On Adaptivity in Quantum Testing
Omar Fawzi, Nicolas Flammarion, Aurélien Garivier, Aadil Oufkir

To cite this version:
Omar Fawzi, Nicolas Flammarion, Aurélien Garivier, Aadil Oufkir. On Adaptivity in Quantum Testing. 2023. hal-04107265

HAL Id: hal-04107265
https://hal.science/hal-04107265
Preprint submitted on 26 May 2023

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L’archive ouverte pluridisciplinaire HAL, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d’enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.
On Adaptivity in Quantum Testing

Omar Fawzi
Ens de Lyon
omar.fawzi@ens-lyon.fr

Nicolas Flammarion
EPFL
nicolas.flammarion@epfl.ch

Aurélien Garivier
Ens de Lyon
aurelien.garivier@ens-lyon.fr

Aadil Oufkir
Ens de Lyon
aadil.oufkir@ens-lyon.fr

Abstract

Can adaptive strategies outperform non-adaptive ones for quantum hypothesis selection? We exhibit problems where adaptive strategies provably reduce the number of required samples by a factor four in the worst case, and possibly more when the actual difficulty of the problem makes it possible. In addition, we exhibit specific hypothesis classes for which there is a provable polynomial separation between adaptive and non-adaptive strategies – a specificity of the quantum framework that does not appear in classical testing.

1 Introduction

We consider the hypothesis selection problem using independent measurements, where the tester is asked to determine the hypothesis set containing the unknown quantum state $\rho$ with high probability. This problem is ubiquitous in the quantum learning theory literature, and several variants are considered: testing identity (O’Donnell & Wright, 2015; Bubeck et al., 2020; Chen et al., 2022c), testing closeness (Yu, 2020), binary hypothesis testing (Hiai & Petz, 1991), (Audenaert et al., 2007; Nussbaum & Szkoła, 2009), composite quantum hypothesis testing (Bjelaković et al., 2005). If the tester is limited to independent measurements, the problem is very related to classical testing problems. Indeed, on the one hand, every classical testing problem on discrete distributions can be cast into a quantum testing problem by taking diagonal quantum states corresponding to the discrete distributions. Measuring these quantum states is equivalent to sampling from the classical distributions. On the other hand, the quantum hypothesis selection problem can be seen as a bandit problem (see e.g. (Garivier & Kaufmann, 2019; Lumbreras et al., 2022; Brahmachari et al., 2023)). Born’s rule defines exactly the classical distribution of the reward when pulling a particular arm (performing a measurement). Note that these probability distributions are not arbitrary: they are governed by the unknown quantum state. This connection leads to an important question: Can sequential strategies outperform non-sequential ones for some hypothesis selection problem with independent measurements? In other words, if the tester is allowed to choose the measurement device at a given step depending on the previous observations, would it require fewer copies of the unknown quantum state? Moreover, measurements come with a considerable cost, so we would like to reduce the number of measurements. Besides using entangled measurements which require a large quantum memory, one idea is to focus on independent measurements and try to adapt the new devices according to the accumulated information given by the previous outcomes. This approach has no additional cost because the number of adaptive measurements will be always less than its non adaptive counterpart. Classically, sequential strategies prove to have an advantage over non-sequential ones for instance for binary hypothesis testing problems (see (Wald, 1945)), testing continuous distributions (see (Zhao et al., 2016; Balasubramani & Ramdas, 2015)), testing identity and closeness problems with small alphabet size (see (Fawzi...
This speedup comes, mainly, from the fact that a sequential algorithm can make comparisons at each step and can respond earlier because it has the enough confidence. However, sequential strategies in the quantum setting have not only the capacity to choose the stopping time, but also to change the measurement devices adaptively. We expect then a larger gap between sequential and non-sequential strategies. To avoid confusion, sequential strategies can choose the stopping time according to the previous observations and thus they have random stopping times, while adaptive strategies are allowed to adapt their measurement devices at each step according to past observations. With these definitions, a strategy can be sequential and adaptive, sequential and non-adaptive, non-sequential and adaptive, or non-sequential and non-adaptive. When we don’t specify whether the strategy is non-sequential or sequential (resp. non-adaptive or adaptive), it can be both and the statement remains true.

On the other hand, non-adaptive strategies have been shown to be optimal for many interesting quantum testing problems, including testing identity by Chen et al. (2021), purity testing and shadow tomography by Chen et al. (2021), tomography by Chen et al. (2022b). These works suggest that adaptive/sequential strategies cannot outperform non-adaptive non-sequential ones. The goal of the article is to show the contrary: there are some situations where sequential or adaptive strategies require fewer measurements than non-adaptive non-sequential ones.

Let $d$ be the dimension of quantum states, $\varepsilon > 0$ be the precision parameter and $\delta \in (0, 1/2)$ be the error probability.

**Contributions** When the number of hypotheses $m$ is equal to 2 and the hypotheses are simple (i.e., only one possible state), we can precisely characterize the optimal worst case complexity for non-sequential and sequential strategies. We show that sequential strategies outperform non-sequential ones by a factor 4. For the lower bounds, we show how to reduce this problem to the classical testing identity problem, then apply the lower bounds of Fawzi et al. (2022). For the sequential upper bound, we design stopping rules inspired by time uniform concentration inequalities.

Moreover, we show that sequential algorithms can adapt to the actual difficulty for the testing mixedness and testing closeness problems. For this, we show a lower bound on the TV-distance between the probability distributions after measurement depending on the actual 1-norm between the quantum states (see Lemma 3.5). This inequality helps to reduce quantum testing to classical testing at the cost of a factor $1/\sqrt{d}$ and can be useful for other applications.

For a number of hypotheses $m \geq 2$, we prove a separation between adaptive and non-adaptive strategies for a specific problem. The learner has the information that the unknown quantum state can be diagonalized in a basis amongst $m$ known orthonormal bases and would like to approximate it. We show that this problem can be solved by adaptive algorithms using $O(d \log(m)/\varepsilon^2)$ copies of $\rho$. On the other hand, every non-adaptive algorithm solving this problem will require $\Omega(\min\{md/\log(m)\varepsilon^2, d^2/\varepsilon^2\})$ copies of $\rho$. The upper bounds follow from the shadow tomography algorithm of Huang et al. (2020). For the lower bounds, we construct an $\varepsilon$-separated family of quantum states close to the maximally mixed state $(I/d)$ and use it to encode a message from $[me^{\log(d)}]$. A learning algorithm can be used to decode this message with the same success probability. Hence, the encoder and decoder should share at least $\Omega(\log(m) + d)$ bits of information (Fano’s inequality [Fano 1961]). On the other hand, after each step, we show that the correlation between the encoder and decoder can only increase by at most $O(\varepsilon^2 \log(m)/m + \varepsilon^2/d)$ bits for non-adaptive strategies and it can only increase by at most $O(\varepsilon^2)$ bits for adaptive strategies. We obtain an improvement by a factor $d$ or $m/\log(m)$ for non-adaptive strategies by exploiting the randomness in the construction and the independence of the observations at different steps.

**Related work** Quantum testing identity using entangled measurements is well understood (O’Donnell & Wright 2015; Bădescu et al. 2019): it is known that $\Theta(d/\varepsilon^2)$ copies are necessary and sufficient. For independent measurements, it starts with the work of Bubeck et al. (2020) where we have two different lower bounds for testing mixedness problem using independent adaptive and non-adaptive measurements. This result is generalized for general testing identity to some quantum state $\sigma$ by Chen et al. (2022c). Recently Chen et al. (2022a) show that adaptive algorithms cannot significantly outperform non-adaptive ones neither for testing mixedness nor testing identity.

If entangled measurements are allowed, the quantum hypothesis selection problem can be solved using $\poly(\log(m))$ copies of $\rho$ (see Bădescu & O’Donnell 2021). This poly-logarithmic complexity in $m$ can
be explained by the fact that $\rho^{\otimes N}$ can be reused after measurement. In contrast, this is not possible using independent measurement for which the state collapses after performing the measurement. In general, the quantum hypothesis selection problem, where each hypothesis contains only one quantum state, is highly related to the shadow tomography problem where the learner is asked to uniformly approximate the expected values $\{\text{tr}(pO_i)\}_{i \in [m]}$ of $m$ known observables $\{O_i\}_{i \in [m]}$ by measuring the unknown quantum state $\rho$. A popular algorithm for the shadow tomography problem is given by [Huang et al., 2020] and uses at most $O(\log(m)d/\varepsilon^2)$ non-sequential non-adaptive independent measurements. On the other hand, independent adaptive strategies are shown to be useless for shadow tomography (and purity testing) by [Chen et al., 2021]. Moreover, sequential adaptive strategies have been used by [Li et al., 2022b] (see [Li et al., 2022a] for quantum channel discrimination) to achieve the optimal rates given by the quantum relative entropy for both type I and type II errors at the same time for binary hypothesis testing problem using entangled measurements.

Adaptive strategies have been considered for testing quantum channels in [Harrow et al., 2010; Pirandola et al., 2019; Salek et al., 2022]. In particular, [Harrow et al., 2010] and [Salek et al., 2022] provide examples for which adaptive strategies outperform non-adaptive ones for testing quantum channels. We note that for channels, one has the possibility to adapt the input of the channel to the previous observations, but this is not the case for testing states. As such, it is more challenging to find a separation between adaptive and non-adaptive strategies for testing quantum states than it is for channels.

Finally, for the tomography problem, [Chen et al., 2022b] shows that adaptive independent strategies cannot beat non-sequential non-adaptive ones and thus need at least $\Omega(d^3/\varepsilon^2)$ copies to learn the quantum state $\rho$. However, it is unclear whether adaptivity can help for learning restricted families of states such as graph states [Ouyang & Tomamichel, 2022]. On the other hand, sequential strategies were used for (online) state tomography by [Kueng & Ferrie, 2015; Youssry et al., 2019; Stricker et al., 2022; Rambach et al., 2022].

2 Preliminaries

Throughout the paper, $d$ is the dimension of the quantum states. A quantum state is a positive semi-definite Hermitian matrix of trace 1. We use the bra-ket 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 $\phi$ and $\psi$ and, for a unit vector $|\phi\rangle$, $|\phi\rangle \langle \phi |$ is the rank-1 projector on the space spanned by the vector $\phi$. The canonical basis $\{|e_i\rangle\}_{i \in [d]}$ is denoted $\{|i\rangle\}_{i \in [d]}$. We define the trace norm or the 1-norm of a matrix $M$ as $\|M\|_1 = \frac{1}{2} \text{tr}(\sqrt{M^\dagger M})$ and the 2-norm as $\|M\|_2 = \sqrt{\text{tr}(M^\dagger M)}$. An observable is a Hermitian matrix $O$ satisfying $O \succeq 0$ and $I - O \succeq 0$ where $I$ is the identity matrix. Given two quantum states $\rho$ and $\sigma$, we can compare them using the quantum relative entropy defined as:

$$D(\rho||\sigma) = \text{tr}(\rho(\log(\rho) - \log(\sigma)))$$

or the quantum Chernoff divergence defined as:

$$C(\rho,\sigma) = -\log \left( \inf_{0 \leq s \leq 1} \text{tr}(\rho^{1-s}\sigma^s) \right).$$

The total variation (TV) distance between two probability distributions $P$ and $Q$ on $[d]$ is defined as:

$$TV(P,Q) = \frac{1}{2} \sum_{i=1}^{d} |P_i - Q_i|$$

and the Kullback-Leibler (KL) divergence is defined as:

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

Finally, for two number $p, q \in [0,1]$, we denote $KL(p||q) = KL(\text{Ber}(p)||\text{Ber}(q))$.

All the problems discussed in this article are special cases of the general hypothesis selection problem. Given an unknown quantum state $\rho \in \mathbb{C}^{d \times d}$ and $m$ hypothesis classes $\{H_i\}_{i \in [m]}$, the learner is asked to find one of
the hypothesis classes containing $\rho$ with high probability. Formally, we have the promise that at least one of the following assertions is satisfied:

$$\rho \in H_1, \rho \in H_2, \ldots, \rho \in H_m.$$ 

An algorithm $\mathcal{A}$ is $\delta$-correct for this problem if it verifies the following property:

$$\forall i \in [m] : \rho \notin H_i \implies \Pr(\mathcal{A} = i) \leq \delta.$$ 

The difference between quantum and classical testing is that in the quantum case we have the possibility to choose a measurement (given by positive operators summing to the identity). If the quantum states are restricted to be diagonal, we may assume the measurement is always the same and so the problem becomes a classical testing problem (see Lemma 3.2).

The quantum state $\rho$ is unknown, but the learner can extract classical information from it by performing a measurement. The way the unknown quantum state $\rho$ is measured is important and can lead to different results about the number of copies needed for this task. A 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 $\mathcal{M} = \{M_i\}_{i \in \mathcal{X}}$ acting on a Hilbert space $\mathcal{H}$ and satisfying $\sum_{i \in \mathcal{X}} M_i = \mathbb{I}_\mathcal{H}$. Each element $M_i$ in the POVM $\mathcal{M}$ is associated with the outcome $i \in \mathcal{X}$. The tuple $\{\text{tr}(\rho M_i)\}_{i \in \mathcal{X}}$ is non-negative and sums to 1: it thus defines a probability denoted by $\rho(\mathcal{M})$. Born’s rule (Born, 1926) says that the probability that the measurement on a quantum state $\rho$ using the POVM $\mathcal{M}$ will output $i$ is exactly $\text{tr}(\rho M_i)$. We distinguish between two types of measurements depending on the considered Hilbert space:

1. An entangled measurement is given by a POVM on the Hilbert space $\mathcal{H} = (\mathbb{C}^d)^{\otimes N}$, where $N$ is the number of copies available of the quantum state $\rho$. We can measure the whole state $\rho^{\otimes N}$ at once. An interesting POVM related to the observable $O$ on $\mathbb{C}^d$ is given by $\mathcal{M}(O) = \{M_k\}_{0 \leq k \leq N}$ where $M_k = \sum_{x \in \{0, 1\}^N, |x| = k} O^{x_1} \otimes \cdots \otimes O^{x_N}$. Measuring $\rho^{\otimes N}$ with the POVM $\mathcal{M}(O)$ outputs a sample from the binomial distribution $\text{Bin}(n, \text{tr}(\rho O))$.

2. An independent (or incoherent) measurement is given by a sequence of POVMs $\{M_t\}_{t \in [N]}$, each of them acts on the Hilbert space $\mathcal{H} = \mathbb{C}^d$. In this case, we measure at step $t$ the quantum state $\rho$ using the POVM $M_t$. For instance, for an observable $O$, measuring $\rho$ with the POVM $\mathcal{M}(O) = (\mathbb{I} - O, O)$ outputs a sample from the Bernoulli distribution $\text{Ber}(\text{tr}(\rho O))$. If the POVMs $\{M_t\}_t$ are fixed in advance (i.e., do not depend on the outcomes of the previous measurements), the procedure is called non-adaptive; when $M_t$ can be chosen depending on the results of the previous measurements with the $(M_t)_{s<t}$, we call it an adaptive algorithm. If the number of measurements is not fixed beforehand and can be chosen as a function of the previous measurement outcomes, the algorithm is called sequential and has a random stopping time $N$. In this case, the expected copy complexity of the procedure is $E(N)$. Otherwise, the algorithm has a fixed number of measurements $N$ and is called non-sequential.

In this article, we focus on algorithms using independent measurements and our goal is to assess the potential improvement of sequential/adaptive algorithms over non-adaptive non-sequential ones.

3 Sequential improvement for problems involving two hypotheses

In this section, we focus on sequential algorithms for problems having only two hypotheses ($m = 2$), which can be simple or not. The results of this Section are true for either adaptive and non-adaptive settings.

3.1 Provable constant improvement of sequential strategies

The simplest case for hypothesis selection problem with $m = 2$ corresponds to hypothesis sets containing only one known quantum state. Formally, the learner would like to distinguish two hypothesis: $H_1 = \{\sigma_1\}$ and $H_2 = \{\sigma_2\}$. We want to characterize the exact number of copies the learner needs to solve this problem using sequential and non-sequential independent measurements.
Proposition 3.1. \[\|\sigma_1 - \sigma_2\|_\text{tr} = \text{tr}((\sigma_1 - \sigma_2)O)\].

