

Quantum Channel Certification with Incoherent Strategies

Omar Fawzi

Univ Lyon, Inria, ENS Lyon, UCBL, LIP, F-69342, Lyon Cedex 07, France

OMAR.FAWZI@ENS-LYON.FR

Nicolas Flammarion

EPFL, Lausanne, Switzerland

NICOLAS.FLAMMARION@EPFL.CH

Aurélien Garivier

Univ Lyon, ENS de Lyon, UMPA UMR 5669, F-69364 Lyon Cedex 07, France

AURELIEN.GARIVIER@ENS-LYON.FR

Aadil Oufkir

Univ Lyon, Inria, ENS Lyon, UCBL, LIP, F-69342, Lyon Cedex 07, France

AADIL.OUFKIR@ENS-LYON.FR

Editors: Gergely Neu and Lorenzo Rosasco

Abstract

In the problem of quantum channel certification, we have black box access to a quantum process and would like to decide if this process matches some predefined specification or is ε -far from this specification. The objective is to achieve this task while minimizing the number of times the black box is used. Here, we focus on optimal incoherent strategies for two relevant extreme cases of channel certification. The first one is when the predefined specification is a unitary channel, e.g., a gate in a quantum circuit. In this case, we show that testing whether the black box is described by a fixed unitary operator in dimension d or ε -far from it in the trace norm requires $\Theta(d/\varepsilon^2)$ uses of the black box. The second setting we consider is when the predefined specification is a completely depolarizing channel with input dimension d_{in} and output dimension d_{out} . In this case, we prove that, in the non-adaptive setting, $\tilde{\Theta}(d_{\text{in}}^2 d_{\text{out}}^{1.5}/\varepsilon^2)$ uses of the channel are necessary and sufficient to verify whether it is equal to the depolarizing channel or ε -far from it in the diamond norm. Finally, we prove a lower bound of $\Omega(d_{\text{in}}^2 d_{\text{out}}/\varepsilon^2)$ for this problem in the adaptive setting. Note that the special case $d_{\text{in}} = 1$ corresponds to the well-studied quantum state certification problem.

Keywords: Quantum testing, testing identity, quantum channel, adaptive strategies.

1. Introduction

We consider the problem of quantum channel certification which consists in verifying whether a quantum process to which we have black box access behaves as intended. A valid process in quantum theory is modeled by a quantum channel. A quantum channel with input dimension d_{in} and output dimension d_{out} is a linear map $\mathbb{C}^{d_{\text{in}} \times d_{\text{in}}} \rightarrow \mathbb{C}^{d_{\text{out}} \times d_{\text{out}}}$ satisfying some positivity and normalization conditions (see Section 2 for details). Given a complete description of a known quantum channel \mathcal{N}_0 and N copies of an unknown quantum channel \mathcal{N} that can be either \mathcal{N}_0 or ε -far from it, at each step $1 \leq t \leq N$, we can choose an input quantum state, send it through the unknown process \mathcal{N} then measure the output quantum state. After collecting a sufficient amount of classical observations, our goal is to decide in which case is the quantum channel \mathcal{N} with high probability and while minimizing N . We also call this problem testing identity to the quantum channel \mathcal{N}_0 .

This testing task is important for many reasons. Firstly, the building blocks of a quantum computation are unitary gates. It is thus important to understand the complexity of checking that an unknown channel implements a given gate as specified. Secondly, quantum channel certification

is the natural generalization of the quantum state certification. Indeed, if the channels are constant quantum states, then testing them becomes equivalent to testing those states. It might seem at first sight that using the Choi–Jamiołkowski isomorphism, quantum channel certification can be obtained by applying quantum state certification algorithms to the corresponding Choi states. However, there are at least two reasons this is not true: first, in models where an auxiliary system is not allowed the Choi state cannot easily be prepared from a black box implementing the channel and second, the natural notion of distance for channels does not correspond to the trace distance between Choi states. Finally, quantum process tomography, the problem of learning completely a channel in the diamond norm is costly (Surawy-Stepney et al., 2022; Oufkir, 2023), and our hope is that certification can be done with fewer copies than full tomography.

In this paper, we focus on two extreme cases, $\mathcal{N}_0(\rho) = \mathcal{N}_U(\rho) = U\rho U^\dagger$ is a unitary channel where U is a unitary matrix and $\mathcal{N}_0(\rho) = \mathcal{D}(\rho) = \text{Tr}(\rho)\frac{\mathbb{I}}{d_{\text{out}}}$ is the completely depolarizing channel.

Contribution. We propose an incoherent ancilla-free testing algorithm for testing identity to a fixed unitary channel \mathcal{N}_U in the trace distance using $\mathcal{O}(d/\varepsilon^2)$ measurements (here $d_{\text{in}} = d_{\text{out}} = d$). The tester chooses a random input state and measures with the corresponding POVM conjugated by the unitary U . This result is stated in Thm. 1. The standard inequality relating the 1-norm of a Choi state and the diamond norm of the channel only implies an upper bound $\mathcal{O}(d^2/\varepsilon^2)$. We obtain the quadratic improvement in the dimension dependency by proving a new inequality between the entanglement fidelity and the trace distance to the identity channel (Lem. 10). Moreover, we establish a matching lower bound of $\Omega(d/\varepsilon^2)$ for testing identity to a fixed unitary channel in the trace distance. This lower bound applies even for ancilla-assisted strategies. For this, we construct a well-chosen distribution of channels ε -far from the identity channel. After a sufficient number of measurements, the observations under the two hypotheses should be distinguishable, i.e., the (Kullback-Leibler) KL divergence is $\Omega(1)$. However, we can show that for this particular choice of distribution over channels, any adaptive tester can only increase the KL divergence by at most $\mathcal{O}(\varepsilon^2/d)$ after a measurement no matter the dependence on the previous observations. The lower bound is stated and proved in Thm. 11.

Concerning the certification of the completely depolarizing channel $\mathcal{D}(\rho) = \text{Tr}(\rho)\frac{\mathbb{I}}{d_{\text{out}}}$, we propose an incoherent ancilla-free strategy to distinguish between $\mathcal{N} = \mathcal{D}$ and \mathcal{N} is ε -far from it in the diamond distance using $\mathcal{O}(d_{\text{in}}^2 d_{\text{out}}^{1.5}/\varepsilon^2)$ measurements (see Thm. 5). For this we show how to reduce this certification problem to the certification of the maximally mixed state (testing mixedness) $\frac{\mathbb{I}}{d_{\text{out}}}$. We choose the input state $|\phi\rangle\langle\phi|$ randomly and we compare the 2-norm between the output state $\mathcal{N}(|\phi\rangle\langle\phi|)$ and the maximally mixed state $\frac{\mathbb{I}}{d_{\text{out}}}$. We show that with at least a probability $\Omega(1)$, we have $Y = \|\mathcal{N}(|\phi\rangle\langle\phi|) - \mathbb{I}/d_{\text{out}}\|_2^2 \geq \varepsilon^2/(4d_{\text{out}}d_{\text{in}}^2)$. This inequality is sufficient to obtain the required complexity, however, it requires some work to be proved. First, we show a similar inequality in expectation using Weingarten calculus. Then we control the variance of the random variable Y carefully in a way that this upper bound depends on the actual difficulty of the problem, mainly the expectation of Y and the diamond distance between \mathcal{N} and \mathcal{D} . Next, we obtain the anti-concentration inequality using the Paley-Zygmund inequality.

On the other hand, we establish a lower bound of $\Omega(d_{\text{in}}^2 d_{\text{out}}^{1.5}/(\log(d_{\text{in}}d_{\text{out}}/\varepsilon)^2\varepsilon^2))$ for testing identity to the depolarizing channel with non-adaptive strategies (Thm. 6). For this, we construct a random quantum channel whose output states are almost $\mathcal{O}(\varepsilon/d_{\text{in}})$ -close (in the 1-norm) to the maximally mixed state $\frac{\mathbb{I}}{d_{\text{out}}}$ except for a neighborhood of an input state chosen randomly whose output is ε -far from $\frac{\mathbb{I}}{d_{\text{out}}}$ in the 1-norm. Then we use LeCam’s method (LeCam, 1973) as in (Bubeck et al.,

Testing identity to \mathcal{N}_0	Lower bound <i>Ancilla-assisted</i>	Upper bound <i>Ancilla-free</i>
$\mathcal{N}_0 = \mathcal{N}_U$ adaptive strategies in trace distance d_{Tr}	$\Omega\left(\frac{d}{\varepsilon^2}\right)$, Thm. 1	$\mathcal{O}\left(\frac{d}{\varepsilon^2}\right)$, Thm. 1
$\mathcal{N}_0 = \mathcal{N}_U$ adaptive strategies in diamond distance d_\diamond	$\Omega\left(\frac{d}{\varepsilon^2}\right)$, Thm. 1	$\mathcal{O}\left(\frac{d}{\varepsilon^4}\right)$, Thm. 1
$\mathcal{N}_0 = \mathcal{D}$ non-adaptive strategies	$\Omega\left(\frac{d_{\text{in}}^2 d_{\text{out}}^{1.5}}{\log(d_{\text{in}} d_{\text{out}}/\varepsilon)^2 \varepsilon^2}\right)$, Thm. 6	$\mathcal{O}\left(\frac{d_{\text{in}}^2 d_{\text{out}}^{1.5}}{\varepsilon^2}\right)$, Thm. 5
$\mathcal{N}_0 = \mathcal{D}$ adaptive strategies	$\Omega\left(\frac{d_{\text{in}}^2 d_{\text{out}} + d_{\text{out}}^{1.5}}{\varepsilon^2}\right)$, Thm. 7	$\mathcal{O}\left(\frac{d_{\text{in}}^2 d_{\text{out}}^{1.5}}{\varepsilon^2}\right)$, Thm. 5

Table 1: Lower and upper bounds for testing identity of quantum channels in the diamond and trace distances using incoherent strategies. \mathcal{N}_U is the unitary quantum channel $\mathcal{N}_U(\rho) = U\rho U^\dagger$ and \mathcal{D} is the depolarizing channel $\mathcal{D}(\rho) = \text{Tr}(\rho)\frac{\mathbb{I}}{d_{\text{out}}}$. Our proposed algorithms (upper bounds) are ancilla-free while the lower bounds hold even for ancilla-assisted algorithms.

2020) with some differences. First, we need to condition on the event that the input states chosen by the testing algorithm have very small overlaps with the best input state. This conditioning is the main reason for the additional logarithmic factor we obtain in the lower bound. Next, with a construction using random matrices with Gaussian entries rather than Haar distributed unitaries, we can invoke hypercontractivity (Aubrun and Szarek, 2017, Proposition 5.48) which allows us to control all the moments once we upper bound the second moment. In the special case $d_{\text{in}} = 1$, this recovers a result of (Bubeck et al., 2020) while significantly simplifying their analysis. Furthermore, a lower bound of $\Omega(d_{\text{in}}^2 d_{\text{out}}/\varepsilon^2)$ is proved for adaptive strategies (Thm. 7) using the same construction. In this proof, we use Kullback-Leibler divergence instead of the Total-Variation distance. We refer to Table 1 for a summary of these results.

Related work. Testing identity to a unitary channel can be seen as a generalization of the usual testing identity problem for discrete distributions (Valiant and Valiant, 2016) and quantum states (Chen et al., 2022f). However, in the worst-case setting, testing identity to the identity channel requires $\Omega(d/\varepsilon^2)$ measurements in contrast to testing identity to a rank 1 quantum state or a Dirac distribution which can be done with only $\mathcal{O}(1/\varepsilon^2)$ measurements/samples. Also, in the definition of testing identity to a unitary channel problem, we don't require the *unknown* tested channel to be unitary. In this latter setting, efficient tests can be designed easily if an auxiliary system is allowed. This can be found along with other tests on properties of unitary channels in (Wang, 2011). We also refer to the survey (Montanaro and de Wolf, 2013) for other examples of tests on unitary channels. Since a unitary channel has a Choi rank equal to 1 and the depolarizing channel has a Choi rank equal to $d_{\text{in}}d_{\text{out}}$, this work is a first step to obtain instance-optimal quantum channel certification as for the classical case (Valiant and Valiant, 2016) or quantum states (Chen et al., 2022f). On the other hand, testing identity to the completely depolarizing channel is a generalization of identity testing of distributions (Diakonikolas et al., 2017) and testing mixedness of states (Bubeck et al., 2020; Chen et al., 2022d). In particular, if the input dimension is $d_{\text{in}} = 1$, the channels are constant and the problem reduces to a testing mixedness of states of dimension d_{out} . In this case, we recover the optimal complexity of (Bubeck et al., 2020; Chen et al., 2022d). Another noteworthy work is

unitarity estimation of (Chen et al., 2022a). In this work, it is shown that ancilla-free non-adaptive strategies could estimate $\text{Tr}(\mathcal{J}_{\mathcal{N}}^2)$ to within ε using $\mathcal{O}(d^{0.5}/\varepsilon^2)$ measurements where $\mathcal{J}_{\mathcal{N}}$ is the Choi state of the channel \mathcal{N} . In particular, this estimation can be used to distinguish between $\mathcal{N} = \mathcal{N}_U$ for which $\text{Tr}(\mathcal{J}_{\mathcal{N}}^2) = 1$ and $\mathcal{N} = \mathcal{D}$ for which $\text{Tr}(\mathcal{J}_{\mathcal{N}}^2) = 1/d^2$. A matching lower bound (in d) is given for adaptive strategies in (Chen et al., 2022a) improving the previous lower bound of (Chen et al., 2022c). This complexity may seem to contradict our results but this is not the case. Indeed, such a test cannot be used for testing identity to a fixed unitary channel for instance since we can have two unitary channels that are ε -far in the diamond distance. Finally, we note that testing problems for states were also studied for the class of coherent or entangled strategies where one can use arbitrary entangled measurements: see e.g., (Bădescu et al., 2019) for state certification in this setting. In this article, we focus on incoherent strategies where entangled inputs to the different uses of the channel or entanglement measurements are not allowed.

2. Preliminaries

We consider quantum channels of input dimension d_{in} and output dimension d_{out} . We adopt the bracket notation: a column vector is denoted $|\phi\rangle$ and its adjoint is denoted $\langle\phi| = |\phi\rangle^\dagger$. With this notation, $\langle\phi|\psi\rangle$ is the dot product of the vectors ϕ and ψ and, for a unit vector $|\phi\rangle \in \mathbf{S}^d$, $|\phi\rangle\langle\phi|$ is the projector on the space spanned by ϕ . The canonical basis $\{e_i\}_{i \in [d]}$ is denoted $\{|i\rangle\}_{i \in [d]} := \{e_i\}_{i \in [d]}$. A quantum state is a positive semi-definite Hermitian matrix of trace 1. The fidelity between two quantum states is defined $F(\rho, \sigma) = (\text{Tr} \sqrt{\sqrt{\rho} \sigma \sqrt{\rho}})^2$. It is symmetric and admits the simpler expression if one of the quantum states ρ or σ has rank 1: $F(\rho, |\phi\rangle\langle\phi|) = \langle\phi|\rho|\phi\rangle$. A $(d_{\text{in}}, d_{\text{out}})$ -dimensional quantum channel is a map $\mathcal{N} : \mathbb{C}^{d_{\text{in}} \times d_{\text{in}}} \rightarrow \mathbb{C}^{d_{\text{out}} \times d_{\text{out}}}$ of the form $\mathcal{N}(\rho) = \sum_k A_k \rho A_k^\dagger$ (Kraus decomposition) where the Kraus operators $\{A_k\}_k$ satisfy $\sum_k A_k^\dagger A_k = \mathbb{I}$. For instance, the identity map $\text{id}_d(\rho) = \rho$ admits the Kraus operator $\{\mathbb{I}_d\}$ and the completely depolarizing channel $\mathcal{D}(\rho) = \text{Tr}(\rho) \frac{\mathbb{I}}{d_{\text{out}}}$ admits the Kraus operators $\left\{ \frac{1}{\sqrt{d_{\text{out}}}} |i\rangle\langle j| \right\}_{j \in [d_{\text{in}}], i \in [d_{\text{out}}]}$. Given a unitary matrix U , the corresponding unitary channel $\mathcal{N}_U(\rho) = U \rho U^\dagger$ admits the Kraus operator $\{U\}$. We denote by $\text{Haar}(d)$ the Haar probability measure over the compact group of unitary $d \times d$ matrices. A Haar random vector is then any column vector of a Haar distributed unitary.

We define the trace distance between two quantum channels \mathcal{N} and \mathcal{M} as the trace norm of their difference: $d_{\text{Tr}}(\mathcal{N}, \mathcal{M}) := \max_\rho \|(\mathcal{N} - \mathcal{M})(\rho)\|_1$ where the maximization is over quantum states and the Schatten p -norm of a matrix M is defined as $\|M\|_p^p = \text{Tr}(\sqrt{M^\dagger M}^p)$. In some situations, it can be helpful to allow an auxiliary system and apply the identity on it. In this case, we obtain the diamond distance which is defined formally as $d_\diamond(\mathcal{N}, \mathcal{M}) := \max_\rho \|\text{id}_d \otimes (\mathcal{N} - \mathcal{M})(\rho)\|_1$ where the maximization is over quantum states $\rho \in \mathbb{C}^{d \times d} \otimes \mathbb{C}^{d_{\text{in}} \times d_{\text{in}}}$. Note that because of the Schmidt decomposition we can always suppose that $d = d_{\text{in}}$. The trace/diamond distance can be thought of as a worst-case distance, while we can define an average case distance by the Schatten 2-norm between the corresponding Choi states. We define the Choi state of the channel \mathcal{N} as $\mathcal{J}_{\mathcal{N}} = \text{id} \otimes \mathcal{N}(|\Psi\rangle\langle\Psi|)$ where $|\Psi\rangle = \frac{1}{\sqrt{d_{\text{in}}}} \sum_{i=1}^{d_{\text{in}}} |i\rangle \otimes |i\rangle$ is the maximally entangled state. The map $\mathcal{J} : \mathcal{N} \mapsto \text{id} \otimes \mathcal{N}(|\Psi\rangle\langle\Psi|)$ is an isomorphism called the Choi–Jamiołkowski isomorphism (Choi, 1975; Jamiołkowski, 1972). Note that for any quantum channel \mathcal{N} , $\mathcal{J}_{\mathcal{N}}$ is positive semi-definite and satisfy $\text{Tr}_2(\mathcal{J}_{\mathcal{N}}) = \frac{\mathbb{I}}{d_{\text{in}}}$. Moreover, any \mathcal{K} satisfying these conditions is called a Choi state and we can construct a quantum channel \mathcal{N} such that $\mathcal{J}_{\mathcal{N}} = \mathcal{K}$.

We consider the problem of testing identity to a fixed channel. Given a fixed quantum channel \mathcal{N}_0 and a precision parameter $\varepsilon > 0$, the goal is to test whether an unknown quantum channel \mathcal{N} is exactly \mathcal{N}_0 or ε -far from it with at least a probability $2/3$:

$$H_0 : \mathcal{N} = \mathcal{N}_0 \quad \text{vs.} \quad H_1 : \text{dist}(\mathcal{N}, \mathcal{N}_0) \geq \varepsilon$$

where $\text{dist} \in \{d_\diamond, d_{\text{Tr}}\}$. H_0 is called the null hypothesis while H_1 is called the alternate hypothesis. An algorithm \mathcal{A} is $1/3$ -correct for this problem if it outputs H_1 while H_0 is true with a probability at most $1/3$ and outputs H_0 while H_1 is true with a probability at most $1/3$. If $0 < \text{dist}(\mathcal{N}, \mathcal{N}_0) < \varepsilon$, the algorithm \mathcal{A} can output any hypothesis. The natural figure of merit for this test is the diamond (resp. trace) distance because it characterizes the minimal error probability to distinguish between two quantum channels when auxiliary systems are allowed (resp. not allowed) (Watrous, 2018).

A testing algorithm can only extract classical information from the unknown quantum channel \mathcal{N} by performing a measurement on the output state. In this article we only consider incoherent strategies. That is, the testing algorithm can only use one copy of the channel at each step. In other words, for a $(d_{\text{in}}, d_{\text{out}})$ dimensional channel, the testing algorithm could only use d_{in} dimensional input states and d_{out} dimensional measurement devices. Precisely, a d -dimensional measurement is defined by a POVM (positive operator-valued measure) with a finite number of elements: this is a set of positive semi-definite matrices $\mathcal{M} = \{M_x\}_{x \in \mathcal{X}}$ acting on the Hilbert space \mathbb{C}^d and satisfying $\sum_{x \in \mathcal{X}} M_x = \mathbb{I}$. Each element M_x in the POVM \mathcal{M} is associated with the outcome $x \in \mathcal{X}$. The tuple $\{\text{Tr}(\rho M_x)\}_{x \in \mathcal{X}}$ is non-negative and sums to 1: it thus defines a probability. Born's rule (Born, 1926) says that the probability that the measurement on a quantum state ρ using the POVM \mathcal{M} will output x is exactly $\text{Tr}(\rho M_x)$. Depending on whether an auxiliary system is allowed to be used, we distinguish two types of incoherent strategies.

- **Ancilla-free strategies.** At each step t , the learner would choose an input d_{in} -dimensional state ρ_t and a d_{out} -dimensional measurement device $\mathcal{M}_t = \{M_x^t\}_{x \in \mathcal{X}_t}$. It thus sees the outcome $x_t \in \mathcal{X}_t$ with a probability $\text{Tr}(\mathcal{N}(\rho_t) M_{x_t}^t)$. If the choice of the state ρ_t and measurement device \mathcal{M}_t can depend on the previous observations (x_1, \dots, x_{t-1}) the strategy is called **adaptive**, otherwise it is called **non-adaptive** (see Fig. 1 for an illustration).
- **Ancilla-assisted strategies.** At each step t , the learner would choose an input $d_{\text{anc}} \times d_{\text{in}}$ -dimensional state $\rho_t \in \mathbb{C}^{d_{\text{anc}} \times d_{\text{anc}}} \otimes \mathbb{C}^{d_{\text{in}} \times d_{\text{in}}}$ (for some arbitrary d_{anc}) and a $d_{\text{anc}} \times d_{\text{out}}$ -dimensional measurement device $\mathcal{M}_t = \{M_x^t\}_{x \in \mathcal{X}_t}$. It thus sees the outcome $x_t \in \mathcal{X}_t$ with a probability $\text{Tr}(\text{id}_{d_{\text{anc}}} \otimes \mathcal{N}(\rho_t) M_{x_t}^t)$. If the choice of the state ρ_t and measurement device \mathcal{M}_t can depend on the previous observations (x_1, \dots, x_{t-1}) the strategy is called **adaptive**, otherwise it is called **non-adaptive** (see Fig. 2 for an illustration).

Note that we can see an ancilla-free strategy as a special case of an ancilla-assisted strategy with $d_{\text{anc}} = 1$. But it turns out that ancilla-assisted strategies have an advantage over ancilla-free strategies for some problems e.g., (Chen et al., 2022b,c). However, in this article, we show that ancilla-free strategies suffice to achieve the optimal complexity for testing identity to a fixed unitary channel or to the depolarizing channel.

3. Testing identity to a unitary channel

In this section, we focus on the problem of testing identity to a fixed unitary channel in the diamond and trace distances. Given a fixed unitary U and a precision parameter $\varepsilon > 0$, the goal is to

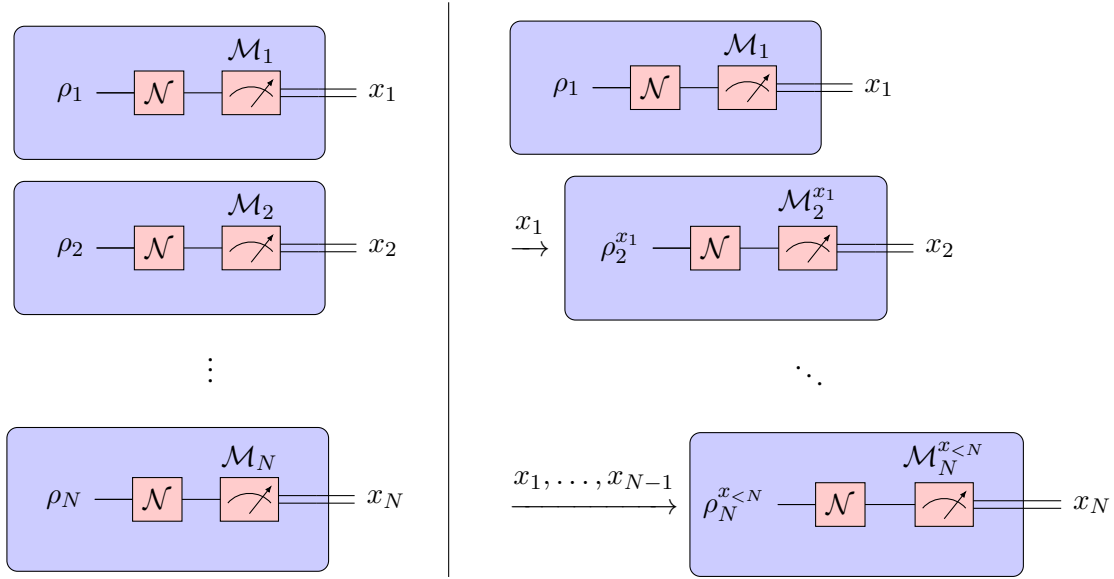


Figure 1: Illustration of an ancilla-free incoherent non-adaptive (left) and adaptive (right) strategies for testing identity of quantum channels. The observations (x_1, \dots, x_N) are then processed with a classical algorithm to answer H_0 or H_1 .

distinguish between the hypotheses:

$$H_0 : \mathcal{N} = \mathcal{N}_U = U \cdot U^\dagger \quad \text{vs.} \quad H_1 : \text{dist}(\mathcal{N}, \mathcal{N}_U) \geq \varepsilon$$

with at least a probability $2/3$ where $\text{dist} \in \{d_\diamond, d_{\text{Tr}}\}$. Since we consider a unitary channel, the input and output dimensions should be equal $d_{\text{in}} = d_{\text{out}} = d$.

Reduction to the case $U = \mathbb{I}$. Knowing the unitary channel \mathcal{N}_U is equivalent to knowing U . We can thus reduce every testing identity to \mathcal{N}_U to testing identity to $\mathcal{N}_{\mathbb{I}} = \text{id}_d$ by conjugating the measurement device by U . This is possible because the trace/diamond distance is unitary invariant: $\text{dist}(\mathcal{N}, \mathcal{N}_U) = \text{dist}(U^\dagger \mathcal{N} U, \text{id})$ and $\text{Tr}(U^\dagger \mathcal{N}(\rho) U M) = \text{Tr}(\mathcal{N}(\rho) U M U^\dagger)$ for all ρ and M . From now on, we only consider the case $U = \mathbb{I}$ and we call this particular testing problem to $\mathcal{N}_{\mathbb{I}} = \text{id}_d$ simply “testing identity to identity”.

Given the nature of the diamond and trace distances, under the alternate hypothesis, a channel \mathcal{N} could be equal to the identity channel except on a neighbourhood of some state. In addition, this state is unknown to the learner. When the algorithm is allowed to use an auxiliary system, it can prepare the Choi state $\mathcal{J}_{\mathcal{N}}$ of the channel \mathcal{N} (which essentially captures everything about the channel) by taking as input the maximally entangled state $|\Psi\rangle\langle\Psi|$. Under the null hypothesis H_0 , the Choi state is exactly $\mathcal{J}_{\text{id}} = \text{id} \otimes \text{id}(|\Psi\rangle\langle\Psi|) = |\Psi\rangle\langle\Psi|$ while under the alternate hypothesis H_1 , the Choi state $\mathcal{J}_{\mathcal{N}}$ has a fidelity with $|\Psi\rangle\langle\Psi|$ satisfying:

$$\text{Tr}(\text{id} \otimes \mathcal{N}(|\Psi\rangle\langle\Psi|) |\Psi\rangle\langle\Psi|) = F(\mathcal{J}_{\mathcal{N}}, |\Psi\rangle\langle\Psi|) \leq 1 - \frac{1}{4} \|\mathcal{J}_{\mathcal{N}} - \mathcal{J}_{\text{id}}\|_1^2 \leq 1 - \frac{d_\diamond(\mathcal{N}, \text{id})^2}{4d^2}$$

where we use a Fuchs–van de Graaf inequality (Fuchs and Van De Graaf, 1999) and the standard inequality relating the diamond norm between two channels and the trace norm between their corresponding Choi states: $\|\mathcal{J}_{\mathcal{N}} - \mathcal{J}_{\mathcal{M}}\|_1 \geq \frac{d_\diamond(\mathcal{N}, \mathcal{M})}{d}$ (e.g., Jenčová and Plávala (2016)). Thus, a

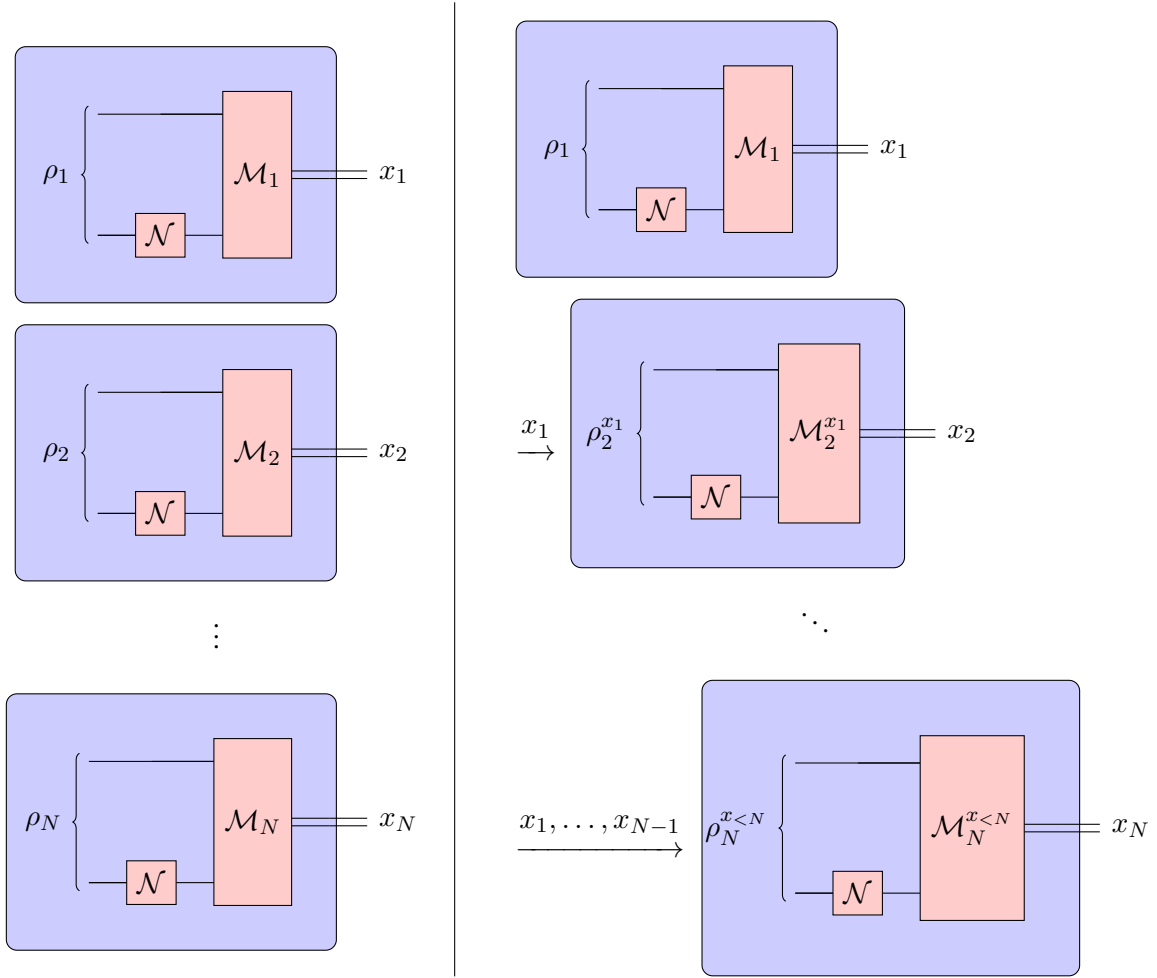


Figure 2: Illustration of an ancilla-assisted incoherent non-adaptive (left) and adaptive (right) strategies for testing identity of quantum channels. The observations (x_1, \dots, x_N) are then processed with a classical algorithm to answer H_0 or H_1 .

measurement using the POVM $\mathcal{M}_\Psi = \{|\Psi\rangle\langle\Psi|, \mathbb{I} - |\Psi\rangle\langle\Psi|\}$ can distinguish between the two situations. However, if the tester is not allowed to use an auxiliary system it can neither prepare the Choi state $\mathcal{J}_\mathcal{N}$ nor measure using the POVM \mathcal{M}_Ψ . Instead, we use a random d -dimensional rank-1 input state. Indeed, this choice is natural because the expected fidelity between the input state $|\phi\rangle\langle\phi|$ and the output state $\mathcal{N}(|\phi\rangle\langle\phi|)$ can be easily related to the fidelity between Choi states: $\mathbb{E}_{|\phi\rangle\sim\text{Haar}}[\text{F}(\mathcal{N}(|\phi\rangle\langle\phi|), |\phi\rangle\langle\phi|)] = \frac{1+d \text{F}(\mathcal{J}_\mathcal{N}, |\Psi\rangle\langle\Psi|)}{1+d}$ (see Lem. 8 for a proof). This Lemma is well known because it relates the average fidelity $\mathbb{E}_{|\phi\rangle\sim\text{Haar}}[\text{F}(\mathcal{N}(|\phi\rangle\langle\phi|), |\phi\rangle\langle\phi|)]$ and the entanglement fidelity $\text{F}(\mathcal{J}_\mathcal{N}, |\Psi\rangle\langle\Psi|)$. If we measure using the measurement device $\mathcal{M}_\phi = \{|\phi\rangle\langle\phi|, \mathbb{I} - |\phi\rangle\langle\phi|\}$, the error probability under H_0 is 0, and under H_1 is $\mathbb{E}_{|\phi\rangle\sim\text{Haar}}[\langle\phi|\mathcal{N}(|\phi\rangle\langle\phi|)|\phi\rangle] = \mathbb{E}_{|\phi\rangle\sim\text{Haar}}[\text{F}(\mathcal{N}(|\phi\rangle\langle\phi|), |\phi\rangle\langle\phi|)]$. The algorithm is detailed in Alg. 1.

Algorithm 1: Testing identity to identity in the diamond/trace distance

$N = \mathcal{O}(d/\varepsilon^4)$ (replace with $N = \mathcal{O}(d/\varepsilon^2)$ for testing in the trace distance).

for $k = 1 : N$ **do**

 Sample ϕ_k a Haar random vector in \mathbf{S}^d .

 Measure the output state $\mathcal{N}(|\phi_k\rangle\langle\phi_k|)$ using the POVM $\{|\phi_k\rangle\langle\phi_k|, \mathbb{I} - |\phi_k\rangle\langle\phi_k|\}$.

 Observe $X_k \sim \text{Bern}(1 - \langle\phi_k|\mathcal{N}(|\phi_k\rangle\langle\phi_k|)|\phi_k\rangle)$.

end for

if $\exists k : X_k = 1$ **then return** \mathcal{N} is ε -far from id **else return** $\mathcal{N} = \text{id}$.

We can upper bound the error probability under H_1 using the well-known Lem. 8 and our Lem. 10:

$$\mathbb{E}_{|\phi\rangle\sim\text{Haar}} [\mathbb{F}(\mathcal{N}(|\phi\rangle\langle\phi|), |\phi\rangle\langle\phi|)] = \frac{1 + d \mathbb{F}(\mathcal{J}_{\mathcal{N}}, |\Psi\rangle\langle\Psi|)}{1 + d} \leq 1 - \frac{d_{\text{Tr}}(\mathcal{N}, \text{id})^2}{4(d+1)} \leq 1 - \frac{d_{\diamond}(\mathcal{N}, \text{id})^4}{16(d+1)}.$$

Observe that the standard inequality $\|\mathcal{J}_{\mathcal{N}} - \mathcal{J}_{\mathcal{M}}\|_1 \geq \frac{d_{\diamond}(\mathcal{N}, \mathcal{M})}{d}$ implies: $\mathbb{E}_{\phi} [\mathbb{F}(\mathcal{N}(|\phi\rangle\langle\phi|), |\phi\rangle\langle\phi|)] \leq 1 - \frac{d_{\diamond}(\mathcal{N}, \text{id})^2}{4d(d+1)}$ which has a better dependency in the diamond distance but a worst dependency in the dimension d . This simple lemma (Lem. 10), which relates the entanglement fidelity and the trace/diamond distance when one of the channels is unitary might be of independent interest. To obtain a 1/3 correct algorithm it suffices to repeat the described procedure using $N = \mathcal{O}(d/\varepsilon^2)$ copies of $|\phi\rangle\langle\phi|$ in the case of trace distance and $N = \mathcal{O}(d/\varepsilon^4)$ copies of $|\phi\rangle\langle\phi|$ in the case of diamond distance. Indeed, for instance for the trace distance, the probability of error under H_1 can be controlled as follows:

$$\begin{aligned} \mathbb{P}_{H_1}(\text{error}) &= \mathbb{P}_{H_1}(\forall k \in [N] : X_k = 0) = \prod_{k=1}^N \mathbb{P}_{H_1}(X_k = 0) \\ &\leq \left(1 - \frac{\varepsilon^2}{4(d+1)}\right)^N \leq \exp\left(-\frac{\varepsilon^2 N}{4(d+1)}\right) \leq \frac{1}{3} \end{aligned}$$

for $N = 4 \log(3)(d+1)/\varepsilon^2 = \mathcal{O}(d/\varepsilon^2)$ ¹. A similar proof shows that $\mathcal{O}(d/\varepsilon^4)$ copies are sufficient to test in the diamond distance. This concludes the correctness of Alg. 1. A matching lower bound of $N = \Omega\left(\frac{d}{\varepsilon^2}\right)$ is proved in App. B. For this we construct a random quantum channel ε -far from the identity channel in the trace/diamond distance but looks similar to the identity channel for the majority of the input states. Then we compare the observations under the two hypotheses using the KL divergence. Interestingly, the analogous classical problem, testing identity to identity has a complexity $\Theta(d/\varepsilon)$. Thus, for this task, when going to the quantum case, the dependence on the dimension d remains the same whereas the dependency in the precision parameter ε changes from ε to ε^2 . In fact, obtaining the correct ε^2 dependence is the main difficulty in this lower bound. It requires a carefully chosen construction inspired by the quantum skew divergence (Audenaert, 2014) and a fine analysis using Weingarten calculus. We summarize the main result of this section in the following theorem.

Theorem 1 *There is an incoherent ancilla-free algorithm for testing identity to identity in the trace distance using only $N = \mathcal{O}\left(\frac{d}{\varepsilon^2}\right)$ measurements. Moreover, this algorithm can also solve the testing*

1. All the logs of this paper are taken in base e and the information is measured in “nats”.

identity to identity problem in the diamond distance using only $N = \mathcal{O}\left(\frac{d}{\varepsilon^4}\right)$ measurements. On the other hand, any incoherent adaptive ancilla-assisted strategy requires, in the worst case, a number of measurements satisfying $N = \Omega\left(\frac{d}{\varepsilon^2}\right)$ to distinguish between $\mathcal{N} = \text{id}$ and $d_\diamond(\mathcal{N}, \text{id}) > \varepsilon$ (or $d_{\text{Tr}}(\mathcal{N}, \text{id}) > \varepsilon$) with a probability at least $2/3$.

