseteq M^{-1/2}|\psi\rangle\langle\psi|M^{-1/2},$$

where $M^{-1/2}$ is the pseudo-inverse of $M^{1/2}$. Then

$$I_{\mathrm{supp}(M)} \sqsupseteq M^{-1/2}|\psi\rangle\langle\psi|M^{-1/2} \iff 1 \ge \mathrm{tr}(M^{-1/2}|\psi\rangle\langle\psi|M^{-1/2}) = \langle\psi|M^{-1}|\psi\rangle.$$

$\square$

Fact 5.3. *Suppose $x, M > 0$, we have*

$$x\ln(M/x) \le M/e.$$

Proof. The derivative of the function $f(x) = x\ln(M/x)$ is $\ln(M/x) - 1$ which is monotonically decreasing and equal to zero when $M = ex$. Therefore, the $f(x) \le f(M/e) = M/e$. $\square$

References

[BHK+19] Frédéric Bouchard, Felix Hufnagel, Dominik Koutnỳ, Aazad Abbas, Alicia Sit, Khabat Heshami, Robert Fickler, and Ebrahim Karimi. Quantum process tomography of a high-dimensional quantum communication channel. *Quantum*, 3:138, 2019.

[BM99] Dagmar Bruß and Chiara Macchiavello. Optimal state estimation for d-dimensional quantum systems. *Physics Letters A*, 253(5-6):249–251, 1999.

[BMQ21] Jessica Bavaresco, Mio Murao, and Marco Túlio Quintino. Strict hierarchy between parallel, sequential, and indefinite-causal-order strategies for channel discrimination. *Physical review letters*, 127(20):200504, 2021.

[BMQ22] Jessica Bavaresco, Mio Murao, and Marco Túlio Quintino. Unitary channel discrimination beyond group structures: Advantages of sequential and indefinite-causal-order strategies. *Journal of Mathematical Physics*, 63(4), 2022.

[Car24] Matthias C Caro. Learning quantum processes and hamiltonians via the pauli transfer matrix. *ACM Transactions on Quantum Computing*, 5(2):1–53, 2024.

[CDP08] Giulio Chiribella, G Mauro D'Ariano, and Paolo Perinotti. Quantum circuit architecture. *Physical review letters*, 101(6):060401, 2008.

[CDP09] Giulio Chiribella, Giacomo Mauro D'Ariano, and Paolo Perinotti. Theoretical framework for quantum networks. *Physical Review A—Atomic, Molecular, and Optical Physics*, 80(2):022339, 2009.

[Cho75] Man-Duen Choi. Completely positive linear maps on complex matrices. *Linear algebra and its applications*, 10(3):285–290, 1975.

[CN97] Isaac L. Chuang and Michael A. Nielsen. Prescription for experimental determination of the dynamics of a quantum black box. *Journal of Modern Optics*, 44(11-12):2455–2467, 1997.

[CWZ24] Kean Chen, Qisheng Wang, and Zhicheng Zhang. Local test for unitarily invariant properties of bipartite quantum states. *arXiv preprint arXiv:2404.04599*, 2024.

[CYZ25] Kean Chen, Nengkun Yu, and Zhicheng Zhang. Quantum channel tomography and estimation by local test. *arXiv preprint arXiv:2512.13614*, 2025.

[DP01] GM D'Ariano and P Lo Presti. Quantum tomography for measuring experimentally the matrix elements of an arbitrary quantum operation. *Physical review letters*, 86(19):4195, 2001.

[FFGO23] Omar Fawzi, Nicolas Flammarion, Aurélien Garivier, and Aadil Oufkir. Quantum channel certification with incoherent measurements. In Gergely Neu and Lorenzo Rosasco, editors, *Proceedings of Thirty Sixth Conference on Learning Theory*, volume 195 of *Proceedings of Machine Learning Research*, pages 1822–1884. PMLR, 12–15 Jul 2023.

[GKKT20] Madalin Guţă, Jonas Kahn, Richard Kueng, and Joel A. Tropp. Fast state tomography with optimal error bounds. *Journal of Physics A: Mathematical and Theoretical*, 53(20):204001, 2020.

[GML25] Filippo Girardi, Francesco Anna Mele, and Ludovico Lami. Random purification channel made simple. *arXiv preprint arXiv:2511.23451*, 2025.

[GMZ+25] Filippo Girardi, Francesco Anna Mele, Haimeng Zhao, Marco Fanizza, and Ludovico Lami. Random stinespring superchannel: converting channel queries into dilation isometry queries. *arXiv preprint arXiv:2512.20599*, 2025.

[Har13] Aram W Harrow. The church of the symmetric subspace. *arXiv preprint arXiv:1308.6595*, 2013.

[Hay98] Masahito Hayashi. Asymptotic estimation theory for a finite-dimensional pure state model. *Journal of Physics A: Mathematical and General*, 31(20):4633, 1998.

[Hay17] Masahito Hayashi. *Quantum information theory*. Springer, 2017.

[HCP23] Hsin-Yuan Huang, Sitan Chen, and John Preskill. Learning to predict arbitrary quantum processes. *PRX Quantum*, 4(4):040337, 2023.