The tester knows the quantum states \(\sigma_1\) and \(\sigma_2\) and can hence calculate the actual 1-norm between them, denoted by \(\varepsilon = \|\sigma_1 - \sigma_2\|_\text{tr}\). The optimal POVM to distinguish between \(\sigma_1\) and \(\sigma_2\) is thus given by \(\mathcal{M} = (I - O, O)\) (Holevo-Helstrom theorem, see [Watrous 2018]) where \(0 \ll O \ll I\) satisfies \[\varepsilon = \|\sigma_1 - \sigma_2\|_\text{tr} = \text{tr}((\sigma_1 - \sigma_2)O)\].

The latter inequality follows from Pinsker’s inequality ([Fedotov et al. 2003]). Note that this previous upper bound is optimal in the worst case setting where we fix \(\varepsilon\) and take the infimum over all \(\sigma_1\) and \(\sigma_2\) satisfying \(\|\sigma_1 - \sigma_2\|_\text{tr} = \varepsilon\). This first result is summarized in the following proposition:

Proposition 3.1. There is a non-sequential algorithm for testing \(H_1 : \rho = \sigma_1\) vs \(H_2 : \rho = \sigma_2\) using a number of measurements

\[N \leq \frac{2\log(1/\delta)}{\varepsilon^2}\].

Moreover, there exists two quantum states \(\sigma_1\) and \(\sigma_2\) satisfying \(\|\sigma_1 - \sigma_2\|_\text{tr} = \varepsilon\) so that every non-sequential algorithm distinguishing between \(H_1 : \rho = \sigma_1\) and \(H_2 : \rho = \sigma_2\) needs a number of measurements satisfying

\[\liminf_{\delta \to 0} \frac{N}{\log(1/\delta)} \geq \max \left\{ \frac{\log(1/\delta)}{\text{KL}(1/2 + \alpha \varepsilon/1/2)} , \frac{1}{\text{KL}(1/2 - \beta \varepsilon/1/2)} \right\} \sim \frac{2}{\varepsilon^2}\,

where \(\alpha \in (0,1)\) and \(\beta \in (0,1)\) are defined such that \(\text{KL}(1/2 + \alpha \varepsilon/1/2) = \text{KL}(1/2 + \alpha \varepsilon/1/2 + \varepsilon)\) and \(\text{KL}(1/2 - \beta \varepsilon/1/2) = \text{KL}(1/2 - \beta \varepsilon/1/2 - \varepsilon)\).

For the lower bound, construct two quantum states, \(\sigma_1 = \mathbb{I}/2\) and \(\sigma_2\) an \(\varepsilon\) perturbation of it. For each POVM, we show that the optimal sample complexity is at least \(\frac{2\log(1/\delta)}{\varepsilon^2}\) (when \(\varepsilon \to 0\)), with equality if the POVM is the optimal one defined in Eq. (1). This reduction can be proven using the following lemma on measurements of diagonal quantum states.

Lemma 3.2. Let \(\mathcal{D}_1\) and \(\mathcal{D}_2\) be two discrete distributions and \(\rho_1\) and \(\rho_2\) their corresponding diagonal quantum states. Let \(\mathcal{M}\) be a POVM. Measuring the quantum state \(\rho_1\) (resp. \(\rho_2\)) with the POVM \(\mathcal{M}\) can be seen as post-processing (independent of the quantum states) of samples from the distribution \(\mathcal{D}_1\) (resp. \(\mathcal{D}_2\)).

Hence, for each POVM, measuring the constructed quantum states \(\sigma_1\) and \(\sigma_2\) is a post-processing of samples from \(\mathcal{D}_1 = \text{Ber}(1/2)\) and \(\mathcal{D}_2 = \text{Ber}(1/2 + \varepsilon)\). Note that this reduction (and the lower bound) works even for entangled strategies. Once the reduction to classical testing identity is done, we can invoke the lower bound of [Fawzi et al. 2022]. The proof is deferred to App. A.1.

3.1.2 Sequential strategies

If we allow the tester to adapt the measurements and choose its stopping time according to previous observations, it can outperform (in expectation) every non-sequential algorithms by a factor 4. Precisely, it can be proven that an expected number of measurements asymptotically equivalent to \(\frac{\log(1/\delta)}{\varepsilon^2}\) is sufficient to distinguish between \(H_1 : \rho = \sigma_1\) and \(H_2 : \rho = \sigma_2\) with probability at least \(1 - \delta\). We use again the optimal POVM \(\mathcal{M}\) defined in Eq. (1) to distinguish between \(\sigma_1\) and \(\sigma_2\). Let \(X_1, \ldots, X_t \sim \text{Ber}(\text{tr}(\rho O))\) the outcomes...
of measuring $\rho$ by the POVM $\mathcal{M}$. Let $S_t = \frac{1}{t} \sum_{i=1}^{t} X_i$ the empirical mean until the time $t$. Contrary to the algorithm described in the previous subsection, a sequential algorithm can make comparisons at each time $t$ until the tester is confident enough to answer the correct answer $H_1$ or $H_2$. Under $H_1$, the statistic $S_t$ has an expected value $\text{tr}(\sigma_1)$. On the other hand, under $H_2$, the statistic $S_t$ has an expected value $\text{tr}(\sigma_2)$. These expected values are known to the tester, so it can compare at each time the statistic $S_t$ with two thresholds: $\text{tr}(\sigma_1) - \phi(\delta, t)$ and $\text{tr}(\sigma_2) + \phi(\delta, t)$ where $\phi(\delta, t)^2 = \frac{1}{\delta} \log \left( \frac{2^{t(t+1)}}{\delta} \right)$. If $S_t \leq \text{tr}(\sigma_1) - \phi(\delta, t)$, the tester can answer $H_2$ confidently. Similarly, it would answer $H_1$ if $S_t \geq \text{tr}(\sigma_2) + \phi(\delta, t)$. However if none of these inequalities is verified it does not answer and makes a new measurement, and so forth until the regions defined by the thresholds coincide. The idea of comparing the statistic with time dependent thresholds has been previously used for classical sequential testing by (Balsubramani & Ramdas, 2015; Fawzi et al., 2021, 2022). In these latter articles, it is proven that in expectation this algorithm outperform the non sequential one by a factor 4. We adapt their result to the quantum setting in the following proposition.

**Proposition 3.3.** There is a sequential algorithm for testing $H_1 : \rho = \sigma_1$ vs $H_2 : \rho = \sigma_2$ using an expected number of measurements:

$$E(N) \leq \frac{\log(1/\delta)}{2\varepsilon^2} + \frac{\log(1/\delta)^{2/3} + 2 \log(1/\delta)^{1/3} + \log(\log(1/\delta)/2\varepsilon^2) + 1}{\varepsilon^2}.$$ 

Moreover, there are two quantum states $\sigma_1$ and $\sigma_2$ satisfying $\|\sigma_1 - \sigma_2\|_1 = \varepsilon$ so that every sequential algorithm distinguishing between $H_1 : \rho = \sigma_1$ and $H_2 : \rho = \sigma_2$ needs a number of measurements satisfying:

$$E(N) \geq \frac{\log(1/\delta)}{\min \{\text{KL}(1/2 \pm \varepsilon || 1/2)\}} \sim 0 \frac{1}{2\varepsilon^2}.$$ 

Note that the expected stopping time is the most natural figure of merit for the sample complexity of sequential algorithms. Moreover, using the same analysis for the algorithm, one can also obtain similar bounds on the number of measurements with high probability.

Observe that the upper bound admits the asymptotic limit $\limsup_{\delta \to 0} \frac{E(N)}{\log(1/\delta)} \leq \frac{1}{2\pi}$ hence $\frac{\log(1/\delta)}{2\varepsilon^2}$ is asymptotically the worst-case optimal complexity of discriminating between two quantum states at the limit $\delta, \varepsilon \to 0$. The correctness of the algorithm presented here is proved using the following time uniform concentration inequality which is an application of union bound and Hoeffding’s inequality (Hoeffding, 1963):

$$\mathbb{P} \left( \exists t \geq 1 : |S_t - \mathbb{E}(S_t)| > \phi(\delta, t) \right) \leq \delta$$

where $\phi(\delta, t) = \frac{1}{\delta} \log \left( \frac{2^{t(t+1)}}{\delta} \right)$.

The lower bound follows from the previous proof’s reduction and the lower bound on the expected number of samples for testing uniform using sequential algorithms: $\text{Ber}(1/2)$ vs $\text{Ber}(1/2 \pm \varepsilon)$ (see Fawzi et al., 2022). The detailed proof can be found in App. A.1.

Note that Li et al. (2022b) have also established an advantage of sequential adaptive strategies over non-adaptive non-sequential ones in terms of the error exponents. The type I error is the probability that the testing algorithm answers the hypothesis $H_1$ while the hypothesis $H_0$ is the correct one while the type II error is the probability that the testing algorithm answers the hypothesis $H_0$ while the hypothesis $H_1$ is the correct one:

$$\alpha_N = \mathbb{P}_{H_0}(A_N = 1) \quad \text{and} \quad \beta_N = \mathbb{P}_{H_1}(A_N = 0)$$

where $N$ is the number of copies used. The error exponents (rates) are then given by

$$R_0 = \lim_{N \to \infty} - \frac{\log(\alpha_N)}{N} \quad \text{and} \quad R_1 = \lim_{N \to \infty} - \frac{\log(\beta_N)}{N}.$$ 

Concretely, Li et al. (2022b) show that adaptive sequential strategies can achieve the best rates (at the same time) given by the quantum relative entropy between two states for both type I and II errors. On the other
hand, it is known that non sequential non adaptive strategies can only achieve the quantum Chernoff rate exponent when the error probabilities are equal \cite{Nussbaum2009,Andenaert2007}. For the particular states \( \sigma_1 = \frac{1}{d} \) and \( \sigma_2 = \text{diag}(\frac{1}{2} + \varepsilon, \frac{1}{2} - \varepsilon) \), we can show that the quantum relative entropy and the quantum Chernoff divergence between \( \sigma_1 \) and \( \sigma_2 \) are asymptotically equivalent to:

\[
D(\sigma_1 || \sigma_2), D(\sigma_2 || \sigma_1) \sim 2\varepsilon^2 \quad \text{and} \quad C(\sigma_1, \sigma_2) \sim \frac{\varepsilon^2}{2}.
\]

Therefore, we can recover the factor 4 improvement by comparing the quantum relative entropy and the quantum Chernoff divergence:

\[
\frac{D(\sigma_1 || \sigma_2)}{C(\sigma_1, \sigma_2)}, \frac{D(\sigma_2 || \sigma_1)}{C(\sigma_1, \sigma_2)} \sim \frac{2\varepsilon^2}{\varepsilon^2} = 4.
\]

We refer to App. A.1.3 for the detailed computations.

### 3.2 Sequential strategies adapt on the actual difficulty of the problem without prior knowledge

In this section, we change the previous setting by letting the second hypothesis be multiple. Precisely, \cite{Chen2022} has proved that the optimal non-sequential adaptive copy complexity is \( \Theta(d^{3/2}/\varepsilon^2) \). We show that while non-sequential adaptive algorithms cannot improve the copy complexity, sequential non-adaptive algorithms can be used to adapt to the actual difficulty of the problem. Mainly we show the following result:

**Proposition 3.4.** There is a sequential algorithm for testing identity problem using a number of measurements satisfying:

\[
\mathbb{E}(N) = O \left( \min \left\{ \frac{d^{3/2} \log(1/\delta)}{\varepsilon^2}, \frac{d^{1/2} \log(1/\delta)}{\| \rho - \mathbb{I}/d \|_F^2} \right\} \right).
\]

In particular, the expected copy complexity can be reduced to \( O(rd^{1/2} \log(1/\delta)) \) if the quantum state \( \rho \) has low rank \( r \leq d/2 \) or \( O \left( \frac{rd^{1/2} \log(1/\delta)}{\| \rho - \mathbb{I}/d \|_F^2} \right) \) if the trace-less matrix \( \rho - \mathbb{I}/d \) has low rank \( r \) even if the algorithm does not have any information about these ranks (see App. A.2). The algorithm uses random measurements and a time-dependent stopping rule. Since we have already sequential algorithms for the classical testing identity problem, it is sufficient to show how to reduce the quantum problem to the classical one. For a POVM \( \mathcal{M} \) and a quantum state \( \rho \), 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 3.5.** For all \( \delta > 0 \), let \( l = \frac{1}{4} \log(2/\delta) \) and \( U^1, U^2, \ldots, U^l \in \mathbb{C}^{d \times d} \) be Haar-random unitary matrices of columns \( \{ U_i^j \}_{1 \leq i \leq d, 1 \leq j \leq l} \), \( \mathcal{M} = \{ \{ U_i^1 \} \} \) is a POVM and for all quantum states \( \rho \) and \( \sigma \) we have with a probability at least \( 1 - \delta \):

\[
\text{TV}(\rho(\mathcal{M}), \sigma(\mathcal{M})) \geq \frac{\| \rho - \mathbb{I}/d \|_2}{20} \geq \frac{\| \rho - \sigma \|_F}{20 \sqrt{r}},
\]

where \( r \) is the rank of \( \rho - \sigma \).

It is, in general, difficult to compute the expected value of the 1-norm under Haar measure, but the 2 and 4-norms can be computed exactly with the Weingarten calculus (see Lemma D.1 and Lemma D.2), so we use Hölder’s inequality to lower bound the 1-norm by an expression involving the 2 and 4-norms. Moreover, this will only give a lower bound in expectation, so we sample more Haar-distributed unitaries and construct a new measurement device by concatenating a fraction of the columns of each unitary. Then, we need to show that the TV-distance is Lipschitz to be able to apply a concentration inequality for functions of Haar-distributed unitaries (Theorem D.3). This is done by carefully applying the Cauchy Schwarz inequality. The complete proof can be found at App. A.2 \cite{Sen2006} proved a slightly weaker (by a logarithmic factor)
lower bound on the TV distance using a POVM constructed with Gaussian random variables. Also, a similar lower bound (in expectation) 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.

Lemma 3.5 gives a POVM for which our problem reduces to testing identity: $P = U_n$ vs $TV(P, U_n) \geq \frac{\varepsilon}{20\sqrt{d}}$ with high probability, where $n = \frac{1}{4} d \log(2/\delta)$ and $P = \mathcal{M}(\rho)$. Under the alternative hypothesis $H_2$, the TV distance between $P$ and $U_n$ can be lower bounded by $TV(P, U_n) \geq \frac{1}{d} \|\rho - I/d\|_2$. Therefore we can apply the sequential classical testing uniform result of [Fawzi et al., 2022] to obtain a copy complexity $O\left(\frac{d^{3/2} \log(1/\delta)}{\max\{\varepsilon^2, d \|\rho - I/d\|_2^2\}}\right)$.

A matching lower bound can be obtained in the worst case setting where we are interested only in the parameters $d$, $\varepsilon$ and $\|\rho - I/d\|_{tr}$. This can be done using Markov’s inequality to transform the algorithm to a deterministic-time one then invoking the lower bound of [Chen et al., 2022]: Any adaptive algorithm for testing identity would require $\Omega(d^{3/2}/\varepsilon^2)$ copies of $\rho$.

Note that, using Lemma 3.5 and the sequential tester of [Fawzi et al., 2022], we obtain the same copy complexity for testing closeness (i.e., testing $\rho = \sigma$ vs $\|\rho - \sigma\|_{tr} \geq \varepsilon$ where we can measure the unknown quantum states $\rho$ and $\sigma$) as for testing identity. This is different from the classical case where testing identity [Diakonikolas et al., 2017] can be done with much less copies than testing closeness [Diakonikolas et al., 2020].

4 Provable separation between adaptive and non-adaptive strategies

In this section, we focus only on non-sequential algorithms meaning that the number of measurements is always deterministic.