4. Testing identity to the depolarizing channel

In this section, we move to study the problem of testing identity to the completely depolarizing channel $\mathcal{N}_0 = \mathcal{D}$ in the diamond distance. Given a precision parameter $\varepsilon > 0$ and an unknown quantum channel \mathcal{N} , we would like to test whether $H_0 : \mathcal{N} = \mathcal{D}$ or $H_1 : d_\diamond(\mathcal{N}, \mathcal{D}) \geq \varepsilon$ with a probability of error at most $1/3$. If $\mathcal{N} = \mathcal{D}$, the tester should answer the null hypothesis H_0 with a probability at least $2/3$ whereas if $d_\diamond(\mathcal{N}, \mathcal{D}) \geq \varepsilon$, the tester should answer the alternate hypothesis H_1 with a probability at least $2/3$. The alternate condition means that

$$d_\diamond(\mathcal{N}, \mathcal{D}) \geq \varepsilon \iff \exists |\phi\rangle \in \mathbf{S}^{d_{\text{in}} \times d_{\text{in}}} : \|\text{id}_{d_{\text{in}}} \otimes \mathcal{N}(|\phi\rangle\langle\phi|) - \text{id}_{d_{\text{in}}} \otimes \mathcal{D}(|\phi\rangle\langle\phi|)\|_1 \geq \varepsilon.$$

This inequality implies a lower bound of the 1-norm between the Choi states: $\|\mathcal{J}_\mathcal{N} - \mathcal{J}_\mathcal{D}\|_1 \geq \frac{\varepsilon}{d_{\text{in}}}$. The simplest idea would be to use this inequality and reduce the problem of testing channels to testing states. Actually, this kind of reduction from channels to states has been used for quantum process tomography (Surawy-Stepney et al., 2022) and shadow process tomography (Kunjummen et al., 2021). The Choi state of the depolarizing channel \mathcal{D} is $\mathcal{J}_\mathcal{D} = \frac{1}{d_{\text{in}}} \sum_{i,j=1}^{d_{\text{in}}} |i\rangle\langle j| \otimes \text{Tr}(|i\rangle\langle j|) \frac{\mathbb{I}}{d_{\text{out}}} = \frac{\mathbb{I}_{d_{\text{in}}} \otimes \mathbb{I}_{d_{\text{out}}}}{d_{\text{in}} d_{\text{out}}} = \frac{\mathbb{I}_{d_{\text{in}} d_{\text{out}}}}{d_{\text{in}} d_{\text{out}}}$, so by applying the previous inequality, we obtain for a quantum channel \mathcal{N} ε -far from the depolarizing channel \mathcal{D} : $\left\| \mathcal{J}_\mathcal{N} - \frac{\mathbb{I}}{d_{\text{in}} d_{\text{out}}} \right\|_1 \geq \frac{\varepsilon}{d_{\text{in}}}$. Then, we can apply a reduction to the testing mixedness of quantum states (Bubeck et al., 2020) to design an ancilla-assisted strategy requiring $\mathcal{O}\left(\frac{d_{\text{in}}^{1.5} d_{\text{out}}^{1.5}}{(\varepsilon/d_{\text{in}})^2}\right) = \mathcal{O}\left(\frac{d_{\text{in}}^{3.5} d_{\text{out}}^{1.5}}{\varepsilon^2}\right)$ measurements since the dimension of the states $\mathcal{J}_\mathcal{N}$ and $\frac{\mathbb{I}}{d_{\text{in}} d_{\text{out}}}$ is $d_{\text{in}} d_{\text{out}}$ and the precision parameter is $\frac{\varepsilon}{d_{\text{in}}}$. However, this approach has two problems. First, we need to be able to use an auxiliary system to prepare the Choi state $\mathcal{J}_\mathcal{N}$, which is an additional resource. Next, the complexity $\mathcal{O}\left(\frac{d_{\text{in}}^{3.5} d_{\text{out}}^{1.5}}{\varepsilon^2}\right)$, as we shall see later, is not optimal. If one tries to reduce to testing identity of states in the 2-norm (App. E) one obtains a slightly better bound but still not optimal and requires using an auxiliary system.

Inspired by the testing identity to identity problem (Sec. 3), when we do not know one of the best input states, we choose it to be random. Let $|\phi\rangle$ be a Haar random vector. If the input state is $|\phi\rangle\langle\phi|$, the output state under H_0 is $\mathcal{D}(|\phi\rangle\langle\phi|) = \frac{\mathbb{I}}{d_{\text{out}}}$ and under H_1 is $\mathcal{N}(|\phi\rangle\langle\phi|)$. So it is natural to ask what would be the distance between $\mathcal{N}(|\phi\rangle\langle\phi|)$ and $\frac{\mathbb{I}}{d_{\text{out}}}$. Note that in general, it is much easier to compute the expectation of the 2-norms than the 1-norms. For this reason, we start by computing the expectation of the 2-norm between $\mathcal{N}(|\phi\rangle\langle\phi|)$ and $\frac{\mathbb{I}}{d_{\text{out}}}$ (see Lem. 13 for a proof).

Lemma 2 *Let $\mathcal{M} = \mathcal{N} - \mathcal{D}$ and $\mathcal{J}_\mathcal{M} = \text{id} \otimes \mathcal{M}(|\Psi\rangle\langle\Psi|)$. We have:*

$$\mathbb{E}_{|\phi\rangle \sim \text{Haar}} \left(\|\mathcal{M}(|\phi\rangle\langle\phi|)\|_2^2 \right) = \frac{\|\mathcal{M}(\mathbb{I})\|_2^2 + d_{\text{in}}^2 \|\mathcal{J}_\mathcal{M}\|_2^2}{d_{\text{in}}(d_{\text{in}} + 1)} \geq \frac{d_{\text{in}}}{d_{\text{in}} + 1} \|\mathcal{J}_\mathcal{M}\|_2^2.$$

We now need to relate the 2-norm between the Choi state of the channel \mathcal{N} and the Choi state of the depolarizing channel $\|\mathcal{J}_\mathcal{N} - \mathcal{J}_\mathcal{D}\|_2$ with the diamond distance between them $d_\diamond(\mathcal{N}, \mathcal{D})$. This is done in the following Lemma whose proof can be found in App. C.1:

Lemma 3 Let \mathcal{N}_1 and \mathcal{N}_2 be two $(d_{\text{in}}, d_{\text{out}})$ -quantum channels. We have:

$$\|\mathcal{J}_{\mathcal{N}_1} - \mathcal{J}_{\mathcal{N}_2}\|_2 \geq \frac{d_{\diamond}(\mathcal{N}_1, \mathcal{N}_2)}{d_{\text{in}}\sqrt{d_{\text{out}}}}.$$

Let \mathcal{N} be a channel satisfying $d_{\diamond}(\mathcal{N}, \mathcal{D}) \geq \varepsilon$ and $X = \left\| \mathcal{N}(|\phi\rangle\langle\phi|) - \frac{\mathbb{I}}{d_{\text{out}}} \right\|_2^2$, we obtain from Lem. 2, 3:

$$\mathbb{E}(X) = \mathbb{E}_{|\phi\rangle \sim \text{Haar}} \left(\left\| \mathcal{N}(|\phi\rangle\langle\phi|) - \frac{\mathbb{I}}{d_{\text{out}}} \right\|_2^2 \right) \geq \frac{d_{\text{in}}}{d_{\text{in}} + 1} \left\| \mathcal{J}_{\mathcal{N}} - \frac{\mathbb{I}}{d_{\text{in}}d_{\text{out}}} \right\|_2^2 \geq \frac{\varepsilon^2}{2d_{\text{in}}^2 d_{\text{out}}}. \quad (1)$$

If we could show that X is larger than $\Omega(\mathbb{E}(X))$ with constant probability, then we can reduce our problem to the usual testing identity of quantum states in the 2-norm (quantum state certification in App. E) and obtain an incoherent *ancilla-free* algorithm using $\mathcal{O}\left(\frac{\sqrt{d_{\text{out}}}}{(\varepsilon/d_{\text{in}}\sqrt{d_{\text{out}}})^2}\right) = \mathcal{O}\left(\frac{d_{\text{in}}^2 d_{\text{out}}^{1.5}}{\varepsilon^2}\right)$ measurements. Establishing this turns out to be the most technical part of the proof as is summarized in the following theorem.

Theorem 4 Let $|\phi\rangle$ be a Haar distributed vector in \mathbf{S}^d (or any 4-design). Let $X = \left\| \mathcal{N}(|\phi\rangle\langle\phi|) - \frac{\mathbb{I}}{d_{\text{out}}} \right\|_2^2$. We have:

$$\text{Var}(X) = \mathcal{O}([\mathbb{E}(X)]^2).$$

This Theorem is the most technical part of the paper and we believe that it can be generalized for any difference of channels with a similar approach. Moreover, applying this inequality along with the Paley-Zygmund inequality are sufficient for our reduction: we only need to repeat our test $\mathcal{O}(1)$ times to reduce the error probability to 1/3 for testing identity to the depolarizing channel.

Sketch of the proof. We observe first that $\text{Var}(X) = \text{Var}\left(\text{Tr}\left[\left(\mathcal{N}(|\phi\rangle\langle\phi|)\right)^2\right]\right)$. Then using Weingarten calculus (Lem. 31,33), we can compute the expectation

$$\mathbb{E}\left(\left(\text{Tr}\left[\left(\mathcal{N}(|\phi\rangle\langle\phi|)\right)^2\right]\right)^2\right) = \frac{1}{d_{\text{in}}(d_{\text{in}} + 1)(d_{\text{in}} + 2)(d_{\text{in}} + 3)} \sum_{\alpha \in \mathfrak{S}_4} F(\alpha)$$

where for $\alpha \in \mathfrak{S}_4$, $F(\alpha) = \sum_{i,j,k,l,k',l'} \text{Tr}_{\alpha}(A_{l'}^{\dagger} |j\rangle\langle i| A_k, A_k^{\dagger} A_l, A_l^{\dagger} |i\rangle\langle j| A_{k'}, A_{k'}^{\dagger} A_{l'})$ and $\text{Tr}_{\alpha}(M_1, \dots, M_n) = \prod_j \text{Tr}(\prod_{i \in C_j} M_i)$ for $\alpha = \prod_j C_j$ and C_j are cycles. Let $m = \left\| \mathcal{N}(\mathbb{I}) - \frac{d_{\text{in}}}{d_{\text{out}}} \mathbb{I} \right\|_2$ and $\eta = d_{\text{in}} \left\| \mathcal{J}_{\mathcal{N}} - \frac{\mathbb{I}}{d_{\text{in}}d_{\text{out}}} \right\|_2$. Next, we upper bound the function F as shown in Table 2. This is the hardest step of the proof and requires a fine analysis for many of the $F(\alpha)$'s. A particularly useful trick we use repeatedly is known as the *replica trick* and says that if $\mathbb{F} = \sum_{i,j=1}^d (|i\rangle \otimes |j\rangle)(\langle j| \otimes \langle i|)$ is the flip operator then we have for all $A, B \in \mathbb{C}^{d \times d}$: $\text{Tr}((A \otimes B)\mathbb{F}) = \text{Tr}(AB)$ and similarly $\text{Tr}(A \otimes B) = \text{Tr}(A)\text{Tr}(B)$. Moreover, another trick we need frequently is to use the partial transpose to make appear the positive semi-definite matrices $M^{\dagger}M = \sum_{k,l} A_k^{\dagger} A_l \otimes A_k^{\top} \bar{A}_l$ and $MM^{\dagger} = \sum_{k,l} A_k A_l^{\dagger} \otimes \bar{A}_k \bar{A}_l^{\top}$ where $M = \sum_k A_k \otimes \bar{A}_k$ is defined using the Kraus operators $\{A_k\}_k$ of the channel \mathcal{N} . Furthermore we can prove the approximation $\left\| M^{\dagger}M - \frac{d_{\text{in}}}{d_{\text{out}}} |\Psi\rangle\langle\Psi| \right\|_1 \leq 5\eta^2$ where $|\Psi\rangle = \frac{1}{\sqrt{d_{\text{in}}}} \sum_{i=1}^{d_{\text{in}}} |i\rangle \otimes |i\rangle$ is the maximally entangled state (see Lem. 17). This is used for

Permutation α	Upper bound on $F(\alpha)$	Reference
(13)	$\left(\frac{d_{\text{in}}}{d_{\text{out}}} + \eta^2\right)^2$	
id, (132), (314), (24)(13)	$\frac{d_{\text{in}}/d_{\text{out}} + \eta^2}{d_{\text{out}}} + \frac{\eta^2}{d_{\text{out}}} + 5\eta^4$	(Lem. 19)
(312), (134)	$\left(\frac{d_{\text{in}}^2}{d_{\text{out}}} + m^2\right) \left(\frac{d_{\text{in}}}{d_{\text{out}}} + \eta^2\right)$	
(1234)	$\left(\frac{d_{\text{in}}^2}{d_{\text{out}}} + m^2\right)^2$	
(24), (1432)	$\frac{d_{\text{in}}^2}{d_{\text{out}}^2} + \frac{2m^2}{d_{\text{out}}} + 25\eta^4$	(Lem. 20)
(142), (243)	$\frac{d_{\text{in}}/d_{\text{out}} + \eta^2}{d_{\text{out}}} + \frac{\eta^2}{d_{\text{out}}} + 5\eta^4$	(Lem. 18)
(14), (12), (23), (34), (1324), (1423), (1243), (1342)	$\frac{d_{\text{in}}^2}{d_{\text{out}}^2} + \frac{d_{\text{in}}}{d_{\text{out}}} \eta^2 + \frac{m^2}{d_{\text{out}}} + 5m\eta^3$	(Lem. 22)
(12)(34), (14)(23), (234), (124)	$\frac{d_{\text{in}}^3}{d_{\text{out}}^2} + 2\frac{d_{\text{in}}}{d_{\text{out}}} m^2 + m^2 \eta^2$	(Lem. 21)

 Table 2: Upper bounds on the function F for different input permutations.

$\alpha = (142)$ and (24) . An application of the data processing inequality on the previous approximation gives: $\left\| \text{Tr}_2(M^\dagger M) - \frac{1}{d_{\text{out}}} \mathbb{I} \right\|_1 \leq 5\eta^2$ which is used for the permutations $\alpha = \text{id}$ and (14) . It turns out that applying such approximation will not give a sufficiently good upper bound of $F((12)(34))$ because it can be written as $F((12)(34)) = \text{Tr} \left((MM^\dagger)^{T_2} \cdot \mathcal{M}(\mathbb{I})^{\otimes 2} \mathbb{F} \right) + \frac{d_{\text{in}}^3}{d_{\text{out}}^2} + 2\frac{d_{\text{in}}}{d_{\text{out}}} \text{Tr}(\mathcal{M}(\mathbb{I})^2)$ which depends instead on the matrix MM^\dagger . In this case we proceed by projecting MM^\dagger onto the hyperplane orthogonal to $|\Psi\rangle$. This can be interpreted using representation theory. In fact, the space spanned by $|\Psi\rangle$ and its complementary are irreducible representations that decompose the space $(\mathbb{C}^d)^{\otimes 2}$ for the action of $U \otimes \bar{U}$ where U is a unitary matrix. On the other hand, changing the Kraus operators $A_k \leftrightarrow UA_k$ or $A_k \leftrightarrow A_kU$ in the expression of the channel \mathcal{N} does not affect the variance of X because Haar measure is invariant under left and right multiplication with a unitary matrix. The detailed proof of these bounds can be found in App. C.3.

We have now the required tools to design and prove the correctness of an algorithm for testing identity to the depolarizing channel.

Theorem 5 *There is an incoherent ancilla-free algorithm requiring a number of measurements $N = \mathcal{O}\left(\frac{d_{\text{in}}^2 d_{\text{out}}^{1.5}}{\varepsilon^2}\right)$ to distinguish between $\mathcal{N} = \mathcal{D}$ and $d_\diamond(\mathcal{N}, \mathcal{D}) \geq \varepsilon$ with a success probability $2/3$.*

As explained before, our algorithm is a reduction to the testing identity of quantum states. For the convenience of the reader we include this latter with a proof of its correctness in App. E. Note that we need to test quantum states in the 2-norm which is different than the usual quantum state certification (Bubeck et al., 2020). The algorithm for testing identity to the depolarizing channel is described in Alg. 2.

We remark that Alg. 2 uses the channel only on a constant number of random input states $\{|\phi_k\rangle\langle\phi_k|\}_k$. One could think that querying the channel \mathcal{N} on more diverse inputs could lead to a more efficient algorithm. However, it turns out that Alg. 2 is basically optimal as we prove a matching lower bound up to a poly-logarithmic factor.

Algorithm 2: Testing identity to the depolarizing channel in the diamond norm

$M = 2200$.

for $k = 1 : M$ **do**

 Sample ϕ_k a Haar random vector in $\mathbf{S}^{d_{\text{in}}}$.

 Test whether $h_0 : \mathcal{N}(|\phi_k\rangle\langle\phi_k|) = \frac{\mathbb{I}}{d_{\text{out}}}$ or $h_1 : \left\| \mathcal{N}(|\phi_k\rangle\langle\phi_k|) - \frac{\mathbb{I}}{d_{\text{out}}} \right\|_2 \geq \frac{\varepsilon}{2\sqrt{d_{\text{out}}d_{\text{in}}}}$ using the testing identity of quantum states Alg. 3, with an error probability $\delta = 1/(3M)$, that answers the hypothesis $h_{i_k}, i_k \in \{0, 1\}$.

end for

if $\exists k : i_k = 1$ **then return** \mathcal{N} is ε -far from \mathcal{D} **else return** $\mathcal{N} = \mathcal{D}$.

Theorem 6 *Let $\varepsilon \leq 1/32$, $d_{\text{in}} \geq 80$ and $d_{\text{out}} \geq 10$. Any ancilla-assisted non-adaptive algorithm for testing identity to the depolarizing channel (for both trace and diamond distances) requires, in the worst case, a number of measurements satisfying:*

$$N = \Omega \left(\frac{d_{\text{in}}^2 d_{\text{out}}^{1.5}}{\log(d_{\text{in}} d_{\text{out}} / \varepsilon)^2 \varepsilon^2} \right).$$

This theorem shows that our proposed Alg. 2 is almost optimal in the dimensions $(d_{\text{in}}, d_{\text{out}})$ and the precision parameter ε thus the complexity of testing identity to the depolarizing channel is $\tilde{\Theta}(d_{\text{in}}^2 d_{\text{out}}^{1.5} / \varepsilon^2)$ which is slightly surprising. Indeed, we can remark that the complexity of testing identity of discrete distributions and quantum states is the square root (for constant ε) of the complexity of the corresponding learning problems in the same setting. This rule does not apply for quantum channels since we know from (Surawy-Stepney et al., 2022; Oufkir, 2023) that the complexity of learning quantum channels in the diamond distance with non-adaptive incoherent strategies is $\tilde{\Theta}(d_{\text{in}}^3 d_{\text{out}}^3 / \varepsilon^2)$.

Sketch of the proof. Under the null hypothesis $\mathcal{N} = \mathcal{D}$. Under the alternate hypothesis, we construct randomly the quantum channel $\mathcal{N} \sim \mathcal{P}$ of the form: $\mathcal{N}(\rho) = \mathcal{D}(\rho) + \frac{\varepsilon}{d_{\text{out}} \|u\|_2^2} \langle u | \rho | u \rangle U$ where $|u\rangle$ is a standard Gaussian vector and U has Gaussian entries: for all $i \leq j \in [d_{\text{out}}]$, $U_{j,i} = \bar{U}_{i,j} \sim \mathbf{1}\{i \neq j\} \mathcal{N}_c(0, 16/d_{\text{out}})$ conditioned on the event $\mathcal{G} = \{\|U\|_1 \geq d_{\text{out}}, \|U\|_\infty \leq 32\}$. Note that the usual construction applied on the Choi state gives a sub-optimal lower bound in the trace or diamond distances. Using a concentration inequality of Lipschitz functions of Gaussian random variables (Wainwright, 2019), we show that with a high probability \mathcal{N} is ε -far from \mathcal{D} in the trace and diamond distances. Then we use LeCam's method to lower bound the TV distance between the distribution of the observations under the two hypotheses: $\text{TV} \left(\mathbb{P}_{\mathcal{D}}^{I_1, \dots, I_N} \middle\| \mathbb{E}_{\mathcal{N} \sim \mathcal{P}} \mathbb{P}_{\mathcal{N}}^{I_1, \dots, I_N} \right) \geq \frac{1}{3}$ where I_1, \dots, I_N are the observations the algorithm obtains after the measurements and N is a sufficient number of measurements for the correctness of the algorithm. We can suppose w.l.o.g. that the input states are pure $\rho_t = |\psi_t\rangle\langle\psi_t|$ and the measurement devices are given by POVMs of the form $\mathcal{M}_t = \{\lambda_{i_t}^t |\phi_{i_t}^t\rangle\langle\phi_{i_t}^t|\}$. Also, we can write

$$|\psi_t\rangle = A_t \otimes \mathbb{I} |\Psi_{d_{\text{in}}}\rangle, |\phi_{i_t}^t\rangle = B_{i_t}^t \otimes \mathbb{I} |\Psi_{d_{\text{out}}}\rangle \quad \text{where} \quad |\Psi_d\rangle = \frac{1}{\sqrt{d}} \sum_{i=1}^d |ii\rangle.$$

Then we condition on the event \mathcal{E} that u satisfies $\|u\|_2 \geq \sqrt{\frac{d_{\text{in}}}{6}}$ and

$$\forall t \in [N] : P_u^t = \sum_{i_t, j_t} \frac{\lambda_{i_t}^t \lambda_{j_t}^t \langle u | A_t^\dagger B_{i_t}^t B_{j_t}^{t, \dagger} A_t | u \rangle^4}{\text{Tr}(B_{i_t}^{t, \dagger} A_t A_t^\dagger B_{i_t}^t) \text{Tr}(B_{j_t}^{t, \dagger} A_t A_t^\dagger B_{j_t}^t)} \leq (7 \log(N))^4 d_{\text{in}}^2 d_{\text{out}}^3. \quad (2)$$

Note that P_u^t is a polynomial of degree 8 in the entries of u . We can prove that the event \mathcal{E} occurs with a probability at least 9/10 using a concentration inequality deduced from the Hypercontractivity of Gaussian polynomials (Aubrun and Szarek, 2017, Corollary 5.49) and a union bound. Observe that the union bound here adds only a factor of $\log(N)^4$ because for a non-adaptive strategy, there are at most N couples of inputs/measurements. To carry out the analysis, we need to bound the moments of the random variables:

$$Z_t(U, V) = \varepsilon^2 \mathbb{E}_{i_t} \left[\Phi_{u, U}^{t, i_t} \Phi_{v, V}^{t, i_t} \right] \quad \text{where} \quad \Phi_{u, U}^{t, i_t} = \frac{\text{Tr}(B_{i_t}^{t, \dagger} A_t | u \rangle \langle u | A_t^\dagger B_{i_t}^t U)}{\|u\|_2^2 \text{Tr}(B_{i_t}^{t, \dagger} A_t A_t^\dagger B_{i_t}^t)}.$$

Since Z_t is a polynomial of degree 2 (in the entries of U and V) of expectation 0, the Hypercontractivity (Aubrun and Szarek, 2017, Proposition 5.48) implies for all $k \in \{1, \dots, N\} : \mathbb{E}(|Z_t|^k) \leq k^k \mathbb{E}(Z_t^2)^{k/2}$. Hence, it is sufficient to upper bound the second moment which can be done using the inequalities (2): $\mathbb{E}(Z_t^2) \leq \mathcal{O}\left(\frac{\varepsilon^4 \log(N)^4}{d_{\text{in}}^4 d_{\text{out}}^3}\right)$. By a contradiction argument and grouping all these elements, we can prove that $N \log(N)^2 \geq \Omega\left(\frac{d_{\text{in}}^2 d_{\text{out}}^{1.5}}{\varepsilon^2}\right)$ and finally $N \geq \Omega\left(\frac{d_{\text{in}}^2 d_{\text{out}}^{1.5}}{\log(d_{\text{in}} d_{\text{out}}/\varepsilon)^2 \varepsilon^2}\right)$. The detailed proof can be found in App. D.1.

This proof relies crucially on the non-adaptiveness of the strategy. A natural question arises then, can adaptive strategies outperform their non-adaptive counterpart? We do not settle completely this question in this article. Yet, we propose a lower bound for adaptive strategies showing that, if a separation exists, the advantage would be at most $\mathcal{O}(\sqrt{d_{\text{out}}})$.

Theorem 7 *Let $\varepsilon \leq 1/32$ and $d_{\text{out}} \geq 10$. Any incoherent ancilla-assisted adaptive algorithm for testing identity to the depolarizing channel requires, in the worst case, $N = \Omega\left(\frac{d_{\text{in}}^2 d_{\text{out}} + d_{\text{out}}^{1.5}}{\varepsilon^2}\right)$ measurements.*

The proof of this theorem uses the same construction as the one for the non-adaptive lower bound. The main difference is the use of the KL divergence to compare the observations (I_1, \dots, I_N) under the two hypotheses instead of the TV distance. On the one hand, the data processing implies that $\text{KL}\left(\mathbb{P}_{\mathcal{D}}^{I_1, \dots, I_N} \middle\| \mathbb{E}_{\mathcal{N} \sim \mathcal{P}} \mathbb{P}_{\mathcal{N}}^{I_1, \dots, I_N}\right) \geq \frac{1}{3} \log(2)$. On the other hand, using Jensen's inequality and inequalities of the log function we upper bound the KL divergence: $\text{KL}\left(\mathbb{P}_{\mathcal{D}}^{I_1, \dots, I_N} \middle\| \mathbb{E}_{\mathcal{N} \sim \mathcal{P}} \mathbb{P}_{\mathcal{N}}^{I_1, \dots, I_N}\right) \leq \frac{256N\varepsilon^2}{d_{\text{in}}^2 d_{\text{out}}}$. These two inequalities implies $d_{\text{in}}^2 d_{\text{out}}$ part of the lower bound. The $d_{\text{out}}^{1.5}$ part of the lower bound follows easily from the hardness of quantum state certification (Chen et al., 2022d). The detailed proof can be found in App. D.2.

5. Conclusion and open problems

We have generalized the problem of testing identity to quantum channels. We have in particular identified the optimal complexity $\Theta(d/\varepsilon^2)$ for testing identity to a unitary channel in the adaptive

setting. Moreover, we have shown that the complexity for testing identity to the depolarizing channel in the non-adaptive setting is $\tilde{\Theta}(d_{\text{in}}^2 d_{\text{out}}^{1.5} / \varepsilon^2)$. These results open up several interesting questions: can the gap between non-adaptive and adaptive strategies for certification of the depolarizing channel be closed? How to achieve the instance optimality (as in (Valiant and Valiant, 2016; Chen et al., 2022f))? This would allow to adapt the complexity to the tested process \mathcal{N}_0 . Another interesting issue deals with the fact that 4-designs can replace Haar distributed unitaries in Alg. 2. But can the same complexity be achieved for 3 (and lower) designs? Finally, it would be interesting to consider general strategies allowing entanglement between the uses of the channel, as was done for states in (O’Donnell and Wright, 2015).

Acknowledgments

We acknowledge support from the European Research Council (ERC Grant AlgoQIP, Agreement No. 851716) and from the European Union’s Horizon 2020 research and innovation programme under Grant Agreement No 101017733 within the QuantERA II Programme.

Aurélien Garivier acknowledges the support of the Chaire SeqALO (ANR-20-CHIA-0020-01).

Aadil Oufkir would like to thank Guillaume Aubrun for helpful discussions and Moritz Weber for his hospitality and organization of the Focus Semester on Quantum Information at Saarland University.

References

- Guillaume Aubrun and Stanisław J Szarek. *Alice and Bob meet Banach*, volume 223. American Mathematical Soc., 2017.
- Koenraad MR Audenaert. Quantum skew divergence. *Journal of Mathematical Physics*, 55(11):112202, 2014.
- Costin Bădescu, Ryan O’Donnell, and John Wright. Quantum state certification. In *Proceedings of the 51st Annual ACM SIGACT Symposium on Theory of Computing*, pages 503–514, 2019.
- Max Born. Zur Quantenmechanik der Stoßvorgänge. *Zeitschrift für Physik*, 37(12):863–867, December 1926. doi: 10.1007/BF01397477.
- Sebastien Bubeck, Sitan Chen, and Jerry Li. Entanglement is necessary for optimal quantum property testing. In *2020 IEEE 61st Annual Symposium on Foundations of Computer Science (FOCS)*, pages 692–703. IEEE, 2020.
- Kean Chen, Qisheng Wang, Peixun Long, and Mingsheng Ying. Unitarity estimation for quantum channels. *arXiv preprint arXiv:2212.09319*, 2022a.
- Senrui Chen, Sisi Zhou, Alireza Seif, and Liang Jiang. Quantum advantages for pauli channel estimation. *Physical Review A*, 105(3):032435, 2022b.
- Sitan Chen, Jordan Cotler, Hsin-Yuan Huang, and Jerry Li. Exponential separations between learning with and without quantum memory. In *2021 IEEE 62nd Annual Symposium on Foundations of Computer Science (FOCS)*, pages 574–585. IEEE, 2022c.

- Sitan Chen, Brice Huang, Jerry Li, and Allen Liu. Tight bounds for quantum state certification with incoherent measurements. *arXiv preprint arXiv:2204.07155*, 2022d.
- Sitan Chen, Brice Huang, Jerry Li, Allen Liu, and Mark Sellke. Tight bounds for state tomography with incoherent measurements. *arXiv preprint arXiv:2206.05265*, 2022e.
- Sitan Chen, Jerry Li, and Ryan O’Donnell. Toward instance-optimal state certification with incoherent measurements. In *Conference on Learning Theory*, pages 2541–2596. PMLR, 2022f.
- Man-Duen Choi. Completely positive linear maps on complex matrices. *Linear algebra and its applications*, 10(3):285–290, 1975.
- Benoît Collins and Piotr Śniady. Integration with respect to the haar measure on unitary, orthogonal and symplectic group. *Communications in Mathematical Physics*, 264(3):773–795, 2006.
- Benoit Collins, Sho Matsumoto, and Nadia Saad. Integration of invariant matrices and application to statistics. *arXiv preprint arXiv:1205.0956*, 2012.
- Ilias Diakonikolas, Themis Gouleakis, John Peebles, and Eric Price. Optimal identity testing with high probability. *arXiv preprint arXiv:1708.02728*, 2017.
- Christopher A Fuchs and Jeroen Van De Graaf. Cryptographic distinguishability measures for quantum-mechanical states. *IEEE Transactions on Information Theory*, 45(4):1216–1227, 1999.
- Yinzhen Gu. *Moments of random matrices and weingarten functions*. PhD thesis, 2013.
- Andrzej Jamiolkowski. Linear transformations which preserve trace and positive semidefiniteness of operators. *Reports on Mathematical Physics*, 3(4):275–278, 1972.
- Anna Jenčová and Martin Plávala. Conditions for optimal input states for discrimination of quantum channels. *Journal of Mathematical Physics*, 57(12):122203, 2016.
- Jonathan Kunjumen, Minh C Tran, Daniel Carney, and Jacob M Taylor. Shadow process tomography of quantum channels. *arXiv preprint arXiv:2110.03629*, 2021.
- Lucien LeCam. Convergence of estimates under dimensionality restrictions. *The Annals of Statistics*, pages 38–53, 1973.
- William Matthews, Stephanie Wehner, and Andreas Winter. Distinguishability of quantum states under restricted families of measurements with an application to quantum data hiding. *Communications in Mathematical Physics*, 291(3):813–843, 2009.
- Elizabeth Meckes, Mark Meckes, et al. Spectral measures of powers of random matrices. *Electronic communications in probability*, 18, 2013.
- Ashley Montanaro and Ronald de Wolf. A survey of quantum property testing. *arXiv preprint arXiv:1310.2035*, 2013.
- Ryan O’Donnell and John Wright. Quantum spectrum testing. In *Proceedings of the forty-seventh annual ACM symposium on Theory of computing*, pages 529–538, 2015.

Aadil Oufkir. Sample-optimal quantum process tomography with non-adaptive incoherent measurements. *arXiv preprint arXiv:2301.12925*, 2023.

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

Gregory Valiant and Paul Valiant. Instance optimal learning of discrete distributions. In *Proceedings of the forty-eighth annual ACM symposium on Theory of Computing*, pages 142–155, 2016.

Tim Van Erven and Peter Harremoos. Rényi divergence and kullback-leibler divergence. *IEEE Transactions on Information Theory*, 60(7):3797–3820, 2014.

Martin J Wainwright. *High-dimensional statistics: A non-asymptotic viewpoint*, volume 48. Cambridge University Press, 2019.

Guoming Wang. Property testing of unitary operators. *Physical Review A*, 84(5):052328, 2011.

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

Appendix A. Deferred proofs of the analysis of testing identity to identity Alg. 1

Lemma 8 *Let $|\phi\rangle$ be a random Haar vector of dimension d . We have*

$$\mathbb{E}_\phi [\mathbb{F}(\mathcal{N}(|\phi\rangle\langle\phi|), |\phi\rangle\langle\phi|)] = \frac{1 + d \mathbb{F}(\mathcal{J}_\mathcal{N}, |\Psi\rangle\langle\Psi|)}{1 + d}.$$

Proof Using Lem. 31 and Lem. 33, we have

$$\begin{aligned} \mathbb{E}_\phi [\mathbb{F}(\mathcal{N}(|\phi\rangle\langle\phi|), |\phi\rangle\langle\phi|)] &= \sum_k \mathbb{E}_U \left[\langle 0 | U^\dagger A_k U | 0 \rangle \langle 0 | U^\dagger A_k^\dagger U | 0 \rangle \right] \\ &= \sum_k \frac{(\text{Tr}(A_k A_k^\dagger) + \text{Tr}(A_k) \text{Tr}(A_k^\dagger))}{d(d+1)} \\ &= \frac{d + \sum_k |\text{Tr}(A_k)|^2}{d(d+1)} = \frac{1 + d \mathbb{F}(\mathcal{J}_\mathcal{N}, |\Psi\rangle\langle\Psi|)}{1 + d} \end{aligned}$$

where we use Lem. 9.

Lemma 9 *Let \mathcal{N} be a quantum channel of Kraus operators $\{A_k\}_k$. Let $S = \sum_k |\text{Tr}(A_k)|^2$. We can relate the average fidelity and S as follows:*

$$\mathbb{F}(\mathcal{J}_\mathcal{N}, |\Psi\rangle\langle\Psi|) = \frac{S}{d^2}.$$

Proof We have:

$$\begin{aligned} \mathbb{F}(\mathcal{J}_\mathcal{N}, |\Psi\rangle\langle\Psi|) &= \frac{1}{d^2} \sum_{i,j,k,l} \langle ii | \text{id} \otimes \mathcal{N}(|kk\rangle\langle ll|) | jj \rangle = \frac{1}{d^2} \sum_{i,j,k,l} \langle i | I | k \rangle \langle l | | j \rangle \langle i | \mathcal{N}(|k\rangle\langle l|) | j \rangle \\ &= \frac{1}{d^2} \sum_{i,j} \langle i | \mathcal{N}(|i\rangle\langle j|) | j \rangle = \frac{1}{d^2} \sum_{i,j,k} \langle i | A_k | i \rangle \langle j | A_k^\dagger | j \rangle = \frac{1}{d^2} \sum_k |\text{Tr}(A_k)|^2 = \frac{S}{d^2}. \end{aligned}$$

■
■

Lemma 10 *We have for all quantum channels \mathcal{N} :*

$$F(\mathcal{J}_{\mathcal{N}}, |\Psi\rangle\langle\Psi|) \leq 1 - \frac{d_{\text{Tr}}(\mathcal{N}, \text{id})^2}{4d} \leq 1 - \frac{d_{\diamond}(\mathcal{N}, \text{id})^4}{16d}.$$

Proof The following inequality permits to prove the second inequality (Watrous, 2018, Theorem 3.56, rephrased)

$$d_{\text{Tr}}(\mathcal{N}, \text{id}) \geq \frac{d_{\diamond}(\mathcal{N}, \text{id})^2}{2}.$$

It remains to prove the first inequality. For this, let $\varepsilon = d_{\text{Tr}}(\mathcal{N}, \text{id}) = \max_{|\phi\rangle \in \mathbb{S}^d} \|\mathcal{N}(|\phi\rangle\langle\phi|) - |\phi\rangle\langle\phi|\|_1$. Let $|\phi\rangle$ be a unit vector satisfying the previous maximization, we show that using Fuchs–van de Graaf inequality (Fuchs and Van De Graaf, 1999):

$$\langle\phi| \mathcal{N}(|\phi\rangle\langle\phi|) |\phi\rangle = F(\mathcal{N}(|\phi\rangle\langle\phi|), |\phi\rangle\langle\phi|) \leq 1 - \frac{1}{4} \|\mathcal{N}(|\phi\rangle\langle\phi|) - |\phi\rangle\langle\phi|\|_1^2 \leq 1 - \frac{\varepsilon^2}{4}.$$

On the other hand, we use the Kraus decomposition to describe the quantum channel $\mathcal{N}(\rho) = \sum_k A_k \rho A_k^\dagger$. We can write the previous fidelity in terms of the Kraus operators:

$$\langle\phi| \mathcal{N}(|\phi\rangle\langle\phi|) |\phi\rangle = \sum_k \langle\phi| A_k |\phi\rangle \langle\phi| A_k^\dagger |\phi\rangle = \sum_k |\langle\phi| A_k |\phi\rangle|^2.$$

Hence:

$$\sum_k |\langle\phi| A_k |\phi\rangle|^2 \leq 1 - \frac{\varepsilon^2}{4}. \quad (3)$$

Let $|\phi_1\rangle = |\phi\rangle$ and we can complete it to have an ortho-normal basis $\{|\phi_i\rangle\}_{i=1}^d$. Moreover, we have $F(\mathcal{J}_{\mathcal{N}}, |\Psi\rangle\langle\Psi|) = \frac{1}{d^2} \sum_k |\text{Tr}(A_k)|^2$ (Lem. 9). By applying the Cauchy-Schwarz inequality and using the inequality (3):

$$\begin{aligned} \sum_k |\text{Tr}(A_k)|^2 &= \sum_k \left| \sum_{i=1}^d \langle\phi_i| A_k |\phi_i\rangle \right|^2 \leq \sum_{k,i} d |\langle\phi_i| A_k |\phi_i\rangle|^2 \\ &= d \sum_k |\langle\phi_1| A_k |\phi_1\rangle|^2 + d \sum_{i=2}^d \sum_k |\langle\phi_i| A_k |\phi_i\rangle|^2 \\ &\leq d(1 - \varepsilon^2/4) + d(d-1) = d(d - \varepsilon^2/4) \end{aligned}$$

because for all $i \geq 2$:

$$\sum_k |\langle\phi_i| A_k |\phi_i\rangle|^2 \leq \sum_k \langle\phi_i| A_k^\dagger A_k |\phi_i\rangle = \langle\phi_i| \sum_k A_k^\dagger A_k |\phi_i\rangle = 1.$$

Finally, $F(\mathcal{J}_{\mathcal{N}}, |\Psi\rangle\langle\Psi|) = \frac{1}{d^2} \sum_k |\text{Tr}(A_k)|^2 \leq 1 - \frac{\varepsilon^2}{4d}$. ■

Appendix B. Lower bound for testing identity to identity

In this section, we establish a general lower bound for any algorithm (possibly adaptive) for testing identity to identity using ancilla-assisted strategies.

