The power of time reversal in Hamiltonian property testing

Richard R. Allen* Matthias C. Caro† Yanlin Chen‡ Tom Gur§ Angus Lowe¶

Abstract

Quantum algorithms enable Heisenberg-limited scaling across many tasks in sensing and learning, achieving precision ε using $O(1/\varepsilon)$ total evolution time. However, in Hamiltonian property testing, the best known algorithms have $O(1/\varepsilon^2)$ total evolution time, unless it is possible to *reverse* the flow of time under the Hamiltonian. In this work, we prove that time reversal is necessary to close this gap. We establish evolution time lower bounds for Hamiltonian certification and locality testing, for a continuous family of error metrics ranging from average- to worst-case. We also prove matching upper bounds for Hamiltonian certification in all cases, both with and without time reversal, showing that the advantage from time reversal persists. Our results follow from a new harmonic analysis-based approach to quantum lower bounds in continuous time, which is sensitive to time reversal and applicable beyond Hamiltonian property testing. This gives an alternative proof that inverses are required for amplitude amplification and estimation, improving the lower bounds of Tang and Wright [TW26] and extending to fractional queries. We also show that, for unstructured search, uncertainty in the phase of the oracle destroys the quantum speedup without inverse queries, even when the oracle is fixed and coherent. Our work rigorously establishes time reversal as a resource governing both the precision of quantum measurement and the robustness of quantum algorithms.

1 Introduction

Reversing time evolution is a ubiquitous and often underappreciated step in quantum information processing. In quantum algorithms, inverses of unitary operations enable a suite of tools, from basic primitives like amplitude amplification [BHMT02] and uncomputation [Ben73], to state-of-the-art methods for Hamiltonian simulation via quantum signal processing [GSLW19]. Time reversal is also used as a resource in quantum metrology [Li+23; Kob+24], while in many-body physics it underpins signatures of chaos and information scrambling like out-of-time-ordered correlators [SBSH16; YCZ20; Goo25].

In light of these applications, it is natural to ask when time reversal is truly necessary. More broadly, a central goal in quantum information theory is to understand which resources confer a provable advantage in solving problems. In quantum learning theory, for instance, prior work has established rigorous separations in the complexity of characterizing quantum systems with and without quantum memory [Hua+22; CCHL22; Che+24b], adaptive measurements [Che+23; CGZ24], or state preparation unitaries [Hug+22; ACGN23]. Yet, the necessity of time-reversed dynamics in learning and testing of quantum systems has been largely unexplored.

*Center for Theoretical Physics — a Leinweber Institute, MIT, USA; allenr@mit.edu
†Department of Computer Science, University of Warwick, UK; matthias.caro@warwick.ac.uk
‡QuICS, University of Maryland, USA ⟶ University of Edinburgh, UK. yanlin.chen@ed.ac.uk
§Department of Computer Science and Technology, University of Cambridge, UK; tg508@cam.ac.uk
¶Center for Theoretical Physics — a Leinweber Institute, MIT, USA; alowe7@mit.edu

Recent work addresses a variant of this question by showing that computational tasks become fundamentally harder without inverses of unitary oracles [FK18; CSM23; SHH25]. A prominent example is the work of Tang and Wright [TW26], which proves that inverse queries are necessary for amplitude amplification and estimation: forward-only algorithms require $\Omega(1/\varepsilon^2)$ queries to achieve precision ε, whereas inverse access reduces this cost to $O(1/\varepsilon)$. However, in this and all prior examples, the separation between forward and inverse access is established only for *discrete* queries, where a fixed unitary oracle U (or $U^\dagger$) is applied an integer number of times. By contrast, in realistic quantum experiments, unitary evolution is generated by *continuous-time* Hamiltonian dynamics.

Given this difference, the power of time reversal remains unclear in more physical settings. Indeed, it is not obvious that separations in the discrete query model should still hold in the continuous time setting. For example, with the ability to perform short-time evolution, Hamiltonian learning is possible using $O(1/\varepsilon)$ total evolution time [HTFS23], whereas with only long-time evolution this is no longer the case[1] [DOS24; Hu+25]. We therefore ask: *Does time reversal enable a provable advantage in continuous-time quantum experiments?*

The emerging field of Hamiltonian property testing provides a natural setting to explore this question [BCO26; ADG25]. For nearly all problems studied here, the best-known algorithms without time reversal achieve $O(1/\varepsilon^2)$ total evolution time, the *standard quantum limit*, even allowing short-time evolution, ancillas, and arbitrary quantum control [KL25; ST25]. By contrast, with time reversal, it is often possible to restore the *Heisenberg limit* of $O(1/\varepsilon)$ scaling [KL25; Gao+26].[2]

1.1 Main results

In this work, we show that time reversal is necessary to close this gap in general. To prove our results, we introduce a new, harmonic analysis-based approach to quantum lower bounds which works naturally in continuous time and distinguishes forward from reverse dynamics. This approach overcomes barriers to continuous-time extensions of existing quantum lower bound techniques, such as the compressed oracle method [Zha19; Fox+26; TW26] (see Section 1.2). Using our new approach, we prove—in a unified manner—that time reversal is necessary for a variety of problems in and beyond Hamiltonian property testing. Moving forward, we anticipate this framework may have broader applications, for example, to studying the complexity of other inherently quantum problems [SY23; Bos+25].

Hamiltonian certification. We first establish lower bounds on the total evolution time required for *Hamiltonian certification* [Gao+26], the task of deciding whether an unknown Hamiltonian H is equal to or far from a known target Hamiltonian:

Problem 1.1 (Hamiltonian certification)**.** Let $\varepsilon \in (0,1)$, and let $H_0 \in \mathbb{C}^{d\times d}$ be a known target Hamiltonian such that $\|H_0\| \le 1$ and $\mathrm{tr}(H_0) = 0$. Given black-box access to time evolution under an unknown Hamiltonian $H \in \mathbb{C}^{d\times d}$ such that $\|H\| \le 1$ and $\mathrm{tr}(H) = 0$, perform the following:

- (completeness) if $H = H_0$, accept with probability at least 99/100;
- (soundness) if $\frac{1}{\sqrt{d}}\|H - H_0\|_2 \ge \varepsilon$, accept with probability at most 1/100.

As is standard, this task is defined with respect to normalized Frobenius norm $\|\cdot\|_2/\sqrt{d}$, which is naturally interpreted as an average-case rate of distinguishability between the pair of Hamiltonians

[1] Unless one is willing to pay a cost that scales exponentially in the number of terms in the Hamiltonian [SLO26].

[2] We note that Heisenberg-limited scaling for Hamiltonian certification is also known to be achievable without time reversal, but only under additional locality assumptions on the unknown Hamiltonian [Blu+26; ST26], see Section 1.3.

(see Appendix A). We assume $\mathrm{tr}(H) = \mathrm{tr}(H_0) = 0$ without loss of generality since Hamiltonian trace is undetectable. The assumption on operator norm is also without loss of generality, since one can rescale the units of energy and time to accommodate the general case. We show:

Theorem 1.2. *Any quantum algorithm without time reversal for Hamiltonian certification (Problem 1.1) requires a total evolution time*

$$T_{\rightarrow} = \Omega\left(\min\left\{\frac{1}{\varepsilon^2}, \frac{\sqrt{d}}{\varepsilon}\right\}\right). \tag{1}$$

We prove this is tight (see below). It should be emphasized that Theorem 1.2 holds for any quantum algorithm without time reversal, including algorithms that use arbitrarily many ancillas, interleaved unitaries, and time evolution queries of any non-negative duration. Comparing Theorem 1.2 with the main result of [Gao+26], which gives an $O(1/\varepsilon)$ time Hamiltonian certification algorithm *with* time reversal, this proves a separation between quantum algorithms with and without time reversal.

From average- to worst-case norms. While the normalized Frobenius norm has become the standard error metric in Hamiltonian property testing, in many settings an average-case guarantee is not sufficient. On the opposite end of the spectrum is the operator norm $\|\cdot\|$, which characterizes the worst-case rate of distinguishability. This is reminiscent of the error metrics used in learning and tomography, where the goal is to obtain a complete description of the queried object. In these settings, Heisenberg-limited scaling typically *is* attainable without time reversal or inverses [HTFS23; HKOT23]. One may therefore ask whether the separation between Hamiltonian property testing with and without time reversal persists for other choices of norm, or if it is particular to the use of an average-case norm.

We prove that the separation persists, for a continuous family of norms interpolating between average- and worst-case; namely, the normalized Schatten p-norms $\|\cdot\|_p/d^{1/p}$ with $p \in [2,\infty]$.[3] We give tight upper and lower bounds for Hamiltonian certification in all such norms, both with and without time reversal. Letting $T_{\rightarrow}$ and $T_{\leftrightarrow}$ denote the total evolution time for Hamiltonian certification without and with time reversal, we prove, for any $p \in [2,\infty]$,

$$T_{\rightarrow} = \Theta\left(\min\left\{\frac{1}{\varepsilon^p}, \frac{d^{1-1/p}}{\varepsilon}\right\}\right) \quad \text{and} \quad T_{\leftrightarrow} = \Theta\left(\min\left\{\frac{1}{\varepsilon^{p/2}}, \frac{d^{1/2-1/p}}{\varepsilon}\right\}\right). \tag{2}$$

This extends the known upper bounds for Hamiltonian certification in normalized Frobenius norm ($p = 2$) with [Gao+26] and without [ST25] time reversal to the high-precision regime $\varepsilon \ll 1/\sqrt{d}$. It also resolves the former work's open question on the difficulty of Hamiltonian certification in norms other than normalized Frobenius norm. With these tight bounds, we fully characterize the time complexity of Hamiltonian certification, from average- to worst-case error.

Hamiltonian locality testing. Beyond certification, our techniques can be used to prove lower bounds for other problems in Hamiltonian property testing. In particular, we consider *Hamiltonian locality testing* [BCO26; ADG25; KL25], the task of deciding whether an unknown Hamiltonian H is k-local or far from all k-local Hamiltonians:

Problem 1.3 (Hamiltonian locality testing)**.** Let $\varepsilon \in (0,1)$, and let k and n be positive integers with $k \leq n$. Given black-box access to time evolution under an unknown n-qubit Hamiltonian $H \in \mathbb{C}^{2^n \times 2^n}$ such that $\|H\| \leq 1$ and $\mathrm{tr}(H) = 0$, perform the following:

[3] Here and throughout the paper, we adopt the conventions $1/\infty = 0$, $x^\infty = 0$ for $|x| < 1$, $x^\infty = \infty$ for $x > 1$, etc. We further treat $p < \infty$ as a constant in all asymptotic bounds.

- (completeness) if H is k-local, accept with probability at least 99/100;
- (soundness) if $\frac{1}{\sqrt{2^n}}\|H - H_{\mathrm{loc}}\|_2 \geq \varepsilon$ for all k-local H_{loc}, accept with probability at most 1/100.

We show the following lower bound for this task.

Theorem 1.4. *For constant $k \geq 1$, any quantum algorithm without time reversal for Hamiltonian locality testing (Problem 1.3) requires a total evolution time*

$$T_{\rightarrow} = \Omega\left(\min\left\{\frac{1}{\varepsilon^2}, \frac{\sqrt{d}}{\varepsilon}\right\}\right). \tag{3}$$

Theorem 1.4 shows that the $O(1/\varepsilon^2)$ time locality testing algorithm without time reversal in [KL25] is optimal (in the low-precision regime $\varepsilon \gg 1/\sqrt{d}$). That work additionally gives an $O(1/\varepsilon)$ time algorithm with time reversal, so Theorem 1.4 again proves a separation between quantum algorithms with and without time reversal.

Amplitude amplification and estimation. Though our techniques are well-suited to proving lower bounds in a continuous time setting, they are also applicable in the traditional unitary oracle model. Here, the analogous question to the role of time reversal is whether or not access to the inverse unitary oracle offers an advantage. Using our new methods, we revisit the question posed in [TW26] on the power of inverses for amplitude amplification and estimation.

Problem 1.5 (Amplitude amplification and estimation)**.** Let $\varepsilon \in (0, 1)$, $\Pi \in \mathbb{C}^{d\times d}$ be a known orthogonal projector, and $|0\rangle \in \mathbb{C}^d$ be a fixed initial state. Let U be a d-dimensional unitary operator such that

$$U|0\rangle = a|\phi_\Pi\rangle + \sqrt{1-a^2}|\phi_{\Pi^\perp}\rangle \tag{4}$$

where $\Pi|\phi_\Pi\rangle = |\phi_\Pi\rangle$ and $\Pi|\phi_{\Pi^\perp}\rangle = 0$. Given black-box access to U, the goal of *amplitude amplification* is to output a state which is 1/100-close to $|\phi_\Pi\rangle$ in trace distance, and the goal of *amplitude estimation* is to output an estimate $\hat{a}$ which is ε-close to a with probability at least 99/100.

We give an alternative proof of the main result in [TW26], which also improves upon their bound in the high-precision regime:

Theorem 1.6. *Given only the ability to apply the d-dimensional unitary U and not its inverse, any algorithm for amplitude amplification or estimation (Problem 1.5) requires*

$$\Omega\left(\min\left\{\frac{1}{a^2}, \frac{\sqrt{d}}{a}\right\}\right) \quad \text{or} \quad \Omega\left(\min\left\{\frac{1}{\varepsilon^2}, \frac{\sqrt{d}}{\varepsilon}\right\}\right) \tag{5}$$

applications of U, respectively, even allowing for fractional queries.

In the high-precision regime ($a, \varepsilon \ll 1/\sqrt{d}$), Theorem 1.6 improves over the $\Omega(\min(1/a^2, d))$ and $\Omega(\min(1/\varepsilon^2, d))$ lower bounds in [TW26], restoring the dependence on precision in all regimes. Moreover, whereas the techniques in [TW26] do not easily generalize to fractional queries (see Section 1.2), our results naturally extend to this setting.

Search with coherent errors. Finally, we demonstrate an application where our techniques can be used to analyze the robustness of oracle speedups without inverse queries:

Problem 1.7 (Search with coherent errors)**.** Let $d \geq 1$ and $0 \leq M \leq d$ be integers, and let $\Delta \in [0, \pi)$. Let $O_f^\theta \in \mathbb{C}^{d \times d}$ be a unitary of the form

$$O_f^\theta = \sum_{x=1}^{d} e^{i\theta_x f(x)} |x\rangle\langle x| \tag{6}$$

for unknown angles $\theta_x \in [\pi - \Delta, \pi + \Delta]$ and unknown $f\colon [d] \to \{0, 1\}$ that marks M elements, i.e., $|f^{-1}(1)| = M$. Given black-box access to O_f^θ:

- if $|f^{-1}(1)| = 0$ output NONE;
- otherwise, output any x such that $f(x) = 1$,

with failure probability at most $1/100$ in each case.