We construct a problem for which we have a separation between adaptive and non-adaptive algorithms. Let $\{\sigma_1, \ldots, \sigma_m\}$ be a set of $\varepsilon$-separated known quantum states. The unknown quantum state $\rho$ is $\varepsilon/3$-close to (at most) one of the quantum states $\sigma_i \in \{\sigma_1, \ldots, \sigma_m\}$ and has the same diagonalisation basis than $\sigma_i$.

We aim to learn the quantum state $\rho$ to within $\varepsilon/10$ with high probability. Formally, the goal is to design an algorithm that measures a number of copies of $\rho$ and returns a quantum state $\hat{\rho}$ (an $\varepsilon/10$-approximation of $\rho$) such that with probability (the randomness comes from the measurements and possibly the algorithm) at least $1 - \delta$:

$$\|\hat{\rho} - \rho\|_{tr} \leq \frac{\varepsilon}{10}.$$ 

The problem described above is not a hypothesis selection problem in the strict sense of the term. However it is equivalent to the following hypothesis selection problem which has the same order of copy complexity. For $i \in [m]$, let $\sigma_i = \sum_k \lambda_k |\phi_k^i\rangle\langle\phi_k^i|$ and $\{\sigma_{i,j}\}_{j \in [M]}$ an $\varepsilon/10$-covering of the set $\{\rho = \sum_k \mu_k |\phi_k^i\rangle\langle\phi_k^i| : TV(\lambda, \mu) \leq \varepsilon/3\}$. Our problem is equivalent to the hypothesis selection problem for $\{H_{i,j} = \{B(\sigma_{i,j}, \varepsilon/10)\} \cap \rho : \rho \sigma_{i,j} = \sigma_{i,j}\rho\}_{i \in [m], j \in [M]}$. For simplicity, we use the first formulation of the problem and refer to it as $(P)$.

4.1 Upper bound

In this section, we present an adaptive algorithm for the problem $(P)$ achieving a copy complexity strictly less than the lower bound which holds for all non-adaptive algorithms. The first step is to determine with high probability the closest quantum state $\sigma_i$ to $\rho$, then it remains to approximate $\rho$ by measuring it in its basis of diagonalization.

4.1.1 Adaptive strategies.

For all $i \neq j \in [m]$ let $O_{i,j}$ an observable satisfying $\|\sigma_i - \sigma_j\|_{tr} = \text{tr} O_{i,j}(\sigma_i - \sigma_j)$. In Sec 3.1 we have seen that such observable $O_{i,j}$ can be used to distinguish between $\rho = \sigma_i$ and $\rho = \sigma_j$ if one of the two hypotheses is satisfied. The quantum state $\sigma_i$ has the property to minimize the 1-norm between $\rho$ and $\{\sigma_i\}_i$, so it is
Algorithm 1 Hypothesis selection problem $(P)$. 

**Input:** $N = O(d \log(m/\delta)/\varepsilon^2)$ independent measurement on $\rho$ and $m$ quantum states $\sigma_1, \ldots, \sigma_m$.

**Output:** Two quantum states $\sigma_i$, and $\tilde{\rho}$ satisfying with a probability at least $1 - \delta$: $\|\sigma_i - \rho\|_{tr} \leq \varepsilon/10$.

For all $i \neq j \in [m]$, let $O_{i,j}$ an observable satisfying $\|\sigma_i - \sigma_j\|_{tr} = \text{tr}(O_{i,j}(\sigma_i - \sigma_j))$.

For all $i \neq j \in [m]$, let $\mu_{i,j}$ an $\varepsilon/10$ approximation of $\text{tr}(\rho O_{i,j})$ given by classical shadow tomography of (Huang et al., 2020).

Let $k^* = \arg\min_{k} \max_{i,j} \mu_{i,j} - \text{tr}(\sigma_i O_{i,j})$.

Let $\mathcal{M} = \{|\phi_i\rangle\langle\phi_i|\}_{i \in [d]}$ the POVM corresponding to the basis of diagonalisation of $\sigma_k$.

Measure $\rho$ independently $M = 200 \log(2^{d+2}/\delta)/\varepsilon^2$ times using the POVM $\mathcal{M}$ and denote the outcomes $\{E_i\}_{1 \leq i \leq M}$.

return $\tilde{\rho} = \sum_{i \in [d]} \left( \sum_{l \in [M]} \frac{1_{E_j = i}}{M} \right) |\phi_i\rangle\langle\phi_i|$.

It amounts to first measuring $\rho$ in all the basis corresponding to the known quantum states $(\sigma_i)_i$ and preparing $m$ approximated quantum states $(\tilde{\rho}_i)_i$. Then the tester can look for the closest quantum state $\sigma_i$ and finally returns the approximated quantum state $\tilde{\rho}_i$. This non-adaptive algorithm has a copy complexity $mN_2 + N_1 = O\left(\frac{md + m \log(1/\delta) + d \log(m/\delta)}{\varepsilon^2}\right)$.

4.1.2 Non-adaptive strategies.

We can slightly modify Alg. 1 to have a non-adaptive algorithm for the problem $(P)$ with independent measurements. It amounts to first measuring $\rho$ in all the basis corresponding to the known quantum states $(\sigma_i)_i$ and preparing $m$ approximated quantum states $(\tilde{\rho}_i)_i$. Then the tester can look for the closest quantum state $\sigma_i$ and finally returns the approximated quantum state $\tilde{\rho}_i$. This non-adaptive algorithm has a copy complexity $mN_2 + N_1 = O\left(\frac{md + m \log(1/\delta) + d \log(m/\delta)}{\varepsilon^2}\right)$.
This complexity is almost optimal for $m \leq d$ (see Theorem 4.2). However, it is no longer optimal for $m \geq d$ since $md/\varepsilon^2 \geq d^2/\varepsilon^2$. In that case, we can still design an almost optimal non-adaptive algorithm as follows: for each $k \in [m]$, let $\{|\phi_k^i\rangle\}_i$ an orthonormal basis of diagonalization for $\sigma_k$. For each $k \in [m]$ and $B \subset [m]$, let $O^k_B = \sum_{i \in B} |\phi_k^i\rangle \langle \phi_k^i|$. We use the classical shadow tomography algorithm of Huang et al. (2020) to predict $(\text{tr}(\rho O_{i,j}))_{i,j \in [m]} \cup (\text{tr}(\rho O^i_B)_{k \in [m], B \subset [m]})$ to within $\varepsilon/40$ simultaneously using $O(d(\log(m^2 + m^2d)/\varepsilon^2) = O((d^2 + \log(m))/\varepsilon^2)$ copies of $\rho$. We find the closest quantum state $\sigma_i$ to $\rho$ the same way as the Alg. 1 does. Next, we look for a probability distribution $\lambda$ satisfying for all $B \subset [m]: |\lambda(B) - \mu^i_B| \leq \varepsilon/40$, where $\mu^i_B$ is the prediction of shadow tomography algorithm for $(\text{tr}(\rho O^i_B))$. Such $\lambda$ exists since the vector $\lambda$ of eigenvalues of $\rho$ satisfies the following property:

$$
\text{tr}(\rho O^i_B) = \text{tr} \left( \sum_{i \in [d]} \lambda_i |\phi^i_i\rangle \langle \phi^i_i| \sum_{i \in B} |\phi^i_i\rangle \langle \phi^i_i| \right) = \sum_{i \in [d], j \in B} \lambda_i |\phi^i_i\rangle \langle \phi^i_i| = \sum_{i \in B} \lambda_i = \lambda(B),
$$

and $|\lambda(B) - \mu^i_B| = |\text{tr}(\rho O^i_B) - \mu^i_B| \leq \varepsilon/40$. We can thus return the quantum state $\tilde{\rho} = \sum_{i \in [d]} \tilde{\lambda}_i |\phi^i_i\rangle \langle \phi^i_i|$ as an approximation of $\rho$. We can verify that it is indeed an $\varepsilon/10$ approximation of $\rho$:

$$
\|\rho - \tilde{\rho}\|_\text{tr} \leq \sum_{i=1}^{d} |\lambda_i - \tilde{\lambda}_i| = 2 \max_{B \subset [d]} \lambda(B) - \tilde{\lambda}(B)
\leq 2 \max_{B \subset [d]} \lambda(B) - \mu^i_B + 2 \max_{B \subset [d]} \mu^i_B - \tilde{\lambda}(B)
\leq 2 \varepsilon/40 + 2 \varepsilon/40 \leq \varepsilon/10.
$$

The copy complexity of this algorithm is $O((d^2 + \log(m))/\varepsilon^2)$ which matches (up to logarithmic factors) the lower bound for $m \geq d$.

### 4.2 Lower bound

In this section, we derive lower bounds for the problem $(P)$ both with adaptive and non-adaptive independent measurements.

We start with a lower bound for non-adaptive algorithms that matches the copy complexity of the algorithm presented in Sec. 4.1.2. For this section, we fix the error probability to $\delta = 1/3$.

**Theorem 4.2.** There is a tuple of quantum states $(\sigma_1, \ldots, \sigma_m)$ such that any learning algorithm with non-adaptive independent measurements requires

$$
N = \Omega \left( \min \left\{ \frac{md}{\log(m)\varepsilon^2}, \frac{d^2}{\varepsilon^2} \right\} \right)
$$

copies of $\rho$ to approximate $\rho$ to at most $\varepsilon/10$ with at least a probability $2/3$.

This result with $m = d$, together with the analysis of the adaptive Alg. 1, gives a nearly quadratic advantage for adaptive algorithms over non-adaptive ones.

**Sketch of the proof.** We construct a large set of quantum states randomly as follows: for $y \in \{1, \ldots, m\}$, $\sigma_y = U_y \Lambda U_y^\dagger = 2^{\frac{1}{d}} - \sigma_{m+1-y}$, where $U_y$ is a $d \times d$ unitary matrix Haar$(d)$-distributed and $\Lambda$ is a diagonal matrix with entries $(1 \pm 10\varepsilon)/d$. Using the concentration inequality for Lipschitz functions of unitaries chosen according to the Haar measure, we can prove that this family is $\varepsilon$-separated with high probability:

**Lemma 4.3.** Suppose that $m \leq \exp(d^2/3000)$. For $y \in [m/2]$, let $U_y \sim \text{Haar}(d)$ and $\sigma_y = U_y \Lambda U_y^\dagger$. We have with at least a probability $9/10$, for all $y \neq z$:

$$
\|\sigma_y - \sigma_z\|_\text{tr} > \varepsilon.
$$

10
Then, for each \( y \), we construct an \( \varepsilon/10 \)-separated family of quantum states on the sphere of center \( \sigma_y \) and radius \( \varepsilon/3 \) which have the same eigen-basis as \( \sigma_y \). This can be done by taking random eigenvalues and using Hoeffding’s inequality. This leads to a family of \( e^{cd} \) states (for some constant \( c \)) that we denote by \( \{ \rho_{x,y} \}_{x \in [e^{cd}]} \).

By definition of the problem \((P)\), any \( \delta \)-correct non-adaptive algorithm for the problem \((P)\) can be used to distinguish between the states \( \{ \rho_{x,y} \}_{x,y} \) with probability at least \( 1 - \delta \). Thus, we can use these quantum states to encode a message in \([e^{cd}] \times [m]\) to a quantum state \( \rho = \rho_{x,y} \) in the family constructed above. The decoder receives this unknown quantum state, performs non-adaptive independent measurements, and learns it. Therefore a \( \delta \)-correct algorithm can decode with a probability of failure at most \( \delta \). By Fano’s inequality, the encoder and decoder should share at least \( \Omega(\log(m) + d) \) bits of information.

**Lemma 4.4** ([Fano 1961]). *The mutual information between the encoder and the decoder is at least*

\[
I \geq 2/3 \log(me^{cd}) - \log(2) \geq \Omega(\log(m) + d).
\]

The remaining and crucial part of the proof is to upper bound the mutual information for a non-adaptive algorithm. After some manipulations, the use of Jensen’s inequality, and some elementary inequalities of the logarithm function, we obtain an upper bound on the mutual information \( I \) of the form:

\[
I \leq \sup_{|\phi|} \left( \frac{8N}{m \times e^{cd}} \sum_{y \in [m/2], x \in [e^{cd}]} \langle \phi | (d \rho_{x,y} - I) | \phi \rangle^2 \right). \tag{2}
\]

The next step is to show that the right hand side of the previous inequality cannot be bigger than \( O \left( (N \varepsilon^2 \left( \log(m) \frac{m}{m} + \frac{1}{m} \right) \right) \) with a probability at least \( 9/10 \). This is the object of the following lemma.

**Lemma 4.5.** By writing \( \rho_{x,y} = \frac{4}{m} + \frac{5}{m} U_y O_{x,y} U_y^\dagger \) and \( M = \frac{2}{m^2 e^{cd}} \), we have with at least a probability \( 9/10 \), for all unit vector \( |\phi| \):

\[
\frac{1}{M} \sum_{x \in [e^{cd}], y \in [m/2]} \langle \phi | (d \rho_{x,y} - I) | \phi \rangle^2 \leq \frac{C \log(m)}{m} + \frac{C}{d} + \frac{2 \|O_{x,y}\|^2}{m}.
\]

This lemma can be proven by considering a concentration inequality for the function

\[
(U_y)_y \mapsto \frac{2}{m \times e^{cd}} \sum_{x \in [e^{cd}], y \in [m/2]} \langle \phi | (d \rho_{x,y} - I) | \phi \rangle^2,
\]

then considering a \( 1/m \)-net on the unit sphere to deduce the required inequality for the previous function uniformly on the sphere. The proof uses techniques similar to the ones of [Haah et al. 2016] and [Chen et al. 2021]. The detailed proof can be found in App. C.1.

A similar proof strategy allows to derive a lower bound on the copy complexity of adaptive strategies. The result is stated in the next proposition.

**Proposition 4.6.** There is a tuple of quantum states \((\sigma_1, \ldots, \sigma_m)\) such that any learning algorithm with possibly adaptive independent measurements requires

\[
N = \Omega \left( \frac{d + \log(m)}{\varepsilon^2} \right)
\]

copies of \( \rho \) to approximate \( \rho \) to at most \( \varepsilon/10 \) with at least a probability \( 2/3 \).

The proof is similar to the one for non-adaptive strategies, with the minor difference that the adaptivity makes difficult to simplify some products, thus we cannot upper bound the mutual information as in Ineq. 2.

We use instead a Cauchy Schwarz inequality to break the dependencies created by the adaptiveness of the algorithm. We obtain then an upper bound on the mutual information \( I \leq O(N \varepsilon^2) \). The detailed proof can be found in App. C.2.
This proposition along with the analysis of Alg. 1 show that the near optimal copy complexity of the problem \((P)\) using adaptive independent measurements is \(\tilde{\Theta}(\frac{d}{\varepsilon^2})\). This latter along with Theorem 4.2 imply the separation between adaptive and non-adaptive strategies for the problem \((P)\) for \(m \gg 1\). In other words, knowing that the eigen-basis of the quantum state belongs to some family of bases gives an advantage to adaptive strategies since they can find the eigen-basis, and then focus on measuring the quantum state with the corresponding POVM. Up to our knowledge, this is the first example for which adaptive independent strategies outperform non-adaptive ones for testing quantum states.

5 Conclusion

We have constructed hypothesis selection problems for which sequential adaptive strategies are more efficient than non-sequential non-adaptive ones. The problem for which the advantage is the most significant is the one presented in Sec. 4. It would be interesting to see if there are other natural problems for which such a separation exists. We conjecture the separation would be polynomial in \(m\) for the composite hypothesis selection problem: distinguishing between \(\rho \in \{\sigma_1, \ldots, \sigma_m\}\) and \(\rho \in \{\sigma_{m+1}, \ldots, \sigma_{2m}\}\) with high probability.

References


Michael Nussbaum and Arleta Szkoła. The chernoff lower bound for symmetric quantum hypothesis testing. 2009.


In this appendix, we give more details and the technical lemmas needed for the proofs of the article’s main results.

