Quantum Search-To-Decision Reductions and the State Synthesis Problem

Sandy Irani
Department of Computer Science, University of California, Irvine, CA, USA

Anand Natarajan
CSAIL, Massachusetts Institute of Technology, Cambridge, MA, USA

Chinmay Nirkhe
Department of Computer Science, University of California, Berkeley, CA, USA
Challenge Institute for Quantum Computation, University of California, Berkeley, CA, USA

Sujit Rao
CSAIL, Massachusetts Institute of Technology, Cambridge, MA, USA

Henry Yuen
Department of Computer Science, Columbia University, New York, NY, USA

Abstract

It is a useful fact in classical computer science that many search problems are reducible to decision problems; this has led to decision problems being regarded as the *de facto* computational task to study in complexity theory. In this work, we explore search-to-decision reductions for quantum search problems, wherein a quantum algorithm makes queries to a classical decision oracle to output a desired quantum state. In particular, we focus on search-to-decision reductions for QMA, and show that there exists a quantum polynomial-time algorithm that can generate a witness for a QMA problem up to inverse polynomial precision by making one query to a PP decision oracle. We complement this result by showing that QMA-search does *not* reduce to QMA-decision in polynomial-time, relative to a quantum oracle.

We also explore the more general *state synthesis problem*, in which the goal is to efficiently synthesize a target state by making queries to a classical oracle encoding the state. We prove that there exists a classical oracle with which any quantum state can be synthesized to inverse polynomial precision using only one oracle query and to inverse exponential precision using two oracle queries. This answers an open question of Aaronson [1], who presented a state synthesis algorithm that makes $O(n)$ queries to a classical oracle to prepare an n-qubit state, and asked if the query complexity could be made sublinear.

2012 ACM Subject Classification Theory of computation → Quantum computation theory

Keywords and phrases Search-to-decision, state synthesis, quantum computing

Digital Object Identifier 10.4230/LIPIcs.CCC.2022.5

Related Version *Full Version*: https://arxiv.org/abs/2111.02999 [8]

Funding *Chinmay Nirkhe*: Supported by NSF Quantum Leap Challenges Institute Grant number OMA2016245 and an IBM Quantum PhD internship.
Henry Yuen: Supported by AFOSR award FA9550-21-1-0040 and NSF CAREER award CCF-2144219.

Acknowledgements SI, CN, and HY were participants in the Simons Institute for the Theory of Computing *Summer Cluster on Quantum Compuatation.* Additionally, we thank Aram Harrow and Zeph Landau for insightful discussions.

COMPUTATIONAL COMPLEXITY CONFERENCE
37th Computational Complexity Conference (CCC 2022).
Editor: Shachar Lovett; Article No. 5; pp. 5:1–5:19
Leibniz International Proceedings in Informatics
LIPICS Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

1 Introduction

It is a useful fact in classical computer science that *search* problems are often efficiently reducible to *decision* problems. For example, the canonical way of constructing a satisfying assignment of a given 3SAT formula φ (if there exists one) using an oracle for the decision version of 3SAT is to adaptively query the oracle for the satisfiability of φ conditioned on some partial assignment to the variables of the formula. Based on the oracle answers, the partial assignment can be extended bit-by-bit to a full assignment. Each oracle query reveals an additional bit of the assignment. This strategy generally works for any problem in NP. Likewise, the optimal value of an optimization problem can be calculated to exponential accuracy using binary search. The main consequence of this is that complexity theory often focuses on decision problems (without losing generality) and less on the complexity of search problems.

Quantum information and computation has shifted our perspective on these traditional notions of classical complexity theory. In this paper we consider *quantum* search problems, where the goal is to output a quantum state (as opposed to a classical bit string) satisfying some condition. In the quantum setting, it is no longer apparent that search-to-decision reductions still hold, and thus it is unclear whether the complexity of quantum search problems can be directly related to the complexity of corresponding quantum decision problems.

To illustrate this, we consider the analogues of P and NP in quantum computing, which are the complexity classes BQP and QMA, respectively[1]. The analogue of the NP-complete problem 3SAT for QMA is the *Local Hamiltonian* problem, in which one has to decide whether the lowest energy state of a local Hamiltonian $H = H_1 + \cdots + H_m$ acting on n qubits has energy greater than a or less than b for $a - b = 1/\mathsf{poly}(n)$, where each term H_i acts non-trivially on only a constant number of qubits. This problem was proven to be QMA-complete by Kitaev [10]. Is there an efficient search-to-decision reduction for the Local Hamiltonians problem, or more generally for the class QMA? In other words, given quantum query access to an oracle deciding the Local Hamiltonians problem, can a polynomial-time quantum algorithm (i.e. BQP machine) efficiently *prepare* a low-energy state $|\psi\rangle$ of a given local Hamiltonian?

The classical strategy of incrementally building a partial assignment does not appear to work in the QMA setting. First, there does not appear to be a natural way of "conditioning" a quantum state on a partial assignment. Second, quantum states are exponentially complex: the description size (complexity) of a general quantum state on n qubits is exponential in n, and this is suspected to remain true even when considering ground states of local Hamiltonians[2]. This complexity of quantum states poses a significant challenge to finding a search-to-decision reduction for QMA; it is not clear how yes/no answers to QMA decision problems (even when obtained in superposition) can be used to construct exponentially-complex QMA witnesses.

On the other hand, there *is* a natural quantum analogue of the bit-by-bit search-to-decision algorithm for NP that works for constructing *general* quantum states. This is due to a general algorithm for *state synthesis* described by Aaronson in [1] (for which we give

[1] Technically speaking, BQP and QMA are better thought of as the quantum analogues of BPP and MA, respectively. However, even in this randomized setting, there are efficient search-to-decision randomized reductions.

[2] Due to the QMA $\neq$ QCMA conjecture [3]. Formally, there is no known poly-sized description of a witness (proof) for every local Hamiltonian problem.

an overview of in Section 1.1): there exists a polynomial-time quantum algorithm A such that every n-qubit state $|\psi\rangle$ can be encoded into a classical oracle f where, by making $O(n)$ superposition queries to the oracle f, the algorithm A will output a state that is exponentially close to $|\psi\rangle$. One can observe that for states $|\psi\rangle$ that QMA witnesses (such as ground states of local Hamiltonians), the oracle f corresponds to a PP function (which is at least as powerful as a QMA oracle). This yields a search-to-decision reduction for QMA, albeit with a decision oracle of higher complexity.

In this work, we explore the complexity of search-to-decision procedures in the quantum setting, where the goal is a quantum *state synthesis* algorithm that outputs a *target* quantum state (e.g. a ground state of a local Hamiltonian) by making quantum queries to a classical decision oracle. We investigate how the complexity of the state synthesis algorithm and the complexity of the decision oracle depend on the type of states we want to generate. We consider both the generalized state synthesis problem for abritrary states in the Hilbert space $(\mathbb{C}^2)^{\otimes n}$ as well as the specific task of generating solutions to QMA problems.

We construct state synthesis and search-to-decision procedures for the quantum setting using only one or two superposition queries as opposed to $O(n)$ superposition queries; for QMA witnesses, the synthesis procedure requires only one query to a PP oracle. Simultaneously, we prove results suggesting the impossibility of any search-to-decision reduction for QMA. More precisely, we show that there exists a *quantum* oracle $\mathcal{O}$ relative to which *all* efficient query algorithms fail to be a good search-to-decision reduction for $\mathsf{QMA}^{\mathcal{O}}$, the relativization of QMA. This stands in contrast to classes such as NP, MA, and QCMA, which all have efficient search to decision reductions, relative to any oracle. As a consequence, proving impossibility of QMA search-to-decision without an oracle is at least as hard as separating QCMA and QMA which is at least as hard as separating P and PP. We believe that the juxtaposition of our results lend further weight to the view that the complexity of tasks where the outputs (and inputs) are quantum states cannot be directly explained by the traditional study of decision problems (which has been the main focus of quantum complexity theory to date). In particular, we believe our results suggest that the relationship between search and decision problems is much more mysterious in the quantum setting. As suggested by Aaronson in [1] and others in some recent works [11, 14], the complexity of quantum states (and more generally, quantum state transformations) deserves to be studied more deeply as a subject in its own right.