In the case $\Delta = 0$, we have $\theta_x = \pi$ for each $x \in [d]$, and $O_f^\theta = O_f \coloneqq \sum_{x=1}^{d} (-1)^{f(x)} |x\rangle\langle x|$; this is the usual phase oracle for a Boolean function f (when $d = 2^n$ and we identify the Hilbert space with that of n qubits). On the other hand, if $\Delta \to \pi$, then O_f^θ could potentially apply no phase to the marked elements, rendering it impossible to detect.

Between these two extremes, one may ask how much of the usual Grover speedup is preserved. If the phases being applied by the oracle are known in advance, then prior work shows that the speedup can remain completely intact [Høy00]. By contrast, we show that when the phases are unknown—but still fixed—the quantum speedup is destroyed:

Theorem 1.8. *Given only the ability to apply O_f^θ, and not its inverse, any algorithm for search with coherent errors (Problem 1.7) with $M = \Theta(1)$ requires at least $\Omega(d\Delta)$ applications of O_f^θ.*

On the other hand, we show in Section 3.2 that $\widetilde{O}(\sqrt{d})$ queries to O_f^θ and $(O_f^\theta)^\dagger$ suffice to solve Problem 1.7, by utilizing ideas from quantum signal processing (QSP). Thus, our result highlights a scenario in which inverses are a necessary ingredient for robust quantum algorithmic speedups.

1.2 Proof overview

We now describe the key technical ingredients for our lower bounds in the absence of time reversal. These are handled in a unified manner, via a reduction from a common one-versus-many distinguishing task: We exhibit a simple Hamiltonian (null hypothesis), together with an ensemble of Hamiltonians (mixture of alternatives), and show that distinguishing between the two cases without time reversal requires a long total evolution time.

1.2.1 Distinguishing task

In our construction, which we describe in full detail in Problem 2.1, we let the null hypothesis H_0 be the zero Hamiltonian. As we explain in Section 3.1, this choice still encompasses the hardest instances of the Hamiltonian certification problem. For our mixture of alternatives, we define a simple random Hamiltonian $\boldsymbol{H}_1 = \sum_i \boldsymbol{h}_i \Pi_i$ for some random $\boldsymbol{h}_i \in \mathbb{R}$ and fixed diagonal projectors $\Pi_i \in \mathbb{C}^{d \times d}$, which we describe shortly. To complete the reduction to property testing, we need only

prove that, with high probability, such a random Hamiltonian does not have the property of interest, while the zero Hamiltonian does.[4]

We let the entries $\boldsymbol{h}_i = \boldsymbol{\beta}_i \boldsymbol{\theta}_i$ of our random Hamiltonian be independent, uniformly random angles $\boldsymbol{\theta}_i \sim \mathrm{Unif}([-\sigma, \sigma])$, each of which is multiplied by an independent Bernoulli random variable $\boldsymbol{\beta}_i \sim \mathrm{Ber}(\mathsf{p})$. The random angles are essential, since they exclude the possibility of engineering a self-inverse operator by evolving for some fixed amount of time. Otherwise, an algorithm could potentially invoke amplitude amplification without explicit access to time reversal.

Decoupling dimension from precision. For $\boldsymbol{H}_1 \in \mathbb{C}^{d \times d}$ to be detectable by Hamiltonian certification against the zero Hamiltonian H_0, we must ensure it has norm at least ε with high probability. In particular, if the projectors Π_i are rank-1, this requires $\mathsf{p} \gtrsim 1/d$ at a minimum, forcing the parameter choices d and p to be coupled. This is in tension with the fact that p controls the distinguishability of the ensemble from zero, and thus a strong lower bound arises from choosing p as small as possible, perhaps as small as ε^2. The resulting bound is therefore not applicable in the high-precision regime where $\varepsilon^2 \ll 1/d$, and a similar obstruction appears in the argument in [TW26]. To circumvent this issue, we decouple these parameters by picking the projectors Π_i to have a rank which depends on the choice of d and the accuracy parameter ε. This allows us to handle both the high- and low-precision regimes in Hamiltonian property testing and amplitude estimation.

Altered ensemble for quantum search lower bounds. To prove our lower bound for search with coherent errors, Problem 1.7, we modify the above ensemble by shifting the random angles to $\boldsymbol{\theta}_i \sim \mathrm{Unif}([\pi - \sigma, \pi + \sigma])$. This also changes the dependence of the hardness on the uncertainty parameter σ compared to the previous setting. For a mean-zero angle as above, a larger deviation σ corresponds to a signal that can be detected. Now, with the shift, the distinguishing task becomes more difficult as σ increases; we are adding inexactness to the phases of an otherwise well-behaved oracle. The lower bound in Theorem 2.2 captures both regimes.

1.2.2 Barriers to existing techniques

There is a wealth of existing techniques for proving quantum lower bounds, but many of these methods are not powerful enough for our setting, because they do not generalize to inverse queries, to continuous time, or to either. For example, a naive first attempt at upper bounding the distance between the states under the null and alternative hypotheses (and thus proving an evolution time lower bound) would be via a variant of the hybrid method [BBBV97]. In the hybrid method, one upper bounds this distance by the contributions from each query, resulting in a sum of distances between "hybrid" states which differ by only a *single* query. However, there is an apparent mismatch between our goal and this route: it is not sensitive to the fact that all our evolution times are non-negative. Indeed, because $\boldsymbol{H}_1$ and $-\boldsymbol{H}_1$ are identically distributed, any expression which depends on only the j-th query is invariant under $t_j \mapsto -t_j$. Therefore, the hybrid argument instead leads to the "trivial" Heisenberg lower bound.

Compressed oracle method. An alternative to this strategy, which was employed successfully in [TW26] to prove lower bounds for amplitude estimation, would be to use the compressed oracle method [Zha19; Fox+26]. While this technique has recently been applied to many problems in quantum query complexity [LZ19; TW26; JZ25] and cryptography [CFHL21; MH25; Car26], it

[4] This ought to be true of most reasonable properties, since a random Hamiltonian of this form is highly unstructured.

appears to break down in the continuous time setting. This prevents a straightforward extension of the proof strategy from [TW26] to Hamiltonian property testing, as we now elaborate.

The starting point in the compressed oracle method is to view the randomness in a random unitary as arising from a purification of the system to a larger Hilbert space. Since isometries acting on the purifying system are undetectable, a key step in the method is to demonstrate that two states are related by such an isometry (or approximately related, as in [TW26]). In many cases, this isometry is recognizable as a group Fourier transform [Fox+26]. Unfortunately, continuous time can destroy this group structure, making it impossible for such an isometry to exist. For example, if the group is $\mathbb{Z}_2^N$, an emblematic set of states are of the form

$$\frac{1}{\sqrt{2^N}} \sum_{f \in \{0,1\}^N} (-1)^{f(x_1)+\cdots+f(x_t)} |f\rangle \tag{7}$$

for some collection of *distinct* $x_1, \ldots, x_t \in \{1, \ldots, N\}$. These states appear in the construction of [MH25], in the purifying register, after querying a phase oracle for f some number of times t. Applying the Fourier transform over $\mathbb{Z}_2^N$, i.e., the tensor product of single-qubit Hadamards, gives $|z_1 \ldots z_N\rangle$, where $z_x = 1$ if $x \in \{x_1, \ldots, x_t\}$. Hence, the original collection of states is isomorphic to the set of basis states $|\{x_1, \ldots, x_t\}\rangle$ indexed by the possible sets of distinct $x_1, \ldots, x_t$.

Now suppose instead that the original states are of the form

$$\frac{1}{\sqrt{2^N}} \sum_{f \in \{0,1\}^N} i^{f(x_1)+\cdots+f(x_t)} |f\rangle\,, \tag{8}$$

once again for distinct $x_1, \ldots, x_t$. This would be the case if we were allowed queries to the square root of the phase oracle for f. These states are not even necessarily orthogonal, and so in particular there is no isometry to basis states indexed by the possible $x_1, \ldots, x_t$. A similar phenomenon, for $\mathbb{Z}_q$ instead of $\mathbb{Z}_2^N$, causes the argument in [TW26] to break down for fractional queries, even given access just to the principal square root $\sqrt{U}$ of the unitary U in amplitude estimation.

1.2.3 Lower bound method

We overcome these barriers by developing a new method for proving quantum lower bounds with random unitary oracles accessed in continuous time. Before illustrating the main ideas behind this method, we provide some basic setup. For simplicity, in this proof sketch we consider only the low-precision regime $\varepsilon^2 \gg 1/d$ (and take the simplest case $\sigma \sim 1$ and $\mathsf{p} \sim \varepsilon^2$), so our goal is to prove a $T = \Omega(1/\varepsilon^2)$ lower bound.

Recall that the random Hamiltonian $\boldsymbol{H}_1$ is specified by a collection of i.i.d. real-valued random variables $\boldsymbol{h}_1, \ldots, \boldsymbol{h}_m$. Suppose a quantum algorithm makes q black-box queries for times $t_1, \ldots, t_q \geq 0$ to time evolution under $\boldsymbol{H}_1$, for a total evolution time of $T \coloneqq \sum_{j=1}^q t_j$. This results in a random final state $|\psi^{(q)}(\boldsymbol{h}_1, \ldots, \boldsymbol{h}_m)\rangle$ determined by the entries $\boldsymbol{h}_i$. Our goal is to prove that the corresponding mixed state is indistinguishable from the null state $|\psi_0^{(q)}\rangle \coloneqq |\psi^{(q)}(0, \ldots, 0)\rangle$ unless $T \gtrsim 1/\varepsilon^2$. For this, it suffices to upper bound the expected transition probability under the null hypothesis,

$$\mathfrak{p} \coloneqq \mathbb{E} \left\| (I - |\psi_0^{(q)}\rangle\langle\psi_0^{(q)}|)\, |\psi^{(q)}(\boldsymbol{h}_1, \ldots, \boldsymbol{h}_m)\rangle \right\|_2^2, \tag{9}$$

by $O(\varepsilon^2 T)$. In particular, the trace distance between the two possible states is at most $\sqrt{\mathfrak{p}}$.

Efron-Stein decomposition. Our first main idea is to analyze the probability in Eq. (9) *one random variable at a time*, rather than one query at a time. To accomplish this, we leverage an idea from Boolean function analysis, namely, the *Efron-Stein decomposition*, which is a generalization of the Fourier transform. (See, for example, [ODo21, Chapter 8], or Appendix B.)

A well-known consequence of this decomposition is the *Efron-Stein inequality*, which states that for i.i.d. random variables $\boldsymbol{x}_i \in \mathbb{R}$ we have

$$\mathrm{Var}[f(\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n)] \leq \frac{1}{2} \sum_{i=1}^{n} \mathbb{E}\left[\left(f(\boldsymbol{x}_1, \ldots, \boldsymbol{x}_i, \ldots, \boldsymbol{x}_n) - f(\boldsymbol{x}_1, \ldots, \boldsymbol{x}'_i, \ldots, \boldsymbol{x}_n)\right)^2\right], \tag{10}$$

where $f\colon \mathbb{R}^n \to \mathbb{R}$ and $\boldsymbol{x}'_i$ is a fresh copy of the random variable $\boldsymbol{x}_i$. We use a vector-valued analogue of this inequality (Lemma 2.5) to bound the probability in Eq. (9) by a sum of m contributions. Specifically, we show that $\mathfrak{p} \lesssim \sum_{i=1}^{m} \mathbb{E}\||\boldsymbol{\Delta}_i\rangle\|_2^2$, where

$$|\boldsymbol{\Delta}_i\rangle = |\psi^{(q)}(\boldsymbol{h}_1, \ldots, \boldsymbol{h}_i, \ldots, \boldsymbol{h}_m)\rangle - |\psi^{(q)}(\boldsymbol{h}_1, \ldots, 0, \ldots, \boldsymbol{h}_m)\rangle\,. \tag{11}$$

Each of the terms has a clear interpretation: it is the distinguishability between the true output state (in the alternative case) and the state obtained by the algorithm when we fix a *single* entry $\boldsymbol{h}_i$ in the Hamiltonian to be zero. We proceed to bound each of these contributions to the overall distinguishability, as described below.

Connection to Brownian motion. Let us focus on the contribution corresponding to a single entry $\boldsymbol{h}_i$ of the Hamiltonian, as justified by the above. We use a standard sum over Feynman paths to expand the final state; thanks to the Efron-Stein decomposition, we need only record whether the i-th subspace (corresponding to Π_i) was visited at a given step along the path. We may then write

$$|\psi^{(q)}(\boldsymbol{h}_1, \ldots, \boldsymbol{h}_m)\rangle = \sum_{z \in \{0,1\}^q} |\varphi_z^{(i)}(\boldsymbol{h}_1, \ldots, \boldsymbol{h}_m)\rangle \tag{12}$$

for some unnormalized $|\varphi_z^{(i)}(\boldsymbol{h}_1, \ldots, \boldsymbol{h}_m)\rangle$, where z is a description of the path taken over the q queries: a "1" indicates that Π_i was visited (see Section 2.2 for rigorous definitions). The true output state accumulates a phase $e^{-i\boldsymbol{h}_i t_j}$ if the j-th query visits Π_i, while the state with $\boldsymbol{h}_i$ fixed to zero does not. The difference vector $|\boldsymbol{\Delta}_i\rangle$ in Eq. (11) is therefore

$$|\boldsymbol{\Delta}_i\rangle = \sum_{z \in \{0,1\}^q} \left(e^{-i\boldsymbol{h}_i \sum_{j:z_j=1} t_j} - 1\right) |\varphi_z^{(i)}(\boldsymbol{h}_1, \ldots, 0, \ldots, \boldsymbol{h}_m)\rangle\,. \tag{13}$$

Taking a step back, recall that our goal is to prove that $\mathfrak{p}$ grows at most linearly with total evolution time T, thereby proving the desired standard quantum limited lower bound. The key idea in establishing this is to relate the growth of the difference vector $|\boldsymbol{\Delta}_i\rangle$ to *Brownian motion*. This is a natural approach, because the standard quantum limit can be interpreted as a *diffusive* growth of distinguishability (as compared with the Heisenberg limit, which corresponds to ballistic growth). To illustrate this connection more quantitatively, let $B(t)$ be a standard Brownian process, and suppose the path amplitudes in Eq. (13) were determined directly according to B, resulting in a difference vector

$$|\widetilde{\boldsymbol{\Delta}}_i\rangle \coloneqq \sqrt{\pi \mathfrak{p}} \sum_{z \in \{0,1\}^q} B\Big(\sum_{j:z_j=1} t_j\Big) |\varphi_z^{(i)}(\boldsymbol{h}_1, \ldots, 0, \ldots, \boldsymbol{h}_m)\rangle\,. \tag{14}$$

Consider adding a query of duration t_j. Every path visiting Π_i advances its Brownian "clock" by t_j. For two such paths, with previous clock readings s and s', we have

$$\mathbb{E}[B(s+t_j)B(s'+t_j)] = \min(s,s') + t_j = \mathbb{E}[B(s)B(s')] + t_j.$$

Thus, the new query adds exactly t_j to their covariance, regardless of how much time either path has already accumulated. This additive contribution leads to overall diffusive growth of the distinguishability, resulting in standard quantum limited scaling.