- We start by stating general tools to reduce quantum testing to classical testing in App. A along with the proofs for upper/lower bounds on the problem of discriminating two quantum states using sequential/non adaptive strategies.
- Then we move to prove the correctness of Alg. 1 in App. B.
- Next, we prove the lower bounds for the hypothesis selection problem \((P)\) in App. C.
- Finally, we group the technical lemmas we often need in App. D.

A Reduction to classical testing problems

One of the main difficulties in quantum testing is the freedom in the choice of measurement at each step. So, to simplify the analysis of quantum testing problems, we provide some techniques permitting the reduction to classical testing problems which are well understood.

A.1 Testing a single hypothesis vs a single hypothesis

A.1.1 Non-sequential strategies

We start by the simple remark that for diagonal quantum states, independent measurement can be seen as a post-processing of samples from the distribution given by the diagonal elements of the quantum state. Moreover, the stochastic map for this post-processing does not depend on the quantum state.

**Lemma A.1.** Let \(D\) be a discrete distribution and \(\rho\) its corresponding diagonal quantum state. Let \(M\) be a POVM. Measuring the quantum state \(\rho\) with the POVM \(M\) can be seen as post-processing of samples from the distribution \(D\).

**Proof.** Let \(M = \{M^i\}_{i \in [k]}\). For each \(i \in [k]\), we can write

\[
M^i = \sum_{x,y} M^i_{x,y} |x\rangle\langle y|.
\]

By Born’s rule, the probability distribution of the outcomes of the measurement of \(\rho\) by the POVM \(M\) is:

\[
\mathcal{M}(\rho) = \{\text{tr}(\rho M^i)\}_{i \in d} = \left\{ \text{tr} \left( \sum_x D_x |x\rangle\langle x| \sum_{x,y} M^i_{x,y} |x\rangle\langle y| \right) \right\}_{i \in d}
\]

\[
= \left\{ \sum_x M^i_{x,x} D_x \right\}_{i \in d} = PD,
\]

where \(P = (M^i_{x,x})_{i,x}\) is a stochastic matrix. Indeed, \(M^i \succcurlyeq 0\) implies \(M^i_{x,x} = \langle x|M^i|x\rangle \geq 0\) and \(\sum_i M^i = I\) implies

\[
\sum_i M^i_{x,x} = \sum_i \langle x|M^i|x\rangle = \langle x|x\rangle = 1.
\]

Note that the post-processing map is independent of the quantum state, hence we can generalize the statement to any number of discrete distributions.

**Corollary A.2.** Let \(D_1\) and \(D_2\) be two discrete distributions and \(\rho_1\) and \(\rho_2\) their corresponding diagonal quantum states. Let \(M\) be a POVM. Measuring the quantum state \(\rho_1\) (resp. \(\rho_2\)) with the POVM \(M\) can be seen as post-processing (independent of the quantum states) of samples from the distribution \(D_1\) (resp. \(D_2\)).
We move now to the proof of the following upper and lower bound on discriminating two quantum states using non-sequential independent measurements:

**Proposition A.3.** There is a non-sequential algorithm for testing \( H_1 : \rho = \sigma_1 \) vs \( H_2 : \rho = \sigma_2 \) using a number of measurements

\[
N \leq \frac{2 \log(1/\delta)}{\varepsilon^2}.
\]

Moreover, there exists two quantum states \( \sigma_1 \) and \( \sigma_2 \) satisfying \( \| \sigma_1 - \sigma_2 \|_1 = \varepsilon \) so that every non-sequential algorithm distinguishing between \( H_1 : \rho = \sigma_1 \) and \( H_2 : \rho = \sigma_2 \) needs a number of measurements satisfying

\[
\liminf_{\varepsilon \to 0} \frac{N}{\log(1/\delta)} \geq \max \left\{ \frac{1}{\text{KL}(1/2 + \alpha \varepsilon/1/2)}, \frac{1}{\text{KL}(1/2 - \beta \varepsilon/1/2)} \right\} \sim \frac{2}{\varepsilon^2},
\]

where \( \alpha \in (0, 1) \) and \( \beta \in (0, 1) \) are defined such that \( \text{KL}(1/2 + \alpha \varepsilon/1/2) = \text{KL}(1/2 + \alpha \varepsilon/1/2 + \varepsilon) \) and \( \text{KL}(1/2 - \beta \varepsilon/1/2) = \text{KL}(1/2 - \beta \varepsilon/1/2 - \varepsilon) \).

**Proof.** The correctness of the batch algorithm presented in Sec. 3.1.1 can be done using Chernoff-Hoeffding inequality, if \( \rho = \sigma_1 \) the error probability can be upper bounded as follows:

\[
P(S - \text{tr}(\sigma_2 O) \leq \varepsilon/2) = P(S - \text{tr}(\sigma_1 O) \leq \varepsilon/2 - \varepsilon) \\
\leq P(S - \text{tr}(\sigma_1 O) \leq -\varepsilon/2) \\
\leq \exp(-N \text{KL}(\text{tr}(\sigma_1 O) - \varepsilon/2||\text{tr}(\sigma_1 O))) .
\]

On the other hand, if \( \rho = \sigma_2 \):

\[
P(S - \text{tr}(\sigma_2 O) \geq \varepsilon/2) \leq \exp(-N \text{KL}(\text{tr}(\sigma_2 O) + \varepsilon/2||\text{tr}(\sigma_2 O))).
\]

Therefore to ensure that the batch algorithm is \( \delta \)-correct we need \( N \) to satisfy

\[
N = \max \left\{ \frac{\log(1/\delta)}{\text{KL}(\text{tr}(\sigma_1 O) - \varepsilon/2||\text{tr}(\sigma_1 O))}, \frac{\log(1/\delta)}{\text{KL}(\text{tr}(\sigma_2 O) + \varepsilon/2||\text{tr}(\sigma_2 O))} \right\} \leq \frac{2 \log(1/\delta)}{\varepsilon^2}.
\]

Moreover by Pinsker’s inequality (Fedotov et al., 2003), the right hand side is upper bounded by:

\[
\max \left\{ \frac{\log(1/\delta)}{\text{KL}(\text{tr}(\sigma_1 O) - \varepsilon/2||\text{tr}(\sigma_1 O))}, \frac{\log(1/\delta)}{\text{KL}(\text{tr}(\sigma_2 O) + \varepsilon/2||\text{tr}(\sigma_2 O))} \right\} \leq \frac{2 \log(1/\delta)}{\varepsilon^2}.
\]

For the lower bound, let \( d = 2 \), \( \sigma_1 = \mathbb{I}/2 \) and \( \sigma_2 = \text{diag}((1 + 2\varepsilon)/2, (1 - 2\varepsilon)/2) = \mathbb{I}/2 + \varepsilon O \) where \( O = \text{diag}(1, -1) \). Let \( \mathcal{A} \) be a non-sequential algorithm that distinguishes between \( H_1 \) and \( H_2 \) using \( N \) measurements. Let the \( i \)-th measurement be \( \mathcal{M}_i = (\mathbb{I} - O_i, O_i) \). Measuring \( \rho = \sigma_1 \) (resp. \( \sigma_2 \)) with the POVM \( \mathcal{M}_i \) is equivalent to sampling from \( \text{Ber} (\text{tr}(O_i)/2) \) (resp. \( \text{Ber} (\text{tr}(O_i)/2 + \varepsilon \text{tr}(O_i)) \)).

The optimal sample complexity of testing identity: \( H_0 : p = \text{tr}(O_i)/2 \) vs \( H_1 : p = \text{tr}(O_i)/2 + \varepsilon \text{tr}(O_i) \) is asymptotically equivalent to (when \( \varepsilon \to 0 \)) (Fawzi et al., 2022):

\[
\frac{8(\text{tr}(O_i)/2)(1 - \text{tr}(O_i)/2) \log(1/\delta)}{\varepsilon^2 \text{tr}(O_i)O_i^2} = \frac{4\text{tr}(O_i)(1 - \text{tr}(O_i)/2) \log(1/\delta)}{\varepsilon^2 \text{tr}(O_i)O_i^2}.
\]

Let’s write \( O_i = \begin{pmatrix} \lambda_1 & \beta \\ \beta & \lambda_2 \end{pmatrix} \), we have \( \text{tr}(O_i)O_i) = \lambda_1 - \lambda_2 \). Since \( 0 < O_i \ll \mathbb{I} \), we have \( 0 \leq \lambda_i \leq 1 \) for \( i = 1, 2 \).

Hence

\[
\frac{4\text{tr}(O_i)(1 - \text{tr}(O_i)/2) \log(1/\delta)}{\varepsilon^2 \text{tr}(O_i)O_i^2} = \frac{2(\lambda_1 + \lambda_2)(2 - \lambda_1 - \lambda_2) \log(1/\delta)}{\varepsilon^2 (\lambda_1 - \lambda_2)^2} \geq \frac{2 \log(1/\delta)}{\varepsilon^2}.
\]

This latter inequality is true since

\[
(\lambda_1 + \lambda_2)(2 - \lambda_1 - \lambda_2) \geq (\lambda_1 - \lambda_2)^2 \iff \lambda_1(1 - \lambda_1) + \lambda_2(1 - \lambda_2) \geq 0,
\]

16
with equality iff \( \lambda_i = 0,1 \) for \( i = 1,2 \). The cases \( \lambda_1 = \lambda_2 \) are eliminated because the sample complexity has a denominator \( (\lambda_1 - \lambda_2) \). It remains the cases \( \lambda_1 = 1 - \lambda_2 \in \{0,1\} \) for which \( O_i \) is a rank 1 projector. Therefore, the optimal measurement reduces to testing uniform: \( \text{Ber}(1/2) \) vs \( \text{Ber}(1/2 + \varepsilon) \). This problem requires a sample complexity asymptotically equivalent to \( \frac{2\log(1/\delta)}{\varepsilon^2} \). Note that we can also use Lemma [A.1] to make the desired reduction. We show how this reduction works for entangled strategies. We have \( \sigma_1^{\otimes N} = \frac{1}{2^N} \) and \( \sigma_2^{\otimes N} = \frac{1}{2^N} \text{diag} \left( (1 + 2\varepsilon)^{|i|}(1 - 2\varepsilon)^{|N - |i|} \right)_{i \in \{0,1\}^N} \) where \( |i| = i_1 + \cdots + i_N \). By Lemma [A.1], measuring the quantum states \( \sigma_1^{\otimes N} \) (resp. \( \sigma_2^{\otimes N} \)) can be seen as post-processing of samples from the distribution \( D_1 = \{1/2^N\}_{i \in \{0,1\}^N} \) (resp. \( D_2 = \{(1/2 - \varepsilon)^{|i|}(1/2 + \varepsilon)^{|N - |i|}\}_{i \in \{0,1\}^N} \)). Observe that a sample \( i = (i_1, \ldots, i_N) \sim D_1 \) is given by \( N \) i.i.d. random variables \( \{i_k \sim \text{Ber}(1/2)\}_{k \in [N]} \). Similarly, a sample \( i = (i_1, \ldots, i_N) \sim D_2 \) is given by \( N \) i.i.d. random variables \( \{i_k \sim \text{Ber}(1/2 - \varepsilon)\}_{k \in [N]} \). Therefore, distinguishing \( \sigma_1 \) from \( \sigma_2 \) using \( N \) entangled copies can be reduced to testing \( \text{Ber}(1/2) \) vs \( \text{Ber}(1/2 - \varepsilon) \) using \( N \) samples. This latter requires a number of samples [Fawzi et al., 2022]:

\[
\liminf_{\delta \to 0} \frac{N}{\log(1/\delta)} \geq \max \left\{ \frac{1}{\text{KL}(1/2 + \alpha\varepsilon||1/2)}, \frac{1}{\text{KL}(1/2 - \beta\varepsilon||1/2)} \right\} \geq \frac{2}{\varepsilon^2},
\]

where \( \alpha \in (0,1) \) and \( \beta \in (0,1) \) are defined such that \( \text{KL}(1/2 + \alpha\varepsilon||1/2) = \text{KL}(1/2 + \alpha\varepsilon||1/2 + \varepsilon) \) and \( \text{KL}(1/2 - \beta\varepsilon||1/2) = \text{KL}(1/2 - \beta\varepsilon||1/2 - \varepsilon) \).

### A.1.2 Sequential strategies

Discriminating two quantum states using sequential strategies can be done with fewer measurements than non-sequential strategies. Since the reduction to lower bound is similar, we give only the proof for the upper bound.

**Proposition A.4.** There is a sequential algorithm for testing \( H_1 : \rho = \sigma_1 \) vs \( H_2 : \rho = \sigma_2 \) using an expected number of measurements:

\[
E(N) \leq \frac{\log(1/\delta)}{2\varepsilon^2} + \frac{\log(1/\delta)^{2/3} + 2\log(1/\delta)^{1/3} + \log(\log(1/\delta)/2\varepsilon^2)}{\varepsilon^2} + 1.
\]

Moreover, there are two quantum states \( \sigma_1 \) and \( \sigma_2 \) satisfying \( \|\sigma_1 - \sigma_2\| = \varepsilon \) so that every sequential algorithm distinguishing between \( H_1 : \rho = \sigma_1 \) and \( H_2 : \rho = \sigma_2 \) with high probability needs in expectation a number

\[
E(N) \geq \frac{\log(1/\delta)}{\min \{\text{KL}(1/2 \pm \varepsilon||1/2)\}}
\]

of measurements.

**Proof.** The algorithm is presented in Sec. [3.1.2](#).

**Correctness.** Let’s start by showing that this algorithm is \( \delta \)-correct. To this end, we need a time uniform concentration inequality which can be obtained by Hoeffding inequality along with the union bound, recall that \( S_t = (\sum_{i=1}^t X_i)/t \) and \( X_i \sim \text{Ber}(\text{tr}(\rho O)) \):

\[
P \left( \exists \, t \geq 1 : |S_t - E(S_t)| > \phi(\delta, t) \right) \leq \sum_{t \geq 1} P \left( |S_t - E(S_t)| > \phi(\delta, t) \right)
\]

\[
\leq \sum_{t \geq 1} \exp\left(-2t\phi(\delta, t)^2\right)
\]

\[
\leq \sum_{t \geq 1} \frac{\delta}{t(t + 1)}
\]

\[
\leq \delta.
\]
**Complexity.** To obtain an upper bound on the complexity, we use the following lemma:

**Lemma A.5.** A random variable taking values in \( N \), we have for all \( k \in N^* \)

\[
E(N) \leq k + \sum_{t \geq k} P(N \geq t).
\]

This inequality can be proved by writing \( E(N) = \sum_{t \geq 0} P(N \geq t) \) then upper bounding the first \( k \) terms by 1.