1.1 Starting point

Before describing our results in more detail, we first explain the starting point for our investigations, which is a simple state synthesis algorithm described by Aaronson [1] in his lecture notes. He shows that there exists a $\mathsf{poly}(n)$-time quantum algorithm A which makes $O(n)$ quantum queries to a classical oracle such that for every n-qubit state $|\psi\rangle = \sum_x \alpha_x |x\rangle$, there exists a classical oracle f for which the algorithm $A^{\mathcal{O}_f}$ will output a state that is $\mathsf{exp}(-n)$-close to $|\psi\rangle$. In [1], Aaronson raises the question as to whether his protocol can be improved to a sublinear number of queries. We show, in fact, that 1 query is sufficient to achieve polynomially small error in synthesizing arbitrary states and 2-queries are sufficient for exponentially small error. Both the 1-query and the 2-query algorithms given here require exponential time and polynomial space.

To understand Aaronson's state synthesis algorithm, we first observe that we can write any quantum state in the form

$$|\psi\rangle = \sum_{x \in \{0,1\}^n} e^{i\theta_x} \sqrt{\mathbf{Pr}[X = x]}\, |x\rangle \qquad (1)$$

where $\mathbf{Pr}[X = x]$ is the probability distribution of some n-bit random variable X and $\{\theta_x\}_{\{0,1\}^n}$ are a set of phases. The synthesis algorithm performs $2n$ queries to synthesize the "QSample state".

$$\sum_{x \in \{0,1\}^n} \sqrt{\mathbf{Pr}[X = x]}\ |x\rangle \tag{2}$$

and then performs two additional queries at the end to apply the phases $e^{i\theta_x}$ to each basis state $|x\rangle$.

The $2n$-query procedure to build the QSample state works in n stages. Inductively assume that after the kth stage, for $k < n$, the intermediate state of the algorithm is the k-qubit state

$$\sum_{y \in \{0,1\}^k} \sqrt{\mathbf{Pr}[X_{\leq k} = y]}\ |y\rangle \tag{3}$$

where $\mathbf{Pr}[X_{\leq k} = y]$ denotes the marginal probability of the first k bits of X are equal to y. Controlled on the prefix $|y\rangle$ the algorithm queries the oracle f to obtain a (classical description of) the conditional probabilities $\mathbf{Pr}[X_{k+1} = 0 \mid X_{\leq k} = y]$ and $\mathbf{Pr}[X_{k+1} = 1 \mid X_{\leq k} = y]$, and prepares a $(k+1)$st qubit in the state

$$\sqrt{\mathbf{Pr}[X_{k+1} = 0 \mid X_{\leq k} = y]}\ |0\rangle + \sqrt{\mathbf{Pr}[X_{k+1} = 1 \mid X_{\leq k} = y]}\ |1\rangle\ . \tag{4}$$

The algorithm performs another query to f to uncompute the descriptions of the conditional probabilities. The resulting $k+1$ qubit state is then equal to

$$\sum_{y \in \{0,1\}^{k+1}} \sqrt{\mathbf{Pr}[X_{\leq k} = y_{\leq k}]} \cdot \sqrt{\mathbf{Pr}[X_{k+1} = y_{k+1} \mid X_{\leq k} = y_{\leq k}]}\ |y\rangle \tag{5}$$

$$= \sum_{y \in \{0,1\}^{k+1}} \sqrt{\mathbf{Pr}[X_{\leq k+1} = y]}\ |y\rangle \tag{6}$$

which maintains the desired invariant. After the nth stage, a similar process applies the phases $\{\theta_x\}$ to generate the output state. The approximations come in when the conditional probabilities and phases are specified with $\mathsf{poly}(n)$ bits of precision, which result in the final state being at most $\mathsf{exp}(-n)$ far from the ideal target state $|\psi\rangle$. With this $O(n)$-query state synthesis algorithm in mind, we now proceed to describe our results.

1.2 Our results

A one-query search-to-decision algorithm for QMA with a PP oracle. We show Section 2 that in the case of generating physically relevant states, i.e. solutions to QMA problems, such as the low-energy states of local Hamiltonians, that there exists a one-query search-to-decision algorithm using a PP oracle. While one would hope to find a search-to-decision reduction in which the oracle complexity is only QMA, PP is the smallest complexity class containing QMA for which we can construct an oracular algorithm for search problems. Furthermore, given our no-go result for QMA search-to-decision (see below), this may be the optimal search-to-decision algorithm.

▶ **Theorem 1** (QMA-search to PP-decision reduction). *There exists a probabilistic polynomial time quantum algorithm making a single query to a* PP *phase oracle such that, given as input a* QMA *problem, either aborts or outputs a witness $|\phi\rangle$. The algorithm will succeed in outputting a witness (i.e. not abort) with all but inverse exponential (in the system size) probability.*

Table 1 Summary of past work and our results on upper bounds for search-to-decision reductions and state synthesis. The "complexity class" column refers to the complexity of the search problem (e.g. computing NP witnesses, or QMA witnesses). The other columns refer to the algorithmic results known for the specified number of queries; furthermore these are *quantum* queries performed by quantum algorithms in superposition.

Complexity class	1 query	2 queries	$O(n)$ queries
NP	**NP oracle, $\Omega(n^{-1})$ success probability**	←	NP oracle, classical queries (folklore)
QCMA	**QCMA oracle, $\Omega(n^{-1})$ success probability**	←	QCMA oracle, classical queries (folklore)
QMA	**PP oracle, 1/poly(n) precision, Theorem 1**	← (Theorem 4 applies but is time-inefficient)	PP oracle, 1/exp(n) precision [1]
QMA$_{\text{exp}}$ (= PSPACE)	**PSPACE oracle $\Omega(1)$ overlap, Theorem 1**	← (Theorem 4 applies but is time-inefficient)	PSPACE oracle, 1/exp(n) precision [1]
Arbitrary states	**Arbitrary oracle, 1/poly(n) precision, Theorem 3**	**Arbitrary oracle, 1/exp(n) precision, 2 queries, Theorem 4**	Arbitrary oracle, 1/exp(n) precision [1]

To start sketching the proof, it is fruitful to notice that a single oracle query $|x\rangle \overset{\mathcal{O}_f}{\mapsto} (-1)^{f(x)}|x\rangle$ for $x \in \{0,1\}^n$ potentially contains 2^n bits of information and a quantum state requires 2^n complex numbers to describe. Furthermore, the collection of 2^{2^n} states

$$|p_f\rangle \overset{\text{def}}{=} \mathcal{O}_f H^{\otimes n}|0^n\rangle = \sum_{x\in\{0,1\}^n} (-1)^{f(x)}|x\rangle \tag{7}$$

defined for any function $f : \{0,1\}^n \to \{0,1\}$ are a diverse set of states in the Hilbert space. These states, referred to as *phase states* henceforth, despite not forming an ϵ-net for $(\mathbb{C}^2)^{\otimes n}$, turn out to provide a good approximation for $(\mathbb{C}^2)^{\otimes n}$ when considering the Haar-random distribution[3]. It follows that if we wanted to synthesize the witness to a QMA-complete problem, such as a low-energy state $|\tau\rangle$ for a local Hamiltonian problem, it suffices to build phase state $|p_f\rangle$ with constant overlap with the low-energy subspace. Finding a state with constant overlap with the target state is sufficient because QMA is efficiently verifiable, and given a state with constant overlap with the low-energy subspace, it is possible to distill a low-energy state with constant probability (by performing an energy measurement). However, it is not necessarily the case that a low-energy state of QMA problem will have a good approximation by a phase state. To solve this issue, we prove that for any state $|\tau\rangle$, with high probability $C|\tau\rangle$ will have a good approximation by a phase state where C is a random

[3] Recall, the Haar-measure is the unique left- and right- invariant distribution over unitary matrices over $(\mathbb{C}^2)^{\otimes n}$ and the Haar-random distribution is the distribution over quantum states $U|0^n\rangle$ where U is sampled according to the Haar-measure.