Of course, the difference vector Eq. (13) is not actually equal to $|\widetilde{\boldsymbol{\Delta}}_i\rangle$. However, we can relate the two; in particular, the second moments of the amplitudes in Eq. (13) are upper bounded by those of Eq. (14). This crucial connection to Brownian motion, which we describe in the following paragraph, is the crux of our proof.

The role of time reversal. Expanding the contribution $\mathbb{E} \| |\boldsymbol{\Delta}_i\rangle \|_2^2$ using the decomposition Eq. (13), we have

$$\mathbb{E}\||\boldsymbol{\Delta}_i\rangle\|_2^2 = \sum_{z,z' \in \{0,1\}^q} c_{z,z'} \underbrace{\mathop{\mathbb{E}}_{\boldsymbol{h}_i} (e^{i\boldsymbol{h}_i \mathtt{t}_{z'}} - 1)(e^{-i\boldsymbol{h}_i \mathtt{t}_z} - 1)}_{=:K(\mathtt{t}_{z'}, \mathtt{t}_z)}, \tag{15}$$

for some coefficients $c_{z,z'}$, where we have defined $\mathtt{t}_z \coloneqq \sum_{j:z_j=1} t_j$. In Lemma 2.6, we upper bound the positive-definite *kernel* $K(\cdot,\cdot)$ by the covariance kernel for Brownian motion (namely, the min kernel); we prove using basic techniques from Fourier analysis that

$$\sum_{z,z'} c_z^* c_{z'} K(\mathtt{t}_z, \mathtt{t}_{z'}) \le \pi \mathtt{p} \sum_{z,z'} c_z^* c_{z'} \min(\mathtt{t}_z, \mathtt{t}_{z'}) \tag{16}$$

for arbitrary $c_z \in \mathbb{C}$, *so long as* $\mathtt{t}_z \ge 0$. This is the crucial—and only—place where we use that the algorithm makes only forward time queries. Note that this bound no longer holds if $\mathtt{t}_z$ can be negative (see the explicit counterexample following the proof of Lemma 2.6). Hence, the kernel being constrained in this manner is a footprint of the lack of time-reversed dynamics.

From Eq. (16), straightforward algebra with the $\min(\cdot,\cdot)$ kernel shows that $\mathfrak{p}$ in Eq. (9) is $O(\varepsilon^2 T)$. This yields the $T = \Omega(1/\varepsilon^2)$ total evolution time lower bound for the low-precision regime. The same proof strategy yields a bound in the high-precision regime where $\varepsilon^2 \ll 1/d$ by choosing different values of σ and $\mathtt{p}$.

1.3 Discussion

Implications for reversing time evolution. Our lower bounds implicitly constrain the cost of engineering time reversal, i.e., accurately approximating reverse time evolution (e.g., in diamond norm) using only forward evolution. However, reproducing the time-reversed dynamics on arbitrary input states is considerably more demanding than the property testing problems studied in our work, so the optimal reversal cost presumably exceeds the bounds inherited from testing. A promising connection is to the literature on inverting unknown unitaries, where inversion requires $\Theta(d^2)$ queries even at constant error [Che+24a; OYM25; CYZ26]. Extending these discrete-query bounds to continuous time is a natural direction for which to employ our techniques.

Beyond arbitrary Hamiltonians, applications in quantum metrology and Hamiltonian engineering motivate studying time reversal of local Hamiltonians [Li+23; Kob+24]. It is already known how to reverse local Hamiltonians with polynomial overhead in the number of qubits, assuming fast control [WRJB02; OKSM24; CBW25]. Notably, our certification lower bound does not apply in this

setting, since we consider non-local Hamiltonians; indeed, Heisenberg-limited certification of local Hamiltonians is already possible using only forward time evolution [Blu+26; ST26]. It would be interesting to determine how the cost of time reversal depends on both the interaction structure of the Hamiltonian and the available controls.

Robustness of quantum algorithms. Our lower bound in Theorem 1.8 adds to a line of work studying the effect of imperfect oracles on quantum speedups, both for unstructured search [RS08; Tem14; Ros23] and other problems [HR14; SC26]. Most prior impossibility results focus on models where a noisy channel is applied between successive calls to the oracle; this includes standard dephasing noise (as in [RS08; Tem14]), where fresh randomness is used at each application of the channel. Our lower bound applies in a different, fully unitary setting. Namely, in our work, we study the impact of coherent errors, unknown deviations in the ideal phases of the oracle which are nevertheless consistent across all queries. Coherent errors are a ubiquitous noise source in quantum computation, due to systematic device miscalibrations and non-Markovian drifts [Bur+19; Sha+24], but their impact on oracle speedups remains comparatively understudied. We show that no Grover-like quantum speedup is possible for search with coherent errors, except with access to the inverse oracle.

Our lower bound is reminiscent of no-go results for general correction of QSP sequences with unknown, but static, perturbations of the signal angles [TLTC23]. We view it as an interesting open question to investigate whether our techniques, or some variant of them, could be used to explore the robustness of these and other quantum algorithms to coherent errors.

Note added. During the preparation of this manuscript, we received a draft of related work by Escudero Gutiérrez, Lee, and Zur [GLZ26]. Their work independently establishes an $\Omega(1/\varepsilon^2)$ lower bound—the same scaling as in our lower bounds for the low-precision regime—on the total evolution time required by any algorithm without time reversal for Hamiltonian locality testing and certification as well as for amplitude estimation with fractional queries. Their proofs use a different approach via an adversary argument.

2 Lower bounds without time reversal

In this section, we prove our main lower bounds without time reversal. We begin with a description of a hard distinguishing task in Section 2.1, where we also show that the problems we study reduce to this task. This section also contains the proofs of our main results assuming the hardness of that task. We then prove a lower bound on the evolution time required to solve the distinguishing task in Section 2.2. Finally, in Section 2.3 we show how these results extend to all Schatten p-norms.

Computational model. We first formally define the computational model we consider throughout this work, which encompasses all possible quantum algorithms which can be executed given black-box queries to a family of unitary operators $U(t) \in \mathrm{U}(d)$. In the setting of Hamiltonian property testing of an unknown Hamiltonian H, we have $U(t) = \exp(-iHt)$. In the setting of fractional queries to a unitary oracle U, we have $U(t) = U^t$ for U^t the t-th principal power of U. A quantum algorithm *without* time reversal, or without inverse queries, can only choose $t \geq 0$, whereas a quantum algorithm *with* time reversal, or with inverse queries, can choose $t \in \mathbb{R}$.

We consider quantum algorithms with access to an ancillary Hilbert space $\mathbb{C}^{d_{\mathrm{anc}}}$ of arbitrarily large dimension d_{anc}. The algorithm is then specified by a pure initial state $|\psi\rangle \in \mathbb{C}^d \otimes \mathbb{C}^{d_{\mathrm{anc}}}$, a sequence of query durations $t_1, \ldots, t_q$, a sequence of interleaving unitaries $V_0, \ldots, V_q \in \mathrm{U}(d \cdot d_{\mathrm{anc}})$,

and a final POVM $\mathcal{F}$ on $\mathbb{C}^d \otimes \mathbb{C}^{d_{\text{anc}}}$. The output of the algorithm is the result of performing the POVM $\mathcal{F}$ on the state

$$V_q(U(t_q) \otimes I)V_{q-1}(U(t_{q-1}) \otimes I) \dots V_1(U(t_1) \otimes I)V_0 \left|\psi\right\rangle, \tag{17}$$

where I denotes the identity on $\mathbb{C}^{d_{\text{anc}}}$.

A few remarks on the generality of this definition are in order. First, it suffices to consider pure initial states and unitary operations, since mixed initial states can be purified and quantum channels can be dilated to unitary operators on a larger Hilbert space, simply by increasing the dimension of the ancillary system. Similarly, this model encompasses adaptive algorithms which perform multiple intermediate measurements and apply unitary operations conditional on the measurement outcomes, again by increasing the dimension of the ancillary system and deferring all measurements.

Throughout this work, our figure of merit is the total evolution time (or total duration of fractional queries), defined as $T = \sum_{k=1}^{q} |t_k|$.

2.1 Reductions from a hard distinguishing task

The proof of Theorem 1.2 is based on the following distinguishing task which, with an appropriate choice of the parameters $d_{\text{eff}}, \mathsf{p}, \sigma, \theta_0$ appearing therein, reduces to several other tasks including Hamiltonian certification and locality testing in d dimensions.

Problem 2.1 (Block distinguishing task)**.** Let $\mathsf{p}, \sigma \in (0, 1/2]$, let $\theta_0 \in [0, 2\pi)$, let $d_{\text{eff}}, d \geq 100$ be positive integers such that $d_{\text{eff}} \leq d$, and let $\boldsymbol{b} \in \{0, 1\}$ be a uniformly random bit. Let $\boldsymbol{H} \in \mathrm{L}(\mathbb{C}^d)$ be a random Hamiltonian such that:

- (null) conditioned on $\boldsymbol{b} = 0$ we have $\boldsymbol{H} = 0$ with certainty; and
- (alternative) conditioned on $\boldsymbol{b} = 1$ we have $\boldsymbol{H} = \boldsymbol{H}_1 - \mathrm{tr}(\boldsymbol{H}_1)\frac{I}{d}$ for $\boldsymbol{H}_1 \coloneqq \sum_{j=1}^{d_{\text{eff}}} \boldsymbol{h}_j \Pi_j$,

where $\{\Pi_j\} \subset \mathrm{L}(\mathbb{C}^d)$ is a fixed set of rank-$\lfloor d/d_{\text{eff}} \rfloor$ diagonal projectors onto d_{eff} orthogonal subspaces, and for each $j \in [d_{\text{eff}}]$ we take $\boldsymbol{h}_j$ to be an independent copy of $\boldsymbol{\beta}\boldsymbol{\theta}$ for independent $\boldsymbol{\beta} \sim \mathrm{Ber}(\mathsf{p})$ and $\boldsymbol{\theta} \sim \mathrm{Unif}([\theta_0 - \sigma, \theta_0 + \sigma])$. Given black-box access to time evolution under $\boldsymbol{H}$, the goal is to output $\hat{\boldsymbol{b}} \in \{0, 1\}$ such that $\hat{\boldsymbol{b}} = \boldsymbol{b}$ with probability at least $3/5$.

Note, we have $d_{\text{eff}} \leq d$ because the number of blocks should not exceed the dimension. We would also like the random Hamiltonian to be traceless and have bounded operator norm, to form a valid input to the Hamiltonian certification problem. These are ensured by construction, due to the explicit centering and the assumption on the possible values of σ.

Our main theorems are consequences of the following lower bound on the total evolution time required to solve Problem 2.1 without access to time reversal:

Theorem 2.2. *Any quantum algorithm which solves Problem 2.1 with $\mathsf{p} = \Theta(1/d_{\text{eff}})$ by making oracle calls only to forward time evolution under $\boldsymbol{H}$ (i.e., $t_1, \dots, t_q \geq 0$) requires a total evolution time*

$$T_{\rightarrow} = \Omega\left(\min\left\{\frac{d_{\text{eff}}}{\sigma}, \frac{d_{\text{eff}}\sigma}{\theta_0^2}\right\}\right). \tag{18}$$

The proof of this theorem is the key technical contribution of our work, which we present in Section 2.2. We now briefly discuss how to interpret Eq. (18). On the one hand, when $\theta_0 = 0$, we are attempting to distinguish identity operations from small random phases being applied in

the standard basis. Hence, as the deviations in the phases $\sigma \to 0$, the distinguishing task becomes impossible. The first expression in the lower bound reflects this limiting case. On the other hand, if $\theta_0 > 0$ is some fixed constant, then large deviations σ are actually harmful for the distinguisher, since they drown out the signal provided by the phase θ_0. This can be seen from the second expression in the bound.

To prove our lower bounds for each of the problems in Section 1.1, we make use of reductions from the distinguishing task in Problem 2.1. The following two lemmas state that the alternative hypothesis is detectable by solving the main problems described in Section 1.1, given appropriate choices of the parameters therein. Hence, Theorem 2.2 implies the lower bound results in Section 1.1—namely, Theorems 1.2, 1.4, 1.6 and 1.8.

Lemma 2.3 (Small-angle reductions)**.** *Let $d \geq 100$ and $\varepsilon_0 \in [0, 1/10)$. Consider the distinguishing task in Problem 2.1 with $d_{\text{eff}} = \min\{d, \lceil 1/\varepsilon_0^2 \rceil\}$, $\mathsf{p} = 50/d_{\text{eff}}$, $\sigma = \varepsilon_0\sqrt{d_{\text{eff}}}/4$, and $\theta_0 = 0$, where we have black-box access to time evolution under the Hamiltonian $\boldsymbol{H} \in \mathbb{C}^{d\times d}$. With these choices, Problem 2.1 can be solved using a single call to a successful algorithm for any of the following problems, taking d and $\varepsilon = \varepsilon_0/40$ to be their dimension and accuracy parameters, respectively:*

1. *Hamiltonian certification (Problem 1.1) if we let $H_0 = 0$ and $\boldsymbol{H}$ be the input Hamiltonian;*
2. *Hamiltonian locality testing[5] (Problem 1.3) if we let $\boldsymbol{H}$ be the input Hamiltonian;*
3. *Amplitude estimation[6] (Problem 1.5) if we let $e^{-i\pi \boldsymbol{H}/2}$ be the unitary oracle and $\Pi = I - |s\rangle\langle s|$ be the known projector, where $|s\rangle = \frac{1}{\sqrt{d}} \sum_{j=1}^{d} |j\rangle$.*

We also have the following reduction when $\theta_0 > 0$, which is relevant for proving the lower bound for unstructured search with coherent errors.

