Quantum Event Learning and Gentle Random Measurements

Adam Bene Watts

Institute for Quantum Computing, University of Waterloo, Canada

John Bostanci

Computer Science Department, Columbia University, New York, NY, USA

Abstract

We prove the expected disturbance caused to a quantum system by a sequence of randomly ordered two-outcome projective measurements is upper bounded by the square root of the probability that at least one measurement in the sequence accepts. We call this bound the *Gentle Random Measurement Lemma*.

We then extend the techniques used to prove this lemma to develop protocols for problems in which we are given sample access to an unknown state ρ and asked to estimate properties of the accepting probabilities $\mathrm{Tr}[M_i \rho]$ of a set of measurements $\{M_1, M_2, \ldots, M_m\}$. We call these types of problems *Quantum Event Learning Problems*. In particular, we show randomly ordering projective measurements solves the Quantum OR problem, answering an open question of Aaronson. We also give a Quantum OR protocol which works on non-projective measurements and which outperforms both the random measurement protocol analyzed in this paper and the protocol of Harrow, Lin, and Montanaro. However, this protocol requires a more complicated type of measurement, which we call a *Blended Measurement*. Given additional guarantees on the set of measurements $\{M_1, \ldots, M_m\}$, we show the random and blended measurement Quantum OR protocols developed in this paper can also be used to find a measurement M_i such that $\mathrm{Tr}[M_i \rho]$ is large. We call the problem of finding such a measurement *Quantum Event Finding*. We also show Blended Measurements give a sample-efficient protocol for *Quantum Mean Estimation*: a problem in which the goal is to estimate the average accepting probability of a set of measurements on an unknown state.

Finally we consider the *Threshold Search Problem* described by O'Donnell and Bădescu where, given given a set of measurements $\{M_1, \ldots, M_m\}$ along with sample access to an unknown state ρ satisfying $\mathrm{Tr}[M_i \rho] \geq 1/2$ for some M_i, the goal is to find a measurement M_j such that $\mathrm{Tr}[M_j \rho] \geq 1/2 - \epsilon$. By building on our Quantum Event Finding result we show that randomly ordered (or blended) measurements can be used to solve this problem using $O(\log^2(m)/\epsilon^2)$ copies of ρ. This matches the performance of the algorithm given by O'Donnell and Bădescu, but does not require injected noise in the measurements. Consequently, we obtain an algorithm for Shadow Tomography which matches the current best known sample complexity (i.e. requires $\tilde{O}(\log^2(m)\log(d)/\epsilon^4)$ samples). This algorithm does not require injected noise in the quantum measurements, but does require measurements to be made in a random order, and so is no longer online.

2012 ACM Subject Classification Theory of computation; Theory of computation → Quantum computation theory; Theory of computation → Quantum information theory

Keywords and phrases Event learning, gentle measurments, random measurements, quantum or, threshold search, shadow tomography

Digital Object Identifier 10.4230/LIPIcs.ITCS.2024.97

Related Version *Extended Version*: `https://arxiv.org/abs/2210.09155`

Funding *John Bostanci*: JB is partially supported by NSF CAREER award CCF-2144219.

Acknowledgements The authors would like to that Aram Harrow, Scott Aaronson and Luke Schaeffer for helpful discussions. Particular thanks is due to Luke Schaeffer for finding the counterexample discussed in Appendix B of this paper. The authors would also like to thank Matthias Caro for spotting a typo in an earlier version of this paper. Additionally, ABW would like to thank Nilin

Abrahamsen and Juspreet Singh Sandhu for a particularly motivating discussion over ice cream during the early days of this work. JB would like to thank Ashwin Nayak and Angus Lowe for the many useful discussions and motivation.

1 Introduction

Quantum measurements change the states that they act on, often in undesired ways. Colloquially called the "information-disturbance trade-off", the *Gentle Measurement Lemma* bounds the damage that a single measurement can cause to a quantum system by relating the probability of a particular outcome to the disturbance when seeing that outcome [1, 13]. Notably, the Gentle Measurement Lemma only bounds the disturbance caused by a single measurement. The *Anti-Zeno Effect* refers to a phenomenon in which a sequence of two-outcome measurements can cause arbitrarily large damage to quantum system, despite the probability of *any* measurement in the sequence accepting being arbitrary small [9].[1]

For sequential measurements, the closest analogue we know to the Gentle Measurement Lemma is known as the Gentle Sequential Measurement Lemma [6] (closely related to the Quantum Union Bound [6, 10]). Crucially, the Gentle Sequential Measurement Lemma bounds the damage a sequence of measurements can cause to a system in terms of the accepting probability of each measurement on the *initial* state of the system, not the accepting probability of the measurements on the state on which they are applied.

The analysis of sequential measurements is closely related to a class of problems we call *Event Learning Problems*. These problems involve an unknown state ρ and set of measurements $M_1, M_2, \ldots, M_m$. The goal is to learn properties of the measurements' accepting probabilities $\mathrm{Tr}[M_1\rho], \mathrm{Tr}[M_2\rho], \ldots, \mathrm{Tr}[M_m\rho]$, while using as few copies of the quantum state ρ as possible. This class of problems includes the well studied *Shadow Tomography* problem [3, 8, 4], but also "easier" problems where the goal is to learn fewer features of the accepting probabilities. Another well studied Event Learning problem is the *Quantum OR* problem. Here, the goal is to approximate the OR of the measurement accepting probabilities, or, more formally, to distinguish between the following cases:

(1) There exists a measurement M_i which accepts on ρ with high probability.

(2) The total accepting probability of all measurements $\sum_i \mathrm{Tr}[M_i\rho]$ is small.

The Quantum OR problem serves as an illustrative example of how the Anti-Zeno Effect, and in general the information-disturbance trade-off, represents substantial barrier to obtaining algorithms for these kinds of tasks that have low sample complexity. In Ref. [2], Aaronson proposed an algorithm for the Quantum OR problem in which a system was prepared in state ρ and measurements $M_1, \ldots, M_m$ were applied to the system in an order chosen uniformly at random. Ref. [7] pointed out a gap in Aaronson's analysis that was closely related to the Anti-Zeno Effect [9]: the original argument did not rule out the possibility that in Case 1 it might be possible that with high probability over the random choice of sequence, all of the measurements in the sequence could all reject with high probability while still causing a large disturbance to the system initially state ρ. Ultimately, this disturbance could cause measurement M_i to reject with high probability, despite it accepting with high probability on the initial state.

[1] Of course, one can apply the Gentle Measurement Lemma repeatedly to each measurement in a sequence of measurements. The reason this approach does not rule out phenomenon such as the Anti-Zeno effect comes from the square root in the original gentle measurement lemma – even when the sum over all measurements' accepting probabilities is small, the sum of the square roots of their accepting probabilities, and hence the resulting bound coming from sequential applications of the gentle measurement lemma, can be large.

The authors of Ref. [7] gave alternate algorithms which solved the Quantum OR problem. These algorithms still required only a single copy of ρ, but involve more complicated measurements than Aaronson's original proposal, and cast aside the idea of using randomly ordered sequences of measurements to solve the problem. Despite the gap found in Aaronson's analysis, no counterexample or proof was given, and it remained open whether randomly ordered measurements could solve the Quantum OR problem. In this paper, we create a toolkit for analyzing the effects of randomly ordered measurements on unknown quantum states. Using these tools, we are able to show that (a small modification to) the original Aaronson Quantum OR algorithm does indeed work, and simplify algorithms that achieve the best known sample complexity on other event learning tasks, most notably shadow tomography, using random sequences of measurements.

1.1 Results

The first major result in this paper is a generalization of the Gentle Measurement Lemma to the setting where a random sequence of measurements is applied to a state ρ. Like the Gentle Measurement Lemma, this lemma gives an upper bound on the "damage" (in trace distance) this sequence of measurements can cause to the state ρ in terms of the probability that at least one measurement in the sequence accepts.

▶ **Theorem 1** (Gentle Random Measurement Lemma). *Let $\mathcal{M} = \{M_1, M_2, \ldots, M_m\}$ be a set of two outcome projective measurements, and ρ be a density matrix. Consider the process where a measurement from the set $\mathcal{M}$ is selected universally at random and applied to a quantum system initially in state $\rho^{(0)} = \rho$. Let $\rho^{(k)}$ be the state of the quantum system after k repetitions of this process where no measurement accepts, so*

$$\rho^{(k)} = \frac{\mathbb{E}_{X_1,\ldots,X_k\sim\mathcal{M}}\left[(1-X_k)\ldots(1-X_1)\rho(1-X_1)\ldots(1-X_k)\right]}{\mathbb{E}_{X_1,\ldots,X_k\sim\mathcal{M}}\left[\mathrm{Tr}\left[(1-X_k)\ldots(1-X_1)\rho(1-X_1)\ldots(1-X_k)\right]\right]} \tag{1}$$

and let $\mathrm{Accept}(k)$ be the probability that at least one measurement accepts during k repetitions of this process (equivalently, the probability that not all measurements reject), so

$$\mathrm{Accept}(k) = 1 - \mathbb{E}_{X_1,\ldots,X_k\sim\mathcal{M}}\left[\mathrm{Tr}[(1-X_k)\ldots(1-X_1)\rho(1-X_1)\ldots(1-X_k)]\right] \tag{2}$$

Then

$$\left\|\rho - \rho^{(k)}\right\|_1 \le 4\sqrt{\mathrm{Accept}(\lceil k/2\rceil)} \le 4\sqrt{\mathrm{Accept}(k)}\,. \tag{3}$$

This theorem shows that randomly ordered sequences of measurements are "gentle" in expectation, provided the expectation is taken over all possible orderings. As a consequence, we find that phenomenon similar to the Anti-Zeno Effect are not likely to occur in randomly ordered measurements. Sections 3.1 and 3.2 of this paper develops some key ideas which are used in the proof of Theorem 1. Section 3.3 proves this theorem.