[HHJ+17] Jeongwan Haah, Aram W. Harrow, Zhengfeng Ji, Xiaodi Wu, and Nengkun Yu. Sample-optimal tomography of quantum states. *IEEE Transactions on Information Theory*, page 1–1, 2017.

[HKOT23] Jeongwan Haah, Robin Kothari, Ryan O'Donnell, and Ewin Tang. Query-optimal estimation of unitary channels in diamond distance. In *2023 IEEE 64th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 363–390. IEEE, 2023.

[Jam72] Andrzej Jamiołkowski. Linear transformations which preserve trace and positive semidefiniteness of operators. *Reports on mathematical physics*, 3(4):275–278, 1972.

[KKEG19] Martin Kliesch, Richard Kueng, Jens Eisert, and David Gross. Guaranteed recovery of quantum processes from few measurements. *Quantum*, 3:171, 2019.

[Kra83] Karl Kraus. *States, effects, and operations.* Springer, 1983.

[KW99] Michael Keyl and Reinhard F Werner. Optimal cloning of pure states, testing single clones. *Journal of Mathematical Physics*, 40(7):3283–3299, 1999.

[Leu00] Debbie Wun Chi Leung. *Towards robust quantum computation.* stanford university, 2000.

[MB25] Antonio Anna Mele and Lennart Bittel. Optimal learning of quantum channels in diamond distance. *arXiv preprint arXiv:2512.10214*, 2025.

[MGC+25] Francesco Anna Mele, Filippo Girardi, Senrui Chen, Marco Fanizza, and Ludovico Lami. Random purification channel for passive gaussian bosons. *arXiv preprint arXiv:2512.16878*, 2025.

[MM13] Elizabeth Meckes and Mark Meckes. Spectral measures of powers of random matrices. *Electronic Communications in Probability*, 18:1 – 13, 2013.

[MRL08] Masoud Mohseni, Ali T Rezakhani, and Daniel A Lidar. Quantum-process tomography: Resource analysis of different strategies. *Physical Review A—Atomic, Molecular, and Optical Physics*, 77(3):032322, 2008.

[NC10] Michael A. Nielsen and Isaac L. Chuang. *Quantum computation and quantum information.* Cambridge university press, 2010.

[OG26] Aadil Oufkir and Filippo Girardi. Improved lower bounds for learning quantum channels in diamond distance. *arXiv preprint arXiv:2601.04180*, 2026.

[Ouf23a] Aadil Oufkir. *On Adaptivity in Classical and Quantum Learning.* PhD thesis, Ecole normale supérieure de lyon-ENS LYON, 2023.

[Ouf23b] Aadil Oufkir. Sample-optimal quantum process tomography with non-adaptive incoherent measurements. In *2023 IEEE International Symposium on Information Theory (ISIT)*, page 1919–1924. IEEE, June 2023.

[OW16] Ryan O'Donnell and John Wright. Efficient quantum tomography. In *Proceedings of the Forty-Eighth Annual ACM Symposium on Theory of Computing*, page 899–912, 2016.

[OW17] Ryan O'Donnell and John Wright. Efficient quantum tomography ii. In *Proceedings of the 49th Annual ACM SIGACT Symposium on Theory of Computing*, pages 962–974, 2017.

[PCZ97] J. F. Poyatos, J. I. Cirac, and P. Zoller. Complete characterization of a quantum process: the two-bit quantum gate. *Physical Review Letters*, 78(2):390–393, 1997.

[PSTW25] Angelos Pelecanos, Jack Spilecki, Ewin Tang, and John Wright. Mixed state tomography reduces to pure state tomography. *arXiv preprint arXiv:2511.15806*, 2025.

[PSW25] Angelos Pelecanos, Jack Spilecki, and John Wright. The debiased keyl's algorithm: a new unbiased estimator for full state tomography. *arXiv preprint arXiv:2510.07788*, 2025.

[RAS+24] Gregory Rosenthal, Hugo Aaronson, Sathyawageeswar Subramanian, Animesh Datta, and Tom Gur. Quantum channel testing in average-case distance. *arXiv preprint arXiv:2409.12566*, 2024.

[SSKKG22] Trystan Surawy-Stepney, Jonas Kahn, Richard Kueng, and Madalin Guta. Projected least-squares quantum process tomography. *Quantum*, 6:844, 2022.

[SSW25] Thilo Scharnhorst, Jack Spilecki, and John Wright. Optimal lower bounds for quantum state tomography. *arXiv preprint arXiv:2510.07699*, 2025.

[Sti55] W Forrest Stinespring. Positive functions on C*-algebras. *Proceedings of the American Mathematical Society*, 6(2):211–216, 1955.

[SW22] Mehdi Soleimanifar and John Wright. Testing matrix product states. In *Proceedings of the 2022 Annual ACM-SIAM Symposium on Discrete Algorithms (SODA)*, pages 1679–1701. SIAM, 2022.

[TWZ25] Ewin Tang, John Wright, and Mark Zhandry. Conjugate queries can help. *arXiv preprint arXiv:2510.07622*, 2025.