Theorem 11 *Any incoherent adaptive ancilla-assisted strategy requires a number of steps satisfying:*

$$N = \Omega\left(\frac{d}{\varepsilon^2}\right)$$

to distinguish between $\mathcal{N} = \text{id}$ and $d_\diamond(\mathcal{N}, \text{id}) \geq \varepsilon$ (or $d_{\text{Tr}}(\mathcal{N}, \text{id}) \geq \varepsilon$) with a probability at least $2/3$.

This theorem shows that Alg 1 has an optimal complexity.

Proof Under the null hypothesis H_0 , the quantum channel $\mathcal{N} = \text{id}$. Under the alternate hypothesis H_1 , we can choose \mathcal{N} so that $d_\diamond(\mathcal{N}, \text{id}) \geq d_{\text{Tr}}(\mathcal{N}, \text{id}) \geq \varepsilon$. A difficult to test channel is a channel sending almost every vector of a basis to itself. With this intuition, we choose $V \in \text{Haar}(d)$, and construct the channel $\mathcal{N}_V(\rho) = \frac{1}{2}\rho + \frac{1}{2}U_V\rho U_V^\dagger$ where U_V satisfies:

$$U_V V |l\rangle = \begin{cases} \sqrt{1-\varepsilon^2}V|0\rangle + \varepsilon V|1\rangle & \text{if } l=0 \\ \sqrt{1-\varepsilon^2}V|1\rangle - \varepsilon V|0\rangle & \text{if } l=1 \\ V|l\rangle & \text{otherwise.} \end{cases}$$

Taking a mixture of the identity channel and the unitary channel $U_V \cdot U_V^\dagger$ in the definition of \mathcal{N}_V is crucial in this proof and is inspired by the quantum skew divergence (Audenaert, 2014). We need to show first that such a channel is ε -far from the identity channel. Indeed, let $|\phi\rangle = V|0\rangle$, we have:

$$\begin{aligned} d_\diamond(\mathcal{N}_V, \text{id}) &\geq d_{\text{Tr}}(\mathcal{N}_V, \text{id}) \geq \|\mathcal{N}_V(|\phi\rangle\langle\phi|) - \text{id}(|\phi\rangle\langle\phi|)\|_1 \\ &= \left\| \frac{1}{2}|\phi\rangle\langle\phi| + \frac{1}{2}U_V|\phi\rangle\langle\phi|U_V^\dagger - |\phi\rangle\langle\phi| \right\|_1 \\ &= \frac{1}{2} \left\| V|0\rangle\langle 0|V^\dagger - U_V V|0\rangle\langle 0|V^\dagger U_V^\dagger \right\|_1 \\ &= \frac{1}{2} \left\| |0\rangle\langle 0| - \left(\sqrt{1-\varepsilon^2}|0\rangle + \varepsilon|1\rangle\right) \left(\sqrt{1-\varepsilon^2}\langle 0| + \varepsilon\langle 1|\right) \right\|_1 \\ &= \frac{1}{2} \left\| \varepsilon^2|0\rangle\langle 0| - \varepsilon\sqrt{1-\varepsilon^2}(|0\rangle\langle 1| + |1\rangle\langle 0|) - \varepsilon^2|1\rangle\langle 1| \right\|_1 = \varepsilon. \end{aligned}$$

Hence a $1/3$ -correct algorithm should distinguish between the identity channel and \mathcal{N}_V with at least a probability $2/3$ of success. This algorithm can only choose an input ρ_t which we can suppose (by the convexity of the KL divergence) of rank 1, that is $\rho_t = |\psi_t\rangle\langle\psi_t|$ at each step t and perform a measurement using the POVM $\mathcal{M}_t = \{\lambda_i^t |\phi_i^t\rangle\langle\phi_i^t|\}_{i \in \mathcal{I}_t}$ on the output quantum state $\text{id} \otimes \mathcal{N}(\rho_t)$. Note that the identity channel id acts on the ancilla space. These choices can depend on the previous observations, that is, the algorithm can be adaptive. Let $I_{\leq N} = (I_1, \dots, I_N)$ be the observations of this algorithm where N is a sufficient number of steps to decide correctly with a probability at least $2/3$. We can compare the distributions of the observations under the two hypotheses using the

Kullback-Leibler divergence. Let P (resp. Q) be the distribution of (I_1, \dots, I_N) under H_0 (resp. H_1). The distribution of (I_1, \dots, I_N) under H_0 is:

$$P := \left\{ \prod_{t=1}^N \lambda_{i_t}^t \langle \phi_{i_t}^t | \rho_t | \phi_{i_t}^t \rangle \right\}_{i_1, \dots, i_N} = \left\{ \prod_{t=1}^N \lambda_{i_t}^t |\langle \phi_{i_t}^t | \psi_t \rangle|^2 \right\}_{i_1, \dots, i_N}.$$

On the other hand, the distribution of (I_1, \dots, I_N) under H_1 conditioned on V is:

$$Q_V := \left\{ \prod_{t=1}^N \lambda_{i_t}^t \langle \phi_{i_t}^t | \text{id} \otimes \mathcal{N}_V(\rho_t) | \phi_{i_t}^t \rangle \right\}_{i_1, \dots, i_N}.$$

Moreover, we can write each rank one input state and measurement vector as follows:

$$|\psi_t\rangle = A_t \otimes \mathbb{I} |w\rangle \quad \text{and} \quad |\phi_{i_t}^t\rangle = B_{i_t}^t \otimes \mathbb{I} |w\rangle$$

where $|w\rangle = \sum_{i=1}^d |ii\rangle$ and the matrices $A_t \in \mathbb{C}^{d_{\text{anc}} \times d}$ and $B_{i_t}^t \in \mathbb{C}^{d_{\text{anc}} \times d}$ verify:

$$\text{Tr}(A_t A_t^\dagger) = 1 \quad \text{and} \quad \text{Tr}(B_{i_t}^t B_{i_t}^{t,\dagger}) = 1.$$

Note that we have for all t , for all $X \in \mathbb{C}^{d_{\text{anc}} \times d_{\text{anc}}}$ we have $\sum_{i_t} \lambda_{i_t}^t B_{i_t}^{t,\dagger} X B_{i_t}^t = \text{Tr}(X) \mathbb{I}$. Indeed, the condition of the POVM \mathcal{M}_t implies:

$$X \otimes \mathbb{I} = X \otimes \mathbb{I} \sum_{i_t} \lambda_{i_t}^t |\phi_{i_t}^t\rangle \langle \phi_{i_t}^t| = \sum_{i_t} \lambda_{i_t}^t X B_{i_t}^t \otimes \mathbb{I} |w\rangle \langle w| B_{i_t}^{t,\dagger} \otimes \mathbb{I}$$

hence by taking the partial trace on the first system we obtain

$$\text{Tr}(X) \mathbb{I} = \sum_{i_t, i, j} \lambda_{i_t}^t \langle j | B_{i_t}^{t,\dagger} X B_{i_t}^t | i \rangle |i\rangle \langle j|.$$

Finally

$$\sum_{i_t} \lambda_{i_t}^t B_{i_t}^{t,\dagger} X B_{i_t}^t = \text{Tr}(X) \mathbb{I}.$$

By taking $X = \mathbb{I}$ and the partial trace on the second system we obtain

$$\sum_{i_t} \lambda_{i_t}^t B_{i_t}^t B_{i_t}^{t,\dagger} = d \mathbb{I}_{d_{\text{anc}}}.$$

Recall that for an adaptive strategy, for all $t \in [N]$, ρ_t and $\mathcal{M}_t = \{\lambda_{i_t}^t |\phi_{i_t}^t\rangle \langle \phi_{i_t}^t|\}_{i_t}$ depend on (i_1, \dots, i_{t-1}) . So, the KL divergence between P and Q_V can be expressed as follows:

$$\begin{aligned} \text{KL}(P \| Q_V) &= \mathbb{E}_{i \sim P} (-\log) \left(\frac{Q_{V,i}}{P_i} \right) \\ &= \sum_{t=1}^N \mathbb{E}_{i \leq N} (-\log) \left(\frac{\langle \phi_{i_t}^t | \text{id} \otimes \mathcal{N}_V(\rho_t) | \phi_{i_t}^t \rangle}{\langle \phi_{i_t}^t | \rho_t | \phi_{i_t}^t \rangle} \right) \\ &= \sum_{t=1}^N \mathbb{E}_{i \leq t} (-\log) \left(\frac{\langle \phi_{i_t}^t | \text{id} \otimes \mathcal{N}_V(\rho_t) | \phi_{i_t}^t \rangle}{\langle \phi_{i_t}^t | \rho_t | \phi_{i_t}^t \rangle} \right) \end{aligned}$$

where we use the notation for $t \in [N]$, $\mathbb{E}_{i_{\leq t}}(X(i_1, \dots, i_t)) = \sum_{i_1, \dots, i_t} \prod_{k=1}^t \lambda_{i_k}^k \langle \phi_{i_k}^k | \rho_k | \phi_{i_k}^k \rangle X(i_1, \dots, i_t)$ and the fact that the term $\frac{\langle \phi_{i_t}^t | \text{id} \otimes \mathcal{N}_V(\rho_t) | \phi_{i_t}^t \rangle}{\langle \phi_{i_t}^t | \rho_t | \phi_{i_t}^t \rangle}$ depends only on (i_1, \dots, i_t) .

Let \mathcal{E} be the event that the algorithm accepts H_0 , we apply the Data-Processing inequality on the KL divergence (see Prop. F.3):

$$\begin{aligned} \text{KL}(P \| Q_V) &\geq \text{KL}(P(\mathcal{E}) \| Q_V(\mathcal{E})) \\ &\geq \text{KL}\left(\frac{2}{3} \parallel \frac{1}{3}\right) = \frac{2}{3} \log(2) - \frac{1}{3} \log(2) = \frac{1}{3} \log(2) \end{aligned}$$

where $\text{KL}(p \| q) = \text{KL}(\text{Bern}(p) \| \text{Bern}(q))$. Hence

$$\mathbb{E}_{V \sim \text{Haar}(d)} \text{KL}(P \| Q_V) \geq \frac{1}{3} \log(2).$$

Let $M_V = \mathbb{I} - U_V$ and $S_V = \mathbb{I} - \frac{1}{2}M_V$. We can write the logarithmic term in the expression of $\text{KL}(P \| Q_V)$ as follows:

$$\begin{aligned} &(-\log) \left(\frac{\langle \phi_{i_t}^t | \text{id} \otimes \mathcal{N}_V(\rho_t) | \phi_{i_t}^t \rangle}{\langle \phi_{i_t}^t | \rho_t | \phi_{i_t}^t \rangle} \right) \\ &= (-\log) \left(\frac{\langle \phi_{i_t}^t | (\frac{1}{2}\rho_t + \frac{1}{2}(\mathbb{I} \otimes U_V)\rho_t(\mathbb{I} \otimes U_V^\dagger)) | \phi_{i_t}^t \rangle}{\langle \phi_{i_t}^t | \rho_t | \phi_{i_t}^t \rangle} \right) \\ &= (-\log) \left(1 - \frac{\Re(\langle \phi_{i_t}^t | (\mathbb{I} \otimes M_V)\rho_t | \phi_{i_t}^t \rangle)}{\langle \phi_{i_t}^t | \rho_t | \phi_{i_t}^t \rangle} + \frac{1}{2} \frac{\langle \phi_{i_t}^t | (\mathbb{I} \otimes M_V)\rho_t(\mathbb{I} \otimes M_V^\dagger) | \phi_{i_t}^t \rangle}{\langle \phi_{i_t}^t | \rho_t | \phi_{i_t}^t \rangle} \right) \\ &= (-\log) \left(1 - \frac{1}{2} \frac{\langle \phi_{i_t}^t | (\mathbb{I} \otimes M_V)\rho_t(\mathbb{I} \otimes S_V^\dagger) | \phi_{i_t}^t \rangle}{\langle \phi_{i_t}^t | \rho_t | \phi_{i_t}^t \rangle} - \frac{1}{2} \frac{\langle \phi_{i_t}^t | (\mathbb{I} \otimes S_V)\rho_t(\mathbb{I} \otimes M_V^\dagger) | \phi_{i_t}^t \rangle}{\langle \phi_{i_t}^t | \rho_t | \phi_{i_t}^t \rangle} \right). \end{aligned}$$

For $t \in [N]$ and $i_{\leq t} = (i_1, \dots, i_t)$, define the event $\mathcal{G}(t, i_{\leq t}) = \left\{ \langle \phi_{i_t}^t | \rho_t | \phi_{i_t}^t \rangle \leq \frac{\varepsilon^2}{d^2} \text{Tr}(A_t^\dagger B_{i_t}^t B_{i_t}^{t,\dagger} A_t) \right\}$. We can distinguish whether the event \mathcal{G} is satisfied or not:

$$\mathbb{E}_{V \sim \text{Haar}(d)} \text{KL}(P \| Q_V) = \sum_{t=1}^N \mathbb{E}_{V \sim \text{Haar}(d)} \mathbb{E}_{i_{\leq t}} (\mathbf{1}\{\mathcal{G}(t, i_{\leq t})\} + \mathbf{1}\{\mathcal{G}^c(t, i_{\leq t})\}) (-\log) \left(\frac{\langle \phi_{i_t}^t | \text{id} \otimes \mathcal{N}_V(\rho_t) | \phi_{i_t}^t \rangle}{\langle \phi_{i_t}^t | \rho_t | \phi_{i_t}^t \rangle} \right).$$

Let us first analyze the setting when the event \mathcal{G} holds. Fix $t \in [N]$, observe that we have the inequality:

$$\begin{aligned} &(-\log) \left(\frac{\langle \phi_{i_t}^t | \text{id} \otimes \mathcal{N}_V(\rho_t) | \phi_{i_t}^t \rangle}{\langle \phi_{i_t}^t | \rho_t | \phi_{i_t}^t \rangle} \right) = (-\log) \left(\frac{\langle \phi_{i_t}^t | (\frac{1}{2}\rho_t + \frac{1}{2}(\mathbb{I} \otimes U_V)\rho_t(\mathbb{I} \otimes U_V^\dagger)) | \phi_{i_t}^t \rangle}{\langle \phi_{i_t}^t | \rho_t | \phi_{i_t}^t \rangle} \right) \\ &= (-\log) \left(\frac{1}{2} + \frac{\langle \phi_{i_t}^t | (\frac{1}{2}(\mathbb{I} \otimes U_V)\rho_t(\mathbb{I} \otimes U_V^\dagger)) | \phi_{i_t}^t \rangle}{\langle \phi_{i_t}^t | \rho_t | \phi_{i_t}^t \rangle} \right) \leq \log(2) \leq 1. \end{aligned}$$

Then we can control the expectation under the event \mathcal{G} as follows:

$$\begin{aligned}
 & \mathbb{E}_{V \sim \text{Haar}(d)} \mathbb{E}_{i \leq t} \mathbf{1}\{\mathcal{G}(t, i_{\leq t})\} (-\log) \left(\frac{\langle \phi_{i_t}^t | \text{id} \otimes \mathcal{N}_V(\rho_t) | \phi_{i_t}^t \rangle}{\langle \phi_{i_t}^t | \rho_t | \phi_{i_t}^t \rangle} \right) \\
 & \leq \mathbb{E}_{V \sim \text{Haar}(d)} \mathbb{E}_{i \leq t-1} \sum_{i_t} \lambda_{i_t}^t \langle \phi_{i_t}^t | \rho_t | \phi_{i_t}^t \rangle \mathbf{1}\{\mathcal{G}(t, i_{\leq t})\} \\
 & \leq \mathbb{E}_{V \sim \text{Haar}(d)} \mathbb{E}_{i \leq t-1} \sum_{i_t} \lambda_{i_t}^t \left(\frac{\varepsilon^2}{d^2} \text{Tr}(A_t^\dagger B_{i_t}^t B_{i_t}^{t,\dagger} A_t) \right) \mathbf{1}\{\mathcal{G}(t, i_{\leq t})\} \\
 & \leq \mathbb{E}_{V \sim \text{Haar}(d)} \mathbb{E}_{i \leq t-1} \sum_{i_t} \lambda_{i_t}^t \left(\frac{\varepsilon^2}{d^2} \text{Tr}(A_t^\dagger B_{i_t}^t B_{i_t}^{t,\dagger} A_t) \right) \\
 & = \mathbb{E}_{V \sim \text{Haar}(d)} \mathbb{E}_{i \leq t-1} \left(\frac{\varepsilon^2}{d^2} \text{Tr}(A_t^\dagger d A_t) \right) = \mathbb{E}_{V \sim \text{Haar}(d)} \mathbb{E}_{i \leq t-1} \left(\frac{\varepsilon^2}{d} \right) = \frac{\varepsilon^2}{d} \quad (4)
 \end{aligned}$$

where we use the fact that under the event \mathcal{G} we have $\langle \phi_{i_t}^t | \rho_t | \phi_{i_t}^t \rangle \leq \frac{\varepsilon^2}{d^2} \text{Tr}(A_t^\dagger B_{i_t}^t B_{i_t}^{t,\dagger} A_t)$, $\text{Tr}(A_t^\dagger A_t) = 1$ and $\sum_{i_t} \lambda_{i_t}^t B_{i_t}^t B_{i_t}^{t,\dagger} = d\mathbb{I}$ which is an implication of the fact that $\mathcal{M}_t = \{\lambda_i^t | \phi_i^t \rangle \langle \phi_i^t | \}_{i \in \mathcal{I}_t}$ is a POVM.

On the other hand under $\mathcal{G}^c(t, i_{\leq t})$, we will use instead the inequality

$$(-\log)(x) \leq (1-x) + (x-1)^2 \quad \text{valid for all } x \in \left[\frac{1}{2}, +\infty \right).$$

We apply this inequality for $x = \frac{\langle \phi_{i_t}^t | \text{id} \otimes \mathcal{N}_V(\rho_t) | \phi_{i_t}^t \rangle}{\langle \phi_{i_t}^t | \rho_t | \phi_{i_t}^t \rangle} = \frac{1}{2} + \frac{\langle \phi_{i_t}^t | (\frac{1}{2}(\mathbb{I} \otimes U_V) \rho_t (\mathbb{I} \otimes U_V^\dagger)) | \phi_{i_t}^t \rangle}{\langle \phi_{i_t}^t | \rho_t | \phi_{i_t}^t \rangle} \geq \frac{1}{2}$, the first term of the upper bound is:

$$\begin{aligned}
 (1-x) &= 1 - \frac{\langle \phi_{i_t}^t | \text{id} \otimes \mathcal{N}_V(\rho_t) | \phi_{i_t}^t \rangle}{\langle \phi_{i_t}^t | \rho_t | \phi_{i_t}^t \rangle} \\
 &= \frac{1}{2} \frac{\langle \phi_{i_t}^t | (\mathbb{I} \otimes M_V) \rho_t (\mathbb{I} \otimes S_V^\dagger) | \phi_{i_t}^t \rangle}{\langle \phi_{i_t}^t | \rho_t | \phi_{i_t}^t \rangle} + \frac{1}{2} \frac{\langle \phi_{i_t}^t | (\mathbb{I} \otimes S_V) \rho_t (\mathbb{I} \otimes M_V^\dagger) | \phi_{i_t}^t \rangle}{\langle \phi_{i_t}^t | \rho_t | \phi_{i_t}^t \rangle} \\
 &= \frac{\Re \langle \phi_{i_t}^t | (\mathbb{I} \otimes M_V) | \psi_t \rangle \langle \psi_t | (\mathbb{I} \otimes S_V^\dagger) | \phi_{i_t}^t \rangle}{\langle \phi_{i_t}^t | \rho_t | \phi_{i_t}^t \rangle} \\
 &= \frac{\Re \langle w | (B_{i_t}^{t,\dagger} A_t \otimes M_V) | w \rangle \langle w | (A_t^\dagger B_{i_t}^t \otimes S_V^\dagger) | w \rangle}{\langle w | (B_{i_t}^{t,\dagger} A_t \otimes \mathbb{I}) | w \rangle \langle w | (A_t^\dagger B_{i_t}^t \otimes \mathbb{I}) | w \rangle} \\
 &= \frac{\Re \text{Tr}(B_{i_t}^{t,\dagger} A_t M_V^\top) \text{Tr}(A_t^\dagger B_{i_t}^t \bar{S}_V)}{\text{Tr}(B_{i_t}^{t,\dagger} A_t) \text{Tr}(A_t^\dagger B_{i_t}^t)} \quad (5)
 \end{aligned}$$

and by using first the inequality $(x + y)^2 \leq 2(x^2 + y^2)$ and then the Cauchy Schwarz inequality applied for the vectors $\sqrt{\rho_t} |\phi_{i_t}^t\rangle$ and $\sqrt{\rho_t} M_V^\dagger |\phi_{i_t}^t\rangle$ we can upper bound the second term as follows:

$$\begin{aligned}
 (x - 1)^2 &= \left(\frac{\langle \phi_{i_t}^t | \text{id} \otimes \mathcal{N}_V(\rho_t) | \phi_{i_t}^t \rangle}{\langle \phi_{i_t}^t | \rho_t | \phi_{i_t}^t \rangle} - 1 \right)^2 \\
 &= \left(\frac{\Re(\langle \phi_{i_t}^t | (\mathbb{I} \otimes M_V) \rho_t | \phi_{i_t}^t \rangle)}{\langle \phi_{i_t}^t | \rho_t | \phi_{i_t}^t \rangle} - \frac{1}{2} \frac{\langle \phi_{i_t}^t | (\mathbb{I} \otimes M_V) \rho_t (\mathbb{I} \otimes M_V^\dagger) | \phi_{i_t}^t \rangle}{\langle \phi_{i_t}^t | \rho_t | \phi_{i_t}^t \rangle} \right)^2 \\
 &\leq 2 \left(\frac{|\langle \phi_{i_t}^t | (\mathbb{I} \otimes M_V) \rho_t | \phi_{i_t}^t \rangle|}{\langle \phi_{i_t}^t | \rho_t | \phi_{i_t}^t \rangle} \right)^2 + 2 \left(\frac{1}{2} \frac{\langle \phi_{i_t}^t | (\mathbb{I} \otimes M_V) \rho_t (\mathbb{I} \otimes M_V^\dagger) | \phi_{i_t}^t \rangle}{\langle \phi_{i_t}^t | \rho_t | \phi_{i_t}^t \rangle} \right)^2 \\
 &\leq 2 \left(\frac{\langle \phi_{i_t}^t | (\mathbb{I} \otimes M_V) \rho_t (\mathbb{I} \otimes M_V^\dagger) | \phi_{i_t}^t \rangle}{\langle \phi_{i_t}^t | \rho_t | \phi_{i_t}^t \rangle} \right) + 2 \left(\frac{1}{2} \frac{\langle \phi_{i_t}^t | (\mathbb{I} \otimes M_V) \rho_t (\mathbb{I} \otimes M_V^\dagger) | \phi_{i_t}^t \rangle}{\langle \phi_{i_t}^t | \rho_t | \phi_{i_t}^t \rangle} \right)^2 \\
 &= 2 \frac{\text{Tr}(B_{i_t}^{t,\dagger} A_t M_V^\top) \text{Tr}(A_t^\dagger B_{i_t}^t \bar{M}_V)}{\text{Tr}(B_{i_t}^{t,\dagger} A_t) \text{Tr}(A_t^\dagger B_{i_t}^t)} + \frac{1}{2} \left(\frac{\text{Tr}(B_{i_t}^{t,\dagger} A_t M_V^\top) \text{Tr}(A_t^\dagger B_{i_t}^t \bar{M}_V)}{\text{Tr}(B_{i_t}^{t,\dagger} A_t) \text{Tr}(A_t^\dagger B_{i_t}^t)} \right)^2 \tag{6}
 \end{aligned}$$

Let us compute the expectation of (5). Let M, S such that $M_V = VMV^\dagger$ and $S_V = VSV^\dagger$. Concretely

$$M = \left(\begin{array}{cc|c} 1 - \sqrt{1 - \varepsilon^2} & -\varepsilon & 0 \\ \varepsilon & 1 - \sqrt{1 - \varepsilon^2} & 0 \\ \hline 0 & 0 & \mathbb{0}_{d-2} \end{array} \right) \quad \text{and} \quad S = \left(\begin{array}{cc|c} \frac{1}{2} + \frac{\sqrt{1 - \varepsilon^2}}{2} & \frac{\varepsilon}{2} & 0 \\ -\frac{\varepsilon}{2} & \frac{1}{2} + \frac{\sqrt{1 - \varepsilon^2}}{2} & 0 \\ \hline 0 & 0 & \mathbb{I}_{d-2} \end{array} \right).$$

Note that $\text{Tr}(M) = 2(1 - \sqrt{1 - \varepsilon^2})$, $\text{Tr}(S) = d - 1 + \sqrt{1 - \varepsilon^2}$, $\text{Tr}(MS^\dagger) = \text{Tr}(M^\dagger S) = 0$ and $MM^\dagger = M + M^\dagger = M^\dagger M$. Let $\varepsilon' = (1 - \sqrt{1 - \varepsilon^2}) = \Theta(\varepsilon^2)$, we have by Weingarten calculus (Lem. 31):

$$\begin{aligned}
 &\left| \mathbb{E}_{V \sim \text{Haar}(d)} \left(\frac{\Re \text{Tr}(B_{i_t}^{t,\dagger} A_t M_V^\top) \text{Tr}(A_t^\dagger B_{i_t}^t \bar{S}_V)}{\text{Tr}(B_{i_t}^{t,\dagger} A_t) \text{Tr}(A_t^\dagger B_{i_t}^t)} \right) \right| \\
 &= \left| \frac{1}{\text{Tr}(B_{i_t}^{t,\dagger} A_t) \text{Tr}(A_t^\dagger B_{i_t}^t)} \Re \mathbb{E}_{V \sim \text{Haar}(d)} \left(\sum_{x,y} \langle x | B_{i_t}^{t,\dagger} A_t V M^\top V^\dagger | x \rangle \langle y | A_t^\dagger B_{i_t}^t V S V^\dagger | y \rangle \right) \right| \\
 &= \left| \frac{1}{\text{Tr}(B_{i_t}^{t,\dagger} A_t) \text{Tr}(A_t^\dagger B_{i_t}^t)} \Re \sum_{\alpha, \beta \in \mathfrak{S}_2} \sum_{x,y} \text{Wg}(\alpha\beta) \text{Tr}_\alpha(M^\top, S) \text{Tr}_{\beta(12)}(|x\rangle \langle y | A_t^\dagger B_{i_t}^t, |y\rangle \langle x | B_{i_t}^{t,\dagger} A_t) \right| \\
 &= \left| \Re \left(\frac{\text{Tr}(MS^\dagger) (d \text{Tr}(A_t^\dagger B_{i_t}^t B_{i_t}^{t,\dagger} A_t) - |\text{Tr}(A_t^\dagger B_{i_t}^t)|^2) + \text{Tr}(M) \text{Tr}(S) (d |\text{Tr}(A_t^\dagger B_{i_t}^t)|^2 - \text{Tr}(A_t^\dagger B_{i_t}^t B_{i_t}^{t,\dagger} A_t))}{d(d^2 - 1) \text{Tr}(B_{i_t}^{t,\dagger} A_t) \text{Tr}(A_t^\dagger B_{i_t}^t)} \right) \right| \\
 &= \left| \Re \left(\frac{2\varepsilon'(d - \varepsilon') (d |\text{Tr}(A_t^\dagger B_{i_t}^t)|^2 - \text{Tr}(A_t^\dagger B_{i_t}^t B_{i_t}^{t,\dagger} A_t))}{d(d^2 - 1) \text{Tr}(B_{i_t}^{t,\dagger} A_t) \text{Tr}(A_t^\dagger B_{i_t}^t)} \right) \right| \\
 &\leq \frac{2\varepsilon^2}{d} + \frac{2\varepsilon^2 \text{Tr}(A_t^\dagger B_{i_t}^t B_{i_t}^{t,\dagger} A_t)}{(d^2 - 1) \text{Tr}(B_{i_t}^{t,\dagger} A_t) \text{Tr}(A_t^\dagger B_{i_t}^t)}
 \end{aligned}$$

Recall the notation $\mathbb{E}_{i \leq t}(X(i_1, \dots, i_t)) = \sum_{i_1, \dots, i_t} \prod_{k=1}^t \lambda_{i_k}^k \langle \phi_{i_k}^k | \rho_k | \phi_{i_k}^k \rangle X(i_1, \dots, i_t)$. If we take the expectation $\mathbb{E}_{i \leq t}$ under the event $\mathcal{G}^c(t, i_{\leq t})$, we obtain

$$\begin{aligned}
 & \mathbb{E}_{V \sim \text{Haar}(d)} \mathbb{E}_{i \leq t} \mathbf{1}\{\mathcal{G}^c(t, i_t)\} \left(\frac{\Re \langle \phi_{i_t}^t | (\mathbb{I} \otimes M_V) \rho_t (\mathbb{I} \otimes S_V^\dagger) | \phi_{i_t}^t \rangle}{\langle \phi_{i_t}^t | \rho_t | \phi_{i_t}^t \rangle} \right) \\
 & \leq \mathbb{E}_{i \leq t} \mathbf{1}\{\mathcal{G}^c(t, i_t)\} \left| \mathbb{E}_{V \sim \text{Haar}(d)} \left(\frac{\Re \langle \phi_{i_t}^t | (\mathbb{I} \otimes M_V) \rho_t (\mathbb{I} \otimes S_V^\dagger) | \phi_{i_t}^t \rangle}{\langle \phi_{i_t}^t | \rho_t | \phi_{i_t}^t \rangle} \right) \right| \\
 & \leq \mathbb{E}_{i \leq t} \mathbf{1}\{\mathcal{G}^c(t, i_t)\} \left(\frac{2\varepsilon^2}{d} + \frac{2\varepsilon^2 \text{Tr}(A_t^\dagger B_{i_t}^t B_{i_t}^{t,\dagger} A_t)}{(d^2 - 1) \text{Tr}(B_{i_t}^{t,\dagger} A_t) \text{Tr}(A_t^\dagger B_{i_t}^t)} \right) \\
 & \leq \mathbb{E}_{i \leq t} \left(\frac{2\varepsilon^2}{d} + \frac{2\varepsilon^2 \text{Tr}(A_t^\dagger B_{i_t}^t B_{i_t}^{t,\dagger} A_t)}{(d^2 - 1) \text{Tr}(B_{i_t}^{t,\dagger} A_t) \text{Tr}(A_t^\dagger B_{i_t}^t)} \right) \\
 & = \frac{2\varepsilon^2}{d} + \mathbb{E}_{i \leq t-1} \sum_{i_t} \lambda_{i_t}^t \langle \phi_{i_t}^t | \rho_t | \phi_{i_t}^t \rangle \times \frac{2\varepsilon^2 \text{Tr}(A_t^\dagger B_{i_t}^t B_{i_t}^{t,\dagger} A_t)}{(d^2 - 1) \langle \phi_{i_t}^t | \rho_t | \phi_{i_t}^t \rangle} \\
 & = \frac{2\varepsilon^2}{d} + \mathbb{E}_{i \leq t-1} \frac{2\varepsilon^2}{d^2 - 1} \sum_{i_t} \lambda_{i_t}^t \text{Tr}(A_t^\dagger B_{i_t}^t B_{i_t}^{t,\dagger} A_t) \\
 & = \frac{2\varepsilon^2}{d} + \mathbb{E}_{i \leq t-1} \frac{2\varepsilon^2}{d^2 - 1} \text{Tr}(A_t^\dagger d A_t) \leq \frac{5\varepsilon^2}{d} \tag{7}
 \end{aligned}$$

where we use $\sum_{i_t} \lambda_{i_t}^t B_{i_t}^t B_{i_t}^{t,\dagger} = d \mathbb{I}$ and $\text{Tr}(A_t A_t^\dagger) = 1$. We move to the expectation $\mathbb{E}_{i \leq t}$ of the first term of (6), it is non negative so we can safely remove the condition $\mathbf{1}\{\mathcal{G}^c(t, i_t)\}$:

$$\begin{aligned}
 & \mathbb{E}_V \mathbb{E}_{i \leq t} \mathbf{1}\{\mathcal{G}^c(t, i_t)\} \frac{2 \langle \phi_{i_t}^t | (\mathbb{I} \otimes M_V) \rho_t (\mathbb{I} \otimes M_V^\dagger) | \phi_{i_t}^t \rangle}{\langle \phi_{i_t}^t | \rho_t | \phi_{i_t}^t \rangle} \\
 & \leq \mathbb{E}_V \mathbb{E}_{i \leq t} \frac{2 \langle \phi_{i_t}^t | (\mathbb{I} \otimes M_V) \rho_t (\mathbb{I} \otimes M_V^\dagger) | \phi_{i_t}^t \rangle}{\langle \phi_{i_t}^t | \rho_t | \phi_{i_t}^t \rangle} \\
 & = \mathbb{E}_V \mathbb{E}_{i \leq t-1} \sum_{i_t} 2 \lambda_{i_t}^t \langle \phi_{i_t}^t | (\mathbb{I} \otimes M_V) \rho_t (\mathbb{I} \otimes M_V^\dagger) | \phi_{i_t}^t \rangle \\
 & = \mathbb{E}_{i \leq t-1} \mathbb{E}_V 2 \text{Tr}((\mathbb{I} \otimes M_V) \rho_t (\mathbb{I} \otimes M_V^\dagger)) \\
 & = \mathbb{E}_{i \leq t-1} \mathbb{E}_V 2 \text{Tr} \left[\left(\mathbb{I} \otimes (M_V + M_V^\dagger) \right) \rho_t \right] \\
 & = \mathbb{E}_{i \leq t-1} \frac{8\varepsilon'}{d} \leq \frac{8\varepsilon^2}{d} \tag{8}
 \end{aligned}$$

because $\mathbb{E}_V M_V = \frac{2(1-\sqrt{1-\varepsilon^2})}{d} \mathbb{I} \preceq \frac{2\varepsilon^2}{d} \mathbb{I}$.

