Online Learning of Quantum States

Scott Aaronson
UT Austin *
aaronson@cs.utexas.edu

Xinyi Chen
Google AI Princeton †
xinyic@google.com

Elad Hazan
Princeton University and Google AI Princeton
ehazan@cs.princeton.edu

Satyen Kale
Google AI, New York
satyenkale@google.com

Ashwin Nayak
University of Waterloo ‡
ashwin.nayak@uwaterloo.ca

Abstract

Suppose we have many copies of an unknown $n$-qubit state $\rho$. We measure some copies of $\rho$ using a known two-outcome measurement $E_1$, then other copies using a measurement $E_2$, and so on. At each stage $t$, we generate a current hypothesis $\omega_t$ about the state $\rho$, using the outcomes of the previous measurements. We show that it is possible to do this in a way that guarantees that $|\text{Tr}(E_i \omega_t) - \text{Tr}(E_i \rho)|$, the error in our prediction for the next measurement, is at least $\varepsilon$ at most $O(n/\varepsilon^2)$ times. Even in the “non-realizable” setting—where there could be arbitrary noise in the measurement outcomes—we show how to output hypothesis states that incur at most $O(\sqrt{Tn})$ excess loss over the best possible state on the first $T$ measurements. These results generalize a 2007 theorem by Aaronson on the PAC-learnability of quantum states, to the online and regret-minimization settings. We give three different ways to prove our results—using convex optimization, quantum postselection, and sequential fat-shattering dimension—which have different advantages in terms of parameters and portability.

1 Introduction

State tomography is a fundamental task in quantum computing of great practical and theoretical importance. In a typical scenario, we have access to an apparatus that is capable of producing many copies of a quantum state, and we wish to obtain a description of the state via suitable measurements. Such a description would allow us, for example, to check the accuracy with which the apparatus constructs a specific target state.

How many single-copy measurements are needed to “learn” an unknown $n$-qubit quantum state $\rho$? Suppose we wish to reconstruct the full $2^n \times 2^n$ density matrix, even approximately, to within $\varepsilon$ in trace distance. If we make no assumptions about $\rho$, then it is straightforward to show that the number of measurements needed grows exponentially with $n$. In fact, even when we allow joint measurement of multiple copies of the state, an exponential number of copies of $\rho$ are required (see, *Supported by a Vannevar Bush Faculty Fellowship from the US Department of Defense. Part of this work was done while the author was supported by an NSF Alan T. Waterman Award.

†Part of this work was done when the author was a research assistant at Princeton University.

‡Research supported in part by NSERC Canada.

e.g., O’Donnell and Wright [2016], Haah et al. [2017]). (A “joint measurement” of two or more states on disjoint sequences of qubits is a single measurement of all the qubits together.)

Suppose, on the other hand, that there is some probability distribution $D$ over possible yes/no measurements, where we identify the measurements with $2^n \times 2^n$ Hermitian matrices $E$ with eigenvalues in $[0, 1]$. Further suppose we are only concerned about learning the state $\rho$ well enough to predict the outcomes of most measurements $E$ drawn from $D$—where “predict” means approximately calculating the probability, $\text{Tr}(E\rho)$, of a “yes” result. Then for how many (known) sample measurements $E_i$, drawn independently from $D$, do we need to know the approximate value of $\text{Tr}(E_i\rho)$, before we have enough data to achieve this?

Aaronson [2007] proved that the number of sample measurements needed, $m$, grows only linearly with the number of qubits $n$. What makes this surprising is that it represents an exponential reduction compared to full quantum state tomography. Furthermore, the prediction strategy is extremely simple. Informally, we merely need to find any “hypothesis state” $\omega$ that satisfies $\text{Tr}(E_i\omega) \approx \text{Tr}(E_i\rho)$ for all the sample measurements $E_1, \ldots, E_m$. Then with high probability over the choice of sample measurements, that hypothesis $\omega$ necessarily “generalizes”, in the sense that $\text{Tr}(E\omega) \approx \text{Tr}(E\rho)$ for most additional $E$’s drawn from $D$. The learning theorem led to followup work including a full characterization of quantum advice (Aaronson and Drucker [2014]); efficient learning for stabilizer states (Rocchetto [2017]); the “shadow tomography” protocol (Aaronson [2018]); and recently, the first experimental demonstration of quantum state PAC-learning (Rocchetto et al. [2017]).

A major drawback of the learning theorem due to Aaronson is the assumption that the sample measurements are drawn independently from $D$—and moreover, that the same distribution $D$ governs both the training samples, and the measurements on which the learner’s performance is later tested. It has long been understood, in computational learning theory, that these assumptions are often unrealistic: they fail to account for adversarial environments, or environments that change over time. This is precisely the state of affairs in current experimental implementations of quantum information processing. Not all measurements of quantum states may be available or feasible in a specific implementation, which measurements are feasible is dictated by Nature, and as we develop more control over the experimental set-up, more sophisticated measurements become available. The task of learning a state prepared in the laboratory thus takes the form of a game, with the theorist on one side, and the experimentalist and Nature on the other: the theorist is repeatedly challenged to predict the behaviour of the state with respect to the next measurement that Nature allows the experimentalist to realize, with the opportunity to refine the hypothesis as more measurement data become available.

It is thus desirable to design learning algorithms that work in the more stringent online learning model. Here the learner is presented a sequence of input points, say $x_1, x_2, \ldots$, one at a time. Crucially, there is no assumption whatsoever about the $x_i$’s: the sequence could be chosen adversarially, and even adaptively, which means that the choice of $x_t$ might depend on the learner’s behavior on $x_1, \ldots, x_{t-1}$. The learner is trying to learn some unknown function $f(x)$, about which it initially knows only that $f$ belongs to some hypothesis class $H$—or perhaps not even that; we also consider the scenario where the learner simply tries to compete with the best predictor in $H$, which might or might not be a good predictor. The learning proceeds as follows: for each $t$, the learner first guesses a value $y_t$ for $f(x_t)$, and is then told the true value $f(x_t)$, or perhaps only an approximation of this value. Our goal is to design a learning algorithm with the following guarantee: regardless of the sequence of $x_t$’s, the learner’s guess, $y_t$, will be far from the true value $f(x_t)$ at most $k$ times (where $k$, of course, is as small as possible). The $x_t$’s on which the learner errs could be spaced arbitrarily; all we require is that they be bounded in number.

This leads to the following question: can the learning theorem established by Aaronson [2007] be generalized to the online learning setting? In other words: is it true that, given a sequence $E_1, E_2, \ldots$ of yes/no measurements, where each $E_i$ is followed shortly afterward by an approximation of $\text{Tr}(E_i\rho)$, there is a way to anticipate the $\text{Tr}(E_i\rho)$ values by guesses $y_t \in [0, 1]$, in such a way that $|y_t - \text{Tr}(E_i\rho)| > \varepsilon$ at most, say, $O(n)$ times (where $\varepsilon > 0$ is some constant, and $n$ again is the number of qubits)? The purpose of this paper is to provide an affirmative answer.

Throughout the paper, we consider only two-outcome measurements of an $n$ qubit mixed state $\rho$, and we specify such a measurement by a $2^n \times 2^n$ Hermitian matrix $E$ with eigenvalues in $[0, 1]$. We say that $E$ “accepts” $\rho$ with probability $\text{Tr}(E\rho)$ and “rejects” $\rho$ with probability $1 - \text{Tr}(E\rho)$. We prove that:
**Theorem 1.** Let $\rho$ be an $n$-qubit mixed state, and let $E_1, E_2, \ldots$ be a sequence of 2-outcome measurements that are revealed to the learner one by one, each followed by a value $b_t \in [0, 1]$ such that $|\text{Tr}(E_t \rho) - b_t| \leq \varepsilon/3$. Then there is an explicit strategy for outputting hypothesis states $\omega_1, \omega_2, \ldots$ such that $|\text{Tr}(E_t \omega_t) - \text{Tr}(E_t \rho)| > \varepsilon$ for at most $O\left(\frac{n}{\varepsilon^2}\right)$ values of $t$.