Let \( \alpha \in (0, 1) \) and \( k \) the smallest integer so that for all \( t \geq k : \phi(\delta, t) \leq \alpha \varepsilon \). We focus only on the case \( \rho = \sigma_1 \) (the other being similar), the expected stopping time of the algorithm can be controlled as follows:

\[
E(N) \leq k + \sum_{t \geq k} P(N \geq t)
\leq k + \sum_{t \geq k} P(S_{t-1} < \text{tr}(\sigma_2 O) + \phi(\delta, t - 1))
\leq k + \sum_{t \geq k-1} P(S_t - \text{tr}(\sigma_1 O) < -\varepsilon + \alpha \varepsilon)
\leq k + \sum_{t \geq k-1} P(S_t - \text{tr}(\sigma_1 O) < -(1 - \alpha)\varepsilon)
\leq k + \sum_{t \geq k-1} 2 \exp(-2t(1 - \alpha)^2 \varepsilon^2)
\leq k + \frac{2 \exp(-2(k - 1)(1 - \alpha)^2 \varepsilon^2)}{1 - \exp(-2(1 - \alpha)^2 \varepsilon^2)}
\leq k + \frac{2 \exp(-2(k - 1)(1 - \alpha)^2 \varepsilon^2)}{(1 - \alpha)^2 \varepsilon^2}.
\]

On the other hand we have \( \phi(\delta, k) \leq \alpha \varepsilon \) and \( \phi(\delta, k - 1) \geq \alpha \varepsilon \) so

\[
\log \left( \frac{(k - 1)k}{\delta} \right) \geq 2(k - 1)\alpha^2 \varepsilon^2.
\]

Therefore:

\[
k - 1 \leq \frac{\log(1/\delta)}{2\alpha^2 \varepsilon^2} + 2 \frac{\log(\log(1/\delta)/(\alpha\varepsilon)^2)}{\alpha^2 \varepsilon^2}.
\]

Hence:

\[
\frac{E(N)}{\log(1/\delta)} \leq \frac{1}{2\alpha^2 \varepsilon^2} + 2 \frac{\log(\log(1/\delta)/(\alpha\varepsilon)^2)}{\log(1/\delta)\alpha^2 \varepsilon^2} + \frac{1}{\log(1/\delta)} + \frac{2 \exp(-2(k - 1)(1 - \alpha)^2 \varepsilon^2)}{\log(1/\delta)(1 - \alpha)^2 \varepsilon^2},
\]

and by taking \( \delta \to 0 \), then \( \alpha \to 1 \) we obtain:

\[
\limsup_{\delta \to 0} \frac{E(N)}{\log(1/\delta)} \leq \frac{1}{2\varepsilon^2}.
\]

A non asymptotic upper bound can be obtained by choosing \( \alpha = (1 + \log(1/\delta)^{-1/3})^{-1} \):

\[
E(N) \leq \frac{\log(1/\delta)}{2\varepsilon^2} + \frac{\log(1/\delta)^{2/3} + 2 \log(1/\delta)^{1/3} + \log(1/\delta)/2\varepsilon^2 + 1}{\varepsilon^2}.
\]

The lower bound follows from the previous reduction to testing \( \text{Ber}(1/2) \) vs \( \text{Ber}(1/2 \pm \varepsilon) \) and (Fawzi et al., 2022).
A.1.3 Asymptotics of the quantum relative entropy and Chernoff divergence.

Recall that we consider the particular states $\sigma_1 = \frac{I}{2}$ and $\sigma_2 = \text{diag}(\frac{1}{2} + \varepsilon, \frac{1}{2} - \varepsilon)$. An asymptotic (when $\varepsilon \to 0$) of the quantum relative entropy between $\sigma_1$ and $\sigma_2$ is given by:

$$D(\sigma_1 \| \sigma_2) = \frac{1}{2} \log \left( \frac{1}{1 + 2\varepsilon} \right) + \frac{1}{2} \log \left( \frac{1}{1 - 2\varepsilon} \right) \sim \frac{2\varepsilon^2}{\varepsilon \to 0},$$

$$D(\sigma_2 \| \sigma_1) = \left( \frac{1}{2} + \varepsilon \right) \log(1 + 2\varepsilon) + \left( \frac{1}{2} - \varepsilon \right) \log(1 - 2\varepsilon) \sim \frac{2\varepsilon^2}{\varepsilon \to 0}.$$

On the other hand, an asymptotic (when $\varepsilon \to 0$) of the quantum Chernoff divergence between the states $\sigma_1$ and $\sigma_2$ can be upper bounded using the inequality $\log(x) \geq (x - 1) - (x - 1)^2$ valid for $x \in (\frac{1}{2}, \infty)$:

$$C(\sigma_1, \sigma_2) = \sup_{0 \leq s \leq 1} -\log(\text{tr}(\sigma_1^s \sigma_2^{1-s})))$$

$$\leq \sup_{0 \leq s \leq 1} \left[ \frac{1}{2} (1 + 2\varepsilon)^s - \frac{1}{2} (1 - 2\varepsilon)^s \right] + \left[ \frac{1}{2} (1 + 2\varepsilon)^s + \frac{1}{2} (1 - 2\varepsilon)^s - 1 \right]^2$$

$$\leq \sup_{0 \leq s \leq 1} [2s(1 - s)\varepsilon^2 + o(\varepsilon^2)] + o(\varepsilon^4) \sim \frac{\varepsilon^2}{2}. \quad (\varepsilon \to 0)$$

Moreover, it can be lower bounded using the inequality $\log(x) \leq x - 1$:

$$C(\sigma_1, \sigma_2) = \sup_{0 \leq s \leq 1} -\log \left( \frac{1}{2} (1 + 2\varepsilon)^s + \frac{1}{2} (1 - 2\varepsilon)^s \right)$$

$$\geq \sup_{0 \leq s \leq 1} \left[ 1 - \frac{1}{2} (1 + 2\varepsilon)^s - \frac{1}{2} (1 - 2\varepsilon)^s \right]$$

$$\geq \sup_{0 \leq s \leq 1} [2s(1 - s)\varepsilon^2 + o(\varepsilon^2)] \sim \frac{\varepsilon^2}{2}. \quad (\varepsilon \to 0)$$

Finally $C(\sigma_1, \sigma_2) \sim \frac{\varepsilon^2}{2}$.

A.2 Testing a single hypothesis vs a multiple hypothesis

In this section, we relate the TV-distance between the distributions obtained after the measurements and the 1-norm between the quantum states.

Lemma A.6. Let $U \in \mathbb{C}^{d \times d}$ be a Haar-random unitary matrix of columns $\{|U_i\rangle\}_{1 \leq i \leq d}$, $\mathcal{M}(U) = \{|U_i\rangle\langle U_i|\}_i$ is a POVM and there exists a universal constant $c$ such that for all quantum states $\rho$ and $\sigma$ we have:

$$\text{E}[\text{TV}(\rho(\mathcal{M}), \sigma(\mathcal{M}))] \geq c \frac{\|\rho - \sigma\|_{\text{tr}}}{\sqrt{d}}.$$

Proof. Let $\xi = \rho - \sigma$, we have $U|e_i\rangle = |U_i\rangle$ and we use Weingarten Calculus $\textbf{D.1}$ and $\textbf{D.2}$ to calculate

$$\text{E} \left[ (U_i|\xi|U_i)^2 \right] = \text{E} \left[ (U_i|\xi|U_i)\langle U_i|\xi|U_i\rangle \right]$$

$$= \text{E} \left[ \text{tr}(\xi(U_i|U_i)\xi(U_i|U_i)) \right]$$

$$= \text{E} \left[ \text{tr}(\xi|U_i\rangle\langle U_i|U_i\rangle) \right]$$

$$= \text{E} \left[ \text{tr}(\xi|U_i\rangle\langle U_i|U_i\rangle) \right]$$

$$= \sum_{\alpha, \beta \in \mathbb{S}_2} \text{Wg}(\beta \alpha^{-1}, d) \text{tr}_{\beta^{-1}}(\xi, \xi) \text{tr}_{\alpha}(|e_i\rangle\langle e_i|, |e_i\rangle\langle e_i|)$$

$$= \frac{1}{d(d + 1)} \text{tr}(\xi^2).$$
Similarly

\[
\begin{align*}
\mathbb{E} [(U_i | \xi | U_i)^4] &= \mathbb{E} [(U_i | \xi | U_i) (U_i | \xi | U_i) (U_i | \xi | U_i) (U_i | \xi | U_i)] \\
&= \mathbb{E} [\text{tr}(\xi|U_i\rangle\langle U_i|\xi|U_i\rangle\langle U_i|\xi|U_i\rangle\langle U_i|\xi|U_i\rangle)] \\
&= \mathbb{E} [\text{tr}(\xi|U_i\rangle\langle U_i|\xi|U_i\rangle\langle U_i|\xi|U_i\rangle\langle U_i|\xi|U_i\rangle)] \\
&= \mathbb{E} [\text{tr}(U^\dagger \xi|U_i\rangle\langle U_i|\xi|U_i\rangle\langle U_i|\xi|U_i\rangle\langle U_i|\xi|U_i\rangle)] \\
&= \sum_{\alpha, \beta \in \mathcal{S}_4} Wg(\beta \alpha^{-1}, \sigma - 1) (\xi, \xi, \xi, \xi) \text{tr} \alpha (|e_i\rangle\langle e_i|, |e_i\rangle\langle e_i|, |e_i\rangle\langle e_i|, |e_i\rangle\langle e_i|) \\
&= \frac{1}{d(d+1)(d+2)(d+3)} (6\text{tr}(\xi^2)^2 + 6\text{tr}(\xi^4)). \\
&\leq \frac{c'}{d(d+1)(d+2)(d+3)} \text{tr}(\xi^2)^2.
\end{align*}
\]

We can now conclude by Hölder’s inequality:

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

This Lemma is about the expected TV distance. Actually, we can prove that we have the same inequality with high probability.

**Lemma A.7.** Let \( l = \Theta (\log(1/\delta)) \) and \( U^1, U^2, \ldots, U^l \in \mathbb{C}^{d \times d} \) be Haar-random unitary matrices of columns \( \{ |U^i_j\rangle \}_{1 \leq i \leq d, 1 \leq j \leq l} \), \( \mathcal{M} = \{ \frac{1}{l} |U^i_j\rangle\langle U^i_j| \}_{i,j} \) is a POVM and there exists a universal constant \( c \) such that for all quantum states \( \rho \) and \( \sigma \) we have with a probability at least \( 1 - \delta \):

\[
\text{TV}(\rho(\mathcal{M}), \sigma(\mathcal{M})) \geq c \frac{\|\rho - \sigma\|_{\text{tr}}}{\sqrt{d}}.
\]

20
Proof. 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:

\[
2|f(U) - f(V)| = \left| \sum_{1 \leq i \leq d, 1 \leq j \leq l} \frac{1}{l} \left| \text{tr}(U_i^j | V_i^j \xi) - \text{tr}(U_i^j | V_i^j \xi) \right| \right|
\leq \sum_{1 \leq i \leq d, 1 \leq j \leq l} \frac{1}{l} \left| \text{tr}((U_i^j | V_i^j \xi) - (V_i^j | V_i^j \xi)) \right|
\leq \sum_{1 \leq i \leq d, 1 \leq j \leq l} \frac{1}{l} \sqrt{\text{tr}(\xi^2)} \sqrt{\text{tr}((U_i^j | V_i^j \xi) - (V_i^j | V_i^j \xi))^2)}
\leq \sqrt{\frac{d}{l}} \sqrt{\text{tr}(\xi^2)} \sqrt{\sum_{1 \leq i \leq d, 1 \leq j \leq l} \text{tr}((U_i^j - V_i^j)^2)}
\leq \sqrt{\frac{d}{l}} \sqrt{\text{tr}(\xi^2)} \|U - V\|_{2,HS},
\]

hence \( f \) is \( L = \sqrt{\frac{d}{l}} \sqrt{\text{tr}(\xi^2)} \)-Lipschitz, therefore by Theorem D.3:

\[
P \left( \left| f(U) - \mathbb{E}(f(U)) \right| > \frac{c}{2} \sqrt{\text{tr}(\xi^2)} \right) \leq e^{-\frac{d^4 \text{tr}(\xi^2)}{8k^2}} = e^{-\frac{c^2}{24}} = \frac{\epsilon}{2},
\]

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

\[
\text{TV}(\rho(\mathcal{M}), \sigma(\mathcal{M})) \geq \mathbb{E}(\text{TV}(\rho(\mathcal{M}), \sigma(\mathcal{M}))) - |\text{TV}(\rho(\mathcal{M}), \sigma(\mathcal{M})) - \mathbb{E}(\text{TV}(\rho(\mathcal{M}), \sigma(\mathcal{M})))|
\geq \frac{c}{2} \sqrt{\text{tr}(\xi^2)} - \frac{c}{2} \sqrt{\text{tr}(\xi^2)}
\geq \frac{c}{2} \sqrt{\text{tr}(\xi^2)}
\geq \frac{c}{2} \frac{\|\rho - \sigma\|_{tr}}{\sqrt{r}},
\]

where \( r \) is the rank of \( (\rho - \mathbb{I}/d) \).

Once we have the lower bound on the TV distance between the distributions obtained after performing the measurements, we can deduce upper bounds on sequential algorithms for testing identity depending on the rank of \( \rho \) or \( \rho - \mathbb{I}/d \).

**Dependence in the rank of \( \rho - \mathbb{I}/d \)** From the previous lower bound on the TV-distance, we can achieve an upper bound using the sequential tester of \cite{fawzi2022testing}:

\[
\mathcal{O} \left( \min \left\{ \frac{n^{1/2} \log(1/\delta)^{1/2}}{\max\{\varepsilon/\sqrt{d}, \|\rho - \mathbb{I}/d\|_2\}^2}, \log(1/\delta) \right\} \right) = \mathcal{O} \left( \frac{d^{3/2} \log(1/\delta)}{\varepsilon^2} \right)
\]

where \( r \) is the rank of \( (\rho - \mathbb{I}/d) \) and we use Cauchy Schwarz to obtain the latter inequality.
Dependence in the rank of $\rho$  The proof of Lemma 3.3 permits to deduce that with high probability:

$$TV(P, U_n) \geq c\|\rho - I/d\|_2 \geq c\sqrt{\sum_{i=1}^{r} \left(\lambda_i - \frac{1}{d}\right)^2 + \frac{d-r}{d^2}}$$

$$\geq c\sqrt{\sum_{i=1}^{r} \lambda_i^2 - \frac{1}{d}} \geq c\sqrt{\frac{1}{r} - \frac{1}{d}} \geq c\sqrt{\frac{1}{2r}},$$

where $r$ is the rank of $\rho$ supposed to be less than $d/2$ and we use Cauchy Schwarz inequality. Therefore we can test whether $\rho = \sigma$ or $\|\rho - \sigma\|_{tr} > \epsilon$ with probability at least $1 - \delta$ using $\min \{ \frac{d^{1/2} \log(1/\delta)}{\epsilon^2}, rd^{1/2} \log(1/\delta) \}$ copies of $\rho$.

### B Analysis of Alg. 1

In this section we prove the correctness of the Alg. 1. We need to show that with probability at least $1 - \delta/2$, Alg. 1 finds the closest quantum state $\sigma^{\star}$ to $\rho$.

**Lemma B.1.** For all $i \neq j \in [m]$, let $\mu_{i,j}$ an $\epsilon/10$ approximation of $\tr(\rho O_{i,j})$ given by classical shadow tomography of [Huang et al., 2020]. Let $k^{\star} = \arg\min_{i,j} \mu_{i,j} - \tr(\sigma^{\star} O_{i,j})$. We have with at least a probability $1 - \delta/2$:

$$\|\rho - \sigma^{\star}\|_{tr} \leq \epsilon/3.$$

**Proof.** Classical shadow tomography of [Huang et al., 2020] permits to have the following approximations

$$\forall i \neq j \in [m]: |\mu_{i,j} - \tr(\rho O_{i,j})| \leq \epsilon/10,$$

with a probability at least $1 - \delta/2$ using only $N = \mathcal{O}(d \log(m)/\epsilon^2)$ copies of $\rho$.

Let $\sigma^{\star}$ the closest quantum state to $\rho$. We want to prove that with high probability $k^{\star} = i^{\star}$. We have for all $l \neq i^{\star}$: $\|\sigma^{\star} - \sigma_l\|_{tr} > \epsilon$ hence:

$$\max_{i,j} \mu_{i,j} - \tr(\sigma_l O_{i,j}) \geq \mu_{i^{\star},j} - \tr(\sigma^{\star} O_{i^{\star},j})$$

$$\geq \tr(\rho O_{i^{\star},j}) - \tr(\sigma^{\star} O_{i^{\star},j}) - \epsilon/10$$

$$\geq \tr(\sigma^{\star} O_{i^{\star},j}) - \tr(\sigma^{\star} O_{i^{\star},j}) + \tr(\rho O_{i^{\star},j}) - \tr(\sigma^{\star} O_{i^{\star},j}) - \epsilon/10$$

$$\geq \|\sigma^{\star} - \sigma_l\|_{tr} - \|\rho - \sigma^{\star}\|_{tr} - \epsilon/10$$

$$\geq \epsilon - \epsilon/3 - \epsilon/10$$

$$> \epsilon/2.$$  

On the other hand

$$\max_{i,j} \mu_{i,j} - \tr(\sigma_l O_{i,j}) \leq \max_{i,j} \mu_{i,j} - \tr(\sigma^{\star} O_{i,j})$$

$$\leq \max_{i,j} \tr(\rho O_{i,j}) - \tr(\sigma^{\star} O_{i,j}) + \epsilon/10$$

$$\leq \|\rho - \sigma^{\star}\|_{tr} + \epsilon/10$$

$$\leq \epsilon/3 + \epsilon/10$$

$$< \epsilon/2.$$  

Therefore, with high probability, $k^{\star}$ cannot be different from $i^{\star}$.

\[\square\]
Once we know, with high probability, the closest quantum state to \( \rho \) we can read its basis and use it to learn \( \rho \). The following lemma indicates how to construct this approximation along with the number of copies/measurements needed for this learning task.