[Wat18] John Watrous. *The theory of quantum information.* Cambridge university press, 2018.

[WW25] Michael Walter and Freek Witteveen. A random purification channel for arbitrary symmetries with applications to fermions and bosons. *arXiv preprint arXiv:2512.15690*, 2025.

[YMM25] Satoshi Yoshida, Jisho Miyazaki, and Mio Murao. Quantum advantage in storage and retrieval of isometry channels. *arXiv preprint arXiv:2507.10784*, 2025.

[YNM25] Satoshi Yoshida, Ryotaro Niwa, and Mio Murao. Random dilation superchannel. *arXiv preprint arXiv:2512.21260*, 2025.

[Yue23] Henry Yuen. An improved sample complexity lower bound for (fidelity) quantum state tomography. *Quantum*, 7:890, 2023.

[ZLK+24] Haimeng Zhao, Laura Lewis, Ishaan Kannan, Yihui Quek, Hsin-Yuan Huang, and Matthias C Caro. Learning quantum states and unitaries of bounded gate complexity. *PRX Quantum*, 5(4):040306, 2024.

[ZRCK25] Leonardo Zambrano, Sergi Ramos-Calderer, and Richard Kueng. Fast quantum measurement tomography with dimension-optimal error bounds. *arXiv preprint arXiv:2507.04500*, 2025.

A Instantiation with odd output dimension

In this section, we present a construction of "hard" isometry set which induces an ε-net of quantum channels. The construction follows that given in [OG26] (see also Section 4 in our notation), but with a slight modification so that it is adapted to the odd output dimension case.

A.1 Construction

Suppose $d_2 > 1$ is an odd number, $r(d_2-1) < 2d_1$ and $rd_2 \geq 2d_1$. Let $\mathcal{H}_\mathrm{A} \cong \mathbb{C}^{d_1}$, $\mathcal{H}_\mathrm{B} \cong \mathbb{C}^{d_2}$ and $\mathcal{H}_\mathrm{anc} \cong \mathbb{C}^r$ be the input, output and ancilla systems. Note that $d_1 = \frac{r(d_2-1)}{2} + \eta$ for some integers $1 \leq \eta \leq \lfloor \frac{r}{2} \rfloor$. Then, we consider the following decomposition

$$\mathcal{H}_\mathrm{A} = \mathcal{H}_\mathrm{a} \oplus \mathcal{H}'_\mathrm{a},$$

$$\mathcal{H}_\mathrm{B} = \mathcal{H}_\mathrm{b0} \oplus \mathcal{H}_\mathrm{b1} \oplus \mathcal{H}'_\mathrm{b},$$

where

$$\mathcal{H}_\mathrm{a} = \mathrm{span}\left\{ |i\rangle_\mathrm{A} \,\middle|\, 1 \leq i \leq \frac{r(d_2-1)}{2} \right\},$$

$$\mathcal{H}'_\mathrm{a} = \mathrm{span}\left\{ |i\rangle_\mathrm{A} \,\middle|\, \frac{r(d_2-1)}{2} + 1 \leq i \leq d_1 \right\},$$

$$\mathcal{H}_\mathrm{b0} = \mathrm{span}\left\{ |i\rangle_\mathrm{B} \,\middle|\, 1 \leq i \leq \frac{d_2-1}{2} \right\},$$

$$\mathcal{H}_\mathrm{b1} = \mathrm{span}\left\{ |i\rangle_\mathrm{B} \,\middle|\, \frac{d_2+3}{2} \leq i \leq d_2 \right\},$$

$$\mathcal{H}'_\mathrm{b} = \mathrm{span}\left\{ |i\rangle_\mathrm{B} \,\middle|\, i = \frac{d_2+1}{2} \right\}.$$

Then we further consider the following decomposition

$$\mathcal{H}'_\mathrm{b} \otimes \mathcal{H}_\mathrm{anc} = \mathcal{H}'_\mathrm{b0} \oplus \mathcal{H}'_\mathrm{b1},$$

where

$$\mathcal{H}'_\mathrm{b0} = \mathrm{span}\left\{ |i\rangle_\mathrm{B} \otimes |j\rangle_\mathrm{anc} \,\middle|\, i = \frac{d_2+1}{2},\ 1 \leq j \leq \left\lfloor \frac{r}{2} \right\rfloor \right\},$$

$$\mathcal{H}'_\mathrm{b1} = \mathrm{span}\left\{ |i\rangle_\mathrm{B} \otimes |j\rangle_\mathrm{anc} \,\middle|\, i = \frac{d_2+1}{2},\ \left\lfloor \frac{r}{2} \right\rfloor + 1 \leq j \leq r \right\}.$$