We also prove a theorem for the so-called regret minimization model (i.e., the “non-realizable case”), where we make no assumption about the input data arising from an actual quantum state, and our goal is simply to do no much worse than the best hypothesis state that could be found with perfect foresight. In this model, the measurements $E_1, E_2, \ldots$ are presented to a learner one-by-one. In iteration $t$, after seeing $E_t$, the learner is challenged to output a hypothesis state $\omega_t$, and then suffers a “loss” equal to $\ell_t(\text{Tr}(E_t \omega_t))$ where $\ell_t$ is a real function that is revealed to the learner. Important examples of loss functions are $L_1$ loss, when $\ell_t(z) := |z - b_t|$, and $L_2$ loss, when $\ell_t(z) := (z - b_t)^2$, where $b_t \in [0, 1]$. The number $b_t$ may be an approximation of $\text{Tr}(E_t \rho)$ for some fixed but unknown quantum state $\rho$, but is allowed to be arbitrary in general. In particular, the pairs $(E_t, b_t)$ may not be consistent with any quantum state. Define the regret $R_T$, after $T$ iterations, to be the amount by which the actual loss of the learner exceeds the loss of the best single hypothesis:

$$R_T := \sum_{t=1}^{T} \ell_t(\text{Tr}(E_t \omega_t)) - \min_{\varphi} \sum_{t=1}^{T} \ell_t(\text{Tr}(E_t \varphi)) .$$

The learner’s objective is to minimize regret. We show that:

**Theorem 2.** Let $E_1, E_2, \ldots$ be a sequence of two-outcome measurements on an $n$-qubit state presented to the learner, and $\ell_1, \ell_2, \ldots$ be the corresponding loss functions revealed in successive iterations in the regret minimization model. Suppose $\ell_t$ is convex and $L$-Lipschitz; in particular, for every $x \in \mathbb{R}$, there is a sub-derivative $\ell_t'(x)$ such that $|\ell_t'(x)| \leq L$. Then there is an explicit learning strategy that guarantees $R_T = O(L \sqrt{Tn})$ for all $T$. This is so even assuming the measurement $E_t$ and loss function $\ell_t$ are chosen adaptively, in response to the learner’s previous behavior.

Specifically, the algorithm applies to $L_1$ loss and $L_2$ loss, and achieves regret $O(\sqrt{Tn})$ for both.

The online strategies we present enjoy several advantages over full state tomography, and even over “state certification”, in which we wish to test whether a given quantum state is close to a desired state or far from it. Optimal algorithms for state tomography (O’Donnell and Wright [2016], Haah et al. [2017]) or certification (Bădescu et al. [2017]) require joint measurements of an exponential number of copies of the quantum state, and assume the ability to perform noiseless, universal quantum computation. On the other hand, the algorithms implicit in Theorems 1 and 2 involve only single-copy measurements, allow for noisy measurements, and capture ground reality more closely. They produce a hypothesis state that mimics the unknown state with respect to measurements that can be performed in a given experimental set-up, and the accuracy of prediction improves as the set of available measurements grows. For example, in the realizable case, i.e., when the data arise from an actual quantum state, the average $L_1$ loss per iteration is $O(\sqrt{n/T})$. This tends to zero, as the number of measurements becomes large. Note that $L_1$ loss may be as large as $1/2$ per iteration in the worst case, but this occurs at most $O(\sqrt{nT})$ times. Finally, the algorithms have run time exponential in the number of qubits in each iteration, but are entirely classical. Exponential run time is unavoidable, as the measurements are presented explicitly as $2^n \times 2^n$ matrices, where $n$ is the number of qubits. If we were required to output the hypothesis states, the length of the output—which is exponential in the number of qubits—would again entail exponential run time.

It is natural to wonder whether Theorems 1 and 2 leave any room for improvement. Theorem 1 is asymptotically optimal in its mistake bound of $O(n/\varepsilon^2)$; this follows from the property that $n$-qubit quantum states, considered as a hypothesis class, have $\varepsilon$-fat-shattering dimension $\Theta(n/\varepsilon^2)$ (see, for example, Arora et al. [2007]). On the other hand, there is room to improve Theorem 2. The bounds of which we are aware are $\Omega(\sqrt{Tn})$ for the $L_1$ loss (see, e.g., Arora et al. [2012] Theorem 4.1) in the non-realizable case and $\Omega(n)$ for the $L_2$ loss in the realizable case, when the feedback consists of the measurement outcomes. (The latter bound, as well as an $\Omega(\sqrt{Tn})$ bound for $L_1$ loss in the same setting, come from considering quantum mixed states that consist of $n$ independent classical coins, each of which could land heads with probability either $1/2$ or $1/2 + \varepsilon$. The parameter $\varepsilon$ is set to $\sqrt{n/T}$.)
We define the trace norm of a matrix $M$ as $\|M\|_\text{Tr} := \text{Tr} \sqrt{MM^\dagger}$, where $M^\dagger$ is the adjoint of $M$. We denote the $i$th eigenvalue of a Hermitian matrix $X$ by $\lambda_i(X)$, its minimum eigenvalue by $\lambda_{\min}(X)$, and its maximum eigenvalue by $\lambda_{\max}(X)$. We sometimes use the notation $X \cdot Y$ to denote the trace.
inner-product $\text{Tr}(X^\dagger Y)$ between two complex matrices of the same dimensions. By ‘log’ we denote the natural logarithm, unless the base is explicitly mentioned.

An $n$-qubit quantum state $\rho$ is an element of $C_n$, where $C_n$ is the set of all trace-1 positive semi-definite (PSD) complex matrices of dimension $2^n$:

$$C_n = \{ M \in \mathbb{C}^{2^n \times 2^n} : M = M^\dagger, M \succeq 0, \text{Tr}(M) = 1 \}.$$ 

Note that $C_n$ is a convex set. A two-outcome measurement of an $n$-qubit state is defined by a $2^n \times 2^n$ Hermitian matrix $E$ with eigenvalues in $[0, 1]$. The measurement $E$ “accepts” $\rho$ with probability $\text{Tr}(E \rho)$, and “rejects” with probability $1 - \text{Tr}(E \rho)$. For the algorithms we present in this article, we assume that a two-outcome measurement is specified via a classical description of its defining matrix $E$. In the rest of the article, unless mentioned otherwise, a “measurement” refers to a “two-outcome measurement”. We refer the reader to the book by Watrous [2018] for a more thorough introduction to the relevant concepts from quantum information.

**Online learning and regret.** In online learning of quantum states, we have a sequence of iterations $t = 1, 2, 3, \ldots$ of the following form. First, the learner constructs a state $\omega_t \in C_n$: we say that the learner “predicts” $\omega_t$. It then suffers a “loss” $\ell_t(\text{Tr}(E_t \omega_t))$ that depends on a measurement $E_t$, both of which are presented by an adversary. Commonly used loss functions are $L_2$ loss (also called “mean square error”), given by

$$\ell_t(z) := (z - b_t)^2,$$

and $L_1$ loss (also called “absolute loss”), given by

$$\ell_t(z) := |z - b_t|,$$

where $b_t \in [0, 1]$. The parameter $b_t$ may be an approximation of $\text{Tr}(E_t \rho)$ for some fixed quantum state $\rho$ not known to the learner, obtained by measuring multiple copies of $\rho$. However, in general, the parameter is allowed to be arbitrary.

The learner then “observes” feedback from the measurement $E_t$; the feedback is also provided by the adversary. The simplest feedback is the realization of a binary random variable $Y_t$ such that

$$Y_t = \begin{cases} 1 \quad \text{with probability } \text{Tr}(E_t \rho) \, , \\ 0 \quad \text{with probability } 1 - \text{Tr}(E_t \rho) \, . \end{cases}$$

Another common feedback is a number $b_t$ as described above, especially in case that the learner suffers $L_1$ or $L_2$ loss.

We would like to design a strategy for updating $\omega_t$ based on the loss, measurements, and feedback in all the iterations so far, so that the learner’s total loss is minimized in the following sense. We would like that over $T$ iterations (for a number $T$ known in advance), the learner’s total loss is not much more than that of the hypothetical strategy of outputting the same quantum state $\varphi$ at every time step, where $\varphi$ minimizes the total loss with perfect hindsight. Formally this is captured by the notion of regret $R_T$, defined as

$$R_T := \sum_{t=1}^T \ell_t(\text{Tr}(E_t \omega_t)) - \min_{\varphi \in C_n} \sum_{t=1}^T \ell_t(\text{Tr}(E_t \varphi)).$$

The sequence of measurements $E_t$ can be arbitrary, even adversarial, based on the learner’s previous actions. Note that if the loss function is given by a fixed state $\rho$ (as in the case of mean square error), the minimum total loss would be 0. This is called the “realizable” case. However, in general, the loss function presented by the adversary need not be consistent with any quantum state. This is called the “non-realizable” case.

A special case of the online learning setting is called agnostic learning: here the measurements $E_t$ are drawn from a fixed and unknown distribution $\mathcal{D}$. The setting is called “agnostic” because we still do not assume that the losses correspond to any actual state $\rho$ (i.e., the setting may be non-realizable).