Lemma 2.4 (Large-angle reduction)**.** *Let $\Delta \in [0, 1/2)$ be a fixed constant and let $d \geq 99$. Consider the distinguishing task in Problem 2.1 with $d_{\text{eff}} = d$, $\mathsf{p} = 50/d_{\text{eff}}$, $\sigma = \Delta$, and $\theta_0 = \pi$, where we have black-box access to time evolution under $\boldsymbol{H} \in \mathbb{C}^{d\times d}$. With these choices, Problem 2.1 can be solved using one call to a successful algorithm for search with coherent errors (Problem 1.7) with input parameters d and Δ, if we let $e^{-i\boldsymbol{H}}$ be the unitary oracle.*

Lemmas 2.3 and 2.4 are proven in Appendix C. The main lower bound results are now immediate based on these lemmas, by repeatedly invoking Theorem 2.2.

2.2 Proof of lower bound on hard distinguishing task

In this section we prove Theorem 2.2, which implies all the main lower bound results in this work, as explained in Section 2.1. The proof is based on a new framework for quantum query lower bounds using tools from Boolean Fourier analysis, namely, the Efron-Stein decomposition. (See [ODo21, Chapter 8].) In particular, a well-known consequence of this decomposition in discrete probability is the Efron-Stein inequality. The first ingredient in the proof of Theorem 2.2 is a variant of this inequality for vector-valued random variables.

[5] Here, we are identifying $\mathbb{C}^d \cong (\mathbb{C}^2)^{\otimes n}$ in the standard manner for n qubits, assuming $d = 2^n$, and using $d_{\text{eff}} = \min\{2^n, 2^{\lceil \log_2(1/\varepsilon_0^2)\rceil}\}$ due to the switch to qubits, but we omit this detail in rounding convention for clarity. We also need the additional assumptions on n and ε_0 which depend on k; see Lemma C.2.

[6] The reduction for amplitude amplification follows nearly identically to the reduction for amplitude estimation, see Section C.3.

Lemma 2.5 (Vector-valued, anchored Efron-Stein inequality)**.** *Let $f\colon \mathbb{R}^n \to \mathbb{C}^m$ be a function and let μ be a probability measure on $\mathbb{R}$. It holds that*

$$\mathop{\mathbb{E}}_{\boldsymbol{x}\sim\mu^{\otimes n}} \left\|f(\boldsymbol{x})\right\|_2^2 - \left\| \mathop{\mathbb{E}}_{\boldsymbol{x}\sim\mu^{\otimes n}} f(\boldsymbol{x})\right\|_2^2 \leq \sum_{i=1}^{n} \mathop{\mathbb{E}}_{\boldsymbol{x}\sim\mu^{\otimes n}} \left\|f(\boldsymbol{x}) - f(\boldsymbol{x}^{(i\to 0)})\right\|_2^2, \tag{19}$$

where $\boldsymbol{x}^{(i\to 0)} \coloneqq (\boldsymbol{x}_1, \ldots, \boldsymbol{x}_{i-1}, 0, \boldsymbol{x}_{i+1}, \ldots, \boldsymbol{x}_n)$ for each $i \in [n]$.

We defer the proof of Lemma 2.5 to Appendix B. In the proof of Theorem 2.2, this inequality is used as a first step to bound the distinguishability of two quantum states: the squared trace distance between them can be bounded from above by a sum of contributions, each of which corresponds to fixing a single term in the random Hamiltonian that generates the time evolution. It thereby suffices to bound the individual terms in the sum, in a way that is sensitive to whether the evolution times are nonnegative. To this end, we make use of the following result as a second ingredient in our proof of Theorem 2.2.

Lemma 2.6 (Kernel bound)**.** *Let $\theta_0, \sigma \in [0, 2\pi)$, let $\boldsymbol{\omega} \sim \mathrm{Unif}([\theta_0 - \sigma, \theta_0 + \sigma])$, and let $K(x, y) \coloneqq \mathbb{E}_{\boldsymbol{\omega}}(1 - e^{ix\boldsymbol{\omega}})(1 - e^{-iy\boldsymbol{\omega}})$. For every $n \in \mathbb{Z}_+$, $x_1, \ldots, x_n \geq 0$, and $c_1, \ldots, c_n \in \mathbb{C}$ it holds that*

$$\sum_{i,j=1}^{n} c_i^* c_j K(x_i, x_j) \leq \frac{\pi(\theta_0 + \sigma)^2}{\sigma} \sum_{i,j=1}^{n} c_i^* c_j \min(x_i, x_j). \tag{20}$$

Proof. Define $f\colon \mathbb{R} \to \mathbb{C}$ through $f(x) = \sum_{j=1}^{n} c_j \mathbf{1}[0 \leq x \leq x_j]$ for every $x \in \mathbb{R}$. We compute

$$\begin{aligned}
\sum_{i,j=1}^{n} c_i^* c_j K(x_i, x_j) &= \mathop{\mathbb{E}}_{\boldsymbol{\omega}} \sum_{i,j=1}^{n} c_i^* c_j (1 - e^{ix_i\boldsymbol{\omega}})(1 - e^{-ix_j\boldsymbol{\omega}}) && (21)\\
&= \mathop{\mathbb{E}}_{\boldsymbol{\omega}} \left| \sum_{j=1}^{n} c_j (1 - e^{-ix_j\boldsymbol{\omega}}) \right|^2 && (22)\\
&= \mathop{\mathbb{E}}_{\boldsymbol{\omega}} \left| \sum_{j=1}^{n} c_j (i\boldsymbol{\omega}) \int_0^{x_j} e^{-ix\boldsymbol{\omega}} \,\mathrm{d}x \right|^2 && (23)\\
&= \mathop{\mathbb{E}}_{\boldsymbol{\omega}} \left| i\boldsymbol{\omega} \int_{-\infty}^{\infty} f(x) e^{-ix\boldsymbol{\omega}} \,\mathrm{d}x \right|^2 && (24)\\
&\leq \frac{(\theta_0 + \sigma)^2}{2\sigma} \int_{\theta_0 - \sigma}^{\theta_0 + \sigma} \left| \int_{-\infty}^{\infty} f(x) e^{-ix\omega} \,\mathrm{d}x \right|^2 \mathrm{d}\omega && (25)\\
&\leq \frac{(\theta_0 + \sigma)^2}{2\sigma} \int_{-\infty}^{\infty} \left| \int_{-\infty}^{\infty} f(x) e^{-ix\omega} \,\mathrm{d}x \right|^2 \mathrm{d}\omega && (26)\\
&= \frac{\pi(\theta_0 + \sigma)^2}{\sigma} \int_{-\infty}^{\infty} |f(x)|^2 \,\mathrm{d}x && (27)\\
&= \frac{\pi(\theta_0 + \sigma)^2}{\sigma} \sum_{i,j=1}^{n} c_i^* c_j \int_{-\infty}^{\infty} \mathbf{1}[0 \leq x \leq x_i] \mathbf{1}[0 \leq x \leq x_j] \,\mathrm{d}x && (28)\\
&= \frac{\pi(\theta_0 + \sigma)^2}{\sigma} \sum_{i,j=1}^{n} c_i^* c_j \min(x_i, x_j), && (29)
\end{aligned}$$

where Eq. (25) follows from Hölder's inequality and in Eq. (27) we applied Plancherel's theorem. □

Notably, the inequality in Eq. (20) is *not* true if $x_1, \dots, x_n$ can be negative. For example, if all the coefficients c_i are equal while half of the points x_i satisfy $x_i = t$ and the other half satisfy $x_i = -t$ for some $t \in \mathbb{R}$, then the left-hand side of Eq. (20) is positive, while the right-hand side is negative. When we apply Lemma 2.6 below, the $x_1, \dots, x_n$ are given by partial sums of the evolution times under H. As mentioned in Section 1.2, this is the only place where we use that the algorithm makes only forward time queries.

We can now prove Theorem 2.2.

Proof of Theorem 2.2. Suppose a quantum algorithm makes $q \in \mathbb{Z}_+$ calls to the forward time evolution under $\boldsymbol{H}$ in Problem 2.1 for times $t_1, \dots, t_q \geq 0$. Let $\mathsf{t} = (t_1, \dots, t_q)$ denote the vector of times. For any $k \in \{0, 1, \dots, q\}$ and $z \in \{0,1\}^k$ we let $\mathsf{t}_z \coloneqq \sum_{j=1}^k z_j t_j$ (i.e., the sum of the first k times restricted to the subset with indicator z), so that $T = \mathsf{t}_{1^q}$ and $\mathsf{t}_{(y,b)} = \mathsf{t}_y + b\, t_k$ for all $y \in \{0,1\}^{k-1}$ and $b \in \{0,1\}$. We will bound the trace distance between the final states of the algorithm in the case where $\boldsymbol{b} = 0$ and $\boldsymbol{b} = 1$, respectively. First, we introduce notation for the different possible intermediate states of the algorithm. For $h \in \mathbb{R}^{d_{\text{eff}}}$ and any integer k such that $0 \leq k \leq q$ we let

$$|\psi_h^{(k)}\rangle \coloneqq V_k(e^{-iHt_k} \otimes I)V_{k-1}(e^{-iHt_{k-1}} \otimes I) \dots V_1(e^{-iHt_1} \otimes I)V_0\,|\psi\rangle \quad \text{where} \quad H = \operatorname{diag}(h). \tag{30}$$

(Recall from our discussion at the beginning of Section 2 that V_j is our notation for the unitary operations fixed by the algorithm.) This is the state of the distinguishing algorithm after k calls to the time evolution operator under $\operatorname{diag}(h)$. Let $\boldsymbol{h} = (\boldsymbol{h}_1, \dots, \boldsymbol{h}_{d_{\text{eff}}})$ where $\boldsymbol{h}_1, \dots, \boldsymbol{h}_{d_{\text{eff}}} \in \mathbb{R}$ are iid copies of $\boldsymbol{\beta}\boldsymbol{\theta}$ for independent $\boldsymbol{\beta} \sim \operatorname{Ber}(\mathsf{p})$ and $\boldsymbol{\theta} \sim \operatorname{Unif}([\theta_{\min}, \theta_{\max}])$, as in Problem 2.1. Conditioned on $\boldsymbol{b} = 0$ the final state of the algorithm is $|\psi_0^{(q)}\rangle$ with certainty, and conditioned on $\boldsymbol{b} = 1$ the final state of the algorithm is the random state $|\psi_{\boldsymbol{h}}^{(q)}\rangle$. Our goal is therefore to bound the quantity

$$\begin{aligned}
\mathrm{d_{tr}}\big(\,|\psi_0^{(q)}\rangle\langle\psi_0^{(q)}|\,, \mathop{\mathbb{E}}_{\boldsymbol{h}} |\psi_{\boldsymbol{h}}^{(q)}\rangle\langle\psi_{\boldsymbol{h}}^{(q)}|\,\big)^2 &\coloneqq \frac{1}{4}\Big\| |\psi_0^{(q)}\rangle\langle\psi_0^{(q)}| - \mathop{\mathbb{E}}_{\boldsymbol{h}} |\psi_{\boldsymbol{h}}^{(q)}\rangle\langle\psi_{\boldsymbol{h}}^{(q)}| \Big\|_1^2 && (31)\\
&\leq \mathop{\mathbb{E}}_{\boldsymbol{h}}(1 - |\langle\psi_0^{(q)}|\psi_{\boldsymbol{h}}^{(q)}\rangle|^2) && (32)\\
&= \mathop{\mathbb{E}}_{\boldsymbol{h}} \big\|\Pi_0^{\perp}\,|\psi_{\boldsymbol{h}}^{(q)}\rangle\,\big\|_2^2\,, && (33)
\end{aligned}$$

where in the final line we defined $\Pi_0^{\perp} \coloneqq I - |\psi_0^{(q)}\rangle\langle\psi_0^{(q)}|$. Specifically, we will show this quantity is at most $o(1)$ so long as $T = o(\sigma d_{\text{eff}}/\theta_{\max}^2)$, where here and throughout we use the shorthand $\theta_{\max} \coloneqq \sigma + \theta_0$.

By our vector-valued, anchored Efron-Stein inequality (Lemma 2.5), we have

$$\mathop{\mathbb{E}}_{\boldsymbol{h}} \big\|\Pi_0^{\perp}|\psi_{\boldsymbol{h}}^{(q)}\rangle\big\|_2^2 - \big\| \mathop{\mathbb{E}}_{\boldsymbol{h}} \Pi_0^{\perp}|\psi_{\boldsymbol{h}}^{(q)}\rangle\big\|_2^2 \leq \sum_{i=1}^{d_{\text{eff}}} \mathop{\mathbb{E}}_{\boldsymbol{h}} \big\|\Pi_0^{\perp}|\psi_{\boldsymbol{h}}^{(q)}\rangle - \Pi_0^{\perp}|\psi_{\boldsymbol{h}^{(i\to 0)}}^{(q)}\rangle\big\|_2^2 \tag{34}$$

where $\boldsymbol{h}^{(i\to 0)} = (\boldsymbol{h}_1, \dots, \boldsymbol{h}_{i-1}, 0, \boldsymbol{h}_{i+1}, \dots, \boldsymbol{h}_{d_{\text{eff}}})$ for each $i \in [d_{\text{eff}}]$. Since $\Pi_0^{\perp}\,|\psi_0^{(q)}\rangle = 0$, we have

$$\big\| \mathop{\mathbb{E}}_{\boldsymbol{h}} \Pi_0^{\perp}\,|\psi_{\boldsymbol{h}}^{(q)}\rangle\,\big\|_2^2 \leq \Pr[\boldsymbol{h} \neq 0] \mathop{\mathbb{E}}_{\boldsymbol{h}} \big\|\Pi_0^{\perp}\,|\psi_{\boldsymbol{h}}^{(q)}\rangle\,\big\|_2^2 \leq [1 - (1-\mathsf{p})^{d_{\text{eff}}}] \mathop{\mathbb{E}}_{\boldsymbol{h}} \big\|\Pi_0^{\perp}\,|\psi_{\boldsymbol{h}}^{(q)}\rangle\,\big\|_2^2\,, \tag{35}$$

which, along with the fact that $\mathsf{p} = \Theta(1/d_{\text{eff}})$, implies

$$\mathop{\mathbb{E}}_{\boldsymbol{h}} \big\|\Pi_0^{\perp}\,|\psi_{\boldsymbol{h}}^{(q)}\rangle\,\big\|_2^2 \leq c_0 \sum_{i=1}^{d_{\text{eff}}} \mathop{\mathbb{E}}_{\boldsymbol{h}} \big\|\Pi_0^{\perp}\,|\psi_{\boldsymbol{h}}^{(q)}\rangle - \Pi_0^{\perp}\,|\psi_{\boldsymbol{h}^{(i\to 0)}}^{(q)}\rangle\,\big\|_2^2 \tag{36}$$

for some universal constant $c_0 > 0$.