Clifford unitary. Therefore, we can instead attempt to synthesize $C|\tau\rangle$ which is the result of Theorem 1. In particular, if we can synthesize a phase state $|p\rangle$ that has constant overlap with $C|\tau\rangle$, then $C^\dagger|p\rangle$ will have constant overlap with the target $|\tau\rangle$.

Furthermore, we show that, using a slight modification of the same algorithm, we can perform a somewhat weaker one-query search-to-decision reduction for $\mathsf{QMA_{exp}}$ (see Theorem 2.4 of the full version [8] for details). Recall $\mathsf{QMA_{exp}}$ is the class of non − deterministic quantum computations with only an inverse exponential gap between completeness and soundness and is known to equal PSPACE [7, 6]. Our algorithm prepares a witness state with constant overlap with a low-energy state with one query to a PSPACE oracle (note that here, we cannot efficiently amplify the overlap with an energy measurement due to the inverse-exponential energy gap). As a further observation, we also show that quantum query access to a classical oracle gives one-query search-to-decision reductions when the witness is classical: in particular, for QCMA and NP (see Theorem 2.7 of the full version [8] for details). The one-query algorithm preparing the witness first reduces QCMA to *unique* QCMA (UQCMA) using the Valiant-Vazirani reduction [4], and then uses the Bernstein-Vazirani algorithm to extract the unique polynomial length witness with a single query.

A no-go result for search-to-decision for QMA. The previous result shows that search-to-decision reductions for QMA are possible with a PP decision oracle. However, the optimal search-to-decision reduction for QMA is with a QMA decision oracle (rather than a stronger PP oracle). We provide evidence that this is unlikely to exist: we prove that there is a quantum oracle relative to which QMA search-to-decision is impossible. This stands in contrast to classes such as NP, MA, and QCMA, which all have efficient search to decision reductions, relative to any oracle.

More precisely, we show that there exists a *quantum* oracle $\mathcal{O}$ relative to which *all* efficient query algorithms fail to be a good search-to-decision reduction for $\mathsf{QMA}^{\mathcal{O}}$, the relativization of QMA. The oracle $\mathcal{O}$ is a reflection $\mathbb{I} - 2|\psi\rangle\langle\psi|$ about a Haar-random state $|\psi\rangle$; we rely on the concentration of measure phenomenon of the Haar measure to prove this oracle no-go result. We formalize this result in Section 3.

▶ **Theorem 2** (Oracle impossibility for QMA search-to-decision). *There exists a quantum oracle $\mathcal{O}$ relative to which* all $\mathsf{poly}(n)$*-time query algorithms fail to be a good search-to-decision reduction for* $\mathsf{QMA}^{\mathcal{O}}$*.*

A one-query state synthesis algorithm with inverse polynomial error. We also investigate the query complexity of synthesizing an arbitrary state, in the same spirit as Aaronson's adaptive state synthesis algorithm outlined in Section 1.1. In particular, we show that that every state $|\tau\rangle$ can be encoded into a classical oracle f_τ such that by making one query to $|\tau\rangle$, a quantum algorithm can prepare $|\tau\rangle$ with inverse polynomial error. The space complexity of the synthesis algorithm is polynomial in n, the number of qubits in the target state $|\tau\rangle$, but the time complexity is exponential. The starting point for the 1-query algorithm is the same observation used in the protocol for synthesizing QMA witnesses, which is that a random state has an expected constant overlap with some phase state. We can think of the oracle function f_τ as hard-coding the target $|\tau\rangle$, but parameterized by unitary U and standard basis state x. The oracle $f_\tau(U, x) = \mathrm{sgn}(\mathrm{Re}(\langle x|U\tau\rangle))$ can be used to create a phase state $|p_U\rangle$ which has constant overlap with $U|\tau\rangle$ with high probability for random U. The state $U^\dagger|p_U\rangle$ is already then a decent approximation for $|\tau\rangle$.

There are two remaining techniques to improve upon this basic synthesis protocol. First, we use a novel distillation procedure based on the swap test (explained below) to take a polynomial number of states generated in this manner, using unitaries $U_1, \ldots, , U_m$, to create a single aggregated output state with greater overlap with the target state. Note that since the target state $|\tau\rangle$ is arbitrary, we do not have a means of measuring the overlap of an output state with $|\tau\rangle$ to boost the overlap as we did when the target state is a QMA witness. Secondly, we address the fact that the algorithm described above suffers from needing *exponential space complexity*; this is because specifying a Haar-random unitary on n qubits requires $\exp(\Omega(n))$ space, and thus the oracle $f_\tau(U, x)$ needs to act on exponentially many input bits. We derandomize this construction, and show via the probabilistic method that there exists a *single* choice of unitaries $U_{\star,1}, \ldots, U_{\star,m}$ that works for *all* n-qubit states. This will reduce the space complexity of the algorithm to polynomial, although implementing the unitaries will still require exponential time.

▶ **Theorem 3** (One Query State Synthesis – Informal). *There is a* 1*-query algorithm that uses polynomial space and exponential time that synthesizes a state* ρ *such that* $\mathrm{Tr}\{\rho\,|\tau\rangle\!\langle\tau|\} \geq 1 - 1/q(n)$ *for some polynomial* q *and an arbitrary target state* $|\tau\rangle$*.*

The Swap Test Distillation Algorithm. This procedure takes in a polynomial number of states each of which has at least a constant overlap with the target state and outputs a state whose overlap with the target is at least $1 - 1/\text{poly}$. In some sense, the Swap Test Distillation algorithm provides a way to take the "mean" of a collection of quantum samples where each state can be decomposed into a "signal" component and a "noise" component such that (1) the signal is some constant fraction of the mass and (2) the noise is roughly random. This may be useful in other contexts in quantum algorithms.

For formally, the algorithm requires that the sequence of input states $|\psi_1\rangle, \ldots, |\psi_m\rangle$ satisfies two properties. The first is that there is a constant a such that $|\langle\psi_j|\tau\rangle|^2 \geq a$ for all j. (We also show that this condition can be relaxed so that the expected overlap of each input state with the target state is at least a, as long as the input states are independently generated.) The second condition is that for every pair of input states, their components orthogonal to $|\tau\rangle$ are close to orthogonal to each other:

$$|\langle\psi_j|\,(\mathbb{I} - |\tau\rangle\!\langle\tau|)\,|\psi_i\rangle|^2 \leq \delta, \tag{8}$$

for δ exponentially small in n. Intuitively, one can imagine that if the $|\psi_j\rangle$ are generated independently, then the error vectors (the components perpendicular to $|\tau\rangle$) would be random and uncorrelated. We prove that under these two conditions, if the number of states is a sufficiently large polynomial, then the overlap of the resulting aggregated state with $|\tau\rangle$ is at least $1 - 1/\text{poly}$. The algorithm is based on the observation that if the swap test is applied to a pair of states which each have overlap at least a with the target state, then conditioning on the swap test succeeding (measuring a 0 in the output bit), the state in each register has an overlap with the target state that is strictly larger than a. In each round of the algorithm, the surviving states are paired up and the swap test is applied to each pair. One state from every pair that succeeds the swap test advances to the next round.

A two-query state synthesis algorithm with inverse exponential error. While we do not know how to improve the error of the previous one-query algorithm beyond inverse polynomial, we show that there is a *two-query* state synthesis algorithm that achieves inverse exponential error.

▶ **Theorem 4** (Two Query State Synthesis – Informal). *There is a* 2*-query algorithm that uses polynomial space and exponential time that with high probability synthesizes a state* ρ *such that* $\mathrm{Tr}\{\rho\,|\tau\rangle\!\langle\tau|\} \geq 1 - 1/r(n)$ *for some function* $r = \exp(n)$ *and an arbitrary target state* $|\tau\rangle$*.*

Like with the one-query synthesis algorithm, we take advantage of the properties of Haar-random unitaries. Let $|\tau\rangle$ denote the target state to be synthesized. Whereas the basic building block of the one-query algorithm described is to synthesize the phase state corresponding to $U|\tau\rangle$ where U is a Haar-random unitary, the two-query algorithm attempts to directly synthesize the state $U|\tau\rangle$, and then apply the inverse unitary $U^\dagger$ to recover $|\tau\rangle$. Since U is Haar-random, the distribution of $U|\tau\rangle$ is that of a Haar-random state.