**Online mistake bounds.** In some online learning scenarios the quantity of interest is not the mean square error, or some other convex loss, but rather simply the total number of “mistakes” made. For example, we may be interested in the number of iterations in which the predicted probability of
acceptance $\text{Tr}(E_t \omega_t)$ is more than $\varepsilon$-far from the actual value $\text{Tr}(E_t \rho)$, where $\rho$ is again a fixed state not known to the learner. More formally, let

$$\ell_t(\text{Tr}(E_t \omega_t)) := |\text{Tr}(E_t \omega_t) - \text{Tr}(E_t \rho)|$$

be the absolute loss function. Then the goal is to bound the number of iterations in which $\ell_t(\text{Tr}(E_t \omega_t)) > \varepsilon$, regardless of the sequence of measurements $E_t$ presented by the adversary. We assume that in this setting the adversary provides as feedback an approximation $b_t \in [0, 1]$ that satisfies $|\text{Tr}(E_t \rho) - b_t| \leq \frac{\varepsilon}{3}$.

3 Online learning of quantum states

In this section, we use techniques from online convex optimization to minimize regret. The same algorithms may be adapted to also minimize the number of mistakes made.

3.1 Regularized Follow-the-Leader

We first follow the template of the Regularized Follow-the-Leader algorithm (RFTL; see, for example, Hazan [2015, Chapter 5]). The algorithm below makes use of von Neumann entropy, which relates to the Matrix Exponentiated Gradient algorithm (Tsuda et al. [2005]).

\begin{algorithm}
1: Input: $T, K := C_n, \eta < \frac{1}{2}$
2: Set $\omega_1 := 2^{-n}I$
3: for $t = 1, \ldots, T$ do
4: Predict $\omega_t$. Consider the convex and $L$-Lipschitz loss function $\ell_t : \mathbb{R} \to \mathbb{R}$ given by measurement $E_t$:
5: $\ell_t(\text{Tr}(E_t \varphi))$. Let $\ell_t'(x)$ be a sub-derivative of $\ell_t$ with respect to $x$. Define
6: $\nabla_t := \ell_t'(\text{Tr}(E_t \omega_t))E_t$.
7: Update decision according to the RFTL rule with von Neumann entropy:
8: $\omega_{t+1} := \arg\min_{\varphi \in K} \left\{ \eta \sum_{s=1}^{t} \text{Tr}(\nabla_s \varphi) + \sum_{i=1}^{2^n} \lambda_i(\varphi) \log \lambda_i(\varphi) \right\}$.
9: end for
\end{algorithm}

Remark 1: The mathematical program in Eq. (1) is convex, and thus can be solved in polynomial time in the dimension, which is $2^n$.

Theorem 3. Setting $\eta = \sqrt{\frac{(\log 2)^n}{2T^2}}$, the regret of Algorithm 1 is bounded by $2L \sqrt{\frac{2 \log 2}{T}}$. The proof of Theorem 3 appears in Appendix B. The proof is along the lines of Hazan [2015, Theorem 5.2], except that the loss function does not take a raw state as input, and our domain for optimization is complex. Therefore, the mean value theorem does not hold, which means we need to approximate the Bregman divergence instead of replacing it by a norm as in the original proof. Another subtlety is that convexity needs to be carefully defined with respect to the complex domain.
3.2 Matrix Multiplicative Weights

The Matrix Multiplicative Weights (MMW) algorithm [Arora and Kale 2016] provides an alternative means of proving Theorem 1. The algorithm follows the template of Algorithm 1 with step 5 replaced by the following update rule:

\[ \omega_{t+1} := \frac{\exp\left(-\frac{n}{T} \sum_{\tau=1}^{T} \nabla_{\tau}\right)}{\text{Tr}\left(\exp\left(-\frac{n}{T} \sum_{\tau=1}^{T} \nabla_{\tau}\right)\right)} . \]

In the notation of [Arora and Kale 2016], this algorithm is derived using the loss matrices \( M_t = \frac{1}{T} \nabla_{t} = \frac{1}{T} \ell'_t(\text{Tr}(E_t \omega_t)) E_t \). Since \( \|E_t\| \leq 1 \) and \( |\ell'_t(\text{Tr}(E_t \omega_t))| \leq L \), we have \( \|M_t\| \leq 1 \), as required in the analysis of the Matrix Multiplicative Weights algorithm. We have the following regret bound for the algorithm (proved in Appendix C):

**Theorem 4.** Setting \( \eta = \sqrt{\frac{(\log 2) n}{4L}} \), the regret of the algorithm based on the update rule (2) is bounded by \( 2L \sqrt{(\log 2) T n} \).

3.3 Proof of Theorem 1

Consider either the RFTL or MMW based online learning algorithm described in the previous subsections, with the 1-Lipschitz convex absolute loss function \( \ell_t(x) = |x - b_t| \). We run the algorithm in a sub-sequence of the iterations, using only the measurements presented in those iterations. The subsequence of iterations is determined as follows. Let \( \omega_t \) denote the hypothesis maintained by the algorithm in iteration \( t \). We run the algorithm in iteration \( t \) if \( \ell_t(\text{Tr}(E_t \omega_t)) > \frac{2\eta}{3} \).

Note that whenever \( |\text{Tr}(E_t \omega_t) - \text{Tr}(E_t \rho)| > \varepsilon \), we have \( \ell_t(\text{Tr}(E_t \omega_t)) > \frac{2\varepsilon}{3} \), so we update the hypothesis according to the RFTL/MMW rule in that iteration.

As we explain next, the algorithm makes at most \( O\left(\frac{2\varepsilon t}{\eta}\right) \) updates regardless of the number of measurements presented (i.e., regardless of the number of iterations), giving the required mistake bound. For the true quantum state \( \rho \), we have \( \ell_t(\text{Tr}(E_t \rho)) < \frac{\varepsilon}{3} \) for all \( t \). Thus if the algorithm makes \( T \) updates (i.e., we run the algorithm in \( T \) of the iterations), the regret bound implies that \( \frac{2\varepsilon}{3} T \leq \frac{\varepsilon}{3} T + O(\sqrt{T n}) \).

Simplifying, we get the bound \( T = O\left(\frac{(\log 2) n}{4L}\right) \), as required.

4 Learning Using Postselection

In this section, we give a direct route to proving a slightly weaker version of Theorem 1 one that does not need the tools of convex optimization, but only tools intrinsic to quantum information.

In the following, by a “register” we mean a designated sequence of qubits. Given a two-outcome measurement \( E \) on \( n \)-qubits states, we define an operator \( \mathcal{M} \) that “postselects” on acceptance by \( E \). (While a measurement results in a random outcome distributed according to the probability of acceptance or rejection, postselection is a hypothetical operation that produces an outcome of one’s choice with certainty.) Let \( U \) be any unitary operation on \( n + 1 \) qubits that maps states of the form \( |\psi\rangle|0\rangle \) to \( \sqrt{E} |\psi\rangle|0\rangle + \sqrt{1 - E} |\psi\rangle|1\rangle \). Such a unitary operation always exists (see, e.g., [Watrous 2018, Theorem 2.42]). Denote the \((n+1)\)th qubit by register \( B \). Let \( \Pi := \Pi \otimes |0\rangle\langle 0| \) be the orthogonal projection onto states that equal \( |0\rangle \) in register \( B \). Then we define the operator \( \mathcal{M} \) as

\[ \mathcal{M}(\phi) := \frac{1}{\text{Tr}(E \phi)} \text{Tr}_B \left(U^{-1} \Pi U \left(\phi \otimes |0\rangle\langle 0|\right) U^{-1} \Pi U \right), \]

if \( \text{Tr}(E \phi) \neq 0 \), and \( \mathcal{M}(\phi) := 0 \) otherwise. Here, \( \text{Tr}_B \) is the partial trace operator over qubit \( B \) [Watrous 2018, Section 1.1]. This operator \( \mathcal{M} \) has the effect of mapping the quantum state \( \phi \) to the (normalized) post-measurement state when we perform the measurement \( E \) and get outcome “yes” (i.e., the measurement “accepts”). We emphasize that we use a fresh ancilla qubit initialized to state \( |0\rangle \) as register \( B \) in every application of the operator \( \mathcal{M} \). We say that the postselection succeeds with probability \( \text{Tr}(E \phi) \).