In the later half of this paper we use the techniques used to prove Theorem 1 to study several Event Learning problems. In Section 4 we consider the Quantum OR problem, and prove correctness of Aaronson's original Quantum OR algorithm, resolving the last unanswered question from Ref. [2].

▶ **Theorem 2** (Random Measurements Solve Quantum OR). *Let $\mathcal{M} = \{M_1, M_2, \ldots, M_m\}$ be a set of two outcome projective measurements. Let ρ be a state such that either there exists an $i \in [m]$ with $\mathrm{Tr}[M_i\rho] > 1-\epsilon$ (Case 1) or $\sum_i \mathrm{Tr}[M_i\rho] \le \delta$ (Case 2). Then consider the process where m measurements are chosen (with replacement) at random from $\mathcal{M}$ and* *applied in sequence to a quantum system initially in state ρ: in Case 1, some measurement in the sequence accepts with probability at least* $(1-\epsilon)^2/4.5$*; in Case 2, the probability of any measurement accepting is at most 2δ.*

We also give a Quantum OR procedure which performs better than the random measurement procedure, and which can be used when the measurements $M_1, \dots, M_m$ are not projective. However this procedure requires more complicated measurements than the random measurement procedure above. Details of this test are given in Section 4.1.

In Section 5 we introduce the problem of *Quantum Event Finding.* This is a variant of the Quantum OR problem where the goal is to accept or reject as in Quantum OR and additionally, in the accepting case, to return a measurement M_i such that $\mathrm{Tr}[M_i\rho]$ is large. We then show the Quantum OR procedure introduced in Section 4.1 can be extended to solve Quantum Event Finding in the case when the total weight of undesirable events is bounded by a constant. Combining this with techniques from Section 3.3, we also show that an algorithm similar to Aaronson's original Quantum OR algorithm halts on a desirable measurement with constant probability (again provided the total weight of undesirable events is bounded by a constant).

▶ **Theorem 3** (Random Measurement Event Finding). *Let $\mathcal{M} = \{M_1, M_2, \dots, M_m\}$ be a set of two outcome measurements. Let ρ be a state such that either there exists an $i \in [m]$ with* $\mathrm{Tr}[M_i\rho] > 1-\epsilon$ *(Case 1) or* $\sum_i \mathrm{Tr}[M_i\rho] \le \delta$ *(Case 2), and let*

$$\beta = \sum_{i:\mathrm{Tr}\{M_i\rho\}\le 1-\epsilon} \mathrm{Tr}[M_i\rho]\,. \tag{4}$$

Then if measurements are chosen uniformly at random (with replacement), in Case 1, with probability at least $(1-\epsilon)^7/(1296(1+\beta)^3)$*, at least one measurement accepts and the first accepting measurement satisfies* $\mathrm{Tr}[M_i\rho] \ge 1-\epsilon$*. In Case 2, a measurement accepts with probability at most 2δ.*

In Section 6, we consider the similar problem of *Quantum Threshold Search*, introduced in Ref. [5]. We begin by extending the event finding results to show that independent of β, the distribution over measurements output by the procedure is correlated with the relative magnitude of $\mathrm{Tr}[M_i\rho]$. We leverage this to state a novel threshold search algorithm based on blended (and random) measurements and prove that it requires $O(\log^2 m)$ copies of the unknown state ρ, matching the best known upper bound.

▶ **Theorem 4** (Random Measurement Threshold Search). *Let $\mathcal{M} = \{M_1, M_2, \dots, M_m\}$ be a set of two-outcome measurements and ρ be an unknown quantum state. Consider the process where a uniformly random threshold $\theta \in [2/5, 3/5]$ is chosen, then m measurements are chosen (with replacement) at random from $\mathcal{M}$, and the corresponding binomial measurements (with threshold θ) are applied in sequence to a quantum state initially in $\rho^{\otimes O(\log^2(m))}$, halting if any measurement accepts. If there is a measurement in $\mathcal{M}$ satisfying* $\mathrm{Tr}[M_i\rho] \ge 3/4$*, then this procedure halts on a measurement satisfying* $\mathrm{Tr}[M_i\rho] \ge 1/3$ *with constant probability.*

We believe that while this algorithm is no longer online, as it requires measurements to be made in random order, it represents a promising path towards improving the upper bounds on shadow tomography.

The extended version of this paper also discusses an additional Event Learning problem called *Quantum Mean Estimation.*

2 Notation and Preliminaries

A quantum system R (as indicated by the font) is a named finite dimensional complex Hilbert space. Given two quantum systems A and B, denote by AB the tensor product of the two associated Hilbert spaces. For a linear operator L acting on system R, we sometimes use the notation L_{R} to indicate that L acts on system R, and we similarly use ρ_{R} to denote that ρ is a state in the quantum system R. When clear from context, we drop the system subscript. We write $\mathrm{Tr}[\cdot]$ to mean the trace, and $\mathrm{Tr}_{\mathsf{R}}[\cdot]$ to mean the partial trace over system R.

Given a linear operator X, define $\|X\|_1 = \mathrm{Tr}(|X|)$ to be its trace norm. For two linear operators X and Y acting on the same system, we say that $X \leq Y$ is $Y - X$ is a positive semi-definite operator. For two quantum states ρ and σ, we define the fidelity $\mathrm{F}(\rho, \sigma) = \left\|\sqrt{\sigma}\sqrt{\rho}\right\|_1$. We denote by $\mathbb{1}$ the identity operator, where the system it acts on should be apparent from context.

A quantum measurement is defined by a finite set of positive semi-definite operators $\{\sqrt{M_i}\}_i$ acting on the same quantum system, satisfying $\sum_i M_i = \mathbb{1}$, where each $\sqrt{M_i}$ is associated with outcome i. When there are 2 outcomes in a measurement, described by the matrices $\{\sqrt{M}, \sqrt{\mathbb{1} - M}\}$, we refer to the resulting measurement as "the two-outcome measurement M". For two-outcome measurements, we refer to the $\sqrt{M}$ outcome as the "accepting" outcome, and the $\sqrt{\mathbb{1} - M}$ outcome as the "rejecting" outcome. We now state the Gentle Measurement Lemma [12, Lemma 9.4.1] formally.

▶ **Lemma 5** (Gentle Measurement Lemma). *Let ρ be a quantum state and $0 \leq M \leq \mathbb{1}$ be a two-outcome measurement. Let $\epsilon := \mathrm{Tr}[M\rho]$ be the accepting probability of the measurement on a quantum system in state ρ and*

$$\rho' := \frac{\sqrt{\mathbb{1} - M}\rho\sqrt{\mathbb{1} - M}}{\mathrm{Tr}[(\mathbb{1} - M)\rho]}\,, \tag{5}$$

be the post measurement state when the reject outcome is observed. Then

$$\|\rho - \rho'\|_1 \leq 2\sqrt{\epsilon}\,. \tag{6}$$

3 Gentle Measurement Lemmas

In this section, we prove that blended and random sequences of measurements obey a variant of the gentle measurement lemma. These results will be core mathematical tools in showing that algorithms presented in later sections work.

3.1 Technical Lemmas

Many of the results in this paper are derived from general statements about positive semi-definite (PSD) matrices. In particular, the following lemma, along with the definition of blended measurements, are the core ingredients in our quantum OR results.

▶ **Lemma 6.** *Let X and Y be PSD matrices a $\mathcal{A} = \{A_1, A_2, \ldots, A_m\}$ be an arbitrary set of matrices and $\{p_1, p_2 \ldots, p_m\}$ be a set of real numbers with $p_i \geq 0$ for all i and $\sum_i p_i = 1$. Then*

$$\sum_{i,j\in[m]} p_i p_j \,\mathrm{Tr}\left[X A_i Y A_j^\dagger\right] \leq \sum_{i\in[m]} p_i \,\mathrm{Tr}\left[X A_i Y A_i^\dagger\right]. \tag{7}$$

Proof. The result follows from Cauchy-Schwarz applied to the Hilbert-Schmidt inner product.

$$\sum_{i,j\in[m]} p_i p_j \operatorname{Tr}\left[XA_iYA_j^\dagger\right] \tag{8}$$

$$= \sum_{i,j\in[m]} p_i p_j \left\langle \sqrt{Y}A_i^\dagger\sqrt{X} \middle| \sqrt{Y}A_j^\dagger\sqrt{X} \right\rangle \tag{9}$$

$$\leq \sum_{i,j\in[m]} p_i p_j \sqrt{\left\langle \sqrt{Y}A_i^\dagger\sqrt{X} \middle| \sqrt{Y}A_i^\dagger\sqrt{X} \right\rangle \left\langle \sqrt{Y}A_j^\dagger\sqrt{X} \middle| \sqrt{Y}A_j^\dagger\sqrt{X} \right\rangle} \tag{10}$$

$$\leq \sum_{i,j\in[m]} \frac{p_i p_j}{2} \left(\left\langle \sqrt{Y}A_i^\dagger\sqrt{X} \middle| \sqrt{Y}A_i^\dagger\sqrt{X} \right\rangle + \left\langle \sqrt{Y}A_j^\dagger\sqrt{X} \middle| \sqrt{Y}A_j^\dagger\sqrt{X} \right\rangle \right) \tag{11}$$

$$= \sum_i p_i \left\langle \sqrt{Y}A_i^\dagger\sqrt{X} \middle| \sqrt{Y}A_i^\dagger\sqrt{X} \right\rangle \tag{12}$$

$$= \sum_i p_i \operatorname{Tr}\left[XA_iYA_i^\dagger\right], \tag{13}$$

where we used Cauchy-Schwarz on the second line, the arithmatic-geometric mean inequality on the third, and the fact that $\sum_i p_i = 1$ on the fourth. ◀

We can apply this to prove a corollary more suited to the randomized measurement setting. Before this, we introduce some notation useful for keeping track of the matrix products that appear when analyzing random and blended measurements.