We then argue that with overwhelmingly high probability, a Haar-random state can be synthesized via two queries to a classical oracle. This relies on the observation that the *amplitude profile* of a Haar-random state concentrates extremely tightly around a fixed profile. By profile, we mean the list of absolute values of amplitudes of the state in sorted order. In other words, there exists a fixed, universal state $|\theta\rangle = \sum_x \beta_x |x\rangle$ such that, with very high probability, a Haar-random state $|\psi\rangle = \sum_x \alpha_x |x\rangle$ satisfies the following: there exists a permutation σ on the set of basis states $|x\rangle$ such that the distance

$$\left\| |\theta\rangle - \sum_x |\alpha_x| \, |\sigma(x)\rangle \right\| \tag{9}$$

is exponentially small. To prove this, we utilize bounds from the theory of optimal transport that control the convergence of the *Wasserstein distance* (also known as the *Earth Mover Distance*) between a log-concave distribution and the empirical distribution resulting from sampling from the distribution.

Given this, the two-query algorithm to synthesize $|\tau\rangle$ to exponential precision is clear: the algorithm first prepares the universal state $|\theta\rangle$. It then queries the classical oracle to determine how to permute the basis states $|x\rangle$ and what phase to apply to all the basis states. The algorithm applies the permutation and the phases in superposition. Finally, the algorithm queries the oracle again to uncompute the permutation/phase information.

Just as with the one-query algorithm, we also perform a derandomization step in order to make the query algorithm space-efficient (but not necessarily time-efficient). By expanding the dimension of the random unitary U, we show that there exists (via the probabilistic method) a *single* unitary $U_\star$ that maps *every* target state $|\tau\rangle$ to one whose amplitude profile is exponentially close to the universal one.

Open Questions. We conclude with some open questions which are elaborated in greater detail in Section 7. Can the 1- and 2-query algorithms for general state synthesis be improved to polynomial time by using random Cliffords instead of Haar-random unitaries? Is there a 1-query algorithm for state synthesis that also achieves inverse exponential error? What is the power of a QMA decision oracle? In particular, what states can be synthesized with queries to a QMA oracle in superposition? Is there a weaker oracle class than PP that can achieve search-to-decision for QMA witnesses?

Preliminaries. Preliminaries and definitions necessary are listed in Appendix A of the full version [8].

2 Search-to-decision for QMA problems

In the traditional search-to-decision paradigm, the goal is to create a witness $|\psi\rangle$ which could convince a verifier that indeed some string is in a particular QMA language. The creation of this witness should be carried out by a quantum machine running in polynomial time with access to a QMA oracle. There are multiple ways to relax this paradigm; here we consider using a PP oracle instead of a QMA oracle and show that there is a polynomial time quantum algorithm which makes only one PP oracle call[4] and generates a solution to a QMA-complete problem.

Our algorithm proceeds from two observations:

1. Any phase state $|p_f\rangle = 2^{-n/2} \sum_{x \in \{0,1\}^n} (-1)^{f(x)} |x\rangle$ for which the function f is computable in PP may be prepared by a single quantum query to a PP oracle.
2. *Any* state $|\tau\rangle$, after applying a random unitary U, looks like a phase state: in particular, with high probability over the choice of U, the state $U|\tau\rangle$ has constant overlap with some phase state.

2.1 One-query search-to-decision for QMA

We now consider the QMA search problem with respect to phase oracles. In general, the statement of the QMA search problem is to construct, given a verification circuit for some QMA language, and an input χ in the language, a state $|\psi_\chi\rangle$ that is accepted by the verification circuit with high probability. Rather than working with general verifiers, we will restrict to verifiers that measure the energy of a local Hamiltonian on the witness state up to inverse-polynomial precision. This restriction is almost without loss of generality, for two reasons. First, the local Hamiltonian problem with this precision is QMA-complete, so any QMA language has a verifier of this form. And secondly, the reduction to local Hamiltonian can be performed so that every low-energy state is very close to an accepting witness $|\psi\rangle$ for the original verifier. More precisely, given a general QMA verification circuit V, we can apply the padding trick of Nirkhe, Vazirani and Yuen [13] to generate a local Hamiltonian instance H such that any ground-state ρ of H, $\|\rho - \sigma \otimes \Phi\| \leq \delta$ where σ is an accepting witness of V and Φ is a fixed state independent of the instance. The size of the Hamiltonian instance H scales as $\mathsf{poly}(1/\delta)$ and therefore the approximation can be chosen as any inverse polynomial function of the system size.

Assume the input to the problem is an instance $\chi = (H, a, b)$ of the Local Hamiltonian problem with Hamiltonian H on n qubits and two thresholds $a < b$ such that $b-a = 1/\mathsf{poly}(n)$. Moreover, we assume that χ is a YES instance, so the minimum eigenvalue of H is at most a: $\lambda_{\min}(H) \leq a$. The goal is to construct a state $|\phi\rangle$ such that

$$\langle\phi|H|\phi\rangle \leq \frac{a+b}{2}. \tag{10}$$

While it would be ideal to construct a state for which the energy is at most a (since one exists), this may drastically increase the computational complexity of the function $f : \{0,1\}^n \to \{0,1\}$ defining the oracle. Instead, due to the promise gap in the problem, it suffices to construct a *witness* state which proves that the Hamiltonian has a state with energy at most $< b$. A state $|\phi\rangle$ satisfying eq. (10) is a proof that χ is a yes instance. We now prove the formal version of Theorem 1.

▶ **Theorem 5** (QMA-search to PP-decision reduction). *There exists a probabilistic polynomial time quantum algorithm with access to a single* PP *phase oracle query that, given as input an instance (H, a, b) of the local Hamiltonian problem on n qubits, either aborts or outputs a witness $|\phi\rangle$ with $\langle\phi|H|\phi\rangle \leq (a+b)/2$ for $b - a = 1/\mathsf{poly}(n)$. The algorithm will succeed in outputting a witness (i.e. not abort) with probability*[5] $\geq 1/1024$.

[4] The improvement over the algorithm of Aaronson [1] is in the number of oracle queries.

[5] We will later argue that this probability can be amplified through a variation of parallel repetition to improve to any function $1 - \exp(-n)$.

See Theorem 2.1 in the full version [8] for proof.

We remark that we see that the algorithm achieves something stronger: if the algorithm does not abort, then the output state is almost entirely supported on states of energy less than $a + (b - a)/4 + \epsilon$, where $\epsilon = 1/\mathsf{poly}(n)$ is a precision parameter much smaller than $b - a$. This is performed by using phase estimation to "check" the outcome of the query algorithm by measuring the energy.

At this point, it is useful to remember that in general, the notion of a QMA *witness* is defined only with reference to a specific verifier. The guarantee we achieve ensures that the "standard" verifier, which measures the energy of the local Hamiltonian H, has a high chance of accepting the given state. If one is willing to use a more sophisticated verifier, e.g. a verifier that performs the Marriott-Watrous amplification procedure [12], a witness of considerably worse quality could still be acceptable. Our theorem also sidesteps the issue of unique witnesses: we only guarantee that the energy of our state is low, not that it is the *unique* such state.

One can easily boost probability that our algorithm does not abort to $1 - \mathsf{exp}(-n)$ by repeating the construction in parallel with independent randomness and selecting any witness which did not cause the algorithm to abort. Furthermore, from the design of the algorithm, one can merge the oracle queries into a single larger PP query[6], so the query complexity does not increase.

Additional remarks. In Section 2.1 of the full version [8], we also provide remarks on why it is difficult to improve the oracle complexity as well as how to extend this argument for the class $\mathsf{QMA}_{\mathsf{exp}} = \mathsf{PSPACE}$ (see Section 2.2 of the full version [8]). Furthermore, Section 2.3 of the full version [8] includes a completely different procedure, which generates one oracle query search-to-decision for QCMA.