We need a slight variant of a well-known result, which Aaronson called the “Quantum Union Bound” (see, for example, [Aaronson 2006, 2016, Wilde 2013]).
Theorem 5 (variant of Quantum Union Bound [Gao 2015]). Suppose we have a sequence of twooutcome measurements \( E_1, \ldots, E_k \), such that each \( E_i \) accepts a certain mixed state \( \varphi \) with probability at least \( 1 - \varepsilon \). Consider the corresponding operators \( M_1, M_2, \ldots, M_k \) that postselect on acceptance by the respective measurements \( E_1, E_2, \ldots, E_k \). Let \( \tilde{\varphi} \) denote the state \( (M_k M_{k-1} \cdots M_1)(\varphi) \) obtained by applying each of the \( k \) postselection operations in succession. Then the probability that all the postselection operations succeed, i.e., the \( k \) measurements all accept \( \varphi \), is at least \( 1 - 2\sqrt{k\varepsilon} \). Moreover, \( \| \tilde{\varphi} - \varphi \|_{\text{Tr}} \leq 4\sqrt{k\varepsilon} \).

We may infer the above theorem by applying Theorem 1 from [Gao 2015] to the state \( \varphi \).

Moreover, let 
\[
\text{Tr}(\rho) = \left| \sum_{i=1}^{3^n} a_i \right|^2,
\]
where \( a_i \) are the coefficients of the state \( \rho \) in the basis \( |x\rangle \), and let \( \varepsilon > 0 \) be a set of functions \( f : \{0, 1\}^n \rightarrow [0, 1] \), such as long as \( |b_i - \text{Tr}(E_i \rho)| \leq \varepsilon / 3 \) for every \( t \), we have
\[
|\text{Tr}(E_{i+1} \omega_t) - \text{Tr}(E_{i+1} \rho)| > \varepsilon
\]
for at most \( O\left(\frac{n}{\varepsilon} \log \frac{n}{\varepsilon}\right) \) values of \( t \). Here the \( E_i \)’s and \( b_i \)’s can otherwise be chosen adversarially.

5 Learning Using Sequential Fat-Shattering Dimension

In this section, we prove regret bounds using the notion of sequential fat-shattering dimension. Let \( S \) be a set of functions \( f : U \rightarrow \{0, 1\} \), and \( \varepsilon > 0 \). Then, following [Rakhlin et al. 2015], let the \( \varepsilon \)-sequential fat-shattering dimension of \( S \), or \( \text{sfat}_\varepsilon(S) \), be the largest \( k \) for which we can construct a complete binary tree \( T \) of depth \( k \), such that

- each internal vertex \( v \in T \) has associated with it a point \( x_v \in U \) and a real \( a_v \in [0, 1] \), and
- for each leaf vertex \( v \in T \) there exists an \( f \in S \) that causes us to reach \( v \) if we traverse \( T \) from the root such that at any internal node \( w \) we traverse the left subtree if \( f(x_w) \leq a_w - \varepsilon \) and the right subtree if \( f(x_w) \geq a_w + \varepsilon \). If we view the leaf \( v \) as a \( k \)-bit string, the function \( f \) is such that for all ancestors \( u \) of \( v \), we have \( f(x_u) \leq a_u - \varepsilon \) if \( v_i = 0 \), and \( f(x_u) \geq a_u + \varepsilon \) if \( v_i = 1 \), when \( u \) is at depth \( i - 1 \) from the root.

An \( n \)-qubit state \( \rho \) induces a function \( f \) on the set of two-outcome measurements \( E \) defined as \( f(E) := \text{Tr}(E \rho) \). With this correspondence in mind, we establish a bound on the sequential fat-shattering dimension of the set of \( n \)-qubit quantum states. The bound is based on a generalization of “random access coding” [Nayak 1999, Ambainis et al. 2002] called “serial encoding”. We derive the following bound on the length of serial encoding. Let \( H(x) := -x \log_2 x - (1 - x) \log_2(1 - x) \) be the binary entropy function.

Corollary 7. Let \( k \) and \( n \) be positive integers. For each \( k \)-bit string \( y := y_1 \cdots y_k \), let \( \rho_y \) be an \( n \)-qubit mixed state such that for each \( i \in \{1, 2, \ldots, k\} \), there is a two-outcome measurement \( E' \) that depends only on \( i \) and the prefix \( v := y_1 y_2 \cdots y_{i-1} \), and has the following properties

(iii) if \( y_i = 0 \) then \( \text{Tr}(E' \rho_y) \leq a_v - \varepsilon \), and
(iv) if \( y_i = 1 \) then \( \text{Tr}(E' \rho_y) \geq a_v + \varepsilon \),

where \( \varepsilon \in (0, 1/2] \) and \( a_v \in [0, 1] \) is a “pivot point” associated with the prefix \( v \). Then
\[
n \geq \left(1 - H\left(\frac{1-\varepsilon}{2}\right)\right) k.
\]

In particular, \( k = O\left(n/\varepsilon^2\right) \).
We conclude with some questions arising from this work. The regret bound established in Theorem 2
with

Theorem 8 establishes an earlier result due to [Aaronson 2007], which proved the same upper
bound for the “ordinary” (non-sequential) fat-shattering dimension of quantum states considered as a hypothesis class.

Now we may use existing results from the literature, which relate sequential fat-shattering dimension to online learnability. In particular, in the non-realizable case, [Rakhlin et al. 2015] recently showed the following:

**Theorem 9 [Rakhlin et al. 2015].** Let $S$ be a set of functions $f : U \rightarrow [0, 1]$ and for every integer $t \geq 1$, let $\ell_t : [0, 1] \rightarrow \mathbb{R}$ be a convex, $L$-Lipschitz loss function. Suppose we are sequentially presented elements $x_1, x_2, \ldots \in U$, with each $x_t$ followed by the loss function $\ell_t$. Then there exists a learning strategy that lets us output a sequence of hypotheses $f_1, f_2, \ldots \in S$, such that the regret is upper-bounded as:

\[
\sum_{t=1}^{T} \ell_t (f_t(x_t)) \leq \min_{f \in S} \sum_{t=1}^{T} \ell_t(f(x_t)) + 2LT \inf_{\alpha} \left\{ 4\alpha + \frac{12}{\sqrt{T}} \int_{\alpha}^{1} \sqrt{\text{sfat}_\beta(S) \log \left( \frac{2cT}{\beta} \right)} d\beta \right\}.
\]

This follows from Theorem 8 in [Rakhlin et al. 2015] as in the proof of Proposition 9 in the same article.

Combining Theorem 8 with Theorem 9 gives us the following:

**Corollary 10.** Suppose we are presented with a sequence of two-outcome measurements $E_1, E_2, \ldots$ of an $n$-qubit state, with each $E_t$ followed by a loss function $\ell_t$ as in Theorem 9. Then there exists a learning strategy that lets us output a sequence of hypothesis states $\omega_1, \omega_2, \ldots$ such that the regret after the first $T$ iterations is upper-bounded as:

\[
\sum_{t=1}^{T} \ell_t (\text{Tr}(E_t\omega_t)) \leq \min_{\omega \in C_n} \sum_{t=1}^{T} \ell_t (\text{Tr}(E_t\omega)) + O\left( L\sqrt{nT \log^{3/2} T} \right).
\]

Note that the result due to [Rakhlin et al. 2015] is non-explicit. In other words, by following this approach, we do not derive any specific online learning algorithm for quantum states that has the stated upper bound on regret; we only prove non-constructively that such an algorithm exists.

We expect that the approach in this section, based on sequential fat-shattering dimension, could also be used to prove a mistake bound for the realizable case, but we leave that to future work.

### 6 Open Problems

We conclude with some questions arising from this work. The regret bound established in Theorem 4 for $L_1$ loss is tight. Can we similarly achieve optimal regret for other loss functions of interest, for example for $L_2$-loss? It would also be interesting to obtain regret bounds in terms of the loss of the best quantum state in hindsight, as opposed to $T$ (the number of iterations), using the techniques in this article. Such a bound has been shown by [Tsuda et al. 2005, Lemma 3.2] for $L_2$-loss using the Matrix Exponentiated Gradient method.

In what cases can one do online learning of quantum states, not only with few samples, but also with a polynomial amount of computation? What is the tight generalization of our results to measurements with $d$ outcomes? Is it the case, in online learning of quantum states, that any algorithm works, or is there a polynomial amount of computation? Is it the case, in online learning of quantum states, that any algorithm works, so long as it produces hypothesis states that are approximately consistent with all the data seen so far? Note that none of our three proof techniques seem to imply this general conclusion.

### References


A Auxiliary Lemmas

The following lemma is from (Tsuda et al. [2005]), given here for completeness.

**Lemma 11.** For Hermitian matrices $A, B$ and Hermitian PSD matrix $X$, if $A \succeq B$, then $\text{Tr}(AX) \geq \text{Tr}(BX)$.