▶ **Definition 7.** *Given a set of matrices $\mathcal{A} = \{A_1, A_2, \dots, A_m\}$ define the set of matrix products*

$$\mathcal{T}_{\mathcal{A}}^{(k)} = \left\{ \prod_{\alpha=1}^{k} A_{i_\alpha} \right\}_{\vec{i}\in[m]^k}. \tag{14}$$

where use the notation $\vec{i} = (i_1, i_2, \dots, i_k)$ to label components of a vector $\vec{i}$. $\mathcal{T}_A^{(k)}$ contains possible length k products of matrices drawn with replacement from the set $\mathcal{A}$.

▶ **Corollary 8.** *Let ρ be a state, X be a PSD matrix and $\mathcal{M}$ be a set of m self-adjoint matrices. Define $\mathcal{T}_{\mathcal{M}}^{(k)}$ as in Definition 7. Then*

$$m^{-k} \sum_{T\in\mathcal{T}_{\mathcal{M}}^{(k)}} \operatorname{Tr}\left[XT\rho T^\dagger\right] \geq m^{-2k} \sum_{T,S\in\mathcal{T}_{\mathcal{M}}^{(k)}} \operatorname{Tr}\left[XT\rho S^\dagger\right] = m^{-2k} \sum_{T,S\in\mathcal{T}_{\mathcal{M}}^{(k)}} \operatorname{Tr}[XT\rho S]. \tag{15}$$

Proof. The first inequality is immediate from Lemma 6 with $Y = \rho$, $\mathcal{A} = \mathcal{T}_{\mathcal{M}}^{(k)}$ and $p_1 = p_2 = \ldots = p_{m^k} = m^{-k}$. The second equality holds because

$$\left(\mathcal{T}_{\mathcal{M}}^{(k)}\right)^\dagger = \left\{ \left(\prod_{\alpha=1}^{k} M_{i_\alpha} \right)^\dagger \right\}_{\vec{i}\in[m]^k} = \left\{ \prod_{\alpha=1}^{k} M_{i'_\alpha} \right\}_{\vec{i}'\in[m]^k} = \mathcal{T}_{\mathcal{M}}^{(k)}. \tag{16}$$

◀

3.2 Gentle Blended Measurements

In this section we prove a number of results about repeated blended measurements. We begin by defining blended measurements.

▶ **Definition 9** (Blended Measurement). *Given a set of two outcome measurements $\mathcal{M} = \{M_1, M_2, \dots, M_m\}$ the blended measurement $\mathcal{B}(\mathcal{M})$ is defined to be the $m+1$ outcome measurement with measurement operators*

$$E_0 = \sqrt{1 - \sum_{i=1}^{m} \frac{M_i}{m}} \quad \text{and} \quad E_i = \sqrt{\frac{M_i}{m}} \quad \text{for } i \in \{1, \dots, m\}. \tag{17}$$

We refer to outcome E_0 as the "reject" outcome, and $E_1, \dots, E_m$ as "accepting" outcomes.

We will be particularly interested in the analyzing what happens when k blended measurements are applied in sequence to a quantum system initially in state ρ. In preparation for this, we define the state $\rho^{(k)}_{\mathcal{B}(\mathcal{M})}$ and probability $\mathrm{Accept}_{\mathcal{B}(\mathcal{M})}(k)$ to be the blended measurement analogues of the state $\rho^{(k)}$ and probability $\mathrm{Accept}(k)$ introduced in Section 1.

▶ **Definition 10.** *Given a state ρ and set of two outcome measurements $\mathcal{M}$ let the state $\rho^{(k)}_{\mathcal{B}(\mathcal{M})}$ be the resulting state when the measurement $\mathcal{B}(\mathcal{M})$ is applied k times in sequence to a quantum system initially in state ρ and the reject outcome is observed each time, so*

$$\rho^{(k)}_{\mathcal{B}(\mathcal{M})} = \frac{E_0^k \rho E_0^k}{\mathrm{Tr}\left[E_0^k \rho E_0^k\right]}. \tag{18}$$

Let $\mathrm{Accept}_{\mathcal{B}(\mathcal{M})}(k)$ be the probability that at least one accepting outcome is observed when the measurement $\mathcal{B}(\mathcal{M})$ is applied k times in sequence to a quantum system in state ρ (equivalently, the probability that not all outcomes observed are reject), so

$$\mathrm{Accept}_{\mathcal{B}(\mathcal{M})}(k) = 1 - \mathrm{Tr}\left[E_0^k \rho E_0^k\right]. \tag{19}$$

When the set of measurements $\mathcal{M}$ is clear from context we will refer to these objects using the simplified notation $\rho^{(k)}_{\mathcal{B}}$ and $\mathrm{Accept}_{\mathcal{B}}(k)$.

▶ Remark 11. We can also write $\mathrm{Accept}_{\mathcal{B}}(k)$ as

$$\mathrm{Accept}_{\mathcal{B}}(k) = \sum_{i=0}^{k-1} (1 - \mathrm{Accept}_{\mathcal{B}}(i)) \,\mathrm{Tr}\left[(1 - E_0^2)\rho^{(i)}_{\mathcal{B}}\right]. \tag{20}$$

We note that (unlike in the random measurements case) the states ρ and $\rho^{(k)}_{\mathcal{B}}$ are related in a very simple way – via conditioning on the single PSD matrix E_0^k. We can use this observation to prove some basic results about $\rho^{(k)}_{\mathcal{B}}$ and $\mathrm{Accept}_{\mathcal{B}}(k)$.

▶ **Lemma 12** (Gentle Blended Measurements). *Let ρ be a state, $\mathcal{M}$ be a set of two outcome measurements and define $\rho^{(k)}_{\mathcal{B}}$ and $\mathrm{Accept}_{\mathcal{B}}(k)$ as in Definition 10. Then,*

$$\left\|\rho^{(k)}_{\mathcal{B}} - \rho\right\|_1 \leq 2\sqrt{\mathrm{Accept}_{\mathcal{B}}(k)}. \tag{21}$$

Proof. Immediate from the gentle measurement lemma. ◀

▶ **Lemma 13.** *For any blended measurement $\mathcal{B}(\mathcal{M})$ and states $\rho^{(k)}_{\mathcal{B}}$ defined as in Lemma 12 we have*

$$\mathrm{Tr}\left[E_0^2 \rho^{(k)}_{\mathcal{B}}\right] \geq \mathrm{Tr}\left[E_0^2 \rho^{(k-1)}_{\mathcal{B}}\right] \tag{22}$$

where $k \geq 1$ and $\rho^{(0)}_{\mathcal{B}} = \rho$.

Proof. Immediate since conditioning on a measurement outcome can only increase the probability of that measurement outcome occurring again. See extended version for details. ◀

3.3 Gentle Random Measurements

In this section we apply the tools from Section 3.1, and Section 3.2 to attain bounds on the disturbance caused by and accepting probability of repeated random measurements. First, we show how the notation introduced in Definition 7 can be used to describe the quantities $\mathrm{Accept}(k)$ and $\rho^{(k)}$ defined in Section 1.

▶ Remark 14. Let $\mathcal{M} = \{M_1, M_2, \dots, M_m\}$ be a set of two outcome projective measurements and ρ be a state. Define the set of matrices $\overline{\mathcal{M}} = \{1 - M_1, 1 - M_2, \dots, 1 - M_m\}$. Then we can restate $\mathrm{Accept}(k)$ and $\rho^{(k)}$ from Theorem 1 as

$$\mathrm{Accept}(k) = 1 - \frac{1}{m^k} \sum_{T \in \mathcal{T}^{(k)}_{\overline{\mathcal{M}}}} \mathrm{Tr}\big[T\rho T^\dagger\big] \quad \text{and} \tag{23}$$

$$\rho^{(k)} = \frac{1}{m^k(1 - \mathrm{Accept}(k))} \sum_{T \in \mathcal{T}^{(k)}_{\overline{\mathcal{M}}}} T\rho T^\dagger \,. \tag{24}$$

▶ **Lemma 15.** *Given a state ρ and set of two outcome projective measurements $\mathcal{M}$, define $\rho^{(k)}$ as in Section 1 (so $\rho^{(k)}$ gives the state of the system initially in state ρ after k random measurements reject) and $\mathrm{Accept}_{\mathcal{B}}(k)$ as in Section 3.2 (so $\mathrm{Accept}_{\mathcal{B}}(k)$ gives the probability that at least one of k repeated blended measurements applied to ρ accepts). Then*

$$\mathrm{F}\left(\rho^{(k)}, \rho\right) \geq 1 - \mathrm{Accept}_{\mathcal{B}}(k)\,. \tag{25}$$

Proof. We first prove the result when $\rho = |\psi\rangle\!\langle\psi|$ is a pure state. In that case, we find

$$\begin{aligned}
\mathrm{F}\left(\rho, \rho^{(k)}\right)^2 &= \langle\psi|\rho^{(k)}|\psi\rangle && (26)\\
&= \frac{1}{m^k} \sum_{T \in \mathcal{T}^{(k)}_{\overline{\mathcal{M}}}} \mathrm{Tr}\big[|\psi\rangle\!\langle\psi|\, T\, |\psi\rangle\!\langle\psi|\, T^\dagger\big] (1 - \mathrm{Accept}(k))^{-1} && (27)\\
&\geq \frac{1}{m^{2k}} \sum_{T,S \in \mathcal{T}^{(k)}_{\overline{\mathcal{M}}}} \mathrm{Tr}[|\psi\rangle\!\langle\psi|\, T\, |\psi\rangle\!\langle\psi|\, S] (1 - \mathrm{Accept}(k))^{-1} && (28)\\
&= \left(\frac{1}{m^k} \sum_{T \in \mathcal{T}^{(k)}_{\overline{\mathcal{M}}}} \mathrm{Tr}[T\, |\psi\rangle\!\langle\psi|]\right)^2 (1 - \mathrm{Accept}(k))^{-1} && (29)\\
&= (1 - \mathrm{Accept}_{\mathcal{B}}(k))^2 \, (1 - \mathrm{Accept}(k))^{-1} \geq (1 - \mathrm{Accept}_{\mathcal{B}}(k))^2 \,. && (30)
\end{aligned}$$

In the derivation above we used Remark 14 (Equation (24)) to go from the first line to the second, Corollary 8 to go from the second line to the third. Then we replace the definition of $\mathrm{Accept}_{\mathcal{B}}(k)$ from Definition 10 (Equation (19)) to get the desired result.