Concerning the expectation of the second term of (6), we apply again the Weingarten calculus

(Lem. 31) after denoting $C = A_t^\dagger B_{i_t}^t$:

$$\begin{aligned}
 \mathbb{E}_{V \sim \text{Haar}(d)} \frac{1}{2} \left(\frac{\text{Tr}(B_{i_t}^{t,\dagger} A_t M_V^\top) \text{Tr}(A_t^\dagger B_{i_t}^t \bar{M}_V)}{\langle \phi_{i_t}^t | \rho_t | \phi_{i_t}^t \rangle} \right)^2 &= \frac{1}{2} \frac{\mathbb{E}_{V \sim \text{Haar}(d)} \text{Tr}(B_{i_t}^{t,\dagger} A_t M_V^\top)^2 \text{Tr}(A_t^\dagger B_{i_t}^t \bar{M}_V)^2}{\langle \phi_{i_t}^t | \rho_t | \phi_{i_t}^t \rangle^2} \\
 &= \frac{1}{2} \sum_{x,y,z,t} \frac{\mathbb{E}_{V \sim \text{Haar}(d)} \text{Tr}(|t\rangle \langle x| C^\dagger V M^\top V^\dagger |x\rangle \langle z| C V M V^\dagger |z\rangle \langle y| C^\dagger V M^\top V^\dagger |y\rangle \langle t| C V M V^\dagger)}{\langle \phi_{i_t}^t | \rho_t | \phi_{i_t}^t \rangle^2} \\
 &= \frac{1}{2 \langle \phi_{i_t}^t | \rho_t | \phi_{i_t}^t \rangle^2} \sum_{x,y,z,t} \sum_{\alpha, \beta \in \mathfrak{S}_4} \text{Wg}(\alpha\beta) \text{Tr}_\beta(M^\top, M, M^\top, M) \text{Tr}_{\alpha\gamma}(|t\rangle \langle x| C^\dagger, |x\rangle \langle z| C, |z\rangle \langle y| C^\dagger, |y\rangle \langle t| C)
 \end{aligned}$$

We can remark that for all $\alpha \in \mathfrak{S}_4$ there is $\beta \in \mathfrak{S}_4$ such that :

$$\begin{aligned}
 \left| \sum_{x,y,z,t} \text{Tr}_\alpha(|t\rangle \langle x| C^\dagger, |x\rangle \langle z| C, |z\rangle \langle y| C^\dagger, |y\rangle \langle t| C) \right| &= \left| \text{Tr}_\beta(C^\dagger, C, C^\dagger, C) \right| \\
 &\leq \max\{\text{Tr}(C C^\dagger), |\text{Tr}(C)|^2\}^2
 \end{aligned}$$

where the last inequality is only non trivial for $\beta = (ijk)$. For instance if $\beta = (123)$ we have by the Cauchy Schwarz inequality:

$$\begin{aligned}
 \text{Tr}_\beta(C^\dagger, C, C^\dagger, C) &= \text{Tr}(C^\dagger C C^\dagger) \text{Tr}(C) \leq \sqrt{\text{Tr}(C C^\dagger C C^\dagger) \text{Tr}(C C^\dagger)} |\text{Tr}(C)| \\
 &\leq \text{Tr}(C C^\dagger)^{3/2} |\text{Tr}(C)| \\
 &\leq \max\{\text{Tr}(C C^\dagger), |\text{Tr}(C)|^2\}^{3/2} \max\{\text{Tr}(C C^\dagger), |\text{Tr}(C)|^2\}^{1/2} \\
 &= \max\{\text{Tr}(C C^\dagger), |\text{Tr}(C)|^2\}^2.
 \end{aligned}$$

Moreover, it is clear that when β is not a 4-cycle, we have $|\text{Tr}_\beta(M, M^\top, M, M^\top)| \leq \mathcal{O}(\varepsilon^4)$ since it can be written as a product of at least two elements each of them is $\mathcal{O}(\varepsilon^2)$. In the case β is a 4 cycle we have $\text{Tr}(M M^\top M M^\top) = \text{Tr}(M M M^\top M^\top) = \text{Tr}((M + M^\top)^2) = 2(2 - 2\sqrt{1 - \varepsilon^2})^2 \leq 8\varepsilon^4$. On the other hand, we know that for all $(\alpha, \beta) \in \mathfrak{S}_4^2$, $|\text{Wg}(\alpha\beta)| \leq \frac{2}{d^4}$ (Collins and Śniady, 2006) so

$$\begin{aligned}
 &\sum_{x,y,z,t} \sum_{\alpha, \beta \in \mathfrak{S}_4} \text{Wg}(\alpha\beta) \text{Tr}_\beta(M^\top, M, M^\top, M) \text{Tr}_{\alpha\gamma}(|t\rangle \langle x| C^\dagger, |x\rangle \langle z| C, |z\rangle \langle y| C^\dagger, |y\rangle \langle t| C) \\
 &\leq \mathcal{O} \left(\frac{\varepsilon^4}{d^4} \max\{\text{Tr}(C C^\dagger), |\text{Tr}(C)|^2\}^2 \right).
 \end{aligned}$$

Therefore we have:

$$\mathbb{E}_{V \sim \text{Haar}(d)} \frac{1}{2} \left(\frac{\text{Tr}(B_{i_t}^{t,\dagger} A_t M_V^\top) \text{Tr}(A_t^\dagger B_{i_t}^t \bar{M}_V)}{\langle \phi_{i_t}^t | \rho_t | \phi_{i_t}^t \rangle} \right)^2 \leq \mathcal{O} \left(\frac{\varepsilon^4 \max\{\text{Tr}(C C^\dagger), |\text{Tr}(C)|^2\}^2}{d^4 \langle \phi_{i_t}^t | \rho_t | \phi_{i_t}^t \rangle^2} \right).$$

Recall that $C = A_t^\dagger B_{i_t}^t$, now, if we take the expectation $\mathbb{E}_{i \leq t}$ under the event

$$\mathcal{G}^c(t, i \leq t) = \left\{ \langle \phi_{i_t}^t | \rho_t | \phi_{i_t}^t \rangle > \frac{\varepsilon^2}{d^2} \text{Tr}(A_t^\dagger B_{i_t}^t B_{i_t}^{t,\dagger} A_t) \right\} = \left\{ |\text{Tr}(C)|^2 > \frac{\varepsilon^2}{d^2} \text{Tr}(C C^\dagger) \right\},$$

we obtain:

$$\begin{aligned}
 & \mathbb{E}_{i_{\leq t}} \mathbb{E}_{V \sim \text{Haar}(d)} \mathbf{1}\{\mathcal{G}^c(t, i_{\leq t})\} \frac{1}{2} \left(\frac{\text{Tr}(B_{i_t}^{t,\dagger} A_t M_V^\top) \text{Tr}(A_t^\dagger B_{i_t}^t \bar{M}_V)}{\langle \phi_{i_t}^t | \rho_t | \phi_{i_t}^t \rangle} \right)^2 \\
 & \leq \mathbb{E}_{i_{\leq t}} \mathbf{1}\{\mathcal{G}^c(t, i_{\leq t})\} \mathcal{O} \left(\frac{\varepsilon^4 \max\{\text{Tr}(CC^\dagger), |\text{Tr}(C)|^2\}^2}{d^4 \langle \phi_{i_t}^t | \rho_t | \phi_{i_t}^t \rangle^2} \right) \\
 & \leq \mathbb{E}_{i_{\leq t}} \mathbf{1}\{\mathcal{G}^c(t, i_{\leq t})\} \mathcal{O} \left(\frac{\varepsilon^4 |\text{Tr}(C)|^4}{d^4 \langle \phi_{i_t}^t | \rho_t | \phi_{i_t}^t \rangle^2} + \frac{\varepsilon^4}{d^4 \langle \phi_{i_t}^t | \rho_t | \phi_{i_t}^t \rangle} \times \frac{\text{Tr}(CC^\dagger)^2}{\langle \phi_{i_t}^t | \rho_t | \phi_{i_t}^t \rangle} \right) \\
 & = \mathbb{E}_{i_{\leq t}} \mathbf{1}\{\mathcal{G}^c(t, i_{\leq t})\} \mathcal{O} \left(\frac{\varepsilon^4}{d^4} + \frac{\varepsilon^4}{d^4 \langle \phi_{i_t}^t | \rho_t | \phi_{i_t}^t \rangle} \times \frac{\text{Tr}(CC^\dagger)^2}{|\text{Tr}(C)|^2} \right) \\
 & \leq \mathbb{E}_{i_{\leq t}} \mathbf{1}\{\mathcal{G}^c(t, i_{\leq t})\} \mathcal{O} \left(\frac{\varepsilon^4}{d^4} + \frac{\varepsilon^4}{d^4 \langle \phi_{i_t}^t | \rho_t | \phi_{i_t}^t \rangle} \times \frac{d^2 \text{Tr}(CC^\dagger)}{\varepsilon^2} \right) \quad \left(\text{under } \mathcal{G}^c : |\text{Tr}(C)|^2 > \frac{\varepsilon^2}{d^2} \text{Tr}(CC^\dagger) \right) \\
 & \leq \mathbb{E}_{i_{\leq t-1}} \sum_{i_t} \lambda_{i_t}^t \langle \phi_{i_t}^t | \rho_t | \phi_{i_t}^t \rangle \mathcal{O} \left(\frac{\varepsilon^4}{d^4} + \frac{\varepsilon^2 \text{Tr}(A_t^\dagger B_{i_t}^t B_{i_t}^{t,\dagger} A_t)}{d^2 \langle \phi_{i_t}^t | \rho_t | \phi_{i_t}^t \rangle} \right) \\
 & \leq \mathbb{E}_{i_{\leq t-1}} \mathcal{O} \left(\frac{\varepsilon^4}{d^4} \right) + \mathcal{O} \left(\frac{\varepsilon^2 \sum_{i_t} \lambda_{i_t}^t \text{Tr}(A_t^\dagger B_{i_t}^t B_{i_t}^{t,\dagger} A_t)}{d^2} \right) \\
 & \leq \mathbb{E}_{i_{\leq t-1}} \mathcal{O} \left(\frac{\varepsilon^4}{d^4} \right) + \mathcal{O} \left(\frac{\varepsilon^2 \text{Tr}(A_t^\dagger d A_t)}{d^2} \right) = \mathbb{E}_{i_{\leq t-1}} \mathcal{O} \left(\frac{d \varepsilon^2}{d^2} \right) = \mathcal{O} \left(\frac{\varepsilon^2}{d} \right) \tag{9}
 \end{aligned}$$

where we use $\sum_{i_t} \lambda_{i_t}^t B_{i_t}^t B_{i_t}^{t,\dagger} = d \mathbb{I}$ and $\text{Tr}(A_t A_t^\dagger) = 1$. By adding up (7), (8) and (9), we obtain:

$$\begin{aligned}
 & \mathbb{E}_{i_{\leq t}} \mathbb{E}_{V \sim \text{Haar}(d)} \mathbf{1}\{\mathcal{G}^c(t, i_{\leq t})\} (-\log) \left(\frac{\langle \phi_{i_t}^t | \text{id} \otimes \mathcal{N}_V(\rho_t) | \phi_{i_t}^t \rangle}{\langle \phi_{i_t}^t | \rho_t | \phi_{i_t}^t \rangle} \right) \\
 & \leq \mathbb{E}_{i_{\leq t}} \mathbb{E}_{V \sim \text{Haar}(d)} \mathbf{1}\{\mathcal{G}^c(t, i_{\leq t})\} \left(\frac{\Re(\langle \phi_{i_t}^t | (\mathbb{I} \otimes M_V) \rho_t (\mathbb{I} \otimes S_V^\dagger) | \phi_{i_t}^t \rangle)}{\langle \phi_{i_t}^t | \rho_t | \phi_{i_t}^t \rangle} + \frac{1}{2} \frac{\langle \phi_{i_t}^t | (\mathbb{I} \otimes M_V) \rho_t (\mathbb{I} \otimes M_V^\dagger) | \phi_{i_t}^t \rangle^2}{\langle \phi_{i_t}^t | \rho_t | \phi_{i_t}^t \rangle^2} \right) \\
 & + \mathbb{E}_{i_{\leq t}} \mathbb{E}_{V \sim \text{Haar}(d)} \mathbf{1}\{\mathcal{G}^c(t, i_{\leq t})\} \left(2 \frac{\langle \phi_{i_t}^t | (\mathbb{I} \otimes M_V) \rho_t (\mathbb{I} \otimes M_V^\dagger) | \phi_{i_t}^t \rangle}{\langle \phi_{i_t}^t | \rho_t | \phi_{i_t}^t \rangle} \right) = \mathcal{O} \left(\frac{\varepsilon^2}{d} \right).
 \end{aligned}$$

Therefore using this upper bound and the upper bound (4) we get an upper bound on the expected KL divergence:

$$\begin{aligned}
 \mathbb{E}_{V \sim \text{Haar}(d)} \text{KL}(P \| Q_V) & = \sum_{t=1}^N \mathbb{E}_{i_{\leq t}} \mathbb{E}_{V \sim \text{Haar}(d)} (\mathbf{1}\{\mathcal{G}(t, i_{\leq t})\} + \mathbf{1}\{\mathcal{G}^c(t, i_{\leq t})\}) (-\log) \left(\frac{\langle \phi_{i_t}^t | \text{id} \otimes \mathcal{N}_V(\rho_t) | \phi_{i_t}^t \rangle}{\langle \phi_{i_t}^t | \rho_t | \phi_{i_t}^t \rangle} \right) \\
 & \leq \sum_{t=1}^N \mathcal{O} \left(\frac{\varepsilon^2}{d} \right) + \mathcal{O} \left(\frac{\varepsilon^2}{d} \right) = \mathcal{O} \left(\frac{N \varepsilon^2}{d} \right).
 \end{aligned}$$

Finally since $\mathbb{E}_{V \sim \text{Haar}(d)} \text{KL}(P \| Q_V) \geq \frac{\log(2)}{3}$ we conclude:

$$N = \Omega \left(\frac{d}{\varepsilon^2} \right).$$

■

Appendix C. Deferred proofs of the analysis of testing identity to the depolarizing channel Alg. 2

C.1. Proof of Lem. 3

Lemma 12 *Let \mathcal{N}_1 and \mathcal{N}_2 be two quantum channels and d_{in} (resp. d_{out}) be the dimension of their input (resp. output) states. We have:*

$$d_{\diamond}(\mathcal{N}_1, \mathcal{N}_2) \leq d_{\text{in}} \sqrt{d_{\text{out}}} \|\mathcal{J}_{\mathcal{N}_1} - \mathcal{J}_{\mathcal{N}_2}\|_2.$$

Proof Denote by $\mathcal{M} = \mathcal{N}_1 - \mathcal{N}_2$ and $\mathcal{J} = \mathcal{J}_{\mathcal{M}} = \mathcal{J}_{\mathcal{N}_1} - \mathcal{J}_{\mathcal{N}_2}$. Let $|\phi\rangle$ be a maximizing unit vector of the diamond norm, i.e., $\|\text{id} \otimes \mathcal{M}(|\phi\rangle\langle\phi|)\|_1 = d_{\diamond}(\mathcal{N}_1, \mathcal{N}_2)$. We can write $|\phi\rangle = A \otimes \mathbb{I} |\Psi\rangle$ where $|\Psi\rangle = \frac{1}{\sqrt{d_{\text{in}}}} \sum_{i=1}^{d_{\text{in}}} |i\rangle \otimes |i\rangle$ is the maximally entangled state. $|\phi\rangle$ has norm 1 so $\text{Tr}(A^\dagger A) = d_{\text{in}}$. We can write the diamond distance as follows:

$$\begin{aligned} d_{\diamond}(\mathcal{N}_1, \mathcal{N}_2) &= \|\text{id} \otimes \mathcal{M}(|\phi\rangle\langle\phi|)\|_1 = \|\text{id} \otimes \mathcal{M}(A \otimes \mathbb{I} |\Psi\rangle\langle\Psi| A^\dagger \otimes \mathbb{I})\|_1 \\ &= \|(A \otimes \mathbb{I}) \text{id} \otimes \mathcal{M}(|\Psi\rangle\langle\Psi|)(A^\dagger \otimes \mathbb{I})\|_1 = \|(A \otimes \mathbb{I}) \mathcal{J}_{\mathcal{M}}(A^\dagger \otimes \mathbb{I})\|_1. \end{aligned}$$

$\mathcal{J}_{\mathcal{M}}$ is Hermitian so can be written as : $\mathcal{J}_{\mathcal{M}} = \sum_i \lambda_i |\psi_i\rangle\langle\psi_i|$. Using the triangle inequality and the Cauchy Schwarz inequality, we obtain:

$$\begin{aligned} \|(A \otimes \mathbb{I}) \mathcal{J}_{\mathcal{M}}(A^\dagger \otimes \mathbb{I})\|_1 &= \left\| (A \otimes \mathbb{I}) \sum_i \lambda_i |\psi_i\rangle\langle\psi_i| (A^\dagger \otimes \mathbb{I}) \right\|_1 \\ &\leq \sum_i |\lambda_i| \|(A \otimes \mathbb{I}) |\psi_i\rangle\langle\psi_i| (A^\dagger \otimes \mathbb{I})\|_1 \leq \sqrt{\sum_i \lambda_i^2} \sqrt{\sum_i \langle\psi_i| (A^\dagger A \otimes \mathbb{I}) |\psi_i\rangle^2} \\ &\leq \|\mathcal{J}\|_2 \sqrt{\sum_i \langle\psi_i| (A^\dagger A A^\dagger A \otimes \mathbb{I}) |\psi_i\rangle} = \|\mathcal{J}_{\mathcal{M}}\|_2 \sqrt{\text{Tr}(A^\dagger A A^\dagger A \otimes \mathbb{I})} \\ &= \|\mathcal{J}_{\mathcal{M}}\|_2 \sqrt{d_{\text{out}} \text{Tr}(A^\dagger A A^\dagger A)} \leq \|\mathcal{J}_{\mathcal{M}}\|_2 \sqrt{d_{\text{out}} (\text{Tr}(A^\dagger A))^2} = d_{\text{in}} \sqrt{d_{\text{out}}} \|\mathcal{J}_{\mathcal{M}}\|_2. \end{aligned}$$

■

C.2. Proof of Lem. 2

Lemma 13 *Let $\mathcal{J} = \text{id} \otimes \mathcal{N}(|\Psi\rangle\langle\Psi|)$ be the Choi state corresponding to the channel \mathcal{N} .*

$$\mathbb{E} \left(\left\| \mathcal{N}(|\phi\rangle\langle\phi|) - \frac{\mathbb{I}}{d_{\text{out}}} \right\|_2^2 \right) = \frac{\left(\text{Tr} \left(\mathcal{N}(\mathbb{I}) - \frac{d_{\text{in}}}{d_{\text{out}}} \mathbb{I} \right)^2 + d_{\text{in}}^2 \left\| \mathcal{J} - \frac{\mathbb{I}}{d_{\text{in}} d_{\text{out}}} \right\|_2^2 \right)}{d_{\text{in}}(d_{\text{in}} + 1)} \geq \frac{d_{\text{in}}}{d_{\text{in}} + 1} \left\| \mathcal{J} - \frac{\mathbb{I}}{d_{\text{in}} d_{\text{out}}} \right\|_2^2.$$

Proof We write

$$\mathbb{E} \left(\left\| \mathcal{N}(|\phi\rangle\langle\phi|) - \frac{\mathbb{I}}{d_{\text{out}}} \right\|_2^2 \right) = \mathbb{E} (\text{Tr}(\mathcal{N}(|\phi\rangle\langle\phi|)^2)) - \frac{1}{d_{\text{out}}}.$$

then if we use the Kraus decomposition of the quantum channel $\mathcal{N}(\rho) = \sum_k A_k \rho A_k^\dagger$, we can compute the following expectation using Weingarten calculus (Lem. 31 and Lem. 33):

$$\begin{aligned} \mathbb{E} (\text{Tr}(\mathcal{N}(|\phi\rangle\langle\phi|)^2)) &= \mathbb{E} \left(\text{Tr} \left(\sum_k A_k |\phi\rangle\langle\phi| A_k^\dagger \right)^2 \right) = \sum_{k,l} \mathbb{E} \left(\text{Tr}(A_k |\phi\rangle\langle\phi| A_k^\dagger A_l |\phi\rangle\langle\phi| A_l^\dagger) \right) \\ &= \frac{1}{d_{\text{in}}(d_{\text{in}} + 1)} \left(\sum_{k,l} \text{Tr}(A_k^\dagger A_l A_l^\dagger A_k) + \sum_{k,l} |\text{Tr}(A_k A_l^\dagger)|^2 \right) \\ &= \frac{1}{d_{\text{in}}(d_{\text{in}} + 1)} \left(\text{Tr} \left(\sum_k A_k A_k^\dagger \right)^2 + \sum_{k,l} |\text{Tr}(A_k A_l^\dagger)|^2 \right) \\ &= \frac{1}{d_{\text{in}}(d_{\text{in}} + 1)} \left(\text{Tr}(\mathcal{N}(\mathbb{I})^2) + \sum_{k,l} |\text{Tr}(A_k A_l^\dagger)|^2 \right) \end{aligned}$$

Observe that $\text{Tr}(\mathcal{N}(\mathbb{I})^2) = \text{Tr} \left(\mathcal{N}(\mathbb{I}) - \frac{d_{\text{in}}}{d_{\text{out}}} \mathbb{I} \right)^2 + \frac{d_{\text{in}}^2}{d_{\text{out}}}$. Moreover,

$$\begin{aligned} \text{Tr}(\mathcal{J}^2) &= \text{Tr} \left(\frac{1}{d_{\text{in}}} \sum_{i,j} |i\rangle\langle j| \otimes \mathcal{N}(|i\rangle\langle j|) \right)^2 = \frac{1}{d_{\text{in}}^2} \sum_{i,j} \text{Tr}(\mathcal{N}(|i\rangle\langle j|) \mathcal{N}(|j\rangle\langle i|)) \\ &= \frac{1}{d_{\text{in}}^2} \sum_{i,j,k,l} \text{Tr}(A_k |i\rangle\langle j| A_k^\dagger A_l |j\rangle\langle i| A_l^\dagger) = \frac{1}{d_{\text{in}}^2} \sum_{k,l} |\text{Tr}(A_k^\dagger A_l)|^2 \end{aligned}$$

hence:

$$\begin{aligned} \mathbb{E} (\text{Tr}(\mathcal{N}(|\phi\rangle\langle\phi|)^2)) &= \mathbb{E} \left(\text{Tr} \left(\sum_k A_k |\phi\rangle\langle\phi| A_k^\dagger \right)^2 \right) \\ &= \frac{1}{d_{\text{in}}(d_{\text{in}} + 1)} \left(\text{Tr} \left(\mathcal{N}(\mathbb{I}) - \frac{d_{\text{in}}}{d_{\text{out}}} \mathbb{I} \right)^2 + \frac{d_{\text{in}}^2}{d_{\text{out}}} + d_{\text{in}}^2 \text{Tr}(\mathcal{J}^2) \right) \end{aligned}$$

Finally,

$$\begin{aligned}
 \mathbb{E} \left(\left\| \mathcal{N}(|\phi\rangle\langle\phi|) - \frac{\mathbb{I}}{d_{\text{out}}} \right\|_2^2 \right) &= \mathbb{E} \left(\text{Tr}(\mathcal{N}(|\phi\rangle\langle\phi|)^2) \right) - \frac{1}{d_{\text{out}}} \\
 &= \frac{1}{d_{\text{in}}(d_{\text{in}} + 1)} \left(\text{Tr} \left(\mathcal{N}(\mathbb{I}) - \frac{d_{\text{in}}}{d_{\text{out}}} \mathbb{I} \right)^2 + \frac{d_{\text{in}}^2}{d_{\text{out}}} + d_{\text{in}}^2 \text{Tr}(\mathcal{J}^2) \right) - \frac{1}{d_{\text{out}}} \\
 &= \frac{1}{d_{\text{in}}(d_{\text{in}} + 1)} \left(\text{Tr} \left(\mathcal{N}(\mathbb{I}) - \frac{d_{\text{in}}}{d_{\text{out}}} \mathbb{I} \right)^2 + d_{\text{in}}^2 \text{Tr}(\mathcal{J}^2) - \frac{d_{\text{in}}}{d_{\text{out}}} \right) \\
 &= \frac{1}{d_{\text{in}}(d_{\text{in}} + 1)} \left(\text{Tr} \left(\mathcal{N}(\mathbb{I}) - \frac{d_{\text{in}}}{d_{\text{out}}} \mathbb{I} \right)^2 + d_{\text{in}}^2 \left\| \mathcal{J} - \frac{\mathbb{I}}{d_{\text{in}}d_{\text{out}}} \right\|_2^2 \right).
 \end{aligned}$$

■

C.3. Proof of Thm 4

Theorem 14 *Let $|\phi\rangle$ be a Haar distributed vector in \mathbf{S}^d . Let $X = \left\| \mathcal{N}(|\phi\rangle\langle\phi|) - \frac{\mathbb{I}}{d_{\text{out}}} \right\|_2^2$. We have:*

$$\text{Var}(X) = \mathcal{O} \left(\mathbb{E}(X)^2 \right).$$

Proof Recall that $X = \left\| \mathcal{N}(|\phi\rangle\langle\phi|) - \frac{\mathbb{I}}{d_{\text{out}}} \right\|_2^2$. We can observe that:

$$\text{Var}(X) = \text{Var} \left(\text{Tr}(\mathcal{N}(|\phi\rangle\langle\phi|))^2 - \frac{1}{d_{\text{out}}} \right) = \text{Var} \left(\text{Tr}(\mathcal{N}(|\phi\rangle\langle\phi|))^2 \right).$$

We use the Kraus notation $\mathcal{N}(\rho) = \sum_k A_k \rho A_k^\dagger$ and $d = d_{\text{in}}$. By the Weingarten calculus (Lem. 31 and Lem. 33), we can compute the expectation:

$$\begin{aligned}
 \mathbb{E} \left(\left(\text{Tr}(\mathcal{N}(|\phi\rangle\langle\phi|))^2 \right)^2 \right) &= \mathbb{E} \left(\left(\text{Tr} \sum_{k,l} A_k |\phi\rangle\langle\phi| A_k^\dagger A_l |\phi\rangle\langle\phi| A_l^\dagger \right)^2 \right) \\
 &= \sum_{i,j} \sum_{k,l,k',l'} \mathbb{E} \left(\text{Tr} A_{l'}^\dagger |j\rangle \langle i| A_k |\phi\rangle\langle\phi| A_k^\dagger A_l |\phi\rangle\langle\phi| A_l^\dagger |i\rangle \langle j| A_{k'} |\phi\rangle\langle\phi| A_{k'}^\dagger A_{l'} |\phi\rangle\langle\phi| \right) \\
 &= \sum_{i,j} \sum_{k,l,k',l'} \frac{1}{d(d+1)(d+2)(d+3)} \sum_{\alpha \in \mathfrak{S}_4} \text{Tr}_\alpha(A_{l'}^\dagger |j\rangle \langle i| A_k, A_k^\dagger A_l, A_l^\dagger |i\rangle \langle j| A_{k'}, A_{k'}^\dagger A_{l'}) \\
 &= \frac{1}{d(d+1)(d+2)(d+3)} \sum_{\alpha \in \mathfrak{S}_4} \sum_{i,j,k,l,k',l'} \text{Tr}_\alpha(A_{l'}^\dagger |j\rangle \langle i| A_k, A_k^\dagger A_l, A_l^\dagger |i\rangle \langle j| A_{k'}, A_{k'}^\dagger A_{l'}) \\
 &= \frac{1}{d(d+1)(d+2)(d+3)} \sum_{\alpha \in \mathfrak{S}_4} F(\alpha)
 \end{aligned}$$

where for $\alpha \in \mathfrak{S}_4$ we adopt the notation $F(\alpha) = \sum_{i,j,k,l,k',l'} \text{Tr}_\alpha(A_{l'}^\dagger |j\rangle \langle i| A_k, A_k^\dagger A_l, A_l^\dagger |i\rangle \langle j| A_{k'}, A_{k'}^\dagger A_{l'})$ where $\text{Tr}_\alpha(M_1, \dots, M_n) =$

$\Pi_j \text{Tr}(\Pi_{i \in C_j} M_i)$ for $\alpha = \Pi_j C_j$ and C_j are cycles. It is thus necessary to control each of these 24 terms in order to upper bound the variance. Furthermore, we need to be careful so that our upper bounds on $\{F(\alpha)\}_{\alpha \in \mathfrak{S}_4}$ depend on the actual parameters of the testing problem. Recall that the expected value of X can be expressed as follows:

$$\mathbb{E}(X) = \frac{1}{d_{\text{in}}(d_{\text{in}} + 1)} \left(\text{Tr} \left(\mathcal{N}(\mathbb{I}) - \frac{d_{\text{in}}}{d_{\text{out}}} \mathbb{I} \right)^2 + d_{\text{in}}^2 \left\| \mathcal{J} - \frac{\mathbb{I}}{d_{\text{in}} d_{\text{out}}} \right\|_2^2 \right).$$

Let us define $\mathcal{M} = \mathcal{N} - \mathcal{D}$, $m = \|\mathcal{M}(\mathbb{I}_{d_{\text{in}}})\|_2 = \left\| \mathcal{N}(\mathbb{I}) - \frac{d_{\text{in}}}{d_{\text{out}}} \mathbb{I} \right\|_2$ and $\eta = d_{\text{in}} \left\| \mathcal{J} - \frac{\mathbb{I}}{d_{\text{in}} d_{\text{out}}} \right\|_2$.

We state a useful Lemma relating η , \mathcal{M} and the Kraus operators $\{A_k\}_k$:

Lemma 15 *Let $\eta = d_{\text{in}} \|\mathcal{J} - \mathbb{I}/(d_{\text{in}} d_{\text{out}})\|_2$ and $\mathcal{M} = \mathcal{N} - \mathcal{D}$, we have:*

- $\eta^2 = \sum_{k,l} |\text{Tr}(A_k^\dagger A_l)|^2 - \frac{d_{\text{in}}}{d_{\text{out}}}$,
- $\eta^2 = \sum_{x,y=1}^{d_{\text{in}}} \|\mathcal{M}(|x\rangle \langle y|)\|_2^2$.

Proof Recall that we use the Kraus representation of the channel $\mathcal{N}(\rho) = \sum_k A_k \rho A_k^\dagger$. We can express η^2 :

$$\begin{aligned} \eta^2 &= \left\| d_{\text{in}} \mathcal{J} - \frac{\mathbb{I}}{d_{\text{out}}} \right\|_2^2 = d_{\text{in}}^2 \text{Tr}(\mathcal{J}^2) - \frac{d_{\text{in}}}{d_{\text{out}}} = \text{Tr} \left(\sum_{i,j,k} |i\rangle \langle j| \otimes A_k |i\rangle \langle j| A_k^\dagger \right)^2 - \frac{d_{\text{in}}}{d_{\text{out}}} \\ &= \sum_{i,j,k,l} \text{Tr}(A_k |i\rangle \langle j| A_k^\dagger A_l |j\rangle \langle i| A_l^\dagger) - \frac{d_{\text{in}}}{d_{\text{out}}} = \sum_{k,l} |\text{Tr}(A_k^\dagger A_l)|^2 - \frac{d_{\text{in}}}{d_{\text{out}}}. \end{aligned}$$

We move to the second point, we have $\mathcal{J} - \mathbb{I}/(d_{\text{in}} d_{\text{out}}) = \mathcal{J}_{\mathcal{N}} - \mathcal{J}_{\mathcal{D}} = \mathcal{J}_{\mathcal{M}} = \text{id} \otimes \mathcal{M}(|\Psi\rangle \langle \Psi|)$ so

$$\begin{aligned} \eta^2 &= d_{\text{in}}^2 \text{Tr}(\text{id} \otimes \mathcal{M}(|\Psi\rangle \langle \Psi|))^2 = \text{Tr}(\text{id} \otimes \mathcal{M}(d_{\text{in}} |\Psi\rangle \langle \Psi|))^2 = \text{Tr} \left(\sum_{x,y} |x\rangle \langle y| \otimes \mathcal{M}(|x\rangle \langle y|) \right)^2 \\ &= \sum_{x,y} \text{Tr}(\mathcal{M}(|x\rangle \langle y|) \mathcal{M}(|y\rangle \langle x|)) = \sum_{x,y} \|\mathcal{M}(|x\rangle \langle y|)\|_2^2. \end{aligned}$$

■

On the other hand, when dealing with some $F(\alpha)$'s, we will need to have some properties of the matrix $\sum_k A_k \otimes \bar{A}_k$.

Lemma 16 *Let $M = \sum_k A_k \otimes \bar{A}_k$. Let $\{\lambda_i\}_i$ be the set of the eigenvalues of $M^\dagger M$ (in a decreasing order) corresponding to the eigenstates $\{|\phi_i\rangle\}_i$. We have:*

- $\sum_i \lambda_i = \frac{d_{\text{in}}}{d_{\text{out}}} + \eta^2$,
- $\lambda_1 \geq \frac{d_{\text{in}}}{d_{\text{out}}}$, $\sum_{i>1} \lambda_i \leq \eta^2$,
- $\frac{d_{\text{in}}^2}{d_{\text{out}}^2} (1 - |\langle \phi_1 | \Psi \rangle|^2) \leq \frac{2m^2 \eta^2}{d_{\text{in}}} + 2\eta^4$,

$$\bullet \langle \Psi | M M^\dagger | \Psi \rangle = \frac{d_{\text{in}}}{d_{\text{out}}}.$$

Proof We have $\sum_i \lambda_i = \text{Tr}(M^\dagger M) = \sum_{k,l} \text{Tr}(A_k^\dagger A_l) \text{Tr}(A_k^\top \bar{A}_l) = \sum_{k,l} |\text{Tr}(A_k^\dagger A_l)|^2 = \frac{d_{\text{in}}}{d_{\text{out}}} + \eta^2$ by Lem. 15. Recall the definition of the unnormalized maximally entangled state $\sqrt{d_{\text{in}}} |\Psi\rangle = \sum_i |i\rangle \otimes |i\rangle$, we can compute its image by the matrix $M^\dagger M$:

$$\begin{aligned} M^\dagger M(\sqrt{d_{\text{in}}} |\Psi\rangle) &= \sum_{i,k,l} A_k^\dagger A_l |i\rangle \otimes A_k^\top \bar{A}_l |i\rangle = \sum_{x,y,i,k,l} \langle x | A_k^\dagger A_l |i\rangle \langle y | A_k^\top \bar{A}_l |i\rangle |xy\rangle \\ &= \sum_{x,y,i,k,l} \langle x | A_k^\dagger A_l |i\rangle \langle i | A_l^\dagger A_k |y\rangle |xy\rangle = \sum_{x,y,k} \langle x | A_k^\dagger \mathcal{N}(\mathbb{I}) A_k |y\rangle |xy\rangle \end{aligned}$$

therefore

$$\langle \Psi | M^\dagger M | \Psi \rangle = \frac{1}{d_{\text{in}}} \sum_{i,k} \langle i | A_k^\dagger \mathcal{N}(\mathbb{I}) A_k |i\rangle = \frac{\text{Tr}(\mathcal{N}(\mathbb{I})^2)}{d_{\text{in}}} \geq \frac{d_{\text{in}}^2}{d_{\text{in}} d_{\text{out}}} = \frac{d_{\text{in}}}{d_{\text{out}}}$$

where we used the Cauchy-Schwarz inequality. This implies that the largest eigenvalue verifies $\lambda_1 \geq \frac{d_{\text{in}}}{d_{\text{out}}}$ thus $\sum_{i>1} \lambda_i = \frac{d_{\text{in}}}{d_{\text{out}}} + \eta^2 - \lambda_1 \leq \eta^2$.

We move to prove the third point. Recall the notation $\mathcal{M}(\rho) = (\mathcal{N} - \mathcal{D})(\rho) = \sum_k A_k \rho A_k^\dagger - \text{Tr}(\rho) \frac{\mathbb{I}}{d_{\text{out}}}$. We have on the one hand:

$$\begin{aligned} M^\dagger M(\sqrt{d_{\text{in}}} |\Psi\rangle) &= \sum_{x,y,k} \langle x | A_k^\dagger \mathcal{N}(\mathbb{I}) A_k |y\rangle |xy\rangle = \sum_{x,y} \text{Tr}(\mathcal{N}(\mathbb{I}) \mathcal{N}(|y\rangle \langle x|)) |xy\rangle \\ &= \sum_{x,y} \text{Tr}(\mathcal{N}(\mathbb{I}) \mathcal{M}(|y\rangle \langle x|)) |xy\rangle + \sum_{x,y} \text{Tr}(\mathcal{N}(\mathbb{I}) \mathcal{D}(|y\rangle \langle x|)) |xy\rangle \\ &= \sum_{x,y} \text{Tr}(\mathcal{M}(\mathbb{I}) \mathcal{M}(|y\rangle \langle x|)) |xy\rangle + \sum_x \frac{1}{d_{\text{out}}} \text{Tr}(\mathcal{N}(\mathbb{I}) \mathbb{I}) |xx\rangle \\ &= \sum_{x,y} \text{Tr}(\mathcal{M}(\mathbb{I}) \mathcal{M}(|y\rangle \langle x|)) |xy\rangle + \frac{d_{\text{in}}}{d_{\text{out}}} \sqrt{d_{\text{in}}} |\Psi\rangle. \end{aligned}$$

On the other hand, using the spectral decomposition of $M^\dagger M$, we can write:

$$\sum_{x,y} \text{Tr}(\mathcal{M}(\mathbb{I}) \mathcal{M}(|y\rangle \langle x|)) |xy\rangle + \frac{d_{\text{in}}}{d_{\text{out}}} \sqrt{d_{\text{in}}} |\Psi\rangle = M^\dagger M(\sqrt{d_{\text{in}}} |\Psi\rangle) = \sum_i \lambda_i \sqrt{d_{\text{in}}} \langle \phi_i | \Psi \rangle | \phi_i \rangle.$$

Therefore

$$\lambda_1 \langle \phi_1 | \Psi \rangle | \phi_1 \rangle - \frac{d_{\text{in}}}{d_{\text{out}}} \sqrt{d_{\text{in}}} |\Psi\rangle = \frac{1}{\sqrt{d_{\text{in}}}} \sum_{x,y} \text{Tr}(\mathcal{M}(\mathbb{I}) \mathcal{M}(|y\rangle \langle x|)) |xy\rangle - \sum_{i>1} \lambda_i \langle \phi_i | \Psi \rangle | \phi_i \rangle.$$

Taking the 2-norm squared on both sides, then applying the triangle inequality, the fact $(x + y)^2 \leq 2(x^2 + y^2)$ and the Cauchy-Schwarz inequality we obtain:

$$\begin{aligned}
 & \lambda_1^2 |\langle \phi_1 | \Psi \rangle|^2 + \frac{d_{\text{in}}^2}{d_{\text{out}}^2} - 2 \frac{d_{\text{in}}}{d_{\text{out}}} \lambda_1 |\langle \phi_1 | \Psi \rangle|^2 \\
 &= \left\| \frac{1}{\sqrt{d_{\text{in}}}} \sum_{x,y} \text{Tr}(\mathcal{M}(\mathbb{I}) \mathcal{M}(|y\rangle \langle x|)) |xy\rangle - \sum_{i>1} \lambda_i \langle \phi_i | \Psi \rangle |\phi_i\rangle \right\|_2^2 \\
 &\leq \left(\left\| \frac{1}{\sqrt{d_{\text{in}}}} \sum_{x,y} \text{Tr}(\mathcal{M}(\mathbb{I}) \mathcal{M}(|y\rangle \langle x|)) |xy\rangle \right\|_2 + \left\| \sum_{i>1} \lambda_i \langle \phi_i | \Psi \rangle |\phi_i\rangle \right\|_2 \right)^2 \\
 &\leq 2 \left\| \frac{1}{\sqrt{d_{\text{in}}}} \sum_{x,y} \text{Tr}(\mathcal{M}(\mathbb{I}) \mathcal{M}(|y\rangle \langle x|)) |xy\rangle \right\|_2^2 + 2 \left\| \sum_{i>1} \lambda_i \langle \phi_i | \Psi \rangle |\phi_i\rangle \right\|_2^2 \\
 &\leq \frac{2}{d_{\text{in}}} \sum_{x,y} |\text{Tr}(\mathcal{M}(\mathbb{I}) \mathcal{M}(|y\rangle \langle x|))|^2 + 2 \sum_{i>1} \lambda_i^2 \\
 &\leq \frac{2}{d_{\text{in}}} \sum_{x,y} \|\mathcal{M}(\mathbb{I})\|_2^2 \|\mathcal{M}(|y\rangle \langle x|)\|_2^2 + 2 \left(\sum_{i>1} \lambda_i \right)^2 \leq \frac{2m^2 \eta^2}{d_{\text{in}}} + 2\eta^4.
 \end{aligned}$$

Observe that the LHS can be lower bounded as follows:

$$\begin{aligned}
 \lambda_1^2 |\langle \phi_1 | \Psi \rangle|^2 + \frac{d_{\text{in}}^2}{d_{\text{out}}^2} - 2 \frac{d_{\text{in}}}{d_{\text{out}}} \lambda_1 |\langle \phi_1 | \Psi \rangle|^2 &= \left(\lambda_1 - \frac{d_{\text{in}}}{d_{\text{out}}} \right)^2 |\langle \phi_1 | \Psi \rangle|^2 + \frac{d_{\text{in}}^2}{d_{\text{out}}^2} - \frac{d_{\text{in}}^2}{d_{\text{out}}^2} |\langle \phi_1 | \Psi \rangle|^2 \\
 &\geq \frac{d_{\text{in}}^2}{d_{\text{out}}^2} (1 - |\langle \phi_1 | \Psi \rangle|^2).
 \end{aligned}$$

Finally, we deduce from the two previous inequalities:

$$\frac{d_{\text{in}}^2}{d_{\text{out}}^2} (1 - |\langle \phi_1 | \Psi \rangle|^2) \leq \frac{2m^2 \eta^2}{d_{\text{in}}} + 2\eta^4.$$

We move to the fourth point. We have:

$$\begin{aligned}
 MM^\dagger(\sqrt{d_{\text{in}}} |\Psi\rangle) &= \sum_{i,k,l} A_k A_l^\dagger |i\rangle \otimes \bar{A}_k A_l^\top |i\rangle = \sum_{x,y,i,k,l} \langle x | A_k A_l^\dagger |i\rangle \langle y | \bar{A}_k A_l^\top |i\rangle |xy\rangle \\
 &= \sum_{x,y,i,k,l} \langle x | A_k A_l^\dagger |i\rangle \langle i | A_l A_k^\dagger |y\rangle |xy\rangle = \sum_{x,y} \langle x | \mathcal{N}(\mathbb{I}) |y\rangle |xy\rangle \\
 &= \sum_{x,y} \langle x | \mathcal{M}(\mathbb{I}) |y\rangle |xy\rangle + \frac{d_{\text{in}}}{d_{\text{out}}} \sqrt{d_{\text{in}}} |\Psi\rangle.
 \end{aligned}$$

Hence:

$$\langle \Psi | MM^\dagger |\Psi\rangle = \frac{1}{d_{\text{in}}} \sum_x \langle x | \mathcal{M}(\mathbb{I}) |x\rangle + \frac{d_{\text{in}}}{d_{\text{out}}} \langle \Psi | \Psi \rangle = \frac{1}{d_{\text{in}}} \text{Tr}(\mathcal{M}(\mathbb{I})) + \frac{d_{\text{in}}}{d_{\text{out}}} = \frac{d_{\text{in}}}{d_{\text{out}}}.$$

■

The first and fourth points will be used in the proof of Lemma 21. The first three points imply that the matrix $M^\dagger M$ (when normalized) is close to the maximally entangled state in the 1-norm.

Lemma 17 *Let $M = \sum_k A_k \otimes \bar{A}_k$ and $|\Psi\rangle = \frac{1}{\sqrt{d_{\text{in}}}} \sum_{i=1}^{d_{\text{in}}} |i\rangle \otimes |i\rangle$. We have:*

$$\left\| M^\dagger M - \frac{d_{\text{in}}}{d_{\text{out}}} |\Psi\rangle\langle\Psi| \right\|_1 \leq 5\eta^2.$$

Proof Let $|\phi_1\rangle$ the eigenvector of $M^\dagger M$ corresponding to the largest eigenvalue. Using the Fuchs–van de Graaf inequality (Fuchs and Van De Graaf, 1999) and Lem. 16:

$$\| |\phi_1\rangle\langle\phi_1| - |\Psi\rangle\langle\Psi| \|_1 \leq 2\sqrt{1 - |\langle\phi_1|\Psi\rangle|^2} \leq 2\frac{d_{\text{out}}}{d_{\text{in}}} \sqrt{\frac{2m^2\eta^2}{d_{\text{in}}} + 2\eta^4} \leq 4\frac{d_{\text{out}}}{d_{\text{in}}}\eta^2$$

where we use the Cauchy Schwarz inequality and Lem. 15:

$$\begin{aligned} m^2 &= \text{Tr}(\mathcal{M}(\mathbb{I})^2) = \sum_{i,j} \text{Tr}(\mathcal{M}(|i\rangle\langle i|)\mathcal{M}(|j\rangle\langle j|)) \\ &\leq \sum_{i,j} \text{Tr}(\mathcal{M}(|i\rangle\langle i|)^2) = d_{\text{in}} \sum_i \text{Tr}(\mathcal{M}(|i\rangle\langle i|)^2) \leq d_{\text{in}}\eta^2. \end{aligned}$$

By the triangle inequality and Lem. 16 we deduce:

$$\begin{aligned} \left\| M^\dagger M - \frac{d_{\text{in}}}{d_{\text{out}}} |\Psi\rangle\langle\Psi| \right\|_1 &\leq \left\| M^\dagger M - \frac{d_{\text{in}}}{d_{\text{out}}} |\phi_1\rangle\langle\phi_1| \right\|_1 + \frac{d_{\text{in}}}{d_{\text{out}}} \| |\phi_1\rangle\langle\phi_1| - |\Psi\rangle\langle\Psi| \|_1 \\ &\leq \lambda_1 - \frac{d_{\text{in}}}{d_{\text{out}}} + \sum_{i>1} \lambda_i + 4\eta^2 = 5\eta^2. \end{aligned}$$

■

This Lemma will be used in the proofs of Lemmas 18, 20, 19 and 22. We move now to upper bound different values of the function F .