**Proof.** Let $C := A - B$. By definition, $C \succeq 0$. It suffices to show that $\text{Tr}(CX) \geq 0$. Let $VQV^*$ be the eigendecomposition of $X$, and let $C = VPV^*$, where $P := V^*CV \succeq 0$. Then $\text{Tr}(CX) = \text{Tr}(VPQV^*) = \text{Tr}(QP) = \sum_{i=1}^n P_iQ_{ii}$. Since $P \succeq 0$ and all the eigenvalues of $X$ are nonnegative, $P_{ii} \geq 0$, $Q_{ii} \geq 0$. Therefore $\text{Tr}(CX) \geq 0$.

**Lemma 12.** If $A, B$ are Hermitian matrices, then $\text{Tr}(AB) \in \mathbb{R}$.

**Proof.** The proof is similar to Lemma 11. Let $VQV^*$ be the eigendecomposition of $A$. Then $Q$ is a real diagonal matrix. We have $B = VPV^*$, where $P := V^*BV$. Note that $P^* = V^*B^*V = P$, so $P$ has a real diagonal. Then $\text{Tr}(AB) = \text{Tr}(VQV^*VPV^*) = \text{Tr}(VQPV^*) = \text{Tr}(QP) = \sum_{i=1}^n Q_{ii}P_{ii}$. Since $Q_{ii}, P_{ii} \in \mathbb{R}$ for all $i$, $\text{Tr}(AB) \in \mathbb{R}$.

B Proof of Theorem

**Proof of Theorem** Since $\ell_t$ is convex, for all $\varphi \in \mathcal{K}$,

$$
\ell_t(\text{Tr}(E_t\omega_t)) - \ell_t(\text{Tr}(E_t\varphi)) \leq \ell_t'(\text{Tr}(E_t\omega_t)) [\text{Tr}(E_t\omega_t) - \text{Tr}(E_t\varphi)] = \nabla_t \cdot (\omega_t - \varphi).
$$

(Recall that $\cdot \cdot'$ denotes the trace inner-product between complex matrices of the same dimensions.)

Summing over $t$,

$$
\sum_{t=1}^T [\ell_t(\text{Tr}(E_t\omega_t)) - \ell_t(\text{Tr}(E_t\varphi))] \leq \sum_{t=1}^T [\text{Tr}(\nabla_t\omega_t) - \text{Tr}(\nabla_t\varphi)].
$$

Define $g_t(X) = \nabla_t \cdot X$, and $g_0(X) = \frac{1}{\eta}R(X)$, where $R(X)$ is the negative von Neumann Entropy of $X$ (in nats). Denote $D_R^2 := \max_{\varphi, \varphi' \in \mathcal{K}}\{R(\varphi) - R(\varphi')\}$. By [Hazan 2015] Lemma 5.2, for any $\varphi \in \mathcal{K}$, we have

$$
\sum_{t=1}^T [g_t(\omega_t) - g_t(\varphi)] \leq \sum_{t=1}^T \nabla_t \cdot (\omega_t - \omega_{t+1}) + \frac{1}{\eta}D_R^2.
$$

(4)

Define $\Phi_t(X) = \{\eta \sum_{s=1}^t \nabla_s \cdot X + R(X)\}$, then the convex program in line 5 of Algorithm finds the minimizer of $\Phi_t(X)$ in $\mathcal{K}$. The following claim shows that that the minimizer is always positive definite (proof provided later in this section):

**Claim 13.** For all $t \in \{1, 2, ..., T\}$, we have $\omega_t > 0$.

For $X > 0$, we can write $R(X) = \text{Tr}(X \log X)$, and define

$$
\nabla \Phi_t(X) := \eta \sum_{s=1}^t \nabla_s + \mathbb{1} + \log X.
$$

The definition of $\nabla \Phi_t(X)$ is analogous to the gradient of $\Phi_t(X)$ if the function is defined over real symmetric matrices. Moreover, the following condition, similar to the optimality condition over a real domain, is satisfied (proof provided later in this section).

**Claim 14.** For all $t \in \{1, 2, \ldots, T - 1\}$,

$$
\nabla \Phi_t(\omega_{t+1}) \cdot (\omega_t - \omega_{t+1}) \geq 0.
$$

(5)
Denote 
\[ B_{\Phi_t}(\omega_t||\omega_{t+1}) := \Phi_t(\omega_t) - \Phi_t(\omega_{t+1}) - \nabla \Phi_t(\omega_{t+1}) \cdot (\omega_t - \omega_{t+1}) \, . \]

Then by the Pinsker inequality (see, for example, Carlen and Lieb [2014] and the references therein),
\[ \frac{1}{2} \| \omega_t - \omega_{t+1} \|_{\text{Tr}}^2 \leq \text{Tr}(\omega_t \log \omega_t) - \text{Tr}(\omega_t \log \omega_{t+1}) = B_{\Phi_t}(\omega_t||\omega_{t+1}) \, . \]

We have
\[
B_{\Phi_t}(\omega_t||\omega_{t+1}) = \Phi_t(\omega_t) - \Phi_t(\omega_{t+1}) - \nabla \Phi_t(\omega_{t+1}) \cdot (\omega_t - \omega_{t+1}) \\
\leq \Phi_t(\omega_t) - \Phi_t(\omega_{t+1}) \\
= \Phi_{t-1}(\omega_t) - \Phi_{t-1}(\omega_{t+1}) + \eta \nabla \Phi_t(\omega_t - \omega_{t+1}) \\
\leq \eta \nabla \Phi_t(\omega_t - \omega_{t+1}) \, ,
\]
where the first inequality follows from Claim 14, and the second because \( \Phi_{t-1}(\omega_t) \leq \Phi_{t-1}(\omega_{t+1}) \) \( \omega_t \) minimizes \( \Phi_{t-1}(X) \). Therefore
\[
\frac{1}{2} \| \omega_t - \omega_{t+1} \|_{\text{Tr}}^2 \leq \eta \nabla \Phi_t(\omega_t - \omega_{t+1}) \, .
\]

Let \( \| M \|_{*}^{\text{tr}} \) denote the dual of the trace norm, i.e., the spectral norm of the matrix \( M \). By Generalized Cauchy-Schwartz [Bhatia, 1997, Exercise IV.1.14, page 90],
\[
\nabla \Phi_t(\omega_t - \omega_{t+1}) \leq \| \nabla \Phi_t \|_{\text{tr}} \| \omega_t - \omega_{t+1} \|_{\text{Tr}} \\
\leq \| \nabla \Phi_t \|_{\text{tr}} \sqrt{2\eta} \nabla \Phi_t(\omega_t - \omega_{t+1}) \, ,
\]
by Eq. (7).

Rearranging,
\[
\nabla \Phi_t(\omega_t - \omega_{t+1}) \leq \frac{2\eta \nabla \Phi_t(\omega_t - \omega_{t+1})}{|Q| G_R} \leq 2\eta G_R^2 \, ,
\]
where \( G_R \) is an upper bound on \( \| \nabla \Phi_t \|_{\text{tr}} \). Combining with Eq. (4), we arrive at the following bound
\[
\sum_{t=1}^{T} \| \nabla \Phi_t(\omega_t - \omega_{t+1}) \|_{\text{tr}} \leq \frac{1}{\eta} D_R^2 \leq 2\eta TG_R^2 + \frac{1}{\eta} D_R^2 \, .
\]

Taking \( \eta = \frac{D_R}{G_R \sqrt{2T}} \), we get
\[
\sum_{t=1}^{T} \| \nabla \Phi_t(\omega_t - \omega_{t+1}) \|_{\text{tr}} \leq 2D_R G_R \sqrt{2T} \, .
\]

Combining with Eq. (7), we get the following bound
\[
\sum_{t=1}^{T} \left[ \ell_t(\text{Tr}(E_t \omega_t)) - \ell_t(\text{Tr}(E_t \varphi)) \right] \leq \sum_{t=1}^{T} \| \nabla \Phi_t(\omega_t - \omega_{t+1}) \|_{\text{tr}} \leq 2D_R G_R \sqrt{2T} \, .
\]

We proceed to show that \( D_R = \sqrt{(\log 2)n} \). Let \( \Delta_{2^n} \) denote the set of probability distributions over \( [2^n] \). By definition,
\[
D_R = \max_{\varphi, \varphi' \in \Delta_{2^n}} \{ R(\varphi) - R(\varphi') \} = \max_{\varphi \in \Delta_{2^n}} \frac{1}{L} \log \frac{1}{\lambda_i} = n \log 2 \, .
\]

Since the dual norm of the trace norm is the spectral norm, we have
\[
\| \nabla \Phi_t \|_{\text{tr}} = \| \ell_t'(\text{Tr}(E_t \omega_t)) E_t \| \leq L \| E_t \| \leq L \, .
\]

