Proceedings of Machine Learning Research vol 291:1–59, 2025 38th Annual Conference on Learning Theory

Quantum State and Unitary Learning Implies Circuit Lower Bounds

Nai-Hui Chia NC67@RICE.EDU
Rice University

Daniel Liang DANLIANG@PDX.EDU
Rice University and Portland State University

Fang Song FSONG@PDX.EDU
Portland State University

Editors: Nika Haghtalab and Ankur Moitra

Abstract

We establish connections between state tomography, pseudorandomness, quantum state synthesis, and circuit lower bounds. In particular, let $\mathfrak{C}$ be a family of non-uniform quantum circuits of polynomial size and suppose that there exists an algorithm that, given copies of $|\psi\rangle$, distinguishes whether $|\psi\rangle$ is produced by $\mathfrak{C}$ or is Haar random, promised one of these is the case. For arbitrary fixed constant c, we show that if the algorithm uses at most $O\left(2^{n^c}\right)$ time and $2^{n^{0.99}}$ samples then $\mathsf{stateBQE} \not\subset \mathsf{state}\mathfrak{C}$. Here $\mathsf{stateBQE} := \mathsf{stateBQTIME}\left[2^{O(n)}\right]$ and $\mathsf{state}\mathfrak{C}$ are state synthesis complexity classes as introduced by Rosenthal and Yuen (2022), which capture problems with classical inputs but quantum output. Note that efficient tomography implies a similarly efficient distinguishing algorithm against Haar random states, even for nearly exponential-time algorithms. Because every state produced by a polynomial-size circuit can be learned with $2^{O(n)}$ samples and time, or $\omega(\mathrm{poly}(n))$ samples and $2^{\omega(\mathrm{poly}(n))}$ time, we show that even slightly non-trivial quantum state tomography algorithms would lead to new statements about quantum state synthesis. Finally, a slight modification of our proof shows that distinguishing algorithms for quantum states can imply circuit lower bounds for decision problems as well. We then take these results and port them over to the setting of unitary learning and unitary synthesis. All combined, this helps shed light on why time-efficient tomography algorithms for non-uniform quantum circuit classes has only had limited and partial progress.

Our work extends the results of Arunachalam et al. (2022b), which revealed a connection between quantum learning of *Boolean functions* and circuit lower bounds for *classical* circuit classes, to the setting of state (resp. unitary) tomography and state (resp. unitary) synthesis. As a result, we establish a conditional pseudorandom state (resp. unitary) generator, a circuit size hierarchy theorems for non-uniform state (resp. unitary) synthesis, and connections between state (resp. unitary) synthesis class separations and decision class separations, which may be of independent interest.

Keywords: quantum learning, tomography, circuit complexity, computational complexity

1. Introduction

Quantum state tomography is the task of constructing an accurate classical description of an unknown quantum state given copies of said unknown state, and is the quantum generalization of learning a probability distribution given access to samples from said distribution. Dating back to the 1950s (Fano, 1957), it has become a fundamental problem in quantum information that has numerous applications in verification of quantum experiments and the like (Mauro D'Ariano et al., 2003; Banaszek et al., 2013).

However, for general quantum states this becomes a famously expensive task (O'Donnell and Wright, 2016; Haah et al., 2017; Chen et al., 2023) and requires $\Omega(2^n)$ samples even for pure states (Bruß and Macchiavello, 1999). As such, major attention has been placed on performing efficient tomography for specific classes of quantum states, such as stabilizer states (Aaronson and Gottesman, 2008; Montanaro, 2017) (and some of their generalizations (Lai and Cheng, 2022; Grewal et al., 2023a; Leone et al., 2023; Hangleiter and Gullans, 2023; Chia et al., 2023; Grewal et al., 2023b)), non-interacting fermion states (Aaronson and Grewal, 2023), matrix product states (Landon-Cardinal et al., 2010), and low-degree phase states (Arunachalam et al., 2022a).

However, the class of states produced by low-complexity circuits has remained particularly challenging. Informally, we define low-complexity circuits to have depth or number of gates that cannot be too large. For instance, only recently do we have an efficient algorithm for learning the output of states produced by polynomial-size constant-depth unitary circuits of 2-local gates (i.e., QNC^0), but with the strong restriction that their connectivity must lie on a finite dimensional lattice (Huang et al., 2024; Landau and Liu, 2024). Likewise, only recently do we have a *quasi-poly sample* algorithm for learning the *Choi* states produced by constant-depth unitary circuits with both 2-local gates and n-ary Toffoli gates (i.e., Choi states of QAC^0 circuits), with the runtime still exponential in the number of qubits (Nadimpalli et al., 2024; Bao and Escudero-Gutiérrez, 2025), with a strong restriction on the number of ancilla qubits allowed ($O(n^{1/d})$ where d is the depth) and that there is only one qubit of output. Only when the number of ancilla is logarithmic do we have a quasi-poly *time* algorithm that recovers a description of the unitary (Vasconcelos and Huang, 2024).

In contrast to these quantum results, NC^0 is trivially easy to Probably Approximately Correct (PAC) learn and AC^0 has a quasi-poly *time* (uniform distribution) PAC learning algorithm (Linial et al., 1993).[1] See (Kearns and Vazirani, 1994; Hanneke, 2016) for details on the PAC learning model.

Lower bounds for non-uniform circuit classes have been similarly challenging in the world of computational complexity theory. The best known circuit lower bounds for explicit functions follow from Kumar (2023), which holds for a class of circuits in-between AC^0 and TC^0. Meanwhile, the breakthrough results of Williams (2014, 2018); Murray and Williams (2020) showed that non-deterministic quasi-poly time (i.e., $\mathsf{NTIME}\left[n^{\log^{O(1)} n}\right]$) cannot be expressed as quasi-poly-size ACC^0 circuits (or even ACC^0 with a bottom layer of threshold gates), where ACC^0 is another class that sits between AC^0 and TC^0. In both of these cases, TC^0 remains a major roadblock for proving circuit lower bounds.

In this work, we relate the hardness of learning low-depth quantum circuit classes to lower bounds for non-uniform state synthesis. Specifically, let $\mathfrak{C}$ refer to a class of non-uniform polynomial-size quantum circuits. We relate the difficulty of giving learning algorithms for states produced by $\mathfrak{C}$ to lower bounds for the set of quantum states that $\mathfrak{C}$ can produce. This is done through the language of state synthesis complexity classes, such as $\mathsf{stateBQP}, \mathsf{statePSPACE}, \mathsf{state}\mathfrak{C}$, etc., which were introduced in a series of recent work (Rosenthal and Yuen, 2022; Metger and Yuen, 2023; Delavenne et al., 2023; Bostanci et al., 2023; Rosenthal, 2024). While the standard decision problem complexity classes capture problems with classical input and classical output (even for quantum models of computations), these state synthesis complexity classes attempt to capture the complexity of problems with classical inputs and quantum outputs. Despite their differences, these

1. The uniform distribution setting for learning AC^0 somewhat matches the Frobenius distance measure used in the QAC^0 learning algorithms, as that is characterized by the average Trace Distance when fed a Haar random input state.

state synthesis complexity classes seem to (and, in many cases, are *designed to*) mirror the usual decision classes, such as in the case of $\mathsf{statePSPACE} = \mathsf{stateQIP}$ (Rosenthal and Yuen, 2022; Metger and Yuen, 2023; Rosenthal, 2024). We also generalize these results by relating the complexity of state tomography to circuit lower bounds for decision problems (Theorem 3), as well as relating the complexity of process tomography to circuit lower bounds for unitary synthesis (Theorem 4). We hope that future work will both further explore the relationship between learning and lower bounds against non-uniform circuits, as well instantiate this relationship to give useful and novel lower bounds.

We now informally state our main result about state synthesis. We show that the existence of a sufficiently efficient (in both time and samples) learner for states produced by a circuit class $\mathfrak{C}$ implies that, for every $k \geq 1$, there exists a sequence of pure states $(|\psi_x\rangle)_{x\in\{0,1\}^*}$ that can be synthesized to arbitrary inverse-exponential accuracy by a uniform quantum algorithm in time $2^{O(n)}$ but not by non-uniform $\mathfrak{C}$ circuits of size at most $O(n^k)$.

Theorem 1 (Informal statement of Corollary 67) *Let $\mathfrak{C}$ be a class of non-uniform quantum circuits. Suppose that for some fixed constant c, states produced by $\mathfrak{C}$ could be learned to constant precision (in trace distance) and constant success probability using no more than $O\left(2^{n^c}\right)$ time and $2^{n^{0.99}}$ many samples. Then, for every $k \geq 1$, there exists a state sequence in $\mathsf{stateBQE}$ that cannot be synthesized by non-uniform $\mathfrak{C}$ circuits of size at most n^k.*[2]

Note that any class of pure states can be learned in $2^{\Theta(n)}$ time and samples by running general pure state tomography (França et al., 2021). Furthermore, a counting argument (see Corollary 58) and classical shadows (Huang et al., 2020) allows one to use $\omega(\text{poly}(n))$ samples instead, at the cost of $2^{\omega(\text{poly}(n))}$ time. Thus, even slightly non-trivial learning algorithms would imply state synthesis lower bounds for $\mathfrak{C}$.

More carefully, we actually show that non-trivial *distinguishing* of pure states produced by $\mathfrak{C}$ from Haar random states either separates $\mathsf{stateBQE}$ from $\mathsf{state}\mathfrak{C}$ or separates $\mathsf{stateBQSUBEXP} := \bigcap_{\gamma\in(0,1)} \mathsf{stateBQTIME}\left[2^{n^\gamma}\right]$ from all polynomial-size circuits from 1 and 2-qubit quantum gates (i.e., $\mathsf{BQSIZE}[n^k]$). This distinguishing task is generally a much easier task to do than tomography (see Section 1.3 for a discussion of this), making the result all the more striking. In particular, we show that even a $\frac{1}{2^{n^{0.99}}}$ advantage in distinguishing a state from $\mathfrak{C}$ from Haar random, while using at most $2^{n^{0.99}}$ samples and $O\left(2^{n^c}\right)$ time gives interesting and novel lower bounds for state synthesis.

Theorem 2 (Informal statement of Corollary 66) *Let $\mathfrak{C}$ be a class of non-uniform quantum circuits. Suppose for some fixed constant c that there exists an algorithm that can distinguish states produced by $\mathfrak{C}$ from Haar random states, with at least $\frac{1}{2} + \frac{1}{2^{n^{0.99}}}$ success probability, using no more than $O\left(2^{n^c}\right)$ time and $2^{n^{0.99}}$ many samples. Then at least one of the following is true:*

- *For every $k \geq 1$, there exists a state sequence in $\mathsf{stateBQSUBEXP}$ that cannot be synthesized by non-uniform quantum circuits of arbitrary 1 and 2 qubit gates of size at most $O(n^k)$,*
- *There exists a state sequence in $\mathsf{stateBQE}$ that cannot be synthesized by polynomial size $\mathfrak{C}$ circuits (i.e., $\mathsf{stateBQE} \not\subset \mathsf{state}\mathfrak{C}$).*

2. We define $\mathsf{BQE} = \mathsf{BQTIME}\left[2^n\right]$ to be algorithms that run in strictly $2^{O(n)}$ time, rather than $2^{\text{poly}(n)}$, which is how BQEXP is defined.

The only restriction on the circuit class is that (1) all states produced by $\mathfrak{C}$ circuits of size at most s be approximated to 0.49 in trace distance to states produced by non-uniform circuits of size $\mathrm{poly}(s)$ in the commonly used $\{H, \mathrm{CNOT}, T\}$ gate set and (2) the circuits do not somehow get 'weaker' when the input size increases such that if $|\psi\rangle$ is a quantum state that can be efficiently synthesized in terms of input size n, then $|\psi\rangle$ can also be synthesized on inputs of size greater than n. This is a very weak set of restrictions and includes a wide variety of circuit classes, such as circuits of bounded depth (such as QNC), circuits with bounded locality, circuits with non-standard gate sets (such as QAC^0_f), circuits with bounds on the how many times a particular gate can be used (such as the T gate count in the Clifford + T model), etc. Here QAC^0_f is defined as constant-depth unitary circuits with both 2-local gates, n-ary Toffoli gates, and the additional *fanout* gate, a unitary that allows parallel *classical* copying of a single qubit to many output qubits.[3] This mimics the power of classical circuits to have *unbounded* fanout, whereas the laws of quantum mechanics do not permit the cloning of quantum data. In this way, the fanout gate ensures that $\mathsf{AC}^0 \subset \mathsf{QAC}^0_f$, whereas it is unknown if $\mathsf{AC}^0 \subset \mathsf{QAC}^0$. The addition of the fanout gate even implies $\mathsf{TC}^0 \subset \mathsf{QAC}^0_f$ (Hoyer and Spalek, 2005; Takahashi and Seiichiro, 2016).

We remark that, while both conclusions of Theorem 2 are plausible, showing this is another matter. If the intuition that state synthesis complexity classes mirror their decision problem counterparts, formally proving these separations would be highly non-trivial. Interestingly, when the circuit class in question contains QAC^0_f, we can somewhat formalize this connection and show that distinguishing would *also* imply breakthrough circuit lower bounds for the traditional setting of decision problems. As such, it illustrates how problems purely about state synthesis and state distinguishing can have breakthrough consequences for the traditional model of complexity theory.

Theorem 3 (Informal statement of Theorem 72) *Let $\mathfrak{C} \supseteq \mathsf{QAC}^0_f$ be a class of non-uniform quantum circuits. Suppose that there exists a fixed constant c such that states produced by $\mathfrak{C}$-circuits of depth at most $d+3$ could be distinguished from Haar random states, with at least $\frac{1}{2} + \frac{1}{2^{n^{0.99}}}$ success probability, using no more than $O\left(2^{n^c}\right)$ time and $2^{n^{0.99}}$ many samples. Then at least one of the following is true:*

- *For every $k \geq 1$, there exists a language in $\mathsf{BQSUBEXP}$ that cannot be decided by non-uniform quantum circuits of arbitrary 1 and 2 qubit gates of size at most $O(n^k)$,*
- *There exists a language in E that cannot be decided to bounded error by $\mathfrak{C}$ circuits of depth at most d (i.e., $\mathsf{E} \not\subset$ (depth d)-$\mathfrak{C}$).*[4]

This follows as a combination of the proof of Theorem 2 along with ideas from Arunachalam et al. (2022b) and Chia et al. (2022). We remark that Theorems 1 and 2 (as well as Theorem 4) preserve the fine-grained depth of $\mathfrak{C}$ exactly, unlike Theorem 3, which only preserves it up to a constant. As an example, non-trivial distinguishing of states produced by depth 5 QAC^0_f circuits would imply $\mathsf{E} \not\subset$ (depth 2)-$\mathsf{QAC}^0_\mathsf{f}$ as the second possible scenario in Theorems 2 and 3.

As a result of Theorems 1, 2 and 3, it would seem unlikely to prove formal learning results for states produced by non-uniform polynomial-size quantum circuits given the difficulty that surrounds

3. Think of the CNOT gate as *classical* copying of a single qubit to a single output qubit. The fanout gate is multiple CNOT with the same target qubit being applied as a single action.

4. As is usually the case in complexity theory, we abuse notation and also refer to the set of languages that can be decided by circuits in $\mathfrak{C}$ as $\mathfrak{C}$ as well. We also take $\mathsf{E} \coloneqq \mathsf{DTIME}\left[2^{O(n)}\right]$.

non-uniform circuit lower bounds. A more optimistic view would indicate that this illuminates a possible plan of attack for showing state synthesis separation against non-uniform models of computation.

Finally, we show that the ability to distinguish *unitaries* produced by $\mathfrak{C}$ circuits of size n^k implies circuit lower bounds for *unitary synthesis*. Unitary complexity classes consider an even broader class of problems with quantum outputs (Metger and Yuen, 2023; Bostanci et al., 2023).

Theorem 4 (Informal statement of Theorem 89) *Let $\mathfrak{C}$ be a class of non-uniform quantum circuits. Suppose that there exists a fixed constant c such that unitaries produced by $\mathfrak{C}$ could be distinguished from Haar random unitaries with $\frac{1}{2^{n^{0.99}}}$ success probability, using no more than $O\left(2^{n^c}\right)$ time and $2^{n^{0.99}}$ many queries. Then, at least one of the following is true:*

- *For every $k \geq 1$, there exists a unitary sequence in* $\mathsf{unitaryBQSUBEXP}$ *that cannot be synthesized by non-uniform quantum circuits of arbitrary 1 and 2 qubit gates of size at most $O(n^k)$,*
- *There exists a unitary sequence in* $\mathsf{unitaryBQE}$ *that cannot be synthesized by polynomial size $\mathfrak{C}$ circuits (i.e.,* $\mathsf{unitaryBQE} \not\subset \mathsf{unitary}\mathfrak{C}$*).*

This is a consequence of recent results on pseudorandom unitaries by Metger et al. (2024) and follow-up work by Ma and Huang (2024); Schuster et al. (2025) to show that the construction is secure against adaptivity, as well as inverse queries.

We likewise show that unitary learning can also lead to separations for decision problem.

Theorem 5 (Informal statement of Theorem 95) *Let $\mathfrak{C} \supseteq \mathsf{QAC}^0_f$ be a class of non-uniform quantum circuits. Suppose that there exists a fixed constant c such that unitaries produced by $\mathfrak{C}$-circuits could be distinguished from Haar random unitaries, with at least $\frac{1}{2} + \frac{1}{2^{n^{0.99}}}$ success probability, using no more than $O\left(2^{n^c}\right)$ time and $2^{n^{0.99}}$ many queries. Then at least one of the following is true:*

- *For every $k \geq 1$, there exists a language in* $\mathsf{BQSUBEXP}$ *that cannot be decided by non-uniform quantum circuits of arbitrary 1 and 2 qubit gates of size at most $O(n^k)$,*
- *There exists a language in* E *that cannot be decided to bounded error by $\mathfrak{C}$ circuits.*

Because distinguishing a unitary from Haar random is strictly easier than distinguishing a state from Haar random, this gives us an even more powerful approach to proving circuit lower bounds. However, we lose the fine-grained relationship with depth that Theorem 72 has.

1.1. Proof Techniques

1.1.1. LEARNING BOOLEAN FUNCTIONS IMPLIES CIRCUIT LOWER BOUNDS

We model our proof of Theorem 1 heavily after the work of Arunachalam et al. (2022b), which examined the relationship of quantum learning of Boolean functions with separations between BQE and circuit lower bounds. This was itself a generalization of a line of works for *classical* learning of Boolean functions (Fortnow and Klivans, 2009; Harkins and Hitchcock, 2013; Klivans et al., 2013; Volkovich, 2014, 2016; Oliveira and Santhanam, 2017, 2018). Let $\mathfrak{C}[s]$ denote circuits from $\mathfrak{C}$ of size at most $O(s)$. Informally, Arunachalam et al. (2022b, Theorem 3.7) states that sufficiently efficient learning algorithms for boolean functions implemented by $O(n^k)$-size *classical* circuit class $\mathfrak{C}$ implies that $\mathsf{BQE} \not\subset \mathfrak{C}[n^k]$. The high-level of their proof works as follows:

1. Assume there exists a Pseudorandom Generator (PRG) that is secure against sub-exponential-time uniform *quantum* adversaries that can also be computed in $2^{O(n)}$ time.
2. Create a language $L \in \mathsf{BQE}$ that requires being able to compute the PRG.
3. Show that a sufficiently efficient learner for $\mathfrak{C}$ implies that no sub-exponential-secure PRG can be computed by $\mathfrak{C}$.
4. Conclude that $L \notin \mathfrak{C}$.

Unfortunately, this proof also has the added condition of this PRG existing, and no unconditional PRGs with even close to that security guarantee are known exist. As is the case in many predecessor works, Arunachalam et al. (2022b) uses a win-win argument to get around this. The two cases depend on the relationship between PSPACE being 'a subset of' or 'not a subset of' $\mathsf{BQSUBEXP} = \bigcap_{\gamma\in(0,1)} \mathsf{BQTIME}\left[2^{n^\gamma}\right]$.

1. Unconditionally, for every $k \geq 1$, $\mathsf{PSPACE} \not\subset \mathfrak{C}[n^k]$ via a diagonalization argument (Arunachalam et al., 2022b, Lemma 3.3).
2. Appeal to a win-win argument based on the relationship between PSPACE and $\mathsf{BQSUBEXP}$:
   - If $\mathsf{PSPACE} \subset \mathsf{BQSUBEXP}$ then, for every $k \geq 1$, $\mathsf{BQSUBEXP}$ and BQE can also diagonalize against $\mathfrak{C}[n^k]$.
   - If $\mathsf{PSPACE} \not\subset \mathsf{BQSUBEXP}$ then a PRG exists such that the above argument holds.
3. Observe that either way, for every $k \geq 1$, $\mathsf{BQE} \not\subset \mathfrak{C}[n^k]$.

1.1.2. HIGH-LEVEL PROOF FOR THEOREM 1

In our work, we follow a similar high-level path except where (1) $\mathfrak{C}$ now refers to a quantum circuit and (2) the PRG is replaced by a new, inherently quantum, pseudorandom object called a Pseudorandom State (PRS). This object was introduced by Ji et al. (2018) as a quantum analogue for PRGs and involves an ensemble of quantum *pure* states that are indistinguishable from a Haar random state by computationally bounded adversaries. Our win-win argument is then replaced by looking at the relationship of a variant of $\mathsf{statePSPACE}$, which we call $\mathsf{statePSPACESIZE}$ (see Definition 23), versus $\mathsf{stateBQSUBEXP}$.

In particular, when $\mathsf{statePSPACESIZE} \not\subset \mathsf{stateBQSUBEXP}$ then there exists a PRS that is secure against sub-exponential time uniform quantum adversaries that can also be synthesized in $2^{O(n)}$ time (i.e., is in $\mathsf{stateBQE}$). Conversely, a sufficiently efficient learning algorithm for states produced by $\mathfrak{C}$ implies that $\mathfrak{C}$ cannot synthesize *any* PRS that is sub-exponential-time-secure against uniform quantum adversaries.

On the other hand, when $\mathsf{statePSPACESIZE} \subset \mathsf{stateBQSUBEXP}$, we can similarly prove that, for all $k \geq 1$, $\mathsf{statePSPACESIZE} \not\subset \mathsf{state}\mathfrak{C}[n^k]$ to complete both sides of the win-win argument.

Despite the noticeable similarities between our proof and that of Arunachalam et al. (2022b), there are a number of differences that arise due to the difference in learning models as well as the change to state synthesis complexity classes. We highlight the effect of some of the most salient differences, as well as how we alter the proofs with respect to them.

Learning Implies Non-Pseudorandomness Learning and cryptography are natural antagonists of one another: learning implies lower bounds for constructing cryptographic objects and cryptographic objects imply hardness for learning. One of the key ingredients in both our proof as well as Arunachalam et al. (2022b) is utilizing this relationship to show that learning implies that certain complexity classes cannot contain pseudorandom objects. This was done previously via a quantum natural property, where classical natural properties also appeared in Volkovich (2014); Oliveira and Santhanam (2017). Without going into too much detail, a natural property against classical circuit class $\mathfrak{C}$ is an polynomial time (in the input size of $N = 2^n$) algorithm that acts on the truth table of a Boolean function and accepts with high probability for most random functions and instead rejects with high probability when given a truth table for a function in $\mathfrak{C}$.

In Section C we completely eschew the notion of natural properties, or any generalization of them. Instead, we utilize the fact that pseudorandom quantum states (PRS) always involve pure states. This means that a SWAP test can be performed to determine how close a mixed state ρ is to the pseudorandom state. By letting ρ be the output of a sub-exponential-time quantum learning algorithm for $\mathtt{state}\mathfrak{C}$ that takes m copies of the state, we can run the SWAP test on an extra copy to verify if our learning algorithm did a good job. By the definition of a learning algorithm, when given an (initially) unknown state that is in $\mathtt{state}\mathfrak{C}$ the SWAP test will accept with probability bounded away from $\frac{1}{2}$ by a non-negligible amount. On the other hand, when given a Haar random state, any sub-exponential-sample learning algorithm will fail to output a quantum state that is even remotely close to the sampled state. Thus the SWAP test will accept with probability at most $\frac{1}{2}+\exp(-n)$. We conclude that the two cases are distinguishable such that $\mathfrak{C}$ cannot synthesize any sub-exponential-sample-secure PRS.

Remark 6 *We emphasize that using a SWAP test for learning-to-distinguishing is certainly not a novel idea, but that we could not find an existing analysis in the literature that fit our purposes. For instance, a similar analysis was done in Zhao et al. (2023, Theorem 14, Theorem 15). However, it is not sufficient because the sample and time complexity of the algorithms they consider (as stated) are limited to* $\mathrm{poly}(n)$*, whereas we need our reduction to hold even when the learning algorithms use up to* $O\left(2^{n^{0.99}}\right)$ *samples and* $2^{\mathrm{poly}(n)}$ *time. Other benefits of Lemma 55 include (1) a much simpler proof, (2) tighter bounds (specifically in terms of time complexity), and (3) a fine-grained reduction from the parameters of the learning algorithm to the distinguishing algorithm. Likewise, the non-cloneability of pseudorandom states as shown by Ji et al. (2018, Theorem 2) is lossy in several ways. For instance, if the* cloning *algorithm uses* m *copies, then the distinguisher from Ji et al. (2018, Theorem 2) will use* $2m+1$ *copies, rather than the* $m+1$ *in Lemma 55. More importantly, to get a cloning algorithm from a learning algorithm, the learning algorithm will potentially (and, in fact, likely will) destroy all* m *copies via measurement. Therefore, to create the* $m+1$ *approximate copies of* $|\psi\rangle$ *necessary to call this an approximate cloning algorithm, we must produce* $|\widehat{\psi}\rangle^{\otimes m+1}$ *from scratch, where* $|\widehat{\psi}\rangle$ *is the output of the learning algorithm. It follows from the Fuchs-van de Graaf inequalities (see Corollary 13) that in order to get* ε*-approximate cloning, the trace distance between* $|\psi\rangle$ *and* $|\widehat{\psi}\rangle$ *needs to be at most* $\frac{\varepsilon}{\sqrt{m}}$*. Since* $m = O\left(2^{n^{0.99}}\right)$ *in our circumstances, this is incredibly lossy for all but the smallest values of* ε*.*

We note that, because the SWAP test only takes $O(n)$ time rather than $2^{O(n)}$ time like a natural property, we can break the security of a PRS with large amounts of samples and time, and also very small accuracy. Arunachalam et al. (2022b, Theorem 3.1) instead has a trade-off between time/samples and accuracy, where taking more time/samples requires the learning algorithm to get more accurate learning and vice-versa. Our approach also allows for achieving tighter bounds if the PRS constructions can be improved. See Section 1.3 for a discussion on this.