As in the proof of the Gentle Measurement Lemma, when ρ is a mixed state we can recover the same bound by applying the previous proof to a purification of ρ. The result follows from Uhlmann's theorem [11]. See extended version for details. ◀

With this we can bound the damage caused by random measurements by the accepting probability of a blended measurement procedure.

▶ **Corollary 16.** *Given a state ρ and set of two outcome projective measurements $\mathcal{M}$, define $\rho^{(k)}$ as in Section 1 and $\mathrm{Accept}_{\mathcal{B}}(k)$ as in Section 3.2. Then*

$$\left\|\rho - \rho^{(k)}\right\|_1 \leq 2\sqrt{2\,\mathrm{Accept}_{\mathcal{B}}(k)}\,. \tag{31}$$

Proof. Immediate from the Fuchs-Van de Graaf Inequalities. See extended version for details. ◀

Now we relate the acceptance probability of the random measurement procedure to the accept probability of the blended measurement procedure. We begin with a slight restatement of Corollary 8 which gives a relationship between the probability of measurement outcomes being observed on states $\rho^{(k)}$ and $\rho_{\mathcal{B}}^{(2k)}$.

▶ Remark 17. We can expand out the definition of $\rho_{\mathcal{B}}^{(2k)}$ in Definition 10 to get the following formulation:

$$\rho_{\mathcal{B}}^{(2k)} = \frac{m^{-2k}}{1 - \mathrm{Accept}_{\mathcal{B}}(2k)} \left(\sum_{T,S \in \mathcal{T}_{\mathcal{M}}^{(k)}} T\rho S \right). \tag{32}$$

▶ **Corollary 18.** *For any state ρ and set of two outcome projective measurements $\mathcal{M}$ define states $\rho^{(k)}$, $\rho_{\mathcal{B}}^{(k)}$ and probabilities* $\mathrm{Accept}(k)$ *and* $\mathrm{Accept}_{\mathcal{B}}(k)$ *as in Section 1 and Section 3.2. Also, let X be an arbitrary PSD matrix. Then*

$$(1 - \mathrm{Accept}(k)) \operatorname{Tr}\left[X\rho^{(k)}\right] \geq (1 - \mathrm{Accept}_{\mathcal{B}}(2k)) \operatorname{Tr}\left[X\rho_{\mathcal{B}}^{(2k)}\right]. \tag{33}$$

Proof. Immediate from Remark 14 (Equation (24)), Corollary 8, and Remark 17. See extended version for details. ◀

Next, we show that Corollary 18 gives an easy upper bound $\mathrm{Accept}(k)$ in terms of $\mathrm{Accept}_{\mathcal{B}}(k)$. This bound is not required for the proof of Theorem 1, but does give a useful relationship between the random and blended measurement procedures which we will use in future sections.

▶ **Theorem 19.** *For any state ρ and set of two outcome projective measurements $\mathcal{M}$ define* $\mathrm{Accept}(k)$, $\mathrm{Accept}_{\mathcal{B}}(k)$ *as in Section 1 and Section 3.2. Then we have*

$$1 - \mathrm{Accept}(k) \geq 1 - \mathrm{Accept}_{\mathcal{B}}(2k) \geq (1 - \mathrm{Accept}_{\mathcal{B}}(k))^2. \tag{34}$$

Proof. Omitted as it is not necessary for Theorem 1. See extended version of details. ◀

We can also use Corollary 18 to lower bound of $\mathrm{Accept}(k)$ in terms of $\mathrm{Accept}_{\mathcal{B}}(k)$. This is the direction required for the proof of Theorem 1.

▶ **Theorem 20.** *For any state ρ and set of two outcome projective measurements $\mathcal{M}$ define* $\mathrm{Accept}(k)$, $\mathrm{Accept}_{\mathcal{B}}(k)$ *as in Section 1 and Section 3.2. We have*

$$\mathrm{Accept}(k) \geq \frac{1}{2}\mathrm{Accept}_{\mathcal{B}}(2k) \tag{35}$$

Proof. Define $\mathbf{M} = 1 - E_0^2$. Note that for any state σ, $\operatorname{Tr}[\mathbf{M}\sigma]$ gives the probability that the blended measurement $\mathcal{B}(\mathcal{M})$ results in an accepting outcome, which is equal to the probability that a measurement chosen uniformly at random from $\mathcal{M}$ accepts on σ. We calculate

$$\begin{aligned}
\mathrm{Accept}(k) &= \sum_{i=0}^{k-1}(1-\mathrm{Accept}(i))\,\mathrm{Tr}\Big(\mathbf{M}\rho^{(i)}\Big) && (36)\\
&\geq \sum_{i=0}^{k-1}(1-\mathrm{Accept}_{\mathcal{B}}(2i))\,\mathrm{Tr}\Big(\mathbf{M}\rho_{\mathcal{B}}^{(2i)}\Big) && (37)\\
&\geq \frac{1}{2}\sum_{j=0}^{2k-1}(1-\mathrm{Accept}_{\mathcal{B}}(j))\,\mathrm{Tr}\Big(\mathbf{M}\rho_{\mathcal{B}}^{(j)}\Big) && (38)\\
&= \frac{1}{2}\,\mathrm{Accept}_{\mathcal{B}}(2k)\,. && (39)
\end{aligned}$$

The first and last lines follows from a telescoping sums argument for both blended and randomized measurements. The second line is a direct application of Corollary 18, and the final line follows from Lemma 13. ◀

Finally, we are in a position to prove Theorem 1. We begin by repeating the theorem.

▶ **Theorem 1.** *Let $\mathcal{M} = \{M_1, M_2, \ldots, M_m\}$ be a set of two outcome projective measurements, and ρ be a pure state. Consider the process where a measurement from the set $\mathcal{M}$ is selected universally at random and applied to a quantum system initially in state ρ. Let $\mathrm{Accept}(k)$ be the probability that at least one measurement accepts after k repetitions of this process, and let $\rho^{(k)}$ be the state of this quantum system after k repetitions where no measurement accepts. Then*

$$\left\|\rho-\rho^{(k)}\right\|_1 \leq 4\sqrt{\mathrm{Accept}(\lceil k/2\rceil)} \leq 4\sqrt{\mathrm{Accept}(k)}\,. \tag{40}$$

Proof. Immediate from Corollary 16 and Theorem 20. See extended version for details. ◀

4 Algorithms for Quantum OR

In our first application of the results from Section 3.2 and Section 3.3, we give two different procedures for Quantum OR. We call a procedure a "Quantum OR" if it has properties similar to Corollary 11 from Ref. [7], which we restate here.

▶ **Theorem 21** (Corollary 11 From Ref. [7])**.** *Let $\Lambda_1, \Lambda_2, \ldots, \Lambda_m$ be a sequence of projectors and fix $\epsilon > 1/2, \delta$. Let ρ be a state such that either there exists an $i \in [m]$ with $\mathrm{Tr}[\Lambda_i\rho] > 1-\epsilon$ (Case 1) or $\mathbb{E}_j[\mathrm{Tr}[\Lambda_j\rho]] \leq \delta$ (Case 2). Then there exists a test that uses one copy of ρ and: in Case 1, accepts with probability $(1-\epsilon)^2/7$; in Case 2, accepts with probability at most $4\delta m$.*

4.1 Repeated Blended Measurements

We first show that repeated application of the blended measurement defined in Section 3.2 yields a Quantum OR protocol. We define the protocol next.

The following result shows that Algorithm 1 solves the Quantum OR problem and obtains better parameters than the protocol given in Ref. [7].

Algorithm 1 Blended Measurement Quantum OR.

Input: A classical description of a set of two outcome measurements $\mathcal{M} = \{M_1, M_2, \ldots, M_m\}$ and a single copy of a state ρ.

Output: ACCEPT or REJECT.

1. Prepare a quantum system in state ρ.
2. Repeat m times:
   a. Perform the blended measurement $\mathcal{B}(\mathcal{M})$ on the state. If the measurement accepts, return ACCEPT.
3. Return REJECT.

▶ **Theorem 22** (Blended Quantum OR). *Let $\mathcal{M} = \{M_1, M_2, \ldots, M_m\}$ be a set of two outcome measurements and let ρ be a quantum state. Define*

$$p_\downarrow = \max_i \{\mathrm{Tr}[M_i \rho]\}, \; p_\uparrow = \sum_i \mathrm{Tr}[M_i \rho], \text{ and} \tag{41}$$

$$p_{accept} = \mathbb{P}\,(\text{Algorithm 1 accepts with input } \mathcal{M} \text{ and } \rho)\,. \tag{42}$$

Then the following inequalities hold:

$$p_\downarrow^2/4 < p_{accept} < p_\uparrow\,. \tag{43}$$

Proof. We first prove the upper bound. Let $p_{reject} = 1 - p_{accept}$ be the probability the algorithm rejects, and let $p_{reject}(k)$ be the probability that the algorithm does not accept on the k^{th} measurement, conditioned on the algorithm not accepting any of the $i-1$ measurements prior. We note

$$p_{reject}(1) = \frac{1}{m}\sum_i (1 - \mathrm{Tr}[M_i\rho]) = 1 - \frac{p_\uparrow}{m} \quad \text{and} \quad p_{reject}(k) \geq p_{reject}(1)\,. \tag{44}$$

Plugging these into the definition of p_{accept}

$$p_{accept} = 1 - p_{reject} = 1 - \prod_{k=1}^{m} p_{reject}(k) \leq 1 - \left(1 - \frac{p_\uparrow}{m}\right)^m \leq 1 - e^{-p_\uparrow} \leq p_\uparrow\,. \tag{45}$$

We first apply Lemma 13, then the definition of e^x and the inequality $1 + x \leq e^x$.