Next, we introduce notation to describe a sum-over-paths decomposition for the state after q queries when $\boldsymbol{h} = h$. First, fix an index $i \in [d_{\text{eff}}]$ which determines our notion of a "path"; namely, we coarse-grain the labels for the standard basis states, keeping track only of whether the path has value "i" or "not i" at each step of the algorithm. Precisely, given $k \in \{0, 1, \ldots, q\}$, $z \in \{0,1\}^k$, and $h \in \mathbb{R}^{d_{\text{eff}}}$, we define the subnormalized state

$$|\varphi_z^{(i)}(h)\rangle \coloneqq V_k(e^{-iHt_k} P_{z_k}^{(i)} \otimes I) V_{k-1}(e^{-iHt_{k-1}} P_{z_{k-1}}^{(i)} \otimes I) \ldots V_1(e^{-iHt_1} P_{z_1}^{(i)} \otimes I) V_0 |\psi\rangle, \tag{37}$$

where $H = \operatorname{diag}(h)$, $P_1^{(i)} = \Pi_i$, and $P_0^{(i)} = I - \Pi_i$. (So, in the language above, 1 indicates "i" and 0 indicates not "i".) Note that $|\varphi_z^{(i)}(h)\rangle$ involves only the first k steps of the algorithm; for $k = 0$ the only path is the empty string $\varnothing$, and $|\varphi_\varnothing^{(i)}(h)\rangle = V_0 |\psi\rangle$. With this notation, we can insert resolutions of identity to conclude

$$|\psi_h^{(k)}\rangle = \sum_{z \in \{0,1\}^k} |\varphi_z^{(i)}(h)\rangle \qquad \text{for all } k \in \{0, 1, \ldots, q\}. \tag{38}$$

One may also readily verify

$$|\varphi_z^{(i)}(h)\rangle = e^{-ih_i \mathtt{t}_z} |\varphi_z^{(i)}(h^{(i\to 0)})\rangle \tag{39}$$

for all $z \in \{0,1\}^k$, where $h^{(i\to 0)} = (h_1, \ldots, h_{i-1}, 0, h_{i+1}, \ldots, h_{d_{\text{eff}}})$.

With this notation, the ith term in the sum in Eq. (36) is at most

$$\mathop{\mathbb{E}}_{\boldsymbol{h}} \big\| |\psi_{\boldsymbol{h}}^{(q)}\rangle - |\psi_{\boldsymbol{h}^{(i\to 0)}}^{(q)}\rangle \big\|_2^2 = \mathop{\mathbb{E}}_{\boldsymbol{h}} \Big\| \sum_{z \in \{0,1\}^q} (e^{-i\boldsymbol{h}_i \mathtt{t}_z} - 1) |\varphi_z^{(i)}(\boldsymbol{h}^{(i\to 0)})\rangle \Big\|_2^2 \tag{40}$$

$$= \sum_{z,z' \in \{0,1\}^q} \mathop{\mathbb{E}}_{\boldsymbol{h}_i} (e^{i\boldsymbol{h}_i \mathtt{t}_{z'}} - 1)(e^{-i\boldsymbol{h}_i \mathtt{t}_z} - 1) \mathop{\mathbb{E}}_{\boldsymbol{h}^{(i\to 0)}} \langle \varphi_{z'}^{(i)}(\boldsymbol{h}^{(i\to 0)}) | \varphi_z^{(i)}(\boldsymbol{h}^{(i\to 0)})\rangle \tag{41}$$

$$= \mathsf{p} \sum_{z,z' \in \{0,1\}^q} K(\mathtt{t}_{z'}, \mathtt{t}_z) \mathop{\mathbb{E}}_{\boldsymbol{h}^{(i\to 0)}} \langle \varphi_{z'}^{(i)}(\boldsymbol{h}^{(i\to 0)}) | \varphi_z^{(i)}(\boldsymbol{h}^{(i\to 0)})\rangle \tag{42}$$

$$\le \pi \mathsf{p} \cdot \frac{\theta_{\max}^2}{\sigma} \sum_{z,z' \in \{0,1\}^q} \min(\mathtt{t}_z, \mathtt{t}_{z'}) \mathop{\mathbb{E}}_{\boldsymbol{h}^{(i\to 0)}} \langle \varphi_{z'}^{(i)}(\boldsymbol{h}^{(i\to 0)}) | \varphi_z^{(i)}(\boldsymbol{h}^{(i\to 0)})\rangle \tag{43}$$

$$= \frac{\pi \mathsf{p}}{1 - \mathsf{p}} \cdot \frac{\theta_{\max}^2}{\sigma} \mathop{\mathbb{E}}_{\boldsymbol{h}} \mathbf{1}[\boldsymbol{h}_i = 0] \sum_{z,z' \in \{0,1\}^q} \min(\mathtt{t}_z, \mathtt{t}_{z'}) \langle \varphi_{z'}^{(i)}(\boldsymbol{h}) | \varphi_z^{(i)}(\boldsymbol{h})\rangle \tag{44}$$

where the first line follows from Eq. (39), the third line uses the definition of $K(\cdot,\cdot)$ from Lemma 2.6, the fourth line follows from Lemma 2.6, and in the final line we used $1 = \Pr[\boldsymbol{h}_i = 0]/(1 - \mathsf{p})$ as well as $h^{(i\to 0)} = h$ if $h_i = 0$.

We now introduce the shorthand $|\boldsymbol{\varphi}_z^{(i)}\rangle \coloneqq |\varphi_z^{(i)}(\boldsymbol{h})\rangle$ for each $z \in \{0,1\}^k$ and $k \in \{0, 1, \ldots, q\}$, and for each such k consider the quantity

$$S_k(\boldsymbol{h}) \coloneqq \sum_{z,z' \in \{0,1\}^k} \min(\mathtt{t}_z, \mathtt{t}_{z'}) \langle \boldsymbol{\varphi}_{z'}^{(i)} | \boldsymbol{\varphi}_z^{(i)}\rangle. \tag{45}$$

Then we can express the inequality given in Eq. (44) and the preceding lines as

$$\mathop{\mathbb{E}}_{\boldsymbol{h}} \big\| |\psi_{\boldsymbol{h}}^{(q)}\rangle - |\psi_{\boldsymbol{h}^{(i\to 0)}}^{(q)}\rangle \big\|_2^2 \le \frac{\pi \mathsf{p}}{1 - \mathsf{p}} \cdot \frac{\theta_{\max}^2}{\sigma} \mathop{\mathbb{E}}_{\boldsymbol{h}} \mathbf{1}[\boldsymbol{h}_i = 0] S_q(\boldsymbol{h}) \tag{46}$$

We proceed to bound the right-hand side of the above inequality by writing $S_q(\boldsymbol{h})$ in a more transparent form.

Let $1 \le k \le q$, and write $z = (y, b)$ and $z' = (y', b')$ for some $y, y' \in \{0,1\}^{k-1}$ and $b, b' \in \{0,1\}$. By definition, $|\boldsymbol{\varphi}_z^{(i)}\rangle = V_k(e^{-i\boldsymbol{H}t_k} P_b^{(i)} \otimes I)\,|\boldsymbol{\varphi}_y^{(i)}\rangle$ with $\boldsymbol{H} = \mathrm{diag}(\boldsymbol{h})$ (up to shift by identity), and $V_k(e^{-i\boldsymbol{H}t_k} \otimes I)$ is unitary, so

$$\langle \boldsymbol{\varphi}_{z'}^{(i)} | \boldsymbol{\varphi}_z^{(i)} \rangle = \langle \boldsymbol{\varphi}_{y'}^{(i)} | P_b^{(i)} | \boldsymbol{\varphi}_y^{(i)} \rangle \delta_{b,b'}. \tag{47}$$

Combining this with $\mathsf{t}_{(y,b)} = \mathsf{t}_y + b\,t_k$, we have

$$\begin{aligned} S_k(\boldsymbol{h}) &= \sum_{y,y' \in \{0,1\}^{k-1}} \Big[\min(\mathsf{t}_y, \mathsf{t}_{y'}) \langle \boldsymbol{\varphi}_{y'}^{(i)} | P_0^{(i)} | \boldsymbol{\varphi}_y^{(i)} \rangle + \big(\min(\mathsf{t}_y, \mathsf{t}_{y'}) + t_k \big) \langle \boldsymbol{\varphi}_{y'}^{(i)} | P_1^{(i)} | \boldsymbol{\varphi}_y^{(i)} \rangle \Big] && (48) \\ &= \sum_{y,y' \in \{0,1\}^{k-1}} \min(\mathsf{t}_y, \mathsf{t}_{y'}) \langle \boldsymbol{\varphi}_{y'}^{(i)} | \boldsymbol{\varphi}_y^{(i)} \rangle + t_k \sum_{y,y' \in \{0,1\}^{k-1}} \langle \boldsymbol{\varphi}_{y'}^{(i)} | \Pi_i | \boldsymbol{\varphi}_y^{(i)} \rangle && (49) \\ &= S_{k-1}(\boldsymbol{h}) + t_k \langle \psi_{\boldsymbol{h}}^{(k-1)} | \Pi_i | \psi_{\boldsymbol{h}}^{(k-1)} \rangle, && (50) \end{aligned}$$

where the last line uses the definition of $S_{k-1}(\boldsymbol{h})$ and Eq. (38) with $k-1$ in place of k. Since $\mathsf{t}_\varnothing = 0$, we have $S_0(\boldsymbol{h}) = 0$, so by induction on k we arrive at

$$S_q(\boldsymbol{h}) = \sum_{j=1}^{q} t_j \langle \psi_{\boldsymbol{h}}^{(j-1)} | \Pi_i | \psi_{\boldsymbol{h}}^{(j-1)} \rangle. \tag{51}$$

Hence, Eq. (46) is equivalent to

$$\mathop{\mathbb{E}}_{\boldsymbol{h}} \big\| \, |\psi_{\boldsymbol{h}}^{(q)}\rangle - |\psi_{\boldsymbol{h}^{(i\to 0)}}^{(q)}\rangle \, \big\|_2^2 \le \frac{\pi \mathsf{p}}{1-\mathsf{p}} \cdot \frac{\theta_{\max}^2}{\sigma} \mathop{\mathbb{E}}_{\boldsymbol{h}} \sum_{j=1}^{q} t_j \langle \psi_{\boldsymbol{h}}^{(j-1)} | \Pi_i | \psi_{\boldsymbol{h}}^{(j-1)} \rangle \cdot \mathbf{1}[\boldsymbol{h}_i = 0] \tag{52}$$

which in turn implies the right-hand side of Eq. (36) is at most

$$\begin{aligned} &\frac{c_0 \pi \mathsf{p}}{1-\mathsf{p}} \cdot \frac{\theta_{\max}^2}{\sigma} \sum_{i=1}^{d_{\mathrm{eff}}} \mathop{\mathbb{E}}_{\boldsymbol{h}} \sum_{j=1}^{q} t_j \langle \psi_{\boldsymbol{h}}^{(j-1)} | \Pi_i | \psi_{\boldsymbol{h}}^{(j-1)} \rangle \cdot \mathbf{1}[\boldsymbol{h}_i = 0] && (53) \\ &= \frac{c_0 \pi \mathsf{p}}{1-\mathsf{p}} \cdot \frac{\theta_{\max}^2}{\sigma} \mathop{\mathbb{E}}_{\boldsymbol{h}} \sum_{j=1}^{q} t_j \langle \psi_{\boldsymbol{h}}^{(j-1)} | Q_{\boldsymbol{h}} | \psi_{\boldsymbol{h}}^{(j-1)} \rangle && (54) \\ &\le \frac{c_0 \pi \mathsf{p}}{1-\mathsf{p}} \cdot \frac{\theta_{\max}^2}{\sigma} \mathop{\mathbb{E}}_{\boldsymbol{h}} \sum_{j=1}^{q} t_j \| |\psi_{\boldsymbol{h}}^{(j-1)}\rangle \|_2^2 && (55) \\ &= \frac{c_0 \pi \mathsf{p}}{1-\mathsf{p}} \cdot \frac{\theta_{\max}^2}{\sigma} \cdot \sum_{j=1}^{q} t_j && (56) \end{aligned}$$

where in the second line we defined the random projection operator $Q_{\boldsymbol{h}} \coloneqq \sum_{i=1}^{d_{\mathrm{eff}}} \mathbf{1}[\boldsymbol{h}_i = 0] \Pi_i$. Noting $d_{\mathrm{eff}} \ge 2$, $\mathsf{p} = \Theta(1/d_{\mathrm{eff}})$, and $T = \sum_j t_j$, we have

$$\mathrm{d_{tr}}\big(|\psi_0^{(q)}\rangle\langle\psi_0^{(q)}| \,, \mathop{\mathbb{E}}_{\boldsymbol{h}} |\psi_{\boldsymbol{h}}^{(q)}\rangle\langle\psi_{\boldsymbol{h}}^{(q)}| \big)^2 \le c_1 \cdot \frac{\theta_{\max}^2 T}{\sigma d_{\mathrm{eff}}} \tag{57}$$

for some universal constant $c_1 > 0$, which completes the proof. □

2.3 Beyond average-case error

In this section, we prove our lower bounds without time reversal extend to *any* normalized Schatten p-norm $\|\cdot\|_p/d^{1/p}$, with $p \in [2,\infty]$. Note that $p=2$ corresponds to normalized Frobenius norm, while $p=\infty$ gives the operator norm, so this family of norms interpolates smoothly between average- and worst-case error. Formally, we define Hamiltonian certification in normalized Schatten p-norm as follows:

Problem 2.7 (Hamiltonian certification in normalized Schatten norms)**.** Let $\varepsilon \in (0,1)$ and let $p \in [2,\infty]$. Let $H_0 \in \mathbb{C}^{d\times d}$ be a known target Hamiltonian such that $\|H_0\| \le 1$ and $\mathrm{tr}(H_0) = 0$. Given black-box access to time evolution under an unknown Hamiltonian $H \in \mathbb{C}^{d\times d}$ such that $\|H\| \le 1$ and $\mathrm{tr}(H) = 0$, perform the following:

- (completeness) if $H = H_0$, accept with probability at least 99/100;
- (soundness) if $\frac{1}{d^{1/p}}\|H - H_0\|_p \ge \varepsilon$, accept with probability at most 1/100.