Then, note that

$$\dim(\mathcal{H}_\mathrm{a}) = \frac{r(d_2-1)}{2}, \quad \dim(\mathcal{H}'_\mathrm{a}) = \eta \leq \left\lfloor \frac{r}{2} \right\rfloor,$$

$$\dim(\mathcal{H}_\mathrm{b0}) = \dim(\mathcal{H}_\mathrm{b1}) = \frac{(d_2-1)}{2}, \quad \dim(\mathcal{H}'_\mathrm{b}) = 1$$

$$\dim(\mathcal{H}'_\mathrm{b0}) = \left\lfloor \frac{r}{2} \right\rfloor, \quad \dim(\mathcal{H}'_\mathrm{b1}) = r - \left\lfloor \frac{r}{2} \right\rfloor \geq \left\lfloor \frac{r}{2} \right\rfloor.$$

Define the isometry $V_0 : \mathcal{H}_\mathrm{a} \to \mathcal{H}_\mathrm{b0} \otimes \mathcal{H}_\mathrm{anc}$ as

$$V_0 = \sum_{i=1}^{r} |i\rangle_\mathrm{anc} \otimes K_i, \tag{19}$$

such that $K_i : \mathcal{H}_{\mathrm{a}} \to \mathcal{H}_{\mathrm{b0}}$ satisfy

$$\left|\mathrm{tr}\left(K_i^\dagger K_j\right)\right| \le \frac{2\dim(\mathcal{H}_{\mathrm{a}})}{\dim(\mathcal{H}_{\mathrm{anc}})} \cdot \mathbb{1}_{i=j},$$

where the existence of such isometry is proven in [OG26, Appendix B]. Define $V_0' : \mathcal{H}_{\mathrm{a}}' \to \mathcal{H}_{\mathrm{b0}}'$ be an arbitrary isometry. Define $\Delta : \mathcal{H}_{\mathrm{a}} \to \mathcal{H}_{\mathrm{b1}} \otimes \mathcal{H}_{\mathrm{anc}}$ be an arbitrary isometry. Define $\Delta' : \mathcal{H}_{\mathrm{a}}' \to \mathcal{H}_{\mathrm{b1}}'$ be an arbitrary isometry. Then, for $\varepsilon \in (0,1)$ and $U \in \mathbb{U}_{r(d_2-1)/2}$, we define the isometry $V_{\varepsilon,U} : \mathcal{H}_{\mathrm{A}} \to \mathcal{H}_{\mathrm{B}} \otimes \mathcal{H}_{\mathrm{anc}}$ as

$$V_{\varepsilon,U} \coloneqq \sqrt{1-\varepsilon^2}(V_0 + V_0') + \varepsilon(U\Delta + \Delta'), \tag{20}$$

where U acts on $\mathcal{H}_{\mathrm{b1}} \otimes \mathcal{H}_{\mathrm{anc}}$ and $V_0 + V_0' = V_0 \oplus V_0'$, $U\Delta + \Delta' = U\Delta \oplus \Delta'$ are both direct sums of linear operators. Moreover, the image of $U\Delta + \Delta'$ (i.e., $(\mathcal{H}_{\mathrm{b1}} \otimes \mathcal{H}_{\mathrm{anc}}) \oplus \mathcal{H}_{\mathrm{b1}}'$) is orthogonal to the image of $V_0 + V_0'$ (i.e., $(\mathcal{H}_{\mathrm{b0}} \otimes \mathcal{H}_{\mathrm{anc}}) \oplus \mathcal{H}_{\mathrm{b0}}'$). Therefore, any subset of $\{V_{\varepsilon,U} \,|\, U \in \mathbb{U}_{r(d_2-1)/2}\}$ is a "hard" isometry set.

A.2 Existence

We have shown that any subset of $\{V_{\varepsilon,U} \,|\, U \in \mathbb{U}_{r(d_2-1)/2}\}$ (see Equation (20)) is a "hard" isometry set. Then, we prove that there exists a large subset with good separation property.

Theorem A.1. *There exists a finite subset $\mathcal{N}$ of $\{V_{\varepsilon,U} \,|\, U \in \mathbb{U}_{r(d_2-1)/2}\}$ for $V_{\varepsilon,U}$ defined in Equation (20) with cardinality $|\mathcal{N}| \ge \exp(rd_1d_2/100001)$, such that for any $V_1 \neq V_2 \in \mathcal{N}$ we have*

$$\|\,\mathrm{tr}_{\mathcal{H}_{\mathrm{anc}}}(V_1(\cdot)V_1^\dagger) - \mathrm{tr}_{\mathcal{H}_{\mathrm{anc}}}(V_2(\cdot)V_2^\dagger)\|_\diamond \ge 0.07\varepsilon.$$

Proof. The proof follows essentially the argument in [OG26], with slight modifications. First, we need the following lemma.