Therefore
\[
\sum_{t=1}^{T} \left[ \ell_t(\text{Tr}(E_t \omega_t)) - \ell_t(\text{Tr}(E_t \varphi)) \right] \leq 2L \sqrt{(2 \log 2)nT} \, .
\]

**Proof of Claim 14** Let \( P \in \mathcal{K} \) be such that \( \lambda_{\min}(P) = 0 \). Suppose \( P = VQV^\dagger \), where \( Q \) is a diagonal matrix with real values on the diagonal. Assume that \( Q_{1,1} = \lambda_{\max}(P) \) and \( Q_{2^n,2^n} = \lambda_{\min}(P) = 0 \). Let \( P' = VQ'V^\dagger \) such that \( Q'_{1,1} = Q_{1,1} - \epsilon, Q'_{2^n,2^n} = \epsilon \) for \( \epsilon < \lambda_{\max}(P) \), and \( Q'_{i,i} = Q_{i,i} \) for \( i \in \{2, 3, ..., 2^n - 1\} \), so \( P' \in \mathcal{K} \). We show that there exists \( \epsilon > 0 \) such that \( \Phi_{t}(P') \leq \Phi_{t}(P) \). Expanding both sides of the inequality, we see that it is equivalent to showing that for some \( \epsilon \),
\[
\eta \sum_{s=1}^{t} \nabla \Phi_t(\omega_{t+s}) \leq \lambda_1(P) \log \frac{1}{\lambda_1(P)} - \lambda_1(P') \log \frac{1}{\lambda_1(P')} - \epsilon \log \epsilon \, .
\]
Let $\alpha = \lambda_1(P) = Q_{1,1}$, and $A = \eta \sum_{s=1}^t \nabla s$. The inequality then becomes

$$A \cdot (P' - P) \leq \alpha \log \alpha - (\alpha - \varepsilon) \log(\alpha - \varepsilon) - \varepsilon \log \varepsilon .$$

Observe that $\|A\| \leq \eta \sum_{s=1}^t \|\nabla s\| = \eta \sum_{s=1}^t \|\ell'_s(\text{Tr}(E_s \omega_s))\|E_s\| \leq \eta Lt$. So by the Generalized Cauchy-Schwartz inequality,

$$A \cdot (P' - P) \leq \eta Lt \|P' - P\|_{\text{Tr}} \leq 2\varepsilon \eta Lt .$$

Since $\eta, t, \alpha, L$ are finite and $-\log \varepsilon \to \infty$ as $\varepsilon \to 0$, there exists $\varepsilon$ small such that $2\eta Lt \leq \log \alpha - \log \varepsilon$. We have

$$2\eta Lt \varepsilon \leq \varepsilon \log \alpha - \varepsilon \log \varepsilon = \alpha \log \alpha - (\alpha - \varepsilon) \log(\alpha - \varepsilon) - \varepsilon \log \varepsilon \leq \alpha \log \alpha - (\alpha - \varepsilon) \log(\alpha - \varepsilon) - \varepsilon \log \varepsilon .$$

So there exists $\varepsilon > 0$ such that $\Phi_t(P') \leq \Phi_t(P)$. If $P$ has multiple eigenvalues that are 0, we can repeat the proof and show that there exists a PD matrix $P''$ such that $\Phi_t(P'') \leq \Phi_t(P)$. Since $\omega_t$ is a minimizer of $\Phi_{t-1}$ and $\omega_1 \succ 0$, we conclude that $\omega_t \succ 0$ for all $t$.

**Proof of Claim 14** Suppose $\nabla \Phi_t(\omega_{t+1}) \cdot (\omega_t - \omega_{t+1}) < 0$. Let $a \in (0, 1)$ and $X = (1 - a)\omega_{t+1} + a\omega_t$, then $X$ is a density matrix and is positive definite. Define $\Delta = X - \omega_{t+1} = a(\omega_t - \omega_{t+1})$. We have

$$\Phi_t(X) - \Phi_t(\omega_{t+1}) = a \nabla \Phi_t(\omega_{t+1}) \cdot (\omega_t - \omega_{t+1}) + B_{\Phi_t}(X) \|\omega_{t+1}\| \leq a \nabla \Phi_t(\omega_{t+1}) \cdot (\omega_t - \omega_{t+1}) + B_{\Phi_t}(0) \|\omega_{t+1}\| .$$

The above inequality is due to [Audenaert and Eisert 2005 Theorem 2]. Dividing by $a$ on both sides, we have

$$\frac{\Phi_t(X) - \Phi_t(\omega_{t+1})}{a} \leq \nabla \Phi_t(\omega_{t+1}) \cdot (\omega_t - \omega_{t+1}) + \frac{a^2 \text{Tr}((\omega_t - \omega_{t+1})^2)}{\lambda_{\text{min}}(\omega_{t+1})} .$$

So we can find $a$ small enough such that the right hand side of the above inequality is negative. However, we would have $\Phi_t(X) - \Phi_t(\omega_{t+1}) \leq 0$, which is a contradiction. So $\nabla \Phi_t(\omega_{t+1}) \cdot (\omega_t - \omega_{t+1}) \geq 0$.

**C Proof of Theorem 4**

**Proof of Theorem 4** Note that for any density matrix $\varphi$, we have $M_t \cdot \varphi = \sum_{i=1}^T \ell'_t(\text{Tr}(E_i \omega_t)) \text{Tr}(E_i \varphi)$. Then, the regret bound for Matrix Multiplicative Weights [Arora and Kale 2016 Theorem 3.1] implies that for any density matrix $\varphi$, we have

$$\sum_{i=1}^T \ell'_t(\text{Tr}(E_i \omega_t)) \text{Tr}(E_i \varphi) \leq \sum_{i=1}^T \ell'_t(\text{Tr}(E_i \omega_t)) \text{Tr}(E_i \varphi) + \eta LT + \frac{L \log(2^n)}{\eta} .$$

Here, we used the bound $M_t^2 \cdot \omega_t \leq 1$. Next, since $\ell_t$ is convex, we have

$$\ell'_t(\text{Tr}(E_i \omega_t)) \text{Tr}(E_i \varphi) - \ell'_t(\text{Tr}(E_i \omega_t)) \text{Tr}(E_i \varphi) \geq \ell_t(\text{Tr}(E_i \omega_t)) - \ell_t(\text{Tr}(E_i \varphi)) .$$

Using this bound, and the stated value of $\eta$, we get the required regret bound.

**D Proof of Theorem 6**

**Proof of Theorem 6** Let $\rho^* := \rho^\otimes k$ be an amplified version of $\rho$, over a Hilbert space of dimension $D := 2^{kn}$, for some $k$ to be set later. Throughout, we maintain a classical description of a $D$-dimensional “amplified hypothesis state” $\omega_t^*$, which we view as being the state of $k$ registers with $n$
qubits each. We ensure that $\omega^*_t$ is always symmetric under permuting the $k$ registers. Given $\omega^*_t$, our actual $n$-qubit hypothesis state $\omega_i$ is then obtained by simply tracing out $k - 1$ of the registers.

Given an amplified hypothesis state $\omega^*$, let $E^*_t$ be a two-outcome measurement that acts on $\omega^*$ as follows: it applies the measurement $E_t$ to each of the $k$ registers separately, and accepts if and only if the fraction of measurements that accept equals $b_t$, up to an additive error at most $\varepsilon/2$.

Here is the learning strategy. Our initial hypothesis, $\omega_0^* := \mathbb{I}/D$, is the $D$-dimensional maximally mixed state, corresponding to $\omega_0 := \mathbb{I}/2^n$. (The maximally mixed state corresponds to the notion of a uniformly random quantum superposition.) For each $t \geq 1$, we are given descriptions of the measurements $E_1, \ldots, E_t$, as well as real numbers $b_1, \ldots, b_t$ in $[0, 1]$, such that $|b_t - \text{Tr}(E_t \rho)| \leq \varepsilon/3$ for all $i \in [t]$. We would like to update our old hypothesis $\omega^*_{t-1}$ to a new hypothesis $\omega^*_t$, ideally such that the difference $|\text{Tr}(E_{t+1} \omega_t) - \text{Tr}(E_{t+1} \rho)|$ is small. We do so as follows:

- Given $b_t$, as well classical descriptions of $\omega^*_{t-1}$ and $E_t$, decide whether $\text{Tr}(E^*_t \omega^*_{t-1}) \geq 1 - \frac{\varepsilon}{6}$.
- If yes, then set $\omega^*_t := \omega^*_{t-1}$ (i.e., we do not change the hypothesis).
- Otherwise, let $\omega^*_t$ be the state obtained by applying $E^*_t$ to $\omega^*_{t-1}$ and postselecting on $E^*_t$ accepting. In other words, $\omega^*_t := \mathcal{M}(\omega^*_{t-1})$, where $\mathcal{M}$ is the operator that postselects on acceptancy by $E^*_t$ (as defined above).