Lemma 18 *We can upper bound $F((142))$ and $F((243))$ as follows:*

$$F((142)) = F((243)) \leq \frac{d_{\text{in}}/d_{\text{out}} + \eta^2}{d_{\text{out}}} + \frac{\eta^2}{d_{\text{out}}} + 5\eta^4.$$

Proof Recall the notation $\mathcal{M}(\rho) = (\mathcal{N} - \mathcal{D})(\rho) = \sum_k A_k \rho A_k^\dagger - \text{Tr}(\rho) \frac{\mathbb{I}}{d_{\text{out}}}$. We will first write $F((142))$ as a sum of an ideal term reflecting the null hypothesis ($\mathcal{N} = \mathcal{D}$) and an error term reflecting the difference between \mathcal{N} and \mathcal{D} . The ideal term is computed exactly and depends on dimensions d_{in} and d_{out} . The error term can also be splitted to a simple error depending on η and d_{out} and a more involved term that depends on the Kraus operators $\{A_k\}_k$ and the difference of channels \mathcal{M} . To control this latter error, we first write it in a closed form in terms of \mathcal{M} , $M = \sum_k A_k \otimes A_k^\dagger$ and the flip operator \mathbb{F} . Then we can use the spectral decomposition of the matrix $M^\dagger M - \frac{d_{\text{in}}}{d_{\text{out}}} |\Psi\rangle\langle\Psi|$ in order to decompose this error term into a combination of negligible elements. The final step requires to control the ℓ_1 norm of the coefficients of this combination which is done using Lemma 17.

We have:

$$\begin{aligned}
 F((142)) &= \sum_{k,l,k',l'} \text{Tr}(A_k A_{k'}^\dagger A_{l'} A_k^\dagger A_l A_{l'}^\dagger A_{k'} A_l^\dagger) = \sum_{k,l} \text{Tr}(\mathcal{N}(A_l^\dagger A_k) \mathcal{N}(A_k^\dagger A_l)) \\
 &= \sum_{k,l} \text{Tr}(\mathcal{M}(A_l^\dagger A_k) \mathcal{N}(A_k^\dagger A_l)) + \text{Tr}(\mathcal{D}(A_l^\dagger A_k) \mathcal{N}(A_k^\dagger A_l)) \\
 &= \sum_{k,l} \text{Tr}(\mathcal{M}(A_l^\dagger A_k) \mathcal{M}(A_k^\dagger A_l)) + \text{Tr}(\mathcal{D}(A_l^\dagger A_k) \mathcal{N}(A_k^\dagger A_l)) + \text{Tr}(\mathcal{M}(A_l^\dagger A_k) \mathcal{D}(A_k^\dagger A_l)) \\
 &= \sum_{k,l} \text{Tr}(\mathcal{M}(A_l^\dagger A_k) \mathcal{M}(A_k^\dagger A_l)) + \frac{\text{Tr}(A_l^\dagger A_k)}{d_{\text{out}}} \text{Tr}(\mathcal{N}(A_k^\dagger A_l)) + \frac{\text{Tr}(A_k^\dagger A_l)}{d_{\text{out}}} \text{Tr}(\mathcal{M}(A_l^\dagger A_k)) \\
 &= \sum_{k,l} \text{Tr}(\mathcal{M}(A_l^\dagger A_k) \mathcal{M}(A_k^\dagger A_l)) + \frac{\text{Tr}(A_l^\dagger A_k)}{d_{\text{out}}} \text{Tr}(A_k^\dagger A_l) \\
 &= \sum_{k,l} \text{Tr}(\mathcal{M}(A_l^\dagger A_k) \mathcal{M}(A_k^\dagger A_l)) + \frac{\eta^2 + d_{\text{in}}/d_{\text{out}}}{d_{\text{out}}}.
 \end{aligned}$$

It remains to control the sum $\sum_{k,l} \text{Tr}(\mathcal{M}(A_l^\dagger A_k) \mathcal{M}(A_k^\dagger A_l))$. Let $T_2 : X \otimes Y \mapsto X \otimes Y^\top$ be the partial transpose operator and $M = \sum_l A_l \otimes \bar{A}_l$. Let $\mathbb{F} = \sum_{i,j=1}^d (|i\rangle \otimes |j\rangle)(\langle j| \otimes \langle i|)$ be the flip operator, we have $\text{Tr}(A \otimes B \mathbb{F}) = \sum_{i,j,k,l} A_{i,j} B_{k,l} \text{Tr}(|i\rangle \langle j| \otimes |k\rangle \langle l| \mathbb{F}) = \sum_{i,j,k,l} A_{i,j} B_{k,l} \text{Tr}(|i\rangle \langle l| \otimes |k\rangle \langle j|) = \sum_{i,j} A_{i,j} B_{j,i} = \text{Tr}(AB)$ which is known as the replica trick. We have using the replica trick:

$$\begin{aligned}
 \sum_{k,l} \text{Tr}(\mathcal{M}(A_l^\dagger A_k) \mathcal{M}(A_k^\dagger A_l)) &= \sum_{k,l} \text{Tr}(\mathcal{M}(A_l^\dagger A_k) \otimes \mathcal{M}(A_k^\dagger A_l) \mathbb{F}) \\
 &= \text{Tr} \left(\mathcal{M} \otimes \mathcal{M} \left(\sum_{k,l} A_l^\dagger A_k \otimes A_k^\dagger A_l \right) \mathbb{F} \right) \\
 &= \text{Tr} \left(\mathcal{M} \otimes \mathcal{M} \circ T_2 \left(\sum_{k,l} A_l^\dagger A_k \otimes A_l^\top \bar{A}_k \right) \mathbb{F} \right) \\
 &= \text{Tr} \left(\mathcal{M} \otimes \mathcal{M} \circ T_2(M^\dagger M) \mathbb{F} \right)
 \end{aligned}$$

Let $|\phi\rangle$ be a unit vector, we can write $|\phi\rangle = \sum_{x,y} \phi_{x,y} |x\rangle \otimes |y\rangle$ then we can express:

$$\begin{aligned}
 |\mathrm{Tr}(\mathcal{M} \otimes \mathcal{M} \circ \mathrm{T}_2(|\phi\rangle\langle\phi|)\mathbb{F})| &= \left| \sum_{x,y,z,t} \phi_{x,y} \bar{\phi}_{z,t} \mathrm{Tr}(\mathcal{M} \otimes \mathcal{M} \circ \mathrm{T}_2(|x\rangle\langle z| \otimes |y\rangle\langle t|)\mathbb{F}) \right| \\
 &= \left| \sum_{x,y,z,t} \phi_{x,y} \bar{\phi}_{z,t} \mathrm{Tr}(\mathcal{M} \otimes \mathcal{M}(|x\rangle\langle z| \otimes |t\rangle\langle y|)\mathbb{F}) \right| \\
 &= \left| \sum_{x,y,z,t} \phi_{x,y} \bar{\phi}_{z,t} \mathrm{Tr}(\mathcal{M}(|x\rangle\langle z|) \otimes \mathcal{M}(|t\rangle\langle y|)\mathbb{F}) \right| \\
 &= \left| \sum_{x,y,z,t} \phi_{x,y} \bar{\phi}_{z,t} \mathrm{Tr}(\mathcal{M}(|x\rangle\langle z|)\mathcal{M}(|t\rangle\langle y|)) \right| \\
 &\leq \sqrt{\sum_{x,y,z,t} |\phi_{x,y} \bar{\phi}_{z,t}|^2 \sum_{x,y,z,t} |\mathrm{Tr}(\mathcal{M}(|x\rangle\langle z|)\mathcal{M}(|t\rangle\langle y|))|^2} \\
 &= \sqrt{\sum_{x,y,z,t} \|\mathcal{M}(|x\rangle\langle z|)\|_2^2 \|\mathcal{M}(|t\rangle\langle y|)\|_2^2} = \eta^2
 \end{aligned}$$

where we use the Cauchy Schwarz inequality and Lem. 15. On the other hand, we can compute:

$$\begin{aligned}
 \mathrm{Tr}(\mathcal{M} \otimes \mathcal{M} \circ \mathrm{T}_2(|\Psi\rangle\langle\Psi|)\mathbb{F}) &= \frac{1}{d_{\mathrm{in}}} \sum_{i,j} \mathrm{Tr}(\mathcal{M} \otimes \mathcal{M} \circ \mathrm{T}_2(|ii\rangle\langle jj|)\mathbb{F}) \\
 &= \frac{1}{d_{\mathrm{in}}} \sum_{i,j} \mathrm{Tr}(\mathcal{M}(|i\rangle\langle j|)\mathcal{M}(|j\rangle\langle i|)) = \frac{\eta^2}{d_{\mathrm{in}}}.
 \end{aligned}$$

Then, we can decompose the Hermitian matrix $M^\dagger M - \frac{d_{\mathrm{in}}}{d_{\mathrm{out}}} |\Psi\rangle\langle\Psi| = \sum_i \mu_i |\psi_i\rangle\langle\psi_i|$. Hence Lem. 17 implies:

$$\begin{aligned}
 \sum_{k,l} \mathrm{Tr}(\mathcal{M}(A_l^\dagger A_k) \mathcal{M}(A_k^\dagger A_l)) &= \mathrm{Tr}(\mathcal{M} \otimes \mathcal{M} \circ \mathrm{T}_2(M^\dagger M)\mathbb{F}) \\
 &= \frac{d_{\mathrm{in}}}{d_{\mathrm{out}}} \mathrm{Tr}(\mathcal{M} \otimes \mathcal{M} \circ \mathrm{T}_2(|\Psi\rangle\langle\Psi|)\mathbb{F}) + \sum_i \mu_i \mathrm{Tr}(\mathcal{M} \otimes \mathcal{M} \circ \mathrm{T}_2(|\psi_i\rangle\langle\psi_i|)\mathbb{F}) \\
 &\leq \frac{\eta^2}{d_{\mathrm{out}}} + \sum_i |\mu_i| \eta^2 = \frac{\eta^2}{d_{\mathrm{out}}} + \mathrm{Tr} \left| M^\dagger M - \frac{d_{\mathrm{in}}}{d_{\mathrm{out}}} |\Psi\rangle\langle\Psi| \right| \eta^2 \leq \frac{\eta^2}{d_{\mathrm{out}}} + 5\eta^4.
 \end{aligned}$$

Finally,

$$F((142)) = \sum_{k,l} \mathrm{Tr}(\mathcal{M}(A_l^\dagger A_k) \mathcal{M}(A_k^\dagger A_l)) + \frac{d_{\mathrm{in}}}{d_{\mathrm{out}}} + \eta^2 \leq \frac{d_{\mathrm{in}}}{d_{\mathrm{out}}} + \frac{\eta^2}{d_{\mathrm{out}}} + \frac{\eta^2}{d_{\mathrm{out}}} + 5\eta^4.$$

■

Lemma 19 We can upper bound $F(\text{id})$, $F((132))$, $F((314))$ and $F((24)(13))$ as follows:

$$F(\text{id}) = F((132)) = F((314)) = F((24)(13)) \leq \frac{d_{\text{in}}/d_{\text{out}} + \eta^2}{d_{\text{out}}} + \frac{\eta^2}{d_{\text{out}}} + 5\eta^4.$$

Proof For the identity permutation, the function F can be expressed as follows:

$$\begin{aligned} F(\text{id}) &= \sum_{k,l,k',l'} \text{Tr}(A_k A_{l'}^\dagger A_{k'} A_l^\dagger) \text{Tr}(A_{k'}^\dagger A_{l'}) \text{Tr}(A_k^\dagger A_l) \\ &= \sum_{k,l,k',l'} \sum_{i,j} \text{Tr}(|j\rangle \langle i| A_{l'}^\dagger A_{k'} A_l^\dagger A_k |i\rangle \langle j| A_k^\dagger A_l) \text{Tr}(A_{k'}^\dagger A_{l'}) \\ &= \sum_{k',l'} \sum_{i,j} \text{Tr}(\mathcal{N}(|j\rangle \langle i| A_{l'}^\dagger A_{k'}) \mathcal{N}(|i\rangle \langle j|)) \text{Tr}(A_{k'}^\dagger A_{l'}) \\ &= \sum_{k',l'} \sum_{i,j} \text{Tr}(\mathcal{N}(|j\rangle \langle i| A_{l'}^\dagger A_{k'}) \mathcal{M}(|i\rangle \langle j|)) \text{Tr}(A_{k'}^\dagger A_{l'}) + \sum_{k',l'} \sum_{i,j} \text{Tr}(\mathcal{N}(|j\rangle \langle i| A_{l'}^\dagger A_{k'}) \mathcal{D}(|i\rangle \langle j|)) \text{Tr}(A_{k'}^\dagger A_{l'}) \\ &= \sum_{k',l'} \sum_{i,j} \text{Tr}(\mathcal{N}(|j\rangle \langle i| A_{l'}^\dagger A_{k'}) \mathcal{M}(|i\rangle \langle j|)) \text{Tr}(A_{k'}^\dagger A_{l'}) + \sum_{k',l'} \sum_i \frac{1}{d_{\text{out}}} \text{Tr}(\mathcal{N}(|i\rangle \langle i| A_{l'}^\dagger A_{k'})) \text{Tr}(A_{k'}^\dagger A_{l'}) \\ &= \sum_{k',l'} \sum_{i,j} \text{Tr}(\mathcal{N}(|j\rangle \langle i| A_{l'}^\dagger A_{k'}) \mathcal{M}(|i\rangle \langle j|)) \text{Tr}(A_{k'}^\dagger A_{l'}) + \sum_{k',l'} \frac{1}{d_{\text{out}}} \text{Tr}(A_{l'}^\dagger A_{k'}) \text{Tr}(A_{k'}^\dagger A_{l'}) \\ &= \sum_{k',l'} \sum_{i,j} \text{Tr}(\mathcal{M}(|j\rangle \langle i| A_{l'}^\dagger A_{k'}) \mathcal{M}(|i\rangle \langle j|)) \text{Tr}(A_{k'}^\dagger A_{l'}) + \frac{d_{\text{in}}/d_{\text{out}} + \eta^2}{d_{\text{out}}} \text{ (because } \mathcal{M} \text{ is a trace less channel)} \\ &= \sum_{i,j} \text{Tr}(\mathcal{M}(|j\rangle \langle i| N) \mathcal{M}(|i\rangle \langle j|)) + \frac{d_{\text{in}}/d_{\text{out}} + \eta^2}{d_{\text{out}}} \end{aligned}$$

where $N = \sum_{k,l} \text{Tr}(A_k^\dagger A_l) A_l^\dagger A_k$. Let us introduce $\tilde{N} = N - \frac{\mathbb{I}}{d_{\text{out}}} = \sum_i \mu_x |\psi_x\rangle \langle \psi_x|$ (this is possible because N is Hermitian) so that we can write using Lem. 15:

$$\begin{aligned} \sum_{i,j} \text{Tr}(\mathcal{M}(|j\rangle \langle i| N) \mathcal{M}(|i\rangle \langle j|)) &= \sum_{i,j} \text{Tr}(\mathcal{M}(|j\rangle \langle i| \tilde{N}) \mathcal{M}(|i\rangle \langle j|)) + \frac{1}{d_{\text{out}}} \sum_{i,j} \text{Tr}(\mathcal{M}(|j\rangle \langle i|) \mathcal{M}(|i\rangle \langle j|)) \\ &= \sum_{i,j,x} \mu_x \text{Tr}(\mathcal{M}(|j\rangle \langle i| |\psi_x\rangle \langle \psi_x|) \mathcal{M}(|i\rangle \langle j|)) + \frac{\eta^2}{d_{\text{out}}} \\ &= \sum_{i,j,x} \mu_x \langle i | \psi_x \rangle \text{Tr}(\mathcal{M}(|j\rangle \langle \psi_x|) \mathcal{M}(|i\rangle \langle j|)) + \frac{\eta^2}{d_{\text{out}}} \\ &= \sum_{i,j,x,k} \mu_x \text{Tr}(\langle i | \psi_x \rangle \mathcal{M}(|j\rangle \langle k|) \langle \psi_x | k \rangle \mathcal{M}(|i\rangle \langle j|)) + \frac{\eta^2}{d_{\text{out}}} \\ &\leq \frac{1}{2} \sum_{i,j,x,k} |\mu_x| (\| \langle i | \psi_x \rangle \mathcal{M}(|j\rangle \langle k|) \|_2^2 + \| \langle \psi_x | k \rangle \mathcal{M}(|i\rangle \langle j|) \|_2^2) + \frac{\eta^2}{d_{\text{out}}} \\ &= \text{Tr}|\tilde{N}| \eta^2 + \frac{\eta^2}{d_{\text{out}}}. \end{aligned}$$

We can see the matrix $N = \sum_{k,l} \text{Tr}(A_k^\dagger A_l) A_l^\dagger A_k$ as a partial trace of $M^\dagger M$:

$$\begin{aligned} \text{Tr}_2(M^\dagger M) &= \text{Tr}_2 \left(\sum_{k,l} A_l^\dagger A_k \otimes A_l^\top \bar{A}_k \right) = \sum_{k,l} \text{Tr}(A_l^\top \bar{A}_k) A_l^\dagger A_k \\ &= \sum_{k,l} \text{Tr}(A_l A_k^*) A_l^\dagger A_k = N. \end{aligned}$$

Moreover $\frac{\mathbb{I}}{d_{\text{in}}} = \text{Tr}_2(|\Psi\rangle\langle\Psi|)$ so by the data processing inequality (the partial trace is a valid quantum channel) and Lem. 17, we deduce:

$$\text{Tr}|\tilde{N}| = \left\| \text{Tr}_2(M^\dagger M) - \frac{d_{\text{in}}}{d_{\text{out}}} \text{Tr}_2(|\Psi\rangle\langle\Psi|) \right\|_1 \leq \left\| M^\dagger M - \frac{d_{\text{in}}}{d_{\text{out}}} |\Psi\rangle\langle\Psi| \right\|_1 \leq 5\eta^2.$$

Finally,

$$F(\text{id}) = \sum_{i,j} \text{Tr}(\mathcal{M}(|j\rangle\langle i|N)\mathcal{M}(|i\rangle\langle j|)) + \frac{d_{\text{in}}/d_{\text{out}} + \eta^2}{d_{\text{out}}} \leq \frac{d_{\text{in}}/d_{\text{out}} + \eta^2}{d_{\text{out}}} + \frac{\eta^2}{d_{\text{out}}} + 5\eta^4.$$

■

Lemma 20 *We can upper bound $F((24))$ and $F((1432))$ as follows:*

$$F((24)) = F((1432)) \leq \frac{d_{\text{in}}^2}{d_{\text{out}}^2} + \frac{2m^2}{d_{\text{out}}} + 25\eta^4.$$

Proof Recall that $\langle \Psi | M^\dagger M | \Psi \rangle = \frac{\text{Tr}(\mathcal{N}(\mathbb{I})^2)}{d_{\text{in}}} = \frac{d_{\text{in}}}{d_{\text{out}}} + \frac{m^2}{d_{\text{in}}}$. We use the fact that $\text{Tr}(X)\text{Tr}(Y) = \text{Tr}(X \otimes Y)$:

$$\begin{aligned}
 F((24)) &= \sum_{k,l,k',l'} \text{Tr}(A_k^\dagger A_l A_{k'}^\dagger A_{l'}) \text{Tr}(A_k A_{l'}^\dagger A_{k'} A_l^\dagger) \\
 &= \sum_{k,l,k',l'} \text{Tr}(A_k^\dagger A_l A_{k'}^\dagger A_{l'} \otimes A_l^\dagger A_k A_{l'}^\dagger A_{k'}) \\
 &= \text{Tr} \left(\sum_{k,l} A_k^\dagger A_l \otimes A_l^\dagger A_k \right) \left(\sum_{k,l} A_k^\dagger A_l \otimes A_l^\dagger A_k \right) \\
 &= \text{Tr} \left(\sum_{k,l} A_k^\dagger A_l \otimes A_k^\top \bar{A}_l \right)^{\text{T}_2} \left(\sum_{k,l} A_k^\dagger A_l \otimes A_k^\top \bar{A}_l \right)^{\text{T}_2} \\
 &= \text{Tr}(M^\dagger M)^{\text{T}_2} (M^\dagger M)^{\text{T}_2} = \text{Tr}(M^\dagger M)(M^\dagger M) \\
 &= \text{Tr} \left(M^\dagger M - \frac{d_{\text{in}}}{d_{\text{out}}} |\Psi\rangle\langle\Psi| \right) M^\dagger M + \frac{d_{\text{in}}}{d_{\text{out}}} \text{Tr}(|\Psi\rangle\langle\Psi| M^\dagger M) \\
 &= \text{Tr} \left(M^\dagger M - \frac{d_{\text{in}}}{d_{\text{out}}} |\Psi\rangle\langle\Psi| \right) \left(M^\dagger M - \frac{d_{\text{in}}}{d_{\text{out}}} |\Psi\rangle\langle\Psi| \right) \\
 &\quad + \frac{d_{\text{in}}}{d_{\text{out}}} \langle\Psi| \left(M^\dagger M - \frac{d_{\text{in}}}{d_{\text{out}}} |\Psi\rangle\langle\Psi| \right) |\Psi\rangle + \frac{d_{\text{in}}^2}{d_{\text{out}}^2} + \frac{m^2}{d_{\text{out}}} \\
 &\leq \left(\text{Tr} \left| M^\dagger M - \frac{d_{\text{in}}}{d_{\text{out}}} |\Psi\rangle\langle\Psi| \right| \right)^2 + \frac{d_{\text{in}}^2}{d_{\text{out}}^2} + \frac{2m^2}{d_{\text{out}}} \\
 &\leq \frac{d_{\text{in}}^2}{d_{\text{out}}^2} + \frac{2m^2}{d_{\text{out}}} + 25\eta^4
 \end{aligned}$$

where we have used the fact that $\text{Tr}(A^{\text{T}_2} B^{\text{T}_2}) = \text{Tr}(AB)$ and Lem. 17. ■

Lemma 21 *We can upper bound $F((12)(34))$, $F((14)(23))$, $F((234))$ and $F((124))$ as follows:*

$$F((12)(34)) = F((14)(23)) = F((234)) = F((124)) \leq \frac{d_{\text{in}}^3}{d_{\text{out}}^2} + 2\frac{d_{\text{in}}}{d_{\text{out}}} m^2 + \eta^2 m^2.$$

Proof Using the expression of $F(\alpha)$ for the permutation $\alpha = (12)(34)$ and the fact that $\sum_k A_k^\dagger A_k = \mathbb{I}$, we have:

$$\begin{aligned}
 F((12)(34)) &= \sum_{k,l,k',l'} \text{Tr}(A_k A_k^\dagger A_l A_l^\dagger A_{k'} A_{k'}^\dagger A_{l'} A_{l'}^\dagger) = \sum_{k,l} \text{Tr}(A_l^\dagger \mathcal{N}(\mathbb{I}) A_l A_k^\dagger \mathcal{N}(\mathbb{I}) A_k) \\
 &= \sum_{k,l} \text{Tr}(A_l^\dagger \mathcal{M}(\mathbb{I}) A_l A_k^\dagger \mathcal{N}(\mathbb{I}) A_k) + \frac{d_{\text{in}}}{d_{\text{out}}} \sum_{k,l} \text{Tr}(A_l^\dagger A_l A_k^\dagger \mathcal{N}(\mathbb{I}) A_k) \\
 &= \sum_{k,l} \text{Tr}(A_l^\dagger \mathcal{M}(\mathbb{I}) A_l A_k^\dagger \mathcal{M}(\mathbb{I}) A_k) + \frac{d_{\text{in}}}{d_{\text{out}}} \sum_{k,l} \text{Tr}(A_l^\dagger \mathcal{M}(\mathbb{I}) A_l A_k^\dagger A_k) + \frac{d_{\text{in}}}{d_{\text{out}}} \sum_k \text{Tr}(A_k^\dagger \mathcal{N}(\mathbb{I}) A_k) \\
 &= \sum_{k,l} \text{Tr}(A_l^\dagger \mathcal{M}(\mathbb{I}) A_l A_k^\dagger \mathcal{M}(\mathbb{I}) A_k) + \frac{d_{\text{in}}}{d_{\text{out}}} \text{Tr}(\mathcal{M}(\mathbb{I}) \mathcal{N}(\mathbb{I})) + \frac{d_{\text{in}}}{d_{\text{out}}} \text{Tr}(\mathcal{N}(\mathbb{I})^2) \\
 &= \sum_{k,l} \text{Tr}(A_l^\dagger \mathcal{M}(\mathbb{I}) A_l A_k^\dagger \mathcal{M}(\mathbb{I}) A_k) + \frac{d_{\text{in}}^3}{d_{\text{out}}^2} + 2 \frac{d_{\text{in}}}{d_{\text{out}}} \text{Tr}(\mathcal{M}(\mathbb{I})^2)
 \end{aligned}$$

Then, if we focus on the first term,

we can use the replica trick again to obtain:

$$\begin{aligned}
 \sum_{k,l} \text{Tr}(A_l^\dagger \mathcal{M}(\mathbb{I}) A_l A_k^\dagger \mathcal{M}(\mathbb{I}) A_k) &= \sum_{k,l} \text{Tr}(A_k A_l^\dagger \mathcal{M}(\mathbb{I}) \otimes A_l A_k^\dagger \mathcal{M}(\mathbb{I}) \mathbb{F}) \\
 &= \text{Tr} \left(\sum_{k,l} A_k A_l^\dagger \otimes A_l A_k^\dagger \cdot \mathcal{M}(\mathbb{I})^{\otimes 2} \mathbb{F} \right) = \text{Tr} \left(T_2 \left(\sum_{k,l} A_k A_l^\dagger \otimes \bar{A}_k A_l^\top \right) \cdot \mathcal{M}(\mathbb{I})^{\otimes 2} \mathbb{F} \right) \\
 &= \text{Tr} \left((MM^\dagger)^{T_2} \cdot \mathcal{M}(\mathbb{I})^{\otimes 2} \mathbb{F} \right) \\
 &= \text{Tr} \left(((\mathbb{I} - |\Psi\rangle\langle\Psi|) MM^\dagger (\mathbb{I} - |\Psi\rangle\langle\Psi|))^{T_2} \cdot \mathcal{M}(\mathbb{I})^{\otimes 2} \mathbb{F} \right) + \text{Tr} \left((MM^\dagger |\Psi\rangle\langle\Psi|)^{T_2} \cdot \mathcal{M}(\mathbb{I})^{\otimes 2} \mathbb{F} \right) \\
 &+ \text{Tr} \left((|\Psi\rangle\langle\Psi| MM^\dagger)^{T_2} \cdot \mathcal{M}(\mathbb{I})^{\otimes 2} \mathbb{F} \right) - \text{Tr} \left((|\Psi\rangle\langle\Psi| MM^\dagger |\Psi\rangle\langle\Psi|)^{T_2} \cdot \mathcal{M}(\mathbb{I})^{\otimes 2} \mathbb{F} \right).
 \end{aligned}$$

We can simplify the latter terms. First we have $|\Psi\rangle\langle\Psi|^{T_2} = \mathbb{F}$ and $\mathbb{F}^2 = \mathbb{I}$ so

$$\begin{aligned}
 \text{Tr} \left((|\Psi\rangle\langle\Psi| MM^\dagger |\Psi\rangle\langle\Psi|)^{T_2} \cdot \mathcal{M}(\mathbb{I})^{\otimes 2} \mathbb{F} \right) &= \langle\Psi| MM^\dagger |\Psi\rangle \text{Tr} \left((|\Psi\rangle\langle\Psi|)^{T_2} \cdot \mathcal{M}(\mathbb{I})^{\otimes 2} \mathbb{F} \right) \\
 &= \langle\Psi| MM^\dagger |\Psi\rangle \text{Tr} (\mathbb{F} \mathcal{M}(\mathbb{I})^{\otimes 2} \mathbb{F}) = \langle\Psi| MM^\dagger |\Psi\rangle \text{Tr} (\mathcal{M}(\mathbb{I})^{\otimes 2}) = \langle\Psi| MM^\dagger |\Psi\rangle \text{Tr} (\mathcal{M}(\mathbb{I}))^2 = 0.
 \end{aligned}$$

Next by Lem. 16 we have $MM^\dagger |\Psi\rangle = \frac{1}{\sqrt{d_{\text{in}}}} \sum_{x,y} \langle x | \mathcal{N}(\mathbb{I}) | y \rangle |xy\rangle$ so

$$\begin{aligned}
 \text{Tr} \left(\left(MM^\dagger |\Psi\rangle \langle \Psi| \right)^{T_2} \cdot \mathcal{M}(\mathbb{I})^{\otimes 2} \mathbb{F} \right) &= \frac{1}{d_{\text{in}}} \sum_{x,y,z} \langle x | \mathcal{N}(\mathbb{I}) | y \rangle \text{Tr} \left((|xy\rangle \langle zz|)^{T_2} \cdot \mathcal{M}(\mathbb{I})^{\otimes 2} \mathbb{F} \right) \\
 &= \frac{1}{d_{\text{in}}} \sum_{x,y,z} \langle x | \mathcal{N}(\mathbb{I}) | y \rangle \text{Tr} (|x\rangle \langle z| \otimes |z\rangle \langle y| \cdot \mathcal{M}(\mathbb{I})^{\otimes 2} \mathbb{F}) \\
 &= \frac{1}{d_{\text{in}}} \sum_{x,y,z} \langle x | \mathcal{N}(\mathbb{I}) | y \rangle \text{Tr} (|x\rangle \langle z| \mathcal{M}(\mathbb{I}) |z\rangle \langle y| \mathcal{M}(\mathbb{I})) \\
 &= \frac{1}{d_{\text{in}}} \sum_{x,y} \langle x | \mathcal{N}(\mathbb{I}) | y \rangle \text{Tr} (|x\rangle \text{Tr}(\mathcal{M}(\mathbb{I})) \langle y| \mathcal{M}(\mathbb{I})) = 0.
 \end{aligned}$$

Similarly we prove:

$$\begin{aligned}
 \text{Tr} \left(\left(|\Psi\rangle \langle \Psi| MM^\dagger \right)^{T_2} \cdot \mathcal{M}(\mathbb{I})^{\otimes 2} \mathbb{F} \right) &= \frac{1}{d_{\text{in}}} \sum_{x,y,z} \langle x | \mathcal{N}(\mathbb{I}) | y \rangle \text{Tr} \left((|zz\rangle \langle xy|)^{T_2} \cdot \mathcal{M}(\mathbb{I})^{\otimes 2} \mathbb{F} \right) \\
 &= \frac{1}{d_{\text{in}}} \sum_{x,y,z} \langle x | \mathcal{N}(\mathbb{I}) | y \rangle \text{Tr} (|z\rangle \langle x| \otimes |y\rangle \langle z| \cdot \mathcal{M}(\mathbb{I})^{\otimes 2} \mathbb{F}) \\
 &= \frac{1}{d_{\text{in}}} \sum_{x,y,z} \langle x | \mathcal{N}(\mathbb{I}) | y \rangle \text{Tr} (|z\rangle \langle x| \mathcal{M}(\mathbb{I}) |y\rangle \langle z| \mathcal{M}(\mathbb{I})) \\
 &= \frac{1}{d_{\text{in}}} \sum_{x,y} \langle x | \mathcal{N}(\mathbb{I}) | y \rangle \langle y | \mathcal{M}(\mathbb{I}) |x\rangle \text{Tr}(\mathcal{M}(\mathbb{I})) = 0.
 \end{aligned}$$

Now the matrix $(\mathbb{I} - |\Psi\rangle \langle \Psi|)MM^\dagger(\mathbb{I} - |\Psi\rangle \langle \Psi|)$ is Hermitian and positive semi-definite so can be written as $(\mathbb{I} - |\Psi\rangle \langle \Psi|)MM^\dagger(\mathbb{I} - |\Psi\rangle \langle \Psi|) = \sum_i \lambda_i |\phi_i\rangle \langle \phi_i|$, and for each i , we can write the

Schmidt's decomposition of $|\phi\rangle = \sum_{x,y} \phi_{x,y} |xy\rangle$. Therefore

$$\begin{aligned}
 & \sum_{k,l} \text{Tr}(A_l^\dagger \mathcal{M}(\mathbb{I}) A_l A_k^\dagger \mathcal{M}(\mathbb{I}) A_k) = \text{Tr} \left(\left((\mathbb{I} - |\Psi\rangle\langle\Psi|) M M^\dagger (\mathbb{I} - |\Psi\rangle\langle\Psi|) \right)^{T_2} \cdot \mathcal{M}(\mathbb{I})^{\otimes 2} \mathbb{F} \right) \\
 & = \sum_i \lambda_i \text{Tr} \left(T_2(|\phi_i\rangle\langle\phi_i|) \cdot \mathcal{M}(\mathbb{I})^{\otimes 2} \mathbb{F} \right) = \sum_i \sum_{x,y,z,t} \lambda_i \phi_{x,y} \bar{\phi}_{z,t} \text{Tr} \left(T_2(|xy\rangle\langle zt|) \cdot \mathcal{M}(\mathbb{I})^{\otimes 2} \mathbb{F} \right) \\
 & = \sum_i \sum_{x,y,z,t} \lambda_i \phi_{x,y} \bar{\phi}_{z,t} \text{Tr} \left(|x\rangle\langle z| \otimes |t\rangle\langle y| \cdot \mathcal{M}(\mathbb{I})^{\otimes 2} \mathbb{F} \right) \\
 & = \sum_i \sum_{x,y,z,t} \lambda_i \phi_{x,y} \bar{\phi}_{z,t} \text{Tr} \left(|x\rangle\langle z| \mathcal{M}(\mathbb{I}) \otimes |t\rangle\langle y| \mathcal{M}(\mathbb{I}) \mathbb{F} \right) \\
 & = \sum_i \sum_{x,y,z,t} \lambda_i \phi_{x,y} \bar{\phi}_{z,t} \text{Tr} \left(|x\rangle\langle z| \mathcal{M}(\mathbb{I}) |t\rangle\langle y| \mathcal{M}(\mathbb{I}) \right) \\
 & = \sum_i \sum_{x,y,z,t} \lambda_i \phi_{x,y} \bar{\phi}_{z,t} \langle z| \mathcal{M}(\mathbb{I}) |t\rangle\langle y| \mathcal{M}(\mathbb{I}) |x\rangle \\
 & \leq \sum_i \sum_{x,y,z,t} \lambda_i |\phi_{x,y}|^2 |\langle z| \mathcal{M}(\mathbb{I}) |t\rangle|^2 + \sum_i \sum_{x,y,z,t} \lambda_i |\phi_{z,t}|^2 |\langle y| \mathcal{M}(\mathbb{I}) |x\rangle|^2 \\
 & \leq \sum_i \sum_{x,y,z,t} \lambda_i |\phi_{x,y}|^2 |\langle z| \mathcal{M}(\mathbb{I}) |t\rangle|^2 + \sum_i \sum_{x,y,z,t} \lambda_i |\phi_{z,t}|^2 |\langle y| \mathcal{M}(\mathbb{I}) |x\rangle|^2 \\
 & = \text{Tr} \left| (\mathbb{I} - |\Psi\rangle\langle\Psi|) M M^\dagger (\mathbb{I} - |\Psi\rangle\langle\Psi|) \right| \text{Tr}(\mathcal{M}(\mathbb{I})^2)
 \end{aligned}$$

By Lem. 16 we have $\langle\Psi| M M^\dagger |\Psi\rangle = \frac{d_{\text{in}}}{d_{\text{out}}}$ and $\text{Tr}(M M^\dagger) = \frac{d_{\text{in}}}{d_{\text{out}}} + \eta^2$ so we have:

$$\text{Tr} \left| (\mathbb{I} - |\Psi\rangle\langle\Psi|) M M^\dagger (\mathbb{I} - |\Psi\rangle\langle\Psi|) \right| = \text{Tr}(\mathbb{I} - |\Psi\rangle\langle\Psi|) M M^\dagger (\mathbb{I} - |\Psi\rangle\langle\Psi|) = \eta^2.$$

Finally

$$F((12)(34)) \leq \frac{d_{\text{in}}^3}{d_{\text{out}}^2} + 2 \frac{d_{\text{in}}}{d_{\text{out}}} m^2 + \eta^2 m^2.$$

This concludes the proof for $F((12)(34))$. ■

Lemma 22 *We can upper bound $F((14))$, $F((12))$, $F((23))$ and $F((34))$ as follows:*

$$F((14)) = F((12)) = F((23)) = F((34)) \leq \frac{d_{\text{in}}^2}{d_{\text{out}}^2} + \frac{d_{\text{in}}}{d_{\text{out}}} \eta^2 + \frac{m^2}{d_{\text{out}}} + 5m\eta^3.$$

Proof Recall the notation $N = \sum_{k,l} \text{Tr}(A_k A_l^\dagger) A_k^\dagger A_l$. We can write the spectral decomposition of the Hermitian matrix:

$$N - \frac{\mathbb{I}}{d_{\text{out}}} = \text{Tr}_2 \left(\sum_{k,l} A_l^\dagger A_k \otimes A_l^\top \bar{A}_k - \frac{d_{\text{in}}}{d_{\text{out}}} |\Psi\rangle\langle\Psi| \right) = \sum_i \lambda_i |\phi_i\rangle\langle\phi_i|.$$