PRS from State Synthesis Separations Perhaps the most important technical contribution of Arunachalam et al. (2022b) is proving the existence of sub-exponential-secure PRG against uniform *quantum* adversaries given $\mathsf{PSPACE} \not\subset \mathsf{BQSUBEXP}$. For the win-win argument to go through, we now need a sub-exponential-secure PRS against uniform quantum computation given $\mathsf{statePSPACESIZE} \not\subset \mathsf{stateBQSUBEXP}$. To do this, we note that there are constructions of PRS given a quantum-secure *pseudorandom function* (PRF) (Ji et al., 2018; Brakerski and Shmueli, 2019; Aaronson et al., 2022; Giurgica-Tiron and Bouland, 2023; Jeronimo et al., 2024). Likewise, there exist quantum-secure PRF constructions when given a quantum-secure PRG (Goldreich et al., 1984; Zhandry, 2021). As such, we show in Section B the existence of a sub-exponential-secure PRS against uniform quantum computation given $\mathsf{PSPACE} \not\subset \mathsf{BQSUBEXP}$

Remark 7 *We need these constructions to retain the sub-exponential security of the underlying PRG to get a sub-exponential-secure PRS, whereas most analysis of these reductions only consider polynomial-time adversaries. This is more restrictive than it sounds. For instance, constructions such as random subset states (Giurgica-Tiron and Bouland, 2023; Jeronimo et al., 2024) are not known to be secure against sub-exponential-time adversaries. Additionally, because the PRG from Arunachalam et al. (2022b) requires $2^{\mathrm{poly}(n)}$ time to compute, the usual method of obtaining a quantum-secure PRF from a quantum-secure PRG (Goldreich et al., 1984; Zhandry, 2021) cannot be used. Finally, other constructions such as non-binary phase states (Ji et al., 2018) and random subset states with random phases (Aaronson et al., 2022) would not allow us to achieve Theorem 3, as they (to the author's knowledge) require super-constant depth in the construction even for QAC^0_f.*

While this is close to what we want, we still need a PRS conditional on $\mathsf{statePSPACESIZE} \not\subset \mathsf{stateBQSUBEXP}$, rather than their decision version counterparts. To bridge the gap, in Lemma 48 we show that $\mathsf{statePSPACESIZE} \not\subset \mathsf{stateBQSUBEXP}$ implies $\mathsf{PSPACE} \not\subset \mathsf{BQSUBEXP}$. This is done by defining a decision problem L based on a particular bit in the description of the separating circuit in $\mathsf{statePSPACESIZE}$. Therefore, if $L \in \mathsf{BQSUBEXP}$ then, by iterating over all bits in the description, the entire description can be learned. This is why we need to use $\mathsf{statePSPACESIZE}$, where the circuits always have polynomial size descriptions, as opposed to $\mathsf{statePSPACE}$, where the description could potentially have unbounded size. In this way, the entire circuit description can be learned bit-by-bit by a $\mathsf{BQSUBEXP}$ algorithm. Having the circuit description allows us to then synthesize the state, ultimately implying $\mathsf{statePSPACESIZE} \subset \mathsf{stateBQSUBEXP}$, which contradicts the initial assumption.

State Synthesis "Diagonalization" On the other side of the win-win argument, the proof of: for every $k \geq 1$, $\mathsf{PSPACE} \not\subset \mathfrak{C}[n^k]$ uses a diagonalization argument. At a high level, the strategy involves computing what the majority of some set of circuits in $\mathfrak{C}[n^k]$ do for a particular input and then outputting the opposite bit. By iterating over each element of the truth table, each new input cuts the number of $\mathfrak{C}[n^k]$ circuits that agree with the PSPACE algorithm by at least a half. Since there are only $2^{\mathrm{poly}(n)}$ circuits in $\mathfrak{C}[n^k]$ (since they are polynomial size), after about $\mathrm{poly}(n)$ entries in the truth table no circuits will agree.

Unfortunately, such a bit-flipping method does not apply to state synthesis, nor does it work against the notion of non-uniformity used in state synthesis (see Remark 25). For instance, there's no clear definition of what the "majority" state is for a given set of states.[5] Thus it's not clear how to perturb a state to make it disagree with many other states. Additionally, while bit strings (even when viewed as computational basis states) are "well-spaced", the set of quantum states produced by quantum circuits can be arbitrarily close to each other in trace distance. Thus even if the state is successfully perturbed, it might not even be appreciably far from the set of old states.

Nevertheless, we still need to show that a $\mathrm{poly}(n)$-space algorithm can find a quantum state that is ε-far from any state produced by a n^k-size quantum circuit for some fixed $k \in \mathbb{N}$. To do so, we utilize a result of Oszmaniec et al. (2024), which gives a lower bound for a quantity known as the packing number (see Definition 57) for circuits of bounded depth. Informally, the packing number is the maximal number of states that are ε-far from each other. Therefore, for sets of states $A \subset B$, if the packing number of A is strictly less than the packing number of B then some state in B is ε-far from all states in A.

Utilizing the above lower bound, as well as another counting argument, we establish a circuit-size hierarchy theorem for state synthesis in Section D.1. In particular, we prove that circuits of size $s' := \mathrm{poly}(s)$ can always create a state far away from anything in produced by size at most s. Finally, in Section D.2 we use the fact that trace distance can be approximated in $\mathrm{poly}(n)$-space (Watrous, 2002) to iterate through circuits of s'-size and find said state.

1.1.3. UNITARY SYNTHESIS SEPARATIONS FROM UNITARY DISTINGUISHING

The proof of Theorem 4 follows the same strategy as Theorem 2, but with the conditional PRS replaced by a conditional Pseudorandom Unitary (PRU) (Ji et al., 2018). Notably, we rely on the work of Ma and Huang (2024) to show the existence of a conditional strong PRU based on the PFC construction of Metger et al. (2024). Namely, we use the $CPFC'$ construction, where C and C' are independent random Cliffords, P is a (pseudo)random permutation matrix, and F is a diagonal matrix with (pseudo)random ± 1 entries is secure against adaptivity and inverse queries. Like with the PRS construction, care needs to be taken to ensure that the sub-exponential security is retained in these reductions.

1.1.4. TOMOGRAPHY IMPLIES CIRCUIT LOWER BOUNDS FOR DECISION PROBLEMS

The proof of Theorems 3 and 5 much more closely resembles Arunachalam et al. (2022b) as we are now dealing with decision problems. As such, the win-win argument now centers around PSPACE and BQSUBEXP. In a world where PSPACE $\subset$ BQSUBEXP, we note that BQSUBEXP can now diagonalize against general non-uniform quantum circuits (Chia et al., 2022).[6] Conversely, when PSPACE $\not\subset$ BQSUBEXP then we use the argument of Arunachalam et al. (2022b) to construct a language L that is in BQE and defines a pseudorandom function. Furthermore, if L was in (depth

5. Buhrman et al. (2023) is *not* applicable here, as we are not deciding between two pairs of orthogonal single-qubit quantum states, but rather a collection of n-qubit quantum states that has no restrictions to their pair-wise inner products.
6. We re-emphasize that the notion of non-uniformity differs between state synthesis and decision problems. Thus this result does *not* imply the work in Section 1.1.2.

d)-$\mathfrak{C}$ then (depth $d+3$)-$\mathfrak{C}$ could create a PRS, which is contradicted by an assumed existence of a learning algorithm for states. This implies $L \notin (\text{depth } d) - \mathfrak{C}$.

To achieve a similar result for Unitaries with Theorem 5, we need to work with a more depth-efficient strong PRU construction. That is, even with a PRG/PRF that is computable by $\mathfrak{C}$, the only known quantum-secure pseudorandom permutations seem to require polynomial depth (Zhandry, 2016) even for more powerful circuit classes like QAC. To get around this technical barrier, we use further follow-up work of Schuster et al. (2025) by replacing the (pseudo)random permutation with a 2-round Feistel network so that the PRU can be implemented in constant QAC^0_f depth. This allows us to use our quantum-secure pseudorandom function that, if it could be computed by $\mathfrak{C} \supseteq \mathsf{QAC}^0_f$, would be able to be transformed into a quantum-secure strong PRU that can be synthesized by $\mathsf{unitaryQAC}^0_f$. Unlike Theorem 3, the depth increase of this transformation is some large constant.

1.2. Related Work

Despite our work largely paralleling the proof techniques of Arunachalam et al. (2022b), we note that our result and theirs are not directly comparable. In their model, the learning is given access to an oracle that implements a Boolean function $f : \{0,1\}^n \to \{0,1\}$. The learner then needs to output a single-qubit-output quantum process C_f such that

$$\mathop{\mathbf{E}}_{x\sim\{0,1\}^n}\left[\operatorname{tr}\left(|f(x)\rangle\langle f(x)| \cdot C_f\left(|x\rangle\langle x|\right)\right)\right]$$

is large. This makes their model a restricted form of unitary learning where the unitary must have strictly diagonal entries. The circuit classes they deal with are also strictly classical.

Additionally, Zhao et al. (2023) recently used the fact that $\mathsf{TC}^0 \subset \mathsf{QNC}$ to show that learning QNC circuits is as hard as a variant of Learning with Errors, which can be encoded into a TC^0 circuit (Banerjee et al., 2012; Arunachalam et al., 2021).[7] While the hardness of Learning with Errors is certainly not only plausible but currently widely-believed, it could only be super-polynomial hardness or just not hard at all. Our result complements their result by giving hardness without the need of any cryptographic assumptions. Put another way, in a world where an sub-exponential-time attack against Learning with Errors was possible, sufficiently non-trivial learning of QAC^0_f states could still imply interesting results.

Finally, Chia et al. (2022) made statements of similar flavors to Theorem 3 in the context of the Minimum Circuit Size Problem (MCSP) for quantum circuits. This is the problem of deciding if the truth table of a function requires a certain circuit size to compute. Our work is most relevant to their notion of State Minimum Circuit Size (SMCSP), for which there were no similar results.

1.3. Discussion and Open Questions

Distinguishing Without Learning One may note that, as per Theorems 2 and 3, that the only assumption really necessary for a lower bound is a *distinguisher* from Haar random and not a learner. While we show (in Lemma 55) that learning implies distinguishing to eventually achieve Theorem 1, there is the possibility of a distinguisher existing whereas a learning algorithm does not. For instance, at the time of writing this manuscript, Clifford + T circuits only up to $O(\log n)$ T gates can be efficiently learned (Grewal et al., 2023a; Leone et al., 2023; Hangleiter and Gullans, 2023;

7. Using $\mathsf{TC}^0 \subset \mathsf{QAC}^0_f \subset \mathsf{QNC}^1$ (Hoyer and Spalek, 2005; Takahashi and Seiichiro, 2016; Rosenthal, 2023) one can extend this result to hardness for logarithmic depth rather than just poly-logarithmic.

Chia et al., 2023; Grewal et al., 2023b), whereas up to n T gates can be distinguished from Haar random in polynomial time (Grewal et al., 2023c).

We remark that this is the opposite intuition of what's formally stated in Lemma 55, where the distinguisher is slower than the learner by a log factor. This is entirely a consequence of the log factors in Fact 19 needed to test the algorithm via the SWAP test with only black-box access to the learning algorithm. However, in an informal sense, learning should actually be *harder* than distinguishing. Thus, it is usually the case that a learner can be turned into a distinguisher that runs as fast as (or oftentimes, even faster than) the learning algorithm by not using the SWAP test approach, but rather the underlying structure of the state it is trying to learn.

Faster PRS Gives Better Circuit Lower Bounds In this work, we show that a sufficiently efficient learning/distinguishing algorithm for states prepared by $\mathsf{state}\mathfrak{C}$ implies new circuit lower bounds for state synthesis (or decision problems resp.). This bound holds regardless of how efficient the learning algorithm is, as long as it is more efficient than a certain threshold. However, it would be great if a poly-time (or quasi-poly) learning algorithm implied a stronger lower bound, such as $\mathsf{pureStateBQP}_{\exp} \not\subset \mathsf{pureState}\mathfrak{C}_{\exp}$.[8]

The major technical roadblock is the construction of a PRS against uniform quantum computations that can be computed more efficiently than $O(2^{\kappa})$, where κ is the key length (see Definition 37). In turn, we don't need the PRS to be as secure, since we have assumed a much faster algorithm for distinguishing. For instance, suppose the underlying PRG (see Lemma 45) could be computed in time $O(f(\kappa))$ for $f = o(2^{\kappa})$, but was only secure against polynomial time adversaries. This would imply that the PRS lies in $\mathsf{pureStateBQTIME}[f]_{\exp}$ instead, improving the lower bound.

A second approach would be to directly get a PRS from a state synthesis complexity theoretic assumption such as $\mathsf{pureStatePSPACESIZE}_{\delta} \not\subset \mathsf{stateBQTIME}[f]_{\delta+\varepsilon}$ without using a PRF or PRG as an intermediary. By the work of Kretschmer (2021); Kretschmer et al. (2023, 2024), there is evidence to believe that a PRS may be possible in scenarios where a PRG/PRF (or quantum-secure OWF, more generally) is not. Both approaches are independently interesting and the proof techniques necessary would likely have many significant consequences.

Note that a unique benefit of using the SWAP test over something akin to a natural property (Razborov and Rudich, 1997), is that the learning-to-distinguishing (see Section 1.1.2) argument holds even when the parameters of the PRS are significantly altered. In contrast, the analogous results in Arunachalam et al. (2022b); Chia et al. (2022) require the security of the PRG to have nearly exponential stretch and the security to then be super-polynomial in the stretch (i.e., also nearly exponential).

Better Security Allows For Stronger Adversaries The parameters of the underlying PRG also affect the proof in other ways, such that improvements would affect different parameters in the statements of Theorems 1, 2 and 3. This is documented precisely in Lemma 64. For instance, if the PRG was secure against stronger adversaries, relative to the number of output bits, then the running time of the learning/distinguishing algorithms would increase accordingly. Quantitatively, if the number of output bits of the PRG is 2^{ℓ} (such that the PRS is on ℓ-qubits) and the security is $f(\ell)$, then the allowed running time of the distinguishing algorithm simply becomes $f(n)$. As $f(n)$ grows, the requirements to invoke our learning-to-circuit-lowerbound results becomes weaker, making this an appealing open direction.

8. $\mathsf{pureStateC}$ is the same as stateC but with a *pure* state sequence. See Section A.3 for details.

Finally, we note that in the proof of Lemma 40, one might naïvely hope to truncate the output of the PRG to artificially decrease the stretch relative to the security. This would make the security very big relative to the output bits, which, as pointed out above, allows for a learner with larger and larger amounts of time to still imply lower bounds. However, when the truncation is too great, Lemma 64 tells us that we will only be proving results about very small circuits. For instance, when the output of the PRG is truncated to a polynomial number of bits, we we will only be able to say things about poly-logarithmic size circuits.

Another way of seeing this is that, because the key length does not change, this will make the state synthesis about producing (or rather, not producing) pseudo-random states on a smaller and smaller number of qubits. From the point of view of a learning algorithm, the size of the quantum circuit that produces the state will be growing inversely relative to the truncation. Therefore, a learning algorithm allowed to run in time $2^{f(n)}$ in the number of qubits n will have to learn states produced by $\mathfrak{C}[\mathrm{poly}(f(n))]$, making the problem seemingly no more tractable if f grows super-polynomially. In fact, at a large enough growth of $f(n)$, $\mathfrak{C}[\mathrm{poly}\,(f(n))]$ may simply be able to produce state sequences that are *statistically* indistinguishable from Haar random, making the problem completely intractable.

Acknowledgments

We would like to thank William Kretschmer, Sabee Grewal, Vishnu Iyer, Shih-Han Hung, Srinivasan Arunachalam, Henry Yuen, Scott Aaronson, Kai-Min Chung, and Ruizhe Zhang for useful discussions and feedback. DL would also like to thank Igor Oliviera for helping fix bugs in the statement of the PRG in Lemma 45, Nick Hunter-Jones for helping with all of Section D.1, Gregory Rosenthal for helping with the name of statePSPACESIZE and aiding in the understanding of the results in Rosenthal (2024), Greg Kuperberg for helping understand the runtime of the Solovay-Kitaev algorithm, and Robert Huang and Fermi Ma for updates on their PRU analysis (Ma and Huang, 2024; Schuster et al., 2025). Part of this research was performed while DL was visiting the Institute for Pure and Applied Mathematics (IPAM), which is supported by the National Science Foundation (Grant No. DMS-1925919). DL is supported by the US NSF award FET-2243659 and CCF-2224131. FS is supported in part by the US NSF grants CCF-2054758 (CAREER) and CCF-2224131. NHC is supported by NSF Awards FET-2243659 and FET-2339116 (CAREER), Google Scholar Award, and DOE Quantum Testbed Finder Award DE-SC0024301.

References

Scott Aaronson and Daniel Gottesman. Improved Simulation of Stabilizer Circuits. *Physical Review A*, 70(5), 2004. doi: 10.1103/physreva.70.052328. URL https://doi.org/10.1103/physreva.70.052328.

Scott Aaronson and Daniel Gottesman. Identifying Stabilizer States, 2008. https://pirsa.org/08080052.

Scott Aaronson and Sabee Grewal. Efficient Tomography of Non-Interacting-Fermion States. In Omar Fawzi and Michael Walter, editors, *18th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC 2023)*, volume 266 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 12:1–12:18, Dagstuhl, Germany, 2023. Schloss Dagstuhl

– Leibniz-Zentrum für Informatik. ISBN 978-3-95977-283-9. doi: 10.4230/LIPIcs.TQC.2023.12.

Scott Aaronson, Adam Bouland, Bill Fefferman, Soumik Ghosh, Umesh Vazirani, Chenyi Zhang, and Zixin Zhou. Quantum Pseudoentanglement, 2022.

Noga Alon, Alexandr Andoni, Tali Kaufman, Kevin Matulef, Ronitt Rubinfeld, and Ning Xie. Testing k-wise and almost k-wise independence. In *Proceedings of the Thirty-Ninth Annual ACM Symposium on Theory of Computing*, STOC '07, page 496–505, New York, NY, USA, 2007. Association for Computing Machinery. ISBN 9781595936318. doi: 10.1145/1250790.1250863. URL https://doi.org/10.1145/1250790.1250863.

Srinivasan Arunachalam, Alex Bredariol Grilo, and Aarthi Sundaram. Quantum Hardness of Learning Shallow Classical Circuits. *SIAM Journal on Computing*, 50(3):972–1013, 2021. doi: 10.1137/20M1344202.

Srinivasan Arunachalam, Sergey Bravyi, Arkopal Dutt, and Theodore J. Yoder. Optimal algorithms for learning quantum phase states, 2022a.

Srinivasan Arunachalam, Alex B. Grilo, Tom Gur, Igor C. Oliveira, and Aarthi Sundaram. Quantum learning algorithms imply circuit lower bounds. In *2021 IEEE 62nd Annual Symposium on Foundations of Computer Science (FOCS)*, pages 562–573, 2022b. doi: 10.1109/FOCS52979.2021.00062.

K. Banaszek, M. Cramer, and D. Gross. Focus on quantum tomography. *New Journal of Physics*, 15 (12):125020, 2013. doi: 10.1088/1367-2630/15/12/125020. URL https://doi.org/10.1088/1367-2630/15/12/125020.

Abhishek Banerjee, Chris Peikert, and Alon Rosen. Pseudorandom functions and lattices. In David Pointcheval and Thomas Johansson, editors, *Advances in Cryptology – EUROCRYPT 2012*, pages 719–737, Berlin, Heidelberg, 2012. Springer Berlin Heidelberg. ISBN 978-3-642-29011-4.

Jinge Bao and Francisco Escudero-Gutiérrez. Learning junta distributions, quantum junta states, and qac^0 circuits, 2025. URL https://arxiv.org/abs/2410.15822.

Adriano Barenco, André Berthiaume, David Deutsch, Artur Ekert, Richard Jozsa, and Chiara Macchiavello. Stabilization of Quantum Computations by Symmetrization. *SIAM Journal on Computing*, 26(5):1541–1557, 1997. doi: 10.1137/S0097539796302452.

Michael Ben-Or, Ephraim Feig, Dexter Kozen, and Prasoon Tiwari. A Fast Parallel Algorithm for Determining All Roots of a Polynomial with Real Roots. *SIAM Journal on Computing*, 17(6): 1081–1092, 1988. doi: 10.1137/0217069.

Ethan Bernstein and Umesh Vazirani. Quantum Complexity Theory. *SIAM Journal on Computing*, 26(5):1411–1473, 1997. doi: 10.1137/S0097539796300921. URL https://doi.org/10.1137/S0097539796300921.

Allan Borodin. On Relating Time and Space to Size and Depth. *SIAM Journal on Computing*, 6(4): 733–744, 1977. doi: 10.1137/0206054.

John Bostanci, Yuval Efron, Tony Metger, Alexander Poremba, Luowen Qian, and Henry Yuen. Unitary Complexity and the Uhlmann Transformation Problem, 2023.

Zvika Brakerski and Omri Shmueli. (Pseudo) Random Quantum States with Binary Phase. In *Theory of Cryptography*, 2019. doi: 10.1007/978-3-030-36030-6_10. URL https://doi.org/10.1007/978-3-030-36030-6_10.

Dagmar Bruß and Chiara Macchiavello. Optimal state estimation for d-dimensional quantum systems. *Physics Letters A*, 253(5):249–251, 1999. ISSN 0375-9601. doi: https://doi.org/10.1016/S0375-9601(99)00099-7.

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, page 1398–1411. Association for Computing Machinery, 2021. doi: 10.1145/3406325.3451109. URL https://doi.org/10.1145/3406325.3451109.

Harry Buhrman, Richard Cleve, John Watrous, and Ronald de Wolf. Quantum Fingerprinting. *Phys. Rev. Lett.*, 87:167902, Sep 2001. doi: 10.1103/PhysRevLett.87.167902.

Harry Buhrman, Noah Linden, Laura Mančinska, Ashley Montanaro, and Maris Ozols. Quantum Majority Vote. In Yael Tauman Kalai, editor, *14th Innovations in Theoretical Computer Science Conference (ITCS 2023)*, volume 251 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 29:1–29:1, Dagstuhl, Germany, 2023. Schloss Dagstuhl – Leibniz-Zentrum für Informatik. ISBN 978-3-95977-263-1. doi: 10.4230/LIPIcs.ITCS.2023.29. URL https://drops-dev.dagstuhl.de/entities/document/10.4230/LIPIcs.ITCS.2023.29.

Chi-Fang Chen, Adam Bouland, Fernando G. S. L. Brandão, Jordan Docter, Patrick Hayden, and Michelle Xu. Efficient unitary designs and pseudorandom unitaries from permutations, 2024.

S. Chen, B. Huang, J. Li, A. Liu, and M. Sellke. When does adaptivity help for quantum state learning? In *2023 IEEE 64th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 391–404, Los Alamitos, CA, USA, nov 2023. IEEE Computer Society. doi: 10.1109/FOCS57990.2023.00029.

Nai-Hui Chia, Chi-Ning Chou, Jiayu Zhang, and Ruizhe Zhang. Quantum Meets the Minimum Circuit Size Problem. In Mark Braverman, editor, *13th Innovations in Theoretical Computer Science Conference (ITCS 2022)*, volume 215 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 47:1–47:16, Dagstuhl, Germany, 2022. Schloss Dagstuhl – Leibniz-Zentrum für Informatik. ISBN 978-3-95977-217-4. doi: 10.4230/LIPIcs.ITCS.2022.47.

Nai-Hui Chia, Ching-Yi Lai, and Han-Hsuan Lin. Efficient learning of t-doped stabilizer states with single-copy measurements, 2023.

L. Csanky. Fast parallel matrix inversion algorithms. In *16th Annual Symposium on Foundations of Computer Science (sfcs 1975)*, pages 11–12, 1975. doi: 10.1109/SFCS.1975.14.

Christoph Dankert, Richard Cleve, Joseph Emerson, and Etera Livine. Exact and approximate unitary 2-designs and their application to fidelity estimation. *Phys. Rev. A*, 80:012304, Jul 2009. doi: 10.1103/PhysRevA.80.012304.

Christopher M. Dawson and Michael A. Nielsen. The solovay-kitaev algorithm, 2005.

Hugo Delavenne, François Le Gall, Yupan Liu, and Masayuki Miyamoto. Quantum merlin-arthur proof systems for synthesizing quantum states, 2023. URL https://arxiv.org/abs/2303.01877.

Ugo Fano. Description of States in Quantum Mechanics by Density Matrix and Operator Techniques. *Reviews of Modern Physics*, 29(1):74, 1957. doi: 10.1103/RevModPhys.29.74. URL https://doi.org/10.1103/RevModPhys.29.74.

Lance Fortnow and Adam R. Klivans. Efficient learning algorithms yield circuit lower bounds. *Journal of Computer and System Sciences*, 75(1):27–36, 2009. ISSN 0022-0000. doi: https://doi.org/10.1016/j.jcss.2008.07.006. Learning Theory 2006.

Daniel Stilck França, Fernando G.S L. Brandão, and Richard Kueng. Fast and Robust Quantum State Tomography from Few Basis Measurements. In *16th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC 2021)*, volume 197 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 7:1–7:13, 2021. doi: 10.4230/LIPIcs.TQC.2021.7. URL https://doi.org/10.4230/LIPIcs.TQC.2021.7.

C.A. Fuchs and J. van de Graaf. Cryptographic distinguishability measures for quantum-mechanical states. *IEEE Transactions on Information Theory*, 45(4):1216–1227, 1999. doi: 10.1109/18.761271.

Tudor Giurgica-Tiron and Adam Bouland. Pseudorandomness from subset states, 2023.

O. Goldreich, S. Goldwasser, and S. Micali. How To Construct Randolli Functions. In *25th Annual Symposium on Foundations of Computer Science, 1984.*, pages 464–479, 1984. doi: 10.1109/SFCS.1984.715949.

Daniel Gottesman and Isaac Chuang. Quantum Digital Signatures, 2001.

Frederic Green, Debajyoti Bera, Stephen Fenner, and Steve Homer. Efficient Universal Quantum Circuits. *Quantum Information and Computation*, 10, 07 2009. doi: 10.1007/978-3-642-02882-3_42.

Sabee Grewal, Vishnu Iyer, William Kretschmer, and Daniel Liang. Efficient Learning of Quantum States Prepared With Few Non-Clifford Gates, 2023a.

Sabee Grewal, Vishnu Iyer, William Kretschmer, and Daniel Liang. Efficient Learning of Quantum States Prepared With Few Non-Clifford Gates II: Single-Copy Measurements, 2023b.

Sabee Grewal, Vishnu Iyer, William Kretschmer, and Daniel Liang. Improved stabilizer estimation via bell difference sampling, 2023c.

Jeongwan Haah, Aram W. Harrow, Zhengfeng Ji, Xiaodi Wu, and Nengkun Yu. Sample-Optimal Tomography of Quantum States. *IEEE Transactions on Information Theory*, 63(9):5628–5641, 2017. doi: 10.1109/TIT.2017.2719044. URL https://doi.org/10.1109/TIT.2017.2719044.

Dominik Hangleiter and Michael J. Gullans. Bell sampling from quantum circuits, 2023.

Steve Hanneke. The optimal sample complexity of pac learning. *J. Mach. Learn. Res.*, 17(1): 1319–1333, jan 2016. ISSN 1532-4435.

Ryan C. Harkins and John M. Hitchcock. Exact learning algorithms, betting games, and circuit lower bounds. *ACM Trans. Comput. Theory*, 5(4), nov 2013. ISSN 1942-3454. doi: 10.1145/2539126.2539130. URL https://doi.org/10.1145/2539126.2539130.

Peter Hoyer and Robert Spalek. Quantum fan-out is powerful. *Theory Computing*, 1:81–103, 2005. doi: 10.4086/toc.2005.v001a005.

Hsin-Yuan Huang, Richard Kueng, and John Preskill. Predicting many properties of a quantum system from very few measurements. *Nature Physics*, 16(10):1050–1057, 2020. doi: 10.1038/s41567-020-0932-7. URL https://doi.org/10.1038/s41567-020-0932-7.

Hsin-Yuan Huang, Yunchao Liu, Michael Broughton, Isaac Kim, Anurag Anshu, Zeph Landau, and Jarrod R. McClean. Learning shallow quantum circuits. In *Proceedings of the 56th Annual ACM Symposium on Theory of Computing*, STOC 2024, page 1343–1351, New York, NY, USA, 2024. Association for Computing Machinery. ISBN 9798400703836. doi: 10.1145/3618260.3649722.

Fernando Granha Jeronimo, Nir Magrafta, and Pei Wu. Pseudorandom and pseudoentangled states from subset states, 2024.

Zhengfeng Ji, Yi-Kai Liu, and Fang Song. Pseudorandom Quantum States. In *Advances in Cryptology - CRYPTO 2018 - 38th Annual International Cryptology Conference*, pages 126–152. Springer, 2018. doi: 10.1007/978-3-319-96878-0_5. URL https://doi.org/10.1007/978-3-319-96878-0_5.

Michael J. Kearns and Umesh V. Vazirani. *An introduction to computational learning theory*. MIT Press, Cambridge, MA, USA, 1994. ISBN 0262111934.

Adam Klivans, Pravesh Kothari, and Igor C. Oliveira. Constructing Hard Functions Using Learning Algorithms. In *2013 IEEE Conference on Computational Complexity*, pages 86–97, 2013. doi: 10.1109/CCC.2013.18.

William Kretschmer. Quantum Pseudorandomness and Classical Complexity. In *16th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC 2021)*, volume 197 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 2:1–2:20, 2021. doi: 10.4230/LIPIcs.TQC.2021.2. URL https://doi.org/10.4230/LIPIcs.TQC.2021.2.