**Lemma B.2.** Let \( \rho = \sum_{i=1}^{d} \lambda_i |\phi_i\rangle\langle \phi_i| \). Let \( A_1, \ldots, A_N \) the outcomes of the measurement of \( \rho \) independently by the POVM \( M = \{ |\phi_i\rangle\langle \phi_i| \}_i \). The quantum state

\[
\tilde{\rho} = \sum_{i=1}^{d} \left( \frac{\sum_{j=1}^{N} 1_{A_j=i}}{N} \right) |\phi_i\rangle\langle \phi_i|
\]

is \( \varepsilon/10 \)-close in 1-norm to \( \rho \) with a probability at least \( 1 - \delta/2 \) if \( N = 200 \log(2^{d+2}/\delta)/\varepsilon^2 \).

**Proof.** \( \rho \) is a quantum state so it is a Hermitian matrix positive semi definite of trace 1. Hence, we can write \( \rho = \sum_{i=1}^{d} \lambda_i |\phi_i\rangle\langle \phi_i| \) where \( \{ \lambda_i \}_i \) is a probability distribution and \( \{ \phi_i \}_i \) is an orthonormal basis. Therefore \( \sum_{i=1}^{d} |\phi_i\rangle\langle \phi_i| = I \) and \( M \) is a valid POVM. Measuring \( \rho \) via the POVM \( M \) is equivalent to sampling from the distribution \( \{ \text{tr}(|\phi_i\rangle\langle \phi_i| \rho) \}_i = \{ \sum_j \lambda_j \text{tr}(|\phi_j\rangle\langle \phi_j| \rho) \}_i = \{ \lambda_i \}_i \) hence

\[
A_1, \ldots, A_N \overset{i.i.d.}{\sim} \{ \lambda_i \}_i.
\]

On the other hand \( \rho \) and \( \tilde{\rho} \) have the same basis of diagonalization so the 1 norm between them is simply

\[
||\rho - \tilde{\rho}||_\text{tr} = \left\| \sum_{i=1}^{d} \lambda_i |\phi_i\rangle\langle \phi_i| - \sum_{i=1}^{d} \tilde{\lambda}_i |\phi_i\rangle\langle \phi_i| \right\|_\text{tr}
\]

\[
= \sum_{i=1}^{d} \left( |\lambda_i - \tilde{\lambda}_i| \right) \text{tr}(|\phi_i\rangle\langle \phi_i|)
\]

\[
= \sum_{i=1}^{d} |\lambda_i - \tilde{\lambda}_i|
\]

\[
= 2 \text{TV}(\lambda, \tilde{\lambda}),
\]

where \( \{ \tilde{\lambda}_i \}_i = \{ \sum_{j=1}^{N} 1_{A_j=i}/N \}_i \). It is well known that the TV distance can be written as:

\[
\text{TV}(\lambda, \tilde{\lambda}) = \max_{B \subset [d]} (\tilde{\lambda}(B) - \lambda(B))
\]

Chernoff-Hoeffding ([Hoeffding, 1963]) inequality implies for all \( B \subset [d] \):

\[
P \left( \left| \frac{\sum_{j=1}^{N} 1_{A_j \in B}}{N} - \lambda(B) \right| > \frac{\varepsilon}{20} \right) \leq 2 \exp \left( -2N \left( \frac{\varepsilon}{20} \right)^2 \right).
\]

Therefore by union bound we obtain

\[
P (||\rho - \tilde{\rho}||_\text{tr} > \varepsilon/10) = P (2 \text{TV}(\lambda, \tilde{\lambda}) > \varepsilon/10)
\]

\[
= P \left( \exists B \subset [d] : \left| \frac{\sum_{j=1}^{N} 1_{A_j \in B}}{N} - \lambda(B) \right| > \frac{\varepsilon}{20} \right)
\]

\[
\leq 2^{d+1} \exp \left( -2N \left( \frac{\varepsilon}{20} \right)^2 \right).
\]

Finally for \( N = 200 \log(2^{d+1}/\delta)/\varepsilon^2 \), we have with at least a probability \( 1 - \delta \): \( ||\rho - \tilde{\rho}||_\text{tr} \leq \varepsilon/10 \). \qed

Grouping the two previous Lemmas, Alg. 1 finds the closest quantum state \( \sigma_1 \), and returns an \( \varepsilon/10 \)-approximation of \( \rho \) with a probability at least \( 1 - (\delta/2 + \delta/2) = 1 - \delta \). Finally, Alg. 1 is \( \delta \)-correct.
C  Lower bound for the problem \((P)\)

In this section, we focus on proving lower bounds for hypothesis selection problem \((P)\) for non-adaptive and adaptive strategies.

C.1  Non-adaptive strategies

We recall the theorem we want to prove:

**Theorem C.1.** There is a tuple of quantum states \(\{\sigma_1, \ldots, \sigma_m\}\) such that any learning algorithm for problem \((P)\) with non-adaptive independent measurements requires

\[
N = \Omega \left( \min \left\{ \frac{md}{\log(m)\varepsilon^2}, \frac{d^2}{\varepsilon^2} \right\} \right)
\]

Copies of \(\rho\).

**Construction**  For the construction, we choose \(m\) unitary matrices \(\{U_y\}_y\) chosen randomly from the Haar\((d)\) distribution, then we choose for each unitary (orthonormal basis) random eigenvalues:

**Lemma C.2.** Let \(m \leq \exp(d^2/3000)\). Let \(\{U_y\}_{y \in [m/2]} m/2\) unitaries Haar\((d)\) distributed. For \(y \in [m/2]\), let \(\sigma_y = 2I/d - \sigma_{m+1-y} = U_y\Lambda U_y^\dagger\) where \(\Lambda = \frac{1}{d} + \text{diag} \left( \{\lambda_i\}_{i \in [d]} \right) = \text{diag} \left( \left\{ \frac{1+(-1)^i\varepsilon}{d} \right\}_{i \in [d]} \right)\). We have with a probability at least \(9/10\), for all \(y \neq z \in [m]\):

\[
\|\sigma_y - \sigma_z\|_\text{tr} \geq \varepsilon.
\]

**Proof.** Let \(y \neq z \in [m/2]\) and \(0 \ll O \ll I\) satisfying \(\text{tr diag} \left( \{\lambda_i\}_{i \in [d]} \right) O = -5\varepsilon\). Let \(f(U) = \text{tr} \left( U \text{diag} \left( \{\lambda_i\}_{i \in [d]} \right) U^\dagger - \text{diag} \left( \{\lambda_i\}_{i \in [d]} \right) \right) O\) where \(U \sim \text{Haar}(d)\), we have \(E(f(U)) = -\text{tr diag} \left( \{\lambda_i\}_{i \in [d]} \right) O = 5\varepsilon\) (see Weingarten Calculus \([D.1] \)). The function \(f\) is \(\frac{20\varepsilon}{\sqrt{d}}\)-Lipschitz:

\[
|f(U) - f(V)| \leq |\text{tr} (U \text{diag} \left( \{\lambda_i\}_{i \in [d]} \right) U^\dagger - \text{diag} \left( \{\lambda_i\}_{i \in [d]} \right) O) - \text{tr} (V \text{diag} \left( \{\lambda_i\}_{i \in [d]} \right) V^\dagger - \text{diag} \left( \{\lambda_i\}_{i \in [d]} \right) O)|
\]

\[
\leq |\text{tr} (U \text{diag} \left( \{\lambda_i\}_{i \in [d]} \right) U^\dagger - V \text{diag} \left( \{\lambda_i\}_{i \in [d]} \right) V^\dagger) O|
\]

\[
\leq \|(U - V) \text{diag} \left( \{\lambda_i\}_{i \in [d]} \right) U^\dagger\|_\text{tr} + \|V \text{diag} \left( \{\lambda_i\}_{i \in [d]} \right) (U - V)^\dagger\|_\text{tr}
\]

\[
\leq \|U - V\|_2 \| \text{diag} \left( \{\lambda_i\}_{i \in [d]} \right) U^\dagger\|_2 + \|V \text{diag} \left( \{\lambda_i\}_{i \in [d]} \right) \|_2 \|(U - V)^\dagger\|_2
\]

\[
\leq \frac{10 \varepsilon}{d} (\|U - V\|_2\| \text{diag} \left( \{(-1)^i\}_{i \in [d]} \right) U^\dagger\|_2 + \|V \text{diag} \left( \{(-1)^i\}_{i \in [d]} \right) \|_2 \|(U - V)^\dagger\|_2)
\]

\[
\leq \frac{20 \varepsilon}{\sqrt{d}} \|U - V\|_2,
\]

where we have used Cauchy Schwarz inequality.

Using the fact that the Haar distribution is invariant under the multiplication by a unitary and the concentration inequality for Lipschitz functions \([D.3] \), the probability that the states \(\{\sigma_y\}_{y \in [m/2]}\) are not \(\varepsilon\)-separated
Proof. We start by writing the eigen-decomposition of the known quantum states such that for each \( \lambda_i \in [d] \), we have

\[
\sigma_y = U_y \left( \sum_{i=1}^d \lambda_i |i\rangle \langle i| \right) U_y^\dagger.
\]

We claim that we can choose \( \alpha_i^c \) to construct an \( \varepsilon/5 \)-separated family of \( mc^d \) quantum states (where \( c \) is a constant to be chosen later) of the form

\[
\rho_{x,y} = U_y \left( \sum_{i=1}^d \left( \lambda_i^y + \frac{\alpha_i^c(2\varepsilon/3)}{d} \right) |i\rangle \langle i| \right) U_y^\dagger.
\]

\( \Box \)

which is smaller than \( 1/10 \) if \( m^2 \leq 2 \exp(d^2/1000)/5 \).

For the case when \( y \in [m/2] \) and \( z \in [m] \setminus [m/2] \), let \( x = m + 1 - z \in [m/2] \) we have

\[
\| \sigma_y - \sigma_z \|_{tr} = \| \sigma_y - 2 \mathbb{I}/d + \sigma_x \|_{tr} \\
\geq \| \sigma_x - 2 \mathbb{I}/d + \sigma_x \|_{tr} - \| \sigma_y - \sigma_x \|_{tr} \\
\geq 2\| \sigma_x - \mathbb{I}/d \|_{tr} + \| \sigma_y - \sigma_x \|_{tr} \\
\geq \varepsilon.
\]

Finally, for the case when \( y \in [m] \setminus [m/2] \) and \( z \in [m] \setminus [m/2] \), let \( y' = m + 1 - y \in [m/2] \) and \( z' = m + 1 - z \in [m/2] \) we have

\[
\| \sigma_y - \sigma_z \|_{tr} = \| 2 \mathbb{I}/d - \sigma_y' - 2 \mathbb{I}/d + \sigma_z' \|_{tr} \\
\geq \| \sigma_y' - \sigma_z' \|_{tr} \\
\geq \varepsilon.
\]
for $|x| \in [e^{cd}]$ and $y \in [m]$. Note that for convenience of notation, the labels $x$ can be positive and negative. Moreover the distance between $\rho_{x,y}$ and $\sigma_y$ is exactly:

$$\|\rho_{x,y} - \sigma_y\|_{tr} = \frac{\varepsilon}{3}.$$ 

Concretely, we look for $\{\alpha^x_i\}_{1 \leq i \leq d, 1 \leq |x| \leq e^{cd}/2}$ such that

1. $\alpha^x_i = \pm 1$,
2. $\alpha_{i}^{-x} = -\alpha_{i}^{x}$,
3. $\alpha_{i}^{x} + \alpha_{i+d/2}^{x} = 0$ (we suppose $d$ is even) and
4. $\forall x \neq x': \sum_{i=1}^{d/2} |\alpha_{i}^{x} - \alpha_{i}^{x'}| > (d/2 - 1/200)$.

The third point ensures that $\rho$ has trace 1 while the fourth one implies $\|\rho_{x,y} - \rho_{x',y}\|_{tr} > \varepsilon/3 - \varepsilon/100 > \varepsilon/5$. Starting by the simple quantum states $\rho_{1,y} = \sigma_y + \sum_{i=1}^{d/2} \frac{(2\pi/3)}{d} U_{y_i} |i\rangle\langle i| U_{y_i}^*$ and $\rho_{-1,y} = 2\mathbb{I}/d - \rho_{1,y} = \sigma_{m+1-y} - \sum_{i=1}^{d/2} \frac{(2\pi/3)}{d} U_{y_i} |i\rangle\langle i| U_{y_i}^*$ and $\rho_{-1,y} = 2\mathbb{I}/d - \rho_{1,y} = \sigma_{m+1-y} - \sum_{i=1}^{d/2} \frac{(2\pi/3)}{d} U_{y_i} |i\rangle\langle i| U_{y_i}^*$ and $\rho_{-1,y} = 2\mathbb{I}/d - \rho_{1,y} = \sigma_{m+1-y} - \sum_{i=1}^{d/2} \frac{(2\pi/3)}{d} U_{y_i} |i\rangle\langle i| U_{y_i}^*$ and $\rho_{-1,y} = 2\mathbb{I}/d - \rho_{1,y} = \sigma_{m+1-y} - \sum_{i=1}^{d/2} \frac{(2\pi/3)}{d} U_{y_i} |i\rangle\langle i| U_{y_i}^*$ and we suppose that we have constructed $\mathcal{Q}$ an $\varepsilon$-separated family of the form described above of cardinality $M < e^{cd}$. Let $\alpha_1, \ldots, \alpha_{d/2}$ i.i.d. random variables taken values in $\{\pm 1\}$ with probability $1/2$ each. We have by Hoeffding’s inequality

$$P \left( \exists \rho_x \in \mathcal{Q} : \sum_{i=1}^{d/2} |\alpha_{i}^{x} - \alpha_{i}| \leq d(1/2 - 1/200) \right)$$

$$= P \left( \exists \rho_x \in \mathcal{Q} : \sum_{i=1}^{d/2} |\alpha_{i}^{x} - \alpha_{i}| \leq d(1/2 - 1/200) \right)$$

$$\leq M \frac{d}{2} P \left( \sum_{i=1}^{d/2} 1_{\alpha_{i}^{x} = \alpha_{i}} > d/4 + d/400 \right)$$

$$\leq M e^{-d/2000},$$

which is strictly less than 1 if $M < e^{d/2000}$. So let’s take $c = 1/2000$, we deduce that

$$P \left( \forall \rho_x \in \mathcal{Q} : \sum_{i=1}^{d/2} |\alpha_{i}^{x} - \alpha_{i}| > d(1/2 - 1/200) \right) > 0.$$

therefore there exists some $\alpha \in \{\pm 1\}^d$ verifying the desired conditions. We can repeat this construction until Card($\mathcal{Q}$) $\geq e^{cd}$.