Lemma A.2. *There exists a finite subset $\mathcal{M} \subseteq \mathbb{U}_{r(d_2-1)/2}$ with cardinality $|\mathcal{M}| \ge \exp(rd_1d_2/100001)$ such that for any $U_1 \neq U_2 \in \mathcal{M}$,*

$$\frac{1}{d_1}\left\|\mathrm{tr}_{\mathcal{H}_{\mathrm{anc}}}\Big((|V_0\rangle\!\rangle + |V_0'\rangle\!\rangle)\Big(\langle\!\langle U_1\Delta| - \langle\!\langle U_2\Delta|\Big)\Big)\right\|_1 \ge 0.05. \tag{21}$$

Define the quantum channel $\mathcal{E}_{\varepsilon,U} : \mathcal{L}(\mathcal{H}_{\mathrm{A}}) \to \mathcal{L}(\mathcal{H}_{\mathrm{B}})$ as

$$\mathcal{E}_{\varepsilon,U}(\cdot) \coloneqq \mathrm{tr}_{\mathcal{H}_{\mathrm{anc}}}\left(V_{\varepsilon,U}(\cdot)V_{\varepsilon,U}^\dagger\right).$$

Let $C_{\mathcal{E}}$ denote the (unnormalized) Choi state of quantum channel $\mathcal{E}$ and $\mathcal{M}$ be the set given in Lemma A.2. Then, for any $U_1 \neq U_2 \in \mathcal{M}$, we have

$$\begin{aligned}\left\|C_{\mathcal{E}_{\varepsilon,U_1}} - C_{\mathcal{E}_{\varepsilon,U_2}}\right\|_1 &= \left\|\,\mathrm{tr}_{\mathcal{H}_{\mathrm{anc}}}(|V_{\varepsilon,U_1}\rangle\!\rangle\langle\!\langle V_{\varepsilon,U_1}|) - \mathrm{tr}_{\mathcal{H}_{\mathrm{anc}}}(|V_{\varepsilon,U_2}\rangle\!\rangle\langle\!\langle V_{\varepsilon,U_2}|)\,\right\|_1 \\ &= \Big\|\varepsilon^2\Big(\,\mathrm{tr}_{\mathcal{H}_{\mathrm{anc}}}(|\Delta_{U_1}\rangle\!\rangle\langle\!\langle \Delta_{U_1}|) - \mathrm{tr}_{\mathcal{H}_{\mathrm{anc}}}(|\Delta_{U_2}\rangle\!\rangle\langle\!\langle \Delta_{U_2}|)\Big) \\ &\qquad + \varepsilon\sqrt{1-\varepsilon^2}\,\mathrm{tr}_{\mathcal{H}_{\mathrm{anc}}}\Big(|V_0 + V_0'\rangle\!\rangle\langle\!\langle (U_1 - U_2)\Delta|\Big) \\ &\qquad + \varepsilon\sqrt{1-\varepsilon^2}\,\mathrm{tr}_{\mathcal{H}_{\mathrm{anc}}}\Big(|(U_1 - U_2)\Delta\rangle\!\rangle\langle\!\langle V_0 + V_0'|\Big)\Big\|_1 \\ &\ge \varepsilon\sqrt{1-\varepsilon^2}\Big\|\,\mathrm{tr}_{\mathcal{H}_{\mathrm{anc}}}\Big(|V_0 + V_0'\rangle\!\rangle\langle\!\langle (U_1 - U_2)\Delta|\Big)\end{aligned} \tag{22}$$

$$+ \operatorname{tr}_{\mathcal{H}_{\mathrm{anc}}}\Big(|(U_1-U_2)\Delta\rangle\!\rangle\langle\!\langle V_0+V_0'|\Big)\Big\|_1 - 2\varepsilon^2 d_1 \tag{23}$$

$$= 2\varepsilon\sqrt{1-\varepsilon^2}\Big\| \operatorname{tr}_{\mathcal{H}_{\mathrm{anc}}}\Big(|V_0+V_0'\rangle\!\rangle\langle\!\langle (U_1-U_2)\Delta|\Big)\Big\|_1 - 2\varepsilon^2 d_1 \tag{24}$$

$$\geq 0.1\varepsilon\sqrt{1-\varepsilon^2}d_1 - 2\varepsilon^2 d_1 \tag{25}$$

$$\geq 0.07\varepsilon d_1. \tag{26}$$

In Equation (22) we define $\Delta_U = U\Delta + \Delta'$. In Equation (23) we used

$$\|\operatorname{tr}_{\mathcal{H}_{\mathrm{anc}}}(|\Delta_U\rangle\!\rangle\langle\!\langle\Delta_U|)\|_1 = \operatorname{tr}(|\Delta_U\rangle\!\rangle\langle\!\langle\Delta_U|) = \dim(\mathcal{H}_{\mathrm{a}}) + \dim(\mathcal{H}_{\mathrm{a}}') = d_1.$$

In Equation (24) we used the fact that $\operatorname{tr}_{\mathcal{H}_{\mathrm{anc}}}\Big(|V_0+V_0'\rangle\!\rangle\langle\!\langle(U_1-U_2)\Delta|\Big)$ is a linear operator supported on $\mathcal{H}_{\mathrm{A}}\otimes\mathcal{H}_{\mathrm{b1}}$ and its image is in $\mathcal{H}_{\mathrm{A}}\otimes(\mathcal{H}_{\mathrm{b0}}\oplus\mathcal{H}_{\mathrm{b}}')$, which is orthogonal to $\mathcal{H}_{\mathrm{A}}\otimes\mathcal{H}_{\mathrm{b1}}$; and for any linear operator X such that $X^2=0$, we have