William Kretschmer, Luowen Qian, Makrand Sinha, and Avishay Tal. Quantum Cryptography in Algorithmica. In *Proceedings of the 55th Annual ACM Symposium on Theory of Computing*, STOC 2023, page 1589–1602, New York, NY, USA, 2023. Association for Computing Machinery. ISBN 9781450399135. doi: 10.1145/3564246.3585225. URL https://doi.org/10.1145/3564246.3585225.

William Kretschmer, Luowen Qian, and Avishay Tal. Quantum-computable one-way functions without one-way functions, 2024. URL https://arxiv.org/abs/2411.02554.

Richard Kueng and David Gross. Qubit stabilizer states are complex projective 3-designs, 2015.

Vinayak M. Kumar. Tight Correlation Bounds for Circuits Between AC0 and TC0. In Amnon Ta-Shma, editor, *38th Computational Complexity Conference (CCC 2023)*, volume 264 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 18:1–18:40, Dagstuhl, Germany, 2023. Schloss Dagstuhl – Leibniz-Zentrum für Informatik. ISBN 978-3-95977-282-2. doi: 10.4230/LIPIcs.CCC.2023.18.

Greg Kuperberg. Breaking the cubic barrier in the Solovay-Kitaev algorithm, 2023.

Ching-Yi Lai and Hao-Chung Cheng. Learning Quantum Circuits of Some T Gates. *IEEE Transactions on Information Theory*, 68(6):3951–3964, 2022. doi: 10.1109/TIT.2022.3151760. URL https://doi.org/10.1109/TIT.2022.3151760.

Zeph Landau and Yunchao Liu. Learning quantum states prepared by shallow circuits in polynomial time, 2024. URL https://arxiv.org/abs/2410.23618.

Olivier Landon-Cardinal, Yi-Kai Liu, and David Poulin. Efficient Direct Tomography for Matrix Product States, 2010.

Lorenzo Leone, Salvatore F. E. Oliviero, and Alioscia Hamma. Learning t-doped stabilizer states, 2023.

Nathan Linial, Yishay Mansour, and Noam Nisan. Constant depth circuits, Fourier transform, and learnability. *J. ACM*, 40(3):607–620, jul 1993. ISSN 0004-5411. doi: 10.1145/174130.174138. URL https://doi.org/10.1145/174130.174138.

Chuhan Lu, Minglong Qin, Fang Song, Penghui Yao, and Mingnan Zhao. Quantum pseudorandom scramblers, 2023.

Fermi Ma and Hsin-Yuan Huang. How to Construct Random Unitaries, 2024.

G. Mauro D'Ariano, Matteo G.A. Paris, and Massimiliano F. Sacchi. Quantum Tomography. *Advances in Imaging and Electron Physics*, 128:205–308, 2003. doi: 10.1016/S1076-5670(03)80065-4. URL https://doi.org/10.1016/S1076-5670(03)80065-4.

T. Metger and H. Yuen. stateQIP = statePSPACE. In *2023 IEEE 64th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 1349–1356, Los Alamitos, CA, USA, nov 2023. IEEE Computer Society. doi: 10.1109/FOCS57990.2023.00082.

Tony Metger, Alexander Poremba, Makrand Sinha, and Henry Yuen. Simple constructions of linear-depth t-designs and pseudorandom unitaries, 2024.

Ashley Montanaro. Learning stabilizer states by Bell sampling, 2017.

Cristopher Moore. Quantum circuits: Fanout, parity, and counting, 1999.

Cody D. Murray and R. Ryan Williams. Circuit lower bounds for nondeterministic quasi-polytime from a new easy witness lemma. *SIAM Journal on Computing*, 49(5):STOC18–300–STOC18–322, 2020. doi: 10.1137/18M1195887.

Shivam Nadimpalli, Natalie Parham, Francisca Vasconcelos, and Henry Yuen. On the pauli spectrum of qac0, 2024.

C. Andrew Neff. Specified precision polynomial root isolation is in NC. *Journal of Computer and System Sciences*, 48(3):429–463, 1994. ISSN 0022-0000. doi: https://doi.org/10.1016/S0022-0000(05)80061-3.

Michael A. Nielsen and Isaac Chuang. Quantum Computation and Quantum Information, 2002. URL https://doi.org/10.1017/CBO9780511976667.

Ryan O'Donnell and John Wright. Efficient Quantum Tomography. In *Proceedings of the Forty-Eighth Annual ACM Symposium on Theory of Computing*, pages 899–912, 2016. doi: 10.1145/2897518.2897544. URL https://doi.org/10.1145/2897518.2897544.

Igor Oliveira and Rahul Santhanam. Pseudo-Derandomizing Learning and Approximation. In Eric Blais, Klaus Jansen, José D. P. Rolim, and David Steurer, editors, *Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques (APPROX/RANDOM 2018)*, volume 116 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 55:1–55:19, Dagstuhl, Germany, 2018. Schloss Dagstuhl – Leibniz-Zentrum für Informatik. ISBN 978-3-95977-085-9. doi: 10.4230/LIPIcs.APPROX-RANDOM.2018.55.

Igor C. Oliveira and Rahul Santhanam. Conspiracies between learning algorithms, circuit lower bounds, and pseudorandomness. In *Proceedings of the 32nd Computational Complexity Conference*, CCC '17, Dagstuhl, DEU, 2017. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik. ISBN 9783959770408.

Michał Oszmaniec, Marcin Kotowski, Michał Horodecki, and Nicholas Hunter-Jones. Saturation and recurrence of quantum complexity in random local quantum dynamics, 2024.

Alexander A Razborov and Steven Rudich. Natural proofs. *Journal of Computer and System Sciences*, 55(1):24–35, 1997. ISSN 0022-0000. doi: https://doi.org/10.1006/jcss.1997.1494.

Rizwana Rehman and Ilse C. F. Ipsen. La budde's method for computing characteristic polynomials, 2011.

Gregory Rosenthal. Query and depth upper bounds for quantum unitaries via grover search, 2023.

Gregory Rosenthal. Efficient quantum state synthesis with one query. In *Proceedings of the 2024 Annual ACM-SIAM Symposium on Discrete Algorithms (SODA)*, pages 2508–2534, 2024. doi: 10.1137/1.9781611977912.89.

Gregory Rosenthal and Henry Yuen. Interactive Proofs for Synthesizing Quantum States and Unitaries. In Mark Braverman, editor, *13th Innovations in Theoretical Computer Science Conference (ITCS 2022)*, volume 215 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 112:1–112:4, Dagstuhl, Germany, 2022. Schloss Dagstuhl – Leibniz-Zentrum für Informatik. ISBN 978-3-95977-217-4. doi: 10.4230/LIPIcs.ITCS.2022.112.

Thomas Schuster, Jonas Haferkamp, and Hsin-Yuan Huang. Random unitaries in extremely low depth, 2024.

Thomas Schuster, Fermi Ma, Fernando G.S.L. Brandão, and Hsin-Yuan Huang. In preparation, 2025. The forthcoming paper establishes the minimum time required to generate strong random unitary designs and strong pseudorandom unitaries (PRUs). Among other results, it proves that strong PRUs over n qubits can be efficiently constructed in O(log n) depth by replacing permutation operators in the CPFC construction with 2-round Luby-Rackoff/Feistel networks.

Yasuhiro Takahashi and Tani Seiichiro. Collapse of the Hierarchy of Constant-Depth Exact Quantum Circuits. *computational complexity*, 25:849–881, 2016. ISSN 1420-8954. doi: 10.1007/s00037-016-0140-0.

Ewout Van Den Berg. A simple method for sampling random clifford operators. In *2021 IEEE International Conference on Quantum Computing and Engineering (QCE)*, pages 54–59, 2021. doi: 10.1109/QCE52317.2021.00021.

Francisca Vasconcelos and Hsin-Yuan Huang. Learning shallow quantum circuits with many-qubit gates, 2024. URL https://arxiv.org/abs/2410.16693.

Ilya Volkovich. On learning, lower bounds and (un)keeping promises. In Javier Esparza, Pierre Fraigniaud, Thore Husfeldt, and Elias Koutsoupias, editors, *Automata, Languages, and Programming*, pages 1027–1038, Berlin, Heidelberg, 2014. Springer Berlin Heidelberg. ISBN 978-3-662-43948-7.

Ilya Volkovich. A guide to learning arithmetic circuits. In Vitaly Feldman, Alexander Rakhlin, and Ohad Shamir, editors, *29th Annual Conference on Learning Theory*, volume 49 of *Proceedings of Machine Learning Research*, pages 1540–1561, Columbia University, New York, New York, USA, 23–26 Jun 2016. PMLR. URL https://proceedings.mlr.press/v49/volkovich16.html.

John Watrous. Space-Bounded Quantum Complexity. *Journal of Computer and System Sciences*, 59(2):281–326, 1999. ISSN 0022-0000. doi: https://doi.org/10.1006/jcss.1999.1655.

John Watrous. Quantum statistical zero-knowledge, 2002.

John Watrous. On the complexity of simulating space-bounded quantum computations. *compational complexity*, 12:48–84, June 2003. ISSN 1420-8954. doi: 10.1007/s00037-003-0177-8.

John Watrous. *The Theory of Quantum Information*. Cambridge University Press, 2018.

Jonathan Welch, Alex Bocharov, and Krysta M. Svore. Efficient Approximation of Diagonal Unitaries over the Clifford+T Basis. *Quantum Info. Comput.*, 16(1–2):87–104, jan 2016. ISSN 1533-7146. doi: 10.26421/QIC16.15-16-8.

J. H. Wilkinson. *The algebraic eigenvalue problem*. Oxford University Press, Inc., USA, 1988. ISBN 0198534183.

R. Ryan Williams. New algorithms and lower bounds for circuits with linear threshold gates. *Theory of Computing*, 14(17):1–25, 2018. doi: 10.4086/toc.2018.v014a017.

Ryan Williams. Nonuniform acc circuit lower bounds. *J. ACM*, 61(1), jan 2014. ISSN 0004-5411. doi: 10.1145/2559903. URL https://doi.org/10.1145/2559903.

Henry Yuen. An Improved Sample Complexity Lower Bound for (Fidelity) Quantum State Tomography. *Quantum*, 7:890, January 2023. ISSN 2521-327X. doi: 10.22331/q-2023-01-03-890. URL https://doi.org/10.22331/q-2023-01-03-890.

Mark Zhandry. A note on quantum-secure prps, 2016.

Mark Zhandry. How to Construct Quantum Random Functions. *J. ACM*, 68(5), aug 2021. ISSN 0004-5411. doi: 10.1145/3450745. URL https://doi.org/10.1145/3450745.

Haimeng Zhao, Laura Lewis, Ishaan Kannan, Yihui Quek, Hsin-Yuan Huang, and Matthias C. Caro. Learning quantum states and unitaries of bounded gate complexity, 2023.

Contents

Appendix A. Preliminaries

For functions $f : X \to Y$ and $f : Y \to Z$ we define $f \circ g : X \to Z$ to be the composition of f and g.

We define the p-norm of vector v to be $\|v\|_p \coloneqq \sqrt[p]{\sum_i v_i^p}$. The Schatten p-norm of a matrix A is defined to be $\|A\|_p \coloneqq \sqrt[p]{\mathrm{tr}\left[(A^\dagger A)^p\right]}$ or the p-norm of the singular values of A, with the convention that $\|\cdot\|_\infty$ is the operator norm.

A.1. Quantum States, Maps, and Measurements

Definition 8 *A quantum state on n qubits is a $2^n \times 2^n$ positive semi-definite Hermitian matrix ρ such that $\mathrm{tr}[\rho] = 1$.*

We will refer to quantum states ρ such that the rank of ρ is 1 as *pure states*. Oftentimes such pure states will simply be written as a 2^n-dimensional complex unit column vector $|\psi\rangle$ or row vector $\langle\psi|$ such that their outer-product $|\psi\rangle\langle\psi| = \rho$. Quantum states that cannot be written in such a manner will often be referred to as *mixed states*.

We will denote the set of quantum states on n qubits as $\mathcal{D}_n$, while the set of of quantum pure states on n qubits is denoted by $\mathcal{S}_n$. For convenience we will often drop the subscript as the n will be obvious from context.

A trace-preserving completely positive map from n-qubits to n-qubits is any linear map $\Phi : \mathcal{D}_n \to \mathcal{D}_n$ such that $\mathrm{Id}_m \otimes \Phi : \mathcal{D}_{m+n} \to \mathcal{D}_{m+n}$ for any $m \in \mathbb{N}$, where Id_m is the identity map on m qubits.

A positive operator-valued measurement on n-qubits is a set of positive semi-definite matrices $\{\Pi_i\}$ such that $\sum_i \Pi_i$ is the $2^n \times 2^n$ identity matrix. We define the probability of event i happening when measuring a state ρ with $\{\Pi_i\}$ to be $\mathrm{tr}[\Pi_i \rho]$.

A.1.1. Distances Between Quantum States

The following is the standard notion of distance between quantum states used in this paper.

Definition 9 (Trace Distance) *The trace distance between two states ρ and σ is*

$$d_{\mathrm{tr}}(\rho, \sigma) \coloneqq \frac{1}{2}\|\rho - \sigma\|_1.$$

The trace distance is useful because it tells us that distinguishing one copy of ρ from one copy of σ can be done with bias at most $d_{\mathrm{tr}}(\rho, \sigma)$.

Fact 10 (Nielsen and Chuang, 2002) *For any positive operater-valued measurement $\{\Pi_i\}$ and quantum states ρ and σ,*

$$d_{\mathrm{tr}}(\rho, \sigma) \geq \frac{1}{2}\sum_i |\mathrm{tr}[\Pi_i \rho] - \mathrm{tr}[\Pi_i \sigma]| = \frac{1}{2}\sum_i |\mathrm{tr}[\Pi_i \cdot (\rho - \sigma)]|.$$

Another useful notion of distance, known as fidelity, will be relevant in Section C.

Definition 11 (Fidelity) *The fidelity between two quantum states ρ and σ is*

$$\mathcal{F}(\rho, \sigma) \coloneqq \left(\mathrm{tr}\sqrt{\sqrt{\rho}\sigma\sqrt{\rho}}\right)^2.$$

It is well known that if ρ is a pure state $|\psi\rangle\langle\psi|$ then the fidelity becomes $\mathcal{F}(|\psi\rangle\langle\psi|, \sigma) = \langle\psi|\sigma|\psi\rangle$. Likewise, it is well known that both fidelity and trace distance lie in the interval $[0, 1]$.

To relate the two quantities, we give bounds between trace distance and fidelity when one of the states is a pure state. They can be seen as a form of Fuchs-van de Graaf inequality (Fuchs and van de Graaf, 1999; Watrous, 2018).

Fact 12 (Folklore) *Given pure state $|\psi\rangle$ and mixed state σ then*

$$1 - \mathcal{F}(|\psi\rangle\langle\psi|, \sigma) \leq d_{\mathrm{tr}}(|\psi\rangle\langle\psi|, \sigma) \leq \sqrt{1 - \mathcal{F}(|\psi\rangle\langle\psi|, \sigma)}.$$

Furthermore, the upper bound is tight when σ is also a pure state.

Proof The second inequality and its condition when σ is a pure state follows from the standard Fuchs-van de Graaf inequality.

For the first inequality, consider the POVM $\{|\psi\rangle\langle\psi|, I - |\psi\rangle\langle\psi|\}$. This implies the following lower bound on the trace distance:

$$\begin{aligned} d_{\mathrm{tr}}(|\psi\rangle\langle\psi|, \sigma) &\geq \frac{1}{2}\left(\Big|\mathrm{tr}[|\psi\rangle\langle\psi| \cdot (|\psi\rangle\langle\psi| - \sigma)]\Big| + \Big|\mathrm{tr}[(I - |\psi\rangle\langle\psi|) \cdot (|\psi\rangle\langle\psi| - \sigma)]\Big|\right) \quad \text{(Fact 10)} \\ &= \Big|1 - \mathcal{F}(|\psi\rangle\langle\psi|, \sigma)\Big| \\ &= 1 - \mathcal{F}(|\psi\rangle\langle\psi|, \sigma) \end{aligned}$$

where the second line follows from $\mathrm{tr}[\rho - \sigma] = 0$ for any two quantum states and the third line follows because fidelity is never bigger than 1. ■

We can use the upper bound of Fact 12 being tight for pure states to derive the following bounds for the trace distance between multiple copies of two pure states.

Corollary 13 *For pure states $|\psi\rangle$ and $|\phi\rangle$ and $m \in \mathbb{N}$,*

$$d_{\mathrm{tr}}(|\psi\rangle^{\otimes m}, |\phi\rangle^{\otimes m}) \leq \sqrt{m} \cdot d_{\mathrm{tr}}(|\psi\rangle, |\phi\rangle).$$

Proof

$$\begin{aligned} d_{\mathrm{tr}}(|\psi\rangle^{\otimes m}, |\phi\rangle^{\otimes m}) &= \sqrt{1 - \mathcal{F}(|\psi\rangle^{\otimes m}, |\phi\rangle^{\otimes m})} && \text{(Fact 12)} \\ &= \sqrt{1 - \mathcal{F}(|\psi\rangle, |\phi\rangle)^m} \\ &= \sqrt{1 - (1 - d_{\mathrm{tr}}(|\psi\rangle, |\phi\rangle)^2)^m} && \text{(Fact 12)} \\ &\leq \sqrt{m} \cdot d_{\mathrm{tr}}(|\psi\rangle, |\phi\rangle), \end{aligned}$$

where the second line holds from the multiplicativity of fidelity with respect to the tensor product. ■

We can also upper bound the trace distance of pure states to their distance as vectors. This largely follows because their distance as vectors cares about global phase, whereas trace distance knows that global phase does not matter in quantum mechanics.

Fact 14 *For pure states $|\psi\rangle$ and $|\phi\rangle$,*

$$d_{\mathrm{tr}}(|\psi\rangle, |\phi\rangle) \leq \||\psi\rangle - |\phi\rangle\|_2.$$

Proof

$$\begin{aligned}
d_{\mathrm{tr}}(|\psi\rangle, |\phi\rangle) &= \sqrt{1 - |\langle\psi|\phi\rangle|^2} && \text{(Fact 12)} \\
&= \sqrt{(1 + |\langle\psi|\phi\rangle|)(1 - |\langle\psi|\phi\rangle|)} \\
&\leq \sqrt{2 - 2|\langle\psi|\phi\rangle|} \\
&\leq \sqrt{\langle\psi|\psi\rangle + \langle\phi|\phi\rangle - 2\mathrm{Re}\left[\langle\psi|\phi\rangle\right]} \\
&= \||\psi\rangle - |\phi\rangle\|_2
\end{aligned}$$

■

Because $\|U|\psi\rangle - V|\psi\rangle\|_2 \leq \|U - V\|_\infty$, acting on a state with unitary V instead of unitary U only affects the resulting quantum state by at most $\|U - V\|_\infty$.

A.2. Quantum Circuits

We largely follow the notation of Bostanci et al. (2023) and Rosenthal (2024) both here and in Section A.3. Note that we will regularly abuse notation, such that for functions acting on the natural numbers we will actually be implicitly referring to the output of that function on n, the input size. For instance, given $f : \mathbb{N} \to [0, 1]$, we will generally shorthand $f(n)$ to just f.

A *unitary quantum circuit* is any circuit that obeys the following pattern: (1) initializing ancilla qubits, (2) applying gates from $\{H, \mathrm{CNOT}, T\}$, and (3) optional tracing out of ancilla qubits at the end.[9]

A *general quantum circuit* adds the ability to perform *intermediate* single-qubit non-unitary gates: (1) prepare an auxiliary qubit in the $|0\rangle$ state (2) trace out a qubit and (3) measure a qubit in the computational basis. These actions can be taken at any point in the computational process. We will often denote a general quantum circuit C acting on input state ρ to be $C(\rho)$ for brevity.

We note that the actual gate set is not important, so long as there are only $O(1)$ distinct gates, each gate has algebraic entries, and the gate set is universal for quantum computation and contains its own inverses. The $O(1)$ distinct gates is necessary in Lemmas 26 and 58 to bound the number of quantum circuits of polynomial size. The algebraic entries allows the distance between states to be computed in polynomial space (see Lemma 61). Finally, the universality (along with the algebraic entries) and inverse gates allows us to use the Solovay-Kitaev algorithm. We now state the most recent version of the Solovay-Kitaev algorithm due to Kuperberg (2023).

Lemma 15 (Solovay-Kitaev algorithm) *Given a universal gateset $\mathcal{G}$ containing its own inverses and a fixed $k \in \mathbb{N}$, any k-qubit unitary can be approximated by a unitary $\widehat{U}$ via a finite sequence of gates from $\mathcal{G}$ with length $O\left(\log^\alpha \frac{1}{\varepsilon}\right)$ that can be generated in time $\tilde{O}\left(\log^\alpha \frac{1}{\varepsilon}\right)$ such that $\|U - \widehat{U}\|_\infty \leq \varepsilon$ for any $\alpha > \log_\phi 2 = 1.44042\ldots$.*[10]

9. $\{H, \mathrm{CNOT}, T\}$ is well-known to be a universal quantum gate set (Nielsen and Chuang, 2002, Chapter 4.5),
10. The time efficiency is currently not explicitly stated in the manuscript of Kuperberg (2023), but it has been verified via personal communications with the author. Note that this is the time to generate an uncompressed word, while a compressed version can be found more quickly (see Dawson and Nielsen, 2005 for a similar example).

Observe that, since trace distance is contractive under trace-preserving completely positive maps (which adding an ancilla qubit, measuring a qubit, and tracing out a qubit fall under), these non-unitary actions do not contribute to any error in synthesizing, regardless of the unitary gate set.

Our choice of gate set has the advantage of being able to exactly perform all classical computations, as it can exactly construct the Toffoli gate, which is universal for classical reversible computation.

Fact 16 (Welch et al., 2016) *The Toffoli gate has an exact construction in the* $\{H, \mathrm{CNOT}, T\}$ *gate set .*

Throughout the paper, we will just assume that efficient classical computation can be performed efficiently on the $\{H, \mathrm{CNOT}, T\}$ gate set without error.

Definition 17 (Quantum Circuit Size and Space) *We say that the* size *of a general (resp. unitary) quantum circuit C is the number of gates (both unitary and non-unitary) used in C. We say that the* space *of a general (resp. unitary) quantum circuit C is the maximum number of qubits used at any point in the circuit. Finally we say that the* depth *of a general (resp. unitary) quantum circuit C is the maximum number of layers of gates that are needed.*

Note that a size k circuit on n qubits of input uses space at most $n+2k$ with any 2-local gate set, such as the $\{H, \mathrm{CNOT}, T\}$ gate set that we will default to. Additionally, a depth d space s circuit has size at most $s \cdot d$

Definition 18 (Uniform Circuit Families) *For $t : \mathbb{N} \to \mathbb{R}^+$, a family of quantum circuits $(C_x)_{x\in\{0,1\}^*}$ is called* t-time-uniform *if $(C_x)_{x\in\{0,1\}^*}$ is size at most* $\mathrm{poly}(|x|, t(|x|))$ *and there exists a classical Turing machine that on input $x \in \{0,1\}^*$ outputs the description of C_x in time at most $O(t(|x|)$. Similarly, for $s : \mathbb{N} \to \mathbb{R}^+$ a family of quantum circuits $(C_x)_{x\in\{0,1\}^*}$ is called* s-space-uniform *if $(C_x)_{x\in\{0,1\}^*}$ uses space at most* $\mathrm{poly}(|x|, s(|x|))$ *and there exists a classical Turing machine that on inputs $x \in \{0,1\}^*$ and $i \in \mathbb{N}$ outputs the i-th bit of the description of C_x in space at most $O(s(|x|))$.*

We will oftentimes refer to uniform *general* quantum circuits simply as quantum algorithms. We will also use the circuit sequence $(C_n)_{n\in\mathbb{N}}$ to be composed of C_{1^n} from uniform quantum circuits $(C_x)_{x\in\{0,1\}^*}$ as a shorthand for uniform circuit families that only depend on the length of the input. These too will often be referred to as simply quantum algorithms.

As with Arunachalam et al. (2022b), it will be necessary throughout this work that given a valid *description*, $\mathrm{desc}(U)$, of a *unitary* circuit U, there is an efficient procedure to *apply* said unitary circuit in time polynomial in the size of the input and the size of the description within the gateset $\{H, \mathrm{CNOT}, T\}$.

Fact 19 (Green et al., 2009, Theorem 3) *Fix $n \in \mathbb{N}$ and $s : \mathbb{N} \to \mathbb{R}^+$ and let $\mathrm{DESC}(C) \in \{0,1\}^m$ refer to the description of a* unitary *quantum circuit U on n qubits of size $s(n)$. There exists an $(n+m)$-qubit $O((n+s)\log(n+s))$-time-uniform* unitary *quantum circuit $\mathcal{U}$ such that*

$$\mathcal{U}(|x\rangle \otimes |\mathrm{DESC}(U)\rangle) = (U|x\rangle) \otimes |\mathrm{DESC}(U)\rangle$$

for all $x \in \{0,1\}^n$.

A.3. State Synthesis Complexity Classes

We now define the state synthesis version of some complexity classes. Defined previously in Rosenthal and Yuen (2022); Metger and Yuen (2023); Bostanci et al. (2023); Rosenthal (2024), they capture the complexity of problems with quantum output. Informally, let A be a decision class associated with some computational models and let $\mathfrak{C}_\mathsf{A}$ be the set of circuit sequences $(C_x)_{x\in\{0,1\}^*}$ (uniform or otherwise) associated with A with $\mathrm{poly}(|x|)$-qubits of output. Then stateA_δ is simply the set of state sequences $(\rho_x)_{x\in\{0,1\}^*}$ such that there exists a corresponding $(C_x)_{x\in\{0,1\}^*} \in \mathfrak{C}_\mathsf{A}$ that outputs a state that is δ-close to each ρ_x in trace distance. As an example, $\mathsf{stateBQE}_\delta$ (see Definition 22), is, informally, the set of state sequences that can be synthesized to trace distance at most δ by $2^{O(n)}$-time-uniform general quantum circuits. To make sure that these classes are properly comparable, we will restrict the number of qubits of each ρ_x to be $\mathrm{poly}(|x|)$.[11]

We will generally want to work with arbitrary inverse-polynomial or arbitrary inverse-exponential trace distance. As such, for a complexity class stateA_δ, define stateA and $\mathsf{stateA}_{\exp}$ to be

$$\mathsf{stateA} \coloneqq \bigcap_q \mathsf{stateA}_{1/q}$$

$$\mathsf{stateA}_{\exp} \coloneqq \bigcap_q \mathsf{stateA}_{\exp(-q)}$$

where the union is over all polynomials $q : \mathbb{N} \to \mathbb{R}$. Furthermore, for an arbitrary state synthesis complexity class over mixed states stateA_δ, we define $\mathsf{pureStateA}_\delta \subset \mathsf{stateA}_\delta$ to be the subset of stateA_δ with state sequences consisting only of pure states $(|\psi_x\rangle\langle\psi_x|)_{x\in\{0,1\}^*}$. We will generally be dealing with pure state synthesis classes throughout this work. We will also abuse notation and often write down such pure state sequences simply as $(|\psi_x\rangle)_{x\in\{0,1\}^*}$.

We now state some (largely trivial) facts about state synthesis complexity classes and their variations, to aid in intuition.

Fact 20 *For arbitrary state synthesis complexity classes* stateA_δ *and* $\mathsf{stateB}_\varepsilon$*:*

(i) $\mathsf{stateA}_\delta \subseteq \mathsf{stateA}_{\delta'}$ *for* $\delta \leq \delta'$.

(ii) $\mathsf{stateA}_\delta \subset \mathsf{stateB}_\varepsilon \Rightarrow \mathsf{pureStateA}_\delta \subset \mathsf{pureStateB}_\varepsilon$.

(iii) $\mathsf{stateA}_\delta \subset \mathsf{stateB}_\varepsilon \Rightarrow \mathsf{stateA}_{\delta+\gamma} \subset \mathsf{stateB}_{\varepsilon+\gamma}$.