We extend our lower bounds to all normalized Schatten norms:

Theorem 2.8. *Let $p \in [2,\infty]$. Any quantum algorithm without time reversal for Hamiltonian certification in normalized Schatten p-norm (Problem 2.7) requires a total evolution time*

$$T_{\to} = \Omega\left(\min\left\{\frac{1}{\varepsilon^p}, \frac{d^{1-1/p}}{\varepsilon}\right\}\right). \tag{58}$$

As in the case of normalized Frobenius norm, the proof of Theorem 2.8 follows via reduction from the distinguishing task in Problem 2.1, for a slightly modified choice of parameters. The reduction is captured in the following lemma:

Lemma 2.9. *Let $d \ge 100$ and $\varepsilon_0 \in [0, 1/10)$. Let $p \in [2,\infty]$. Consider the distinguishing task in Problem 2.1 with $d_{\mathrm{eff}} = \min\{d, \lceil 1/\varepsilon_0^p\rceil\}$, $\mathsf{p} = 50/d_{\mathrm{eff}}$, $\sigma = \varepsilon_0 {d_{\mathrm{eff}}}^{1/p}/4$, and $\theta_0 = 0$, where we have black-box access to time evolution under the Hamiltonian $\boldsymbol{H} \in \mathbb{C}^{d\times d}$. With these choices, Problem 2.1 can be solved using a single call to a successful algorithm for Hamiltonian certification in normalized Schatten p-norm (Problem 2.7), taking d and $\varepsilon = \varepsilon_0/40$ as the dimension and accuracy parameters, respectively.*

Note that Lemma 2.9 is identical to Item 1 in Lemma 2.3, with d_{eff} and σ generalized by changing $\min\{d, \lceil 1/\varepsilon_0^2\rceil\}$ to $\min\{d, \lceil 1/\varepsilon_0^p\rceil\}$ and $\varepsilon_0\sqrt{d_{\mathrm{eff}}}/4$ to $\varepsilon_0 {d_{\mathrm{eff}}}^{1/p}/4$, respectively. Accordingly, the proof is identical with these substitutions.

3 Upper bounds with time reversal

In Sections 2.2 and 2.3, we have proven lower bounds for quantum algorithms without time reversal. Now, we demonstrate the power of having time reversal for each of the problems considered so far. Specifically, in Section 3.1, we prove tight bounds for Hamiltonian certification in all normalized Schatten-p norms $p \in [2,\infty]$, while in Section 3.2 we prove that, for search with coherent errors, a quadratic quantum advantage can be restored. As it is already well-known that $O(1/\varepsilon)$ queries suffice for performing amplitude estimation to precision ε, we omit further discussion of this task; of course, there is a separation here as well.

3.1 Hamiltonian certification with time reversal

We begin by proving upper bounds for Hamiltonian certification with time reversal, giving an improvement over Theorem 2.8 for all choices of normalized Schatten p-norm with $p \in [2, \infty]$ to demonstrate that time reversal provides an advantage across average- to worst-case measures of error:

Theorem 3.1. *Let $p \in [2, \infty]$. There is a quantum algorithm with time reversal for Hamiltonian certification in normalized Schatten p-norm (Problem 2.7) which takes total evolution time*

$$T_{\leftrightarrow} = O\left(\min\left\{\frac{1}{\varepsilon^{p/2}}, \frac{d^{1/2-1/p}}{\varepsilon}\right\}\right). \tag{59}$$

We first observe that it suffices to consider the case that the target Hamiltonian is $H_0 = 0$, since we can simulate $\exp(-i(H - H_0)t)$ to arbitrarily small error via Trotterization, without any overhead in evolution time. Indeed, for r Trotter steps, we have [Chi+21]

$$\left\| \left(e^{iH_0 t/r} e^{-iHt/r}\right)^r - e^{-i(H-H_0)t} \right\| \leq \frac{t^2}{2r} \|[H_0, H]\| \leq \frac{t^2}{r}. \tag{60}$$

Increasing r makes the simulation arbitrarily accurate without increasing the total evolution time t under H.[7] We therefore restrict to certifying the zero Hamiltonian in what follows, a task which we call *zero testing*.

Our zero testing algorithm is based on repeated Bell measurements, whose success probability is coherently amplified using time reversal. Specifically, we introduce a d-dimensional ancillary Hilbert space and prepare the Bell state $|\Phi\rangle = \sum_{i=1}^{d} |ii\rangle / \sqrt{d}$, then apply the unitary $e^{-iH/2} \otimes I$. Suppose we perform a two-outcome Bell measurement $\{\Pi_\Phi, I - \Pi_\Phi\}$, where $\Pi_\Phi = |\Phi\rangle\langle\Phi|$. If $H = 0$, the measurement always returns Π_Φ (accept). If $H \neq 0$, however, then with probability scaling as $\|H\|_2^2/d$ we measure $I - \Pi_\Phi$ (reject). We can use time reversal to coherently amplify this success probability [BHMT02]. We give a complete description of the approach in Algorithm 1. To prove its correctness, we first describe how to use time reversal to amplify the rejection probability of a single Bell measurement.

Lemma 3.2 (Bell measurement amplification)**.** *Let $H \in \mathbb{C}^{d \times d}$ with $\mathrm{tr}(H) = 0$ and $\|H\| \leq 1$. Define $\Pi_\Phi = |\Phi\rangle\langle\Phi|$, $R = 2\Pi_\Phi - I$, and $W = e^{-iH/2} \otimes I$. Draw $\boldsymbol{k} \sim \mathrm{Unif}(\{0, \ldots, M-1\})$ for integer $M \geq 1$ and perform a Bell measurement $\{\Pi_\Phi, I - \Pi_\Phi\}$ of the state $(WRW^\dagger R)^{\boldsymbol{k}} W |\Phi\rangle$. If $M\|H\|_2/\sqrt{d} \geq 2$, the probability $p_{\mathrm{rej}}(M)$ of measuring $I - \Pi_\Phi$ is at least $1/4$.*

Proof. Let $\boldsymbol{X}, \boldsymbol{Y}$ be independent uniformly random eigenvalues of H. Prior to amplification, the state $W|\Phi\rangle$ has Bell measurement rejection probability $p_{\mathrm{rej}}(1) = \mathbb{E}(1 - \cos((\boldsymbol{X} - \boldsymbol{Y})/2))$. For $|z| \leq 1$, we have $z^2/4 \leq 1 - \cos(z) \leq z^2/2$; since $|\boldsymbol{X} - \boldsymbol{Y}|/2 \leq 1$, we have

$$\frac{\|H\|_2^2}{8d} \leq p_{\mathrm{rej}}(1) \leq \frac{\|H\|_2^2}{4d}. \tag{61}$$

We may write $W|\Phi\rangle = \cos(\theta)|\psi_\Phi\rangle + \sin(\theta)|\psi_{\Phi^\perp}\rangle$ for $\Pi_\Phi|\psi_\Phi\rangle = |\psi_\Phi\rangle$ and $\Pi_\Phi|\psi_{\Phi^\perp}\rangle = 0$. Then $p_{\mathrm{rej}}(1) = \sin^2(\theta)$; since $p_{\mathrm{rej}}(1) \leq \|H\|_2^2/(4d) \leq 1/4$ we may assume without loss of generality that

[7] Of course, even though the total evolution time is unchanged, this approach has poor gate complexity. [Fla+26] demonstrates that this is not fundamental, providing an algorithm for Hamiltonian certification in normalized Frobenius norm which only requires product state preparation, forward time evolution under H, and single-qubit measurements, at the expense of a $\log(d)$ overhead in evolution time. Because our primary motivation is to understand time evolution, we do not investigate whether these techniques extend to other normalized Schatten norms.

Algorithm 1: Zero testing with time reversal

Input : Black box access to $U(t) = \exp(-iHt)$ for $t \in \mathbb{R}$, $\operatorname{tr}(H) = 0$, $\|H\| \le 1$;
Parameters $\varepsilon \in (0,1)$, $p \in [2,\infty]$.

Set $M \leftarrow \lceil 2\min\{\varepsilon^{-p/2}, d^{1/2-1/p}/\varepsilon\} \rceil$;
Set $W \leftarrow e^{-iH/2} \otimes I$, $R \leftarrow 2\Pi_\Phi - I$ for $\Pi_\Phi = |\Phi\rangle\langle\Phi|$;
for $N = 1, \ldots, 20$ **do**
  Sample $\boldsymbol{k} \sim \mathrm{Unif}(\{0, \ldots, M-1\})$;
  Apply W to the Bell state $|\Phi\rangle$;
  Apply $WRW^\dagger R$ $\boldsymbol{k}$ times;
  Measure $\{\Pi_\Phi, I - \Pi_\Phi\}$;
  if $I - \Pi_\Phi$ **then**
    return reject;
  end
end
return accept.

$\theta \in (0, \pi/6]$. $WRW^\dagger R$ is a rotation in the two-dimensional subspace spanned by $|\psi_\Phi\rangle$ and $|\psi_{\Phi^\perp}\rangle$ by angle 2θ. Therefore, the rejection probability after k steps is $\sin^2((2k+1)\theta)$. Averaging over uniform $\boldsymbol{k}$ we obtain

$$p_{\mathrm{rej}}(M) = \frac{1}{M}\sum_{k=0}^{M-1} \sin^2((2k+1)\theta) = \frac{1}{2} - \frac{\sin(4M\theta)}{4M\sin(2\theta)}. \tag{62}$$

Finally, $M\sin(2\theta) = 2M\sqrt{p_{\mathrm{rej}}(1)(1-p_{\mathrm{rej}}(1))} \ge M\sqrt{2p_{\mathrm{rej}}(1)} \ge M\|H\|_2/(2\sqrt{d}) \ge 1$, where the first inequality is from $p_{\mathrm{rej}}(1) \le 1/4$, the second is Eq. (61), and the third is by assumption. □

Proof of Theorem 3.1. We prove that Algorithm 1 solves Hamiltonian zero testing with probability greater than 99/100; Theorem 3.1 follows by our general Trotterization argument. If $H = 0$, then Algorithm 1 accepts with certainty, so assume $\|H\|_p/d^{1/p} \ge \varepsilon$.

For $p \in [2,\infty)$, we have $\|H\|_p \le \|H\|_2$ and, because $\|H\| \le 1$, $\|H\|_p^p \le \|H\|_2^2$. Hence, we have

$$\frac{\sqrt{d}}{\|H\|_2} \le \min\left\{\frac{\sqrt{d}}{\|H\|_p^{p/2}}, \frac{\sqrt{d}}{\|H\|_p}\right\} \le \min\left\{\frac{1}{\varepsilon^{p/2}}, \frac{d^{1/2-1/p}}{\varepsilon}\right\}. \tag{63}$$

This inequality also holds for $p = \infty$, since $\|H\|_2 \ge \|H\| \ge \varepsilon$. By Lemma 3.2, each Bell measurement rejects with probability at least $1/4$; therefore, the overall failure probability is at most $(3/4)^{20} < 1/100$, as desired. Finally, the algorithm takes $O(M)$ total evolution time, as desired. □

For completeness, we show that the upper bounds in Theorem 3.1 are tight:

Theorem 3.3. *Let $p \in [2,\infty]$. Any quantum algorithm with time reversal for Hamiltonian certification in normalized Schatten p-norm (Problem 2.7) requires a total evolution time*

$$T_{\leftrightarrow} = \Omega\left(\min\left\{\frac{1}{\varepsilon^{p/2}}, \frac{d^{1/2-1/p}}{\varepsilon}\right\}\right). \tag{64}$$

To prove Theorem 3.3, we let the target Hamiltonian H_0 be a diagonal Hamiltonian with an equal number of ± 1 eigenvalues. We construct $\boldsymbol{H}$ by randomly selecting ℓ pairs of ± 1 eigenvalues and

perturbing them by $\pm\eta$. We choose ℓ and η such that $\|\boldsymbol{H} - H_0\|_p/d^{1/p} \geq \varepsilon$ with certainty. Finally, we use a hybrid argument to bound the trace distance between the state of a tester using random $\boldsymbol{H}$ and the state of a tester using H_0 to prove the lower bound.