We now prove the lower bound. First, for ease of notation, we relabel the measurements in $\mathcal{M}$ so that $p_\downarrow = \mathrm{Tr}[M_1\rho]$. Then let $\mathrm{Reject}_{\mathcal{B}}(k)$ be the probability that the first k measurements of Algorithm 1 reject (with $\mathrm{Reject}_{\mathcal{B}}(0) = 1$), and $\rho_{\mathcal{B}}^{(k)}$ be the state of the quantum system initially in state ρ conditioned on the first k measurements of Algorithm 1 rejecting (with $\rho_{\mathcal{B}}^{(0)} = \rho$). By definition, the probability of accepting is at least the sum over all rounds of the probability the algorithm accepts for the first time on a given round with measurement M_1, so

$$p_{accept} \geq \frac{1}{m}\sum_{k=0}^{m-1} \mathrm{Reject}_{\mathcal{B}}(k)\,\mathrm{Tr}\left[M_1 \rho_{\mathcal{B}}^{(k)}\right]. \tag{46}$$

In order to return reject the algorithm must at least reject on the first k measurements, so

$$\mathrm{Reject}_{\mathcal{B}}(k) \geq p_{reject} = 1 - p_{accept}\,. \tag{47}$$

Then applying Lemma 12 and the operational definition of the trace distance to Equation (46) along with the previous two facts gives

$$p_{accept} \geq \frac{1}{m}\sum_{k=0}^{m-1} \mathrm{Reject}_{\mathcal{B}}(k)\left(\mathrm{Tr}[M_1\rho] - \sqrt{1-\mathrm{Reject}_{\mathcal{B}}(k)}\right) \tag{48}$$

$$\geq (1-p_{accept})\left(p_{\downarrow} - \sqrt{p_{accept}}\right), \tag{49}$$

where the last two lines simply apply Equation (47). Rearranging terms we arrive at the following

$$p_{\downarrow} \leq \frac{p_{accept}}{1-p_{accept}} + \sqrt{p_{accept}}\,. \tag{50}$$

We note that $\frac{x}{1-x} \leq \sqrt{x}$ whenever $x \leq \frac{1}{2}(3-\sqrt{5}) \approx 0.38$ (take x to be p_{accept}). Therefore, if $p_{accept} \leq 0.38$, we have $p_{accept} \geq p_{\downarrow}^2/4$. If p_{accept} is greater than 0.38 then it is still larger than $\min(p_{\downarrow}^2/4, 0.38) = p_{\downarrow}^2/4$, which completes the lower bound. ◀

▶ **Corollary 23.** *In the same setting as Theorem 21, but with $\Lambda_1, \ldots, \Lambda_m$ arbitrary (i.e. not necessarily projective) two outcome measurements, there exists a test that uses one copy of ρ and accepts with probability at least $(1-\epsilon)^2/4$ in case 1 and at most δn in case 2.*

Proof. Theorem 22 shows that Algorithm 1 satisfies the required bounds. ◀

4.2 Repeated Random Measurements

Motivated by the original Quantum OR claimed in Ref. [2], we show that repeated random measurements still yield a (weaker) Quantum OR. The Random Measurement Quantum OR protocol is described in Algorithm 2.

Algorithm 2 Random Measurement Quantum OR.

Input: A black-box implementation of each measurement in a set of two outcome measurements $\mathcal{M} = \{M_1, M_2, \ldots, M_m\}$ and a single copy of a state ρ.

Output: ACCEPT or REJECT.

1. Prepare a quantum system in state ρ.
2. Repeat m times:
   a. Pick a random measurement $M_i \in \mathcal{M}$.
   b. Perform the measurement M_i on the current state. If the measurement accepts, return ACCEPT.
3. Return REJECT.

▶ **Theorem 24** (Random Quantum OR). *Let $\mathcal{M} = \{M_1, M_2, \ldots, M_m\}$ be a set of two outcome projective measurements, and ρ be a state. Then using the same definitions for $p_{\downarrow}$ and $p_{\uparrow}$ as in Theorem 22 and letting $p_{accept} = \mathbb{P}$(Algorithm 2 accepts with inputs $\mathcal{M}$ and ρ), the following inequalities hold:*

$$\min\left(p_{\downarrow}^2/4.5, \frac{3-\sqrt{5}}{4}\right) \leq p_{accept} \leq 2p_{\uparrow}\,. \tag{51}$$

Proof. We omit the proof of Theorem 24, as it mirrors the proof of Theorem 22 closely. See extended version for details. ◀

We note that the Random Quantum OR performs worse than the Blended Quantum OR on both the accept and reject case, but performs better in both cases than the test from Ref. [7]. The Random Quantum OR has additional advantages over both protocols, in that it does not require knowledge of a circuit decomposition of the measurements M_i and can even apply the measurements M_i as a black box.

▶ **Corollary 25.** *In the same setting as Theorem 21, there exists a test that uses one copy of ρ, does not require an efficient representation of the measurements Λ_i, and accepts with probability at least $\frac{3-\sqrt{5}}{4}(1-\epsilon)^2$ in case 1 and at most $2\delta n$ in case 2.*

Proof. Theorem 24 shows that Algorithm 2 satisfies the required bounds. ◀

5 Quantum Event Finding

In this section we consider a variant of the quantum OR task in which the goal, given a set of two outcome measurements $\mathcal{M}$ and sample access to a state ρ, is not just to *decide* if there exists a measurement $M_i \in \mathcal{M}$ with $\mathrm{Tr}[M_i\rho]$ large, but also to *find* such a measurement if one exists. We show that the blended measurement procedure described in the previous section solves with problem if certain conditions are met.

▶ **Theorem 26.** *Let $\mathcal{M} = \{M_1, M_2, \ldots, M_m\}$ be a set of two outcome measurements. Let ρ be a state such that either there exists an $i \in [m]$ with $\mathrm{Tr}[M_i\rho] > 1-\epsilon$ (Case 1) or $\sum_i \mathrm{Tr}[M_i\rho] \leq \delta$ (Case 2). Also define*

$$\beta = \sum_{i:\ \mathrm{Tr}[M_i\rho]<1-\epsilon} \mathrm{Tr}[M_i\rho]\,. \tag{52}$$

Then if the blended measurement $\mathcal{B}(\mathcal{M})$ is applied m times in sequence to a quantum system initially in state ρ: in Case 1, with probability at least

$$\frac{(1-\epsilon)^3}{12(1+\beta)}\,, \tag{53}$$

at least one accepting outcome is observed and the first accepting outcome observed corresponds to a measurement M_i with $\mathrm{Tr}[M_i\rho] > 1-\epsilon$; in Case 2, an accepting outcome is observed with probability at most δ.

By relating blended and random measurements as in the proof of Theorem 24, we can also show that the random measurement procedure solves this problem in the same regime as before, but with worse constants and scaling in both ϵ and β.

▶ **Theorem 27.** *Let $\mathcal{M} = \{M_1, M_2, \ldots, M_m\}$ be a set of two outcome projective measurements, and define ρ, β, ϵ and δ as above. Then, if measurements are chosen at random (with replacement) from $\mathcal{M}$ and applied to a quantum system initially in state ρ: in Case 1, with probability at least $(1-\epsilon)^7/(1296(1+\beta)^3)$, at least one measurement accepts and the first accepting measurement is a measurement $M_i \in \mathcal{M}$ with $\mathrm{Tr}[M_i\rho] > 1-\epsilon$; in Case 2, a measurement accepts with probability at most 2δ.*

We begin by proving Theorem 26.

Proof (Theorem 26). The upper bound on the accepting probability in Case 2 follows immediately from the upper bound on the accepting probability in Case 2 of the blended measurement quantum OR procedure stated in Theorem 22.

To prove the lower bound in Case 1 we follow a procedure similar to the one used in the proof of Theorem 22. First, for ease of notation, relabel measurements so that $\mathrm{Tr}[M_j\rho] > 1-\epsilon$ if and only if $j \leq k$ for some constant k. Similar to before, let $\mathrm{Reject}_{\mathcal{B}}(i)$ be the probability that the blended measurement $\mathcal{B}(\mathcal{M})$ is applied i times in sequence to a quantum system initially in state ρ and no measurement accepts, let $\mathrm{Accept}_{\mathcal{B}}(i) = 1 - \mathrm{Reject}_{\mathcal{B}}(i)$, and let $\rho_{\mathcal{B}}^{(i)}$ be the state of the quantum system after i blended measurements all reject. Also let $\mathrm{Return}_{\mathcal{B}}(i)$ be the **event** that the blended measurement procedure accepts for the first time on the i'th measurement and $\mathrm{Success}_{\mathcal{B}}(i)$ be the **event** that the blended measurement procedure accepts for the first time on the ith measurement on a outcome corresponding to a measurement M_j with $\mathrm{Tr}[M_j\rho] > 1-\epsilon$. Then we can lower bound the probability of success on a measurement conditioned on no previous measurement accepting

$$\mathbb{P}\left[\mathrm{Success}_{\mathcal{B}}(i) \,\middle|\, \bigwedge_{j<i} \neg \mathrm{Return}_{\mathcal{B}}(j)\right] \geq \frac{k}{m}\left(1-\epsilon-\sqrt{\mathrm{Accept}_{\mathcal{B}}(i-1)}\right) \tag{54}$$

where the inequality follows from Lemma 12. Additionally, Lemma 13 tells us that

$$\mathbb{P}[\mathrm{Return}_{\mathcal{B}}(i)] \leq (k+\beta)/m\,. \tag{55}$$

Combining these two bounds gives

$$\mathbb{P}[\mathrm{Success}_{\mathcal{B}}(i)|\,\mathrm{Return}_{\mathcal{B}}(i)] \geq \frac{1-\epsilon-\sqrt{\mathrm{Accept}_{\mathcal{B}}(i-1)}}{1+\beta}\,. \tag{56}$$

But we also have that

$$\mathbb{P}[\mathrm{Return}_{\mathcal{B}}(i)] = \mathrm{Accept}_{\mathcal{B}}(i) - \mathrm{Accept}_{\mathcal{B}}(i-1)\,. \tag{57}$$