A.3.1. UNIFORM COMPUTATION

Definition 21 ($\mathsf{stateBQTIME}[f]_\delta$, $\mathsf{stateBQSPACE}[f]_\delta$) *Let* $\delta : \mathbb{N} \to [0,1]$ *and* $f : \mathbb{N} \to \mathbb{R}^+$ *be functions. Then* $\mathsf{stateBQTIME}[f]_\delta$ *(resp.* $\mathsf{stateBQSPACE}[f]_\delta$*) is the class of all sequences of density matrices* $(\rho_x)_{x\in\{0,1\}^*}$ *such that each* ρ_x *is a state on* $\mathrm{poly}(|x|)$ *qubits, and there exists an* f*-time-uniform (resp.* f*-space-uniform) family of general quantum circuits* $(C_x)_{x\in\{0,1\}^*}$ *such that for all sufficiently large input sizes* $|x|$*, the circuit* C_x *takes no inputs and outputs a density matrix* σ_x *such that* $d_{\mathrm{tr}}(\rho_x, \sigma_x) \leq \delta$.

We define the following state synthesis complexity classes, which are the analogues of BQE and PSPACE.

11. Some works, such as Rosenthal (2024) even restrict the final number of qubits to simply be $|x|$.

Definition 22 ($\mathsf{stateBQE}_\delta$, $\mathsf{statePSPACE}_\delta$)

$$\mathsf{stateBQE}_\delta := \bigcup_{c\geq 0} \mathsf{stateBQTIME}\left[2^{c\cdot n}\right]_\delta \quad \textit{and} \quad \mathsf{statePSPACE}_\delta := \bigcup_{p} \mathsf{stateBQSPACE}\left[p\right]_\delta$$

where the union for PSPACE_δ *is over all polynomials* $p : \mathbb{N} \to \mathbb{R}^+$.

We can likewise define $\mathsf{stateBQSUBEXP}_\delta := \bigcap_{\gamma\in(0,1)} \mathsf{stateBQTIME}\left[2^{n^\gamma}\right]_\delta$ and $\mathsf{stateBQP}_\delta := \bigcup_p \mathsf{stateBQTIME}\left[p\right]_\delta$ for polynomials $p : \mathbb{N} \to \mathbb{R}^+$.[12]

It is worth commenting on the choice of gate set and how it affects (or does not affect) $\mathsf{stateBQTIME}\left[f\right]_\delta$. While we use the $\{H, \mathrm{CNOT}, T\}$ gate set, if we had some other universal gate set then we could apply the Solovay-Kitaev algorithm to approximate each of these gates. Because the size is at most $\mathrm{poly}(n, f(n))$, we need to approximate each gate to accuracy $\frac{\delta}{\mathrm{poly}(n,f(n))}$, which increases the runtime by a multiplicative factor of $O\left(\log^{1.441}\left(\frac{n\cdot f(n)}{\delta}\right)\right)$. Thus $\mathsf{stateBQP}$, $\mathsf{stateBQP}_{\mathrm{exp}}$, $\mathsf{stateBQE}$, and $\mathsf{stateBQE}_{\mathrm{exp}}$ are not affected by which universal gate set is used. For comparison, we note the same is not true for a version of $\mathsf{stateBQP}$ with arbitrary doubly-exponentially-small error.

The following will be one of the most important state synthesis classes in our proof. The main difference as compared to $\mathsf{statePSPACESIZE}$ is the fact that the entire circuit must be computable using only polynomial space, rather than have each gate be computable using polyomial space. In Lemma 48, this will allow us to efficiently find the whole description of circuits in $\mathsf{statePSPACESIZE}$ as well as efficiently apply the circuit given its description (see Fact 19).

Definition 23 ($\mathsf{statePSPACESIZE}_\delta$) *Let* $\delta : \mathbb{N} \to [0,1]$ *and* $f : \mathbb{N} \to \mathbb{R}^+$ *be functions.* $\mathsf{stateBQSPACESIZE}\left[f\right]_\delta$ *is the class of all sequences of density matrices* $(\rho_x)_{x\in\{0,1\}^*}$ *such that each* ρ_x *is a state on* $\mathrm{poly}(|x|)$ *qubits, and there exists an* f*-space-uniform family of general quantum circuits* $(C_x)_{x\in\{0,1\}^*}$ *of size at most* $\mathrm{poly}(|x|)$ *such that for all sufficiently large input sizes* $|x|$*, the circuit* C_x *takes no inputs and outputs a density matrix* σ_x *such that* $\mathrm{d}_{\mathrm{tr}}(\rho_x, \sigma_x) \leq \delta$.

A.3.2. NON-UNIFORM COMPUTATION

We now introduce *non-uniform* models of state synthesis. Unlike uniform classes, there does not necessarily need to be an algorithm that finds the correct circuit. It just needs to exist.

The following will be the non-uniform class used the most often in the proofs.

Definition 24 ($\mathsf{stateBQSIZE}\left[s\right]_\delta$) *Let* $\delta : \mathbb{N} \to [0,1]$ *and* $s : \mathbb{N} \to \mathbb{R}^+$. *Then* $\mathsf{stateBQSIZE}\left[s\right]_\delta$ *is the class of all sequences of quantum states* $(\rho_x)_{x\in\{0,1\}^*}$ *such that each* ρ_x *is a state on* $\mathrm{poly}(|x|)$ *qubits, and there exists a family of* unitary *quantum circuits* $(C_x)_{x\in\{0,1\}^*}$, *taking in* $\mathrm{poly}(|x|)$ *qubits as input and of size at most* $O(s)$, *such that for all* $x \in \{0,1\}^*$ *with sufficiently large length* $|x|$, *the circuit* C_x *acting on the all-zeros state outputs a state* $\widehat{\rho}_x$ *satisfying*

$$d_{\mathrm{tr}}(\rho_x, \widehat{\rho}_x) \leq \delta.$$

12. Note that functions that grow as $2^{o(n)}$, such as $2^{\sqrt{n}}$ are also generally referred to as *sub-exponential*. To avoid confusion, we will use the term 'sub-exponential' only to refer to such $2^{o(n)}$ growths, and instead refer to algorithms in $\mathsf{BQSUBEXP}$ as simply '$\mathsf{BQSUBEXP}$ algorithms'.

Remark 25 *As pointed out in Bostanci et al. (2023, Section 3.2), the notion of non-uniformity here is different than that of decision problems. For state synthesis, there is a different circuit allowed for each input $x \in \{0,1\}^*$. For decision problems, there is just one circuit for all $x \in \{0,1\}^n$ and the input becomes $|x\rangle$, rather than the all-zeros state. That is, there is a non-uniform sequence $(C_n)_{n\in\mathbb{N}}$ and for $x \in \{0,1\}^n$, the output ρ_x is $C_n(|x\rangle\langle x|)$. This restriction is necessary, otherwise even the simplest of non-uniform circuits could decide all languages.*

A very important feature for us will be that circuits of bounded size will bounded description lengths.

Lemma 26 (Folklore) *For $s \geq n$, the number of unitary quantum circuits of size s with n-qubits of output can be described using at most $s \cdot (3\log_2 s + 4)$ bits.*

Proof Recall that circuit-size bounds circuit-space. Thus we can assume there are never more than $2s$ qubits (when including ancilla) at any point in the computation. As such, for every gate in a quantum circuit, we can describe its location by which gate it is among $\{H, T, \mathrm{CNOT}\}$ (and tracing out when at the end of the circuit), the qubit(s) it acts on, and what layer). Since the depth is also at most s, this requires at most 2, $2\log_2(2s)$, and $\log_2 s$ bits respectively. The whole circuit of size s can therefore be written using $s \cdot (2 + 2\log_2(2s) + \log_2 s) = s \cdot (3\log_2 s + 4)$ bits.[13] ■

Now let us generally define a set of unitary quantum circuits $\mathfrak{C}[s]$ to be the circuits in some family of size at most $O(s)$ and let

$$\mathfrak{C} \coloneqq \bigcup_p \mathfrak{C}[p]$$

for all polynomials $p : \mathbb{N} \to \mathbb{R}^+$, such that $\mathfrak{C}$ be the set of $\mathfrak{C}$-circuits of arbitrary polynomial size. For clarity, we will sometimes write $\mathfrak{C}[\mathrm{poly}(n)]$ instead.

We will give a special name to the class of all circuits produced by non-uniform polynomial-size quantum circuits.

Definition 27 ($\mathsf{stateBQP/poly}_\delta$)

$$\mathsf{stateBQP/poly}_\delta \coloneqq \bigcup_p \mathsf{stateBQSIZE}\,[p]_\delta$$

where the union is over all polynomials $p : \mathbb{N} \to \mathbb{R}^+$.

As with $\mathsf{stateBQP}$ and $\mathsf{stateBQP}_{\mathrm{exp}}$, $\mathsf{stateBQP/poly}$ and $\mathsf{stateBQP/poly}_{\mathrm{exp}}$ do not depend on the choice of universal gate set.

Theorems 3 and 2 require that $\mathfrak{C}$ be closed under restriction of qubits. That is, if $|\psi_x\rangle$ can be synthesized for inputs of length $|x| = n$, then it can also be synthesized for inputs of length $|x| < n$. This is a very natural restriction that prevents the circuit class from getting weaker when the input size increases.

Theorem 1 additionally requires for circuit class $\mathfrak{C}[s]$ that there exists some fixed constant k such that $\mathsf{pureState}\mathfrak{C}[s]_0 \in \mathsf{pureStateBQSIZE}\left[s^k\right]_\delta$ for all $s = \mathrm{poly}(n)$ and $\delta \in (0, 0.49)$. This

13. In an alternative local gate set, the $+4$ would be replaced by $2 + \lceil \log_2 G \rceil$, where G is the number of gates in the gate set. Our results should hold for any $G = O(1)$.

assumption is only needed to relate it to the results in Section D.2 and applies to a wide variety of circuit models. To instantiate this claim, we prove that it holds for two popular depth-bounded circuit classes: QNC and QAC_f as introduced by Hoyer and Spalek (2005); Moore (1999).

Definition 28 ($\mathsf{QNC}^k[s]$) *For $s : \mathbb{N} \to \mathbb{R}^+$ and $k \in \mathbb{N}$, let $\mathsf{QNC}^k[s]$ be the set of all s-size unitary circuits consisting entirely of arbitrary 1 and 2-qubit gates with depth at most $O(\log^k n)$. Then let $\mathsf{pureStateQNC}^k[s]_\delta$ be the set of state sequences that can be synthesized by a sequence of $\mathsf{QNC}^k[s]$ circuits to trace distance at most δ.*

Definition 29 ($\mathsf{QAC}^k_f[s]$) *For $s : \mathbb{N} \to \mathbb{R}^+$ and $k \in \mathbb{N}$, let $\mathsf{QAC}^k_f[s]$ be the set of all s-size unitary circuits consisting entirely of arbitrary 1 and 2-qubit gates, arbitrary $\mathrm{C}^n\mathrm{NOT}$ gates[14] and arbitrary fanout gates*

$$|b, x\rangle \mapsto |b, x \oplus b^m\rangle \text{ for } b \in \{0, 1\}, x \in \{0, 1\}^m$$

with depth at most $O(\log^k n)$. Then let $\mathsf{pureStateQAC}^k_f[s]_\delta$ be the set of state sequences that can be synthesized by a sequence of $\mathsf{QAC}^k_f[s]$ circuits to trace distance at most δ.

Note that the fanout gate only copies *classical* data, as full quantum fanout is not allowed by the no-cloning theorem. Without fanout, it would not be clear that QAC^0 (i.e., without fanout) contains AC^0. This is unlike QNC^0 trivially containing NC^0, due to the bounded fanin gates limiting the effect of unbounded fanout. Adding this fanout gate to QAC^0 has the knock-on effect that $\mathsf{AC}^0 \subsetneq \mathsf{TC}^0 \subset \mathsf{QAC}^0_f$ (Linial et al., 1993; Hoyer and Spalek, 2005; Takahashi and Seiichiro, 2016).[15]

Rosenthal (2023) showed how to simulate QAC_f circuits with QNC circuits.

Lemma 30 (Rosenthal, 2023, Lemma A.1) *For all space-s, depth-d QAC_f circuits U, there exists a space-$O(s)$, depth-$O(d \log s)$, size-$O(ds)$ QNC circuit C such that*

$$C\left(I \otimes |0 \dots 0\rangle\right) = U \otimes |0 \dots 0\rangle\,.$$

Corollary 31 *For arbitrary $\alpha \geq 1$, $k \in \mathbb{N}$, and polynomial $q : \mathbb{N} \to \mathbb{R}^+$,*

$$\mathsf{pureStateQAC}^k_f[n^\alpha]_0 \subset \mathsf{pureStateQNC}^{k+1}\left[n^\alpha \cdot \log^k n\right]_0$$

and

$$\mathsf{pureStateQNC}^k\left[n^\alpha\right]_0 \subset \mathsf{pureStateBQSIZE}\left[n^\alpha q^{1.441} \log^{1.441} n\right]_{\exp(-q)}\,.$$

Proof The first statement comes directly from Lemma 30.

Two show the second statement, we note that the Solovay-Kitaev algorithm allows us to approximate arbitrary 1 and 2 qubit gates to $\exp(-q)/n^\alpha = \exp\left(-O(q \log n)\right)$ accuracy in operator norm using at most $q^4 \log^4 n$ gates. Let C be an arbitrary circuit in $\mathsf{QNC}^k[n^\alpha]$. By applying Solovay-Kitaev to each gate in C and then taking the triangle inequality over all n^α gates we can construct

14. $\mathrm{C}^1\mathrm{NOT}$ is simply the CNOT gate and $\mathrm{C}^2\mathrm{NOT} = \mathrm{CCNOT}$ is the Toffoli gate.
15. TC^k is the set of $\mathrm{poly}(n)$-size classical circuits of unbounded fan-in AND, OR, NOT, and threshold gates of $O(\log^k n)$ depth.

a unitary approximation $\widehat{C}$ such that $\|C - \widehat{C}\|_\infty \le \exp(-q)$ using at most $O\left(n^\alpha q^{1.441} \log^{1.441} n\right)$ gates. Due to the Fact 14 and nature of the operator norm,

$$d_{\mathrm{tr}}(C\,|\psi\rangle\,, \widehat{C}\,|\psi\rangle) \le \|C\,|\psi\rangle - \widehat{C}\,|\psi\rangle\|_2 \le \exp(-q)$$

for all $|\psi\rangle$. Therefore $\mathsf{pureStateQNC}^{k+1} \subset \mathsf{pureStateBQSIZE}\left[n^\alpha q^{1.441} \log^{1.441} n\right]_{\exp(-q)}$. ■

By Corollary 31, setting $q = \log 100$ gives us

$$\mathsf{pureStateQNC}^k[n^\alpha]_0 \subset \mathsf{pureStateBQSIZE}\left[n^{\alpha+\varepsilon}\right]_{0.01}$$

and

$$\mathsf{pureStateQAC}_f^k[n^\alpha]_0 \subset \mathsf{pureStateBQSIZE}\left[n^{\alpha+\varepsilon}\right]_{0.01}$$

for arbitrary $\varepsilon > 0$.

A.4. Decision Problem Complexity Classes

We can also define the more traditional complexity classes using this language. Given a language $L \subseteq \{0,1\}^*$, let the one-qubit state $|x \in L\rangle$ be defined as

$$|x \in L\rangle := \begin{cases} |1\rangle & x \in L \\ |0\rangle & x \notin L \end{cases}.$$

For a *uniform* state synthesis class stateA_δ, we take decision class A to be the set of languages $L \subseteq \{0,1\}^*$ where there exists a state sequence $(\rho_x) \in \mathsf{stateA}_0$ such that for all $x \in \{0,1\}^*$,

$$\mathrm{tr}\left[|x \in L\rangle\!\langle x \in L| \cdot \rho_x\right] \ge \frac{2}{3}.$$

For a circuit class $\mathfrak{C}[s]$, we take the *non-uniform* decision class $\mathfrak{C}$ to be the set of languages $L \subseteq \{0,1\}^*$ where there exists a $\mathfrak{C}[\mathrm{poly}(n)]$-circuit sequence $(C_n)_{n\in\mathbb{N}}$ such that for all $x \in \{0,1\}^*$,

$$\mathrm{tr}\left[|x \in L\rangle\!\langle x \in L| \cdot C_n(|x\rangle\!\langle x|)\right] \ge \frac{2}{3}.$$

We now define explicitly define some decision classes that will be used in our proofs, namely in Section E.

Definition 32 (PSPACE) *We define* PSPACE *to be the set of languages that can be decided by a deterministic Turing machine that uses at most* $\mathrm{poly}(n)$ *space.*[16]

Definition 33 (BQTIME) *We define* $\mathsf{BQTIME}\left[f\right]$ *to be the set of languages, that can be decided by an* f*-time-uniform general quantum circuit with one qubit of output.*[17] *I.e., for a language* $L \in \mathsf{BQTIME}\left[f(n)\right]$ *there exists a* $(\rho)_x \in \mathsf{BQTIME}\left[f(n)\right]_0$ *such that*

$$\mathrm{tr}\left[|x \in L\rangle\!\langle x \in L| \cdot \rho_x\right] \ge \frac{2}{3}$$

for all $x \in \{0,1\}^*$.

16. Note that $\mathsf{PSPACE} = \mathsf{BQPSPACE}$ (Watrous, 1999, 2003).
17. We note that our definition uses general quantum circuits, while many others (critically Arunachalam et al. (2022b)) use *unitary* quantum circuits, rather than general, where the measurement is only implicitly done at the very end. Since we are now only concerned with measurement statistics, the Principle of Deferred Measurement shows that these are equivalent definitions.

Definition 34 ($\mathsf{BQSIZE}[s]$) *We define* $\mathsf{BQSIZE}[s]$ *to be the set of languages that can be decided by non-uniform quantum circuits in the* $\{H, \mathrm{CNOT}, T\}$ *gate set with size at most* $O(s)$.

Finally, we define complexity classes for deterministic computation.

Definition 35 (DTIME) *We define* $\mathsf{DTIME}[f]$ *to be the set of languages, that can be decided by deterministic Turing machine in time* $O(f)$.

We will specifically take $\mathsf{E} := \mathsf{DTIME}\left[2^{O(n)}\right]$, and $\mathsf{BQSUBEXP} := \bigcap_{\gamma \in (0,1)} \mathsf{BQTIME}\left[2^{n^\gamma}\right]$.

Appendix B. Pseudorandomness

In the theory of pseudorandomness, one aims to efficiently construct states that cannot be distinguished from something that is true uniform random (under varying notions of what randomness means). The strongest form of pseudorandomness would be *statistical* pseudorandomness, such that the object is statistically close to true random. In this way, even an adversary with unbounded computational time cannot distinguish the pseudorandom object. Examples of this include k-wise independent distributions (Alon et al., 2007) and unitary t-designs (Dankert et al., 2009; Oszmaniec et al., 2024).

Unfortunately, constructing such objects can be prohibitively expensive. Instead, we will settle on a weaker, but still very powerful, notion of *computational* pseudorandomness whereby any computationally bounded adversary cannot distinguish the pseudorandom object from true random. The goal will be to construct a set of states that looks like a Haar random state to any observer with at most $2^{n^{2\lambda}}$ time for $\lambda \in (0, 1/5)$ (see Definition 37). The step was analogously done in Arunachalam et al. (2022b) for distributions over bitstrings (i.e., a pseudorandom generator Definition 36), where they impressively gave a conditional PRG with near-optimal stretch with security against $2^{n^{2\lambda}}$-time *quantum* adversaries (see Lemma 45). In fact, we will bootstrap their construction in order to synthesize a set of pseudorandom quantum states.

Let us start by defining a pseudorandom generator (PRG) and a pseudorandom state (PRS), which is a more recent object due to Ji et al. (2018). Recall that for a function f acting on the natural numbers, we implicitly take f to be $f(n)$ for input size n.

Definition 36 (PRG) *Let* $\ell, m : \mathbb{N} \to \mathbb{N}$*, let* $s : \mathbb{N} \to \mathbb{R}^+$*, and let* $\varepsilon : \mathbb{N} \to [0, 1]$*. We say that a family of functions* $\left(G : \{0,1\}^\ell \to \{0,1\}^m\right)_{n \in \mathbb{N}}$ *is a infinitely-often* $(\ell, m, s, \varepsilon)$*-PRG against* uniform *quantum algorithms if no quantum algorithm running in time s can distinguish* $G_n(x)$ *from* y *by at advantage at most* ε*, where* x *is drawn uniformly from* $\{0,1\}^\ell$ *and* y *is drawn uniformly from* $\{0,1\}^m$*. Formally, for all single-qubit sequences* $(\rho_x)_{x \in \{0,1\}^*} \in \mathsf{stateBQTIME}[s]_0$*:*

$$\left| \underset{x \sim \{0,1\}^\ell}{\boldsymbol{E}} \operatorname{tr}\left[|1\rangle\!\langle 1| \cdot \rho_{G_n(x)}\right] - \underset{y \sim \{0,1\}^m}{\boldsymbol{E}} \operatorname{tr}[|1\rangle\!\langle 1| \cdot \rho_y] \right| \leq \varepsilon$$

holds on infinitely many $n \in \mathbb{N}$.

Definition 37 (PRS) *Let* $\kappa, \ell, m : \mathbb{N} \to \mathbb{N}$*, let* $s : \mathbb{N} \to \mathbb{R}^+$*, and let* $\varepsilon : \mathbb{N} \to [0, 1]$*. We say that a sequence of keyed pure states* $\left(\{|\psi_k\rangle\}_{k \in \{0,1\}^\kappa}\right)_{n \in \mathbb{N}}$ *is an infinitely-often* $(\kappa, \ell, m, s, \varepsilon)$*-PRS if for a uniformly random* $k \in \{0,1\}^\kappa$*, no quantum algorithm running in time* s *can distinguish* m

samples of $|\psi_k\rangle$ from m samples of a Haar random state on ℓ qubits by at most ε. Formally, for all s-time-uniform quantum circuits $(C_n)_{n\in\mathbb{N}}$ with one qubit of output:

$$\left| \underset{k\sim\{0,1\}^\kappa}{\boldsymbol{E}} \operatorname{tr}\left[|1\rangle\langle 1| \cdot C_n\left(|\psi_k\rangle\langle\psi_k|^{\otimes m}\right)\right] - \underset{|\psi\rangle\sim\mu_{\text{Haar}}}{\boldsymbol{E}} \operatorname{tr}\left[|1\rangle\langle 1| \cdot C_n\left(|\psi\rangle\langle\psi|^{\otimes m}\right)\right] \right| \le \varepsilon$$

holds on infinitely many $n \in \mathbb{N}$.

We will generally refer to the difference in expectation between the adversary on a pseudorandom object and the adversary on a true random object as the *advantage*.

Note that we can consider the *partial* pure state sequence $(|\varphi_x\rangle)_{n\in\mathbb{N},x\in\{0,1\}^{\kappa(n)}}$, which only holds for the image of κ such that $|\varphi_x\rangle = |\psi_k\rangle$ from $\left(\{|\psi_k\rangle\}_{k\in\{0,1\}^\kappa}\right)_{n\in\mathbb{N}}$. By trivially letting $|\varphi_x\rangle$ be the zero state for input lengths outside the image of κ we get a full state sequence $(|\varphi'_x\rangle)_{x\in\{0,1\}^*}$ such that

$$|\varphi'_x\rangle = \begin{cases} |\psi_x\rangle & \exists y \in \mathbb{N}, |x| = \kappa(y) \\ |0\rangle & \text{otherwise} \end{cases}.$$

Therefore, if the PRS $\left(\{|\psi_k\rangle\}_{k\in\{0,1\}^\kappa}\right)_{n\in\mathbb{N}}$ can be δ-approximately synthesized in time $t : \mathbb{N} \to \mathbb{R}^+$ relative to the security parameter n, then $(|\varphi'_x\rangle) \in \mathsf{pureStateBQTIME}\left[t \circ \kappa^{-1}\right]_\delta$. Likewise, if the PRS $\left(\{|\psi_k\rangle\}_{k\in\{0,1\}^\kappa}\right)_{n\in\mathbb{N}}$ can be δ-approximately synthesized by non-uniform circuit class $\mathfrak{C}[s(n)]$, then $(|\varphi'_x\rangle) \in \mathsf{pureState}\mathfrak{C}\left[s \circ \kappa^{-1}\right]_\delta$. In an abuse of notation, we will often just refer to $(|\varphi'_x\rangle)$ as the PRS.

In order to construct our pseudorandom states we will need to go through an intermediary pseudorandom object called a pseudorandom function, which we will work to define now.

Definition 38 (Quantum Oracle) *Given a function $f : \{0,1\}^\ell \to \{0,1\}^m$, we define the quantum oracle for f to be*

$$\mathcal{O}_f := \sum_{\substack{x\in\{0,1\}^\ell \\ y\in\{0,1\}^m}} |x, y \oplus f(x)\rangle\langle x, y| .$$

We define an oracle circuit, $C^{(\cdot)}$, to be a general quantum circuit with n-qubit placeholder unitary $(\cdot)$ such that $C^{\mathcal{O}}$ is the instantiation of the circuit but with each placeholder replaced by the n-qubit gate $\mathcal{O}$. We refer to s-time-uniform *oracle* quantum circuits as $(C_n^{(\cdot)})_{n\in\mathbb{N}}$.

Denote $\mathfrak{F}_{\ell,m} := \{f : \{0,1\}^\ell \to \{0,1\}^m\}$ as the set of all functions from ℓ-bits to m-bits.

Definition 39 (PRF) *Let $\kappa, \ell, m : \mathbb{N} \to \mathbb{N}$, let $q, s : \mathbb{N} \to \mathbb{R}^+$, and let $\varepsilon : \mathbb{N} \to [0,1]$. We say that a sequence of keyed-functions $\left(\{F_k \in \mathfrak{F}_{\ell,m}\}_{k\in\{0,1\}^\kappa}\right)_{n\in\mathbb{N}}$ is an infinitely-often $(\kappa, \ell, m, q, s, \varepsilon)$-PRF if for a uniformly random $k \in \{0,1\}^\kappa$, no quantum algorithm running in time s can distinguish black-box access to $\mathcal{O}_{F_k}$ from black-box access to $\mathcal{O}_f$ for random function $f \in \mathfrak{F}_{\ell,m}$ using at most q queries by at most ε. Formally, for all s-time-uniform oracle quantum circuits $(C_n^{(\cdot)})_{n\in\mathbb{N}}$ such that each $C_n^{\mathcal{O}}$ takes no inputs, queries $\mathcal{O}$ at most q times, and outputs a single qubit state $\rho_n^{\mathcal{O}}$:*

$$\left| \underset{k\sim\{0,1\}^\kappa}{\boldsymbol{E}} \operatorname{tr}\left[|1\rangle\langle 1| \cdot \rho_n^{\mathcal{O}_{F_k}}\right] - \underset{f\sim\mathfrak{F}_{\ell,m}}{\boldsymbol{E}} \operatorname{tr}\left[|1\rangle\langle 1| \cdot \rho_n^{\mathcal{O}_f}\right] \right| \le \varepsilon$$

holds on infinitely many $n \in \mathbb{N}$.

The reason we need these pseudorandom functions, is that there does not seem to be a direct quantum-secure PRG-to-PRS construction in the literature. There are, however, known constructions of a quantum-secure PRF given a quantum-secure PRG as well as a PRS given a quantum-secure PRF. We formalize these statements as follows, stated carefully for even sub-exponential time quantum adversaries.

We start with a PRG-to-PRF construction that works especially well when the stretch of the PRG is very large. A similar idea was used by Arunachalam et al. (2022b, Theorem 3.4), where the output of a PRG is viewed as the truth table of the function. Thus, if the stretch in the PRG G was the ideal $\{0,1\}^n \to \{0,1\}^{2^n}$ then one could view the string $G(k)$ as the truth table for a function $F_k : \{0,1\}^n \to \{0,1\}$.