Proof. Assume d is even for simplicity; the case that d is odd can be handled similarly. Let $m = d/2$ and let H_0 be a fixed diagonal Hamiltonian with an equal number of $+1$ and -1 eigenvalues, which we group in pairs and identify with $[m]$. Note that $\mathrm{tr}(H_0) = 0$ and $\|H_0\| \leq 1$, by construction. For $\ell \in [m]$ and $\eta \in (0, 2]$, choose a random ℓ-element subset $\boldsymbol{S} \subseteq [m]$ and define $H_{\boldsymbol{S}}$ as the Hamiltonian with eigenvalue pairs $(1, -1)$ in $\boldsymbol{S}$ replaced by $(1-\eta, -1+\eta)$. $H_{\boldsymbol{S}}$ continues to satisfy $\mathrm{tr}(H_{\boldsymbol{S}}) = 0$ and $\|H_{\boldsymbol{S}}\| \leq 1$, by construction. Note that $\|H_0 - H_{\boldsymbol{S}}\|_p/d^{1/p} = \eta(\ell/m)^{1/p}$ with certainty. Furthermore,

$$\mathop{\mathbb{E}}_{\boldsymbol{S}}(H_0 - H_{\boldsymbol{S}})^2 = \frac{\eta^2\ell}{m} I. \tag{65}$$

We now consider a general quantum algorithm for Hamiltonian certification with time reversal. As explained in Section 2, we can write the final state of the algorithm with unknown Hamiltonian H as

$$|\psi_H\rangle = V_q(e^{-iHt_q} \otimes I)V_{q-1}(e^{-iHt_{q-1}} \otimes I) \cdots V_1(e^{-iHt_1} \otimes I)V_0 |\psi\rangle , \tag{66}$$

where the time durations $t_1, \ldots, t_q$ can be positive or negative and the unitaries V_j are fixed by the algorithm. The trace distance between the final states of the algorithm for $H = H_0$ and $H = H_{\boldsymbol{S}}$ is

$$\mathrm{d_{tr}}\big(|\psi_{H_0}\rangle\langle\psi_{H_0}|, \mathop{\mathbb{E}}_{\boldsymbol{S}} |\psi_{H_{\boldsymbol{S}}}\rangle\langle\psi_{H_{\boldsymbol{S}}}|\big) \leq \mathop{\mathbb{E}}_{\boldsymbol{S}} \sum_{k=1}^{q} \big\|(e^{-iH_0t_k} \otimes I) |\psi_k\rangle - (e^{-iH_{\boldsymbol{S}}t_k} \otimes I) |\psi_k\rangle \big\|_2, \tag{67}$$

by the triangle inequality and the relationship between trace distance and Euclidean distance for pure states, where the states $|\psi_k\rangle$ are independent of the random subset $\boldsymbol{S}$. Since H_0 and $H_{\boldsymbol{S}}$ commute, we have

$$\begin{aligned}
\mathop{\mathbb{E}}_{\boldsymbol{S}} \sum_{k=1}^{q} \big\|(e^{-iH_0t_k} \otimes I) |\psi_k\rangle - (e^{-iH_{\boldsymbol{S}}t_k} \otimes I) |\psi_k\rangle \big\|_2 &= \mathop{\mathbb{E}}_{\boldsymbol{S}} \sum_{k=1}^{q} \big(2\big(1 - \mathrm{Re}\big\{\langle\psi_k|e^{i(H_0-H_{\boldsymbol{S}})t_k}|\psi_k\rangle\big\}\big)\big)^{\frac{1}{2}} && (68)\\
&\leq \mathop{\mathbb{E}}_{\boldsymbol{S}} \sum_{k=1}^{q} \big(\langle\psi_k|(H_0 - H_{\boldsymbol{S}})^2 t_k^2|\psi_k\rangle\big)^{\frac{1}{2}} && (69)\\
&\leq \sum_{k=1}^{q} \big(\langle\psi_k| \mathop{\mathbb{E}}_{\boldsymbol{S}}(H_0 - H_{\boldsymbol{S}})^2 t_k^2|\psi_k\rangle\big)^{\frac{1}{2}} && (70)\\
&= \eta\sqrt{\frac{\ell}{m}} \sum_{k=1}^{q} |t_k|, && (71)
\end{aligned}$$

where Eq. (69) follows from $\cos(z) \geq 1 - z^2/2$, Eq. (70) is Jensen's inequality, and the final line uses Eq. (65). Choose $\eta = 2\varepsilon(m/\ell)^{1/p}$ and let $\ell = 1 + \lfloor m\varepsilon^p \rfloor$. First, we have $\|H_0 - H_S\|_p/d^{1/p} = 2\varepsilon > \varepsilon$, so by Eq. (71) any algorithm for Hamiltonian certification must satisfy $T = \Omega(\sqrt{m/\ell}/\eta)$, where $T = \sum_{k=1}^{q} |t_k|$ denotes the total absolute time. Since $\ell \leq 2\max\{1, m\varepsilon^p\}$, we have

$$T = \Omega\left(\frac{1}{\varepsilon}\left(\frac{m}{\ell}\right)^{1/2-1/p}\right) = \Omega\left(\min\left\{\frac{1}{\varepsilon^{p/2}}, \frac{d^{1/2-1/p}}{\varepsilon}\right\}\right), \tag{72}$$

as desired. □

3.2 Search with coherent errors and inverses

We now give an algorithm to solve search with coherent errors, Problem 1.7, with the usual quadratic quantum speedup, given access to both forward and inverse queries. This algorithm makes use of an ancilla qubit and the quantum signal processing (QSP) toolkit [LYC16; LC19; GSLW19; MRTC21].

Our goal throughout the remainder of this section will be to construct an η-accurate approximation to the standard reflection operator $O_f = \sum_{x=1}^{d} (-1)^{f(x)} |x\rangle\langle x|$. Specifically, we wish to implement a unitary operator $\widetilde{R}$ acting on $\mathbb{C}^2 \otimes \mathbb{C}^d$ such that $\|\widetilde{R} - I \otimes O_f\| \leq \eta$ using as few queries to O_f^θ and $(O_f^\theta)^\dagger$ as possible. We may then solve the search problem by running the algorithm of Ref. [BBHT98] for search with an unknown number of marked items, using $\widetilde{R}$ in place of the ideal oracle O_f.

Recall that this algorithm repeatedly applies a randomly chosen number of Grover iterations, drawn from a range that grows exponentially from one round to the next, then measures and checks whether the outcome is marked. When $M \geq 1$, it finds a marked element using $O(\sqrt{d/M})$ queries in expectation. Stopping after a budget of $O(\sqrt{d})$ queries and outputting NONE if no marked element has been found yields, by Markov's inequality, an algorithm that solves Problem 1.7 with the ideal oracle O_f for every $M = \Theta(1)$ (including $M = 0$) using at most $q = O(\sqrt{d})$ queries. Taking $\eta = O(1/q)$ with a sufficiently small constant therefore gives the desired result. In summary, this shows:

Proposition 3.4. *There exists an algorithm which solves search with coherent errors, Problem 1.7, for any fixed $0 \leq \Delta < \pi/2$ and $M = \Theta(1)$ using $O\big(\sqrt{d}\log(d)\big)$ queries to O_f^θ and $(O_f^\theta)^\dagger$.*

Proof. Recall that the oracle with coherent errors, which we call the inexact oracle, is defined as:

$$O_f^\theta = \sum_{x=1}^{d} e^{i\theta_x f(x)} |x\rangle\langle x| \tag{73}$$

for some unknown $f\colon [d] \to \{0,1\}$ and $\theta_x \in [\pi - \Delta, \pi + \Delta]$. First, we observe that we can without loss of generality assume controlled versions of the inexact oracles O_f^θ and $(O_f^\theta)^\dagger$, controlled on an ancilla qubit. This is by a standard trick originally due to Kitaev [Kit95] and also appearing in [SMM09]. For an unmarked $x_0 \in [d]$[8], we run the circuit in Figure 1a, which one may verify has the desired action

$$|0\rangle |x\rangle \mapsto |0\rangle |x\rangle \tag{74}$$

$$|1\rangle |x\rangle \mapsto e^{i\theta_x f(x)} |1\rangle |x\rangle . \tag{75}$$

ignoring the register prepared in the state $|x_0\rangle$. We can implement controlled access to $(O_f^\theta)^\dagger$ in a similar manner.

Using the controlled version of the unitaries O_f^θ and $(O_f^\theta)^\dagger$, we implement the unitary given by the circuit in Figure 1b, which is the qubitized signal processing operator

$$W_X \coloneqq \sum_{x=1}^{d} e^{-i\varphi_x X} \otimes |x\rangle\langle x| , \quad \text{where } \varphi_x \coloneqq \theta_x f(x) \text{ for all } x \in [d]. \tag{76}$$

[8] In more detail, fix an $x_0 \in [d]$ such that $f(x_0) = 0$. Note that this is without loss of generality, since we can always pick x_0 at random; this fails with arbitrarily small probability for sufficiently large d. Overall, this step adds just a constant number of queries to the overall cost.



(a) (b)

Figure 1: (a) Circuit implementing controlled-O_f^θ operation. The first register is an ancilla qubit. (b) Circuit implementing the signal processing operator W_X. Here, H is the Hadamard operation.

Here and below, let X, Z denote the Pauli-X and Pauli-Z operators, respectively. Now, for any $\vec{\phi} \in [0, 2\pi)^{D+1}$ let

$$U_{\vec{\phi}} \coloneqq (e^{i\phi_0 Z} \otimes I) \prod_{k=1}^{D} W_X (e^{i\phi_k Z} \otimes I). \tag{77}$$

For $a \in [-1, 1]$, let $B(a) \coloneqq e^{i\phi_0 Z} \prod_{k=1}^{D} W(a) e^{i\phi_k Z}$, where $W(a)$ is the signal rotation operator in [MRTC21, Eq. (1)]. Then

$$U_{\vec{\phi}} = \sum_{x=1}^{d} Z^{b_x} B(a_x) Z^{b_x} \otimes |x\rangle\langle x| \,, \tag{78}$$

where $a_x \coloneqq \cos\varphi_x$, and $b_x \coloneqq 1$ if $\sin\varphi_x > 0$ and $b_x \coloneqq 0$ otherwise, since $e^{-i\varphi_x X} = Z^{b_x} W(a_x) Z^{b_x}$ and Z commutes with $e^{i\phi_k Z}$.

By Theorem 10 of [MRTC21] (see also [GSLW19]), for any real polynomial g of degree at most D with parity $D \bmod 2$ such that $|g(a)| \leq 1$ for all $a \in [-1, 1]$, we may choose $\vec{\phi}$ such that $\langle +| B(a) |+\rangle = g(a)$ for all $a \in [-1, 1]$.

Note that $B(a)$ has eigenvalues $e^{\pm i\alpha}$, where $\cos\alpha = \mathrm{Re}\,\langle +| B(a) |+\rangle = g(a)$. We take g to be the standard odd approximation to the sign function given in [MRTC21, Sec. III]: for any $\Delta' > 0$ and $\varepsilon \in (0, \sqrt{2/(e\pi)})$ there is an odd real polynomial g of degree $O(\frac{1}{\Delta'} \log(\frac{1}{\varepsilon}))$ such that $|g(a)| \leq 1$ for all $a \in [-1, 1]$, and $|g(a) - \mathrm{sign}(a)| \leq \varepsilon$ for all $a \in [-1, 1]$ such that $|a| \geq \Delta'/2$. Picking $\Delta' = 2\cos\Delta$, $\varepsilon = \eta^2/2$ and D odd, we have $|g(a_x) - 1| \leq \eta^2/2$ if x is unmarked, and $|g(a_x) + 1| \leq \eta^2/2$ if x is marked, where $D = O(\log(1/\eta)/\cos\Delta)$.

Now setting $\widetilde{R} \coloneqq U_{\vec{\phi}}$ and letting $s_x \coloneqq (-1)^{f(x)}$, we compute

$$\|\widetilde{R} - I \otimes O_f\| = \max_{x \in [d]} \|B(a_x) - s_x I\| = \max_{x \in [d]} \sqrt{2(1 - s_x g(a_x))} \leq \eta \tag{79}$$

by our choice of g. Here, the first equality holds because conjugation by Z^{b_x} preserves the norm. Each use of W_X costs one query to each of O_f^θ and $(O_f^\theta)^\dagger$, so implementing $\widetilde{R}$ costs $2D$ total queries. The truncated algorithm of [BBHT98] described above uses at most $q = O(\sqrt{d})$ queries to O_f, so setting $\eta = O(1/q)$ we can accurately simulate the entire algorithm, using

$$2Dq = O\Big(\sqrt{d} \frac{\log(\sqrt{d})}{\cos\Delta}\Big) = O\left(\sqrt{d}\log(d)\right) \tag{80}$$

such queries, where we made use of the assumption that $0 \leq \Delta < \pi/2$ is some fixed constant. □

4 Upper bounds without time reversal

For Hamiltonian certification in normalized Frobenius norm, our main result Theorem 1.2 shows that one cannot attain better than standard quantum limited scaling without time reversal (in the low-precision regime $\varepsilon \gg 1/\sqrt{d}$). This shows that testers based on Bell measurements [ADG25; KL25; ST25] or state certification with random input states [Fla+26], which achieve $O(1/\varepsilon^2)$ scaling, are optimal in the low-precision regime.

In this section, we extend these results, proving tight upper bounds for Hamiltonian certification in all normalized Schatten p-norms for $p \in [2, \infty]$, and in both the high- and low-precision regimes. Together with our matching lower bounds for all such normalized Schatten norms in Theorem 2.8, this resolves the time complexity of Hamiltonian certification without time reversal from average- to worst-case.

Theorem 4.1. *Let $p \in [2, \infty]$. There is a quantum algorithm without time reversal for Hamiltonian certification in normalized Schatten p-norm (Problem 2.7) which takes total evolution time*

$$T_{\to} = O\left(\min\left\{\frac{1}{\varepsilon^p}, \frac{d^{1-1/p}}{\varepsilon}\right\}\right). \tag{81}$$

By the Trotterization argument in Section 3.1, it suffices to consider $H_0 = 0$. Our algorithm is once again based on Bell sampling. We apply $e^{-iHt} \otimes I$ and perform the Bell measurement $\{\Pi_\Phi, I - \Pi_\Phi\}$ for $\Pi_\Phi = |\Phi\rangle\langle\Phi|$. If $H = 0$, this measurement always returns Π_Φ (accepts). For any H, the measurement returns $I - \Pi_\Phi$ (rejects) with probability $1 - |\operatorname{tr}(e^{-iHt})|^2/d^2$. We randomly choose $0 \le t \le \tau$ to avoid fine-tuned cancellations in the spectrum of H and show that, in general, the rejection probability of the Bell measurement is at least half the fraction of eigenvalue pairs with difference at least $\sim 1/\tau$. Therefore, by choosing longer evolution times τ, we can probe smaller eigenvalue gaps in H. In particular, we show it suffices to take a single choice of $\tau = O(\max\{1/(\varepsilon d^{1/p}), 1\})$ and repeat the Bell measurement $O(\min\{d, 1/\varepsilon^p\})$ times.

A complete description of our zero testing algorithm is given in Algorithm 2. To prove its correctness, we begin by estimating the rejection probability of a single Bell measurement.

Algorithm 2: Zero testing without time reversal

Input : Black box access to $U(t) = \exp(-iHt)$ for $t \ge 0$, $\operatorname{tr}(H) = 0$, $\|H\| \le 1$;
Parameters $\varepsilon \in (0, 1)$, $p \in [2, \infty]$.

Set $B \leftarrow \min\{d, 1/\varepsilon^p\}$, $\tau \leftarrow 1/(\varepsilon B^{1/p})$;
for $N = 1, \ldots, \lceil 20B \rceil$ **do**
  Sample $\boldsymbol{t} \sim \mathrm{Unif}([0, 4\tau])$;
  Apply $e^{-iH\boldsymbol{t}} \otimes I$ to the Bell state $|\Phi\rangle$;
  Measure $\{\Pi_\Phi, I - \Pi_\Phi\}$ for $\Pi_\Phi = |\Phi\rangle\langle\Phi|$;
  if $I - \Pi_\Phi$ **then**
    return reject
  end
end
return accept.