We have constructed the $\varepsilon$-separated family of quantum states $\{\sigma_y\}_y$ an the corresponding $\varepsilon/5$-separated $\{\rho_{x,y}\}_x$ for all $y$, we can use tools from communication theory to deduce the lower bound (see [Haah et al. 2016]). Alice encodes a message $(x,y) \in \{1, \ldots, e^{cd}\} \times [m]$ in $\rho_{x,y}$ and sends it to Bob. To read the message, Bob tries to approximate the quantum state that he received from Alice. We suppose that Bob can approximate (up to $\varepsilon/10$ in trace norm) a state $\varepsilon/3$ close to one of $\{\sigma_y\}$ and diagonalized in the same basis of this quantum state with a probability at least $2/3$. Bob uses $N$ copies to decode Alice’s message and returns $(x', y') \in \{1, \ldots, e^{cd}\} \times [m]$, therefore by Fano’s inequality ([Fano 1961]) we have the following lower bound on the mutual information:

**Lemma C.4** (Fano). The mutual information can be lower bounded:

$$I(X,Y : X', Y') \geq 2/3 \log(m e^{cd}) - \log(2) \geq \Omega(\log(m) + d).$$
On the other hand we can upper bound the mutual information between \((X, Y)\) and \((X', Y')\). Let \(I_1, \ldots, I_N\) be the outcomes of a non-adaptive algorithm solving the problem \((P)\). By using the data-processing inequality for the Kullback-Leibler divergence and the fact that every non-adaptive algorithm for the problem \((P)\) can be used as a 2/3-correct decoder we can upper bound the mutual information as follows:

**Lemma C.5** (Data-processing). The mutual information between \((X, Y)\) and \((X', Y')\) is smaller than the mutual information between \((X, Y)\) and \((I_1, \ldots, I_N)\):

\[
I(X, Y : X', Y') \leq I(X, Y : I_1, \ldots, I_N).
\]

The next step is to upper bound the mutual information between \((X, Y)\) and \((I_1, \ldots, I_N)\). This latter depends on the quantum states \(\{\sigma_y\}_y\), therefore it is a random variable. We will show that with at least a probability 9/10, it is upper bounded by an expression involving the parameters of the problem. First we start by proving the following upper bound relating the mutual information with the unitaries \(\{U_y\}_y\) defining the quantum states \(\{\sigma_y\}_y\).

**Lemma C.6.** For all unitaries \(\{U_y\}_y\), we have:

\[
I(X, Y : I_1, \ldots, I_N) \leq 4N \sup_{\phi, \|\phi\|_2 \leq 1} \frac{1}{M} \sum_{|x|, |y| \leq m/2} \langle \phi | U_y O_{x,y} U_y^\dagger | \phi \rangle^2 \epsilon^2,
\]

where for \((x, y)\), \(O_{x,y} = U_y^\dagger (d \rho_{x,y} - 1) U_y\).

**Proof.** We suppose that the eigenvalues of \(\sigma_y\) have the form

\[
\lambda_i = \frac{1 + 10 \beta_i^y \epsilon}{d},
\]

where \(\beta_i^y = \pm 1\) satisfying \(\sum_i \beta_i^y = 0\) (exactly half are equal to +1) and \(\beta^y = -\beta^{m+1-y}\) (we suppose \(m\) even). The diagonalizing matrices \(\{U_y\}_y\) are chosen randomly so as they satisfy \(U_{m+1-y} = U_y\) for all \(y \leq m/2\) and other conditions to be specified later.

Let us denote by \(\mathcal{M}^t\) the POVM used at step \(t\). Without loss of generality, we can suppose that the non-adaptive algorithm performs only measurements of the following form:

\[
\mathcal{M}^t = \{\{\phi_i^t\}|\{\phi_i^t\}\}_i.
\]

where we have the condition \(\sum_i |\phi_i^t\rangle \langle \phi_i^t| = 1\) implying for all \(i\) and \(t\): \(\|\phi_i^t\|_2 \leq 1\).

Let \(M = 2me^cd\), we can write the mutual information as follows:

\[
I(X, Y : I_1, \ldots, I_N) = H \left( \frac{1}{M} \sum_{x,y} \text{tr}((\rho_{x,y})^\otimes N \otimes_{i=1}^N \mathcal{M}^t) \right) - \frac{1}{M} \sum_{x,y} H \left( \text{tr}((\rho_{x,y})^\otimes N \otimes_{i=1}^N \mathcal{M}^t) \right)
\]

\[
= \frac{1}{M} \sum_{x,y} \sum_{i_1, \ldots, i_N} \prod_{t=1}^N \langle \phi_i^t | \rho_{x,y} | \phi_i^t \rangle \log \left( \frac{\prod_{i=1}^N \langle \phi_i^t | \rho_{x,y} | \phi_i^t \rangle}{\frac{1}{M} \sum_{x,y} \prod_{i=1}^N \langle \phi_i^t | \rho_{x,y} | \phi_i^t \rangle} \right) = \Sigma_1 + \Sigma_2,
\]

where \(\Sigma_1\) and \(\Sigma_2\) are defined as follows:

\[
\Sigma_1 = \frac{1}{M} \sum_{x,y} \sum_{i_1, \ldots, i_N} \prod_{t=1}^N \langle \phi_i^t | \rho_{x,y} | \phi_i^t \rangle \log \left( \prod_{i=1}^N \langle \phi_i^t | d \rho_{x,y} | \phi_i^t \rangle \right),
\]

\[
\Sigma_2 = -\frac{1}{M} \sum_{x,y} \sum_{i_1, \ldots, i_N} \prod_{t=1}^N \langle \phi_i^t | \rho_{x,y} | \phi_i^t \rangle \log \left( \frac{1}{M} \sum_{x,y} \prod_{i=1}^N \langle \phi_i^t | d \rho_{x,y} | \phi_i^t \rangle \right).
\]

Since

\[
\rho_{x,y} = U_y \text{diag} \left( \left\{ \frac{1 + (10 \beta_i^y + 2 \alpha_i^y) \epsilon}{d} \right\}_{i \in [d]} \right) U_y^\dagger,
\]
we can write

\[ \langle \phi_{i}^{t} | \rho_{x,y} | \phi_{i}^{t} \rangle = \frac{1 + u_{i_{t}}^{t,x,y} \varepsilon}{d}, \]

where \( u_{i_{t}}^{t,x,y} = \langle \phi_{i}^{t} | U_{y} \, \text{diag} \left( (10 \beta_{i}^{y} + 2\alpha_{i}^{x}/3)_{i \in [d]} \right) U_{y} | \phi_{i}^{t} \rangle \in (-11,11). \) Denote by \( O_{x,y} = \text{diag} \left( (10 \beta_{i}^{y} + 2\alpha_{i}^{x}/3)_{i \in [d]} \right), \) we remark that

\[
\sum_{i=1}^{d} u_{i_{t}}^{t,x,y} = \sum_{i=1}^{d} \langle \phi_{i}^{t} | U_{y} \, \text{diag} \left( (10 \beta_{i}^{y} + 2\alpha_{i}^{x}/3)_{i \in [d]} \right) U_{y} | \phi_{i}^{t} \rangle = \text{tr} \, U_{y} \, \text{diag} \left( (10 \beta_{i}^{y} + 2\alpha_{i}^{x}/3)_{i \in [d]} \right) U_{y} = \text{tr} \, \text{diag} \left( (10 \beta_{i}^{y} + 2\alpha_{i}^{x}/3)_{i \in [d]} \right) = \sum_{i=1}^{d} 10 \beta_{i}^{y} + 2\alpha_{i}^{x}/3 = 0.
\]

Moreover, the couples of quantum states \( (\rho_{x,y}, \rho_{-x,y}) \) and \( (\rho_{x,y}, \rho_{x,m+1-y}) \) are symmetric with respect to \( \mathbb{I}/d \) by the construction of \( (\alpha_{i}^{x})_{i,x} \) and \( (\beta_{i}^{x})_{i,x} \) hence

\[
u^{t,-x,m+1-y} = \langle \phi_{i}^{t} | U_{m+1-y} \, \text{diag} \left( (10 \beta_{i}^{m+1-y} + 2\alpha_{i}^{x}/3)_{i \in [d]} \right) U_{m+1-y} | \phi_{i}^{t} \rangle = -\langle \phi_{i}^{t} | U_{y} \, \text{diag} \left( (10 \beta_{i}^{y} + 2\alpha_{i}^{x}/3)_{i \in [d]} \right) U_{y} | \phi_{i}^{t} \rangle = -u_{i_{t}}^{t,x,y}.
\]

Suppose that \( \varepsilon \leq 0.05. \) We can start by controlling \( \Sigma_{2} \) using Jensen’s inequality:

\[
\Sigma_{2} = -\frac{1}{M} \sum_{x,y} \sum_{i_{1}, \ldots, i_{N}} \prod_{t=1}^{N} \left( 1 + \frac{u_{i_{t}}^{t,x,y} \varepsilon}{d} \right) \log \left( \frac{1}{M} \sum_{x,y} \prod_{t=1}^{N} \left( 1 + \frac{u_{i_{t}}^{t,x,y} \varepsilon}{d} \right) \right) 
\leq -\frac{1}{M} \sum_{x,y} \prod_{t=1}^{N} \left( 1 + \frac{u_{i_{t}}^{t,x,y} \varepsilon}{d} \right) \left( \frac{1}{M} \sum_{x,y} \log \left( \prod_{t=1}^{N} \left( 1 + \frac{u_{i_{t}}^{t,x,y} \varepsilon}{d} \right) \right) \right) 
= -\frac{1}{M} \sum_{x,y} \prod_{t=1}^{N} \left( 1 + \frac{u_{i_{t}}^{t,x,y} \varepsilon}{d} \right) \left( \frac{1}{M} \sum_{x,y,t} \log \left( 1 + \frac{u_{i_{t}}^{t,x,y} \varepsilon}{d} \right) \right) 
= -\frac{1}{M} \sum_{x,y} \prod_{t=1}^{N} \left( 1 + \frac{u_{i_{t}}^{t,x,y} \varepsilon}{d} \right) \left( \frac{1}{M} \sum_{|x|,|y| \leq m/2,t} \log \left( 1 + \frac{u_{i_{t}}^{t,x,y} \varepsilon}{d} \right) + \log \left( 1 - \frac{u_{i_{t}}^{t,x,y} \varepsilon}{d} \right) \right) 
= -\frac{1}{M} \sum_{x,y} \prod_{t=1}^{N} \left( 1 + \frac{u_{i_{t}}^{t,x,y} \varepsilon}{d} \right) \left( \frac{1}{M} \sum_{|x|,|y| \leq m/2,t} \log \left( 1 - \frac{u_{i_{t}}^{t,x,y} \varepsilon}{d} \right)^{2} \right). 
\]
Lemma C.7. Let $\{U_y\}_y$ be unitary matrices Haar$(d)$ distributed. We have with a probability at least $9/10$:

$$4N \sup_{\phi, \|\phi\|_2 \leq 1} \frac{1}{M} \sum_{|x|, |y| \leq m/2} \langle \phi | U_y O_{x,y} U_y^\dagger | \phi \rangle^2 \leq \mathcal{O} \left( \frac{N \varepsilon^2 \log(m)}{m} + \frac{N \varepsilon^2}{d} \right).$$

Now, we can use the inequality $-\log(1 - x^2) \leq 2x^2$ for $|x| \leq 1/\sqrt{2}$:

$$\Sigma_2 \leq -\frac{1}{M} \sum_{x,y,t} \prod_{i=1}^N \left( \frac{1 + u_{it}^{x,y} \varepsilon}{d} \right) \left( \frac{1}{M} \sum_{|x|, |y| \leq m/2,t} \log \left( 1 - \left( u_{it}^{x,y} \varepsilon \right)^2 \right) \right)$$

$$\leq \frac{1}{M} \sum_{x,y,t} \prod_{i=1}^N \left( \frac{1 + u_{it}^{x,y} \varepsilon}{d} \right) \left( \frac{1}{M} \sum_{|x|, |y| \leq m/2,t} 2\left( u_{it}^{x,y} \varepsilon \right)^2 \right)$$

$$\leq \frac{1}{M} \sum_{x,y,t} \prod_{i=1}^N \left( 1 + u_{it}^{x,y} \varepsilon \right) \left( \sum_{\phi, \|\phi\|_2 \leq 1} \frac{1}{M} \sum_{|x|, |y| \leq m/2} 2\langle \phi | U_y O_{x,y} U_y^\dagger | \phi \rangle^2 \varepsilon^2 \right)$$

Using the fact that $\sum_{i} u_{it}^{x,y} = 0$ for all $t, x, y$ along with the inequality $(1+x) \log(1+x) + (1-x) \log(1-x) \leq 2x^2$ for $|x| \leq 1/\sqrt{2}$ we can upper bound the first sum $\Sigma_1$:

$$\Sigma_1 = \frac{1}{M} \sum_{x,y,t} \prod_{i=1}^N \left( 1 + u_{it}^{x,y} \varepsilon \right) \log \left( \prod_{i=1}^N \left( 1 + u_{it}^{x,y} \varepsilon \right) \right)$$

$$\leq \frac{1}{M} \sum_{x,y,t} \prod_{i=1}^N \left( 1 + u_{it}^{x,y} \varepsilon \right) \log \left( 1 + u_{it}^{x,y} \varepsilon \right)$$

$$\leq \frac{1}{M} \sum_{x,y,t} \prod_{i=1}^N \left( 1 + u_{it}^{x,y} \varepsilon \right) \log \left( 1 + u_{it}^{x,y} \varepsilon \right)$$

$$\leq \frac{1}{M} \sum_{x,y,t} \prod_{i=1}^N \left( 1 + u_{it}^{x,y} \varepsilon \right) \log \left( 1 + u_{it}^{x,y} \varepsilon \right)$$

$$\leq \frac{1}{M} \sum_{x,y,t} \prod_{i=1}^N \left( 1 + u_{it}^{x,y} \varepsilon \right) \log \left( 1 + u_{it}^{x,y} \varepsilon \right)$$

Finally the upper bounds on $\Sigma_1$ and $\Sigma_2$ imply the required upper bound on their sum $\Sigma_1 + \Sigma_2 = I(X, Y : I_1, \ldots, I_N)$.

Note that we need to take a supremum over all possible vectors $\phi$ because the learner knows the quantum states $\{\sigma_y\}_y$ and so it can choose measurements dependent on the unitaries $\{U_y\}_y$. We can now show that with high probability on the choice of the unitaries $\{U_y\}_y$, the latter supremum can bounded and so the mutual information too.