3 Impossibility of search-to-decision for QMA in oracle model

In this section we show that efficient search-to-decision reductions for QMA do not exist in general in the oracle setting, perhaps providing some evidence that QMA does not have efficient search-to-decision reductions "in the real world." More precisely, we show that there exists a *quantum* oracle $\mathcal{O}$ relative to which *all* polynomial-time quantum query algorithms fail to be a good search-to-decision reduction for $\mathsf{QMA}^{\mathcal{O}}$, the relativization of QMA. Equivalently, $\mathsf{QMA}^{\mathcal{O}}$-search problems are not reducible to $\mathsf{QMA}^{\mathcal{O}}$-decision problems. We contrast this impossibility result with the fact that complexity classes like NP, MA and QCMA all have efficient search-to-decision reductions, relative to any oracle (i.e. the reductions relativize)! For example, it is not hard to verify that the search-to-decision procedure for QCMA described in Section 2.3 of the full version [8] relativizes. Thus, Theorem 6 illustrates that, at least in the relativized setting, changing the proof model from classical to quantum nullifies the possibility of search-to-decision reductions.

We first define $\mathsf{QMA}^{\mathcal{O}}$ by way of a complete problem. Fix a small constant $\delta < \frac{1}{100}$. Define an *$\mathcal{O}$-verifier* circuit C to be a quantum circuit that can make queries to $\mathcal{O}$ (which can be viewed as applying a unitary gate for $\mathcal{O}$), and also takes as input a quantum proof state $|\phi\rangle$, as well as some ancilla qubits set to $|0\rangle$. Define the promise problem $\mathcal{O}$-QCircuitSAT

[6] One way to see that the merged oracle is also definable in PP is through the connection PP = PostBQP. The merged oracle can be seen as the logical exclusive-or (XOR) of multiple PP functions, and it is easy to create a new PostBQP function equal to the logical XOR of multiple PostBQP functions.

whose YES instances consist of $\mathcal{O}$-verifier circuits C for which there is a quantum proof state $|\phi\rangle$ such that $C(|\phi\rangle)$ accepts with probability at least $1-\delta$, and the NO instances are those circuits such that on all quantum witness states, C accepts with probability at most δ. Without access to $\mathcal{O}$, this is simply the canonical QMA-complete problem QCircuitSAT. The class $\mathsf{QMA}^{\mathcal{O}}$ is then the set of all promise decision problems that are polynomial-time reducible to $\mathcal{O}$-QCircuitSAT.

Now we formalize the notion of search-to-decision reductions for $\mathsf{QMA}^{\mathcal{O}}$. Consider quantum circuits that can make queries in superposition to both the quantum oracle $\mathcal{O}$ and a *classical* oracle $A^{\mathcal{O}}$ that decides the promise problem $\mathcal{O}$-QCircuitSAT as well as the controlled-versions of these oracles. Alternatively, we can consider a standard quantum circuit with special oracle “gates” implementing $\mathcal{O}$ and $A^{\mathcal{O}}$ unitary transformations. Specifically, the oracle $A^{\mathcal{O}}$ implements the unitary transformation

$$|C\rangle\,|b\rangle \mapsto |C\rangle\,|b \oplus A^{\mathcal{O}}(C)\rangle \tag{11}$$

where C is supposed to be a description of an $\mathcal{O}$-oracle circuit, $b \in \{0,1\}$, $A^{\mathcal{O}}(C) \in \{0,1\}$ with $A^{\mathcal{O}}(C) = 1$ if C is a YES instance of $\mathcal{O}$-QCircuitSAT, $A^{\mathcal{O}}(C) = 0$ if C is a NO instance, and otherwise $A^{\mathcal{O}}(C)$ is defined arbitrarily. This is sufficiently general as we previously remarked that all $\mathsf{QMA}^{\mathcal{O}}$ problems can be expressed as $\mathcal{O}$-oracle circuits C. We then say that such a quantum circuit S is an *ϵ-good search-to-decision reduction* for the problem $\mathcal{O}$-QCircuitSAT – or, alternatively, *ϵ-solves the search version* of $\mathcal{O}$-QCircuitSAT – if when given a YES instance C of $\mathcal{O}$-QCircuitSAT, it outputs a state that is accepted by C with probability at least $1-\delta-\epsilon$.

We now state the main result of this section (the technical version of Theorem 2).

▶ **Theorem 6.** *There exists a constant $\epsilon > 0$ and a quantum oracle $\mathcal{O}$ relative to which there is no $\mathsf{poly}(n)$-sized ϵ-good search-to-decision reduction for $\mathcal{O}$-QCircuitSAT.*[7]

See Theorem 3.1 in the full version [8] for proof.

4 1-query state synthesis algorithm with polynomially small error

We describe here a 1-query, polynomial-space algorithm that achieves polynomially small error. The state synthesis algorithm will not be efficient. We will start with a first attempt, which has exponential space complexity and then fix it so that it has polynomial space complexity. The algorithm makes use of the Swap Test Distillation algorithm described in 5 that takes as input a polynomial number of states, each with at least constant overlap with the target state, and uses successive applications of the Swap Test to produce a final state whose overlap with the target state is at least $1 - 1/\mathsf{poly}(n)$.

4.1 A space-inefficient algorithm

Let $d = 2^n$, $n' = n^2$, and $d' = 2^{n'}$. The m applications of the 1-query algorithm along with the Swap Test Distillation algorithm will be applied to n'-qubit registers with target state $|\tau'\rangle = |\tau\rangle \otimes |0\rangle^{\otimes(n'-n)}$. The expansion of the space is important for derandomizing the

[7] Technically, we should be considering an infinite family of oracles $\mathcal{O}$ and $A^{\mathcal{O}}$ where each oracle is parameterized by some input length n. However for simplicity we shall just deal with one input length; we will forgo the trouble of spelling out the details of stating our results for asymptotic n. To that end, let $\mathcal{O}$ be a unitary that acts on n qubits, and we only consider $\mathcal{O}$-verifier circuits who accept n-qubit quantum proof states; the verifier circuits themselves will be of size $\mathsf{poly}(n)$.

algorithm later on. In particular, we will show that there is a fixed sequence of unitaries that works for all $|\tau'\rangle$ of the form $|\tau\rangle \otimes |0\rangle^{\otimes(n'-n)}$. This will allow us to hard-code the unitaries into the oracle function. The resulting algorithm will still require exponential time to implement the unitaries, but the derandomized algorithm will require only polynomial space.

We will define a function $f_{\tau'} : \mathrm{U}(d') \times \{0,1\}^{n'} \to \{0,1\}$, where $\mathrm{U}(d')$ is the space of all unitaries on a d'-dimensional Hilbert space, and

$$f_{\tau'}(U,x) \overset{\mathsf{def}}{=} \operatorname{sgn}\left(\operatorname{Re}\left(\langle x| U |\tau'\rangle\right)\right) \tag{12}$$

The corresponding phase state is

$$|p_U\rangle = \sum_{x\in\{0,1\}^{n'}} (-1)^{f_{\tau'}(U,x)} |x\rangle \tag{13}$$

```
OneQueryStateSynthesis (space inefficient version)
(1) for $j = 1, \ldots, m$ in parallel:
(2)         Sample Haar-random $n'$-qubit unitary $U_j$.
(3)         In the $j$th $n$'-qubit register, prepare the equal superposition $\sum_{x\in\{0,1\}^{n'}} |x\rangle$.
(3)         Controlled on basis state $|x\rangle$, query the oracle on input $(U_j, x)$ to apply
                $f_{\tau'}(U_j, x)$ and produce phase state $|p_{U_j}\rangle$ on $n'$ qubits.
(4)         Apply $U_j^\dagger$ to the phase state.
(5) Apply the SwapTestDistillation Algorithm (Figure 2) to the $m$ resulting
                states $|\psi_1\rangle, \ldots, |\psi_m\rangle$.
(6) Output the first $n$ qubits of any surviving register.
```

Figure 1 Pseudo-code for the OneQueryStateSynthesis query algorithm that uses exponential space complexity.

The algorithm will output m expanded registers on n' qubits. We will apply the Swap Test Distillation algorithm to m states on n' qubits generated by m parallel (and independent) applications of the 1-query algorithm and analyze the probability that the resulting state has at least $1 - 1/\mathsf{poly}(n)$ overlap with $|\tau'\rangle$. The mixed state ρ in the first n-qubits will also have $\mathrm{Tr}\{\rho\, |\tau\rangle\!\langle\tau|\} \geq 1 - 1/\mathsf{poly}(n)$.