Lemma 40 *Let G be an infinitely-often $(\kappa, m, s, \varepsilon)$-PRG against uniform quantum computations that is computable in time t by a deterministic Turing machine. Then for $\ell \leq \lfloor \log_2 \frac{m}{d} \rfloor$ there exists an infinitely-often $(\kappa, \ell, d, q, s - O(q \cdot m), \varepsilon)$-PRF against uniform quantum computations that can be computed in time $O(t)$.*

Proof Observe that when given a string $s \in \{0,1\}^{2^{k+d}}$ for some $k \in \mathbb{N}$, we can view it as the truth table of a function $\mathrm{fnc}^s : \{0,1\}^k \to \{0,1\}^d$ such that $\mathrm{fnc}^s(x)$ is the x^{th} d-bit block of s. Furthermore, if s is a uniformly random string then fnc^s is a random function in $\mathfrak{F}_{k,d}$. Therefore, let $G' : \{0,1\}^\kappa \to \{0,1\}^{2^{\ell+d}}$ compute the first $2^{\ell+d}$ bits (note that $2^{\ell+d} \leq m$) of the output of G. Then we define our PRF to be $F_k(x) = \mathrm{fnc}^{G'(k)}(x)$. Note that $F_k(x)$ can be computed in time $O(t + 2^{\ell+d}) = O(t)$, because $t = \Omega(m) = \Omega\big(2^{\ell+d}\big)$ as it always takes at least $\Omega(m)$ time to just write down the output string.

Let n be some hard instance for G. If we consider an adversary $\mathcal{A}$ for G that, given either a uniform output of $G(x)$ or a truly random string, by truncating to the first $2^{\ell+d}$ bits it will have the truth table to either some F_k or a random $f \in \mathfrak{F}_{\ell,d}$. If there existed a distinguisher $\mathcal{B}$ for $\{F_k\}$ in time $s - O\,(q \cdot m)$ and advantage ε, then $\mathcal{A}$ could simulate the q queries to O_{F_k} or O_f respectively in time $O(q \cdot m)$ and therefore distinguish G from a random string in time s with advantage ε as well. By contradiction, this means that $\{F_k\}$ must be an infinitely-often $(\kappa, \ell, d, q, s - O(q \cdot m), \varepsilon)$-PRF against uniform quantum computations. ■

Note that using something like the Goldreich, Goldwasser, and Micali (1984) construction, which is known to be quantum-secure (Zhandry, 2021, Theorem 5.5), is insufficient for our purposes. This is because the Goldreich, Goldwasser, and Micali (1984) construction of PRFs requires running the PRG multiple times. Since the PRG in our specific setting is more expensive to compute than the adversaries it is secure against (see Lemma 45), the usual way to distinguish the PRG will take more time than is allowed to break the security of the PRG. Specifically, let's say that we are given a secure PRG $G : \{0,1\}^\kappa \to \{0,1\}^{2\kappa}$ that is fed into the Goldreich, Goldwasser, and Micali (1984) PRG-to-PRF construction to arrive at function $F \coloneqq \{F_k \in \mathfrak{F}_{\kappa,\kappa}\}_{k \in \{0,1\}^\kappa}$, and assume for contradiction that F is not pseudorandom. Zhandry (2021) shows that by using $O(\kappa)$ queries to G, one can turn the distinguisher for F into a distinguisher for G. This would (in most settings) contradict G being a PRG, so F must also be pseudorandom. However, since our PRG in Lemma 45 requires time $O(2^\kappa)$ to compute, this forces the Zhandry (2021) distinguisher for G to run in time $\Omega(\kappa \cdot 2^\kappa)$, regardless of how fast the assumed distinguisher for F is. Since the PRG in Lemma 45 is only secure against adversaries that run in time $o(2^\kappa)$, our distinguisher does not actually break the proven security guarantees, so no contradiction is made and we cannot assume that F is pseudorandom! Meanwhile, observe that in Lemma 40 we don't need additional queries to G , thus making the algorithm to break the security of the underlying PRG remain "efficient".

To get a PRS from a Boolean output PRF, we utilize the following result of Brakerski and Shmueli (2019) that gives an information theoretic hardness of distinguishing random binary phase states from Haar random states.

Definition 41 (Phase State) *For $f:\{0,1\}^n \to \{0,1\}$, define n-qubit state $|f\rangle$ as:*

$$|f\rangle := \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} (-1)^{f(x)} |x\rangle .$$

Lemma 42 (Brakerski and Shmueli, 2019, Theorem 1) *For all $t \in \mathbb{R}^+$, m-copies of $|f\rangle$, for f chosen uniformly from $\mathfrak{F}_{n,1}$, cannot be distinguished from m-copies of a Haar random state by any (potentially computationally unbounded) adversary by advantage at most $\frac{4m^2}{2^n}$.*

Lemma 43 (Generalization of Brakerski and Shmueli, 2019, Section 3.1) *Let $(\{F_k\})$ be an infinitely-often $(\kappa, \ell, 1, m, s, \varepsilon)$-PRF against uniform quantum computations that can be computed in time t. Then there exists an infinitely-often $\left(\kappa, \ell, m, s - O(\ell), \varepsilon + \frac{4m^2}{2^\ell}\right)$-PRS against uniform quantum computations that can be synthesized* exactly *in time $O(t+\ell)$ in the $\{H, \mathrm{CNOT}, T\}$ gate set.*

Proof Recall that any efficient classical computation can be exactly expressed as a similarly efficient quantum circuit in the $\{H, \mathrm{CNOT}, T\}$ gate set. Thus, initializing the state $|0^\ell\rangle|1\rangle$, we can apply $H^{\otimes(\ell+1)}$ then O_{F_k} to get

$$\frac{1}{\sqrt{2^\ell}} \sum_{x\in\{0,1\}^\ell} (-1)^{F_k(x)} |x\rangle |-\rangle$$

without any errors. Tracing out the last qubit gives us $|F_k\rangle$. This takes time at most $O(\ell + t)$. Furthermore, for arbitrary function $f \in \mathfrak{F}_{\ell,1}$, if O_f is given as a black-box that takes $O(1)$ time, then this becomes time $O(\ell)$ and uses only a single query.

If $(\{F_k\}_{k\in\{0,1\}^\kappa})_{n\in\mathbb{N}}$ represents the $(\kappa, \ell, 1, m, s, \varepsilon)$-PRF, we now claim that $(\{|F_k\rangle\})$ forms our desired PRS. First, let $n \in \mathbb{N}$ be an arbitrary "hard" instance of the infinitely-often PRF. We define 3 states

$$\rho^m_{\text{PRS}} := \mathop{\mathbf{E}}_{k\sim\{0,1\}^\kappa} \left[|F_k\rangle\langle F_k|^{\otimes m}\right], \quad \rho^m_{\text{phase}} := \mathop{\mathbf{E}}_{f\sim\mathfrak{F}_{\ell,1}} \left[|f\rangle\langle f|^{\otimes m}\right], \quad \rho^m_{\mu_{\text{Haar}}} := \mathop{\mathbf{E}}_{|\psi\rangle\sim\mu_{\text{Haar}}} \left[|\psi\rangle\langle\psi|^{\otimes m}\right]$$

and show that they cannot be easily distinguished by an $[s - O(\ell)]$-time quantum algorithm. By Definition 39 and the fact that $|f\rangle$ can be constructing in $O(\ell)$ time and a single query from O_f, ρ^m_{PRS} and ρ^m_{phase} respectively cannot be distinguished by more than ε in time $s - O(\ell)$. By applying Lemma 42, ρ^m_{phase} and $\rho^m_{\mu_{\text{Haar}}}$ cannot be distinguished by *any* adversary with advantage more than $\frac{4m^2}{2^\ell}$. Using the reverse triangle inequality, an $[s - O(\ell)]$-time algorithm that distinguishes between ρ^m_{PRS} and $\rho^m_{\mu_{\text{Haar}}}$ with advantage $\varepsilon + \frac{4m^2}{2^\ell}$ would imply an $[s - O(\ell)]$-time distinguisher for ρ^m_{PRS} and ρ^m_{phase} with advantage ε, a contradiction. Therefore $(\{|F_k\rangle\}_{k\in\{0,1\}^\kappa})_{n\in\mathbb{N}}$ forms an infinitely-often $\left(\kappa, \ell, m, s - O(\ell), \varepsilon + \frac{4m^2}{2^\ell}\right)$-PRS against uniform quantum computations ■

Remark 44 *In a different gate set, a quantum adversary may not necessarily be able to exactly prepare the binary phase state (see Definition 41). Because the adversary in Lemma 43, when given* O_f*, only needs to apply* $n+1$ *Hadamard gates and a single* X *gate to prepare* $|f\rangle$*, the Solovay-Kitaev algorithm ensures that* $|f\rangle$ *can be prepared in any universal gate set to trace distance* $\exp(-k)$ *using* $O\left(k^{1.441} + \log^{1.441} n\right)$ *extra time. By the reverse triangle inequality, contractivity of trace distance under trace-preserving completely positive maps, and Fact 10, this would turn the PRS in Lemma 43 into an infinitely-often* $\left(\kappa, \ell, m, s - O\left(\ell + k^{1.441} + \log^{1.441} n\right), \varepsilon + \frac{4m^2}{2^\ell} + \exp(-k)\right)$*-PRS against uniform quantum computation for all* $k \in \mathbb{N}$*. We will choose to ignore this effect because (1) when used for our purposes,* $k = \Theta(\ell)$ *and* $\ell = \omega(\mathrm{poly}\log n)$ *such that the effect will be negligible and (2) it is not such a strong assumption that the universal gate set used instead can still exactly create the Hadamard gate and* X *gate in constant size.*

B.1. Pseudorandom Objects From Decision Problem Separations

We finally state the critical result of Arunachalam et al. (2022b), which showed how to produce a nearly-optimal quantum-secure PRG given a complexity theoretic assumption. By combining Lemmas 45, 40 and 43 we get our desired final result of a conditional PRS that is secure even against sub-exponential time adversaries that can be constructed in $2^{O(n)}$ time.

Lemma 45 (Arunachalam et al., 2022b, Theorem 3.2, Theorem 5.1) *Suppose there exists a* $\gamma > 0$ *such that* $\mathsf{PSPACE} \not\subset \mathsf{BQTIME}\left[2^{n^\gamma}\right]$*. Then, for some choice of constants* $\alpha \geq 1$ *and* $\lambda \in (0, 1/5)$*, there exists an infinitely-often* $(\ell, m, s, 1/m)$*-PRG against uniform quantum computations where* $\ell(n) \leq n^\alpha$*,* $m(n) = \lfloor 2^{n^\lambda} \rfloor$*, and* $s(n) = 2^{n^{2\lambda}}$*.*

In addition, the PRG is computable by a deterministic Turing machine in time $O\left(2^\ell\right)$*.*

In the following statements and proofs of Corollaries 46 and 47, note that $r(n)$ takes the place of $m(n)$, and $\kappa(n)$ takes the place of $\ell(n)$ in the Lemma 45.

Corollary 46 *Suppose there exists a* $\gamma > 0$ *such that* $\mathsf{PSPACE} \not\subset \mathsf{BQTIME}\left[2^{n^\gamma}\right]$*. Then, for some choice of constants* $\alpha \geq 1$ *and* $\lambda \in (0, 1/5)$*, there exists an infinitely-often*

$$(\kappa, \ell, 1, q, s - O\left(q \cdot r\right), 1/r)\text{-}\mathit{PRF}$$

against uniform quantum computations where $\kappa(n) \leq n^\alpha$*,* $r(n) = \lfloor 2^{n^\lambda} \rfloor$*,* $\ell \leq \lfloor \log_2 r \rfloor$*, and* $s(n) = 2^{n^{2\lambda}}$*.*

In addition, the PRF is computable by a deterministic Turing machine in time $O\left(2^\kappa\right)$*.*

Proof By Lemma 45, there exists an infinitely-often $(\kappa, r, s, 1/r)$-PRG against uniform quantum computations that can be computed in time $O\left(2^\kappa\right)$. Applying Lemma 40, there must exist an infinitely-often

$$(\kappa, \ell, 1, q, s - O\left(q \cdot r\right), 1/r)\text{-PRF}$$

against uniform quantum computations that can be computed in time $O(2^\kappa)$. ■

Corollary 47 *Suppose there exists a $\gamma > 0$ such that $\mathsf{PSPACE} \not\subset \mathsf{BQTIME}\left[2^{n^\gamma}\right]$. Then, for some choice of constants $\alpha \geq 1$ and $\lambda \in (0, 1/5)$, there exists an infinitely-often*

$$\left(\kappa, \ell, m, s - O(m \cdot r), \frac{1}{r} + \frac{4m^2}{2^\ell}\right)\text{-PRS}$$

against uniform quantum computations where $\kappa(n) \leq n^\alpha$, $r(n) = \lfloor 2^{n^\lambda} \rfloor$, $\ell \leq \lfloor \log_2 r \rfloor$, and $s(n) = 2^{n^{2\lambda}}$.

In addition, the PRS can be exactly *synthesized in time $O\left(2^\kappa\right)$ in the $\{H, \mathrm{CNOT}, T\}$ gate set.*

Proof We can utilize Corollaries 46 and 43 to show that there must exist an infinitely-often

$$\left(\kappa, \ell, m, s - O(m \cdot r + \ell), \frac{4m^2}{2^\ell} + \frac{1}{r}\right)\text{-PRS}$$

against uniform quantum computations that can be exactly constructed in time $O\left(2^\kappa\right)$ in the $\{H, \mathrm{CNOT}, T\}$ gate set.

■

B.2. Pseudorandom States From State Synthesis Separations

We note that Corollary 47 relies on a separation between decision problem complexity class separations. However, it will be important for us to condition on state synthesis class separations instead for the win-win argument in our main result Theorem 65. Observe that, while decision problem separations between uniform models of computation immediately imply state synthesis separations, the converse is not always clear. However, if the size of the circuits are not too large then we can say the following.

Lemma 48 *Let $k : \mathbb{N} \to \mathbb{R}^+$. For any $\mathsf{stateA}_\delta \subset \mathsf{stateBQP/poly}_\delta$, if $\mathsf{stateA}_\delta \not\subset \mathsf{stateBQTIME}\left[k \cdot f\right]_{\delta + \exp(-k)}$ then $\mathsf{A} \not\subset \mathsf{BQTIME}\left[\frac{f}{n^\nu}\right]$ for some $\nu \geq 1$.*

Proof By assumption, there exists some fixed state sequence $\{\rho_x\}_{x \in \{0,1\}^n} \in \mathsf{stateA}_\delta$ synthesized by a sequence of s-size unitary circuits $(C_x)_{x \in \{0,1\}^*}$ to accuracy δ for $s = \mathrm{poly}(n)$ and sufficiently large n. On the other hand, no circuit sequence that can be described by a deterministic Turing machine using $O(k \cdot f)$ time can approximately synthesize $\{\rho_x\}_{x \in \{0,1\}^n}$ to even $\delta + \exp(-k)$ accuracy in trace distance such that $\{\rho_x\}_{x \in \{0,1\}^n} \notin \mathsf{stateBQTIME}\left[k \cdot f\right]_{\delta + \exp(-k)}$. By Lemma 26, the description length of each C_x is at most $d := O(s \log s)$ and define $\nu \geq 1$ to be some constant such that $d \log d \leq n^\nu$. We now define the language L on $n' := n + \lceil \log_2 d \rceil = O(n)$ bits to be the problem of: Given inputs $x \in \{0,1\}^n$ and $i \in \{0, 1, \ldots, d-1\}$ (encoded in binary), output the i-th bit of the circuit description of C_x. L is trivially in A, and we will now show that $L \notin \mathsf{BQTIME}\left[f\right]$.

Observe that if L could be decided in *deterministic* f time then the whole circuit description of C_x could learned by iterating through all d possible values of i, giving an $O(d \cdot f)$-time algorithm to describe the synthesis circuit for each $|\psi_x\rangle$. This naïvely implies that $\mathsf{A} \not\subset \mathsf{DTIME}\left[\frac{f}{d}\right]$, where DTIME is the classical deterministic version of BQTIME. We now need to argue that not even a *quantum* algorithm could succeed.

For the sake of contradiction, suppose on inputs (x, i) of length n' that there did exist an $\frac{f}{n^\nu}$-time-uniform general quantum circuit U that decided L (i.e., $L \in \mathsf{BQTIME}\left[\frac{f}{n^\nu}\right]$). Using standard error reduction for decision problems we can construct a quantum circuit U' such that it has at most an $\exp(-2k)$ failure probability, with a multiplicative overhead of $O(k)$. Then, via the union bound, there exists a quantum circuit V that uses U' as a sub-routine and, for a fixed $x \in \{0,1\}^n$, iterates through all of the various possible bits i to learn the entire description of C_x with at most an $\exp(-2k)$ failure probability and an additional $O(d \log d)$ multiplicative overhead.[18] This is equivalent to saying that the fidelity with $|\textsc{desc}(U)\rangle$ is at least $1 - \exp(-2k)$, so by the upper bound of Fact 12, there is at most an $\exp(-k)$ trace distance to the computational basis state with the correct description of $\textsc{desc}(C_x)$). In $O(d \log d)$ time, the algorithm can then utilize Fact 19 to apply C_x to a set of ancillary qubits, then trace out the qubits holding the description. By the Fact 10, our output state will have distance at most $\exp(-k)$ from the output state of C_x. Finally, by the triangle inequality and the accuracy of (C_x) in synthesizing (ρ_x) to distance δ, the resulting output quantum state $\widehat{\rho}_x$ will then have

$$d_{\mathrm{tr}}(\rho_x, \widehat{\rho}_x) \leq \delta + \exp(-k)$$

for all sufficiently large n.

Overall, for all sufficiently large n and arbitrary $x \in \{0,1\}^n$, a circuit that approximates ρ_x to $\delta + \exp(-k)$ trace distance can be output by a deterministic Turing machine running in $O\left(kf\frac{d\log d}{n^\nu}\right) = O(k \cdot f)$ time such that $(\rho_x) \in \mathsf{stateBQTIME}\left[k \cdot f\right]_{\mathrm{exp}}$. This is a contradiction of our initial assumption and it follows that $L \notin \mathsf{BQTIME}\left[f\right]$ even though $L \in \mathsf{A}$. ■

Remark 49 *We note that the proof of Lemma 48 can also be used to show that* $\mathsf{stateA}_\delta \not\subset \mathsf{stateBQTIME}[f]_\delta$ *implies* $\mathsf{A} \not\subset \mathsf{EQTIME}[f]$ *where* EQTIME *is the set of languages that can be* exactly *decided by f-time-uniform quantum circuits. This is because U, the circuit that previously decided L with bounded error will have no error when used in contradiction. The resulting circuit V that finds the description of C_x will then also have no error.*

The following is a consequence of Lemma 48, written in a way to most easily use in proving our main result Theorem 65.

Corollary 50 *Suppose there exists a $\gamma > 0$ such that* $\mathsf{pureStatePSPACESIZE}_0 \not\subset \mathsf{pureStateBQTIME}\left[2^{n^\gamma}\right]_{\mathrm{exp}}$. *Then for every $c \geq 1$, for some choice of constants $\alpha \geq 1$ and $\lambda \in (0, 1/5)$ and sufficiently large $n \in \mathbb{N}$, there exists an infinitely-often*

$$\left(\kappa, \lfloor \log_2 r \rfloor^{1/c}, m, s, \frac{4m^2}{2^\ell} + \frac{1}{r}\right)\textit{-PRS}$$

against uniform quantum computations where $\kappa \leq n^\alpha$, $r = \lfloor 2^{n^\lambda} \rfloor$, $s = 2^{n^{2\lambda}}$, and $m = o\left(\frac{s}{r}\right)$. In addition, the PRS lies in $\mathsf{pureStateBQE}_{\mathrm{exp}}$.

18. We note that Toffoli gates, which are classically universal, can be built exactly in the $\{H, \mathrm{CNOT}, T\}$ gate set (Welch et al., 2016).

Proof Observe by Definition 23 that $\mathsf{pureStatePSPACESIZE}_\delta \subset \mathsf{stateBQP/poly}_\delta$. By Lemma 48 and the contrapositives of Facts (ii) and (iii) respectively, $\mathsf{PSPACE} \not\subset \mathsf{BQTIME}\left[\frac{2^{n^\gamma}}{\mathrm{poly}(n)}\right]$. This further implies $\mathsf{PSPACE} \not\subset \mathsf{BQTIME}\left[2^{n^{0.99\cdot\gamma}}\right]$, such that we now invoke Corollary 47 with $m = o\left(\frac{s}{r}\right)$. ■

Appendix C. Quantum State Learning

In this section, we prove that any sub-exponential time quantum state tomography for a class of *pure* states implies the ability to distinguish said class of states from Haar random in sub-exponential time. This ultimately implies that any sequence of pure states that efficiently learned cannot be used to form a sub-exponential-time-secure PRS ensemble, which will be necessary for proving a contradiction in Section E. As will be explained shortly, since the task can always be done in exponential samples (and exponential time), the informal takeaway is that slightly non-trivial learning algorithms imply some sort of lower bound against PRS constructions (with the more non-trivial learning algorithms leading to better lower bounds).

Note that Zhao et al. (2023, Theorem 14) and Ji et al. (2018, Theorem 2) make similar statements. We supplement them with a simple proof that is both tighter and more fine-grained in parameters of the adversary. See Theorem 6 for a discussion of the differences and why proving Lemma 55 was necessary for our purposes.

We begin by defining what it means to learn a quantum pure state in the tomographical sense.

Definition 51 *Let $\mathcal{C}_n$ be a class of n-qubit* pure *quantum states and let $\mathcal{C} = \bigcup_{n\geq 1} \mathcal{C}_n$. We say that $\mathcal{C}$ is $(m, t, \varepsilon, \delta)$-learnable if there exists a t-time-general quantum circuit family $(C_n)_{n\in\mathbb{N}}$ that, with probability at least $1-\delta$, running C_n on m samples of $|\psi\rangle \in \mathcal{C}_n$ outputs the* description *of a unitary circuit that prepares a state $\widehat{\rho}$ such that $d_{\mathrm{tr}}(|\psi\rangle\!\langle\psi|, \widehat{\rho}) \leq \varepsilon$.*

We now introduce a weaker form of learning, which simply involves distinguishing a state from $\mathcal{C}$ from a Haar random state. Informally, distinguishing is the task of breaking pseudorandom states. As such, this will be the true notion of learning that will drive our results.

Definition 52 *Let $\mathcal{C}_n$ be a class of n-qubit quantum states and let $\mathcal{C} = \bigcup_{n\geq 1} \mathcal{C}_n$. We say that $\mathcal{C}$ is (m, t, ε)-distinguishable if there exists a t-time-uniform quantum circuit family with one bit of output $(C_n)_{n\in\mathbb{N}}$ that satisfies the following: For all sufficiently large $n \in \mathbb{N}$, for every $\rho \in \mathcal{C}_n$,*

$$\left| \mathrm{tr}\left[|1\rangle\!\langle 1| \cdot C_n\left(\rho^{\otimes m}\right)\right] - \mathop{\boldsymbol{E}}_{|\psi\rangle\sim\mu_{\mathrm{Haar}}} \mathrm{tr}\left[|1\rangle\!\langle 1| \cdot C_n\left(|\psi\rangle\!\langle\psi|^{\otimes m}\right)\right] \right| \geq \varepsilon.$$

Note the difference between this and a PRS, where the distinguishing needs to hold for worst-case ρ, rather than in average-case. We could have defined a model of learning/distinguishing that applied in average-case over all sufficiently large subsets of $\mathcal{C}$. However, this notion does not seem to be as common in the quantum state learning literature.

It is also important to observe that an t-time and m-sample distinguishing algorithm, in the model of learning, runs in time $t(n)$ and samples $m(n)$ where n is the number of qubits. Meanwhile, for a $(\cdot, \ell, m, s, \cdot)$-PRS, the t-time adversary runs in time $t(n)$ where n is *not* the number of qubits, but rather ℓ is. Therefore, a t-time and m-sample distinguishing algorithm runs in time $t(\ell)$ and uses number of samples $m(\ell)$ relative to n.

Because of Fact 10 and Corollary 13, we can show that distinguishing is robust against small perturbations.

Lemma 53 *Let $\mathcal{C}$ be (m, t, ε)-distinguishable and let $\mathcal{C}_\delta$ be the class of states δ-close to $\mathcal{C}$ in trace distance. Then $\mathcal{C}_\delta$ is $(m, t, \varepsilon - \sqrt{m}\delta)$-distinguishable.*

Proof Let $|\phi\rangle \in \mathcal{C}$ be the closest state in $\mathcal{C}$ to $|\psi\rangle \in \mathcal{C}_\delta$ such that $d_{\mathrm{tr}}(|\psi\rangle, |\phi\rangle) \leq \delta$. Using Corollary 13, we find that $d_{\mathrm{tr}}(|\psi\rangle^{\otimes m}, |\phi\rangle^{\otimes m}) \leq \sqrt{m} \cdot \delta$

Finally, let $(C_n)_{n\in\mathbb{N}}$ form the distinguisher for $\mathcal{C}$. Then by Fact 10

$$\left| \operatorname{tr}\left[|1\rangle\langle 1| \cdot C_n\left(|\psi\rangle\langle\psi|^{\otimes m}\right)\right] - \operatorname{tr}\left[|1\rangle\langle 1| \cdot C_n\left(|\phi\rangle\langle\phi|^{\otimes m}\right)\right] \right| \leq \sqrt{m}\delta.$$

By the triangle inequality, the distinguishing power of (C_n) is at least $\varepsilon - \sqrt{m}\delta$. ∎

We now work to show the implication that learning implies distinguishing from Haar random. The intuition is two-fold. The first is that a Haar random quantum state cannot be learned to even $\varepsilon = 1 - \frac{1}{2^{o(n)}}$ accuracy with sub-exponential samples. The second is that whether or not a learning algorithm for *pure* states succeeds can be verified using the SWAP test (Barenco et al., 1997; Buhrman et al., 2001; Gottesman and Chuang, 2001). Together, running the SWAP test on the output of the learning algorithm should distinguish whether or not the learning algorithm was fed a "correct" input state or a Haar random state.

We utilize the following information theoretic result, which gives the optimal fidelity for learning a Haar random state given a fixed number of copies. It was recently used by Yuen to prove optimal sample complexity for fidelity-based quantum state tomography (Yuen, 2023) and holds for even adversaries with unbounded computational power, as it is entirely information theoretic.

Lemma 54 (Bruß and Macchiavello, 1999, Eqn 16) *Given m copies of an n-qubit Haar random state $|\psi\rangle$, any quantum algorithm outputting a classical description of a state $\widehat{\rho}$ must have*

$$\boldsymbol{E}\left[\mathcal{F}\left(|\psi\rangle\langle\psi|, \widehat{\rho}\right)\right] \leq \frac{m+1}{m+2^n}$$

where the expectation is over both the randomness in the measurement results and the Haar measure.

Lemma 55 *If $\mathcal{C}$ is $(m, t, 1-\eta, 1-\lambda)$-learnable for $\eta \geq 2^{-o(n)}$, $\lambda \geq 2^{-o(n)}$, and $m = 2^{o(n)}$. Then $\mathcal{C}$ is $\left(m+1, t\log t, \frac{1-o(1)}{2}\eta\lambda\right)$-distinguishable.*

Proof The distinguisher is simple to state and uses $m+1$ copies of $|\psi\rangle$. Let $(C_n)_{n\in\mathbb{N}}$ be the learning algorithm for $\mathcal{C}$. First, run C_n on m copies of $|\psi\rangle$ to output a general quantum circuit that prepares $\widehat{\rho}$. Then perform a SWAP test between $\widehat{\rho}$ and an extra copy of $|\psi\rangle$. Recall that the SWAP test between states $\widehat{\rho}$ and $|\psi\rangle\langle\psi|$ accepts with probability $\frac{1}{2}\left(1 + \langle\psi|\widehat{\rho}|\psi\rangle\right)$. Therefore, we simply need to show that the expected bias of the SWAP test (i.e., half the fidelity $\frac{1}{2}\langle\psi|\widehat{\rho}|\psi\rangle$) for each of our two cases is separated by ε for sufficiently large $n \in \mathbb{N}$.