$$\|X+X^\dagger\|_1 = \operatorname{tr}\left(\sqrt{(X+X^\dagger)^2}\right) = \operatorname{tr}\left(\sqrt{XX^\dagger + X^\dagger X}\right) = \operatorname{tr}\left(\sqrt{XX^\dagger}\right) + \operatorname{tr}\left(\sqrt{X^\dagger X}\right),$$

where the last equality is because $\operatorname{supp}(XX^\dagger)\perp\operatorname{supp}(X^\dagger X)$. In Equation (25) we used Equation (21). In Equation (26) we used that $\varepsilon\leq 0.01$. Therefore, we can lower bound the diamond norm

$$\|\mathcal{E}_{\varepsilon,U_1}-\mathcal{E}_{\varepsilon,U_2}\|_\diamond \geq \frac{1}{d}\left\|C_{\mathcal{E}_{\varepsilon,U_1}} - C_{\mathcal{E}_{\varepsilon,U_2}}\right\|_1 \geq 0.07\varepsilon.$$

Thus, the set $\mathcal{N} = \{V_{\varepsilon,U}\,|\,U\in\mathcal{M}\}$ is the desired set. □

A.3 Proof of Lemma A.2

Proof. Let $\hat{V}_0 \coloneqq V_0 + V_0'$. Note that $\hat{V}_0 : \mathcal{H}_{\mathrm{A}} \to (\mathcal{H}_{\mathrm{b0}}\oplus\mathcal{H}_{\mathrm{b}}')\otimes\mathcal{H}_{\mathrm{anc}}$ is an isometry. The isometry $\hat{V}_0$ can also be written as

$$\hat{V}_0 = \sum_{i=1}^{r}|i\rangle_{\mathrm{anc}}\otimes\left(K_i\oplus\left|\frac{d_2+1}{2}\right\rangle\langle z_i|\right),$$

where K_i are defined in Equation (19), $\{|z_i\rangle\}_{i=1}^{\eta}$ are an orthonormal basis of $\mathcal{H}_{\mathrm{a}}'$ and $|z_i\rangle = 0$ for $\eta < i \leq r$. Let us define

$$K_i' = K_i \oplus \left|\frac{d_2+1}{2}\right\rangle\langle z_i|,$$

then K_i' satisfy

$$\left|\operatorname{tr}\left(K_i'^\dagger K_j'\right)\right| = \left|\operatorname{tr}\left(K_i^\dagger K_j\right) + \mathbb{1}_{i=j\in[\eta]}\right| \leq \left(\frac{2\dim(\mathcal{H}_{\mathrm{a}})}{\dim(\mathcal{H}_{\mathrm{anc}})}+1\right)\cdot\mathbb{1}_{i=j} \leq \frac{3\dim(\mathcal{H}_{\mathrm{A}})}{\dim(\mathcal{H}_{\mathrm{anc}})}\cdot\mathbb{1}_{i=j} = \frac{3d_1}{r}\cdot\mathbb{1}_{i=j}, \tag{27}$$

where in the last inequality we used that $\dim(\mathcal{H}_{\mathrm{a}}) = r(d_2-1)/2 \geq r = \dim(\mathcal{H}_{\mathrm{anc}})$ and $\dim(\mathcal{H}_{\mathrm{a}}) \leq \dim(\mathcal{H}_{\mathrm{A}})$. On the other hand, $U\Delta$ is an isometry from $\mathcal{H}_{\mathrm{a}}\subseteq\mathcal{H}_{\mathrm{A}}$ to $\mathcal{H}_{\mathrm{b1}}\otimes\mathcal{H}_{\mathrm{anc}}$.

Then, we need the following lemma:

Lemma A.3. *For $U_x, U_y \in \mathbb{U}_{r(d_2-1)/2}$, let us define*

$$F(U_x,U_y) = \frac{1}{d_1}\operatorname{tr}_{\mathcal{H}_{\mathrm{anc}}}\left(|\hat{V}_0\rangle\!\rangle\left(\langle\!\langle U_x\Delta| - \langle\!\langle U_y\Delta|\right)\right),$$

then the function $f(U_x, U_y) = \|F(U_x, U_y)\|_1 = \mathrm{tr}(|F(U_x, U_y)|)$ *is* $\sqrt{\frac{2}{d_1}}$*-Lipschitz with respect to the* ℓ_2*-sum of the 2-norms (Frobenius norm). Furthermore, for independent random* $U_x, U_y \sim \mathbb{U}_{r(d_2-1)/2}$*, we have* $\mathbf{E}\big[\mathrm{tr}(|F(U_x, U_y)|^2)\big] = \frac{d_2-1}{d_1}$*, and* $\mathbf{E}\big[\mathrm{tr}(|F(U_x, U_y)|^4)\big] \leq \frac{288}{r^3}$*.*