The following lemma establishes that with high probability after step (4) of the algorithm, the conditions for the Swap Test Distillation Algorithm are met.

▶ **Lemma 7** (Probability Conditions Satisfied for Swap Test Distillation). *Let $|\psi_1\rangle \otimes \cdots \otimes |\psi_m\rangle$ be the states in the m registers after Step (4). There is a constant C such that*

1. $\mathbf{Pr}_{U_1,\cdots,U_m}\left[\min_j\{|\langle\psi_j|\tau'\rangle|^2\} \leq 1/8\right] \leq m \cdot \exp(-Cd')$
2. $\mathbf{Pr}_{U_1,\cdots,U_m}\left[\max_{i\neq j}\{|\langle\psi_i|(I - |\tau'\rangle\!\langle\tau'|)|\psi_j\rangle|^2\} \geq (d')^{-1/4}\right] \leq m^2 \cdot \exp(-C(d')^{1/2})$

See Lemma 4.1 in the full version [8] for proof.

4.2 A space-efficient algorithm

The algorithm described above suffers from needing *exponential space complexity*; this is because specifying a Haar-random unitary on n' qubits requires $\exp(\Omega(n'))$ space, and thus the oracle $f(U,x)$ needs to act on exponentially many input bits. We derandomize this construction, and show via the probabilistic method that there exists a *single* choice of unitaries $U_{\star,1},\ldots,U_{\star,m}$ that works for *all* n-qubit states – this is why we expanded the space to dimension d'.

Let $|v_1\rangle,\ldots,|v_D\rangle$ denote an ϵ-net for the space of n-qubit quantum states where $\epsilon = d^{-1}$. Then there at most $D \leq \epsilon^{-d} = d^d$ states in this enumeration. Fix an index $1 \leq i \leq D$. Imagine running the 1-query protocol in Figure 1 in parallel m times with target state $|v_i\rangle \otimes |0\rangle$. The probability that the protocol fails to satisfy the conditions for the Swap Test Distillation algorithm from Lemma 7 is at most $2m^2\mathsf{exp}(-\Omega((d')^{3/4}))$ over the choice of $U_1,\ldots,U_m$. By a union bound, the probability that a random choice of $U_1,\ldots,U_m$ fails to satisfy the conditions from Lemma 7 for *a single one* of the $|v_1\rangle,\ldots,|v_D\rangle$ is at most

$$d^d \cdot 2m^2\mathsf{exp}(-\Omega((d')^{1/2})) \leq 2^{n2^n} \cdot 2m^2\mathsf{exp}(-\Omega(2^{n^2/2})). \tag{14}$$

Since m is polynomial in n, for sufficiently large n, this probability is less than 1. Thus there exists a choice of unitaries $U_{\star,1},\ldots,U_{\star,m}$ that results in a set of m states that satisfy the conditions for the Swap Test Distillation algorithm for *all* the $|v_1\rangle,\ldots,|v_D\rangle$. Hardcode these unitaries into the algorithm and oracles: $f_{\tau,i}(x) = f_\tau(U_{\star,i},x)$. Now the oracles only take n' bits as input each, and the resulting query algorithm now only requires $\mathsf{poly}(n)$ space. Note that the implementation of the unitaries $U_{\star,1},\ldots,U_{\star,m}$ will not be time-efficient in general, but they are still fixed unitary operators that act on n' qubits.

Thus for an arbitrary target state $|\tau\rangle$, use the oracles $f_{v_i}(U_{\star,1},x),\ldots,f_{v_i}(U_{\star,m},x)$ corresponding to the nearest state $|v_i\rangle$ in the ϵ-net, which is within d^{-1} of $|\tau\rangle$. Therefore, the one-query algorithm using unitaries $U_{\star,1},\ldots,U_{\star,m}$, followed by the Swap Distillation Algorithm will incur an additional $O(d^{-1})$ error.

▶ **Theorem 8** (One Query State Synthesis Performance). *For every polynomial q, there is a polynomial p and constant C' such that if the* OneQueryStateSynthesis *is run with $m \geq p(n)$ registers, then with probability at least $1 - \mathsf{exp}(-C'n)$, the algorithm produces a state ρ such that $\mathrm{Tr}\{\rho\,|\tau\rangle\langle\tau|\} \geq 1 - 1/q(n)$. The oracle queried by the algorithm will depend on the closest state to $|\tau\rangle$ in the ϵ-net.*

See Theorem 4.2 in the full version [8] for proof.

5 Swap test distillation procedure

If a synthesis protocol is able to produce a state with at least constant overlap with the target state and the target state is a witness for a QMA verifier, then phase estimation can be used to boost the overlap and the probability of success. If the target state is an arbitrary state, we may not have the means to directly measure whether the output state is close to the target. In this section we describe a procedure that can take the output of m parallel applications of a state synthesis protocol, each of which has a constant overlap with the target state and apply a procedure to increase the overlap. The algorithm begins with m states, $|\psi_1\rangle,\ldots|\psi_m\rangle$, each of which is stored in an n-qubit register. We show that if the number of states m is a sufficiently large polynomial in n, then the overlap of the final output state will be at least $1 - 1/\mathsf{poly}(n)$, with high probability. The distillation process is based on the Swap Test and works subject to two conditions on the collection of input states:

1. For all j, $|\langle\psi_j|\tau\rangle|^2 \geq a$, for some constant a.
2. For all $i \neq j$ $|\langle\phi_j|\phi_i\rangle|^2 \leq \delta$, where δ is exponentially small in n and for all j

$$|\phi_j\rangle \overset{\mathsf{def}}{=} \frac{|\psi_j\rangle - \langle\psi_j|\tau\rangle|\tau\rangle}{\||\psi_j\rangle - \langle\psi_j|\tau\rangle|\tau\rangle\|}. \tag{15}$$

The second condition is satisfied if the portion of each state $|\psi_j\rangle$ that is perpendicular to the target state $|\tau\rangle$ is essentially random. If the $|\psi_j\rangle$'s are generated according to some independent randomness, one might expect that the overlap between these perpendicular components to be (exponentially) small. In this section, we analyze the behavior of the Swap Test distillation procedure subject to these two properties. At the end of the section, we will show that the first condition can be relaxed to a lower bound on the expectation of the overlap as long as the m states are generated according to some independent randomness. In Section 4, we showed how the algorithm can be used in conjunction with a 1-query protocol to produce a state that has $1 - 1/\mathsf{poly}(n)$ overlap with the target state.

The Algorithm

Each round of the algorithm begins with some set of surviving registers. The surviving registers are paired up and the swap test is applied to each pair. An auxiliary qubit is used in each application of the swap test which is measured at the end of the swap test. If the outcome is 0 (a *successful* outcome), then one of the two registers is selected to survive to the next iteration. If the outcome is 1 (an *unsuccessful* outcome), neither register survives. Figure 2 shows the pseudocode for the procedure. Figure 3 shows an example of the procedure for one iteration applied to eight input states. Note that the state in a surviving register may be entangled with the other registers. If ρ is the reduced density matrix of the state in one of the surviving registers obtained by tracing out the other registers, we will refer to $\mathrm{Tr}\{\rho\,|\tau\rangle\langle\tau|\}$ as the *overlap* of ρ with $|\tau\rangle$. We will show that for m sufficiently large, with high probability the overlap of a surviving register with $|\tau\rangle$ is at least $1 - 1/\mathsf{poly}(n)$.

Consider one round of the algorithm applied to a particular pair of registers. We will prove that if the swap test succeeds, then the surviving register has an overlap with $|\tau\rangle$ that is at least the average of the overlap of the states in the two registers before the round. Moreover, if each of the two registers at the beginning of a round have overlap at least γ, then the overlap of a surviving register is strictly larger than γ and with enough successful rounds will tend towards 1.

The analysis of the swap test distillation is provided in Section 5.1-2 of the full version [8].