In the case where $|\psi\rangle \in \mathcal{C}$, by Fact 12, C_n will output the description of a circuit that synthesizes $\widehat{\rho}$ such that $\langle\psi|\widehat{\rho}|\psi\rangle \geq 1 - d_{\mathrm{tr}}(\widehat{\rho}, |\psi\rangle\langle\psi|) \geq \eta$ with probability at least λ. The test will accept with expected bias at least $\beta_1 := \eta \cdot \lambda$ as a result. Conversely, when $|\psi\rangle$ is Haar random, we know from Lemma 54 that the average fidelity is at most $\frac{m+1}{2^n+1} = \frac{1}{2^{\Theta(n)}}$. By linearity of expectations, the expected bias of the SWAP test is therefore at most $\frac{m+1}{2^n+1}$ as well. Finally, because $\eta \cdot \lambda \geq 2^{-o(n)}$, the gap in the biases of the two cases, $|\beta_1 - \beta_2| = \frac{1}{2}|\eta\lambda - 2^{-\Theta(n)}|$, is at least $\frac{1-o(1)}{2}\eta\lambda$ for some sufficiently large value of n.

We note that the size of the circuit producing $\widehat{\rho}$ is at most $O(t)$. Therefore, producing $\widehat{\rho}$ from its description must take time at most $O(t \log t)$ by applying Fact 19. It follows that running C_n, producing $\widehat{\rho}$, then running a SWAP test takes at most $O(t \log t)$ time as well. This show that $\mathcal{C}$ is $\left(m+1, t\log t, \frac{1-o(1)}{2}\eta\lambda\right)$-distinguishable. ■

We remark that, realistically, one would expect to be able to able to produce the output of the learned circuit, $\widehat{\rho}$ in time $O(t)$ rather than $O(t \log t)$. With this assumption, we get a $(m+1, t, (1 - o(1)) \cdot \eta\lambda)$-distinguisher instead. Furthermore, this logarithmic overhead is a result of treating the circuit as a black-box algorithm; usually an efficient learning algorithm can be made into a distinguisher in a white-box way in time at least as fast, and sometimes *much* faster. See Section 1.3 for discussion.

Appendix D. $\mathsf{pureStatePSPACESIZE}_0 \not\subset \mathsf{pureStateBQSIZE}\left[n^k\right]_{0.49}$

Our final major technical contribution will be a proof that for any fixed $k \in \mathbb{N}$,

$$\mathsf{pureStatePSPACESIZE}_0 \not\subset \mathsf{pureStateBQSIZE}\left[n^k\right]_{0.49}.$$

This is analogous to Arunachalam et al. (2022b, Lemma 3.3), where they utilize the fact that for any fixed $k > 0$, PSPACE can diagonalize against Boolean circuits of size n^k. However, while state synthesis problems are a generalization of decision problems, we cannot simply use the fact that for all $k \geq 1$, $\mathsf{PSPACE} \not\subset \mathsf{BQSIZE}[n^k]$ (Chia et al., 2022), as the notions of non-uniformity are actually different (see Theorem 25). In more detail, the proofs of Arunachalam et al. (2022b, Lemma 3.3) and Chia et al. (2022) rely on the fact that the ways in which a *single* circuit of bounded size can process all $x \in \{0,1\}^n$ is limited. Since a non-uniform circuit is now allowed to depend on x in the case of state synthesis, it can decide all languages such that the decision separation does not lift to state synthesis in the way it does for uniform models of computation.

Instead, for each $n \in \mathbb{N}$ we need to find a single state that is sufficiently complicated enough, rather than a state sequence (or language) whose relationship with $x \in \{0,1\}^n$ is complicated. Even the high-level proof techniques for diagonalization no longer apply. This is immediately obvious in the sense that quantum states lie in a continuous space, yet bit strings exist as a discrete set. As such, while slightly perturbing a bitstring always creates a "far" string, a non-trivial action on a quantum state could leave you with a state very close in trace distance still. To combat this, we will attempt to discretize the set of n-qubit quantum states via its packing number with respect to the trace distance (see Definition 57). From there, we will argue over the course of Section D.1 that there exists a circuit size hierarchy, in that non-uniform *unitary* circuits of larger size can always create states far away from non-uniform *general* circuits of a smaller size. Then in Section D.2, we will use the ability to estimate the trace distance of states produced by polynomial size circuits using only a polynomial amount of space. By doing a brute-force search over all possible states produced by $\mathsf{pureStateBQSIZE}\left[n^k\right]_{0.49}$, we can find a state in $\mathsf{pureStateCircuit}\left[n^{k'}\right]_0$ for $k' > k$ that is not in $\mathsf{pureStateBQSIZE}\left[n^k\right]_{0.49}$. By using said state as part of the state sequence in $\mathsf{pureStatePSPACESIZE}_0$ we get our desired separation of $\mathsf{pureStatePSPACESIZE}_0 \not\subset \mathsf{pureStateBQSIZE}\left[n^k\right]_{0.49}$.

Remark 56 *While a zero-error state synthesis class may seem odd, seeing as it is gate set dependent, we note that Theorem 62 holds for arbitrary universal gate sets as long as* $\mathsf{pureStatePSPACESIZE}$ *and* $\mathsf{pureStateBQSIZE}\left[n^k\right]$ *share the* same *universal gate set. If this happens to not be the case, then the result simply becomes* $\mathsf{pureStatePSPACESIZE}_{\exp} \not\subset \mathsf{pureStateBQSIZE}\left[n^k\right]_{0.49}$ *via the Solovay-Kitaev algorithm.*

D.1. Non-Uniform Quantum Circuit Size Hierarchy Theorem

In order to discretize the set of quantum states, the packing number $\mathcal{N}_{\text{pack}}(\mathcal{Y}, \varepsilon)$ counts how many states in a set $\mathcal{Y}$ are ε-far apart from each other in trace distance. The high-level idea for its use will be that if $A \subset B \subseteq \mathcal{S}$ and $\mathcal{N}_{\text{pack}}(A, \varepsilon) < \mathcal{N}_{\text{pack}}(B, \varepsilon)$ then some state in B is ε-far from *every* state in A.

Definition 57 (Packing Number) *Given a set of pure states on n qubits $\mathcal{Y} \subseteq \mathcal{S}$ we define the* packing number *to be,*

$$\mathcal{N}_{pack}(\mathcal{Y}, \varepsilon) \coloneqq \max\{|S| : \forall \left|\psi\right\rangle, \left|\phi\right\rangle \in S, d_{\text{tr}}(\left|\psi\right\rangle, \left|\phi\right\rangle) \geq \varepsilon, S \subseteq \mathcal{Y}\}$$

To get a hierarchy theorem, we will need both a lower and upper bound on $\mathcal{N}_{\text{pack}}$ for states created by polynomial size circuits. We start with a very crude upper bound by counting how many possible circuits there are, even if they might produce the same quantum state (or states that are ε-close to each other).

Proposition 58 *For $s \geq n$, the number of general quantum circuits of size s is at most*

$$2^{s\cdot(3\log_2 s+4)}.$$

Proof By Lemma 26, we can write all such circuits using at most $s \cdot (3\log_2 s + 4)$ bits. Enumerating over all bits of that length provides an upper bound on the number of circuits. ∎

For the lower bound, we use the following result by Oszmaniec et al. (2024) that was originally used to show that random circuits for unitary t-designs and chaotic quantum systems.

Lemma 59 *Oszmaniec et al., 2024, Lemma 11 Let $\mathcal{S}^r$ be the set of pure states generated by depth r unitary quantum circuits from gate set $\mathcal{G}$ on n-qubits. Then*

$$\mathcal{N}_{pack}(\mathcal{S}^r, \varepsilon) \geq \left(\frac{2^n(1-4\varepsilon^2)}{\alpha(r)}\right)^{\alpha(r)},$$

where $\alpha(r) \coloneqq \lfloor\left(\frac{r}{n^2\cdot c(\mathcal{G})}\right)^{1/11}\rfloor$ *and $c(\mathcal{G})$ is a constant depending on the gate set $\mathcal{G}$.*

With both upper and lower bound in hand, we now state our hierarchy theorem.

Lemma 60 *Let $\mathcal{D}^s$ be the set of states generated by size s* unitary *quantum circuits from $\mathrm{poly}(n)$-qubits to n-qubits and let $\mathcal{S}^{s'}$ be the set of quantum pure states generated by size s'* unitary *quantum circuits on n-qubits (i.e., no ancilla). For sufficiently large n and $s = 2^{o(n)}$, $\mathcal{N}_{pack}(\mathcal{D}^s, 0.495) < \mathcal{N}_{pack}(\mathcal{S}^{s'}, 0.495)$ for some $s' = O(s^{12}n^2c(\mathcal{G}))$ where $c(\mathcal{G})$ is a constant depending on the gate set $\mathcal{G}$.*

Proof By Corollary 58:

$$\mathcal{N}_{\text{pack}}\left(\mathcal{D}^s, 0.495\right) \leq 2^{s\cdot(3\log_2 s+4)} = o\left(2^{s^{12/11}}\right)$$

In contrast, we use Lemma 59 to show that $\mathcal{N}_{\text{pack}}(\mathcal{S}^{s'}, 0.495)$ is strictly larger, meaning that there must exist a state in $\mathcal{S}^{s'}$ that is ε far from all states in $\mathcal{D}^s$. Since $s' = O\left(s^{12}n^2c(\mathcal{G})\right)$ we find that $\alpha(s') = \kappa \cdot s^{12/11}$ for some constant $\kappa = O(1)$. We then note that the depth of a circuit of size s is at most s as well. Applying Lemma 59:

$$\begin{aligned}
\mathcal{N}_{\text{pack}}\left(\mathcal{D}^{s'}, \varepsilon\right) &\geq \left(\frac{2^n(1-4\varepsilon^2)}{\alpha(s')}\right)^{\alpha(s')} \\
&= \left(\frac{2^n(1-4\varepsilon^2)}{\kappa\cdot r^{12/11}}\right)^{\kappa\cdot s^{12/11}} \\
&\geq \left(2^{n-5.66-\log_2 s-\log_2 \kappa}\right)^{\kappa\cdot s^{12/11}} \\
&= 2^{\Theta\left(ns^{12/11}\right)}
\end{aligned}$$

where the last step holds because $\log_2\left(1-4\cdot 0.49^2\right) \geq -5.66$ and s is sub-exponential in n such that $\log_2 s = o(n)$. Thus, for sufficiently large number of qubits n we find that $\mathcal{N}_{\text{pack}}(\mathcal{D}^s, 0.495) < \mathcal{N}_{\text{pack}}(\mathcal{S}^{s'}, 0.495)$. ∎

We emphasize that for $\mathcal{N}_{\text{pack}}(\mathcal{S}^{s'}, \varepsilon)$ we don't allow any ancilla. Nevertheless, we still achieve the desired hierarchy result because our bound also lower bounds states produced by size s' *with* ancilla. However, an improvement to Lemma 59 that accounts for extra qubits could greatly reduce the constant powers relating s to s'.

D.2. Quantum State "Diagonalization"

From Lemma 60 we know that for circuits with sub-exponential size, a polynomially larger size can synthesize strictly more state sequences. We now argue that a polynomial space algorithm can find such a state that cannot be created by a smaller circuit size, allowing for $\mathsf{pureStatePSPACESIZE}_0$ to "diagonalize" against any circuit of a fixed polynomial size (i.e., $\mathsf{pureStateBQSIZE}\left[n^k\right]_{0.49}$).

The following folklore result will be a critical subroutine of this algorithm.

Lemma 61 *Let ρ and σ be two n-qubit quantum states that are produced by* unitary *quantum circuits of size at most $2^{\mathrm{poly}(n)}$ and space $\mathrm{poly}(n)$. Then $\mathrm{d}_{\mathrm{tr}}(\rho, \sigma)$ can be approximated to arbitrary $\exp(-\mathrm{poly}(n))$ error by a deterministic Turing machine in $\mathrm{poly}(n)$ space.*

Proof See Appendix I. ■

Theorem 62 *For every fixed $k \in \mathbb{N}$,*

$$\mathsf{pureStatePSPACESIZE}_0 \not\subset \mathsf{pureStateBQSIZE}\left[n^k\right]_{0.49}.$$

Proof For a particular value of n, let $U_1, U_2, \ldots$ be some arbitrary ordering on all *unitary* circuits of size at most $s := O(n^k)$ with n qubits of output such that ρ_i is the n-qubit state produced by C_i. Similarly, let $V_1, V_2, \cdots$ be some arbitrary ordering on all *unitary* circuits of size s' on n-qubits *with no ancilla*, for $s' = \mathrm{poly}(n)$ that we will define later, and let $|\phi_j\rangle$ be produced by V_j.

We now define the *pure* state sequence $\{|\psi_x\rangle\}$ such that $\{|\psi_x\rangle\} \in \mathsf{pureStatePSPACESIZE}_0$ but not $\mathsf{pureStateBQSIZE}\left[n^k\right]$. To trivially show that $\{|\psi_x\rangle\} \in \mathsf{pureStatePSPACESIZE}_0$, we define its synthesizing circuits (C_x) directly in terms of a PSPACE algorithm. The algorithm works as follows: For all V_j, iterate through all U_i and estimate if $d_{\mathrm{tr}}(\rho_i, |\phi_j\rangle\langle\phi_j|)$ to strictly less than $1/40 = 0.025$ accuracy using Lemma 61. The first time an estimate of $d_{\mathrm{tr}}(\rho_i, |\phi_j\rangle\langle\phi_j|)$ is greater than 0.4925, for all $x \in \{0,1\}^n$ set $|\psi_x\rangle := V_j\,|x\rangle$ such that $|\psi_{0^n}\rangle$ is produced by V_j on the all-zeros state. Since both sequences of circuits are of polynomial size, they can be written down using $\mathrm{poly}(n)$ bits (see Lemma 26) and therefore iterated through in $\mathrm{poly}(n)$ space. Combined with the fact that Lemma 61 uses only $\mathrm{poly}(n, \log 41)$ space, the whole algorithm can be performed by a deterministic Turing machine in $\mathrm{poly}(n)$ space. We conclude that the state sequence $(|\psi_x\rangle)_{x\in\{0,1\}^*}$ generated by this procedure, should it terminate, always has an *exact* synthesizing circuit that has $\mathrm{poly}(|x|)$ size, meaning that $(|\psi_x\rangle) \in \mathsf{pureStatePSPACESIZE}_0$.

We now show that this algorithm is not only guaranteed to terminate, but also guaranteed to produce a state that is more than 0.49-far from any state in $\mathsf{pureStateBQSIZE}\left[n^k\right]$. Lemma 60 shows that $\mathcal{N}_{\text{pack}}(\mathcal{D}^s, 0.495) < \mathcal{N}_{\text{pack}}(\mathcal{S}^{s'}, 0.495)$ for some $r' := O\left(s^{12}n^3c(\mathcal{G})\right)$ and sufficiently large n. There must then exist at least one $|\phi_{j^*}\rangle \in \mathcal{S}^{s'}$ that is at least 0.495-far from all $\rho_i \in \mathcal{D}^s$. As a result of the PSPACE algorithm estimating trace distance to accuracy $< 1/40$, if the algorithm reaches this $|\phi_{j^*}\rangle$ then by the triangle inequality it is guaranteed to terminate.

We note that it is also possible for the algorithm to terminate earlier, but by the triangle inequality any state that could cause this must be greater than 0.49-far from any state in $\mathsf{pureStateBQSIZE}\left[n^k\right]_0$, thus also succeeding. ■

Appendix E. Circuit Lower Bounds from Learning

E.1. Learning vs Pseudorandomness

We now formally prove that learning algorithms and pseudorandomness can be combined to give lower bounds for state synthesis. We state Lemma 64 with as much generality as possible relative to the PRS, as we expect improvements to PRS constructions from Corollary 50 to be possible. This will allow the main theorems to be easily improved in the future.

Remark 63 *It is worth reminding the reader that the concept of problem size (i.e., the value of n) differs depending on the context. For a learning problem, for instance, n is the number of qubits in the quantum state. Likewise, n for a PRS is the security parameter and n for a state sequence defined using that PRS is actually the key length κ. Throughout this work we have used n to be consistent* *with the specific type of problem, but in Theorem 65 we will have to move between various ideas of what 'n' means. Importantly, given a $(\kappa, \ell, q, s, \varepsilon)$-PRS, the learning algorithm will run as a function of ℓ. Therefore, if the PRS can be computed as a state sequence with some resource (such as time or space or size) growing as a function of the key length $f(\kappa)$, it is also computed with the same resource growing as $f \circ \kappa \circ \ell^{-1}$ relative to ℓ, which is the viewpoint of the learning algorithm. Similarly, if the PRS has some value $f(n)$ computed relative to the security parameter n, then it will be $f \circ \ell^{-1}$ relative to ℓ.*

Lemma 64 *For arbitrary fixed $f : \mathbb{N} \to \mathbb{R}^+$ and $\delta : \mathbb{N} \to [0,1]$, let $\mathfrak{C}$ be a circuit class that is closed under restrictions and define $\mathcal{C}_\ell$ to be the set of pure states on ℓ qubits that can be constructed by $\mathfrak{C}[f(\ell)]$. Assume the existence of an infinitely-often $(\kappa, \ell, m, s, \varepsilon)$-PRS against uniform quantum computations that can be computed in time t. If the concept class $\mathcal{C} := \bigcup_{\ell \geq 1} \mathcal{C}_\ell$ is $\left(m \circ \ell^{-1},\, s \circ \ell^{-1},\, \varepsilon \circ \ell^{-1} + \sqrt{m \circ \ell^{-1}} \cdot \delta\right)$-distinguishable then*

$$\mathsf{pureStateBQTIME}\left[t \circ \kappa^{-1}\right]_{\exp} \not\subset \mathsf{pureState}\mathfrak{C}\left[f \circ \ell \circ \kappa^{-1}\right]_\delta .$$

Proof It is easy to see that the PRS (as a state sequence) is in $\mathsf{pureStateBQTIME}\left[t \circ \kappa^{-1}\right]_{\exp}$, so we now need to show that it is not in $\mathsf{pureState}\mathfrak{C}\left[f \circ \ell \circ \kappa^{-1}\right]_\delta$. Relative to the security parameter n, the number of samples used by the distinguishing algorithm is $m \circ \ell^{-1} \circ \ell = m(n)$, the running time is $O\left(s \circ \ell^{-1} \circ \ell\right) = O(s(n))$, and the advantage is $\varepsilon \circ \ell^{-1} \circ \ell + \sqrt{m \circ \ell^{-1} \circ \ell} \cdot \delta = \varepsilon + \sqrt{m} \cdot \delta$. Finally, the size of the circuits generating $\mathcal{C}_\ell$ are $O(f \circ \ell) = O\left(f \circ \ell \circ \kappa^{-1} \circ \kappa\right)$ such that the size relative to the key parameter κ is $O\left(f \circ \ell \circ \kappa^{-1}\right)$. It follows by the parameters of the PRS and Lemma 53 that if $\mathcal{C}$ could be learned then the PRS does not lie in $\mathsf{pureState}\mathfrak{C}\left[f \circ \ell \circ \kappa^{-1}\right]_\delta$. ■

E.2. Win-win Argument

We now prove our main theorem of non-trivial quantum state learning (or even just distinguishing) implying state synthesis lower bounds, followed by a similar proof of decision problem circuit lower bounds. As with many of the previous literature on learning-to-hardness for boolean concepts (Fortnow and Klivans, 2009; Klivans et al., 2013; Oliveira and Santhanam, 2017; Arunachalam et al., 2022b), we will use a win-win argument. This will allow us to not have any complexity-theoretic assumptions, despite them being necessary in Lemmas 45 and 47.

The first scenario is where $\mathsf{pureStatePSPACESIZE}_{\exp} \subseteq \mathsf{pureStateBQSUBEXP}_{\exp}$. Here, we do not even have to actually use the assumption of a non-trivial learner and just apply Theorem 62. In the other scenario, we combine Corollaries 50 and 64.

Theorem 65 *For arbitrary $\delta : \mathbb{N} \to [0,1]$, let $\mathfrak{C}$ be a circuit class that is closed under restrictions. There exists universal constants $\alpha \geq 1$ and $\lambda \in (0, 1/5)$ such that the following is true:*

Define $\mathcal{C}_\ell$ to be the set of pure states on ℓ qubits that can be exactly constructed by $\mathfrak{C}[\mathrm{poly}(\ell)]$. For a fixed constant $c \geq 2$, if the concept class $\mathcal{C} := \bigcup_{\ell \geq 1} \mathcal{C}_\ell$ is (m, t, ε)-distinguishable for $m \leq 2^{\ell^{0.99}}$, $t \leq O\left(2^{\ell^c}\right)$, and

$$\varepsilon \geq \frac{63 \cdot 4^{\ell^{0.99}}}{2^\ell} + \frac{1}{2^{n^\lambda}} + \sqrt{m} \cdot \delta,$$

then at least one of the following must be true:

- *for all* $k \geq 1$, $\mathsf{pureStateBQSUBEXP}_{\text{exp}} \not\subset \mathsf{pureStateBQSIZE}\left[n^k\right]_{0.49}$,
- $\mathsf{pureStateBQE}_{\text{exp}} \not\subset \mathsf{pureState}\mathfrak{C}_{\delta}$.

Proof One of two possibilities are true of the relationship between $\mathsf{pureStatePSPACESIZE}_{\text{exp}}$ and $\mathsf{pureStateBQSUBEXP}_{\text{exp}}$, such that we will prove the separation for both possibilities.

In the case that $\mathsf{pureStatePSPACESIZE}_{\text{exp}} \subseteq \mathsf{pureStateBQSUBEXP}_{\text{exp}}$ then Theorem 62 tells us that, for each $k \geq 1$, there exists some state sequence $(|\psi_x\rangle)_{x\in\{0,1\}^*}$ that is in $\mathsf{pureStatePSPACESIZE}_0$ but not $\mathsf{pureStateBQSIZE}\left[n^k\right]_{\delta}$. Since $\mathsf{pureStatePSPACESIZE}_0 \subseteq \mathsf{pureStateBQSUBEXP}_{\text{exp}}$ by our assumption, $(|\psi_x\rangle)_{x\in\{0,1\}^*} \in \mathsf{pureStateBQSUBEXP}_{\text{exp}}$ as well. This completes one side of the win-win argument.

On the other hand, if $\mathsf{pureStatePSPACESIZE}_{\text{exp}} \not\subset \mathsf{pureStateBQSUBEXP}_{\text{exp}}$ then Corollary 50 tells us that there exists an infinitely-often

$$\left(\kappa, \lfloor \log_2 r \rfloor^{2/c}, q, s, \frac{4q^2}{2^{\lfloor \log_2 r\rfloor^{2/c}}} + \frac{1}{r}\right)\text{-PRS}$$

against uniform quantum computation that lies in $\mathsf{pureStateBQTIME}\left[2^{\kappa\circ\kappa^{-1}(n)}\right]_{\text{exp}} = \mathsf{pureStateBQE}_{\text{exp}}$ for some $\lambda \in (0, 1/5)$, $\alpha \geq 1$, $\kappa(n) \leq n^{\alpha}$, $r(n) = \lfloor 2^{n^{\lambda}} \rfloor$, $q = 2^{n^{1.98\cdot\lambda/c}}$ and $s(n) = 2^{n^{2\lambda}}$. Observe that for $n \geq 1$:

$$n^{\lambda} \geq \log_2 r \geq \lfloor \log_2 r \rfloor > \log_2 r - 1 = \log_2 \lfloor 2^{n^{\lambda}} \rfloor - 1 > \log_2\left(2^{n^{\lambda}} - 1\right) - 1 \geq n^{\lambda} - 2.$$

Therefore, for sufficiently large $\ell := \lfloor \log_2 r \rfloor^{2/c} = O\left(n^{2\lambda/c}\right)$:

$$\begin{aligned}
m(\ell) &= m\left(\lfloor \log_2 r\rfloor^{2/c}\right) \leq 2^{\lfloor \log_2 r\rfloor^{1.98/c}} < 2^{n^{1.98\cdot\lambda/c}} = q = q \circ \ell^{-1}(\ell) \\
t(\ell) &= t\left(\lfloor \log_2 r\rfloor^{2/c}\right) \leq 2^{\lfloor \log_2 r\rfloor^{2}} < 2^{n^{2\lambda}} = s = s \circ \ell^{-1}(\ell) \\
\varepsilon(\ell) &= \varepsilon\left(\lfloor \log_2 r\rfloor^{2/c}\right) \geq \frac{63\cdot 4^{\lfloor \log_2 r\rfloor^{1.98/c}}}{2^{\lfloor \log_2 r\rfloor^{2/c}}} + \frac{1}{2^{n^{\lambda}}} + \sqrt{m}\cdot\delta \\
&> \frac{4\cdot 4^{n^{1.98\cdot\lambda/c}}}{2^{\lfloor \log_2 r\rfloor^{2/c}}} + \frac{1}{2^{n^{\lambda}}} + \sqrt{m}\cdot\delta \geq \frac{4q^2}{2^{\lfloor \log_2 r\rfloor^{2/c}}} + \frac{1}{r} + \sqrt{m}\cdot\delta
\end{aligned}$$

Consequently, because $\mathcal{C}$ is (m, t, ε)-distinguishable, then by Lemma 64 we find that

$$\mathsf{pureStateBQTIME}\left[t\circ\kappa^{-1}\right]_{\text{exp}} \not\subset \mathsf{pureState}\mathfrak{C}\left[\text{poly}(\ell\circ\kappa^{-1})\right]_{\delta} = \mathsf{pureState}\mathfrak{C}[\text{poly}(n)]_{\delta}.$$

■

While the choice of parameters may seem somewhat opaque, the most important thing is to consider the relationship between m and δ and how it affects ε. For example, when $m = \text{poly}(n)$ then there exists some inverse-poly distinguishing that gives a separation with $\mathsf{pureState}\mathfrak{C}$. Similarly, when m is just less than $2^{\ell^{0.99}}$ then inverse-sub-exponential distinguishing gives a separation from $\mathsf{pureState}\mathfrak{C}_{\text{exp}}$. We formally prove the latter statement.

Corollary 66 (Formal statement of Theorem 2) *Let $\mathfrak{C}$ be a circuit class that is closed under restrictions. Define $\mathcal{C}_\ell$ to be the set of pure states on ℓ qubits that can be exactly constructed by $\mathfrak{C}[\mathrm{poly}(\ell)]$. If there exists some constant $c \geq 2$ such that $\mathcal{C} := \bigcup_{\ell \geq 1} \mathcal{C}_\ell$ is (m, t, ε)-distinguishable for $m \leq 2^{\ell^{0.99}}$, $t \leq O\left(2^{\ell^c}\right)$, and $\varepsilon \geq \frac{1}{2^{\ell^{0.99}}}$, then at least one of the following must be true:*

- *for all $k \geq 1$, $\mathsf{pureStateBQSUBEXP}_{\exp} \not\subset \mathsf{pureStateBQSIZE}\left[n^k\right]_{0.49}$,*
- $\mathsf{pureStateBQE}_{\exp} \not\subset \mathsf{pureState}\mathfrak{C}_{\exp}$.

Proof For arbitrary polynomial p,

$$\varepsilon \geq \frac{1}{2^{\ell^{0.99}}} \geq \frac{63 \cdot 4^{\ell^{0.99}}}{2^\ell} + \frac{1}{2^{\ell^{c/2}}} + \sqrt{2^{\ell^{0.99}}} \cdot \exp(-p) \geq \frac{63 \cdot 4^{\ell^{0.99}}}{2^\ell} + \frac{1}{2^{n^\lambda}} + \sqrt{m} \cdot \exp(-p)$$

with sufficiently large ℓ. By Theorem 65, either (1) for all $k \geq 1$, $\mathsf{pureStateBQSUBEXP}_{\exp} \not\subset \mathsf{pureStateBQSIZE}\left[n^k\right]_{0.49}$ or (2) $\mathsf{pureStateBQE} \not\subset \mathsf{pureState}\mathfrak{C}_{\exp(-p)}$. In case (2), since p is an arbitrary polynomial, the state is not in $\mathsf{pureState}\mathfrak{C}_{\exp}$ as well. ■

Using our connection between learning and distinguishing (see Lemma 55) we can now state our main result. Note that instead of listing two possible outcomes like in Corollary 66, we take the intersection of the outcomes such that it is true regardless of which outcome. However, while the implied result would still be interesting for many circuit classes, it is decidedly weaker than either of the two original possibilities.