Then we can bound the overall fraction of the first accepting events in which the accepting outcome corresponds to a measurement M_i with $\mathrm{Tr}[M_i\rho] > 1-\epsilon$ as

$$\frac{\sum_{i=1}^m \mathbb{P}[\mathrm{Success}_{\mathcal{B}}(i)]}{\sum_{i=1}^m \mathbb{P}[\mathrm{Return}_{\mathcal{B}}(i)]} = \frac{\sum_{i=1}^m \mathbb{P}[\mathrm{Return}_{\mathcal{B}}(i)]\mathbb{P}[\mathrm{Success}_{\mathcal{B}}(i)|\,\mathrm{Return}_{\mathcal{B}}(i)]}{\sum_{i=1}^m \mathbb{P}[\mathrm{Return}_{\mathcal{B}}(i)]} \tag{58}$$

$$\geq \frac{1-\epsilon}{3(1+\beta)}\,. \tag{59}$$

Where the inequalities come from the observation that the quantity being summed is a increasing function of $\mathrm{Accept}_{\mathcal{B}}(i)$. Combining this bound with the lower bound on the accepting probability of the repeated blended measurement given in Theorem 22 we see that, in Case 1, the probability that the repeated blended measurement accepts at least once and the first outcome it accepts corresponds on a measurement M_i with $\mathrm{Tr}[M_i\rho] > 1-\epsilon$ is bounded below by

$$\frac{(1-\epsilon)}{3(1+\beta)}\frac{(1-\epsilon)^2}{4} \geq \frac{(1-\epsilon)^3}{12(1+\beta)}\,, \tag{60}$$

as claimed. ◀

Proof of Theorem 27. We omit the proof of Theorem 27 for brevity, as it mirrors closely the proof of Theorem 26. See extended version for details. ◀

6 Quantum Threshold Search

In Section 5, we were able to show that in certain cases performing repeated blended or random measurements solves event finding which we defined to be the problem of identifying an event that has a high probability of accepting on an unknown state, assuming such a measurement exists. In this section we present a finer-grained version of that analysis. We show that the average accepting probability of the measurement returned by the blended (or random) measurement procedure is related to the average accepting probability of the measurement returned by repeatedly applying (random selected) measurements to fresh copies of the unknown state and returning the first measurement that accepts. In the later part of this section, we show we can use this stronger event finding lemma to improve our blended measurement protocol to a *threshold search* protocol which uses $O(\log^2(m))$ copies of the unknown state.

6.1 A Stronger Event Finding Lemma

We will state the stronger event finding lemma in terms of averages γ, and $\widetilde{\gamma}_j^{\mathcal{B}}$, which we now define. Fix a set $\mathcal{M} = \{M_i\}_{i\in[m]}$ of measurements that one wants to perform event finding over, and let $\rho \in \mathbb{C}^{d\times d}$ be an unknown quantum state. Then define the following quantity (that depends implicitly on $\mathcal{M}$).

$$\gamma = \frac{\sum_{i\in[m]} \mathrm{Tr}[M_i\rho]^2}{\sum_{i\in[m]} \mathrm{Tr}[M_i\rho]} . \tag{61}$$

To gain some intuition for γ, consider the following two-step procedure: (1) select a measurement M_i at random from $\mathcal{M}$ and apply it to ρ; (2) return M_i and success if the measurement accepts and return failure otherwise. The quantity γ is the average accepting probability of the measurement returned by this procedure conditioning on success.

We are interested in the average accepting probability of the measurement returned by the m round blended event finding procedure (in the event the blended event finding procedure does not return a measurement we say it has returned a measurement with accepting probability zero). Denoting this quantity by $\widetilde{\gamma}^{\mathcal{B}}$ we see we can write it as.

$$\widetilde{\gamma}^{\mathcal{B}} = \sum_{i=1}^{m}\sum_{j=0}^{m-1}(1-\mathrm{Accept}_{\mathcal{B}}(j))\frac{\mathrm{Tr}\left[M_i\rho_{\mathcal{B}}^{(j)}\right]\mathrm{Tr}[M_i\rho]}{m} . \tag{62}$$

We now show that this quantity is lower bounded by a polynomial function of γ.

▶ **Lemma 28.** *Let $\mathcal{M}$ be a set of measurements, and ρ be an unknown quantum state. Let γ and $\widetilde{\gamma}^{\mathcal{B}}$ be defined as in Equation (61) and Equation (62). Then the following inequality holds: $\widetilde{\gamma}^{\mathcal{B}} \geq \frac{\gamma^3}{8}(1-\gamma^2/4)$*

Proof. Fix a value of j and consider the following equation:

$$\sum_{i=1}^{m}(1-\mathrm{Accept}_{\mathcal{B}}(j))\frac{\mathrm{Tr}\left[M_i\rho_{\mathcal{B}}^{(j)}\right]\mathrm{Tr}[M_i\rho]}{m} \tag{63}$$

$$\geq \sum_{i=1}^{m}(1-\mathrm{Accept}_{\mathcal{B}}(j))\frac{\mathrm{Tr}[M_i\rho]}{m}\left(\mathrm{Tr}[M_i\rho]-\sqrt{\mathrm{Accept}_{\mathcal{B}}(j)}\right) \tag{64}$$

$$= \mathrm{Accept}_{\mathcal{B}}(0)(1-\mathrm{Accept}_{\mathcal{B}}(j))\left(\gamma-\sqrt{\mathrm{Accept}_{\mathcal{B}}(j)}\right) . \tag{65}$$

In going from the first to second line, we apply the gentle blended measurement lemma (Lemma 12) and the operational definition of the trace distance. We then use the definition of $\text{Accept}_{\mathcal{B}}(0)$, which is the denominator in the definition of γ. Since we are trying to lower bound the sum, let m^* be the smallest index such that $\text{Accept}_{\mathcal{B}}(m^*) \geq \gamma^2/4$. By Theorem 22, this index is guaranteed to exist. Then taking the sum up to m^*, we get

$$\begin{aligned}\widetilde{\gamma}^{\mathcal{B}} &\geq \sum_{j=0}^{m^*-1} \sum_{i=1}^{m} (1 - \text{Accept}_{\mathcal{B}}(j)) \frac{\text{Tr}\left[M_i \rho_{\mathcal{B}}^{(j)}\right] \text{Tr}[M_i \rho]}{m} \\ &\geq \sum_{j=0}^{m^*-1} \text{Accept}_{\mathcal{B}}(0) \left(\gamma - \sqrt{\text{Accept}_{\mathcal{B}}(j)}\right) (1 - \text{Accept}_{\mathcal{B}}(j)) \\ &= \frac{\gamma^3}{8}(1 - \gamma^2/4)\,.\end{aligned}$$

We first substitute the lower bound for each individual j. Then we use the fact that for all $j < m^*$, $\text{Accept}_{\mathcal{B}}(j) < \gamma^2/4$ to turn $\gamma - \sqrt{\text{Accept}_{\mathcal{B}}(j)}$ into $\gamma/2$. Finally we use the fact that every $\text{Accept}_{\mathcal{B}}(i) \leq i\, \text{Accept}_{\mathcal{B}}(0)$ to go from $m^* \,\text{Accept}_{\mathcal{B}}(0)$ down to $\text{Accept}_{\mathcal{B}}(m^*)$, and then the assumption that $\text{Accept}_{\mathcal{B}}(m^*) \geq \gamma^2/4$. This completes the proof. Note that $\gamma \leq 1$, so we could take $(1 - \gamma^2/4) \geq 3/4 \geq 1/2$ to get a cleaner looking lower bound of $\gamma^3/16$. ◀

Similar to the blended case, we can prove a strong event finding lemma for sequences of random measurements. Recall that $\rho^{(j)}$ is the post-measurement state after applying j many random measurements from $\mathcal{M}$ and only seeing rejects. We similarly define $\widetilde{\gamma}$, the average accepting probability of the measurement returned by m rounds of random measurements.

$$\widetilde{\gamma} = \sum_{j=0}^{m-1} (1 - \text{Accept}(j)) \left(\frac{\sum_{i=1}^{m} \text{Tr}[M_i \rho] \,\text{Tr}\left[M_i \rho^{(j)}\right]}{m} \right). \tag{66}$$

▶ **Lemma 29.** *Let $\mathcal{M}$ be a set of projective measurements and ρ be an unknown state. Let γ and $\widetilde{\gamma}$ be as defined in Equation (61) and Equation (66). Then the following inequality holds: $\widetilde{\gamma} \geq \frac{\gamma^3}{16}(1 - \gamma^2/4)$.*

Proof. Omitted as the proof mirrors closely the proof of Lemma 28, but with Corollary 16 instead of Lemma 12. See extended version for details. ◀

6.2 Threshold Search via Repeated Blended Measurements

In the previous section, we strengthened the quantum event finding lemma A related problem to quantum event finding is *threshold search* [5]. In threshold search, one is asked to output a measurement satisfying $\text{Tr}[M_i \rho] \geq 1/3$ with constant probability, given the fact that there exists a measurement with $\text{Tr}[M_i \rho] \geq 3/4$. Ref [5] show that if this problem can be solved for projective measurements using k copies of the unknown state, then there is an algorithm for Shadow Tomography [3] that uses $O\left(\frac{\log(d) L(k+L)}{\epsilon^4}\right)$ copies of the unknown state, where $L = \log\left(\frac{\log d}{\delta \epsilon}\right)$. In this section, we show that the repeatedly applying blended or random measurements, while "boosting" around a uniformly random threshold, solves threshold search using $O(\log^2(m))$ copies of the unknown state, matching the best known shadow tomography upper bounds from Ref. [5].

We first introduce the *binomial measurement*, which boosts the sensitivity of a measurements to values far from a threshold θ.