6 2-query state synthesis algorithm with exponentially small error

We now describe a 2-query state synthesis algorithm that achieves *exponentially small* error. Like with the 1-query algorithm from Section 4, it will be space-efficient, but not time-efficient. And also like in Section 4, we first describe a version of the algorithm with exponential space complexity, and then describe how to reduce the space complexity to polynomial.

6.1 A space-inefficient algorithm

Let $d = 2^n$, $n' = n^2$ and $d' = 2^{n'}$. Let $\{\sigma_{U,V}\}_{U,V}$ denote a set of permutations on $\{0,1\}^{n'}$, indexed by unitaries U, V on n' qubits. For all unitaries U, V and n'-bit strings x, let $\phi(U,V,x)$ denote a number in $[0, 2\pi)$, representable using $(n')^2$ bits. We will specify $\{\sigma_{U,V}\}$ and ϕ later. Define the oracles

$$f(U,V,x) \overset{\mathsf{def}}{=} (\phi(U,V,x), \sigma_{U,V}(x)) \quad \text{and} \quad g(U,V,y) = (\sigma^{-1}_{U,V}(y), \phi(U,V,\sigma^{-1}_{U,V}(y))) \ . \tag{16}$$

These oracles have the property that if $f(U,V,x) = (\phi, y)$, then $g(U,V,y) = (x, \phi)$.

An analysis of the correctness of the algorithm is provided in Section 6.1 of the full version [8].

```
SwapTestDistillation
Input: $m$ states $|\psi_1\rangle, \dots |\psi_m\rangle$ stored in $n$-qubit registers numbered 1 through $m$
    Initialize $(R_1, \dots, R_m) \leftarrow (1, \dots, m)$
    $\ell = \lfloor \log_6(m/n) \rfloor$
    for $k = 1, \dots, \ell$:
        count = 0
        for $j = 1, \dots, \lfloor m/2 \rfloor$
            if SwapTest($R_{2j-1}, R_{2j}$) returns 0
                count = count +1
                $R_{count} = R_{2j-1}$
        end
        $m$ = count
end
```

```
SwapTest($R, R'$)
Start with auxiliary qubit $b$ initialized to $|0\rangle$
    Apply:
        $H_b \otimes I_{R,R'}$
        Controlled SWAP operation on Registers $R$ and $R'$, controlled by qubit $b$
        $H_b \otimes I_{R,R'}$
    Measure qubit $b$ and return the result
end
```

Figure 2 Pseudo-code for SwapTestDistillation algorithm.

6.2 A space-efficient algorithm

The algorithm described above suffers from needing *exponential space complexity*; this is because specifying a Haar-random unitary on n' qubits requires $\mathsf{exp}(\Omega(n'))$ space, and thus the oracles f, g need to act on exponentially many input bits. We derandomize this construction, and show via the probabilistic method that there exists a *single* choice of unitary $U_\star, V_\star$ that works for *all* n-qubit states – this is why we expanded the space to dimension d'.

Let $|\psi_1\rangle, \dots, |\psi_D\rangle$ denote an ϵ-net for the space of n-qubit quantum states. Set $\epsilon = d^{-1}$. Then there at most $D \le \epsilon^{-d} = d^d$ states in this enumeration. Fix an index $1 \le i \le D$. Imagine running the aforementioned protocol on state $|\psi_i\rangle$. As discussed, the probability that the protocol fails to synthesize a $(d')^{-1/4}$-approximation to $|\psi_i\rangle$ is at most $\mathsf{exp}(-\Omega((d')^{1/4}))$ over the choice of U, V. By a union bound, the probability that a random choice of U, V fails to synthesize a $(d')^{-1/4}$-approximation to *a single one* of the $|\psi_1\rangle, \dots, |\psi_D\rangle$ is at most

$$d^d \cdot \mathsf{exp}(-\Omega((d')^{1/4})) \le 2^{n2^n} \cdot \mathsf{exp}(-\Omega(2^{n^2/4})) \tag{17}$$

which, for sufficiently large n, is less than 1. Thus there exists a choice of unitaries $U_\star, V_\star$ that enables successful synthesis of *all* the $|\psi_1\rangle, \dots, |\psi_D\rangle$. Hardcode these unitaries into the algorithm and oracles in Figure 4; i.e., the oracles f and g only take n' bits as input. The resulting query algorithm now only requires $\mathsf{poly}(n)$ space. Note that the implementation of the unitaries $U_\star, V_\star$ will not be time-efficient in general, but they are still fixed n'-qubit unitary operators that are independent of the state being synthesized.

Thus for an arbitrary state $|\psi\rangle$, by letting the oracles A, B correspond to the nearest state $|\psi_i\rangle$ in the ϵ-net that is within d^{-1} of $|\psi\rangle$, the two-query algorithm synthesizes $|\psi\rangle$ with $O(d^{-1})$ error.

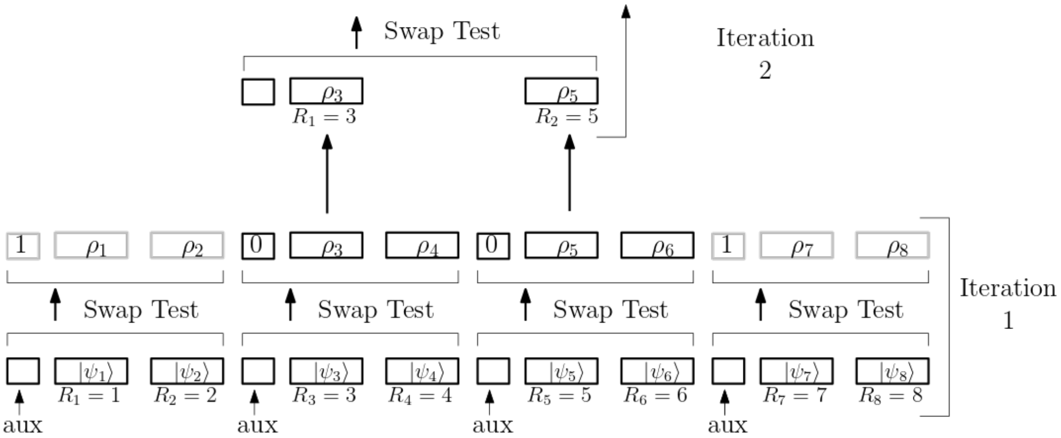

Figure 3 The Swap Test Distillation algorithm applied to eight input registers. The value measured in the auxiliary qubit indicates whether an application of the Swap Test is successful. In the first iteration, the swap tests applied to pairs $|\psi_3\rangle, |\psi_4\rangle$ and $|\psi_5\rangle, |\psi_6\rangle$ are successful. The resulting states in registers 3 and 5 advance to the next round. In each iteration, the sequence $(R_1, R_2, \ldots)$ indicates the indices of the surviving registers from left to right.

```
TwoQueryStateSynthesis (space inefficient version)
(1) Sample Haar-random $n'$-qubit unitaries $U, V$.
(2) Prepare the state $|\theta\rangle = U|0\rangle^{\otimes n'}$ in an $n'$-qubit register A.
(3) Controlled on basis state $|x\rangle$ in register A, call the oracle $f$ on input $(U, V, x)$
      to obtain $\phi \in [0, 2\pi)$ in register B and $y \in \{0,1\}^{n'}$ in register C.
(4) Controlled on basis state $|\phi\rangle$ in register B, apply the phase $e^{i\phi}$.
(5) Controlled on basis state $|y\rangle$ in register C, call the oracle $g$ on input $(U, V, y)$ to
      uncompute $|x\rangle \otimes |\phi\rangle$ in registers A and B.
(6) Apply the inverse unitary $V^\dagger$ on register C.
(7) Output the first $n$ qubits of register C.
```

Figure 4 Pseudo-code for the TwoQueryStateSynthesis query algorithm that uses exponential space complexity.