Corollary 67 (Formal statement of Theorem 1) *Let $\mathfrak{C}$ be a circuit class that $\mathsf{pureState}\mathfrak{C}_{\exp} \subset \mathsf{pureStateBQP/poly}_{0.49}$. Define $\mathcal{C}_\ell$ to be the set of pure states on ℓ qubits that can be exactly constructed by $\mathfrak{C}[\mathrm{poly}(\ell)]$. If there exists some constant $c \geq 2$ such that $\mathcal{C} := \bigcup_{\ell \geq 1} \mathcal{C}_\ell$ is $(m, t, 1-\eta, 1-\gamma)$-learnable for $m - 1 \leq 2^{\ell^{0.99}}$, $t \leq O\left(\frac{2^{\ell^c}}{\ell^c}\right)$ and $\eta \cdot \gamma = \frac{4}{2^{\ell^{0.99}}}$, then for every $k \geq 1$, $\mathsf{pureStateBQE}_{\exp} \not\subset \mathsf{pureState}\mathfrak{C}[n^k]_{\exp}$.*

Proof Lemma 55 tells us that each $\mathcal{C}^k$ is (m, t', ε)-distinguishable for $t' = t \log t \leq O\left(2^{\ell^2}\right)$ and $\varepsilon = \frac{1-o(1)}{2}\eta \cdot \gamma \geq \frac{1}{2^{\ell^{0.99}}}$ for sufficiently large ℓ. We then appeal to Corollary 66. By invoking the condition that $\mathsf{pureState}\mathfrak{C}_{\exp} \subset \mathsf{pureStateBQP/poly}_{0.49}$, in both cases the following statement is true: for every $k \geq 1$, $\mathsf{pureStateBQE}_{\exp} \not\subset \mathsf{pureState}\mathfrak{C}[n^k]_{\exp}$. ■

Remark 68 *It is actually possible to have a more fine-grained approach to the learning/distinguishing algorithm than in Theorems 65 and 66. For instance, if the learning algorithm only holds up to $\mathfrak{C}[n^k]$ for some fixed k, then by a more careful application of Lemma 64, the separation in the second case would be*

$$\mathsf{pureStateBQE}_{\exp} \not\subset \mathsf{pureState}\mathfrak{C}\left[n^{\alpha \cdot k/\lambda}\right]_\delta$$

instead. As a result, Corollary 67 remains true if there is a learning algorithm for each $\mathcal{C}^k := \bigcup_{\ell \geq 1} \mathcal{C}_\ell^k$ where $\mathcal{C}_\ell^k$ refers to ℓ-qubit states produced by $\mathfrak{C}[n^k]$. That is, the learning algorithm can work up to any polynomial size, but needs to know an upper bound on the polynomial in advance.

Appendix F. Decision Problem Circuit Lower Bounds With an Extra Circuit Constraint

We now show the interesting result that non-trivial quantum state tomography can imply decision complexity class separations between entirely *classical* computational models. However, we will need to impose two assumptions on $\mathfrak{C}$. The weaker assumption is the ability to implement the unitary $H^{\otimes(n+1)} \cdot I^{\otimes n} \otimes X$, which was used in Lemma 43 to construct binary phase states. The second assumption is the ability to perform error reduction to arbitrary $\exp(-\mathrm{poly}(n))$ accuracy. The simplest way to get error reduction is via majority and fanout gates, but since it's not clear that QNC^0 or QAC^0 can compute these gates, the weakest circuit class that we've introduced that *does* meet these requirements is QAC^0_f. It also happens that QAC^0 can implement $H^{\otimes(n+1)} \cdot I^{\otimes n} \otimes X$ exactly. As such, we will state our results in terms of QAC^0_f for succinctness, though it should be understood that any circuit class that meets these two requirements suffices as well.

Lemma 69 *For arbitrary fixed $f : \mathbb{N} \to \mathbb{R}^+$ and $\delta : \mathbb{N} \to [0,1]$, let $\mathfrak{C} \supseteq \mathsf{QAC}^0_f$ be a circuit class that is closed under restrictions and define $\mathcal{C}_\ell$ to be the set of pure states on ℓ qubits that can be constructed by $\mathfrak{C}[f(\ell)+\ell]$ with depth at most $d+3$. Assume the existence of an infinitely-often $(\kappa, \ell, 1, m, s, \varepsilon)$-PRF against uniform quantum computations that can be computed in time t by a deterministic Turing machine. If the concept class $\mathcal{C} := \bigcup_{\ell \geq 1} \mathcal{C}_\ell$ is $\left(m \circ \ell^{-1},\, s \circ \ell^{-1},\, \varepsilon \circ \ell^{-1} + \sqrt{m \circ \ell^{-1}} \cdot \delta\right)$-distinguishable then*

$$\mathsf{DTIME}\left[t \circ \kappa^{-1}\right] \not\subseteq \text{(depth } d\text{)-}\mathfrak{C}\left[f \circ \ell \circ \kappa^{-1}\right].$$

Proof Let $\left(\{F_k\}_{k \in \{0,1\}^{\kappa(n)}}\right)_{n \in \mathbb{N}}$ be the the infinitely-often PRF against uniform quantum computations. Define the language L such that inputs $(x, k) \in L$ if and only if $F_k(x) = 1$ when $x \in \{0,1\}^\ell$ and $k \in \{0,1\}^\kappa$. Because the PRF is computable in time t by a deterministic Turing machine, L lies in $\mathsf{DTIME}\left[t \circ \kappa^{-1}\right]$.

We now need to show that L is not in (depth d)-$\mathfrak{C}\left[f \circ \ell \circ \kappa^{-1}\right]$. For the sake of contradiction, assume that it was. Then using Lemma 43 and error-reduction via majority and fanout, (depth $d+3$)-$\mathfrak{C}\left[n + f \circ \ell \circ \kappa^{-1}(n)\right]$ can create approximately synthesize pseudorandom states.

The fact that the depth only increases by 3 follows from the fact that $\mathfrak{C} \supset \mathsf{QAC}^0_f$ allows us to perform arbitrary classical fanout, approximately compute the PRF, then take the majority, to perform error reduction using only a depth increase of 2. Performing the circuit in Lemma 43 adds the final extra layer of depth. Since this only needs $O(n)$ Hadamard and X gates, the size increases by at most $O(n)$ as well. Relative to the security parameter n: the number of samples used by the distinguishing algorithm is $m \circ \ell^{-1} \circ \ell = m(n)$, the running time is $O\left(s \circ \ell^{-1} \circ \ell\right) = O(s(n))$, and the advantage is $\varepsilon \circ \ell^{-1} \circ \ell + \sqrt{m \circ \ell^{-1} \circ \ell} \cdot \delta = \varepsilon + \sqrt{m} \cdot \delta$. Finally, the size of the circuits generating $\mathcal{C}_\ell$ are $O\left(f \circ \ell\right) = O\left(f \circ \ell \circ \kappa^{-1} \circ \kappa\right)$ such that the size relative to the key parameter κ is $O\left(f \circ \ell \circ \kappa^{-1}\right)$. It follows by the parameters of the PRS and Lemma 53 that if $\mathcal{C}$ could be learned then the PRS does not lie in $\mathsf{pureState}\mathfrak{C}\left[f \circ \ell \circ \kappa^{-1}\right]_\delta$. This is a contradiction, meaning that $L \notin$ (depth d)-$\mathfrak{C}\left[f \circ \ell \circ \kappa^{-1}\right]$. ∎

Remark 70 *Observe that Lemma 69 requires a PRF while Lemma 64 only requires a PRS. Using Rosenthal (2024, Theorem 7.1), if one only wants to show that $\mathsf{EXP} \not\subseteq$ (depth $d + O(1)$)-$\mathfrak{C}$, it is actually possible to weaken Lemma 69 to only use a PRS with the special property that each amplitude (including phase information) can be computed in time* $\exp(\mathrm{poly}(n))$.

We can now combine Lemma 69 and Corollary 46 to show a conditional circuit lower bound. To handle the other side of the win-win-argument, we need the following result.

Lemma 71 (Chia et al., 2022) *For every $k \in \mathbb{N}$, there exist a language $L_k \in \mathsf{PSPACE}$ such that $L_k \notin \mathsf{BQSIZE}[n^k]$.*

Theorem 72 (Formal Statement of Theorem 3) *Let $\mathfrak{C} \supseteq \mathsf{QAC}_f^0$ be a circuit class that is closed under restrictions. Define $\mathcal{C}_\ell$ to be the set of pure states on ℓ qubits that can be exactly constructed by $\mathfrak{C}[\mathrm{poly}(\ell)]$ with depth at most $d+3$. If there exists a fixed constant $c \geq 2$ such that $\mathcal{C} := \bigcup_{\ell \geq 1} \mathcal{C}_\ell$ is (m, t, ε)-distinguishable for $m \leq 2^{\ell^{0.99}}$, $t \leq O\left(2^{\ell^c}\right)$, and $\varepsilon \geq \frac{1}{2^{\ell^{0.99}}}$, then at least one of the following must be true:*

- *for all $k \geq 1$, $\mathsf{BQSUBEXP} \not\subset \mathsf{BQSIZE}\left[n^k\right]$,*
- *$\mathsf{E} \not\subset$ (depth d)-$\mathfrak{C}[\mathrm{poly}(n)]$.*

Proof [Proof Sketch] We will again use a win-win argument, but now with PSPACE and $\mathsf{BQSUBEXP}$. If $\mathsf{PSPACE} \subseteq \mathsf{BQSUBEXP}$ then using Lemma 71, we get $\mathsf{BQE} \not\subset \mathsf{BQSIZE}[n^k]$.

On the other hand, if $\mathsf{PSPACE} \not\subseteq \mathsf{BQSUBEXP}$ then we can invoke Corollary 46 to show that there exists some infinitely-often $(\kappa, \ell, 1, q, s, \varepsilon)$-PRF against uniform quantum computations where $\kappa(n) \leq n^\alpha$, $r(n) = \lfloor 2^{n^\lambda} \rfloor$, $\ell \leq \lfloor \log_2 r \rfloor$, and $s(n) = 2^{n^{2\lambda}}$. By Lemma 69 and a similar analysis to Theorems 65 and 66, we find that $\mathsf{E} \not\subset$ (depth d)-$\mathfrak{C}[\mathrm{poly}(n)]$. ■

Because $\mathsf{TC}^0 \subset \mathsf{QAC}_f^0$ (Hoyer and Spalek, 2005; Takahashi and Seiichiro, 2016), the second scenario in Theorem 72 also implies that $\mathsf{E} \not\subset \mathsf{TC}^0$.

Appendix G. Conditional Pseudorandom Unitaries and Circuit Lower Bounds for Unitary Synthesis

Due to the recent results on pseudorandom unitaries (Lu et al., 2023; Metger et al., 2024; Chen et al., 2024; Schuster et al., 2024; Ma and Huang, 2024), we sketch how the ability to distinguish unitaries from circuit class $\mathfrak{C}$ from Haar random (including with access to the inverse) implies unitary synthesis separations. Later in Section H we will use the same line of to work show that unitary learning also implies decision class separations when $\mathfrak{C}$ becomes sufficiently powerful. Unitary synthesis capture an even more general set of problems than state synthesis, such as certain kinds of problems with quantum inputs and quantum outputs. For details on unitary synthesis complexity class definitions, see Metger and Yuen (2023) and Bostanci et al. (2023).

We first need to introduce a distance measure between trace-preserving completely positive maps. Like Trace Distance, it bounds the maximum distinguishability between two quantum operations.

Definition 73 (Diamond Distance) *Let $\Phi, \Gamma : \mathcal{D}_m \to \mathcal{D}_n$ be two trace-preserving completely positive maps. We define the diamond distance to be*

$$d_\diamond(\Phi, \Gamma) := \max_{\rho \in \mathcal{D}_{2m}} \left\| (\Phi \otimes 1_m)\, \rho - (\Gamma \otimes 1_m)\, \rho \right\|_1$$

where 1_m is the identity channel on m qubits.

Note that unlike Trace Distance, diamond distance lies in $[0, 2]$.

Definition 74 ($\mathsf{unitaryBQTIME}[f]_\delta$, $\mathsf{unitaryBQSPACESIZE}[f]_\delta$) *Let $\delta : \mathbb{N} \to [0, 1]$ and $f : \mathbb{N} \to \mathbb{R}^+$ be functions. Then $\mathsf{unitaryBQTIME}[f]_\delta$ (resp. $\mathsf{unitaryBQSPACESIZE}[f]_\delta$) is the class of all sequences of unitary matrices $(U_x)_{x\in\{0,1\}^*}$ such that each U_x is a unitary on $\mathrm{poly}(|x|)$ qubits, and there exists an f-time-uniform (resp. f-space-and-size-uniform) family of general quantum circuits $(C_x)_{x\in\{0,1\}^*}$ such that for all sufficiently large input size $|x|$,*

$$d_\diamond(C_x, U_x) \leq \delta.$$

Definition 75 ($\mathsf{unitaryBQP}_\delta$, $\mathsf{unitaryPSPACESIZE}_\delta$)

$$\mathsf{unitaryBQP}_\delta := \bigcup_p \mathsf{unitaryBQTIME}[p]_\delta$$
$$\mathsf{unitaryPSPACESIZE}_\delta := \bigcup_p \mathsf{unitaryBQSPACESIZE}[p]_\delta$$

where the union is over all polynomials $p : \mathbb{N} \to \mathbb{R}$.

We can likewise define $\mathsf{unitaryBQE}_\delta$ and $\mathsf{unitaryBQP/poly}$ to be the analogues of $\mathsf{stateBQE}$ and $\mathsf{stateBQP/poly}$ respectively. Finally, when dealing with *unitary* circuit families, we will refer to the complexity classes with the prefix $\mathsf{pureUnitary}$-, such as in $\mathsf{pureUnitaryBQE}$.

We now need to generalize both Lemmas 48 and 62 but for unitary synthesis. The high-level idea is that both proofs implicitly work at the level of unitaries, rather than states, in that they find a unitary that has the correct property before arguing that the state that the unitary creates also has a similar property. Put another way, Lemmas 48 and 62 actually follow as *corollaries* of Lemmas 76 and 77, which were implicitly proven along the way.

Lemma 76 *Let $k : \mathbb{N} \to \mathbb{R}^+$. For any $\mathsf{unitaryA}_\delta \subset \mathsf{unitaryBQP/poly}_\delta$, if $\mathsf{unitaryA}_\delta \not\subset \mathsf{unitaryBQTIME}\left[k \cdot f\right]_{\delta+\exp(-k)}$ then $\mathsf{A} \not\subset \mathsf{BQTIME}\left[\frac{f}{n^\nu}\right]$ for some $\nu \geq 1$.*

Proof [Proof Sketch] The proof works the same ways as Lemma 48 and using the same language. This is because in the proof of Lemma 48, we argue that if $\mathsf{A} \subset \mathsf{BQTIME}\left[\frac{f}{n^\nu}\right]$ then the description of any unitary in $\mathsf{unitaryA}_\delta$ could be learned to sufficient accuracy in $O(k \cdot f)$ time, presenting a contradiction. ■

Lemma 77 *For every fixed $k \in \mathbb{N}$,*

$$\mathsf{pureUnitaryPSPACE}_0 \not\subset \mathsf{pureUnitaryBQSIZE}[n^k]_{0.98}.$$

Proof [Proof Sketch] The proof of Theorem 62 involves finding a unitary V such that all unitaries U_i that can be synthesized by circuits in $\mathsf{BQSIZE}[n^k]$ cannot create the same state as V when acting on the all zeros state. In fact, no U_i can create a state that is even 0.49-close in Trace Distance. It follows by the definition of Diamond Distance that $d_\diamond(U_i, V) > 0.98$ for all U_i.[19] Since this holds for every k, we find that $\mathsf{pureUnitaryPSPACE}_0 \not\subset \mathsf{pureUnitaryBQSIZE}[n^k]_{0.98}$. ■

19. Recall that Diamond Distance lies in $[0, 2]$.

G.1. Pseudorandom Unitaries

We start by adapting our pseudorandom objects from quantum states to unitaries, which was a notion also introduced by Ji et al. (2018).

Definition 78 (PRU) *Let $\kappa, \ell, m : \mathbb{N} \to \mathbb{N}$, let $s : \mathbb{N} \to \mathbb{R}^+$, and let $\varepsilon : \mathbb{N} \to [0,1]$. We say that a sequence of keyed pure unitaries $\left(\{U_k\}_{k\in\{0,1\}^\kappa}\right)_{n\in\mathbb{N}}$ is an infinitely-often $(\kappa, \ell, m, s, \varepsilon)$-PRU if for a uniformly random $k \in \{0,1\}^\kappa$, no quantum algorithm running in time s can distinguish m queries of U_k from m queries to a Haar random unitary on ℓ qubits by at most ε. Formally, for all s-time-uniform quantum oracle circuits $(C_n^{(\cdot)})_{n\in\mathbb{N}}$ that output the one qubit state $\rho_n^{\mathcal{O}}$ when querying oracle $\mathcal{O}$:*

$$\left| \underset{k\sim\{0,1\}^\kappa}{\boldsymbol{E}} \operatorname{tr}\left[|1\rangle\langle 1| \cdot \rho_n^{U_k}\right] - \underset{\mathcal{U}\sim\mu_{\text{Haar}}}{\boldsymbol{E}} \operatorname{tr}\left[|1\rangle\langle 1| \cdot \rho_n^{\mathcal{U}}\right] \right| \leq \varepsilon$$

holds on infinitely many $n \in \mathbb{N}$.

Metger et al. (2024) recently introduced the PFC construction and showed non-adaptive security. Follow-up work by Ma and Huang (2024) showed that this construction was in-fact adaptively-secure, as well as that the related $CPFC$ construction is secure against inverse queries. Such PRUs that are secure against inverse queries will be reffered to as *strong* PRUs, though it should be understood that all of the PRU constructions we deal with in this work are *strong*.

We now begin to detail the improved construction used in *further* follow-up work by Schuster et al. (2025). We start by defining a Feistel network (also known as a Luby-Rackoff cipher), which is a specific way of constructing "pseudorandom" permutations from pseudorandom functions.[20]

Definition 79 *A k-round Feistel network is a permutation $LR(F_1, \dots, F_k) \in \mathfrak{F}_{\ell,\ell}$ constructed using functions $F_1, \dots, F_k \in \mathfrak{F}_{\ell/2,\ell/2}$ as follows: Split the input into two $n/2$-bit strings $x = (\ell_0, r_0)$. For each round $i = 1, \dots, k$, $\ell_{i+1} = r_i$ and $r_{i+1} = \ell_i \oplus F_i(r_i)$. Output (ℓ_k, r_k).*

We also need a phase unitary, which we implicitly saw a version of in Lemma 43. Unfortunately, due to a technicality of Ma and Huang (2024) involving non-binary phase functions, we will need to work over qudits rather than just qubits. Thus we will update our definition of an oracle from Definition 38.

Definition 80 (Qudit Quantum Oracle) *Given a function $f : \{0,1\}^\ell \to \{0,1,\dots,d-1\}$, we define the quantum oracle for f to be*

$$\mathcal{O}_f \coloneqq \sum_{\substack{x\in\{0,1\}^\ell \\ y\in\{0,1,\dots,d-1\}}} |x, y + f(x) \pmod{d}\rangle\langle x, y| \,.$$

Definition 81 (Phase Unitary) *For $F : \{0,1\}^\ell \to \{0,1,\dots,d-1\}$ define the phase unitary on ℓ qubits as:*

$$U_F |x\rangle \coloneqq e^{\frac{i2\pi F(x)}{d}} |x\rangle \,.$$

20. It is unknown whether the permutations we use are truly quantum-secure pseudorandom, but they will suffice for our purposes.

Fact 82 *For $F : \{0,1\}^\ell \to \{0,1,2,3\}$, U_F can be constructed exactly from a single call to $\mathcal{O}_{\mathcal{F}}$ using one ancilla qudit, 4 additional Hadamard gates, 6 additioanl T gates, and 5 additional* CNOT *gates.*

Proof Let QFT refer to the Quantum Fourier transform on 2-qubits. If we apply $I^{\otimes \ell} \otimes \mathrm{QFT}$ and then $\mathcal{O}_F$ to $|x\rangle |1\rangle$, we get the state

$$|x\rangle \sum_{y \in \{0,1\}^k} i^y |y + F(x) \pmod m\rangle = i^{F(x)} |x\rangle \sum_{y \in \{0,1\}^k} i^y |y\rangle .$$

Tracing out the ancilla qudit gives us the desired transformation. The cost of implementing QFT is 2 additional Hadamard and T gates respectively, and 5 additional CNOT gates (see Nielsen and Chuang, 2002, Section 5.1, namely Box 5.1 and Exercise 5.4). The initial X gate can be constructed using $HT^4H = HZH = X$. ■

Lastly, we need the following fact about efficient sampling of Clifford circuits.

Lemma 83 (Van Den Berg, 2021) *There is a classical algorithm that samples a uniformly random element of the n-qubit Clifford group and outputs a Clifford circuit implementation in time $O(n^2)$.*

We are now ready to state the improved result of Schuster et al. (2025) that shows that the quantum-secure pseudorandom permutation in the CPFC construction can be replaced by a 2-round Feistel network.

Lemma 84 (Schuster et al., 2025) *For $d \geq 3$, let $F_1 \in \{0,1\}^\ell \to \{0,1,\ldots,d-1\}$, and $F_2, F_3 \in \mathfrak{F}_{\ell/2,\ell/2}$ be drawn uniformly at random, and let C and D be independent random Clifford circuit on ℓ qubits. If $\mathcal{U}$ is drawn as an ℓ-qubit Haar random unitary, then for any oracle circuit $\mathcal{A}^{(\cdot)}$ that makes at most m queries (or inverse queries): $\mathcal{A}^{D\cdot LR(F_3,F_2)\cdot U_{F_1}\cdot C}$ is $O\left(\frac{m^2}{2^\ell}\right)$-close to $\mathcal{A}^{\mathcal{U}}$ in expected Diamond Distance.*

Naturally, we will now work to build a strong PRU from a PRG such that we can combine it with Lemma 45.

Lemma 85 *Let G be an infinitely-often $(\kappa, m, s, \varepsilon)$-PRG against uniform quantum computations that is computable in time t by a deterministic Turing machine. Then for $\ell \leq \lfloor \log_2 \frac{m}{4} \rfloor$, there exists an infinitely-often*

$$\left(\kappa + O(\ell^2),\, \ell,\, q,\, s - O\left(q \cdot m\right)),\, \varepsilon + O\left(\frac{q^2}{2^\ell}\right)\right) \textit{ strong PRU}$$

against uniform quantum computations that can be computed in time $O(t)$.

Proof We need to split up the output of the PRG to get two infinitely-often $(\kappa, 2^{\ell/2} \cdot \frac{\ell}{2}, s, \varepsilon)$-PRG and one infinitely-often $(\kappa, 2^{\ell+1}, s, \varepsilon)$-PRG. Note that this ensures that the three PRGs are hard instances at the *same* time, as opposed to three infinitely-often PRGs that may only be hard on different input lengths. To make sure that we have enough bits for this, note that $2^{\ell/2} \cdot \ell \leq 2^{\ell+1}$. Therefore the total number of bits needed is

$$2^\ell 2 \cdot \frac{\ell}{2} \cdot 2 + 2^\ell \leq 2^{\ell+2} \leq m$$

for $\ell \le \lfloor \log_2 \frac{m}{4} \rfloor$.

We will use the infinitely-often $(\kappa, 2^{\ell+1}, s, \varepsilon)$-PRG and Lemma 40 to create an infinitely-often $(\kappa, \ell, 2, q, s - O(q \cdot 2^{\ell}), \varepsilon)$-PRF, $F_1' \in \mathfrak{F}_{\ell,2}$. We can then transform the oracle $O_{F_1'}$ to an oracle for $F_1 : \{0,1\}^{\ell} \to \{0,1,2,3\}$ by implementing a simple 2-bit adder circuit modulo 4. This can be done using a constant number of Toffoli gates and some ancilla qubits. Using Fact 82, we can construct U_{F_1} exactly and efficiently.

Likewise, using Lemma 40 on the two infinitely-often $(\kappa, 2^{\ell/2} \cdot \frac{\ell}{2}, s, \varepsilon)$-PRG we can create create two infinitely-often $\left(\kappa, \ell/2, \ell/2, q, s - O(q \cdot 2^{\ell}), \varepsilon\right)$-PRF $F_2, F_3 \in \mathfrak{F}_{\ell/2,\ell/2}$. Using $O(\ell)$ SWAP operators, we can then construct LR (F_3, F_2) exactly.

Sampling two independent Clifford circuits on ℓ-qubits takes $O(\ell^2)$ time (Lemma 83). This allows us to fully construct the CPFC strong PRU in additional time $O(m + \ell^2) = O(t)$. Therefore, by a standard hybrid argument the strong PRU is secure against $s - O(q \cdot m)$-time adversaries. The key length becomes $\kappa + O(\ell^2)$ to account for the sampling of the random Clifford circuits. By the reverse Triangle inequality, Definitions 73, 10 and 84, the allowed advantage is $\varepsilon + O\left(\frac{q^2}{2^{\ell}}\right)$. ■

Corollary 86 *Suppose there exists a $\gamma > 0$ such that $\mathsf{PSPACE} \not\subset \mathsf{BQTIME}\left[2^{n^{\gamma}}\right]$. Then, for some choice of constants $\alpha \ge 1$, and $\lambda \in (0, 1/5)$ and sufficiently large $n \in \mathbb{N}$, there exists an infinitely-often*

$$\left(\kappa, \lfloor \log_2 \frac{r}{4} \rfloor, q, s, \frac{1}{r} + O\left(\frac{q^2}{2^{\ell}}\right) + \mathrm{poly}(\kappa)\right) \textit{ strong PRU}$$

against uniform quantum computations where $\kappa \le n^{\alpha}$, $r = \lfloor 2^{n^{\lambda}} \rfloor$, $s = 2^{n^{2\lambda}}$, and $q = o\left(\frac{s}{r}\right)$. In addition, the PRU lies in $\mathsf{pureUnitaryBQE}_{\mathrm{exp}}$.

Proof Combine Lemmas 45 and 85 with $\varepsilon' = \exp(-\mathrm{poly}(\kappa))$. Since the number of qubits $\ell = \lfloor \log_2 \frac{r}{4} \rfloor = O(n^{\lambda})$, we can choose a value of α that is slightly bigger than both the key size of Lemma 45 and 2λ. ■

G.2. Unitary Distinguishing Implies Non-Uniform Unitary Synthesis Lower Bounds

Informally, define (m, t, ε)-distinguishing of unitaries from Haar random unitaries to be analogous to distinguishing states from Haar random states (Definition 52). For our purposes, the distinguisher will be allowed access to inverse queries of the unknown unitary, along with adaptivity.

We start by showing that unitary learning is robust to small perturbations, like state learning in Lemma 53

Lemma 87 *Let $\mathcal{C}$ be a class of unitaries that is (m, t, ε)-distinguishable and let $\mathcal{C}_{\delta}$ be the class of unitaries δ-close to $\mathcal{C}$ in diamond distance. Then $\mathcal{C}_{\delta}$ is $(m, t, \varepsilon - m\frac{\delta}{2})$-distinguishable.*

Proof Let $V \in \mathcal{C}$ be the closest state in $\mathcal{C}$ to $U \in \mathcal{C}_{\delta}$ such that $d_{\diamond}(U, V) \le \delta$.