▶ **Lemma 30.** *Let $\rho \in \mathbb{C}^{d\times d}$ be a quantum state and A be a quantum event. Let $n \in \mathbb{N}$ and $\theta \in [0,1]$ be an arbitrary threshold, and let $S \sim \mathsf{Binom}(n, \mathrm{Tr}[A\rho])$. Then there exists a quantum event $\mathsf{B}(A, n, \theta) \in (\mathbb{C}^{d\times d})^{\otimes n}$ such that*

$$\mathrm{Tr}\left[\mathsf{B}(A,n,\theta)\rho^{\otimes n}\right] = \mathbb{P}[S \geq \theta n]\,. \tag{67}$$

We call the measurement $\mathsf{B}(A,n,\theta)$ the binomial measurement of A over n registers with threshold θ. *If A is projective then so is $\mathsf{B}(A,n,\theta)$.*

Given a set of measurement $\mathcal{M}$ for threshold search and a threshold θ, we define the set of binomial measurements with threshold θ using n copies, $\mathsf{B}(\mathcal{M},n,\theta) = \{\mathsf{B}(M_i,n,\theta) : i \in [m]\}$. We can similarly define the blended measurement corresponding to $\mathsf{B}(\mathcal{M},n,\theta)$. Consider the following algorithm for threshold search.

Algorithm 3 Blended Measurement Threshold Search.

Input: A classical description of a set of two outcome measurements $\mathcal{M} = \{M_1, M_2, \ldots, M_m\}$ and $n = 100\log^2 m$ copies of an unknown state ρ.

Output: Measurement M_i or REJECT.

1. Select a random $\theta \in [2/5, 3/5]$.
2. Repeat m times:
   a. Perform the blended measurement $\mathcal{B}(\mathsf{B}(\mathcal{M},n,\theta))$ on n copies of the state. If the measurement accepts, return the accepting outcome.
3. Return REJECT.

In order to show that the algorithm works, we first show that if there is a measurement satisfying $\mathrm{Tr}[M_i\rho] \geq 3/4$ and $\widetilde{\gamma}^{\mathcal{B}} \geq c$ (for any constant c) for a fixed choice of θ, the algorithm outputs a measurement satisfying $\mathrm{Tr}[M_i\rho] \geq 1/3$ with probability at least $c - 1/m$. Then, we show that with constant probability (over the choice of the threshold θ), $\gamma \geq 1/8$, which implies a constant lower bound for $\widetilde{\gamma}^{\mathcal{B}}$ by Lemma 28.

▶ **Lemma 31.** *Fix a choice of threshold θ, let $\widetilde{\gamma}^{\mathcal{B}}$ be defined as in Equation (62) with respect to $\mathsf{B}(\mathcal{M}, 100\log^2(m), \theta)$. Then if there exists a constant c satisfying $\widetilde{\gamma}^{\mathcal{B}} \geq c$, then Algorithm 3 outputs a measurement satisfying $\mathrm{Tr}[M_i\rho] \geq 1/3$ with probability at least $c - 1/m$.*

Proof. $\widetilde{\gamma}^{\mathcal{B}}$ is the average value of $\mathrm{Tr}[\mathsf{B}(M_i,n,\theta)\rho^{\otimes n}]$ over the output distribution of the blended measurement threshold search algorithm. For all measurements satisfying $\mathrm{Tr}[M_i\rho] < 1/3$, we know that the binomial measurement satisfies $\mathrm{Tr}[\mathsf{B}(M_i,n,\theta)\rho^{\otimes n}] < 1/m$. Let p_b be the probability of outputting a measurement satisfying $\mathrm{Tr}[M_i\rho] < 1/3$, and p_g be the probability of outputting a measurement satisfying $\mathrm{Tr}[M_i\rho] \geq 1/3$. Then we have

$$p_g \geq c - p_b/m \geq c - 1/m\,. \tag{68}$$

Thus the probability of outputting a measurement satisfying $\mathrm{Tr}[M_i\rho] \geq 1/3$ is at least $c - 1/m$. ◀

Up to this point, we have shown $\widetilde{\gamma}^{\mathcal{B}}$ is lower bounded by a function of γ, and that having a constant lower bound for $\widetilde{\gamma}^{\mathcal{B}}$ implies a constant success probability for the algorithm. All that remains to be seen is that γ is constant for most choices of the threshold θ. In order to show that most thresholds θ are "good", we define some functions and sets that are going to be used in heavily. Given two numbers, α and β, define the set $\mathcal{M}[\alpha,\beta]$ to be as follows

$$\mathcal{M}[\alpha,\beta] = \{i : \alpha \leq \mathrm{Tr}[M_i\rho] \leq \beta\}\,. \tag{69}$$

Define $n(\alpha, \beta)$ to be the size of $\mathcal{M}[\alpha, \beta]$. We say that a value of θ is "bad" if the following holds

$$\sum_{i \in \mathcal{M}[0,\theta]} \exp\bigl(-100 \log^2 m(\theta - \mathrm{Tr}[M_i \rho])^2\bigr) \geq 4n(\theta, 1) \,. \tag{70}$$

The left hand side is related to the probability that a measurement with accepting probability below θ will be chose and accepted by the binomial measurement (using $k = 100 \log^2 m$ copies of the state), and the right side is related to the probability that a measurement with accepting probability higher than θ will be chosen. "Good" threshold values are those that are not bad.

The following claims show that the set of bad measurements has measure bounded by a constant.

▶ **Lemma 32.** *Assume that for the set of measurements $\mathcal{M}$, $n(\theta, 1) \geq 1$. Let θ be a bad threshold, then there exists a number $\beta_\theta \leq \theta$ such that*

$$n(\beta_\theta, \theta) \geq \exp\bigl(50 \log^2 m(\theta - \beta_\theta)^2\bigr) n(\theta, 1) \,. \tag{71}$$

Proof. Assume for the sake of contradiction that for all $\beta \leq \theta$,

$$n(\beta, \theta) \leq \exp\bigl(50 \log^2 m(\beta - \theta)^2\bigr) \,. \tag{72}$$

We want to arrive at the contradiction with the fact that θ is a bad threshold. To do so, we can evaluate the left hand side of Equation (70). For ease of notation, let $\eta(x) = n(\theta - x, \theta)$, $f(x) = \exp\bigl(-100 \log^2(m) x^2\bigr)$, and $f'(x) = \frac{d}{dx} f(x)$. Also let $L = n(0, \theta)$, and denote by $(y_i)_{i=1}^L$ the list of $\mathrm{Tr}[M_i \rho]$ for $i \in \mathcal{M}[0, \theta]$, in increasing order. Let $x_i = \theta - y_i$. Then we have that

$$\sum_{i \in n(0,\theta)} \exp(-100 \log^2 m(\theta - \mathrm{Tr}[M_i \rho])^2) = -\int_0^\infty \eta(x) f'(x) dx \,. \tag{73}$$

Note that for all $x > 0$ we have $f'(x) = -200 \log^2(m) x \exp\bigl(-100 \log^2(m)(x)^2\bigr) \leq 0$. We can plug in the assumed upper bound on $n(\beta, \theta) = \eta(\theta - \beta)$ to obtain

$$\begin{aligned} &\sum_{i \in n(0,\theta)} \exp(-100 \log^2 m(\theta - \mathrm{Tr}[M_i \rho])^2) \\ &\qquad \leq -4 \exp\bigl(-50 \log^2 m x^2\bigr)\Big|_0^\infty && (74) \\ &\qquad = 4 && (75) \\ &\qquad \leq 4n(\theta, 1) \,. && (76) \end{aligned}$$

Here the last line uses the assumption that $n(\theta, 1) \geq 1$. This contradicts Equation (70), which proves that a suitable choice of β_θ exists. ◀

Now we know that for every bad choice of threshold θ, there is an interval below θ in which the number of measurements that have accepting probabilities lying in the interval is exponentially large, compared to the size of the interval. We recursively define the following sets of intervals, which contain all of the bad thresholds. Let $\theta_0 = \max\{\theta \leq 2/3 : \theta \text{ bad}\}$.

$$\theta_i = \max\{\theta \leq \beta_{\theta_i - 1} : \theta \text{ bad}\} \,. \tag{77}$$

For convenience, define $\beta_i = \beta_{\theta_i}$, and let $d_i = \theta_i - \beta_i$. Let N be the total number of θ_i. First, we show that the total size of the intervals (squared) lower bounds the number of measurements contained in intervals.

▶ **Lemma 33.** *Assume that $n(2/3,1) \geq 1$, then the following bound holds on the number of measurements contained in the intervals.*

$$\sum_{i=0}^{N} n(\beta_i,\theta_i) \geq \exp\left(50\log^2(m)\sum_i d_i^2\right). \tag{78}$$

Proof. We begin by induction. By Lemma 32 and the assumption that $n(2/3,1) \geq 1$ (and therefore $n(\theta_0,1) \geq 1$, we have that

$$n(\beta_0,\theta_0) \geq \exp\bigl(50\log^2(m)d_0^2\bigr). \tag{79}$$

Now assume that the claim holds for the sum from 0 to $j-1$, we evaluate the sum up to j as follows

$$\sum_{i=0}^{j} n(\beta_i,\theta_i) = n(\beta_j,\theta_j) + \sum_{i=0}^{j-1} n(\beta_i,\theta_i) \tag{80}$$

$$\geq \exp\bigl(50\log^2(m)d_j^2\bigr)n(\theta_j,1) + \sum_{i=0}^{j-1} n(\beta_i,\theta_i) \tag{81}$$

$$\geq \exp\left(50\log^2(m)\sum_i d_i^2\right). \tag{82}$$

Going to the second line we use Lemma 32, and to get to the third line we use the fact that the interval from θ_j to 1 contains all of the previous intervals, and the definition of n. ◀

▶ **Lemma 34.** *If $n(2/3,1) \geq 1$, then $N \leq \log(m)$.*

Proof. In order to prove the claim, we show by induction that for all j, $\sum_{i=0}^{j} n(\beta_i,\theta_i) \geq 2^j$. By assumption the assumption that $n(2/3,1) \geq 1$ and Lemma 32, we have that $n(\beta_0,\theta_0) \geq 1$. Now assume that $\sum_{i=0}^{j-1} n(\beta_i,\theta_i) \geq 2^{j-1}$. By Lemma 32, for every j, $n(\beta_j,\theta_j) \geq n(\theta_j,1) \geq \sum_{i=0}^{j-1} n(\beta_i,\theta_i)$. So, we have that

$$\sum_{i=0}^{j} n(\beta_i,\theta_i) \geq 2\sum_{i=0}^{j-1} n(\beta_i,\theta_i) \geq 2^j. \tag{83}$$

Because we have m measurements in total, we must have that $N \leq \log(m)$. ◀

▶ **Lemma 35.** *Assume that $n(\theta,1) \geq 1$. Then the set of bad thresholds has measure less than* $1/6$.