Then using the triangle inequality and the fact that $\sum_k A_k^\dagger A_k = \mathbb{I}$:

$$\begin{aligned}
 F(14) &= \sum_{k,l,k',l'} \text{Tr}(A_k^\dagger A_l) \text{Tr}(A_l^\dagger A_k A_{k'}^\dagger A_{l'} A_{l'}^\dagger A_{k'}) = \sum_{k'} \text{Tr}(N A_{k'}^\dagger \mathcal{N}(\mathbb{I}) A_{k'}) \\
 &= \sum_{k'} \text{Tr}(N A_{k'}^\dagger \mathcal{M}(\mathbb{I}) A_{k'}) + \frac{d_{\text{in}}}{d_{\text{out}}} \text{Tr}(N) = \text{Tr}(\mathcal{N}(N) \mathcal{M}(\mathbb{I})) + \frac{d_{\text{in}}}{d_{\text{out}}} \text{Tr}(N) \\
 &= \text{Tr}(\mathcal{M}(N) \mathcal{M}(\mathbb{I})) + \frac{d_{\text{in}}}{d_{\text{out}}} \text{Tr}(N) = \text{Tr} \left(\mathcal{M} \left(N - \frac{\mathbb{I}}{d_{\text{out}}} \right) \mathcal{M}(\mathbb{I}) \right) + \frac{\text{Tr}(\mathcal{M}(\mathbb{I})^2)}{d_{\text{out}}} + \frac{d_{\text{in}}}{d_{\text{out}}} \text{Tr}(N) \\
 &= \frac{d_{\text{in}}}{d_{\text{out}}} \left(\frac{d_{\text{in}}}{d_{\text{out}}} + \eta^2 \right) + \frac{\text{Tr}(\mathcal{M}(\mathbb{I})^2)}{d_{\text{out}}} + \sum_i \lambda_i \text{Tr}(\mathcal{M}(|\phi_i\rangle\langle\phi_i|) \mathcal{M}(\mathbb{I})) \\
 &\leq \frac{d_{\text{in}}}{d_{\text{out}}} \left(\frac{d_{\text{in}}}{d_{\text{out}}} + \eta^2 \right) + \frac{\text{Tr}(\mathcal{M}(\mathbb{I})^2)}{d_{\text{out}}} + \sum_i |\lambda_i| \|\mathcal{M}(|\phi_i\rangle\langle\phi_i|)\|_2 \|\mathcal{M}(\mathbb{I})\|_2 \\
 &\leq \frac{d_{\text{in}}}{d_{\text{out}}} \left(\frac{d_{\text{in}}}{d_{\text{out}}} + \eta^2 \right) + \frac{m^2}{d_{\text{out}}} + m\eta \sum_i |\lambda_i| = \frac{d_{\text{in}}}{d_{\text{out}}} \left(\frac{d_{\text{in}}}{d_{\text{out}}} + \eta^2 \right) + \frac{m^2}{d_{\text{out}}} + m\eta \cdot \text{Tr} \left| N - \frac{\mathbb{I}}{d_{\text{out}}} \right|
 \end{aligned}$$

because for all unit vector $|\phi\rangle = \sum_i \phi_i |i\rangle$ we have using the Cauchy Schwarz inequality, the AM-GM inequality, and Lem. 15:

$$\begin{aligned}
 \|\mathcal{M}(|\phi\rangle\langle\phi|)\|_2^2 &= \sum_{i,j,k,l} \phi_i \bar{\phi}_j \phi_k \bar{\phi}_l \text{Tr}(\mathcal{M}(|i\rangle\langle j|) \mathcal{M}(|k\rangle\langle l|)) \leq \sum_{i,j,k,l} |\phi_i \bar{\phi}_j \phi_k \bar{\phi}_l| \|\mathcal{M}(|i\rangle\langle j|)\|_2 \|\mathcal{M}(|k\rangle\langle l|)\|_2 \\
 &\leq \frac{1}{2} \sum_{i,j,k,l} |\phi_i|^2 |\phi_j|^2 \|\mathcal{M}(|k\rangle\langle l|)\|_2^2 + \frac{1}{2} \sum_{i,j,k,l} |\phi_k|^2 |\phi_l|^2 \|\mathcal{M}(|i\rangle\langle j|)\|_2^2 = \eta^2.
 \end{aligned}$$

Moreover, using the data processing inequality and Lem. 17 :

$$\begin{aligned}
 \text{Tr} \left| N - \frac{\mathbb{I}}{d_{\text{out}}} \right| &= \text{Tr} \left| \text{Tr}_2 \left(\sum_{k,l} A_l^\dagger A_k \otimes A_l^\top \bar{A}_k - \frac{d_{\text{in}}}{d_{\text{out}}} |\Psi\rangle\langle\Psi| \right) \right| \\
 &\leq \text{Tr} \left| \sum_{k,l} A_l^\dagger A_k \otimes A_l^\top \bar{A}_k - \frac{d_{\text{in}}}{d_{\text{out}}} |\Psi\rangle\langle\Psi| \right| = \text{Tr} \left| M^\dagger M - \frac{d_{\text{in}}}{d_{\text{out}}} |\Psi\rangle\langle\Psi| \right| \leq 5\eta^2.
 \end{aligned}$$

This concludes the proof. ■

For the remaining permutations, we can obtain a closed form for the function F . For the transposition (13), the image of the function F can be expressed as follows:

$$\begin{aligned}
 F((13)) &= \sum_{i,j,k,l,k',l'} \text{Tr}(A_{l'}^\dagger |j\rangle\langle i| A_k A_l^\dagger |i\rangle\langle j| A_{k'}) \text{Tr}(A_k^\dagger A_l) \text{Tr}(A_{k'}^\dagger A_{l'}) \\
 &= \sum_{k,l,k',l'} \text{Tr}(A_{k'}^\dagger A_{l'}) \text{Tr}(A_k A_l^\dagger) \text{Tr}(A_k^\dagger A_l) \text{Tr}(A_{k'}^\dagger A_{l'}) \\
 &= \left(\sum_{k,l} |\text{Tr}(A_k A_l^\dagger)|^2 \right)^2 = \left(\frac{d_{\text{in}}}{d_{\text{out}}} + \eta^2 \right)^2.
 \end{aligned}$$

Then, we remark that the permutations (312) and (134) have the same image:

$$\begin{aligned}
 F((312)) &= F((134)) = \sum_{i,j,k,l,k',l'} \text{Tr}(A_l^\dagger |i\rangle \langle j| A_{k'} A_{l'}^\dagger |j\rangle \langle i| A_k A_k^\dagger A_l) \text{Tr}(A_{k'}^\dagger A_{l'}) \\
 &= \sum_{k,l,k',l'} \text{Tr}(A_{k'} A_{l'}^\dagger) \text{Tr}(A_k A_k^\dagger A_l A_l^\dagger) \text{Tr}(A_{k'}^\dagger A_{l'}) \\
 &= \sum_{k,l} \text{Tr}(A_k A_k^\dagger A_l A_l^\dagger) \sum_{k,l} |\text{Tr}(A_k A_l^\dagger)|^2 \\
 &= \text{Tr}(\mathcal{N}(\mathbb{I})^2) \left(\frac{d_{\text{in}}}{d_{\text{out}}} + \eta^2 \right) = \left(\frac{d_{\text{in}}^2}{d_{\text{out}}} + m^2 \right) \left(\frac{d_{\text{in}}}{d_{\text{out}}} + \eta^2 \right).
 \end{aligned}$$

Next, the image of the cycle (1234) has also a closed expression:

$$\begin{aligned}
 F((1234)) &= \sum_{i,j,k,l,k',l'} \text{Tr}(A_{l'}^\dagger |j\rangle \langle i| A_k A_k^\dagger A_l A_l^\dagger |i\rangle \langle j| A_{k'} A_{l'}^\dagger A_{l'}) \\
 &= \sum_{k,l,k',l'} \text{Tr}(A_k A_k^\dagger A_l A_l^\dagger) \text{Tr}(A_{k'} A_{l'}^\dagger A_{l'} A_{k'}^\dagger) \\
 &= (\text{Tr}(\mathcal{N}(\mathbb{I})^2))^2 = \left(\frac{d_{\text{in}}^2}{d_{\text{out}}} + m^2 \right)^2.
 \end{aligned}$$

To sum up, we have proved so far that:

Lemma 23 *Let $m = \|\mathcal{M}(\mathbb{I})\|_2 = \|\mathcal{N}(\mathbb{I}) - \mathcal{D}(\mathbb{I})\|_2$ and $\eta = d_{\text{in}} \left\| \mathcal{J} - \frac{\mathbb{I}}{d_{\text{in}} d_{\text{out}}} \right\|_2$. We have:*

Permutation α	Upper bound on $F(\alpha)$	Reference
(13)	$\left(\frac{d_{\text{in}}}{d_{\text{out}}} + \eta^2 \right)^2$	
id, (132), (314), (24)(13)	$\frac{d_{\text{in}}/d_{\text{out}} + \eta^2}{d_{\text{out}}} + \frac{\eta^2}{d_{\text{out}}} + 5\eta^4$	(Lem. 19)
(312), (134)	$\left(\frac{d_{\text{in}}^2}{d_{\text{out}}} + m^2 \right) \left(\frac{d_{\text{in}}}{d_{\text{out}}} + \eta^2 \right)$	
(1234)	$\left(\frac{d_{\text{in}}^2}{d_{\text{out}}} + m^2 \right)^2$	
(24), (1432)	$\frac{d_{\text{in}}^2}{d_{\text{out}}} + \frac{2m^2}{d_{\text{out}}} + 25\eta^4$	(Lem. 20)
(142), (243)	$\frac{d_{\text{in}}/d_{\text{out}} + \eta^2}{d_{\text{out}}} + \frac{\eta^2}{d_{\text{out}}} + 5\eta^4$	(Lem. 18)
(14), (12), (23), (34), (1324), (1423), (1243), (1342)	$\frac{d_{\text{in}}^2}{d_{\text{out}}} + \frac{d_{\text{in}}}{d_{\text{out}}} \eta^2 + \frac{m^2}{d_{\text{out}}} + 5m\eta^3$	(Lem. 22)
(12)(34), (14)(23), (234), (124)	$\frac{d_{\text{in}}^3}{d_{\text{out}}} + 2 \frac{d_{\text{in}}}{d_{\text{out}}} m^2 + m^2 \eta^2$	(Lem. 21)

Therefore we have the following upper bound on the second moment using the inequality $m^2 \leq d\eta^2$:

$$\begin{aligned} \mathbb{E} \left(\left(\text{Tr}(\mathcal{N}(|\phi\rangle\langle\phi|)^2) \right)^2 \right) &= \frac{1}{d_{\text{in}}(d_{\text{in}}+1)(d_{\text{in}}+2)(d_{\text{in}}+3)} \sum_{\alpha \in \mathfrak{S}_4} F(\alpha) \\ &\leq \frac{d_{\text{out}}^4 + 6d_{\text{in}}^3 + 2d_{\text{in}}^2 d_{\text{out}} m^2 + 2d_{\text{in}}^2 d_{\text{out}} \eta^2 + 11d_{\text{in}}^2 + 10d_{\text{in}} d_{\text{out}} m^2 + 10d_{\text{in}} d_{\text{out}} \eta^2}{d_{\text{out}}^2 d_{\text{in}} (d_{\text{in}}+1)(d_{\text{in}}+2)(d_{\text{in}}+3)} \\ &\quad + \frac{6d_{\text{in}} + d_{\text{out}}^2 m^4 + 2d_{\text{out}}^2 \eta^2 + 12d_{\text{out}} m^2 + 40d_{\text{out}}^2 m \eta^3 + 81d_{\text{out}}^2 \eta^4 + 12d_{\text{out}} \eta^2}{d_{\text{out}}^2 d_{\text{in}} (d_{\text{in}}+1)(d_{\text{in}}+2)(d_{\text{in}}+3)} \end{aligned}$$

Recall that for the random variable $X = \text{Tr} \left(\mathcal{N}(|\phi\rangle\langle\phi|) - \frac{\mathbb{I}}{d_{\text{out}}} \right)^2 = \text{Tr}(\mathcal{N}(|\phi\rangle\langle\phi|)^2) - \frac{1}{d_{\text{out}}}$ we have:

$$\mathbb{E}(X) = \frac{\left(\text{Tr} \left(\mathcal{N}(\mathbb{I}) - \frac{d_{\text{in}}}{d_{\text{out}}} \mathbb{I} \right)^2 + d_{\text{in}}^2 \left\| \mathcal{J} - \frac{\mathbb{I}}{d_{\text{in}} d_{\text{out}}} \right\|_2^2 \right)}{d_{\text{in}}(d_{\text{in}}+1)} = \frac{1}{d_{\text{in}}(d_{\text{in}}+1)} (\text{Tr}(\mathcal{M}(\mathbb{I})^2) + \eta^2) = \frac{m^2 + \eta^2}{d_{\text{in}}(d_{\text{in}}+1)}.$$

Since $\text{Var}(X) = \text{Var} \left(X + \frac{1}{d_{\text{out}}} \right)$, it can be upper bounded as follows:

$$\begin{aligned} \text{Var}(X) &= \mathbb{E} \left(\left(\text{Tr}(\mathcal{N}(|\phi\rangle\langle\phi|)^2) \right)^2 \right) - \left(\mathbb{E} \left(\text{Tr}(\mathcal{N}(|\phi\rangle\langle\phi|)^2) \right) \right)^2 \\ &\leq \frac{d_{\text{out}}^4 + 6d_{\text{in}}^3 + 2d_{\text{in}}^2 d_{\text{out}} m^2 + 2d_{\text{in}}^2 d_{\text{out}} \eta^2 + 11d_{\text{in}}^2 + 10d_{\text{in}} d_{\text{out}} m^2 + 10d_{\text{in}} d_{\text{out}} \eta^2}{d_{\text{out}}^2 d_{\text{in}} (d_{\text{in}}+1)(d_{\text{in}}+2)(d_{\text{in}}+3)} \\ &\quad + \frac{6d_{\text{in}} + d_{\text{out}}^2 m^4 + 2d_{\text{out}}^2 \eta^2 + 12d_{\text{out}} m^2 + 40d_{\text{out}}^2 m \eta^3 + 81d_{\text{out}}^2 \eta^4 + 12d_{\text{out}} \eta^2}{d_{\text{out}}^2 d_{\text{in}} (d_{\text{in}}+1)(d_{\text{in}}+2)(d_{\text{in}}+3)} - \left(\frac{m^2 + \eta^2}{d_{\text{in}}(d_{\text{in}}+1)} + \frac{1}{d_{\text{out}}} \right)^2 \\ &\leq \left(\frac{80d_{\text{in}}^2 \eta^4 + 10d_{\text{in}}^2 m^2 \eta^2 + 40d_{\text{in}}^2 \eta^3 m}{d_{\text{in}}^2 (d_{\text{in}}+1)^2 (d_{\text{in}}+2)(d_{\text{in}}+3)} \right). \end{aligned}$$

Therefore the upper bound on the variance becomes using the inequalities $(m^2 + \eta^2)^2 \geq 4m^2 \eta^2$ and $(m^2 + \eta^2)^2 \geq 2m\eta^3$ (successive AM-GM):

$$\begin{aligned} \frac{\text{Var}(X)}{\mathbb{E}(X)^2} &\leq \left(\frac{80d_{\text{in}}^2 \eta^4 + 10d_{\text{in}}^2 m^2 \eta^2 + 40d_{\text{in}}^2 \eta^3 m}{(d_{\text{in}}+2)(d_{\text{in}}+3)(\eta^2 + m^2)^2} \right) \\ &\leq 80 \frac{d_{\text{in}}^2 \eta^4}{d_{\text{in}}^2 \eta^4} + 10 \frac{d_{\text{in}}^2 m^2 \eta^2}{4d_{\text{in}}^2 m^2 \eta^2} + 40 \frac{d_{\text{in}}^2 \eta^3 m}{2d_{\text{in}}^2 m \eta^3} \leq 105. \end{aligned}$$

■

Theorem 24 *There is an incoherent ancilla-free algorithm using a number of measurements satisfying*

$$N = \mathcal{O} \left(\frac{d_{\text{in}}^2 d_{\text{out}}^{1.5}}{\varepsilon^2} \right)$$

to distinguish between $\mathcal{N} = \mathcal{D}$ or $d_{\diamond}(\mathcal{N}, \mathcal{D}) > \varepsilon$ with a probability of success at least $2/3$.

Proof Complexity. We start by showing that Alg. 2 uses $\mathcal{O}(d_{\text{in}}^2 d_{\text{out}}^{1.5}/\varepsilon^2)$ measurements. Note that Alg. 3 requires $\mathcal{O}(\sqrt{d_{\text{out}}}\log(3M)/\eta^2)$ to test whether a d_{out} -dimensional quantum state ρ satisfies $\rho = \frac{\mathbb{I}}{d_{\text{out}}}$ or $\left\|\rho - \frac{\mathbb{I}}{d_{\text{out}}}\right\|_2 \geq \eta$ with an error probability $1/(3M)$. We apply this test for the state $\mathcal{N}(|\phi\rangle\langle\phi|)$, which is a d_{out} -dimensional quantum state, and $\eta = \frac{\varepsilon}{2\sqrt{d_{\text{out}}d_{\text{in}}}}$. So the testing identity of states algorithm will use a number of measurements $\mathcal{O}(d_{\text{in}}^2 d_{\text{out}}^{1.5}\log(3M)/\varepsilon^2)$. Since we repeat this test a number of $M = \mathcal{O}(1)$ times, the total number of measurements is $\mathcal{O}(d_{\text{in}}^2 d_{\text{out}}^{1.5}/\varepsilon^2)$.

Correctness. It remains to show that Alg. 2 is 1/3-correct. For this, we need to control two error probabilities. The first one, under the null hypothesis H_0 , the channel $\mathcal{N} = \mathcal{D}$ so for all $k \in [M]$, $\mathcal{N}(|\phi_k\rangle\langle\phi_k|) = \frac{\mathbb{I}}{d_{\text{out}}}$. Hence, for all the quantum states test we are under the null hypothesis h_0 . Therefore

$$\begin{aligned} \mathbb{P}_{H_0}(\text{error}) &= \mathbb{P}_{H_0}(\exists k \in [M] : i_k = 1) \\ &\leq \sum_{k=1}^M \mathbb{P}_{h_0}(i_k = 1) \leq \sum_{k=1}^M \frac{1}{3M} = \frac{1}{3}. \end{aligned}$$

The second error probability concerns the alternate hypothesis H_1 . In this case, the channel \mathcal{N} is ε -far from the depolarizing channel \mathcal{D} . For a given $k \in [M]$, let us lower bound the probability of being under h_1 at step k of the algorithm. Let $X_k = \left\|\mathcal{N}(|\phi_k\rangle\langle\phi_k|) - \frac{\mathbb{I}}{d_{\text{out}}}\right\|_2^2$. Recall that Thm. 4 says:

$$\text{Var}(X_k) \leq 105\mathbb{E}(X_k)^2$$

Therefore, the Paley-Zygmund inequality implies

$$\mathbb{P}\left(X_k \geq \frac{1}{2}\mathbb{E}(X_k)\right) \geq 1 - \frac{1}{\frac{1}{4}\frac{\mathbb{E}(X_k)^2}{\text{Var}(X_k)} + 1} \geq 1 - \frac{1}{\frac{1}{8 \times 105} + 1} \geq 10^{-3}.$$

Recall also that $\mathbb{E}(X_k) = \mathbb{E}\left(\left\|\mathcal{N}(|\phi_k\rangle\langle\phi_k|) - \frac{\mathbb{I}}{d}\right\|_2^2\right) \geq \frac{\varepsilon^2}{2d_{\text{in}}^2 d_{\text{out}}}$ (Ineq. 1). Therefore, with a probability at least 10^{-3} , we have $\left\|\mathcal{N}(|\phi_k\rangle\langle\phi_k|) - \frac{\mathbb{I}}{d_{\text{out}}}\right\|_2 \geq \frac{\varepsilon}{2d_{\text{in}}\sqrt{d_{\text{out}}}}$ which means we are under the alternate hypothesis h_1 . Denote the good event of $E_k = \left\{\left\|\mathcal{N}(|\phi_k\rangle\langle\phi_k|) - \frac{\mathbb{I}}{d_{\text{out}}}\right\|_2 \geq \frac{\varepsilon}{2d_{\text{in}}\sqrt{d_{\text{out}}}}\right\}$,

the probability of error under H_1 can be controlled as follows:

$$\begin{aligned}
 \mathbb{P}_{H_1}(\text{error}) &= \mathbb{P}_{H_1}(\forall k \in [M] : i_k = 0) = \prod_{k=1}^M \mathbb{P}_{H_1}(i_k = 0) \\
 &\leq \prod_{k=1}^M (\mathbb{P}_{H_1}(i_k = 0|E_k)\mathbb{P}(E_k) + \mathbb{P}_{H_1}(i_k = 0|\bar{E}_k)\mathbb{P}(\bar{E}_k)) \\
 &\leq \prod_{k=1}^M (\mathbb{P}_{h_1}(i_k = 0)\mathbb{P}(E_k) + \mathbb{P}(\bar{E}_k)) \\
 &\leq \prod_{k=1}^M (\mathbb{P}_{H_1}(i_k = 0|E_k)\mathbb{P}(E_k) + 1 - \mathbb{P}(E_k)) \\
 &= \prod_{k=1}^M (1 - \mathbb{P}(E_k) \mathbb{P}_{h_1}(i_k = 1|E_k)) \\
 &\leq \left(1 - 10^{-3} \cdot \left(1 - \frac{1}{3M}\right)\right)^M \leq \left(1 - \frac{10^{-3}}{2}\right)^M \leq \frac{1}{3}
 \end{aligned}$$

for $M = 2200 = \mathcal{O}(1)$. This concludes the correctness of Alg. 2. \blacksquare

Appendix D. Lower bounds for testing identity to the depolarizing channel

D.1. Proof of Thm. 6

Theorem 25 *Let $\varepsilon \leq 1/32$, $d_{\text{in}} \geq 80$ and $d_{\text{out}} \geq 10$.² Any incoherent ancilla-assisted non-adaptive algorithm for testing identity to the depolarizing channel (in both the trace and diamond distances) requires, in the worst case, a number of measurements*

$$N = \Omega\left(\frac{d_{\text{in}}^2 d_{\text{out}}^{1.5}}{\log(d_{\text{in}} d_{\text{out}}/\varepsilon)^2 \varepsilon^2}\right).$$

Proof Construction. Under the null hypothesis H_0 the quantum channel is $\mathcal{N}(\rho) = \mathcal{D}(\rho) = \text{Tr}(\rho)\frac{\mathbb{I}}{d_{\text{out}}}$. Under the alternate hypothesis H_1 , we choose the quantum channel $\mathcal{N} \sim \mathcal{P}$ of the form:

$$\mathcal{N}(\rho) = \text{Tr}(\rho)\frac{\mathbb{I}}{d_{\text{out}}} + \frac{\varepsilon}{d_{\text{out}}} \langle \bar{w} | \rho | \bar{w} \rangle U$$

where $|w\rangle = W|0\rangle$, $W \sim \text{Haar}(d_{\text{in}})$, and U satisfies

$$\begin{cases} U_{x,x} = 0 & \text{for all } x \in [d_{\text{out}}], \\ U_{y,x} = \bar{U}_{x,y} \sim \mathcal{N}_c(0, \sigma^2) = \mathcal{N}(0, \sigma^2/2) + i\mathcal{N}(0, \sigma^2/2) & \text{for all } x < y \in [d_{\text{out}}], \end{cases}$$

where the parameter σ would be chosen later and we condition on the event

$$\mathcal{G} = \{\|U\|_1 \geq d_{\text{out}}, \|U\|_\infty \leq 32\}.$$

². We didn't try to optimize these conditions.

We call this distribution \mathcal{P} and use the notation $(w, U) \sim \mathcal{P}$. If we don't condition on the event \mathcal{G} , the distribution of U is denoted \mathcal{P}_0 and we write $U \sim \mathcal{P}_0$. Random constructions with Gaussian random variables were used for proving lower bounds by [Chen et al. \(2022d,e\)](#). Note that \mathcal{N} is trace preserving since $\text{Tr}(U) = 0$. In order to prove that \mathcal{N} is a quantum channel, it remains to show that \mathcal{N} is completely positive which is equivalent to show that the corresponding Choi matrix is positive semi-definite. For this we can express the Choi state of the channel \mathcal{N} :

$$\begin{aligned} \mathcal{J}_{\mathcal{N}} &= \frac{\mathbb{I}}{d_{\text{in}}d_{\text{out}}} + \frac{\varepsilon}{d_{\text{in}}d_{\text{out}}} \sum_{i,j=1}^{d_{\text{in}}} |i\rangle\langle j| \otimes \langle 0| W^\top |i\rangle\langle j| \bar{W} |0\rangle U \\ &= \frac{\mathbb{I}}{d_{\text{in}}d_{\text{out}}} + \frac{\varepsilon}{d_{\text{in}}d_{\text{out}}} \sum_{i,j} |i\rangle\langle j| \otimes \langle i| W |0\rangle \langle 0| W^\dagger |j\rangle U \\ &= \frac{\mathbb{I}}{d_{\text{in}}d_{\text{out}}} + \frac{\varepsilon}{d_{\text{in}}d_{\text{out}}} W |0\rangle \langle 0| W^\dagger \otimes U \\ &= \frac{\mathbb{I}}{D} + \frac{\varepsilon}{D} |w\rangle\langle w| \otimes U \end{aligned}$$

where $D = d_{\text{in}}d_{\text{out}}$.

Observe that $\| |w\rangle\langle w| \otimes U \|_\infty = \|U\|_\infty \leq 32$ thus $\mathcal{J}_{\mathcal{N}} \geq 0$ if $\varepsilon \leq 1/32$. So under the event \mathcal{G} , the map \mathcal{N} is a quantum channel. The parameter σ should be chosen so that $d_\diamond(\mathcal{N}, \mathcal{D}) \geq \varepsilon$. Recall that $|w\rangle = W |0\rangle$, the definition of the diamond distance implies

$$\begin{aligned} d_\diamond(\mathcal{N}, \mathcal{D}) &\geq d_{\text{Tr}}(\mathcal{N}, \mathcal{D}) = \max_{\rho} \|(\mathcal{N} - \mathcal{D})(\rho)\|_1 \\ &\geq \|(\mathcal{N} - \mathcal{D})(|w\rangle\langle w|)\|_1 = \frac{\varepsilon}{d_{\text{out}}} \|U\|_1 \geq \varepsilon \end{aligned}$$

where we use the fact that under the event \mathcal{G} we have $\|U\|_1 \geq d_{\text{out}}$. Note that the lower bound we prove in this theorem holds for the stronger condition given by the trace distance.

Now we move to show that the event \mathcal{G} occurs with high probability.

Lemma 26 *There is a constant $c > 0$ such that we have:*

$$\mathbb{P}(\|U\|_1 - \mathbb{E}(\|U\|_1) > s) \leq \exp\left(-\frac{cs^2}{d_{\text{out}}\sigma^2}\right)$$

Proof The function $U \mapsto \|U\|_1$ is $\sqrt{d_{\text{out}}}$ -Lipschitz w.r.t. the Hilbert-Schmidt norm. Indeed, by the triangle inequality and the Cauchy Schwarz inequality $|\|U\|_1 - \|V\|_1| \leq \|U - V\|_1 \leq \sqrt{d_{\text{out}}}\|U - V\|_2$. The concentration of Lipschitz functions of Gaussian random variables ([Wainwright, 2019](#), Theorem 2.26) yields exactly the desired statement. \blacksquare

Next, we need a lower bound on the expectation of $\|U\|_1$. By the Hölder's inequality:

$$\mathbb{E}(\|U\|_1) \geq \sqrt{\frac{\mathbb{E}(\|U\|_2^2)^3}{\mathbb{E}(\|U\|_4^4)}} \geq \sqrt{\frac{(d_{\text{out}}^2\sigma^2)^3}{4d_{\text{out}}^3\sigma^4}} = \frac{d_{\text{out}}\sqrt{d_{\text{out}}}\sigma}{2}.$$

It is sufficient to choose $\sigma = \frac{4}{\sqrt{d_{\text{out}}}}$ so that $\mathbb{E}(\|U\|_1) \geq 2d_{\text{out}}$ and by [Lem. 26](#), we have $\|U\|_1 \geq d_{\text{out}}$ with a probability $1 - \exp(-\Omega(d_{\text{out}}^2))$. It remains to see that, for this choice of $\sigma = \frac{4}{\sqrt{d_{\text{out}}}}$, the event

$\{\|U\|_\infty \leq 32\}$ also occurs with high probability. Indeed, let \mathcal{S} be a $1/4$ -net of $\mathbf{S}^{d_{\text{out}}}$ of size at most $8^{d_{\text{out}}}$. By the union bound:

$$\begin{aligned} \mathbb{P}(\|U\|_\infty > 32) &= \mathbb{P}\left(\exists \phi \in \mathbf{S}^{d_{\text{out}}} : \langle \phi | U | \phi \rangle = \|U\|_\infty, \|U\|_\infty > 32\right) \\ &\leq \mathbb{P}\left(\exists \phi \in \mathcal{S} : \langle \phi | U | \phi \rangle > \frac{1}{2}\|U\|_\infty, \|U\|_\infty > 32\right) \\ &\leq |\mathcal{S}| \mathbb{P}(\langle \phi | U | \phi \rangle > 16) \leq 8^{d_{\text{out}}} e^{-8d_{\text{out}}} \leq e^{-4d_{\text{out}}}. \end{aligned}$$

Finally, with a probability at least $1 - \exp(-\Omega(d_{\text{out}}^2)) - \exp(-\Omega(d_{\text{out}}))$ the event \mathcal{G} is satisfied and we have a quantum channel \mathcal{N} that is ε -far in the diamond distance from the depolarizing channel \mathcal{D} . A $1/3$ -correct algorithm \mathcal{A} should distinguish between the channels \mathcal{N} and \mathcal{D} with a probability of error at most $1/3$. Let N be a sufficient number of measurements for this task and I_1, \dots, I_N be the observations of the algorithm \mathcal{A} . The Data-Processing inequality applied on the TV-distance gives LeCam's method (LeCam, 1973):

$$\begin{aligned} \text{TV}\left(\mathbb{P}_{H_0}^{I_1, \dots, I_N} \parallel \mathbb{P}_{H_1}^{I_1, \dots, I_N}\right) &\geq \text{TV}\left(\text{Bern}(\mathbb{P}_{H_0}(\mathcal{A} = 1)) \parallel \text{Bern}(\mathbb{P}_{H_1}(\mathcal{A} = 1))\right) \\ &\geq \text{TV}\left(\text{Bern}(1/3) \parallel \text{Bern}(2/3)\right) = \frac{1}{3}. \end{aligned}$$

Now, we need to upper bound this TV distance with an expression involving N , d_{in} , d_{out} and ε .

Upper bound on the TV distance. The non-adaptive algorithm \mathcal{A} would choose at step t the input ρ_t and the measurement device $\mathcal{M}_t = \{\lambda_{i_t}^t | \phi_{i_t}^t \rangle \langle \phi_{i_t}^t | \}_{i_t \in \mathcal{I}_t}$. Observe that we can always reduce w.l.o.g. to such a POVM. Under the null hypothesis H_0 , the quantum channel $\mathcal{N} = \mathcal{D}$ so the probability distribution of the outcomes is exactly:

$$\mathbb{P}_{H_0}^{I_1, \dots, I_N} = \left\{ \prod_{t=1}^N \lambda_{i_t}^t \langle \phi_{i_t}^t | \text{id} \otimes \mathcal{D}(\rho_t) | \phi_{i_t}^t \rangle \right\}_{i_1, \dots, i_N}.$$

On the other hand, under the alternate hypothesis H_1 , the probability of the outcomes is exactly:

$$\mathbb{P}_{H_1}^{I_1, \dots, I_N} = \left\{ \prod_{t=1}^N \lambda_{i_t}^t \langle \phi_{i_t}^t | \text{id} \otimes \mathcal{N}(\rho_t) | \phi_{i_t}^t \rangle \right\}_{i_1, \dots, i_N}$$

Recall that $D = d_{\text{in}} d_{\text{out}}$ and

$$\mathcal{J}_{\mathcal{D}} = \frac{\mathbb{I}}{D} \quad \text{and} \quad \mathcal{J}_{\mathcal{N}} = \frac{\mathbb{I}}{D} + \frac{\varepsilon}{D} |w\rangle \langle w| \otimes U.$$

We can suppose w.l.o.g. that each input state is pure because of the convexity of the TV distance. That is, for $t \in [N]$, we write $\rho_t = |\psi_t\rangle \langle \psi_t|$. Moreover, we can write each rank one input state and measurement vector as follows:

$$|\psi_t\rangle = A_t \otimes \mathbb{I} |\Psi_{d_{\text{in}}}\rangle \quad \text{and} \quad |\phi_{i_t}^t\rangle = B_{i_t}^t \otimes \mathbb{I} |\Psi_{d_{\text{out}}}\rangle$$

where $|\Psi_d\rangle = \frac{1}{\sqrt{d}} \sum_{i=1}^d |ii\rangle$ and the matrices $A_t \in \mathbb{C}^{d_{\text{anc}} \times d_{\text{in}}}$ and $B_{i_t}^t \in \mathbb{C}^{d_{\text{anc}} \times d_{\text{out}}}$ verify:

$$\text{Tr}(A_t A_t^\dagger) = d_{\text{in}} \quad \text{and} \quad \text{Tr}(B_{i_t}^t B_{i_t}^{t,\dagger}) = d_{\text{out}}.$$

Note that we have for all t , for all $X \in \mathbb{C}^{d_{\text{anc}} \otimes d_{\text{anc}}}$ we have $\sum_{i_t} \lambda_{i_t}^t B_{i_t}^{t,\dagger} X B_{i_t}^t = d_{\text{out}} \text{Tr}(X) \mathbb{I}_{d_{\text{out}}}$.
Indeed, the condition of the POVM \mathcal{M}_t implies:

$$X \otimes \mathbb{I} = X \otimes \mathbb{I} \sum_{i_t} \lambda_{i_t}^t |\phi_{i_t}^t\rangle \langle \phi_{i_t}^t| = \sum_{i_t} \lambda_{i_t}^t X B_{i_t}^t \otimes \mathbb{I} |\Psi_{d_{\text{out}}}\rangle \langle \Psi_{d_{\text{out}}}| B_{i_t}^{t,\dagger} \otimes \mathbb{I}$$

hence by taking the partial trace

$$\text{Tr}(X) \mathbb{I} = \frac{1}{d_{\text{out}}} \sum_{i_t, i, j} \lambda_{i_t}^t \langle j | B_{i_t}^{t,\dagger} X B_{i_t}^t | i \rangle | i \rangle \langle j |.$$

Finally

$$\sum_{i_t} \lambda_{i_t}^t B_{i_t}^{t,\dagger} X B_{i_t}^t = d_{\text{out}} \text{Tr}(X) \mathbb{I}_{d_{\text{out}}}.$$

By taking $X = \mathbb{I}$ and the partial trace on the second system we have

$$\sum_{i_t} \lambda_{i_t}^t B_{i_t}^t B_{i_t}^{t,\dagger} = d_{\text{out}}^2 \mathbb{I}_{d_{\text{anc}}}.$$

Now we can re-write the distribution of the observations under the null hypothesis as follows:

$$\begin{aligned} \mathbb{P}_{H_0}^{I_1, \dots, I_N} &= \left\{ \prod_{t=1}^N \lambda_{i_t}^t \langle \phi_{i_t}^t | \text{id} \otimes \mathcal{D}(\rho_t) | \phi_{i_t}^t \rangle \right\}_{i_1, \dots, i_N} \\ &= \left\{ \prod_{t=1}^N \lambda_{i_t}^t \langle \Psi_{d_{\text{out}}} | (B_{i_t}^{t,\dagger} A_t \otimes \mathbb{I}) \mathcal{J}_{\mathcal{D}}(A_t^\dagger B_{i_t}^t \otimes \mathbb{I}) | \Psi_{d_{\text{out}}} \rangle \right\}_{i_1, \dots, i_N} \\ &= \left\{ \prod_{t=1}^N \frac{\lambda_{i_t}^t}{D} \langle \Psi_{d_{\text{out}}} | (B_{i_t}^{t,\dagger} A_t A_t^\dagger B_{i_t}^t \otimes \mathbb{I}) | \Psi_{d_{\text{out}}} \rangle \right\}_{i_1, \dots, i_N} \\ &= \left\{ \prod_{t=1}^N \frac{\lambda_{i_t}^t}{D d_{\text{out}}} \text{Tr}(B_{i_t}^{t,\dagger} A_t A_t^\dagger B_{i_t}^t) \right\}_{i_1, \dots, i_N}, \end{aligned}$$

and under the alternate hypothesis as follows:

$$\begin{aligned} \mathbb{P}_{H_1}^{I_1, \dots, I_N} &= \left\{ \prod_{t=1}^N \lambda_{i_t}^t \langle \phi_{i_t}^t | \text{id} \otimes \mathcal{N}(\rho_t) | \phi_{i_t}^t \rangle \right\}_{i_1, \dots, i_N} \\ &= \left\{ \prod_{t=1}^N \lambda_{i_t}^t \langle \Psi_{d_{\text{out}}} | (B_{i_t}^{t,\dagger} A_t \otimes \mathbb{I}) \mathcal{J}_{\mathcal{N}}(A_t^\dagger B_{i_t}^t \otimes \mathbb{I}) | \Psi_{d_{\text{out}}} \rangle \right\}_{i_1, \dots, i_N} \\ &= \left\{ \prod_{t=1}^N \lambda_{i_t}^t \langle \Psi_{d_{\text{out}}} | (B_{i_t}^{t,\dagger} A_t \otimes \mathbb{I}) \left(\frac{\mathbb{I}}{D} + \frac{\varepsilon}{D} |w\rangle \langle w| \otimes U \right) (A_t^\dagger B_{i_t}^t \otimes \mathbb{I}) | \Psi_{d_{\text{out}}} \rangle \right\}_{i_1, \dots, i_N} \\ &= \left\{ \prod_{t=1}^N \left(\frac{\lambda_{i_t}^t}{D d_{\text{out}}} \text{Tr}(B_{i_t}^{t,\dagger} A_t A_t^\dagger B_{i_t}^t) + \frac{\varepsilon \lambda_{i_t}^t}{D} \langle \Psi_{d_{\text{out}}} | (B_{i_t}^{t,\dagger} A_t |w\rangle \langle w| A_t^\dagger B_{i_t}^t \otimes U) | \Psi_{d_{\text{out}}} \rangle \right) \right\}_{i_1, \dots, i_N} \end{aligned}$$

So, we can express the TV distance as follows:

$$\begin{aligned}
 & 2 \text{TV} \left(\mathbb{P}_{H_0}^{I_1, \dots, I_N} \parallel \mathbb{P}_{H_1}^{I_1, \dots, I_N} \right) \\
 &= \sum_{i_1, \dots, i_N} \left| \mathbb{E}_{(w, U) \sim \mathcal{P}} \prod_{t=1}^N \left(\frac{\lambda_{i_t}^t}{D d_{\text{out}}} \text{Tr}(B_{i_t}^{t, \dagger} A_t A_t^\dagger B_{i_t}^t) + \frac{\varepsilon \lambda_{i_t}^t}{D} \langle \Psi_{d_{\text{out}}} | (B_{i_t}^{t, \dagger} A_t | w \rangle \langle w | A_t^\dagger B_{i_t}^t \otimes U) | \Psi_{d_{\text{out}}} \rangle \right) \right. \\
 &\quad \left. - \prod_{t=1}^N \frac{\lambda_{i_t}^t}{D d_{\text{out}}} \text{Tr}(B_{i_t}^{t, \dagger} A_t A_t^\dagger B_{i_t}^t) \right| \\
 &= \mathbb{E}_{\leq N} \left| \mathbb{E}_{(w, U) \sim \mathcal{P}} \prod_{t=1}^N \left(1 + \varepsilon d_{\text{out}} \frac{\langle \Psi_{d_{\text{out}}} | (B_{i_t}^{t, \dagger} A_t | w \rangle \langle w | A_t^\dagger B_{i_t}^t \otimes U) | \Psi_{d_{\text{out}}} \rangle}{\text{Tr}(B_{i_t}^{t, \dagger} A_t A_t^\dagger B_{i_t}^t)} \right) - 1 \right| \\
 &= \mathbb{E}_{\leq N} \left| \mathbb{E}_{(w, U) \sim \mathcal{P}} \prod_{t=1}^N \left(1 + \varepsilon \cdot \frac{\text{Tr}(B_{i_t}^{t, \dagger} A_t | w \rangle \langle w | A_t^\dagger B_{i_t}^t U)}{\text{Tr}(B_{i_t}^{t, \dagger} A_t A_t^\dagger B_{i_t}^t)} \right) - 1 \right|
 \end{aligned}$$

where we use the notation $\mathbb{E}_{\leq N}(X(i_1, \dots, i_N)) = \sum_{i_1, \dots, i_N} \left(\prod_{t=1}^N \frac{\lambda_{i_t}^t}{D d_{\text{out}}} \text{Tr}(B_{i_t}^{t, \dagger} A_t A_t^\dagger B_{i_t}^t) \right) X(i_1, \dots, i_N)$.