Finally, let $(A_n^{\cdot})_{n \in \mathbb{N}}$ form the distinguisher for $\mathcal{C}$ that uses at most m queries and time t. Then by the subadditivity of diamond distance under tensor product and composition

$$\left| \mathrm{tr}\left[|1\rangle\langle 1| \cdot A_n^{U}\right] - \mathrm{tr}\left[|1\rangle\langle 1| \cdot A_n^{V}\right] \right| \le m\frac{\delta}{2}$$

By the triangle inequality, the distinguishing power of (C_n) is at least $\varepsilon - m\frac{\delta}{2}$. ■

Lemma 88 *For arbitrary fixed $f : \mathbb{N} \to \mathbb{R}^+$ and $\delta : \mathbb{N} \to [0,1]$, let $\mathfrak{C}$ be a circuit class that is closed under restrictions and define $\mathcal{C}_\ell$ to be the set of pure states on ℓ qubits that can be constructed by $\mathfrak{C}[f(\ell)]$. Assume the existence of an infinitely-often $(\kappa, \ell, q, s, \varepsilon)$ strong PRU against uniform quantum computations that can be computed in time t. If the concept class $\mathcal{C} := \bigcup_{\ell \geq 1} \mathcal{C}_\ell$ is $\left(q \circ \ell^{-1},\, s \circ \ell^{-1},\, \varepsilon \circ \ell^{-1} + m \circ \ell^{-1} \cdot \delta\right)$-distinguishable then*

$$\mathsf{pureUnitaryBQTIME}\left[t \circ \kappa^{-1}\right]_{\exp} \not\subset \mathsf{pureUnitary}\mathfrak{C}\left[f \circ \ell \circ \kappa^{-1}\right]_{\delta}.$$

Proof [Proof Sketch] The proof follows the same way as in Lemma 64, except using Lemma 87 in place of Lemma 53. This change from $\sqrt{m}$ to simply $\frac{m}{2}$ does not affect the proof as it is still killed by the $\delta = \exp(-p)$ term for arbitrary polynomial p. ■

Theorem 89 (Formal Statement of Theorem 4) *Let $\mathfrak{C}$ be a circuit class that is closed under restrictions. Define $\mathcal{C}_\ell$ to be the set of unitaries on ℓ qubits that can be exactly constructed by $\mathfrak{C}[\mathrm{poly}(\ell)]$. If there exists a fixed constant $c \geq 2$ such that $\mathcal{C} := \bigcup_{\ell \geq 1} \mathcal{C}_\ell$ is (m, t, ε)-distinguishable for $m \leq 2^{\ell^{0.99}}$, $t \leq O\left(2^{\ell^c}\right)$, and $\varepsilon \geq \omega\left(\frac{1}{2^{\ell^{0.99}}}\right)$, then at least one of the following is true:*

- *for every $k \geq 1$:* $\mathsf{pureUnitaryBQSUBEXP}_{\exp} \not\subset \mathsf{pureUnitaryBQSIZE}[n^k]_{0.49}$,
- $\mathsf{pureUnitaryBQE}_{\exp} \not\subset \mathsf{pureUnitary}\mathfrak{C}_{\exp}$.

Proof [Proof Sketch] We instantiate the win-win argument in the same way as Theorems 65 and 66, but replacing the PRS with the strong PRU from Corollary 86 and with the win-win cases based on the relationship between $\mathsf{pureUnitaryPSPACESIZE}_{\exp}$ and $\mathsf{pureUnitaryBQSUBEXP}_{\exp}$ instead. When $\mathsf{pureUnitaryPSPACESIZE}_{\exp} \subset \mathsf{pureUnitaryBQSUBEXP}_{\exp}$ then we apply Theorem 77. In contrast, when $\mathsf{pureUnitaryPSPACESIZE}_{\exp} \not\subset \mathsf{pureUnitaryBQSUBEXP}_{\exp}$ we use Lemma 76 to show that $\mathsf{PSPACE} \not\subset \mathsf{BQSUBEXP}$. This allows us to use Corollaries 86 and 88 to complete the proof using a similar analysis to Theorems 65 and 66 ■

Remark 90 *Distinguishing copies of a fixed quantum state from Haar random actually follows as a special case of algorithms that distinguish unitaries from Haar random. This makes distinguishing with unitary query access strictly easier, and it intuitively follows that the resulting separation is weaker, as state synthesis separations imply unitary synthesis separations.*

Appendix H. Decision Problem Circuit Lower Bounds from Unitary Learning

In Section F, we showed how to use the ability to distinguish from Haar random states (as well as state learning) to get results about circuit lower bounds for decision problems. We now generalize this result to show that distinguishing from Haar random unitaries can also get results about circuit lower bounds for decision problems. Note that unitary distinguishing from Haar random is strictly easier than distinguishing states from Haar random, meaning that the result in this section is strictly more powerful than Theorem 72 in that regard. However, we lose the fine-grained relationship with depth, as the conversion from PRF to PRU involves increasing the depth by a large constant.[21]

Like Theorem 72, we need some additional assumptions imparted by the CPFC construction of Schuster et al. (2025). The first is the ability to take a (pseudorandom) function and implement the phase unitary modulo 4 (see Definition 81). The second is to be able to take (pseudorandom) functions and construct Feistel networks (see Definition 79), which can be done using SWAP gates. Third, we once again need to be able to perform error reduction. Lastly, one needs to be able to implement Clifford unitaries. Luckily, these assumptions are still satisfied by QAC^0_f, so for succinctness, we will again refer to these requirements as the circuit class satisfying $\mathfrak{C} \supseteq \mathsf{QAC}^0_f$.

Fact 91 (Aaronson and Gottesman, 2004; Rosenthal, 2023) *Every Clifford circuit has an equivalent QAC^0_f circuit.*

We now need to take a PRF and turn it into a strong PRU. The construction will again use the CPFC construction, but now we need break up the PRF into smaller PRFs to instantiate it.

Fact 92 (Folklore) *Every infinitely-often $(\kappa, \ell, 1, q, s, \varepsilon)$-PRF computable it time t can be turned into an infinitely-often $(d \cdot \kappa, \ell', d, q, s - O(q \cdot d \cdot t), \varepsilon)$-PRF for $\ell' \leq \ell$ that is computable in time $O(d \cdot t)$.*

Proof Break apart the key into d κ-bit length strings, $k_1, \ldots, k_d$. Take the PRF $\{F_k\}$ and compute the concatenation of $F_{k_1}(x), \ldots, F_{k_d}(x)$ to get the new PRF. Security follows by a hybrid argument. ■

Lemma 93 *Assume the existence of an infinitely-often $(\kappa, \ell, 1, q, s, \varepsilon)$-PRF against uniform quantum computations that is computable in time t by a deterministic Turing machine. Then there exists an infinitely-often*

$$\left(O\left(\ell \cdot (\kappa + \ell)\right), \ell, q, s - O\left(q \cdot \ell(t + \ell)\right)), \varepsilon + O\left(\frac{q^2}{2^\ell}\right)\right) \textit{ strong PRU}$$

against uniform quantum computations that can be computed in time $O(t)$.

Proof We need to take our single PRF and use Fact 92 three times to construct two infinitely-often $(\kappa \cdot \ell/2, \ell/2, \ell/2, q, s - O(q \cdot \ell \cdot t), \varepsilon)$-PRF ($F_2$ and F_3) and one infinitely-often $(\kappa, \ell, 2, q, s - O(q \cdot t), \varepsilon)$-PRF ($F_1'$). Note that this ensures that the three PRFs are hard instances at the *same* time. We can then transform the oracle $O_{F_1'}$ to an oracle for $F_1 : \{0,1\}^\ell \to \{0,1,2,3\}$ by implementing a simple 2-bit adder circuit modulo 4. This can be done using a constant number of Toffoli gates and some ancilla qubits. Using Fact 82, we can construct U_{F_1} exactly and efficiently. Likewise, using $O(\ell)$ SWAP operators, we can construct LR (F_3, F_2) exactly.

Sampling two Clifford circuits on ℓ-qubits takes $O(\ell^2)$ time (Lemma 83). This allows us to fully construct the CPFC strong PRU in additional time $O(\ell^2 + \ell t)$.

By a standard hybrid argument the strong PRU is secure against $s - O\left(q \cdot \ell \cdot (t + \ell)\right)$-time adversaries. The key length becomes $(\ell + 1) \cdot \kappa + O(\ell^2)$ to account for the sampling of the random

21. This constant could be explicitly worked out, but it appears to be too large to be useful for anything.

Clifford circuit. By the reverse Triangle inequality, Definitions 73, 10 and 84, the allowed advantage is $\varepsilon + O\left(\frac{q^2}{2^\ell}\right)$. ■

Now that we can build a strong PRU from a PRF, the important step is to realize that if a PRF can be computed by QAC^0_f then so can a strong PRU be synthesized using said PRF. That is, the reduction in Lemma 93 only increases the QAC_f-depth by a constant.[22] Using this allows us to show our desired results about learning and decision problem separations.

Lemma 94 *For arbitrary fixed $f : \mathbb{N} \to \mathbb{R}^+$ and $\delta : \mathbb{N} \to [0,1]$, let $\mathfrak{C} \supseteq \mathsf{QAC}^0_f$ be a circuit class that is closed under restrictions and define $\mathcal{C}_\ell$ to be the set of unitaries on ℓ qubits that can be constructed by $\mathfrak{C}\left[f(\ell) + \mathrm{poly}(\ell)\right]$. Assume the existence of an infinitely-often $(\kappa, \ell, 1, m, s, \varepsilon)$-PRF against uniform quantum computations that can be computed in time t by a deterministic Turing machine. If the concept class $\mathcal{C} := \bigcup_{\ell \geq 1} \mathcal{C}_\ell$ is $\left(m \circ \ell^{-1},\, s \circ \ell^{-1},\, \varepsilon \circ \ell^{-1} + m \circ \ell^{-1} \cdot \delta/2\right)$-distinguishable then*

$$\mathsf{DTIME}\left[t \circ (\ell^2 + \ell\kappa)^{-1}\right] \not\subset \mathfrak{C}\left[f \circ \ell \circ (\ell^2 + \ell\kappa)^{-1}\right].$$

Proof Let $\left(\{F_k\}_{k \in \{0,1\}^{\kappa(n)}}\right)_{n \in \mathbb{N}}$ be the the infinitely-often PRF against uniform quantum computations. Define the language L such that inputs $(x,k) \in L$ if and only if $F_k(x) = 1$ when $x \in \{0,1\}^\ell$ and $k \in \{0,1\}^\kappa$. Because the PRF is computable in time t by a deterministic Turing machine, L lies in $\mathsf{DTIME}\left[t \circ \kappa^{-1}\right]$.

We now need to show that L is not in $\mathfrak{C}\left[f \circ \ell \circ \kappa^{-1}\right]$. For the sake of contradiction, assume that it was. Then using Lemma 93 and error-reduction via majority and fanout, $\mathfrak{C}\left[\mathrm{poly}(n) + f \circ \ell \circ \kappa^{-1}(n)\right]$ can create strong pseudorandom unitariess. The fact that the depth only increases by a constant follows from the fact that $\mathfrak{C} \supset \mathsf{QAC}^0_f$ allows us to perform (1) arbitrary classical fanout, (2) approximately compute the PRF, (3) take the majority to perform error reduction, (4) implement Fact 82, (5) implement the SWAP gates needed for the Feistel network, (6) implement the modulo 4 adder circuit to take a function from $\mathfrak{F}_{\ell,2}$ to $\{0,1\}^\ell \to \{0,1,2,3\}$, and (7) exactly implement a Clifford circuit, all in constant depth. The size increase, however, is polynomial.

Relative to the security parameter n: the number of samples used by the distinguishing algorithm is $m \circ \ell^{-1} \circ \ell = m(n)$, the running time is $O\left(s \circ \ell^{-1} \circ \ell\right) = O(s(n))$, and the advantage is $\varepsilon \circ \ell^{-1} \circ \ell + m \circ \ell^{-1} \circ \ell \cdot \delta/2 = \varepsilon + m \cdot \delta/2$. Finally, the size of the circuits generating $\mathcal{C}_\ell$ are $O\left(f \circ \ell\right) = O\left(f \circ \ell \circ \kappa^{-1} \circ \kappa\right)$ such that the size relative to the key parameter κ is $O\left(f \circ \ell \circ \kappa^{-1}\right)$. It follows by the parameters of the strong PRU and Lemma 87 that if $\mathcal{C}$ could be learned then the strong PRU does not lie in $\mathsf{pureState}\mathfrak{C}\left[f \circ \ell \circ (\ell^2 + \ell\kappa)^{-1}\right]_\delta$. This is a contradiction, meaning that $L \notin \mathfrak{C}\left[f \circ \ell \circ (\ell^2 + \ell\kappa)^{-1}\right]$. ■

Theorem 95 (Formal statement of Theorem 5) *Let $\mathfrak{C} \supseteq \mathsf{QAC}^0_f$ be a circuit class that is closed under restrictions. Define $\mathcal{C}_\ell$ to be the set of unitaries on ℓ qubits that can be exactly constructed by $\mathfrak{C}[\mathrm{poly}(\ell)]$ with constant depth. If there exists a fixed constant $c \geq 2$ such that $\mathcal{C} := \bigcup_{\ell \geq 1} \mathcal{C}_\ell$ is (m,t,ε)-distinguishable for $m \leq 2^{\ell^{0.99}}$, $t \leq O\left(2^{\ell^c}\right)$, and $\varepsilon \geq \frac{1}{2^{\ell^{0.99}}}$, then at least one of the following must be true:*

22. This is actually a stronger statement than that of Ma and Huang (2024); Schuster et al. (2024) showing that the CPFC construction exists in QNC^1 assuming the existence of shallow-depth PRF, such as via LWE.

- *for all* $k \geq 1$, $\mathsf{BQSUBEXP} \not\subset \mathsf{BQSIZE}\left[n^k\right]$,
- $\mathsf{E} \not\subset \mathfrak{C}[\mathrm{poly}(n)]$.

Proof [Proof Sketch] We will again use a win-win argument, but now with PSPACE and BQSUBEXP. If $\mathsf{PSPACE} \subseteq \mathsf{BQSUBEXP}$ then using Lemma 71, we get $\mathsf{BQE} \not\subset \mathsf{BQSIZE}[n^k]$.

On the other hand, if $\mathsf{PSPACE} \not\subseteq \mathsf{BQSUBEXP}$ then we can invoke Corollary 46 to show that there exists some infinitely-often $(\kappa, \ell, 1, q, s, \varepsilon)$-PRF against uniform quantum computations where $\kappa(n) \leq n^\alpha$, $r(n) = \lfloor 2^{n^\lambda} \rfloor$, $\ell \leq \lfloor \log_2 r \rfloor$, and $s(n) = 2^{n^{2\lambda}}$. By Lemma 94 and a similar analysis to Theorem 72, we find that $\mathsf{E} \not\subset \mathfrak{C}[\mathrm{poly}(n)]$. ■

Appendix I. Approximating Trace Distance in Polynomial Space

We combine the ideas behind the proof sketch of Watrous (2002, Corollary 10 and Proposition 11) with the proof that $\mathsf{BQP} \subseteq \mathsf{PSPACE}$ (Bernstein and Vazirani, 1997) to show that the trace distance of states produced by $\mathrm{poly}(n)$ size general quantum circuits can be computed using only $\mathrm{poly}(n)$ space by a deterministic Turing machine (i.e., Lemma 61).

To start, we show the folklore result(s) that, when represented as a matrix, any state ρ that is produced by a general quantum circuit of size $\mathrm{poly}(n)$ can have its entries be approximated to arbitrary inverse exponential precision in $\mathrm{poly}(n)$ space (Nielsen and Chuang, 2002, Section 4.5.5).[23] To do so, we first start with applying the unitary (Lemma 96), then tracing out the ancilla qubits (Corollary 97).

For ease of notation, we will say that a value can be computed in $\mathrm{poly}(n)$ space if the value can be approximated to arbitrary $\exp(-\mathrm{poly}(n))$ accuracy in $\mathrm{poly}(n)$ space. This way, if an expression consists only of $\mathrm{poly}(n)$-space computable values, the terms are all bounded in $[-1, 1]$ and there are only $O(\exp(\mathrm{poly}(n)))$-many values, then the triangle inequality and Cauchy-Schwarz ensures us that the whole expression can be approximated to arbitrary $\exp(-\mathrm{poly}(n))$ accuracy in $\mathrm{poly}(n)$ space (i.e., computed in $\mathrm{poly}(n)$ space).

Lemma 96 (Folklore) *Given* unitary *quantum circuit C of size $s \leq 2^{\mathrm{poly}(n)}$ and space $m = \mathrm{poly}(n)$ and a quantum state ρ on at most m qubits whose entries (i.e., $\rho_{ij} := \langle i|\rho|j\rangle$) can computed in $\mathrm{poly}(n)$ space, the entries of $C\rho C^\dagger$ can also be computed in $\mathrm{poly}(n)$ space.*

Proof The proof idea is similar to the one showing that $\mathsf{BQP} \subseteq \mathsf{PSPACE}$. Let C be broken up into its elementary gates as $C := C_1 C_2 \dots C_s$. Since $I = \sum_{y \in \{0,1\}^m} |y\rangle\langle y|$, we can rewrite the output expression as:

$$\begin{aligned}\langle i|C\rho C^\dagger|j\rangle &= \langle i|C_1C_2\dots C_s\rho C_s^\dagger \dots C_2^\dagger C_1^\dagger|j\rangle \\ &= \sum_{y_1, y_2, \dots, y_{2s} \in \{0,1\}^m} \langle i|C_1|y_1\rangle \langle y_1|C_2|y_2\rangle \dots \langle y_{s-1}|C_s|y_s\rangle \langle y_s|\rho|y_{s+1}\rangle \dots \langle y_{2s}|C_1^\dagger|j\rangle .\end{aligned}$$

Since each $C_i \in \{H, T, \mathrm{CNOT}\}$, each $\langle y_i|C_{i+1}|y_{i+1}\rangle$ must lie in the set $\{0, \pm\frac{1}{\sqrt{2}}, 1, i\}$. Therefore, each $\langle y_i|C_{i+1}|y_{i+1}\rangle$ can be computed exactly using $\mathrm{poly}(m)$ space.[24] Furthermore, we observe

23. In the language of Rosenthal (2024, Definition 5.1), these would be considered polyL-explicit.
24. If we weren't using the $\{H, \mathrm{CNOT}, T\}$ gate set, then we can just use the Solovay-Kitaev algorithm to approximate it with the $\{H, \mathrm{CNOT}, T\}$ gate set to sufficient error. This will not affect the amount of space used by more than a polynomial.

that each term in the above summation is the product of $2s$ many $\langle y_i|C_{i+1}|y_{i+1}\rangle$ multiplied by $\langle y_s|\rho|y_{s+1}\rangle$, such that the product either has the form $\langle y_s|\rho|y_{s+1}\rangle \frac{i^\ell}{\sqrt{2}^k}$ for $\ell \in \{0,1,2,3\}$ and $k \in \{0,\ldots,2s\}$ or is just zero. Either way, it can be computed using $\mathrm{poly}(n,m,\log s)$ space. It follows that the entire summation can be approximated to accuracy $\exp(-k)$ in $\mathrm{poly}(n,m,\log s,k) = \mathrm{poly}(n,k)$ space by approximating up to $\mathrm{poly}(k)$-bits of precision. ■

Corollary 97 (Folklore) *Given a* unitary *quantum circuit C of size $s \leq 2^{\mathrm{poly}(n)}$ and space $m = \mathrm{poly}(n)$ and let ρ be the output of C. The (i,j)-th entry of ρ (i.e., $\rho_{ij} \coloneqq \langle i|\rho|j\rangle$) can be computed in $\mathrm{poly}(n)$ space.*

Proof Any unitary circuit can be decomposed into the unitary stage and then the tracing out stage at the end. Since it is clear that the entries of our starting state, $|0\ldots0\rangle\langle0\ldots0|$ can be computed in $\mathrm{poly}(n)$ space, it follows from Lemma 96 that after applying the unitary to the all-zeros state, the new quantum state's entries can be computed in $\mathrm{poly}(n)$ space. We then need to figure out the effect of tracing out at most $\mathrm{poly}(n)$-qubits.

We can assume WLOG that we trace out the final qubit(s) because we use SWAP gates at the end of the unitary to move the qubits that will be traced out to the end. If we are tracing out $k = \mathrm{poly}(n)$ qubits, we can then express the new entries to compute as:

$$\begin{aligned}\langle i|C\rho C^\dagger|j\rangle &= \langle i|\left(\sum_{x\in\{0,1\}}\left(I^{\otimes m-k}\otimes\langle x|\right)\rho\left(I^{\otimes m-k}\otimes|x\rangle\right)\right)|j\rangle\\ &= \sum_{x\in\{0,1\}^k}\langle i,x|\rho|j,x\rangle\,,\end{aligned}$$

which is just the sum of $\exp(\mathrm{poly}(n))$-many things that we can compute in $\mathrm{poly}(n)$ space. ■

We now move onto the problem of approximating trace distance. To compute the trace distance between these two states, we need to find the sum of the absolute value of its eigenvalues. The following two results will allow us to find the roots of the characteristic polynomial (i.e., the eigenvalues) of $\rho - \sigma$.

Lemma 98 (Ben-Or et al., 1988; Neff, 1994) *Given a polynomial $p(z)$ of degree d with m-bit coefficients and an integer μ, the problem of determining all its roots with error less than $2^{-\mu}$ is considered. It is shown that this problem can be solved by a* $\mathrm{polylog}\,(d+m+\mu)$*-space-uniform* Boolean *circuit of depth at most* $\mathrm{polylog}\,(d+m+\mu)$ *on* $\mathrm{poly}\log(d+m+\mu)$ *many bits if $p(z)$ has all real roots.*

Lemma 99 (Borodin, 1977, Lemma 1) *A* space-uniform *Boolean circuit of size s and depth d can be simulated by a deterministic Turing machine in space at most $d + \log(s)$.*

By combining Lemmas 98 and 99, we get that the roots of certain polynomials can be approximate to high precision in $\mathrm{poly}(n)$ space.

We now have the ingredients necessary to show that the trace distance of states produced by $O\left(2^{\mathrm{poly}(n)}\right)$-size and $\mathrm{poly}(n)$-space unitary quantum circuits can also be approximated to high precision in $\mathrm{poly}(n)$ space.

Lemma 100 *Let ρ and σ be two n-qubit quantum states that are produced by* unitary *quantum circuits of size at most $2^{\mathrm{poly}(n)}$ and space $\mathrm{poly}(n)$. Then $d_{\mathrm{tr}}(\rho, \sigma)$ can be approximated to arbitrary $\exp(-\mathrm{poly}(n))$ error by a deterministic Turing machine in $\mathrm{poly}(n)$ space.*

Proof By Corollary 97, each entry of both ρ and σ can be approximated to high accuracy using $\mathrm{poly}(n)$ space, so each entry of $\rho - \sigma$ can also be well approximated. From here, let $f(x)$ be the characteristic polynomial of $\rho-\sigma$. It follows that any coefficient of $f(x)$ can be highly approximated using $\mathrm{poly}(n)$ space as well, via the Faddeev-Leverrier algorithm (Csanky, 1975, Corollary 2).[25]

We note that the characteristic polynomial of $\rho - \sigma$ has a degree 2^n with all real roots. It follows from Lemmas 98 and 99 that $d_{\mathrm{tr}}(\rho, \sigma) := \frac{1}{2}\sum_i |\lambda_i|$ can be computed by a deterministic Turing machine in $\mathrm{poly}(n)$ space. ■

Appendix J. Trivial Learners

Observe that in Corollaries 66 and 72, there are three important parameters of the algorithm that all must simultaneously meet some condition. In this section, we highlight how satisfying any two of these conditions is trivially easy for states produced by polynomial-size unitary quantum circuits. Clearly, if samples are not a concern then full pure state tomography can be done in $2^{O(n)}$ time to constant advantage (França et al., 2021). If one instead wants to satisfy the advantage and sample requirements, for instance, then one can run an exhaustive search using classical shadows (Huang et al., 2020; Bădescu and O'Donnell, 2021; Zhao et al., 2023) over all unitary circuits of size at most $\omega(\mathrm{poly}(n))$. This will only use $\omega(\mathrm{poly}(n))$ samples, but the time complexity will be $2^{\omega(\mathrm{poly}(n))}$.

Finally, if only $O\left(\frac{1}{2^n}\right)$ advantage is desired then no measurements even have to be taken. Specifically, by outputting a random stabilizer state, every concept class can be

$$\left(0, n^2, 1 - \frac{\theta}{2^{n+1}}, (1-\theta)^2\left(\frac{1}{2} + \frac{1}{2^{n+1}}\right)\right)\text{-learned}$$

for arbitrary $\theta \in [0, 1]$. In fact, any 2-design suffices for this argument, the only difference is how efficiently can such a state be sampled directly affects the runtime of the "learner". To this end, we recall that uniformly random stabilizer states can be efficiently sampled in $O(n^2)$ time.

To show that we are guaranteed a state with a certain fidelity, we will need to use the following anti-concentration inequality.

Lemma 101 (Paley-Zygmund inequality) *If $X \geq 0$ is a random variable with finite variance, and if $\theta \in [0, 1]$ then*

$$\boldsymbol{Pr}\left[X > \theta \cdot \boldsymbol{E}\left[x\right]\right] \geq (1-\theta)^2 \frac{\boldsymbol{E}\left[X\right]^2}{\boldsymbol{E}\left[X^2\right]}.$$

Let X be the random variable associated with the fidelity of an arbitrary quantum state with a random stabilizer state. By bounding the moments of X, we can use the Paley-Zygmund inequality to show that our learner succeeds with a certain probability.

25. In principle this approach is not numerically stable (Rehman and Ipsen, 2011; Wilkinson, 1988), such that a more numerically stable approach would be more space efficient. This is because far less bits of precision would have to be used in previous steps to compensate for the numerical instability.

Fact 102 *For arbitrary $\theta \in [0, 1]$, with probability at least $(1-\theta)^2 \left(\frac{1}{2} + \frac{1}{2^{n+1}}\right)$, a random stabilizer state $|\phi\rangle$ will have fidelity at least $\frac{\theta}{2^{n+1}}$ with an arbitrary quantum state $|\psi\rangle$.*

Proof [Proof Sketch] Because stabilizer states are a 3-design (Kueng and Gross, 2015), the values of $\mathbf{E}_{|\phi\rangle\sim\mathrm{Stab}}\left[|\langle\psi|\phi\rangle|^2\right]$ and $\mathbf{E}_{|\phi\rangle\sim\mathrm{Stab}}\left[|\langle\psi|\phi\rangle|^4\right]$ are the same as when $|\phi\rangle$ is replaced by a Haar random state. By symmetry arguments, we get

$$\mathop{\mathbf{E}}_{|\phi\rangle\sim\mathrm{Stab}}\left[|\langle\psi|\phi\rangle|^2\right] = \mathop{\mathbf{E}}_{|\phi\rangle\sim\mu_{\mathrm{Haar}}}\left[|\langle\psi|\phi\rangle|^2\right] = \frac{1}{2^n}$$

and

$$\mathop{\mathbf{E}}_{|\phi\rangle\sim\mathrm{Stab}}\left[|\langle\psi|\phi\rangle|^4\right] = \mathop{\mathbf{E}}_{|\phi\rangle\sim\mu_{\mathrm{Haar}}}\left[|\langle\psi|\phi\rangle|^4\right] = \frac{2}{2^n(2^n+1)}.$$

Since the absolute value of inner products of unit vectors are in the interval $[0, 1]$, by the Paley-Zygmund inequality:

$$\mathop{\mathbf{Pr}}_{|\phi\rangle\sim\mathrm{Stab}}\left[|\langle\psi|\phi\rangle|^2 \geq \frac{\theta}{2^n}\right] \geq (1-\theta)^2 \frac{1}{4^n}\frac{2^n(2^n+1)}{2} = (1-\theta)^2\left(\frac{1}{2} + \frac{1}{2^{n+1}}\right).$$

■

Lemma 103 *For arbitrary $\theta \in [0, 1]$, every concept class $\mathcal{C}$ can be*

$$\left(0, n^2, 1 - \frac{\theta}{2^{n+1}}, (1-\theta)^2\left(\frac{1}{2} + \frac{1}{2^{n+1}}\right)\right)\text{-learned}.$$

Proof In $O(n^2)$ time, we can sample a random n-qubit Clifford circuit using Lemma 83 and then apply it to the all-zeros state to get a random stabilizer state. By outputting this state, Fact 102 ensures us that the fidelity will be at least $\frac{\theta}{2^n}$ with probability at least $(1-\theta)^2\left(\frac{1}{2} + \frac{1}{2^{n+1}}\right)$. Using the upper bound in Fact 12, the trace distance between the unknown quantum and our random stabilizer state is at most $\sqrt{1 - \frac{\theta}{2^n}} \leq 1 - \frac{\theta}{2^{n+1}}$. ■