▶ **Theorem 9** (Two Query State Synthesis Performance). *For all n-qubit states $|\tau\rangle$, the algorithm* TwoQueryStateSynthesis *uses* $\mathsf{poly}(n)$ *space, makes two queries to a classical oracle depending on $|\tau\rangle$, and outputs a mixed state that is* $\exp(-\Omega(n))$*-close in trace distance to $|\tau\rangle\!\langle\tau|$.*

7 Open Questions

We exhibited state synthesis algorithms for QMA witnesses and arbitrary states that only require a *single* query to a classical oracle, that generate the target state up to inverse polynomial error. We also presented a *two*-query state synthesis algorithm that generates the target state up to inverse *exponential* error. As mentioned, this resolves Open Question 3.3.6 of Aaronson [1]. However, there are several remaining open questions regarding these algorithms.

1. The one- and two-query algorithms for arbitrary states use polynomial space, but they aren't time efficient (because their existence is argued by sampling a Haar-random unitary and applying the probabilistic method). Can this probabilistic construction be derandomized (and thus be made time efficient) by using (approximate) unitary designs?
2. Is there a one-query algorithm for state synthesis that also achieves inverse exponential error?

7.1 The power of quantum queries to QMA oracles

Our impossibility result in Section 3 combined with our reduction of QMA-search to PP-decision problems leaves an interesting gap as to what exactly is the power of QMA oracle. More specifically, are there interesting computational tasks solvable only with quantum access to a QMA oracle? One question is to understand the collection of problems which have search-to-decision reductions where the oracle is a QMA oracle. Is this class strictly larger than QCMA, a class with known search-to-decision reductions (see Theorem 2.7 of the full version [8])?

7.2 The Unitary Synthesis Problem

In Aaronson's lecture notes [1] and his published list of open questions in quantum query complexity [2], he identifies the unitary synthesis problem as one of the major unresolved questions.

▶ **Conjecture 10** ([2, Problem 6]). *For every n-qubit unitary transformation U, does there exists an oracle $A : \{0,1\}^* \to \{0,1\}$ such that a BQP^A machine can implement U?*

While, we do not know how to synthesize the unitary U, we do know how to synthesize the Choi - Jamiolkowski state, [5, 9]

$$|g_U\rangle_{LR} \overset{\text{def}}{=} \sqrt{\frac{1}{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle_L \, U \, |x\rangle_R \,, \tag{18}$$

which can also be seen as applying the unitary $\mathbb{I}_L \otimes U_R$ to the maximally entangled state. This comes from the previously constructed state synthesis algorithms or the state synthesis algorithm of Aaronson [1]. While the Choi - Jamiolkowski state contains all the information about U, it is unclear how to use $|g_U\rangle$ to apply the unitary U. One idea is to use the gate-by-teleportation technique from measurement-based quantum computation to apply U. In this procedure, one measures an n-qubit input state $|\psi\rangle$ in register A and the half of $|g_U\rangle$ in register L in the generalized Bell basis, i.e. the POVM with elements $|g_{X^aZ^b}\rangle\langle g_{X^aZ^b}|_{AL}$ for $a, b \in \{0,1\}^n$. It is known that each outcome (a, b) is equally likely to occur and the resulting state on the R register is $UX^aZ^b\,|\psi\rangle$. Unfortunately, the Pauli twirl, X^aZ^b, has been applied inside of the unitary U.

However, note that whenever the measurement outcome $a = b = 0^n$ occurs, the resulting state is $U\,|\psi\rangle$ as desired. Therefore, there is a *post-selection* algorithm which generates the output $U\,|\psi\rangle$ by post-selecting on the outcome $a = b = 0^n$. The issue, of course, is that post-selection is a non-unitary operation. However, we note that while post-selection is non-unitary, the classes PostBQP and PostQMA have definitions as classical complexity theory classes PP and PSPACE, respectively. We previously outlined search-to-decision reductions for both of these classes through their equivalences with PGQMA and $\mathsf{QMA}_{\mathsf{exp}}$, respectively. While not obvious to us at the moment, we suspect that there may be an insight connecting these ideas together to generate a solution to the unitary state synthesis problem.

7.3 Improving the construction of witnesses for $\mathsf{QMA}_{\mathsf{exp}}$

We leave it as an open question as to whether the Swap Test Distillation algorithm can be used to improve the overlap with a $\mathsf{QMA}_{\mathsf{exp}}$ witness produced by the protocol described in Section 2.2 of the full version [8]. The challenge is establishing that the conditions for the distillation algorithm are met when t-designs (such as Clifford unitaries) are used to randomize the target state instead of Haar-random unitaries. We know that Clifford unitaries will produce a state whose expected overlap with the target state is at least a constant. Theorem 5.8 of the full version [8] shows that the Swap Test Distillation algorithm still works under this relaxed condition (instead of requiring that every input state have constant overlap with probability 1). The problem lies in the second condition: showing that with high probability, for two independently generated output states, their components orthogonal to the target state are close to orthogonal to each other. The proof in Lemma 7 showing that this holds for the 1-query protocol that uses Haar-random unitaries relies on the following fact: for any two orthogonal states $|\psi_1\rangle$ and $|\psi_2\rangle$, even when conditioning on the event that $U|\psi_1\rangle = |\phi\rangle$ for some specific $|\phi\rangle$, the state $U|\psi_2\rangle$ is still distributed in a manner that looks close to random. We leave it as an open question whether a similar fact can be shown when U is a t-design or whether there is a different way to establish the second requirement for the Swap Test Distillation algorithm. A proof that t-designs satisfy the second requirement for the distillation algorithm would also result in an improvement over the 1-query protocol for synthesizing arbitrary states shown in Section 4, by reducing the time complexity of the protocol from exponential to polynomial time.

References

1 Scott Aaronson. The complexity of quantum states and transformations: from quantum money to black holes. *arXiv preprint*, 2016. arXiv:1607.05256.

2 Scott Aaronson. Open problems related to quantum query complexity, 2021. arXiv:2109.06917.

3 Scott Aaronson and Greg Kuperberg. Quantum versus classical proofs and advice. *Theory OF Computing*, 3:129–157, 2007.

4 Dorit Aharonov, Michael Ben-Or, Fernando G. S. L. Brandao, and Or Sattath. The pursuit of uniqueness: Extending Valiant-Vazirani theorem to the probabilistic and quantum settings, 2008. arXiv:0810.4840.

5 Man-Duen Choi. Completely positive linear maps on complex matrices. *Linear Algebra and its Applications*, 10(3):285–290, 1975. doi:10.1016/0024-3795(75)90075-0.

6 Abhinav Deshpande, Alexey V. Gorshkov, and Bill Fefferman. The importance of the spectral gap in estimating ground-state energies, 2020. arXiv:2007.11582.

7 Bill Fefferman and Cedric Lin. Quantum Merlin Arthur with Exponentially Small Gap, 2016. arXiv:1601.01975.

8 Sandy Irani, Anand Natarajan, Chinmay Nirkhe, Sujit Rao, and Henry Yuen. Quantum search-to-decision reductions and the state synthesis problem, 2021. arXiv:2111.02999.

9 A. Jamiołkowski. Linear transformations which preserve trace and positive semidefiniteness of operators. *Reports on Mathematical Physics*, 3(4):275–278, 1972. doi:10.1016/0034-4877(72)90011-0.

10 Alexei Yu Kitaev, Alexander Shen, Mikhail N Vyalyi, and Mikhail N Vyalyi. *Classical and quantum computation*. Number 47 in Graduate Studies in Mathematics. American Mathematical Soc., 2002.

11 William Kretschmer. Quantum pseudorandomness and classical complexity. *arXiv preprint*, 2021. arXiv:2103.09320.

12 Chris Marriott and J. Watrous. Quantum Arthur–Merlin games. *computational complexity*, 14:122–152, 2004.

13 Chinmay Nirkhe, Umesh Vazirani, and Henry Yuen. Approximate Low-Weight Check Codes and Circuit Lower Bounds for Noisy Ground States. In *45th International Colloquium on Automata, Languages, and Programming (ICALP 2018)*, Leibniz International Proceedings in Informatics (LIPIcs), pages 91:1–91:11, 2018.

14 Gregory Rosenthal and Henry Yuen. Interactive proofs for synthesizing quantum states and unitaries. In *13th Innovations in Theoretical Computer Science Conference (ITCS 2022)*. Schloss Dagstuhl-Leibniz-Zentrum für Informatik, 2022.