Lemma C.7. Let $\{U_y\}_y$ be unitary matrices Haar$(d)$ distributed. We have with a probability at least $9/10$:
Proof. To upper bound the previous supremum, we use a similar approach to [Chen et al., 2021]: For \( U \sim \text{Haar}(d) \), \( \phi \in B(0,1) \) and a trace-less Hermitian matrix \( O \), let \( f(\phi, U) = \langle \phi | UV^\dagger | \phi \rangle \), we have \( \mathbb{E}(f(\phi, U)) = \frac{1}{d} \text{tr}(O) \text{tr}(\langle \phi | \phi \rangle) = 0 \) (see Weingarten Calculus D.1) and \( f \) is \( 2\|O\|\)-Lipschitz:

\[
|f(U) - f(V)| \leq 2\|\langle \phi | (\mathcal{U} - V)\phi \rangle\| \leq 2\|O\|\|U - V\|_2.
\]

Therefore by the concentration inequality \[D.3\]

\[
P(|f(U)| > t) \leq \exp(-dt^2/48).
\]

Hence

\[
P(|f(U)|^2 > t) \leq \exp(-dt/48).
\]

For \( m/2 \) unitaries \( U_1, \ldots, U_{m/2} \) and \( \lambda = 2d/C \) for sufficiently large \( C \). Denote by \( X = |f(U)|^2 \), by Markov’s inequality:

\[
P\left( \frac{2}{m} \sum_{1 \leq g \leq m/2} |f(U_g)|^2 > t \right) \leq \exp(-\lambda mt/2) \mathbb{E}(f(X)^{m/2}) \leq \exp(-\lambda mt/2) \left( 1 + \int_0^\infty dx \lambda e^{\lambda x} e^{-dx/48} \right)^{m/2}
\]

\[
\leq \exp(-dmt/2C) (C')^{m/2} \leq \exp(-dmt/C + m \log(C'))
\]

with \( C' \) another constant. In order to prove an inequality valid for all \( \phi \in B(0,1) \), let’s take an \( \eta \)-net \( \{\phi_i\}_i \) of size at most \( (1 + 2/\eta)^{2d} \). For \( \phi \in B(0,1) \), there is \( \phi_i \) such that \( \|\phi - \phi_i\|_2 \leq \eta \). Moreover \( |f(\phi, U)| \leq ||O|| \) so

\[
\left| \frac{2}{m} \sum_{1 \leq g \leq m/2} f(\phi, U_g)^2 - f(\phi_1, U_g)^2 \right| \leq \frac{2}{m} \sum_{1 \leq y \leq m/2} |f(\phi, U_y)^2 - f(\phi_1, U_y)^2|
\]

\[
\leq \frac{2}{m} \sum_{1 \leq y \leq m/2} 2\|O\|((\langle \phi | \phi \rangle - \langle \phi_1 | \phi \rangle) U_0 U_0^\dagger | \phi \rangle) \leq 2\eta \|O\|^2.
\]

Therefore

\[
P\left( \exists \phi : \frac{2}{m} \sum_{1 \leq y \leq m/2} |f(\phi, U_y)|^2 > t + 2\eta \|O\|^2 \right) \leq P\left( \exists \phi_i : \frac{1}{m} \sum_{k=1}^m |f(\phi_i, U_k)|^2 > t \right)
\]

\[
\leq (1 + 2/\eta)^{2d} \exp(-dmt/C + m \log(C')).
\]

Taking \( \eta = 1/m \) yields:

\[
P\left( \exists \phi : \frac{2}{m} \sum_{1 \leq y \leq m/2} |f(\phi, U_y)|^2 > t + 2\|O\|^2/m \right) \leq (1 + 2m)^{2d} \exp(-dmt/C + m \log(C')).
\]

Applying the union bound, we can obtain:

\[
P\left( \exists \phi, \exists x, \frac{2}{m} \sum_{y \leq m/2} \langle \phi | U_y O_{x,y} U_y^\dagger | \phi \rangle^2 \geq t + \frac{2\|O_{x,y}\|^2}{m} \right) \leq 4e^{cd}(1 + 2m)^{2d} \exp(-dmt/C + m \log(C')).
\]

Let’s take \( t = C^{\log(4d) + cd + 2d \log(1 + 2m) + m \log(C')} \) in order to have

\[
P\left( \forall \phi, \frac{1}{M} \sum_{|x, y| \leq m/2} \langle \phi | U_y O_{x,y} U_y^\dagger | \phi \rangle^2 \leq t + \frac{2\|O_{x,y}\|^2}{m} \right)
\]

\[
\geq P\left( \forall \phi, \forall x, \frac{1}{m} \sum_{y \leq m/2} \langle \phi | U_y O_{x,y} U_y^\dagger | \phi \rangle^2 \leq t + \frac{2\|O_{x,y}\|^2}{m} \right)
\]

\[
\geq 9/10.
\]
Therefore we have the existence of $\{U_y\}_y$ such that for all $y \neq z$

$$\|\sigma_y - \sigma_z\|_\text{tr} > \varepsilon,$$

and

$$\sup_{\phi, \|\phi\| \leq 1} \frac{1}{M} \sum_{|x|, y \leq m/2} (\phi|U_y O_{x,y} U_y^\dagger|\phi)^2 \leq \frac{\text{tr}(O_{x,y}^2)}{d(d + 1)} + t + \frac{2\|O_{x,y}\|^2}{m} \leq 201 + C \frac{\log(40) + cd + 2d \log(1 + 2m) + m \log(C')}{dm} + \frac{242}{m}.$$

Finally, we showed the existence of quantum states $\{\sigma_{x,y}\}_{x,y}$ such that:

$$I(X, Y : I_1, \ldots, I_N) = O \left( \frac{1}{d} + \frac{\log(m)}{m} \right) N \varepsilon^2.$$

To sum up, we have shown the existence of quantum states $\{\sigma_{x,y}\}_{x,y}$ such that:

$$\Omega(\log(m) + d) \leq I(X, Y : X', Y') \leq I(X, Y : I_1, \ldots, I_N) \leq O \left( \frac{1}{d} + \frac{\log(m)}{m} \right) N \varepsilon^2.$$

We conclude that $N = \Omega \left( \min \left\{ \frac{md}{\log(m) \varepsilon^2}, \frac{d^2}{\varepsilon^2} \right\} \right)$.

### C.2 Adaptive strategies

It is important to see why this proof doesn’t work for adaptive strategies. The lower bound on the mutual information has nothing to do with the non-adaptive/adaptive option of the algorithm so it remains true. However, upper bounding the mutual information cannot be done the same way since now the POVM used at time $t$ depends on the previous outcomes. Let $\{u_t\}_{t=1}^N$ be a sequence constituted by the outcomes of a correct adaptive algorithm. Let $M^a_{<t} = \{|\phi_{<t}^u\rangle\langle\phi_{<t}^u|\}_v$ the POVM used at time $t$ given the previous outcomes $u_{<t}$. Recall that the mutual information between $(X, Y)$ and $(I_1, \ldots, I_N)$ can be expressed as:

$$I(X, Y : I_1, \ldots, I_N) = \Sigma_1 + \Sigma_2.$$

The second sum can be upper bounded by the same technique as before (using for example Jensen’s inequality and the inequality $- \log(1 - x^2) \leq 2x^2$) and yields the same upper bound. The first sum is more involved because the product cannot be simplified due to the dependence between the POVMs and the previous outcomes. To see this, we can try to simplify the first sum as far as possible:

$$\Sigma_1 = \frac{1}{M} \sum_{x,y} \sum_{u_1, \ldots, u_N} \prod_{t=1}^N \langle \phi_{u_t}^{x \vee ty} | \rho_{x,y} | \phi_{u_t}^{x \vee ty} \rangle \log \left( \prod_{t=1}^N \langle \phi_{u_t}^{x \vee ty} | \rho_{x,y} | \phi_{u_t}^{x \vee ty} \rangle \right)$$

$$= \frac{1}{M} \sum_{x,y} \sum_{u_1, \ldots, u_N} \prod_{t=1}^N \langle \phi_{u_t}^{x \vee ty} | \rho_{x,y} | \phi_{u_t}^{x \vee ty} \rangle \sum_{t=1}^N \log \left( \langle \phi_{u_t}^{x \vee ty} | \rho_{x,y} | \phi_{u_t}^{x \vee ty} \rangle \right)$$

$$= \frac{1}{M} \sum_{x,y} \sum_{u_1, \ldots, u_N} \prod_{t=1}^N \langle \phi_{u_t}^{x \vee ty} | \rho_{x,y} | \phi_{u_t}^{x \vee ty} \rangle \log \left( \langle \phi_{u_t}^{x \vee ty} | \rho_{x,y} | \phi_{u_t}^{x \vee ty} \rangle \right)$$

$$= \frac{1}{M} \sum_{x,y} \sum_{u_1, \ldots, u_N} \prod_{t=1}^N \langle \phi_{u_t}^{x \vee ty} | \rho_{x,y} | \phi_{u_t}^{x \vee ty} \rangle \log \left( \langle \phi_{u_t}^{x \vee ty} | \rho_{x,y} | \phi_{u_t}^{x \vee ty} \rangle \right),$$
where the last equality follows from the fact that

\[
\sum_{u_t} \langle \phi_{u_t}^{<t} | \rho_{x,y} | \phi_{u_t}^{<t} \rangle = \text{tr}(\rho_{x,y}) = 1,
\]

for \( t > k \) and \( \log \left( \langle \phi_{u_k}^{<k} | d\rho_{x,y} | \phi_{u_k}^{<k} \rangle \right) \) is independent from \( u_t \). But we are stuck at \( k \), we cannot simplify the sums on \( u_s \) for \( s < k \) since \( \langle \phi_{u_s}^{<s} | \rho_{x,y} | \phi_{u_s}^{<s} \rangle \) has common terms with \( \langle \phi_{u_k}^{<k} | \rho_{x,y} | \phi_{u_k}^{<k} \rangle \) which is inside the log function.

In order to circumvent this difficulty, we can upper bound the \( k^{th} \) term which poses the obstacle of simplification. Using the inequality \( \log(x) \leq x - 1 \) for all \( x > -1 \) we obtain:

\[
\Sigma_1 = \frac{1}{M} \sum_{x,y,k} \sum_{u_1, \ldots, u_k} \prod_{t=1}^{k} \langle \phi_{u_t}^{<t} | \rho_{x,y} | \phi_{u_t}^{<t} \rangle \log \left( \langle \phi_{u_k}^{<k} | d\rho_{x,y} | \phi_{u_k}^{<k} \rangle \right)
\]

\[
= \frac{1}{M} \sum_{x,y,k} \sum_{u_1, \ldots, u_k} \prod_{t=1}^{k} \langle \phi_{u_t}^{<t} | \rho_{x,y} | \phi_{u_t}^{<t} \rangle \left( \langle \phi_{u_k}^{<k} | d\rho_{x,y} | \phi_{u_k}^{<k} \rangle - 1 \right)
\]

\[
= \frac{1}{M} \sum_{x,y,k} \sum_{u_1, \ldots, u_k} \prod_{t=1}^{k} \langle \phi_{u_t}^{<t} | \rho_{x,y} | \phi_{u_t}^{<t} \rangle \left( \langle \phi_{u_k}^{<k} | d\rho_{x,y} | \phi_{u_k}^{<k} \rangle - 1 \right)
\]

\[
= \frac{1}{M} \sum_{x,y,k} \sum_{u_1, \ldots, u_k} \prod_{t=1}^{k} \langle \phi_{u_t}^{<t} | \rho_{x,y} | \phi_{u_t}^{<t} \rangle \left( \frac{I}{d} + \frac{O_{x,y}}{d} \right) |\phi_{u_t}^{<t}| \langle \phi_{u_k}^{<k} | \varepsilon O_{x,y} | \phi_{u_k}^{<k} \rangle
\]

\[
= \frac{1}{M} \sum_{x,y,k} \sum_{u_1, \ldots, u_k} \prod_{t=1}^{k-1} \langle \phi_{u_t}^{<t} | \rho_{x,y} | \phi_{u_t}^{<t} \rangle \left( \frac{I}{d} + \frac{O_{x,y}}{d} \right) |\phi_{u_t}^{<t}| \langle \phi_{u_k}^{<k} | \varepsilon O_{x,y} | \phi_{u_k}^{<k} \rangle
\]

\[
= \frac{1}{M} \sum_{x,y,k} \sum_{u_1, \ldots, u_k} \prod_{t=1}^{k-1} \langle \phi_{u_t}^{<t} | \rho_{x,y} | \phi_{u_t}^{<t} \rangle \left( \frac{I}{d} + \frac{O_{x,y}}{d} \right) |\phi_{u_t}^{<t}| \langle \phi_{u_k}^{<k} | O_{x,y} | \phi_{u_k}^{<k} \rangle
\]

\[
\leq \frac{1}{M} \sum_{x,y,k} \sum_{u_1, \ldots, u_k} \prod_{t=1}^{k-1} \langle \phi_{u_t}^{<t} | \rho_{x,y} | \phi_{u_t}^{<t} \rangle \left( \frac{I}{d} + \frac{O_{x,y}}{d} \right) |\phi_{u_t}^{<t}| \times \frac{1}{d} \times \text{tr}(\varepsilon O_{x,y})
\]

\[
\leq \frac{1}{M} \sum_{x,y,k} \sum_{u_1, \ldots, u_k} \prod_{t=1}^{k-1} \langle \phi_{u_t}^{<t} | \rho_{x,y} | \phi_{u_t}^{<t} \rangle \left( \frac{I}{d} + \frac{O_{x,y}}{d} \right) |\phi_{u_t}^{<t}| \times \frac{1}{d} \times \text{tr}(\varepsilon^2 O_{x,y}^2)
\]

\[
\leq \sum_{x,y,k} \sum_{u_1, \ldots, u_k} \prod_{t=1}^{k-1} \langle \phi_{u_t}^{<t} | \rho_{x,y} | \phi_{u_t}^{<t} \rangle \left( \frac{I}{d} + \frac{O_{x,y}}{d} \right) \leq 1 \times 11^2 \varepsilon^2
\]

\[
\leq 11^2 N\varepsilon^2,
\]

where we use again \( \sum_{u_t} \langle \phi_{u_t}^{<t} | O_{x,y} | \phi_{u_t}^{<t} \rangle = \text{tr}(O_{x,y}) = 0 \) for all \( t \) and

\[
\sum_{u_k} \langle \phi_{u_k}^{<k} | O_{x,y} | \phi_{u_k}^{<k} \rangle^2 = \sum_{u_k} \text{tr}(O_{x,y} | \phi_{u_k}^{<k} \rangle | \phi_{u_k}^{<k} \rangle) \leq \sum_{u_k} \text{tr}(O_{x,y}^2 | \phi_{u_k}^{<k} \rangle | \phi_{u_k}^{<k} \rangle) = \text{tr}(O_{x,y}^2) \leq 11^2 d.
\]
Therefore the mutual information can be upper bounded by
\[
I(X, Y : X', Y') \leq 121N\varepsilon^2 + 2N\sup_{\phi, ||\phi||_2 \leq 1} \frac{1}{M} \sum_{|x|, y \leq m/2} (\phi|U_y O_{x, y} U_y^\dagger|\phi)^2 \varepsilon^2
\]
\[
\leq 123N\varepsilon^2.
\]
Since the mutual information is always lower bounded by \(\Omega(\log(m) + d)\) we conclude that \(N = \Omega((d + \log(m)/\varepsilon^2))\). Finally, we have proven the following lower bound on adaptive strategies for hypothesis selection problem:

**Proposition C.8.** Any learning algorithm with adaptive independent measurements requires
\[
N \geq \Omega\left(\frac{d + \log(m)}{\varepsilon^2}\right)
\]
copies of \(\rho\) to find the closest quantum state \(\sigma_i^*\) to \(\rho\) and approximate \(\rho\) to at most \(\varepsilon/10\) with at least a probability \(2/3\).

This Proposition implies that Alg. \([\text{Alg} 1]\) is almost optimal and \(\tilde{\Theta}(d/\varepsilon^2)\) is the optimal copy complexity of hypothesis selection problem using adaptive independent measurements.

**D Technical lemmas**

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

**D.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 \(\pi\) a permutation of \([n]\), let \(Wg(\pi, d)\) denotes the Weingarten function of dimension \(d\). The following lemma is crucial for our results.

**Lemma D.1.** \(\text{[Gu, 2013]}\) 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
\[
E(\text{tr}(UB_1 U^* A_1 U \ldots UB_n U^* A_n)) = \sum_{\alpha, \beta \in S_n} Wg(\beta\alpha^{-1}, d)\text{tr}_{\beta^{-1}}(B_1, \ldots, B_n)\text{tr}_{\alpha\gamma_n}(A_1, \ldots, A_n),
\]
where \(\gamma_n = (12 \ldots n)\) and \(\text{tr}_\sigma(M_1, \ldots, M_n) = \Pi_j \text{tr}(\Pi_i \in C_j M_i)\) for \(\sigma = \Pi_j C_j\) and \(C_j\) are cycles.

We need also some values of Weingarten function:

**Lemma D.2.**
- \(Wg((1), d) = \frac{1}{d^2}\),
- \(Wg((12), d) = \frac{1}{d^2-1}\),
- \(Wg((1)(2), d) = \frac{1}{d^2-1}\),
- \(Wg((123), d) = \frac{2}{d^2(d^2-1)(d^2-4)}\),
- \(Wg((1)(2)(3), d) = \frac{1}{d^2(d^2-1)(d^2-4)}\),
- \(Wg((1)(2)(3), d) = \frac{d^2-2}{d^2(d^2-1)(d^2-4)}\).

**D.2 Concentration inequalities for Haar-random unitary matrices**

**Theorem D.3.** \(\text{[Meckes et al., 2013]}\) Let \(M = U(d)^k\) endowed by the \(L_2\)-norm of Hilbert-Schmidt metric. If \(F : M \to \mathbb{R}\) is \(L\)-Lipschitz, then for any \(t > 0\)
\[
P(|F(U_1, \ldots, U_k) - E(F(U_1, \ldots, U_k))| \geq t) \leq e^{-dt^2/12L^2},
\]
where \(U_1, \ldots, U_k\) are independent Haar-distributed unitary matrices.