Proof. By definition, every bad threshold is contained in some interval $[\beta_i,\theta_i]$, so to upper bound the measure of bad thresholds, it suffices to upper bound $\sum_i^N d_i$, given that the sum of their squares is upper bounded by $1/50\log(m)$ (from Lemma 33) and $N \leq \log(m)$ (from Lemma 34). The best value one can achieve for this optimization problem occurs when $N = \log(m)$ and $d_1 = d_2 = \ldots = d_N = \sqrt{1/50\log^2(m)}$. Computing the sum of d_i, we get that the measure of bad thresholds is upper bounded by $\sum_i^N d_i \leq \log(m)\sqrt{1/50\log^2(m)} = \sqrt{1/50} \leq 1/6$ This completes the proof. ◀

Before proving that the theorem works, we show that a measurement not being bad implies a lower bound for the value of γ. This implies that if the algorithm chooses a good threshold, it has a constant success probability for the threshold search problem.

▷ Claim 36. If $\gamma_\theta < 1/32$, then θ is bad.

Proof. Letting $n = 100 \log^2 m$, the following is a lower bound for γ by definition

$$\frac{\sum_{i \in \mathcal{M}[\theta,1]} \mathrm{Tr}[\mathsf{B}(M_i, n, \theta)\rho^{\otimes n}]^2}{\sum_i \mathrm{Tr}[\mathsf{B}(M_i, n, \theta)\rho^{\otimes n}]} \le \gamma \le 1/32 \,.$$

The denominator can be re-written as the sum over $\mathcal{M}[\theta, 1]$ and $\mathcal{M}[0, \theta]$. Doing this and rearranging terms, we get that

$$\begin{aligned}\frac{1}{32} &\sum_{i \in \mathcal{M}[0,\theta]} \mathrm{Tr}\big[\mathsf{B}(M_i, n, \theta)\rho^{\otimes n}\big] \\ &\ge \sum_{i \in \mathcal{M}[\theta,1]} \mathrm{Tr}\big[\mathsf{B}(M_i, n, \theta)\rho^{\otimes n}\big]^2 - \frac{1}{32} \sum_{i \in \mathcal{M}[\theta,1]} \mathrm{Tr}\big[\mathsf{B}(M_i, n, \theta)\rho^{\otimes n}\big] \,. \end{aligned} \tag{84}$$

Using the fact that for all indices $i \in \mathcal{M}[\theta, 1]$, we have that $1/2 \le \mathrm{Tr}\big[\mathsf{B}(M_i, n, \theta)\rho^{\otimes k}\big] \le 1$, so the first term on the right side is greater than $n(\theta, 1)/4$, and the second term is less than $n(\theta, 1)/32$, we get the following

$$\frac{1}{32} \sum_{i \in \mathcal{M}[0,\theta]} \mathrm{Tr}\big[\mathsf{B}(M_i, n, \theta)\rho^{\otimes n}\big] \ge \frac{7}{32} n(\theta, 1) \,. \tag{85}$$

Finally, by the Chernoff bound on the binomial distribution, setting $k = 100 \log^2 m$ this is a lower bound the left hand side of Equation (70), showing that θ is bad. ◁

Note that the contrapositive of the previous claim is that if θ is good, then it must be that $\gamma_\theta \ge 1/32$. Now we prove that the blended measurement threshold search solves threshold search.

▶ **Theorem 37** (Blended Measurement Threshold Search). *Let $\mathcal{M}$ be a set of measurements and ρ be an unknown quantum state. Assume that there is a measurement in $\mathcal{M}$ satisfying $\mathrm{Tr}[M_i \rho] \ge 3/4$. Then blended measurement threshold search (Algorithm 3) returns a measurement satisfying $\mathrm{Tr}[M_i \rho] \ge 1/3$ with constant probability.*

Proof. By assumption, there exists at least one measurement satisfying $\mathrm{Tr}[M_i \rho] \ge 3/4$, so by Lemma 35, the algorithm selects a good threshold with probability at least $1/5 - 1/6 = 1/30$. If a good threshold is chosen, then $\gamma_\theta \ge 1/32$ from the previous claim. By the strong event finding lemma (Lemma 28), and Lemma 31, the probability that the algorithm outputs a measurement satisfying $\mathrm{Tr}[M_i \rho] \ge 1/3$, conditioned on selecting a good threshold, is lower bounded by $\frac{\gamma^3}{16} - \frac{1}{m} \ge \frac{1}{32000}$, for a suitably large choice of m. Putting these two together, blended measurement threshold search succeeds in finding a measurement with high accepting probability with probability at least 10^{-6}, which is a constant in m. ◀

6.3 Threshold Search via Repeated Random Measurements

In Section 6.2, we showed that picking a threshold value to boost around uniformly at random is "good" with constant probability. Leveraging those results, we can prove a sequence of random measurements also succeeds in performing threshold search. Consider the following random measurement version of Algorithm 3:

The lower bound on γ and the strong event finding lemma for repeated random measurements hold, so all that remains to be seen is that a constant lower bound on $\widetilde{\gamma}$ implies a constant success probability.

Algorithm 4 Random Measurement Threshold Search.

Input: A classical description of a set of two outcome measurements $\mathcal{M} = \{M_1, M_2, \ldots, M_m\}$ and $n = 100 \log^2 m$ copies of an unknown state ρ.

Output: Measurement M_i or REJECT.

1. Select a random $\theta \in [2/5, 3/5]$.
2. Repeat m times:
   a. Pick a random measurement $M_i \in \mathcal{M}$.
   b. Perform the measurement $\mathsf{B}(M_i, n, \theta)$ on the current state. If the measurement accepts, output M_i.
3. Return REJECT.

▶ **Lemma 38.** *Fix a choice of threshold θ, let $\widetilde{\gamma}$ be defined as in Equation* (66) *with respect to $\mathsf{B}(\mathcal{M}, n, \theta)$. Then if there exists a constant c satisfying $\widetilde{\gamma} \geq c$, then Algorithm 4 outputs a measurement satisfying* $\mathrm{Tr}[M_i \rho] \geq 1/3$ *with probability at least $c - 1/m$.*

Proof. Omitted as it follows closely the proof of Lemma 31. See extended version for details. ◀

▶ **Theorem 39** (Random Measurement Threshold Search)**.** *Let $\mathcal{M}$ be a set of projective measurements and ρ be an unknown quantum state. Assume that there is a measurement in $\mathcal{M}$ satisfying* $\mathrm{Tr}[M_i \rho] \geq 3/4$*. Then random measurement threshold search (Algorithm 4) returns a measurement satisfying* $\mathrm{Tr}[M_i \rho] \geq 1/3$ *with constant probability.*

Proof. Follows from Lemma 38 and Lemma 35, mirroring Theorem 37. ◀

References

1 Scott Aaronson. Limitations of quantum advice and one-way communication. In *Proceedings. 19th IEEE Annual Conference on Computational Complexity, 2004.*, pages 320–332. IEEE, 2004.

2 Scott Aaronson. Qma/qpoly/spl sube/pspace/poly: de-merlinizing quantum protocols. In *21st Annual IEEE Conference on Computational Complexity (CCC'06)*, pages 13–pp. IEEE, 2006.

3 Scott Aaronson. Shadow tomography of quantum states. *SIAM Journal on Computing*, 49(5):STOC18–368, 2019.

4 Scott Aaronson and Guy N Rothblum. Gentle measurement of quantum states and differential privacy. In *Proceedings of the 51st Annual ACM SIGACT Symposium on Theory of Computing*, pages 322–333, 2019.

5 Costin Bădescu and Ryan O'Donnell. Improved quantum data analysis. In *Proceedings of the 53rd Annual ACM SIGACT Symposium on Theory of Computing*, STOC 2021, pages 1398–1411, New York, NY, USA, 2021. Association for Computing Machinery. `doi:10.1145/3406325.3451109`.

6 Jingliang Gao. Quantum union bounds for sequential projective measurements. *Physical Review A*, 92(5):052331, 2015.

7 Aram W Harrow, Cedric Yen-Yu Lin, and Ashley Montanaro. Sequential measurements, disturbance and property testing. In *Proceedings of the Twenty-Eighth Annual ACM-SIAM Symposium on Discrete Algorithms*, pages 1598–1611. SIAM, 2017.

8 Hsin-Yuan Huang, Richard Kueng, and John Preskill. Predicting many properties of a quantum system from very few measurements. *arXiv preprint*, 2020. `arXiv:2002.08953`.

9 B Kaulakys and V Gontis. Quantum anti-zeno effect. *Physical Review A*, 56(2):1131, 1997.

10 Samad Khabbazi Oskouei, Stefano Mancini, and Mark M Wilde. Union bound for quantum information processing. *Proceedings of the Royal Society A*, 475(2221):20180612, 2019.

11 A. Uhlmann. The "transition probability" in the state space of a $*$-algebra. *Reports on Mathematical Physics*, 9(2):273–279, 1976. doi:10.1016/0034-4877(76)90060-4.

12 Mark M Wilde. *Quantum information theory.* Cambridge University Press, 2013.

13 Andreas Winter. Coding theorem and strong converse for quantum channels. *IEEE Transactions on Information Theory*, 45(7):2481–2485, 1999.