Let u be a standard Gaussian vector such that $|w\rangle = \frac{|u\rangle}{\|u\|_2}$. We condition on the event \mathcal{E} that u satisfies:

1. $\|u\|_2 \geq \sqrt{\frac{1}{6} d_{\text{in}}}$ and
2. $\forall t \in [N] : P_u^t \leq \frac{(7 \log(N))^4}{d_{\text{in}}^4 d_{\text{out}}}$

where P_u^t is defined as

$$\begin{aligned}
 P_w^t &= \sum_{i_t, j_t} \frac{\lambda_{i_t}^t \lambda_{j_t}^t}{D^2 d_{\text{out}}^2} \left(\frac{|\langle w | A_t^\dagger B_{i_t}^t B_{j_t}^{t, \dagger} A_t | w \rangle|^4}{\text{Tr}(B_{i_t}^{t, \dagger} A_t A_t^\dagger B_{i_t}^t) \text{Tr}(B_{j_t}^{t, \dagger} A_t A_t^\dagger B_{j_t}^t)} \right) \\
 P_u^t &= \sum_{i_t, j_t} \frac{\lambda_{i_t}^t \lambda_{j_t}^t}{D^2 d_{\text{out}}^2 d_{\text{in}}^4} \left(\frac{|\langle u | A_t^\dagger B_{i_t}^t B_{j_t}^{t, \dagger} A_t | u \rangle|^4}{\text{Tr}(B_{i_t}^{t, \dagger} A_t A_t^\dagger B_{i_t}^t) \text{Tr}(B_{j_t}^{t, \dagger} A_t A_t^\dagger B_{j_t}^t)} \right).
 \end{aligned}$$

Note that under the event \mathcal{E} , we have $P_w^t \leq 6^4 P_u^t$. We claim that for $d_{\text{in}} \geq 80$, we have with probability at least 9/10, the event \mathcal{E} is satisfied. The proof of this claim is deferred to Lemma 27.

Now, we can distinguish whether the event \mathcal{E} is verified or not in the TV distance. Let

$$\Psi_{i, w, U} = \prod_{t=1}^N \left(1 + \varepsilon \cdot \Phi_{w, U}^{t, i_t} \right) \quad \text{where} \quad \Phi_{w, U}^{t, i_t} = \frac{\text{Tr}(B_{i_t}^{t, \dagger} A_t | w \rangle \langle w | A_t^\dagger B_{i_t}^t U)}{\text{Tr}(B_{i_t}^{t, \dagger} A_t A_t^\dagger B_{i_t}^t)}.$$

By the triangle inequality:

$$\begin{aligned}
 & \mathbb{E}_{\leq N} \left| \mathbb{E}_{(w, U) \sim \mathcal{P}} \prod_{t=1}^N \left(1 + \varepsilon \cdot \frac{\text{Tr}(B_{i_t}^{t, \dagger} A_t | w \rangle \langle w | A_t^\dagger B_{i_t}^t U)}{\text{Tr}(B_{i_t}^{t, \dagger} A_t A_t^\dagger B_{i_t}^t)} \right) - 1 \right| \\
 & \leq \mathbb{E}_{\leq N} \left| \mathbb{E}_{(w, U) \sim \mathcal{P}} [\mathbf{1}\{\mathcal{E}\}(\Psi_{i, w, U} - 1)] \right| + \mathbb{E}_{\leq N} \left| \mathbb{E}_{(w, U) \sim \mathcal{P}} [\mathbf{1}\{\bar{\mathcal{E}}\}(\Psi_{i, w, U} - 1)] \right| \\
 & \leq \mathbb{E}_{\leq N} \left| \mathbb{E}_{(w, U) \sim \mathcal{P}} [\mathbf{1}\{\mathcal{E}\}(\Psi_{i, w, U} - 1)] \right| + \mathbb{E}_{\leq N} \mathbb{E}_{(w, U) \sim \mathcal{P}} [\mathbf{1}\{\bar{\mathcal{E}}\}(\Psi_{i, w, U} + 1)] \\
 & = \mathbb{E}_{\leq N} \left| \mathbb{E}_{(w, U) \sim \mathcal{P}} [\mathbf{1}\{\mathcal{E}\}(\Psi_{i, w, U} - 1)] \right| + 2\mathbb{P}(\bar{\mathcal{E}})
 \end{aligned}$$

where we use the fact that $\sum_{i_t} \lambda_{i_t}^t B_{i_t}^{t,\dagger} X B_{i_t}^t = d_{\text{out}} \text{Tr}(X) \mathbb{I}$ and

$$\begin{aligned} \mathbb{E}_{\leq N} \Psi_{i,w,U} &= \sum_{i_1, \dots, i_N} \left(\prod_{t=1}^N \frac{\lambda_{i_t}^t}{D d_{\text{out}}} \cdot \text{Tr}(B_{i_t}^{t,\dagger} A_t A_t^\dagger B_{i_t}^t) \right) \prod_{t=1}^N \left(1 + \varepsilon \cdot \frac{\text{Tr}(B_{i_t}^{t,\dagger} A_t |w\rangle \langle w| A_t^\dagger B_{i_t}^t U)}{\text{Tr}(B_{i_t}^{t,\dagger} A_t A_t^\dagger B_{i_t}^t)} \right) \\ &= \prod_{t=1}^N \sum_{i_t} \left(\frac{\lambda_{i_t}^t}{D d_{\text{out}}} \cdot \text{Tr}(B_{i_t}^{t,\dagger} A_t A_t^\dagger B_{i_t}^t) + \frac{\varepsilon \lambda_{i_t}^t}{D d_{\text{out}}} \cdot \text{Tr}(B_{i_t}^{t,\dagger} A_t |w\rangle \langle w| A_t^\dagger B_{i_t}^t U) \right) \\ &= \prod_{t=1}^N \left(1 + \frac{\varepsilon}{D} \cdot \text{Tr}(A_t |w\rangle \langle w| A_t^\dagger) \text{Tr}(U) \right) = 1. \end{aligned}$$

It remains to upper bound the expectation $\mathbb{E}_{\leq N} |\mathbb{E}_{(w,U) \sim \mathcal{P}} [\mathbf{1}\{\mathcal{E}\}(\Psi_{i,w,U} - 1)]|$. For this, we follow (Bubeck et al., 2020) and apply the Cauchy Schwarz inequality and Hölder's inequality:

$$\begin{aligned} & \left(\mathbb{E}_{\leq N} |\mathbb{E}_{(w,U) \sim \mathcal{P}} [\mathbf{1}\{\mathcal{E}\}(\Psi_{i,w,U} - 1)]| \right)^2 + \mathbb{P}(\mathcal{E})^2 \\ & \leq \mathbb{E}_{\leq N} \left(\mathbb{E}_{(w,U) \sim \mathcal{P}} [\mathbf{1}\{\mathcal{E}(w)\}(\Psi_{i,w,U} - 1)] \right)^2 + \mathbb{P}(\mathcal{E})^2 \\ & = \mathbb{E}_{\leq N} \mathbb{E}_{(w,U) \sim \mathcal{P}} \mathbb{E}_{(z,V) \sim \mathcal{P}} \mathbf{1}\{\mathcal{E}(w)\} \Psi_{i,w,U} \mathbf{1}\{\mathcal{E}(z)\} \Psi_{i,z,V} \\ & \leq \mathbb{E}_{(w,U) \sim \mathcal{P}} \mathbf{1}\{\mathcal{E}(w)\} \mathbb{E}_{(z,V) \sim \mathcal{P}} \mathbf{1}\{\mathcal{E}(z)\} \prod_{t=1}^N \mathbb{E}_{i_t} \left(1 + \varepsilon \cdot \Phi_{w,U}^{t,i_t} \right) \left(1 + \varepsilon \cdot \Phi_{z,V}^{t,i_t} \right) \\ & = \mathbb{E}_{(w,U) \sim \mathcal{P}} \mathbf{1}\{\mathcal{E}(w)\} \mathbb{E}_{(z,V) \sim \mathcal{P}} \mathbf{1}\{\mathcal{E}(z)\} \prod_{t=1}^N \left(1 + \varepsilon^2 \cdot \mathbb{E}_{i_t} \Phi_{w,U}^{t,i_t} \Phi_{z,V}^{t,i_t} \right) \quad (\text{because } \mathbb{E}_{i_t} \Phi_{w,U}^{t,i_t} = 0) \\ & \leq \max_{1 \leq t \leq N} \mathbb{E}_{(w,U) \sim \mathcal{P}} \mathbf{1}\{\mathcal{E}(w)\} \mathbb{E}_{(z,V) \sim \mathcal{P}} \mathbf{1}\{\mathcal{E}(z)\} \left(1 + \varepsilon^2 \cdot \mathbb{E}_{i_t} \Phi_{w,U}^{t,i_t} \Phi_{z,V}^{t,i_t} \right)^N \\ & \leq \frac{1}{\mathbb{P}(\mathcal{G})^2} \max_{1 \leq t \leq N} \mathbb{E}_{U,V \sim \mathcal{P}_0} \mathbb{E}_{w,z} \mathbf{1}\{\mathcal{E}(w)\} \mathbf{1}\{\mathcal{E}(z)\} \left(1 + \varepsilon^2 \cdot \left| \mathbb{E}_{i_t} \Phi_{w,U}^{t,i_t} \Phi_{z,V}^{t,i_t} \right| \right)^N \\ & \leq \frac{1}{(1 - e^{-\Omega(d_{\text{out}})})^2} \max_{1 \leq t \leq N} \mathbb{E}_{U,V \sim \mathcal{P}_0} \mathbb{E}_{w,z} \mathbf{1}\{\mathcal{E}(w)\} \mathbf{1}\{\mathcal{E}(z)\} \left(1 + \varepsilon^2 \cdot \left| \mathbb{E}_{i_t} \Phi_{w,U}^{t,i_t} \Phi_{z,V}^{t,i_t} \right| \right)^N \end{aligned}$$

Note that at the last two inequalities, we don't require anymore that U satisfies $\|U\|_\infty \leq 32$ and $\|U\|_1 \geq d_{\text{out}}$. This is possible because the integrand is positive and $\mathbb{P}(\mathcal{G}) \geq 1 - e^{-\Omega(d_{\text{out}})}$.

For $t \in [N]$, let Z_t be the polynomial in $\{U_{i,j}, V_{i,j}\}_{i,j=1}^{d_{\text{out}}}$ defined as follows:

$$\begin{aligned} Z_t &= \varepsilon^2 \mathbb{E}_{i_t} \Phi_{w,U}^{t,i_t} \Phi_{z,V}^{t,i_t} \\ &= \varepsilon^2 \sum_{i_t} \left(\frac{\lambda_{i_t}^t}{D d_{\text{out}}} \text{Tr}(B_{i_t}^{t,\dagger} A_t A_t^\dagger B_{i_t}^t) \right) \left(\frac{\text{Tr}(B_{i_t}^{t,\dagger} A_t |w\rangle \langle w| A_t^\dagger B_{i_t}^t U)}{\text{Tr}(B_{i_t}^{t,\dagger} A_t A_t^\dagger B_{i_t}^t)} \right) \left(\frac{\text{Tr}(B_{i_t}^{t,\dagger} A_t |z\rangle \langle z| A_t^\dagger B_{i_t}^t V)}{\text{Tr}(B_{i_t}^{t,\dagger} A_t A_t^\dagger B_{i_t}^t)} \right) \\ &= \varepsilon^2 \sum_{i_t} \left(\frac{\lambda_{i_t}^t}{D d_{\text{out}}} \right) \left(\frac{\text{Tr}(B_{i_t}^{t,\dagger} A_t |w\rangle \langle w| A_t^\dagger B_{i_t}^t U) \text{Tr}(B_{i_t}^{t,\dagger} A_t |z\rangle \langle z| A_t^\dagger B_{i_t}^t V)}{\text{Tr}(B_{i_t}^{t,\dagger} A_t A_t^\dagger B_{i_t}^t)} \right) \end{aligned}$$

Note that Z_t is a polynomial of degree 2 of expectation 0. The Hypercontractivity (Aubrun and Szarek, 2017, Proposition 5.48) implies for all $k \in \{1, \dots, N\}$:

$$\mathbb{E}(|Z_t|^k) \leq k^k \mathbb{E}(Z_t^2)^{k/2}.$$

This means that we only need to control the second moment of Z_t . We have:

$$\mathbb{E}_{U,V}(Z_t^2) = \varepsilon^4 \mathbb{E}_{U,V} \left[\sum_{i_t, j_t} \frac{\lambda_{i_t}^t \lambda_{j_t}^t}{D^2 d_{\text{out}}^2} \left(\frac{\text{Tr}(B_{i_t}^{t,\dagger} A_t |w\rangle \langle w| A_t^\dagger B_{i_t}^t U) \text{Tr}(B_{i_t}^{t,\dagger} A_t |z\rangle \langle z| A_t^\dagger B_{i_t}^t V)}{\text{Tr}(B_{i_t}^{t,\dagger} A_t A_t^\dagger B_{i_t}^t)} \right) \cdot \left(\frac{\text{Tr}(B_{j_t}^{t,\dagger} A_t |w\rangle \langle w| A_t^\dagger B_{j_t}^t U) \text{Tr}(B_{j_t}^{t,\dagger} A_t |z\rangle \langle z| A_t^\dagger B_{j_t}^t V)}{\text{Tr}(B_{j_t}^{t,\dagger} A_t A_t^\dagger B_{j_t}^t)} \right) \right].$$

Let $\Xi_{i_t, j_t}(w) = \mathbb{E}_U [\text{Tr}(B_{i_t}^{t,\dagger} A_t |w\rangle \langle w| A_t^\dagger B_{i_t}^t U) \text{Tr}(B_{j_t}^{t,\dagger} A_t |w\rangle \langle w| A_t^\dagger B_{j_t}^t U)]$, we have :

$$\mathbb{E}_{U,V}(Z_t^2) = \varepsilon^4 \sum_{i_t, j_t} \frac{\lambda_{i_t}^t \lambda_{j_t}^t}{D^2 d_{\text{out}}^2} \left(\frac{\Xi_{i_t, j_t}(w) \Xi_{i_t, j_t}(z)}{\text{Tr}(B_{i_t}^{t,\dagger} A_t A_t^\dagger B_{i_t}^t) \text{Tr}(B_{j_t}^{t,\dagger} A_t A_t^\dagger B_{j_t}^t)} \right)$$

For given i_t, j_t , we can upper bound the expectation Ξ_{i_t, j_t} :

$$\begin{aligned} \Xi_{i_t, j_t}(w) &= \mathbb{E}_U [\text{Tr}(B_{i_t}^{t,\dagger} A_t |w\rangle \langle w| A_t^\dagger B_{i_t}^t U) \text{Tr}(B_{j_t}^{t,\dagger} A_t |w\rangle \langle w| A_t^\dagger B_{j_t}^t U)] \\ &= \sum_{x, y, x', y'} \mathbb{E} (U_{x, y} U_{x', y'}) \text{Tr}(B_{i_t}^{t,\dagger} A_t |w\rangle \langle w| A_t^\dagger B_{i_t}^t |x\rangle \langle y|) \text{Tr}(B_{j_t}^{t,\dagger} A_t |w\rangle \langle w| A_t^\dagger B_{j_t}^t |x'\rangle \langle y'|) \\ &\leq \frac{16}{d_{\text{out}}} \sum_{x, y} \langle w| A_t^\dagger B_{i_t}^t |x\rangle \langle x| B_{i_t}^{t,\dagger} A_t |w\rangle \langle w| A_t^\dagger B_{j_t}^t |y\rangle \langle y| B_{j_t}^{t,\dagger} A_t |w\rangle \\ &= \frac{16}{d_{\text{out}}} \langle w| A_t^\dagger B_{i_t}^t B_{j_t}^{t,\dagger} A_t |w\rangle \langle w| A_t^\dagger B_{j_t}^t B_{i_t}^{t,\dagger} A_t |w\rangle \\ &= \frac{16}{d_{\text{out}}} |\langle w| A_t^\dagger B_{i_t}^t B_{j_t}^{t,\dagger} A_t |w\rangle|^2 \end{aligned}$$

Therefore we can upper bound the expectation of Z_t^2 as follows:

$$\begin{aligned} \mathbb{E}_{U,V}(Z_t^2) &= \varepsilon^4 \sum_{i_t, j_t} \frac{\lambda_{i_t}^t \lambda_{j_t}^t}{D^2 d_{\text{out}}^2} \left(\frac{\Xi_{i_t, j_t}(w) \Xi_{i_t, j_t}(z)}{\text{Tr}(B_{i_t}^{t,\dagger} A_t A_t^\dagger B_{i_t}^t) \text{Tr}(B_{j_t}^{t,\dagger} A_t A_t^\dagger B_{j_t}^t)} \right) \\ &= \varepsilon^4 \left(\frac{16^2}{d_{\text{out}}^2} \right) \sum_{i_t, j_t} \frac{\lambda_{i_t}^t \lambda_{j_t}^t}{D^2 d_{\text{out}}^2} \left(\frac{|\langle w| A_t^\dagger B_{i_t}^t B_{j_t}^{t,\dagger} A_t |w\rangle|^2 |\langle z| A_t^\dagger B_{i_t}^t B_{j_t}^{t,\dagger} A_t |z\rangle|^2}{\text{Tr}(B_{i_t}^{t,\dagger} A_t A_t^\dagger B_{i_t}^t) \text{Tr}(B_{j_t}^{t,\dagger} A_t A_t^\dagger B_{j_t}^t)} \right) \end{aligned}$$

This implies an upper bound for every moment, that is for $k = 1, \dots, N$, we have:

$$\begin{aligned}
 & \mathbb{E}_{w,z} \mathbf{1}\{\mathcal{E}(w)\} \mathbf{1}\{\mathcal{E}(z)\} \mathbb{E}_{U,V}(|Z_t|^k) \\
 & \leq \mathbb{E}_{w,z} \mathbf{1}\{\mathcal{E}(w)\} \mathbf{1}\{\mathcal{E}(z)\} k^k \left[\varepsilon^4 \left(\frac{16^2}{d_{\text{out}}^2} \right) \sum_{i_t, j_t} \frac{\lambda_{i_t}^t \lambda_{j_t}^t}{D^2 d_{\text{out}}^2} \left(\frac{|\langle w | A_t^\dagger B_{i_t}^t B_{j_t}^{t,\dagger} A_t | w \rangle|^2 |\langle z | A_t^\dagger B_{i_t}^t B_{j_t}^{t,\dagger} A_t | z \rangle|^2}{\text{Tr}(B_{i_t}^{t,\dagger} A_t A_t^\dagger B_{i_t}^t) \text{Tr}(B_{j_t}^{t,\dagger} A_t A_t^\dagger B_{j_t}^t)} \right) \right]^{k/2} \\
 & \leq k^k \mathbb{E}_{w,z} \mathbf{1}\{\mathcal{E}(w)\} \mathbf{1}\{\mathcal{E}(z)\} \left[\varepsilon^4 \left(\frac{16^2}{d_{\text{out}}^2} \right) \sum_{i_t, j_t} \frac{\lambda_{i_t}^t \lambda_{j_t}^t}{D^2 d_{\text{out}}^2} \left(\frac{|\langle w | A_t^\dagger B_{i_t}^t B_{j_t}^{t,\dagger} A_t | w \rangle|^4 + |\langle z | A_t^\dagger B_{i_t}^t B_{j_t}^{t,\dagger} A_t | z \rangle|^4}{2 \text{Tr}(B_{i_t}^{t,\dagger} A_t A_t^\dagger B_{i_t}^t) \text{Tr}(B_{j_t}^{t,\dagger} A_t A_t^\dagger B_{j_t}^t)} \right) \right]^{k/2} \\
 & = k^k \mathbb{E}_{w,z} \mathbf{1}\{\mathcal{E}(w)\} \mathbf{1}\{\mathcal{E}(z)\} \left[\varepsilon^4 \left(\frac{16^2}{d_{\text{out}}^2} \right) \frac{(P_w^t + P_z^t)}{2} \right]^{k/2} \\
 & \leq k^k \mathbb{E}_{w,z} \mathbf{1}\{\mathcal{E}(w)\} \mathbf{1}\{\mathcal{E}(z)\} \left[\varepsilon^4 \left(\frac{16^2 \cdot 6^4}{d_{\text{out}}^2} \right) \frac{(P_u^t + P_v^t)}{2} \right]^{k/2} \\
 & \leq k^k \mathbb{E}_{w,z} \mathbf{1}\{\mathcal{E}(w)\} \mathbf{1}\{\mathcal{E}(z)\} \left[\varepsilon^4 \left(\frac{16^2 \cdot 6^4}{d_{\text{out}}^2} \right) \left(\frac{(7 \log(N))^4}{d_{\text{in}}^4 d_{\text{out}}^3} \right) \right]^{k/2} \leq k^k \left[\frac{C \varepsilon^4 \log(N)^4}{d_{\text{in}}^4 d_{\text{out}}^3} \right]^{k/2}
 \end{aligned}$$

where $C > 0$ is a universal constant and we used that we are under the events $\mathcal{E}(w)$ and $\mathcal{E}(z)$.

Now, grouping the lower bound and upper bounds on the TV distance, we obtain:

$$\begin{aligned}
 (1 - e^{-\Omega(d_{\text{out}})})^2 \left(\frac{7^2}{15^2} + \frac{9^2}{10^2} \right) & \leq (1 - e^{-\Omega(d_{\text{out}})})^2 \left[\left(2 \text{TV} \left(\mathbb{P}_{H_0}^{I_1, \dots, I_N} \parallel \mathbb{P}_{H_1}^{I_1, \dots, I_N} \right) - 2\mathbb{P}(\bar{\mathcal{E}}) \right)^2 + \mathbb{P}(\mathcal{E})^2 \right] \\
 & \leq (1 - e^{-\Omega(d_{\text{out}})})^2 \left[\left(\mathbb{E}_{\leq N} |\mathbb{E}_{(w,U) \sim \mathcal{P}} [\mathbf{1}\{\mathcal{E}\} (\Psi_{i,w,U} - 1)] \right)^2 + \mathbb{P}(\mathcal{E})^2 \right] \\
 & \leq \max_t \mathbb{E} \left((1 + |Z_t|)^N \right) \\
 & \leq \max_t \sum_{k=0}^N \binom{N}{k} k^k \left(\frac{C \varepsilon^4 \log(N)^4}{d_{\text{in}}^4 d_{\text{out}}^3} \right)^{k/2} \leq \sum_{k=0}^N \left(\frac{C' N \varepsilon^2 \log(N)^2}{d_{\text{in}}^2 d_{\text{out}}^{1.5}} \right)^k
 \end{aligned}$$

where we used $\binom{N}{k} \leq \frac{N^k e^k}{k^k}$ and $C' = \sqrt{C}e$. If $N \log(N)^2 \leq \frac{d_{\text{in}}^2 d_{\text{out}}^{1.5}}{101 C' \varepsilon^2}$ the RHS is upper bounded by $\sum_{k \geq 0} \frac{1}{101^k} = 1.01$ but the LHS is at least $(1 - e^{-\Omega(d_{\text{out}})})^2 \left(\frac{7^2}{15^2} + \frac{9^2}{10^2} \right) \geq 1.02$ for $d_{\text{out}} \geq \Omega(1)$

which is a contradiction. Hence $N \log(N)^2 \geq \frac{d_{\text{in}}^2 d_{\text{out}}^{1.5}}{101 C' \varepsilon^2}$ and finally:

$$N \geq \Omega \left(\frac{d_{\text{in}}^2 d_{\text{out}}^{1.5}}{\log(d_{\text{in}} d_{\text{out}} / \varepsilon)^2 \varepsilon^2} \right).$$

■

We move to prove our claim:

Lemma 27 *Let $d_{\text{in}} \geq 80$. We have with probability at least 9/10, the event \mathcal{E} is satisfied.*

Proof Fix $t \in [N]$, denote $(i, j) = (i_t, j_t)$, $X_i = B_i^\dagger A_t$ and recall that $|w\rangle = \frac{|u\rangle}{\|u\|_2}$ such that u is a standard Gaussian vector. Recall that the event \mathcal{E} is u satisfies:

1. $\|u\|_2 \geq \frac{1}{2}\sqrt{\frac{2}{3}d_{\text{in}}}$ and
2. $\forall t \in [N] : P_u^t \leq \frac{(7 \log(N))^4}{d_{\text{in}}^4 d_{\text{out}}}$

where P_u^t is defined as

$$P_u^t = \sum_{i_t, j_t} \frac{\lambda_{i_t}^t \lambda_{j_t}^t}{D^2 d_{\text{out}}^2 d_{\text{in}}^4} \left(\frac{|\langle u | A_{i_t}^\dagger B_{i_t}^\dagger B_{j_t}^{t, \dagger} A_t | u \rangle|^4}{\text{Tr}(B_{i_t}^{t, \dagger} A_t A_{i_t}^\dagger B_{i_t}^t) \text{Tr}(B_{j_t}^{t, \dagger} A_t A_{j_t}^\dagger B_{j_t}^t)} \right) = \sum_{i, j} \frac{\lambda_i \lambda_j}{D^2 d_{\text{out}}^2 d_{\text{in}}^4} \left(\frac{|\langle u | X_i^\dagger X_j | u \rangle|^4}{\|X_i\|_2^2 \|X_j\|_2^2} \right)$$

First note that with high probability $\|u\|_2 \geq \frac{1}{2}\sqrt{\frac{2}{3}d_{\text{in}}}$. Indeed, the function $u \mapsto \|u\|_2$ is Lipschitz so $\mathbb{P}(\|u\|_2 \leq \mathbb{E}(\|u\|_2) - s) \leq e^{-s^2/2}$ (Wainwright, 2019, Theorem 2.26). On the other hand we have by Hölder's inequality $\mathbb{E}(\|u\|_2) \geq \sqrt{\frac{\mathbb{E}(\|u\|_2^2)^3}{\mathbb{E}(\|u\|_2^4)}} = \sqrt{\frac{d_{\text{in}}^3}{d_{\text{in}}^2 + 2d_{\text{in}}}} \geq \sqrt{\frac{2}{3}d_{\text{in}}}$ hence

$$\mathbb{P}\left(\|u\|_2 \leq \frac{1}{2}\sqrt{\frac{2}{3}d_{\text{in}}}\right) \leq \mathbb{P}\left(\|u\|_2 - \mathbb{E}(\|u\|_2) \leq -\frac{1}{2}\sqrt{\frac{2}{3}d_{\text{in}}}\right) \leq e^{-d_{\text{in}}/32}.$$

For the second point in the event \mathcal{E} , we can see that P_u is a Gaussian polynomial in the entries of u of degree 8. So we can use the concentration inequality of Gaussian polynomials (Aubrun and Szarek, 2017, Corollary 5.49), for any $s > (2e)^{1/4}$ we have:

$$\mathbb{P}\left(|P - \mathbb{E}(P)| \geq s\sqrt{\text{Var}(P)}\right) \leq \exp\left(-\frac{4}{e}s^{1/4}\right)$$

so with probability at least $1 - \frac{1}{N^2}$ we have:

$$P \leq \mathbb{E}(P) + (e \log(N)/2)^4 \sqrt{\text{Var}(P)} \leq 5 \log^4(N) \sqrt{\mathbb{E}(P^2)}.$$

Let us control the expectation of $P^2 = P_u^2$, recall that we denote $(i, j) = (i_t, j_t)$ and $X_i = B_i^\dagger A_t$,

$$\begin{aligned} \mathbb{E}(P^2) &= \mathbb{E}\left[\left(\sum_{i, j} \frac{\lambda_i \lambda_j}{D^2 d_{\text{out}}^2 d_{\text{in}}^4} \left(\|X_i\|_2^{-2} \|X_j\|_2^{-2} |\langle u | X_i^\dagger X_j | u \rangle|^4\right)\right)^2\right] \\ &= \mathbb{E}\left[\sum_{i, j, k, l} \frac{\lambda_i \lambda_j \lambda_k \lambda_l}{D^4 d_{\text{out}}^4 d_{\text{in}}^8} \left(\|X_i\|_2^{-2} \|X_j\|_2^{-2} \|X_k\|_2^{-2} \|X_l\|_2^{-2} |\langle w | X_i^\dagger X_j | w \rangle|^4 |\langle w | X_k^\dagger X_l | w \rangle|^4\right)\right] \mathbb{E}(\|u\|_2^{16}) \\ &\leq \sum_{i, j, k, l} \frac{\lambda_i \lambda_j \lambda_k \lambda_l}{D^4 d_{\text{out}}^4 d_{\text{in}}^8} \cdot \frac{\sum_{\alpha \in \mathfrak{S}_8} \text{Tr}_\alpha(X_i^\dagger X_j, X_j^\dagger X_i, X_i^\dagger X_j, X_j^\dagger X_i, X_k^\dagger X_l, X_l^\dagger X_k, X_k^\dagger X_l, X_l^\dagger X_k)}{(d_{\text{in}} + 7)! [(d_{\text{in}} - 1)!]^{-1} \|X_i\|_2^2 \|X_j\|_2^2 \|X_k\|_2^2 \|X_l\|_2^2} \cdot d_{\text{in}}^8 \\ &\leq \max_{\alpha \in \mathfrak{S}_8} \sum_{i, j, k, l} \frac{8! \lambda_i \lambda_j \lambda_k \lambda_l}{D^4 d_{\text{out}}^4 d_{\text{in}}^8} \cdot \frac{|\text{Tr}_\alpha(X_i^\dagger X_j, X_j^\dagger X_i, X_i^\dagger X_j, X_j^\dagger X_i, X_k^\dagger X_l, X_l^\dagger X_k, X_k^\dagger X_l, X_l^\dagger X_k)|}{\|X_i\|_2^2 \|X_j\|_2^2 \|X_k\|_2^2 \|X_l\|_2^2} \end{aligned}$$

Then we claim that:

Lemma 28 Let $A = X_i^\dagger X_j$ and $B = X_k^\dagger X_l$, we have for all $\alpha \in \mathfrak{S}_8$,

$$\begin{aligned} & |\mathrm{Tr}_\alpha(A, A^\dagger, A, A^\dagger, B, B^\dagger, B, B^\dagger)|^{1/2} \\ & \leq \max\{|\mathrm{Tr}(A)|^4, \mathrm{Tr}(AA^\dagger)^2\} \max\{|\mathrm{Tr}(B)|^4, \mathrm{Tr}(BB^\dagger)^2\} \\ & \leq \|X_i\|_2^2 \|X_j\|_2^2 \|X_k\|_2^2 \|X_l\|_2^2. \end{aligned}$$

Sketch of the proof. The strategy to prove this lemma depends on α , we can give an outline:

- Traces containing one element remain unchanged.
- If we have two successive A (or B) in a trace term, we upper bound this trace with a 2-norm $\mathrm{Tr}(AA^\dagger)$ times the operator norm of the remaining elements. Then we can upper bound the operator norms with the 2-norms.
- Otherwise, we have successive (A, B) (with possible adjoint) inside the trace term. We can apply a Cauchy Schwarz inequality then we find two successive A or B and apply the previous strategy.

For instance we have for $\alpha = (1)(5372648)$:

$$\begin{aligned} \mathrm{Tr}(A)\mathrm{Tr}(BABAA^\dagger B^\dagger A^\dagger B^\dagger) & \leq |\mathrm{Tr}(A)|\mathrm{Tr}(BB^\dagger)\|ABAA^\dagger B^\dagger A^\dagger\|_\infty \\ & \leq |\mathrm{Tr}(A)|\mathrm{Tr}(BB^\dagger)\|BB^\dagger\|_\infty\|AA^\dagger\|_\infty^{3/2} \\ & \leq |\mathrm{Tr}(A)|\mathrm{Tr}(BB^\dagger)\mathrm{Tr}(BB^\dagger)\mathrm{Tr}(AA^\dagger)^{3/2} \\ & \leq \max\{|\mathrm{Tr}(A)|^4, \mathrm{Tr}(AA^\dagger)^2\} \max\{|\mathrm{Tr}(B)|^4, \mathrm{Tr}(BB^\dagger)^2\}. \end{aligned}$$

Another example for $\alpha = (15372648)$:

$$\begin{aligned} \mathrm{Tr}(ABABA^\dagger B^\dagger A^\dagger B^\dagger) & \leq \mathrm{Tr}(ABABB^\dagger A^\dagger B^\dagger A^\dagger)^{1/2} \mathrm{Tr}(BABAA^\dagger B^\dagger A^\dagger B^\dagger)^{1/2} \\ & \leq \mathrm{Tr}(BB^\dagger)\|AA^\dagger\|_\infty^2 \|BB^\dagger\|_\infty \leq \mathrm{Tr}(BB^\dagger)^2 \mathrm{Tr}(AA^\dagger)^2. \end{aligned}$$

Using Lemma 28, we have:

$$\begin{aligned} \mathbb{E}(P^2) & \leq \max_{\alpha \in \mathfrak{S}_8} \sum_{i,j,k,l} \frac{8! \lambda_i \lambda_j \lambda_k \lambda_l}{D^4 d_{\mathrm{out}}^4 d_{\mathrm{in}}^8} \cdot \frac{|\mathrm{Tr}_\alpha(X_i^\dagger X_j, X_j^\dagger X_i, X_i^\dagger X_j, X_j^\dagger X_i, X_k^\dagger X_l, X_l^\dagger X_k, X_k^\dagger X_l, X_l^\dagger X_k)|}{\|X_i\|_2^2 \|X_j\|_2^2 \|X_k\|_2^2 \|X_l\|_2^2} \\ & \leq \max_{\alpha \in \mathfrak{S}_8} \sum_{i,j,k,l} \frac{8! \lambda_i \lambda_j \lambda_k \lambda_l}{D^4 d_{\mathrm{out}}^4 d_{\mathrm{in}}^8} \cdot \sqrt{|\mathrm{Tr}_\alpha(X_i^\dagger X_j, X_j^\dagger X_i, X_i^\dagger X_j, X_j^\dagger X_i, X_k^\dagger X_l, X_l^\dagger X_k, X_k^\dagger X_l, X_l^\dagger X_k)|} \\ & \leq \sum_{i,j,k,l} \frac{8! \lambda_i \lambda_j \lambda_k \lambda_l}{D^4 d_{\mathrm{out}}^4 d_{\mathrm{in}}^8} \cdot \max\{|\mathrm{Tr}(X_i^\dagger X_j)|^2, \mathrm{Tr}(X_i^\dagger X_j X_j^\dagger X_i)\} \max\{|\mathrm{Tr}(X_k^\dagger X_l)|^2, \mathrm{Tr}(X_k^\dagger X_l X_l^\dagger X_k)\} \end{aligned}$$

So we have 4 cases to consider, two of them are similar. Let us define four subsets of indices:

$$\begin{aligned} C_1 & = \{(i, j, k, l) : |\mathrm{Tr}(X_i^\dagger X_j)|^2 > \mathrm{Tr}(X_i^\dagger X_j X_j^\dagger X_i), |\mathrm{Tr}(X_k^\dagger X_l)|^2 > \mathrm{Tr}(X_k^\dagger X_l X_l^\dagger X_k)\}, \\ C_2 & = \{(i, j, k, l) : |\mathrm{Tr}(X_i^\dagger X_j)|^2 \leq \mathrm{Tr}(X_i^\dagger X_j X_j^\dagger X_i), |\mathrm{Tr}(X_k^\dagger X_l)|^2 \leq \mathrm{Tr}(X_k^\dagger X_l X_l^\dagger X_k)\}, \\ C_3 & = \{(i, j, k, l) : |\mathrm{Tr}(X_i^\dagger X_j)|^2 > \mathrm{Tr}(X_i^\dagger X_j X_j^\dagger X_i), |\mathrm{Tr}(X_k^\dagger X_l)|^2 \leq \mathrm{Tr}(X_k^\dagger X_l X_l^\dagger X_k)\}, \\ C_4 & = \{(i, j, k, l) : |\mathrm{Tr}(X_i^\dagger X_j)|^2 \leq \mathrm{Tr}(X_i^\dagger X_j X_j^\dagger X_i), |\mathrm{Tr}(X_k^\dagger X_l)|^2 > \mathrm{Tr}(X_k^\dagger X_l X_l^\dagger X_k)\}. \end{aligned}$$

For the first case where the indices $(i, j, k, l) \in C_1$, we have:

$$\begin{aligned}
 & \sum_{i,j,k,l \in C_1} \frac{8! \lambda_i \lambda_j \lambda_k \lambda_l}{D^4 d_{\text{out}}^4 d_{\text{in}}^8} \cdot \max\{|\text{Tr}(X_i^\dagger X_j)|^2, \text{Tr}(X_i^\dagger X_j X_j^\dagger X_i)\} \max\{|\text{Tr}(X_k^\dagger X_l)|^2, \text{Tr}(X_k^\dagger X_l X_l^\dagger X_k)\} \\
 & \leq \sum_{i,j,k,l} \frac{8! \lambda_i \lambda_j \lambda_k \lambda_l}{D^4 d_{\text{out}}^4 d_{\text{in}}^8} \cdot |\text{Tr}(X_i^\dagger X_j)|^2 \text{Tr}(X_k^\dagger X_l)^2 \\
 & = \sum_{i,j,k,l} \sum_{x,y,x',y'} \frac{8! \lambda_i \lambda_j \lambda_k \lambda_l}{D^4 d_{\text{out}}^4 d_{\text{in}}^8} \cdot \langle x | X_i^\dagger X_j | x \rangle \langle y | X_j^\dagger X_i | y \rangle \langle x' | X_k^\dagger X_l | x' \rangle \langle y' | X_l^\dagger X_k | y' \rangle \\
 & = \sum_{x,y,x',y'} \frac{8!}{D^4 d_{\text{out}}^4 d_{\text{in}}^8} \cdot d_{\text{out}}^4 \text{Tr}[\text{Tr}(A_t |x\rangle \langle y| A_t^\dagger) \mathbb{I}_{d_{\text{out}}} \text{Tr}(A_t |y\rangle \langle x| A_t^\dagger) \mathbb{I}_{d_{\text{out}}}] \\
 & \quad \cdot \text{Tr}[\text{Tr}(A_t |x'\rangle \langle y'| A_t^\dagger) \mathbb{I}_{d_{\text{out}}} \text{Tr}(A_t |y'\rangle \langle x'| A_t^\dagger) \mathbb{I}_{d_{\text{out}}}] \\
 & = \sum_{x,y,x',y'} \frac{8!}{D^4 d_{\text{out}}^4 d_{\text{in}}^8} \cdot d_{\text{out}}^6 \langle y | A_t^\dagger A_t | x \rangle \langle x | A_t^\dagger A_t | y \rangle \langle y' | A_t^\dagger A_t | x' \rangle \langle x' | A_t^\dagger A_t | y' \rangle \\
 & = \frac{8!}{D^4 d_{\text{out}}^4 d_{\text{in}}^8} \cdot d_{\text{out}}^6 \text{Tr}(A_t^\dagger A_t A_t^\dagger A_t)^2 \leq \frac{8!}{D^4 d_{\text{out}}^4 d_{\text{in}}^8} \cdot d_{\text{out}}^6 \text{Tr}(A_t^\dagger A_t)^4 \\
 & = \frac{8!}{D^4 d_{\text{out}}^4 d_{\text{in}}^8} \cdot d_{\text{out}}^6 d_{\text{in}}^4 = \frac{8!}{d_{\text{in}}^8 d_{\text{out}}^2}
 \end{aligned}$$

because $\sum_i \lambda_i X_i M X_i^\dagger = \sum_i \lambda_i B_i^\dagger A_t M A_t^\dagger B_i = d_{\text{out}} \text{Tr}(A_t M A_t^\dagger) \mathbb{I}_{d_{\text{out}}}$ and $\text{Tr}(A_t A_t^\dagger) = d_{\text{in}}$.
 For the second case where the indices $(i, j, k, l) \in C_2$, we have:

$$\begin{aligned}
 & \sum_{i,j,k,l \in C_2} \frac{8! \lambda_i \lambda_j \lambda_k \lambda_l}{D^4 d_{\text{out}}^4 d_{\text{in}}^8} \cdot \max\{|\text{Tr}(X_i^\dagger X_j)|^2, \text{Tr}(X_i^\dagger X_j X_j^\dagger X_i)\} \max\{|\text{Tr}(X_k^\dagger X_l)|^2, \text{Tr}(X_k^\dagger X_l X_l^\dagger X_k)\} \\
 & \leq \sum_{i,j,k,l} \frac{\lambda_i \lambda_j \lambda_k \lambda_l}{D^4 d_{\text{out}}^4 d_{\text{in}}^8} \cdot \text{Tr}(X_i^\dagger X_j X_j^\dagger X_i) \text{Tr}(X_k^\dagger X_l X_l^\dagger X_k) \\
 & = \frac{8!}{D^4 d_{\text{out}}^4 d_{\text{in}}^8} \text{Tr}(A_t A_t^\dagger)^2 \text{Tr}(\mathbb{I}) \text{Tr}(A_t A_t^\dagger)^2 \text{Tr}(\mathbb{I}) d_{\text{out}}^4 \\
 & = \frac{8!}{D^4 d_{\text{out}}^4 d_{\text{in}}^8} d_{\text{in}}^4 d_{\text{out}}^6 = \frac{8!}{d_{\text{in}}^8 d_{\text{out}}^2}.
 \end{aligned}$$

For the third case where the indices $(i, j, k, l) \in C_3$, we have:

$$\begin{aligned}
 & \sum_{i,j,k,l \in C_3} \frac{8! \lambda_i \lambda_j \lambda_k \lambda_l}{D^4 d_{\text{out}}^4 d_{\text{in}}^8} \cdot \max\{|\text{Tr}(X_i^\dagger X_j)|^2, \text{Tr}(X_i^\dagger X_j X_j^\dagger X_i)\} \max\{|\text{Tr}(X_k^\dagger X_l)|^2, \text{Tr}(X_k^\dagger X_l X_l^\dagger X_k)\} \\
 & \leq \sum_{i,j,k,l} \frac{\lambda_i \lambda_j \lambda_k \lambda_l}{D^4 d_{\text{out}}^4 d_{\text{in}}^8} \cdot |\text{Tr}(X_i^\dagger X_j)|^2 \text{Tr}(X_k^\dagger X_l X_l^\dagger X_k) \\
 & = \sum_{i,j,k,l} \frac{\lambda_i \lambda_j \lambda_k \lambda_l}{D^4 d_{\text{out}}^4 d_{\text{in}}^8} \cdot \sum_{x,y} \langle x | X_i^\dagger X_j | x \rangle \langle y | X_j^\dagger X_i | y \rangle \text{Tr}(X_k^\dagger X_l X_l^\dagger X_k) \\
 & = \sum_{i,j,k,l} \frac{\lambda_i \lambda_j \lambda_k \lambda_l}{D^4 d_{\text{out}}^4 d_{\text{in}}^8} \cdot \sum_{x,y} d_{\text{out}}^3 \langle y | A_t^\dagger A_t | x \rangle \langle x | A_t^\dagger A_t | y \rangle d_{\text{out}}^2 \text{Tr}(A_t A_t^\dagger)^2 \text{Tr}(\mathbb{I}) \\
 & \leq \sum_{i,j,k,l} \frac{\lambda_i \lambda_j \lambda_k \lambda_l}{D^4 d_{\text{out}}^4 d_{\text{in}}^8} \cdot d_{\text{out}}^6 \text{Tr}(A_t A_t^\dagger)^4 = \frac{8!}{D^4 d_{\text{out}}^4 d_{\text{in}}^8} d_{\text{out}}^6 d_{\text{in}}^4 = \frac{8!}{d_{\text{in}}^8 d_{\text{out}}^2}.
 \end{aligned}$$

The fourth case, where the indices $(i, j, k, l) \in C_4$, is similar to the previous one.