By the Hölder's inequality we have

$$\mathbf{E}\Big[\mathrm{tr}\big(|F(U_x, U_y)|^2\big)\Big] \leq \mathbf{E}\Big[\mathrm{tr}\big(|F(U_x, U_y)|^4\big)\Big]^{1/3} \mathbf{E}[\mathrm{tr}(|F(U_x, U_y)|)]^{2/3},$$

which, combined with Lemma A.3, implies

$$\mathbf{E}[\mathrm{tr}(|F(U_x, U_y)|)]^2 \geq \frac{(d_2-1)^3 r^3}{288 \cdot d_1^3} \geq \frac{2^3 \cdot 8}{3^3 \cdot 288} = \frac{2}{243},$$

where we used that $d_2 - 1 \geq 2d_2/3$ and $rd_2 \geq 2d_1$. Thus $\mathbf{E}[\mathrm{tr}(|F(U_x, U_y)|)] > 9/100$. Then, we can use a generalized Levy's lemma on compact groups [MM13, Corollary 17] to prove the concentration result:

$$\Pr\left[\mathrm{tr}(|F(U_x, U_y)|) \leq \frac{1}{20}\right] \leq \exp\left(-\frac{r(d_2-1)}{2} \cdot \frac{d_1}{25^2 \cdot 12 \cdot 2}\right) = \exp\left(-\frac{rd_1(d_2-1)}{30000}\right) \leq \exp\left(-\frac{rd_1d_2}{50000}\right).$$

Then, we independently sample $\exp(rd_1d_2/100001)$ Haar random unitaries in $\mathbb{U}_{r(d_2-1)/2}$ and the union bound shows that there exists a non-zero probability that for any pair U_x, U_y, we have $\mathrm{tr}(|F(U_x, U_y)|) \geq 1/20$. Thus, there exists a set with cardinality $\geq \exp(rd_1d_2/100001)$ such that Equation (21) holds. □

A.4 Proof of Lemma A.3

Proof. For the Lipschitz continuity, the proof is the same as that given in [OG26].

Define $K_{x,i} = \langle i|_{\mathrm{anc}} U_x \Delta$, $K_{y,i} = \langle i|_{\mathrm{anc}} U_y \Delta$. This means

$$F(U_x, U_y) = \frac{1}{d_1}\sum_{i=1}^{r} |K_i'\rangle\!\rangle \Big(\langle\!\langle K_{x,i}| - \langle\!\langle K_{y,i}|\Big).$$

Then, we note that

$$\begin{aligned}
\mathbf{E}\big[\mathrm{tr}(|F(U_x, U_y)|^2)\big] &= \frac{1}{d_1^2}\mathbf{E}\left[\mathrm{tr}\left(\sum_{i,j=1}^{r} |K_i'\rangle\!\rangle \Big(\langle\!\langle K_{x,i}| - \langle\!\langle K_{y,i}|\Big)\Big(|K_{x,j}\rangle\!\rangle - |K_{y,j}\rangle\!\rangle\Big)\langle\!\langle K_j'|\right)\right] \\
&= \frac{1}{d_1^2}\mathbf{E}\left[\sum_{i}^{r} \langle\!\langle K_i'|K_i'\rangle\!\rangle \Big(\langle\!\langle K_{x,i}| - \langle\!\langle K_{y,i}|\Big)\Big(|K_{x,i}\rangle\!\rangle - |K_{y,i}\rangle\!\rangle\Big)\right] \\
&= \frac{2}{d_1^2}\sum_{i=1}^{r} \langle\!\langle K_i'|K_i'\rangle\!\rangle \frac{\dim(\mathcal{H}_{\mathrm{a}})}{r} && (28) \\
&= \frac{2}{d_1^2}\frac{\dim(\mathcal{H}_{\mathrm{A}})\dim(\mathcal{H}_{\mathrm{a}})}{r} && (29) \\
&= \frac{d_2-1}{d_1}
\end{aligned}$$

where Equation (28) is because for $z_1, z_2 \in \{x, y\}$, we have

$$\mathbf{E}[\langle\!\langle K_{z_1,i}|K_{z_2,i}\rangle\!\rangle] = \mathbf{E}\Big[\mathrm{tr}\Big(K_{z_1,i}^\dagger K_{z_2,i}\Big)\Big] = \mathrm{tr}\Big(\Delta^\dagger\, \mathbf{E}\Big[U_{z_1}^\dagger |i\rangle_{\mathrm{anc}}\langle i|_{\mathrm{anc}} U_{z_2}\Big]\,\Delta\Big)$$

$$
\begin{aligned}
&= \mathbb{1}_{z_1=z_2}\frac{1}{r}\operatorname{tr}(\Delta^\dagger\Delta) && (30)\\
&= \mathbb{1}_{z_1=z_2}\frac{\dim(\mathcal{H}_\mathrm{a})}{r},
\end{aligned}
$$

where Equation (30) is due to Schur's lemma, and Equation (29) is because $\sum_i \langle\!\langle K_i'|K_i'\rangle\!\rangle = \operatorname{tr}(\sum_i K_i'^\dagger K_i) = \operatorname{tr}(I_\mathrm{A}) = \dim(\mathcal{H}_\mathrm{A})$.