We now analyze this strategy. Call $t$ “good” if $\text{Tr}(E^*_t \omega^*_{t-1}) \geq 1 - \frac{\varepsilon}{6}$, and “bad” otherwise. Below, we show that

(i) there are at most $O\left(\frac{n}{\varepsilon^2 \log \frac{n}{\varepsilon}}\right)$ bad $t$'s, and
(ii) for each good $t$, we have $|\text{Tr}(E_t \omega_{t-1}) - \text{Tr}(E_t \rho)| \leq \varepsilon$.

We start with claim (i). Suppose there have been $\ell$ bad $t$'s, call them $t(1), \ldots, t(\ell)$, where $\ell \leq (n/\varepsilon)^{10}$ (we justify this last assumption later, with room to spare). Then there were $\ell$ events where we postselected on $E^*_t$ accepting $\omega^*_{t-1}$. We conduct a thought experiment, in which the learning strategy maintains a quantum register initially in the maximally mixed state $\mathbb{I}/D$, and applies the postselection operator corresponding to $E^*_t$ to the quantum register whenever $t$ is bad. Let $p$ be the probability that all $\ell$ of these postselection events succeed. Then by definition,

$$p = \text{Tr}\left(E^*_{t(1)} \omega^*_{t(1)-1}\right) \cdots \text{Tr}\left(E^*_{t(\ell)} \omega^*_{t(\ell)-1}\right) \leq \left(1 - \frac{\varepsilon}{6}\right)^\ell.$$ 

On the other hand, suppose counterfactually that we had started with the “true” hypothesis, $\omega_0^* := \rho^* := \rho^{\otimes k}$. In that case, we would have

$$\text{Tr}\left(E^*_{t(i)} \rho^*\right) = \text{Pr}\left[E_{t(i)} \text{ accepts } \rho \text{ between } \left(b_{t(i)} - \frac{\varepsilon}{2}\right) k \text{ and } \left(b_{t(i)} + \frac{\varepsilon}{2}\right) k \text{ times}\right] \geq 1 - 2e^{-2k(\varepsilon/6)^2}$$

for all $i$. Here the second line follows from the condition that $|\text{Tr}(E_{t(i)} \rho) - b_{t(i)}| \leq \varepsilon/6$, together with the Hoeffding bound.

We now make the choice $k := \frac{C}{\varepsilon^2} \log \frac{1}{\varepsilon}$, for some constant $C$ large enough that

$$\text{Tr}\left(E^*_{t(i)} \rho^*\right) \geq 1 - \frac{\varepsilon^{10}}{400n^{10}}$$

for all $i$. So by Theorem 5 all $\ell$ postselection events would succeed with probability at least

$$1 - 2\sqrt{\ell \frac{\varepsilon^{10}}{400n^{10}}} \geq 0.9.$$ 

We may write the maximally mixed state, $\mathbb{I}/D$, as

$$\frac{1}{D} \rho^* + \left(1 - \frac{1}{D}\right) \xi.$$
for some other mixed state $\xi$. For this reason, even when we start with initial hypothesis $\omega_0^* = \mathbb{I}/D$, all $\ell$ postselection events still succeed with probability

$$p \geq \frac{0.9}{D}.$$  

Combining our upper and lower bounds on $p$ now yields

$$\frac{0.9}{2^{kn}} \leq \left(1 - \frac{\varepsilon}{6}\right)^\ell$$

or

$$\ell = O\left(\frac{kn}{\varepsilon} \log \frac{n}{\varepsilon}\right),$$

which incidentally justifies our earlier assumption that $\ell \leq (n/\varepsilon)^{10}$.

It remains only to prove claim (ii). Suppose that

$$\text{Tr}(E_t^* \omega_{t-1}^*) \geq 1 - \frac{\varepsilon}{6}.$$  

(8)

Imagine measuring $k$ quantum registers prepared in the joint state $\omega_{t-1}^*$, by applying $E_t$ to each register. Since the state $\omega_{t-1}^*$ is symmetric under permutation of the $k$ registers, we have that $\text{Tr}(E_t \omega_{t-1}^*)$, the probability that $E_t$ accepts the first register, equals the expected fraction of the $k$ registers that $E_t$ accepts. The bound in Eq. (8) means that, with probability at least $1 - \frac{\varepsilon}{6}$ over the measurement outcomes, the fraction of registers which $E_t$ accepts is within $\pm \frac{\varepsilon}{2}$ of $b_t$. The $k$ measurement outcomes are not necessarily independent, but the fraction of registers accepted never differs from $b_t$ by more than 1. So by the union bound, we have

$$|\text{Tr}(E_t \omega_{t-1}) - b_t| \leq \frac{\varepsilon}{2} + \frac{\varepsilon}{6} = \frac{2\varepsilon}{3}.$$  

Hence by the triangle inequality,

$$|\text{Tr}(E_t \omega_{t-1}) - \text{Tr}(E_t \rho)| \leq \frac{2\varepsilon}{3} + |b_t - \text{Tr}(E_t \rho)| \leq \varepsilon,$$

as claimed. \hfill $\square$

### E Proof of Corollary 7

We begin with a bound for a generalization of “random access coding” (Nayak [1999], Ambainis et al. [2002]) or what is also known as the Index function problem in communication complexity. The generalization was called “serial encoding” by Nayak [1999] and arose in the context of quantum finite automata. The serial encoding problem is also called Augmented Index in the literature on streaming algorithms.

The following theorem places a bound on how few qubits serial encoding may use. In other words, it bounds the number of bits we may encode in an $n$-qubit quantum state when an arbitrary bit out of the $n$ may be recovered well via a two-outcome measurement. The bound holds even when the measurement for recovering $y_i$ may depend adaptively on the previous bits $y_1 y_2 \cdots y_{i-1}$ of $y$, which we need not know.

**Theorem 15** (Nayak [1999]). Let $k$ and $n$ be positive integers. For each $k$-bit string $y := y_1 \cdots y_k$, let $\rho_y$ be an $n$-qubit mixed state such that for each $i \in \{1, 2, \ldots, k\}$, there is a two-outcome measurement $E$ that depends only on $i$ and the prefix $y_1 y_2 \cdots y_{i-1}$ of $y$, which we need not know.

1. if $y_i = 0$ then $\text{Tr}(E \rho_y) \leq p$, and
2. if $y_i = 1$ then $\text{Tr}(E \rho_y) \geq 1 - p$,

where $p \in [0, 1/2]$ is the error in predicting the bit $y_i$ at vertex $v$. (We say $\rho_y$ “serially encodes” $y$.) Then $n \geq (1 - H(p)) k$.  

16
In Appendix F, we present a strengthening of this bound when the bits of $y$ may be only be recovered in an adaptive order that is \textit{a priori} unknown. The stronger bound may be of independent interest.

In the context of online learning, the measurements used in recovering bits from a serial encoding are required to predict the bits with probability bounded away from given “pivot points”. Theorem 15 may be specialized to this case as in Corollary 7, which we prove below.

\textbf{Proof of Corollary 7.} This is a consequence of Theorem 15 when combined with the following observation. Given the measurement operator $E'$, parameter $\varepsilon$, and pivot point $a_v$, as in the statement of the corollary, we define a new two-outcome measurement $E$ to be associated with vertex $v$:

$$E := \begin{cases} 
\frac{E'}{2a_v} & \text{if } a_v \geq \frac{1}{2}, \\
\frac{1}{2(1-a_v)} (E' + (1-2a_v)I) & \text{if } a_v < \frac{1}{2}.
\end{cases}$$

The measurement $E$ may be interpreted as producing a fixed outcome 0 or 1 with some probability depending on $a_v$, and applying the given measurement $E'$ with the remaining probability, so as to translate the pivot point $a_v$ to $1/2$.

We may verify that the operator $E$ satisfies the requirements (i) and (ii) of Theorem 15 with $p := (1-\varepsilon)/2$. We therefore conclude that $n \geq (1-H((1-\varepsilon)/2)k$. Since $H(1/2 - \delta) \leq 1 - 2\delta^2$, for $\delta \in [0, 1/2]$, we get $k = O(n/\varepsilon^2)$. \hfill \square

\section{Lower bound on quantum random access codes}

Here we present an alternative proof of the linear lower bound on quantum random access codes\cite{Nayak99,AmbainisGR02}. It goes via the Matrix Multiplicative Weights algorithm, but gives us a slightly weaker dependence on decoding error. We also present an extension of the original bound to more general codes. These may be of independent interest.