To sum up, we have

$$\begin{aligned}
 \mathbb{E}(P^2) & \leq \sum_{i,j,k,l} \frac{8! \lambda_i \lambda_j \lambda_k \lambda_l}{D^4 d_{\text{out}}^4 d_{\text{in}}^8} \cdot \max\{|\text{Tr}(X_i^\dagger X_j)|^2, \text{Tr}(X_i^\dagger X_j X_j^\dagger X_i)\} \max\{|\text{Tr}(X_k^\dagger X_l)|^2, \text{Tr}(X_k^\dagger X_l X_l^\dagger X_k)\} \\
 & \leq \frac{4 \times 8!}{d_{\text{in}}^8 d_{\text{out}}^2}.
 \end{aligned}$$

So by the union bound, we have with probability at least $1 - \frac{1}{N} - e^{-d_{\text{in}}/32} \geq \frac{9}{10}$, for all $t \in [N]$:

$$P_u \leq 5 \log^4(N)^4 \sqrt{\mathbb{E}(P_u^2)} \leq 5 \log^4(N) \sqrt{\frac{4 \times 8!}{d_{\text{in}}^8 d_{\text{out}}^2}} \leq \frac{(7 \log(N))^4}{d_{\text{in}}^4 d_{\text{out}}}$$

and $\|u\|_2 \geq \sqrt{d_{\text{in}}/6}$, that is the event \mathcal{E} is satisfied. ■

D.2. Proof of Thm. 7

Theorem 29 *Any incoherent ancilla-assisted adaptive algorithm for testing identity to the depolarizing channel requires, in the worst case,*

$$N = \Omega\left(\frac{d_{\text{in}}^2 d_{\text{out}} + d_{\text{out}}^{1.5}}{\varepsilon^2}\right)$$

measurements.

Proof We use the same construction as in the proof of Thm. 6. Mainly, under the null hypothesis H_0 the quantum channel is $\mathcal{N}(\rho) = \mathcal{D}(\rho) = \text{Tr}(\rho) \frac{\mathbb{I}}{d_{\text{out}}}$. Under the alternate hypothesis H_1 , a quantum channel $\mathcal{N} \sim \mathcal{P}$ has the form:

$$\mathcal{N}(\rho) = \text{Tr}(\rho) \frac{\mathbb{I}}{d_{\text{out}}} + \frac{\varepsilon}{d_{\text{out}}} \langle w | \rho | w \rangle U$$

where $|w\rangle = W|0\rangle$ and $W \sim \text{Haar}(d_{\text{in}})$ and for all $i, j \in [d_{\text{out}}]$, $U_{j,i} = U_{i,j} \sim \mathbf{1}\{i \neq j\} \mathcal{N}_c\left(0, \sigma^2 = \frac{16}{d_{\text{out}}}\right)$ and we condition on the event $\mathcal{G} = \{\|U\|_1 \geq d_{\text{out}}, \|U\|_\infty \leq 32\}$. We call this distribution \mathcal{P} and use the notation $(w, U) \sim \mathcal{P}$. Recall that $\mathbb{P}(\mathcal{G}) \geq 1 - \exp(-\Omega(d_{\text{out}})) - \exp(-\Omega(d_{\text{out}}^2))$ and under \mathcal{G} , the map \mathcal{N} is a valid quantum channel ε -far from the quantum channel \mathcal{D} .

Now, given a set of observations $i_{<t} = (i_1, \dots, i_{t-1})$. The adaptive algorithm \mathcal{A} would choose at step t the input $\rho_t^{i_{<t}}$ and the measurement device $\mathcal{M}_t^{i_{<t}} = \left\{ \lambda_{i_t}^{t, i_{<t}} \left| \phi_{i_t}^{t, i_{<t}} \right\rangle \left\langle \phi_{i_t}^{t, i_{<t}} \right| \right\}_{i_t \in \mathcal{I}_t}$.

Under the null hypothesis H_0 , the quantum channel $\mathcal{N} = \mathcal{D}$ so the probability of the outcomes is exactly:

$$\mathbb{P}_{H_0}^{I_1, \dots, I_N} = \left\{ \prod_{t=1}^N \lambda_{i_t}^{t, i_{<t}} \left\langle \phi_{i_t}^{t, i_{<t}} \right| \text{id} \otimes \mathcal{D}(\rho_t^{i_{<t}}) \left| \phi_{i_t}^{t, i_{<t}} \right\rangle \right\}_{i_1, \dots, i_N}.$$

On the other hand, under the alternate hypothesis H_1 , the probability of the outcomes is exactly:

$$\mathbb{P}_{H_1, (w, U)}^{I_1, \dots, I_N} = \left\{ \prod_{t=1}^N \lambda_{i_t}^{t, i_{<t}} \left\langle \phi_{i_t}^{t, i_{<t}} \right| \text{id} \otimes \mathcal{N}_{(w, U)}(\rho_t^{i_{<t}}) \left| \phi_{i_t}^{t, i_{<t}} \right\rangle \right\}_{i_1, \dots, i_N}$$

Recall that

$$\mathcal{J}_{\mathcal{D}} = \frac{\mathbb{I}}{D} \quad \text{and} \quad \mathcal{J}_{\mathcal{N}} = \frac{\mathbb{I}}{D} + \frac{\varepsilon}{D} |w\rangle\langle w| \otimes U.$$

We can suppose w.l.o.g. that each input state is pure because of the convexity of the KL divergence. For $t \in [N]$ and $i_{<t}$, let $\rho_t^{i_{<t}} = \left| \psi_t^{i_{<t}} \right\rangle \left\langle \psi_t^{i_{<t}} \right|$. Moreover, we can write each rank one input state and measurement vector as follows:

$$\left| \psi_t^{i_{<t}} \right\rangle = A_t^{i_{<t}} \otimes \mathbb{I} \left| \Psi_{d_{\text{in}}} \right\rangle \quad \text{and} \quad \left| \phi_{i_t}^{t, i_{<t}} \right\rangle = B_{i_t}^{i_{<t}} \otimes \mathbb{I} \left| \Psi_{d_{\text{out}}} \right\rangle$$

where $|\Psi_d\rangle = \frac{1}{\sqrt{d}} \sum_{i=1}^d |ii\rangle$ and the matrices $A_t^{i_{<t}} \in \mathbb{C}^{d_{\text{anc}} \times d_{\text{in}}}$ and $B_{i_t}^{i_{<t}} \in \mathbb{C}^{d_{\text{anc}} \times d_{\text{out}}}$ verify:

$$\text{Tr}(A_t^{i_{<t}} A_t^{i_{<t}, \dagger}) = d_{\text{in}} \quad \text{and} \quad \text{Tr}(B_{i_t}^{i_{<t}} B_{i_t}^{i_{<t}, \dagger}) = d_{\text{out}}.$$

Note that we have for all t , $\sum_{i_t} \lambda_{i_t}^{t, i_{<t}} B_{i_t}^{i_{<t}, \dagger} X B_{i_t}^{i_{<t}} = d_{\text{out}} \text{Tr}(X) \mathbb{I}$. Indeed, the condition of the POVM \mathcal{M}_t implies:

$$X \otimes \mathbb{I} = X \otimes \mathbb{I} \sum_{i_t} \lambda_{i_t}^t \left| \phi_{i_t}^t \right\rangle \left\langle \phi_{i_t}^t \right| = \sum_{i_t} \lambda_{i_t}^t X B_{i_t}^t \otimes \mathbb{I} \left| \Psi_{d_{\text{out}}} \right\rangle \left\langle \Psi_{d_{\text{out}}} \right| B_{i_t}^{t, \dagger} \otimes \mathbb{I}$$

hence by taking the partial trace

$$\text{Tr}(X) \mathbb{I} = \frac{1}{d_{\text{out}}} \sum_{i_t, i, j} \lambda_{i_t}^t \langle j | B_{i_t}^{t, \dagger} X B_{i_t}^t | i \rangle | i \rangle \langle j |.$$

Finally

$$\sum_{i_t} \lambda_{i_t}^t B_{i_t}^{t, \dagger} X B_{i_t}^t = d_{\text{out}} \text{Tr}(X) \mathbb{I}.$$

Now we can re-write the distribution of the observations under the null hypothesis as:

$$\begin{aligned}
 \mathbb{P}_{H_0}^{I_1, \dots, I_N} &= \left\{ \prod_{t=1}^N \lambda_{i_t}^t \langle \phi_{i_t}^t | \text{id} \otimes \mathcal{D}(\rho_t) | \phi_{i_t}^t \rangle \right\}_{i_1, \dots, i_N} \\
 &= \left\{ \prod_{t=1}^N \lambda_{i_t}^t \langle \Psi_{d_{\text{out}}} | (B_{i_t}^{t, \dagger} A_t \otimes \mathbb{I}) \mathcal{J}_{\mathcal{D}}(A_t^\dagger B_{i_t}^t \otimes \mathbb{I}) | \Psi_{d_{\text{out}}} \rangle \right\}_{i_1, \dots, i_N} \\
 &= \left\{ \prod_{t=1}^N \frac{\lambda_{i_t}^t}{D} \langle \Psi_{d_{\text{out}}} | (B_{i_t}^{t, \dagger} A_t A_t^\dagger B_{i_t}^t \otimes \mathbb{I}) | \Psi_{d_{\text{out}}} \rangle \right\}_{i_1, \dots, i_N} \\
 &= \left\{ \prod_{t=1}^N \frac{\lambda_{i_t}^t}{D d_{\text{out}}} \text{Tr}(B_{i_t}^{t, \dagger} A_t A_t^\dagger B_{i_t}^t) \right\}_{i_1, \dots, i_N},
 \end{aligned}$$

and under the alternate hypothesis as:

$$\begin{aligned}
 \mathbb{P}_{H_1}^{I_1, \dots, I_N} &= \left\{ \prod_{t=1}^N \lambda_{i_t}^t \langle \phi_{i_t}^t | \text{id} \otimes \mathcal{N}(\rho_t) | \phi_{i_t}^t \rangle \right\}_{i_1, \dots, i_N} \\
 &= \left\{ \prod_{t=1}^N \lambda_{i_t}^t \langle \Psi_{d_{\text{out}}} | (B_{i_t}^{t, \dagger} A_t \otimes \mathbb{I}) \mathcal{J}_{\mathcal{N}}(A_t^\dagger B_{i_t}^t \otimes \mathbb{I}) | \Psi_{d_{\text{out}}} \rangle \right\}_{i_1, \dots, i_N} \\
 &= \left\{ \prod_{t=1}^N \lambda_{i_t}^t \langle \Psi_{d_{\text{out}}} | (B_{i_t}^{t, \dagger} A_t \otimes \mathbb{I}) \left(\frac{\mathbb{I}}{D} + \frac{\varepsilon}{D} |w\rangle\langle w| \otimes U \right) (A_t^\dagger B_{i_t}^t \otimes \mathbb{I}) | \Psi_{d_{\text{out}}} \rangle \right\}_{i_1, \dots, i_N} \\
 &= \left\{ \prod_{t=1}^N \left(\frac{\lambda_{i_t}^t}{D d_{\text{out}}} \text{Tr}(B_{i_t}^{t, \dagger} A_t A_t^\dagger B_{i_t}^t) + \frac{\varepsilon \lambda_{i_t}^t}{D} \langle \Psi_{d_{\text{out}}} | (B_{i_t}^{t, \dagger} A_t |w\rangle\langle w| A_t^\dagger B_{i_t}^t \otimes U) | \Psi_{d_{\text{out}}} \rangle \right) \right\}_{i_1, \dots, i_N}
 \end{aligned}$$

We can express the KL divergence as follows:

$$\begin{aligned}
 &\text{KL} \left(\mathbb{P}_{H_0}^{I_1, \dots, I_N} \parallel \mathbb{P}_{H_1, (w, U)}^{I_1, \dots, I_N} \right) \\
 &= \sum_{i_1, \dots, i_N} \prod_{t=1}^N \frac{\lambda_{i_t}^t}{D d_{\text{out}}} \text{Tr}(B_{i_t}^{t, \dagger} A_t A_t^\dagger B_{i_t}^t) \\
 &\quad \times \log \left(\frac{\prod_{t=1}^N \frac{\lambda_{i_t}^t}{D d_{\text{out}}} \text{Tr}(B_{i_t}^{t, \dagger} A_t A_t^\dagger B_{i_t}^t)}{\prod_{t=1}^N \left(\frac{\lambda_{i_t}^t}{D d_{\text{out}}} \text{Tr}(B_{i_t}^{t, \dagger} A_t A_t^\dagger B_{i_t}^t) + \frac{\varepsilon \lambda_{i_t}^t}{D} \langle \Psi_{d_{\text{out}}} | (B_{i_t}^{t, \dagger} A_t |w\rangle\langle w| A_t^\dagger B_{i_t}^t \otimes U) | \Psi_{d_{\text{out}}} \rangle \right)} \right) \\
 &= \sum_{t=1}^N \mathbb{E}_{\leq N} (-\log) \left(1 + \frac{\frac{\varepsilon \lambda_{i_t}^t}{D} \langle \Psi_{d_{\text{out}}} | (B_{i_t}^{t, \dagger} A_t |w\rangle\langle w| A_t^\dagger B_{i_t}^t \otimes U) | \Psi_{d_{\text{out}}} \rangle}{\frac{\lambda_{i_t}^t}{D d_{\text{out}}} \text{Tr}(B_{i_t}^{t, \dagger} A_t A_t^\dagger B_{i_t}^t)} \right) \\
 &= \sum_{t=1}^N \mathbb{E}_{\leq N} (-\log) \left(1 + \varepsilon \frac{\text{Tr}((B_{i_t}^{t, \dagger} A_t |w\rangle\langle w| A_t^\dagger B_{i_t}^t U))}{\text{Tr}(B_{i_t}^{t, \dagger} A_t A_t^\dagger B_{i_t}^t)} \right)
 \end{aligned}$$

where we use the notation $\mathbb{E}_{\leq N}(X(i_1, \dots, i_N)) = \sum_{i_1, \dots, i_N} \left(\prod_{t=1}^N \frac{\lambda_{i_t}^t}{D d_{\text{out}}} \text{Tr}(B_{i_t}^{t,\dagger} A_t A_t^\dagger B_{i_t}^t) \right) X(i_1, \dots, i_N)$.

Using the inequality $(-\log(1+x)) \leq -x + x^2$ valid for $x \geq -1/2$ and since for $\varepsilon \leq 64$, we have

$\varepsilon \frac{\text{Tr}((B_{i_t}^{t,\dagger} A_t |w\rangle\langle w| A_t^\dagger B_{i_t}^t U))}{\text{Tr}(B_{i_t}^{t,\dagger} A_t A_t^\dagger B_{i_t}^t)} \geq -1/2$, we can upper bound the previous integrand as follows:

$$\begin{aligned} & (-\log) \left(1 + \varepsilon \frac{\text{Tr}((B_{i_t}^{t,\dagger} A_t |w\rangle\langle w| A_t^\dagger B_{i_t}^t U))}{\text{Tr}(B_{i_t}^{t,\dagger} A_t A_t^\dagger B_{i_t}^t)} \right) \\ & \leq \varepsilon \frac{\text{Tr}((B_{i_t}^{t,\dagger} A_t |w\rangle\langle w| A_t^\dagger B_{i_t}^t U))}{\text{Tr}(B_{i_t}^{t,\dagger} A_t A_t^\dagger B_{i_t}^t)} + \varepsilon^2 \frac{\text{Tr}((B_{i_t}^{t,\dagger} A_t |w\rangle\langle w| A_t^\dagger B_{i_t}^t U))^2}{\text{Tr}(B_{i_t}^{t,\dagger} A_t A_t^\dagger B_{i_t}^t)^2}. \end{aligned}$$

Observe that the first term vanishes under the expectation:

$$\begin{aligned} & \mathbb{E}_{\leq N} \left(\varepsilon \frac{\text{Tr}((B_{i_t}^{t,\dagger} A_t |w\rangle\langle w| A_t^\dagger B_{i_t}^t U))}{\text{Tr}(B_{i_t}^{t,\dagger} A_t A_t^\dagger B_{i_t}^t)} \right) \\ & = \mathbb{E}_{\leq t-1} \sum_{i_t} \frac{\lambda_{i_t}^t}{D d_{\text{out}}} \text{Tr}(B_{i_t}^{t,\dagger} A_t A_t^\dagger B_{i_t}^t) \cdot \varepsilon \frac{\text{Tr}((B_{i_t}^{t,\dagger} A_t |w\rangle\langle w| A_t^\dagger B_{i_t}^t U))}{\text{Tr}(B_{i_t}^{t,\dagger} A_t A_t^\dagger B_{i_t}^t)} \\ & = \mathbb{E}_{\leq t-1} \sum_{i_t} \frac{\lambda_{i_t}^t}{D d_{\text{out}}} \cdot \varepsilon \text{Tr}((B_{i_t}^{t,\dagger} A_t |w\rangle\langle w| A_t^\dagger B_{i_t}^t U)) \\ & = \mathbb{E}_{\leq t-1} \frac{\varepsilon}{D} \text{Tr}(A_t |w\rangle\langle w| A_t^\dagger) \text{Tr}(U) = 0 \end{aligned}$$

where we used $\sum_{i_t} \lambda_{i_t}^t B_{i_t}^{t,\dagger} X B_{i_t}^t = d_{\text{out}} \text{Tr}(X) \mathbb{I}$. For the second term, we will instead upper bound its expectation under U . Observe that this term is nonnegative, so we can safely remove the condition on the event \mathcal{G} and then we compute the expectation under Haar distributed vector w and Gaussians $\{U_{i,j}\}$.

$$\begin{aligned} \mathbb{E} \left(\varepsilon^2 \frac{\text{Tr}((B_{i_t}^{t,\dagger} A_t |w\rangle\langle w| A_t^\dagger B_{i_t}^t U))^2}{\text{Tr}(B_{i_t}^{t,\dagger} A_t A_t^\dagger B_{i_t}^t)^2} \right) & \leq \frac{32}{d_{\text{out}}} \varepsilon^2 \mathbb{E} \left(\frac{\langle w | A_t^\dagger B_{i_t}^t B_{i_t}^{t,\dagger} A_t |w\rangle^2}{\text{Tr}(B_{i_t}^{t,\dagger} A_t A_t^\dagger B_{i_t}^t)^2} \right) \\ & \leq \frac{64\varepsilon^2}{d_{\text{out}} d_{\text{in}}^2} \cdot \frac{\text{Tr}(A_t^\dagger B_{i_t}^t B_{i_t}^{t,\dagger} A_t)^2}{\text{Tr}(B_{i_t}^{t,\dagger} A_t A_t^\dagger B_{i_t}^t)^2} = \frac{64\varepsilon^2}{d_{\text{in}}^2 d_{\text{out}}}. \end{aligned}$$

Therefore

$$\begin{aligned} \mathbb{E}_{(w,U) \sim \mathcal{P}} \text{KL} \left(\mathbb{P}_{H_0}^{I_1, \dots, I_N} \parallel \mathbb{P}_{H_1, (w,U)}^{I_1, \dots, I_N} \right) & \leq \sum_{t=1}^N \mathbb{E}_{\leq N} \mathbb{E}_{(w,U) \sim \mathcal{P}} (-\log) \left(1 + \varepsilon \frac{\text{Tr}((B_{i_t}^{t,\dagger} A_t |w\rangle\langle w| A_t^\dagger B_{i_t}^t U))}{\text{Tr}(B_{i_t}^{t,\dagger} A_t A_t^\dagger B_{i_t}^t)} \right) \\ & \leq \sum_{t=1}^N \mathbb{E}_{\leq N} \frac{64\varepsilon^2}{d_{\text{in}}^2 d_{\text{out}}} = \frac{64N\varepsilon^2}{d_{\text{in}}^2 d_{\text{out}}}. \end{aligned}$$

On the other hand, the Data-Processing inequality applied on the KL divergence (see Prop. F.3) writes:

$$\begin{aligned} \mathbb{E}_{(w,U) \sim \mathcal{P}} \text{KL} \left(\mathbb{P}_{H_0}^{I_1, \dots, I_N} \parallel \mathbb{P}_{H_1, (w,U)}^{I_1, \dots, I_N} \right) & \geq \mathbb{E}_{(w,U) \sim \mathcal{P}} \text{KL}(\mathbb{P}_{H_0}(\mathcal{A} = 0) \parallel \mathbb{P}_{H_1, (w,U)}(\mathcal{A} = 0)) \\ & \geq \text{KL}(2/3 \parallel 1/3) = \frac{2}{3} \log(2) - \frac{1}{3} \log(2) = \frac{1}{3} \log(2). \end{aligned}$$

Grouping the lower and upper bounds on the KL divergence:

$$\frac{128N\varepsilon^2}{d_{\text{in}}^2 d_{\text{out}}} \geq \mathbb{E}_{(w,U) \sim \mathcal{P}} \text{KL} \left(\mathbb{P}_{H_0}^{I_1, \dots, I_N} \parallel \mathbb{P}_{H_1, (w,U)}^{I_1, \dots, I_N} \right) \geq \frac{1}{3} \log(2)$$

which yields the lower bound:

$$N = \Omega \left(\frac{d_{\text{in}}^2 d_{\text{out}}}{\varepsilon^2} \right).$$

■

Appendix E. Testing identity of quantum states

In this section, we show how to reduce testing quantum states to testing discrete distributions. The same result with another proof can be found in (Chen et al., 2022f). For a POVM \mathcal{M} and a quantum state ρ , let $\rho(\mathcal{M})$ denotes the classical probability distribution $\{\text{Tr}(\rho M_i)\}_i$. The following lemma captures the main ingredient of the reduction:

Lemma 30 *For all $\delta > 0$, let $l = \frac{1}{4} \log(2/\delta)$ and $U^1, U^2, \dots, U^l \in \mathbb{C}^{d \times d}$ be Haar -random unitary matrices of columns $\left\{ \left| U_i^j \right\rangle \right\}_{1 \leq i \leq d, 1 \leq j \leq l}$, $\mathcal{M} = \left\{ \frac{1}{l} \left| U_i^j \right\rangle \left\langle U_i^j \right| \right\}_{i,j}$ is a POVM and for all quantum states ρ and σ we have with a probability at least $1 - \delta$:*

$$\text{TV}(\rho(\mathcal{M}), \sigma(\mathcal{M})) \geq \frac{\|\rho - \mathbb{I}/d\|_2}{20}.$$

A similar statement can be found in (Matthews et al., 2009) where the authors analyze the uniform POVM and a POVM defined by a spherical 4-designs. However, for our reduction, it is important to minimize the number of outcomes of the POVM.

Proof Let $\xi = \rho - \sigma$, we have $U |e_i\rangle = |U_i\rangle$ and we use Weingarten Calculus 31 and 32 to calculate

$$\begin{aligned} \mathbb{E} \left[\langle U_i | \xi | U_i \rangle^2 \right] &= \mathbb{E} [\langle U_i | \xi | U_i \rangle \langle U_i | \xi | U_i \rangle] = \mathbb{E} [\text{Tr}(\xi |U_i\rangle \langle U_i| \xi |U_i\rangle \langle U_i|)] \\ &= \mathbb{E} [\text{Tr}(\xi U |e_i\rangle \langle e_i| U^* \xi U |e_i\rangle \langle e_i| U^*)] = \mathbb{E} [\text{Tr}(U^* \xi U |e_i\rangle \langle e_i| U^* \xi U |e_i\rangle \langle e_i|)] \\ &= \sum_{\alpha, \beta \in \mathcal{S}_2} \text{Wg}(\beta \alpha^{-1}, d) \text{Tr}_{\beta^{-1}}(\xi, \xi) \text{Tr}_{\alpha}(|e_i\rangle \langle e_i|, |e_i\rangle \langle e_i|) = \frac{1}{d(d+1)} \text{Tr}(\xi^2). \end{aligned}$$

Similarly

$$\begin{aligned} \mathbb{E} \left[\langle U_i | \xi | U_i \rangle^4 \right] &= \mathbb{E} [\langle U_i | \xi | U_i \rangle \langle U_i | \xi | U_i \rangle \langle U_i | \xi | U_i \rangle \langle U_i | \xi | U_i \rangle] \\ &= \mathbb{E} [\text{Tr}(\xi |U_i\rangle \langle U_i| \xi |U_i\rangle \langle U_i| \xi |U_i\rangle \langle U_i| \xi |U_i\rangle \langle U_i|)] \\ &= \mathbb{E} [\text{Tr}(\xi U |e_i\rangle \langle e_i| U^* \xi U |e_i\rangle \langle e_i| U^* \xi U |e_i\rangle \langle e_i| U^* \xi U |e_i\rangle \langle e_i| U^*)] \\ &= \mathbb{E} [\text{Tr}(U^* \xi U |e_i\rangle \langle e_i| U^* \xi U |e_i\rangle \langle e_i| U^* \xi U |e_i\rangle \langle e_i| U^* \xi U |e_i\rangle \langle e_i|)] \\ &= \sum_{\alpha, \beta \in \mathfrak{S}_4} \text{Wg}(\beta \alpha^{-1}, d) \text{Tr}_{\beta^{-1}}(\xi, \xi, \xi, \xi) \text{Tr}_{\alpha}(|e_i\rangle \langle e_i|, |e_i\rangle \langle e_i|, |e_i\rangle \langle e_i|, |e_i\rangle \langle e_i|) \\ &= \frac{1}{d(d+1)(d+2)(d+3)} (6\text{Tr}(\xi^2)^2 + 6\text{Tr}(\xi^4)). \\ &\leq \frac{c'}{d(d+1)(d+2)(d+3)} \text{Tr}(\xi^2)^2. \end{aligned}$$

We can now conclude by Hölder's inequality:

$$\begin{aligned}
 2\mathbb{E}[\text{TV}(\rho(\mathcal{M}), \sigma(\mathcal{M}))] &= \sum_{i=1}^d \mathbb{E}[|\langle U_i | \xi | U_i \rangle|] \geq \sum_{i=1}^d \sqrt{\frac{(\mathbb{E}[\langle U_i | \xi | U_i \rangle^2])^3}{\mathbb{E}[\langle U_i | \xi | U_i \rangle^4]}} \\
 &\geq \sum_{i=1}^d \sqrt{\frac{(d^{-1}(d+1)^{-1} \text{Tr}(\xi^2))^3}{c'd^{-1}(d+1)^{-1}(d+2)^{-1}(d+3)^{-1} \text{Tr}(\xi^2)^2}} \\
 &\geq \sum_{i=1}^d c \frac{\sqrt{\text{Tr}(\xi^2)}}{d} \geq c \sqrt{\text{Tr}(\rho - \sigma)^2}.
 \end{aligned}$$

Let $f(U) = \text{TV}(\rho(\mathcal{M}), \sigma(\mathcal{M}))$, we first show that f is Lipschitz by using the triangle and Cauchy Schwarz inequalities:

$$\begin{aligned}
 2|f(U) - f(V)| &= \left| \sum_{1 \leq i \leq d, 1 \leq j \leq l} \frac{1}{l} |\text{Tr}(|U_i^j\rangle\langle U_i^j| \xi) - \text{Tr}(|V_i^j\rangle\langle V_i^j| \xi)| \right| \\
 &\leq \sum_{1 \leq i \leq d, 1 \leq j \leq l} \frac{1}{l} |\text{Tr}((|U_i^j\rangle\langle U_i^j| - |V_i^j\rangle\langle V_i^j|) \xi)| \\
 &\leq \sum_{1 \leq i \leq d, 1 \leq j \leq l} \frac{1}{l} \sqrt{\text{Tr}(\xi^2)} \sqrt{\text{Tr}((|U_i^j\rangle\langle U_i^j| - |V_i^j\rangle\langle V_i^j|)^2)} \\
 &\leq \sqrt{\frac{d}{l}} \sqrt{\text{Tr}(\xi^2)} \sqrt{\sum_{1 \leq i \leq d, 1 \leq j \leq l} \text{Tr}((|U_i^j\rangle\langle U_i^j| - |V_i^j\rangle\langle V_i^j|)^2)} \\
 &\leq \sqrt{\frac{d}{l}} \sqrt{\text{Tr}(\xi^2)} \sqrt{\sum_{1 \leq j \leq l} \text{Tr}((U^j - V^j)^2)} \\
 &\leq \sqrt{\frac{d}{l}} \sqrt{\text{Tr}(\xi^2)} \|U - V\|_{2, \text{HS}},
 \end{aligned}$$

hence f is $L = \sqrt{\frac{d}{2l}} \sqrt{\text{Tr}(\xi^2)}$ -Lipschitz, therefore by Thm. 34:

$$\mathbb{P}\left(|f(U) - \mathbb{E}(f(U))| > \frac{c}{2} \sqrt{\text{Tr}(\xi^2)}\right) \leq e^{-\frac{dc^2 \text{Tr}(\xi^2)}{48L^2}} = e^{-lc^2/24} = \delta/2,$$

for $l = 24 \log(2/\delta)/c^2$. Finally with high probability (at least $1 - \delta/2$) we have

$$\begin{aligned}
 \text{TV}(\rho(\mathcal{M}), \sigma(\mathcal{M})) &\geq \mathbb{E}(\text{TV}(\rho(\mathcal{M}), \sigma(\mathcal{M}))) - |\text{TV}(\rho(\mathcal{M}), \sigma(\mathcal{M})) - \mathbb{E}(\text{TV}(\rho(\mathcal{M}), \sigma(\mathcal{M})))| \\
 &\geq c \sqrt{\text{Tr}(\xi^2)} - \frac{c}{2} \sqrt{\text{Tr}(\xi^2)} \geq \frac{c}{2} \sqrt{\text{Tr}(\xi^2)}.
 \end{aligned}$$

■

Let $\eta = \|\rho - \mathbb{I}/d\|_2$. Under the alternative hypothesis H_2 , the TV distance between P and U_n can be lower bounded by $\text{TV}(P, U_n) \geq \frac{1}{20} \|\rho - \mathbb{I}/d\|_2$. So Lem. 30 gives a POVM for which

our problem reduces to testing identity: $P = U_n$ vs $\text{TV}(P, U_n) \geq \frac{\eta}{20}$ with high probability, where $n = \frac{1}{4}d \log(2/\delta)$ and $P = \mathcal{M}(\rho)$. Therefore we can apply the classical testing uniform result of (Diakonikolas et al., 2017) to obtain a copy complexity:

$$\mathcal{O}\left(\frac{\sqrt{d} \log(1/\delta)}{\eta^2}\right).$$

Algorithm 3: Testing identity of quantum states in the 2-norm with an error probability at most δ .

$l = \frac{1}{4} \log(2/\delta)$.

Sample $U^1, U^2, \dots, U^l \in \mathbb{C}^{d \times d}$ from Haar(d) distribution.

Let $\left\{ \left| U_i^j \right\rangle \right\}_{1 \leq i \leq d, 1 \leq j \leq l}$ be the columns of the unitary matrices U^1, U^2, \dots, U^l

Measure the quantum state ρ using the POVM $\mathcal{M} = \left\{ \frac{1}{l} \left| U_i^j \right\rangle \left\langle U_i^j \right| \right\}_{i,j}$ and observe

$\mathcal{O}\left(\sqrt{d} \log(1/\delta)/\eta^2\right)$ samples from $\rho(\mathcal{M})$.

Test whether $h_0 : \rho(\mathcal{M}) = U_{ld}$ or $h_1 : \text{TV}(\rho(\mathcal{M}), U_{ld}) \geq \eta/20$ using the testing identity of discrete distributions of (Diakonikolas et al., 2017), with an error probability δ , and answer accordingly.

Appendix F. Technical lemmas

In this section, we group technical lemmas useful for the previous proofs of this article.

F.1. Weingarten Calculus

Since we use generally a uniform POVM, which consists in sampling a Haar -unitary matrix, we need some facts from Weingarten calculus in order to compute Haar -unitary integrals. If π a permutation of $[n]$, let $\text{Wg}(\pi, d)$ denotes the Weingarten function of dimension d . The following lemma is crucial for our results.

Lemma 31 (Gu, 2013) *Let U be a $d \times d$ Haar -distributed unitary matrix and $\{A_i, B_i\}_i$ a sequence of $d \times d$ complex matrices. We have the following formula*

$$\begin{aligned} & \mathbb{E}(\text{Tr}(U B_1 U^* A_1 U \dots U B_n U^* A_n)) \\ &= \sum_{\alpha, \beta \in \mathfrak{S}_n} \text{Wg}(\beta \alpha^{-1}, d) \text{Tr}_{\beta^{-1}}(B_1, \dots, B_n) \text{Tr}_{\alpha \gamma_n}(A_1, \dots, A_n), \end{aligned}$$

where $\gamma_n = (12 \dots n)$ and $\text{Tr}_{\sigma}(M_1, \dots, M_n) = \prod_j \text{Tr}(\Pi_{i \in C_j} M_i)$ for $\sigma = \prod_j C_j$ and C_j are cycles.

We need also some values of Weingarten function:

Lemma 32

- $\text{Wg}((1), d) = \frac{1}{d}$,
- $\text{Wg}((12), d) = \frac{-1}{d(d^2-1)}$,

- $\text{Wg}((1)(2), d) = \frac{1}{d^2-1}$,
- $\text{Wg}((123), d) = \frac{2}{d(d^2-1)(d^2-4)}$,
- $\text{Wg}((12)(3), d) = \frac{-1}{(d^2-1)(d^2-4)}$,
- $\text{Wg}((1)(2)(3), d) = \frac{d^2-2}{d(d^2-1)(d^2-4)}$.

In particular it is known that the sum of the Weingarten function has a closed expression:

Lemma 33 (*Collins et al., 2012*) *Let $d, k \in \mathbb{N}^*$. We have*

$$\sum_{\alpha \in \mathfrak{S}_k} \text{Wg}(\alpha, d) = \frac{1}{d(d+1) \cdots (d+k-1)}.$$

F.2. Concentration inequalities for Haar-random unitary matrices

The following concentration inequality is important for our results.

Theorem 34 (*Meckes et al., 2013*) *Let $M = \mathbb{U}(d)^k$ endowed by the L_2 -norm of Hilbert-Schmidt metric. If $F : M \rightarrow \mathbb{R}$ is L -Lipschitz, then for any $t > 0$*

$$\mathbb{P}(|F(U_1, \dots, U_k) - \mathbb{E}(F(U_1, \dots, U_k))| \geq t) \leq e^{-dt^2/12L^2},$$

where U_1, \dots, U_k are independent Haar-distributed unitary matrices.

F.3. Kullback-Leibler divergence

Definition 35 (Kullback Leibler divergence) *The Kullback Leibler divergence is defined for two distributions P and Q on $[d]$ as*

$$\text{KL}(P\|Q) = \sum_{i=1}^d P_i \log \left(\frac{P_i}{Q_i} \right).$$

We denote by $\text{KL}(p\|q) = \text{KL}(\text{Bern}(p)\|\text{Bern}(q))$.

Kullback-Leibler's divergence is non-negative and satisfies the Data-Processing property:

Proposition 36 (*(Van Erven and Harremos, 2014)*) *Let P, P', Q and Q' distributions on $[d]$, we have*

- **Non negativity** $\text{KL}(P\|Q) \geq 0$.
- **Data processing** *Let X a random variable and g a function. Define the random variable $Y = g(X)$, we have*

$$\text{KL}(P^X\|Q^X) \geq \text{KL}(P^Y\|Q^Y).$$