Then, we

$$
\begin{aligned}
\mathbf{E}\big[\operatorname{tr}(|F(U_x,U_y)|^4)\big] &= \frac{1}{d_1^4}\mathbf{E}\Bigg[\sum_{i,j,k,l=1}^{r}\operatorname{tr}\Big(|K_i'\rangle\!\rangle\Big(\langle\!\langle K_{x,i}|-\langle\!\langle K_{y,i}|\Big)\Big(|K_{x,j}\rangle\!\rangle-|K_{y,j}\rangle\!\rangle\Big)\langle\!\langle K_j'| && (31)\\
&\qquad |K_k'\rangle\!\rangle\Big(\langle\!\langle K_{x,k}|-\langle\!\langle K_{y,k}|\Big)\Big(|K_{x,l}\rangle\!\rangle-|K_{y,l}\rangle\!\rangle\Big)\langle\!\langle K_l'|\Big)\Bigg]\\
&\le \frac{9}{r^2d_1^2}\sum_{i,j=1}^{r}\mathbf{E}\left[\left|\Big(\langle\!\langle K_{x,i}|-\langle\!\langle K_{y,i}|\Big)\Big(|K_{x,j}\rangle\!\rangle-|K_{y,j}\rangle\!\rangle\Big)\right|^2\right] && (32)\\
&\le \frac{36}{r^2d_1^2}\sum_{i,j=1}^{r}\mathbf{E}\big[|\langle\!\langle K_{x,i}|K_{x,j}\rangle\!\rangle|^2+|\langle\!\langle K_{y,i}|K_{y,j}\rangle\!\rangle|^2+|\langle\!\langle K_{x,i}|K_{y,j}\rangle\!\rangle|^2+|\langle\!\langle K_{y,i}|K_{x,j}\rangle\!\rangle|^2\big]\\
&\le \frac{72}{r^2d_1^2}\sum_{i,j=1}^{r}\mathbf{E}\big[|\langle\!\langle K_{x,i}|K_{x,j}\rangle\!\rangle|^2+|\langle\!\langle K_{y,i}|K_{y,j}\rangle\!\rangle|^2\big] && (33)\\
&= \frac{144}{r^2d_1^2}\sum_{i,j=1}^{r}\mathbf{E}\big[|\langle\!\langle K_{x,i}|K_{x,j}\rangle\!\rangle|^2\big]\,,\\
&\le \frac{144}{r^2d_1^2}\sum_{i,j=1}^{r}\frac{d_\mathrm{a}}{(rd_\mathrm{b})^2-1}\left(d_\mathrm{b}+\mathbb{1}_{i=j}d_\mathrm{a}d_\mathrm{b}^2-\frac{1}{d_\mathrm{b}r}\left(\mathbb{1}_{i=j}d_\mathrm{b}^2+d_\mathrm{a}d_\mathrm{b}\right)\right) && (34)\\
&\le \frac{144}{r^2}\cdot\frac{1}{d_\mathrm{a}}\cdot\frac{1}{(rd_\mathrm{b})^2-1}\left(r^2d_\mathrm{b}+rd_\mathrm{a}d_\mathrm{b}^2-d_\mathrm{b}-rd_\mathrm{a}\right) && (35)\\
&= \frac{144}{r^2}\left(\frac{1}{d_\mathrm{a}d_\mathrm{b}}+\frac{1}{r}+\frac{1-d_\mathrm{b}^2+d_\mathrm{a}d_\mathrm{b}/r-d_\mathrm{a}d_\mathrm{b}r}{d_\mathrm{a}d_\mathrm{b}(r^2d_\mathrm{b}^2-1)}\right)\\
&\le \frac{288}{r^3}, && (36)
\end{aligned}
$$

where Equation (32) is because Equation (27), Equation (33) is because

$$
\begin{aligned}
\sum_{i,j=1}^{r}|\langle\!\langle K_{x,i}|K_{y,j}\rangle\!\rangle|^2 &= \|K_x^\dagger K_y\|_F^2 = \operatorname{tr}\Big(K_x^\dagger K_y K_y^\dagger K_x\Big) \le \|K_xK_x^\dagger\|_F\cdot\|K_yK_y^\dagger\|_F\\
&\le \frac{1}{2}\left(\|K_x^\dagger K_x\|_F^2+\|K_y^\dagger K_y\|_F^2\right) = \frac{1}{2}\left(\sum_{i,j=1}^{r}|\langle\!\langle K_{x,i}|K_{x,j}\rangle\!\rangle|^2+\sum_{i,j=1}^{r}|\langle\!\langle K_{y,i}|K_{y,j}\rangle\!\rangle|^2\right),
\end{aligned}
$$

where K_x denotes the matrix with columns $|K_{x,i}\rangle\!\rangle$, Equation (34) is due to exactly the same argument as that in Eq. (79) in [OG26] and we set $d_\mathrm{a} = \dim(\mathcal{H}_\mathrm{a})$, $d_\mathrm{b} = \dim(\mathcal{H}_\mathrm{b1})$, Equation (35) uses $d_1 \ge d_\mathrm{a}$ and Equation (36) uses $d_\mathrm{a}d_\mathrm{b} = r(d_2-1)^2/4 \ge r$. $\square$