\textbf{Theorem 16.} Let $k$ and $n$ be positive integers with $k > n$. For all $k$-bit strings $y = y_1, y_2, \ldots, y_k$, let $\rho_y$ be the $n$-qubit quantum mixed state that encodes $y$. Let $p \in [0, 1/2]$ be an error tolerance parameter. Suppose that there exist measurements $E_1, E_2, \ldots, E_k$ such that for all $y \in \{0, 1\}^k$ and all $i \in [k]$, we have $|\text{Tr}(E_i\rho_y) - y_i| \leq p$. Then $n \geq \frac{(1/2-p)^2}{4(\log 2)^2}k$.

\textbf{Proof.} Run the MMW algorithm described in Section 3.2 with the absolute loss function $\ell_t(x) := |x - y_t|$ for $t = 1, 2, \ldots, k$ iterations. In iteration $t$, provide as feedback $E_t$ and the label $y_t \in \{0, 1\}$ defined as follows:

$$y_t = \begin{cases} 
0 & \text{if } \text{Tr}(E_t\omega_t) > \frac{1}{2}, \\
1 & \text{if } \text{Tr}(E_t\omega_t) \leq \frac{1}{2}.
\end{cases}$$

Let $y \in \{0, 1\}^k$ be the bit string formed at the end of the process. Then it is easy to check the following two properties by the construction of the labels: for any $t \in [k]$, we have

1. $\ell_t(\omega_t) = |\text{Tr}(E_t\omega_t) - y_t| \geq 1/2$, and
2. $\ell_t(\rho_y) = |\text{Tr}(E_t\rho_y) - y_t| \leq p$.

By Theorem 4, the MMW algorithm with absolute loss has a regret bound of $2\sqrt{(\log 2)kn}$. So the above bounds imply that $k/2 \leq p k + 2\sqrt{(\log 2)kn}$, which implies that $n \geq \frac{(1/2-p)^2}{4(\log 2)^2}k$. \hfill \square

Note that in the above proof, we may allow the measurement in the $i$th iteration, i.e., the one used to decode the $i$th bit, to depend on the previous bits $y_1, y_2, \ldots, y_{i-1}$. Thus, the lower bound also applies to serial encoding.

Next we consider encoding of bit-strings $y$ into quantum states $\rho_y$ with a more relaxed notion of decoding. The encoding is such that given the encoding for an unknown string $y$, some bit $i_y$ of $y$ can be decoded. Given the value $y_{i_y}$ of this bit, a new bit $i_y$ of $y$ can be decoded, and the index $i_y$ may depend on $y_{i_y}$. More generally, given a sequence of bits $y_{i_1}, y_{i_2}, \ldots, y_{i_j}$, that may be decoded in this manner, a new bit $i_{j+1}$ of $y$ can be decoded, for any $j \in \{0, 1, \ldots, k-1\}$. Here, the index $i_{j+1}$
We first formalize the above generalization of random access encoding. We view a complete binary tree of depth \( d \geq 0 \) as consisting of vertices \( v \in \{0, 1\}^d \). The root of the tree is labeled by the empty string \( \epsilon \) and each internal vertex \( v \) of the tree has two children \( v0, v1 \). We specify an adaptive sequence of measurements through a “measurement decision tree”. The tree specifies the measurement to be applied next, given a prefix of such measurements along with the corresponding outcomes.

**Definition 1.** Let \( k \) be a positive integer: A measurement decision tree of depth \( k \) is a complete binary tree of depth \( k \), each internal vertex \( v \) of which is labeled by a triple \((S, i, E)\), where \( S \in \{1, \ldots, k\} \) is a sequence of length \( l := |v| \) of distinct indices, \( i \in \{1, \ldots, k\} \) is an index that does not occur in \( S \), and \( E \) is a two-outcome measurement. The sequences associated with the children \( v0, v1 \) of \( v \) (if defined) are both equal to \((S, i, E)\).

For a \( k \)-bit string \( y \), and sequence \( S := (i_1, i_2, \ldots, i_l) \) with \( 0 \leq l \leq k \) and \( i_j \in \{1, 2, \ldots, k\} \), let \( y_S \) denote the substring \( y_{i_1}y_{i_2}\cdots y_{i_l} \).

**Theorem 17.** Let \( k \) and \( n \) be positive integers. For each \( k \)-bit string \( y := y_1 \ldots y_k \), let \( \rho_y \) be an \( n \)-qubit mixed state (we say \( \rho_y \) “encodes” \( y \)). Suppose there exists a measurement decision tree \( T \) of depth \( k \) such that for each internal vertex \( v \) of \( T \) and all \( y \in \{0, 1\}^k \) with \( y_S = v \), where \((S, i, E)\) is the triple associated with the vertex \( v \), we have \(|\text{Tr}(E\rho_y) - y_i| \leq p_v \), where \( p_v \in [0, 1/2] \) is the error in predicting the bit \( y_i \) at vertex \( v \). Then \( n \geq (1 - H(p))k \), where \( H \) is the binary entropy function, and \( p := \frac{1}{k} \sum_{i=1}^{2^k} \sum_{v \in \{0,1\}^l} p_v \) is the average error.

**Proof.** Let \( Y \) be a uniformly random \( k \)-bit string. We define a random permutation \( \Pi \) of \( \{1, \ldots, k\} \) correlated with \( Y \) that is given by the sequence of measurements in the root to leaf path corresponding to \( Y \). More formally, let \( \Pi(1) := i \), where \( i \) is the index associated with the root of the measurement decision tree \( T \). For \( l \in \{2, \ldots, k\} \), let \( \Pi(l) := j \), where \( j \) is the index associated with the vertex \( Y_{\Pi(1)}Y_{\Pi(2)}\cdots Y_{\Pi(l-1)} \) of the tree \( T \). Let \( Q \) be a quantum register such that the joint state of \( YQ \) is

\[
\frac{1}{2^k} \sum_{y \in \{0,1\}^k} |y\rangle \langle y| \otimes \rho_y .
\]

The quantum mutual information between \( Y \) and \( Q \) is bounded as \( I(Y : Q) \leq |Q| = n \). Imagine having performed the first \( l - 1 \) measurements given by the tree \( T \) on state \( Q \) and having obtained the correct outcomes \( Y_{\Pi(1)}Y_{\Pi(2)}\cdots Y_{\Pi(l-1)} \). These outcomes determine the index \( \Pi(l) \) of the next bit that may be learned. By the Chain Rule, for any \( l \in \{1, \ldots, k - 1\} \),

\[
I(Y_{\Pi(l)} \cdots Y_{\Pi(k)} : Q \mid Y_{\Pi(1)}Y_{\Pi(2)}\cdots Y_{\Pi(l-1)}) \\
= I(Y_{\Pi(l)} : Q \mid Y_{\Pi(1)}Y_{\Pi(2)}\cdots Y_{\Pi(l-1)}) + I(Y_{\Pi(l+1)} \cdots Y_{\Pi(k)} : Q \mid Y_{\Pi(1)}Y_{\Pi(2)}\cdots Y_{\Pi(l)}) .
\]

Let \( E \) be the operator associated with the vertex \( V := Y_{\Pi(1)}Y_{\Pi(2)}\cdots Y_{\Pi(l-1)} \). By hypothesis, the measurement \( E \) predicts the bit \( Y_{\Pi(l)} \) with error at most \( p_{V} \). Using the Fano Inequality, and averaging over the prefix \( V \), we get

\[
I(Y_{\Pi(l)} : Q \mid Y_{\Pi(1)}Y_{\Pi(2)}\cdots Y_{\Pi(l-1)}) \geq E_V(1 - H(p_{V})) .
\]

Applying this repeatedly for \( l \in \{1, \ldots, k - 1\} \), we get

\[
I(Y : Q) = I(Y_{\Pi(1)} : Q) + I(Y_{\Pi(2)} : Q \mid Y_{\Pi(1)}) + I(Y_{\Pi(3)} : Q \mid Y_{\Pi(1)}Y_{\Pi(2)}) \\
+ \cdots + I(Y_{\Pi(k)} : Q \mid Y_{\Pi(1)}Y_{\Pi(2)}\cdots Y_{\Pi(k-1)}) \\
\geq \sum_{l=1}^{k} \frac{1}{2^l} \sum_{v \in \{0,1\}^l} (1 - H(p_v)) \\
\geq (1 - H(p))k ,
\]

by concavity of the binary entropy function, and the definition of \( p \). \( \square \)