Lemma 4.2 (Bell measurement)**.** *Let $H \in \mathbb{C}^{d\times d}$ with $\operatorname{tr}(H) = 0$ and $\|H\| \le 1$ and let $\tau > 0$. Draw $\boldsymbol{t} \sim \mathrm{Unif}([0, 4\tau])$ and perform a Bell measurement $\{\Pi_\Phi, I - \Pi_\Phi\}$ of the state $(e^{-iH\boldsymbol{t}} \otimes I)|\Phi\rangle$, where*

$\Pi_\Phi = |\Phi\rangle\langle\Phi|$. *The probability* $p_{\mathrm{rej}}(\tau)$ *of measuring* $I - \Pi_\Phi$ *is at least*

$$p_{\mathrm{rej}}(\tau) \geq \frac{1}{2} \Pr[|\boldsymbol{X} - \boldsymbol{Y}| \geq 1/(2\tau)], \tag{82}$$

where $\boldsymbol{X}, \boldsymbol{Y}$ *are independent uniformly random eigenvalues of* H*. Moreover, if* $\|H\| \leq 1/\tau$*, then*

$$p_{\mathrm{rej}}(\tau) \geq (\tau^2/4)\, \mathbb{E}\, \boldsymbol{X}^2. \tag{83}$$

Proof. For a fixed evolution time t, the probability of measuring Π_Φ is

$$\left|\langle\Phi| \left(e^{-iHt} \otimes I\right) |\Phi\rangle\right|^2 = \left|\frac{\mathrm{tr}(e^{-iHt})}{d}\right|^2 = \mathbb{E} \cos((\boldsymbol{X} - \boldsymbol{Y})t). \tag{84}$$

Averaging over $\boldsymbol{t} \sim \mathrm{Unif}([0, 4\tau])$ therefore yields

$$p_{\mathrm{rej}}(\tau) = \mathbb{E} \int_0^1 1 - \cos(4\tau(\boldsymbol{X} - \boldsymbol{Y})u)\ \mathrm{d}u = 1 - \mathbb{E}\, \frac{\sin(4\tau(\boldsymbol{X} - \boldsymbol{Y}))}{4\tau(\boldsymbol{X} - \boldsymbol{Y})}. \tag{85}$$

$1 - \sin(z)/z \geq 0$ for all real z and $1 - \sin(z)/z \geq 1/2$ for $|z| \geq 2$; taking the expectation value of the above implies Eq. (82). Finally, for $|z| \leq 8$, we have $1 - \sin(z)/z \geq z^2/128$; since $\|H\| \leq 1/\tau$ implies $|\boldsymbol{X} - \boldsymbol{Y}| \leq 2/\tau$, we have $p_{\mathrm{rej}}(\tau) \geq (\tau^2/8)\, \mathbb{E}\, |\boldsymbol{X} - \boldsymbol{Y}|^2 = (\tau^2/4)\, \mathbb{E}\, \boldsymbol{X}^2$, where the final step follows because H is traceless. This proves Eq. (83). □

Proof of Theorem 4.1. We prove that Algorithm 2 solves Hamiltonian zero testing (Hamiltonian certification with $H_0 = 0$) with probability greater than 99/100; Theorem 4.1 follows from the Trotterization argument above. If $H = 0$, then Algorithm 2 accepts with certainty, so assume $\|H\|_p / d^{1/p} \geq \varepsilon$. We again let $\boldsymbol{X}, \boldsymbol{Y}$ denote uniformly random eigenvalues of H and let $p_{\mathrm{rej}}(\tau)$ denote the rejection probability of the Bell measurement, as in Lemma 4.2. The probability that the algorithm accepts is $(1 - p_{\mathrm{rej}}(\tau))^N \leq \exp(-N p_{\mathrm{rej}}(\tau))$; we will show that $N p_{\mathrm{rej}}(\tau) \geq 5$, which proves the result.

First, consider the case that $p = \infty$. Then $B = d$ and $\|H\| \geq 1/\tau$. Since H is traceless, it has at least one eigenvalue which is at least distance $1/(2\tau)$ away from at least $d/2$ eigenvalues. Therefore

$$\Pr[|\boldsymbol{X} - \boldsymbol{Y}| \geq 1/(2\tau)] \geq \frac{1}{2d} = \frac{1}{2B}. \tag{86}$$

By Lemma 4.2, we have $p_{\mathrm{rej}}(\tau) \geq 1/(4B)$ and $N p_{\mathrm{rej}}(\tau) \geq 5$, as desired. Next, consider the case that $p \in [2, \infty)$. If $B = d$ and $\|H\| \geq 1/\tau$, then the analysis of the previous case applies. Else, we claim that $\|H\| \leq 1/\tau$; dividing the remaining cases, either $\|H\| \leq 1/\tau$ by assumption, or $B \neq d$, in which case $\tau = 1$ and the claim follows from the assumed bound on the operator norm of H. Hence, by Lemma 4.2, we have

$$p_{\mathrm{rej}}(\tau) \geq \frac{\mathbb{E}\, |\tau \boldsymbol{X}|^2}{4} \geq \frac{\mathbb{E}\, |\tau \boldsymbol{X}|^p}{4} \geq \frac{(\varepsilon\tau)^p}{4} = \frac{1}{4B}, \tag{87}$$

and $N p_{\mathrm{rej}}(\tau) \geq 5$ again, as desired.

Finally, the total evolution time is at most $O(B\tau)$, which upon substituting the expressions for B and τ yields the desired result. □

Acknowledgments

We thank Soonwon Choi, Isaac Chuang, Matthew Ding, Eddie Farhi, Aram Harrow, John Kallaugher, Daniel Liang, Tudor Manole, Seyoon Ragavan, Ewin Tang, and Alexander Zlokapa for helpful discussions. We also thank Francisco Escudero Gutiérrez, Junseo Lee, and Sebastian Zur for sharing their draft [GLZ26] with us to coordinate arXiv posting. RRA was supported by the Simons Foundation (MP-SIP-00001553, AWH) and by the U.S. Department of Energy, Office of Science, National Quantum Information Science Research Centers, Co-design Center for Quantum Advantage (DE-SC0012704). YC was supported by the QuICS Hartree Postdoctoral Fellowship. TG was supported by ERC Starting Grant 101163189 and UKRI Future Leaders Fellowship MR/X023583/1. AL was supported by the Simons Foundation (MP-SIP-00001553, AWH) and the NSF (PHY-2325080).

AI disclosure. All ideas and writing are due to the authors of this work. GPT-6 and Claude Opus 5.5 were used for proofreading the manuscript and suggesting minor edits.

References

[ACGN23] Joran van Apeldoorn, Arjan Cornelissen, András Gilyén, and Giacomo Nannicini. "Quantum tomography using state-preparation unitaries". In: *Proceedings of the 2023 Annual ACM-SIAM Symposium on Discrete Algorithms (SODA)*. Society for Industrial and Applied Mathematics, 2023, pp. 1265–1318. DOI: 10.1137/1.9781611977554.ch47. arXiv: 2207.08800 [quant-ph] (page 1).

[ADG25] Srinivasan Arunachalam, Arkopal Dutt, and Francisco Escudero Gutiérrez. *Testing and Learning Structured Quantum Hamiltonians*. 2025. arXiv: 2411.00082 [quant-ph] (pages 2, 3, 23).

[BBBV97] Charles H. Bennett, Ethan Bernstein, Gilles Brassard, and Umesh V. Vazirani. "Strengths and Weaknesses of Quantum Computing". In: *SIAM Journal on Computing* 26.5 (1997), pp. 1510–1523. DOI: 10.1137/S0097539796300933 (page 6).

[BBHT98] Michel Boyer, Gilles Brassard, Peter Høyer, and Alain Tapp. "Tight Bounds on Quantum Searching". In: *Fortschritte der Physik: Progress of Physics* 46.4-5 (1998), pp. 493–505. DOI: 10.1002/(SICI)1521-3978(199806)46:4/5%3C493::AID-PROP493%3E3.0.CO;2-P (pages 21, 22).

[BCO26] Andreas Bluhm, Matthias C. Caro, and Aadil Oufkir. "Hamiltonian Property Testing". In: *Quantum* 10 (Jan. 2026), p. 1979. DOI: 10.22331/q-2026-01-21-1979 (pages 2, 3, 30).

[Ben73] Charles H. Bennett. "Logical Reversibility of Computation". In: *IBM Journal of Research and Development* 17.6 (1973), pp. 525–532. DOI: 10.1147/rd.176.0525. URL: https://doi.org/10.1147/rd.176.0525 (page 1).

[BHMT02] Gilles Brassard, Peter Høyer, Michele Mosca, and Alain Tapp. "Quantum Amplitude Amplification and Estimation". In: *Quantum Computation and Information* (2002), pp. 53–74. DOI: 10.1090/conm/305/05215 (pages 1, 18).

[Blu+26] Andreas Bluhm, Matthias C. Caro, Francisco Escudero Gutiérrez, Junseo Lee, Aadil Oufkir, Cambyse Rouzé, and Myeongjin Shin. *Certifying and Learning Local Quantum Hamiltonians*. 2026. arXiv: 2603.29809 [quant-ph] (pages 2, 10).

[Bos+25] John Bostanci, Yuval Efron, Tony Metger, Alexander Poremba, Luowen Qian, and Henry Yuen. *Unitary Complexity and the Uhlmann Transformation Problem*. 2025. arXiv: 2306.13073 [quant-ph]. URL: https://arxiv.org/abs/2306.13073 (page 2).

[Bur+19] Jonathan J. Burnett, Andreas Bengtsson, Marco Scigliuzzo, David Niepce, Marina Kudra, Per Delsing, and Jonas Bylander. "Decoherence benchmarking of superconducting qubits". In: *npj Quantum Information* 5.1 (2019). DOI: 10.1038/s41534-019-0168-5. URL: http://dx.doi.org/10.1038/s41534-019-0168-5 (page 10).

[Car26] Joseph Carolan. "Compressed Permutation Oracles". In: *Proceedings of the 58th Annual ACM Symposium on Theory of Computing*. Stoc '26. New York, NY, USA: Association for Computing Machinery, 2026, pp. 150–161. DOI: 10.1145/3798129.3800736 (page 6).

[CBW25] Anirban Chowdhury, Ewout van den Berg, and Pawel Wocjan. *Controlization Schemes Based on Orthogonal Arrays*. 2025. arXiv: 2407.09382 [quant-ph]. URL: https://arxiv.org/abs/2407.09382 (page 9).

[CCHL22] Sitan Chen, Jordan Cotler, Hsin-Yuan Huang, and Jerry Li. "Exponential separations between learning with and without quantum memory". In: *2021 IEEE 62nd Annual Symposium on Foundations of Computer Science (FOCS)*. IEEE. 2022, pp. 574–585. DOI: 10.1109/FOCS52979.2021.00063 (page 1).

[CFHL21] Kai-Min Chung, Serge Fehr, Yu-Hsuan Huang, and Tai-Ning Liao. "On the Compressed-Oracle Technique, and Post-Quantum Security of Proofs of Sequential Work". In: *Advances in Cryptology – EUROCRYPT 2021: 40th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zagreb, Croatia, October 17–21, 2021, Proceedings, Part II*. Berlin, Heidelberg: Springer-Verlag, 2021, pp. 598–629. DOI: 10.1007/978-3-030-77886-6_21 (page 6).

[CGZ24] Sitan Chen, Weiyuan Gong, and Zhihan Zhang. *Adaptivity can help exponentially for shadow tomography*. 2024. arXiv: 2412.19022 [quant-ph]. URL: https://arxiv.org/abs/2412.19022 (page 1).

[Che+23] Sitan Chen, Brice Huang, Jerry Li, Allen Liu, and Mark Sellke. *When Does Adaptivity Help for Quantum State Learning?* 2023. arXiv: 2206.05265 [quant-ph]. URL: https://arxiv.org/abs/2206.05265 (page 1).

[Che+24a] Yu-Ao Chen, Yin Mo, Yingjian Liu, Lei Zhang, and Xin Wang. *Quantum Algorithm for Reversing Unknown Unitary Evolutions*. 2024. arXiv: 2403.04704 [quant-ph]. URL: https://arxiv.org/abs/2403.04704 (page 9).

[Che+24b] Senrui Chen, Changhun Oh, Sisi Zhou, Hsin-Yuan Huang, and Liang Jiang. "Tight Bounds on Pauli Channel Learning without Entanglement". In: *Phys. Rev. Lett.* 132 (18 May 2024), p. 180805. DOI: 10.1103/PhysRevLett.132.180805. URL: https://link.aps.org/doi/10.1103/PhysRevLett.132.180805 (page 1).

[Chi+21] Andrew M. Childs, Yuan Su, Minh C. Tran, Nathan Wiebe, and Shuchen Zhu. "Theory of Trotter Error with Commutator Scaling". In: *Physical Review X* 11.1 (Feb. 2021). DOI: 10.1103/physrevx.11.011020 (page 18).

[CSM23] Jordan Cotler, Thomas Schuster, and Masoud Mohseni. "Information-theoretic hardness of out-of-time-order correlators". In: *Physical Review A* 108 (2023), p. 062608. DOI: 10.1103/PhysRevA.108.062608. arXiv: 2208.02256. URL: https://arxiv.org/abs/2208.02256 (page 2).

[CYZ26] Kean Chen, Nengkun Yu, and Zhicheng Zhang. "Approximation Does Not Help in Quantum Unitary Time-Reversal". In: *Proceedings of the 58th Annual ACM Symposium on Theory of Computing*. STOC '26. Association for Computing Machinery, 2026, pp. 1376–1387. DOI: 10.1145/3798129.3800847. arXiv: 2507.05736 [quant-ph]. URL: https://arxiv.org/abs/2507.05736 (page 9).

[DOS24] Alicja Dutkiewicz, Thomas E. O'Brien, and Thomas Schuster. "The advantage of quantum control in many-body Hamiltonian learning". In: *Quantum* 8 (Nov. 2024), p. 1537. DOI: 10.22331/q-2024-11-26-1537. URL: https://doi.org/10.22331/q-2024-11-26-1537 (page 2).

[FK18] Bill Fefferman and Shelby Kimmel. "Quantum vs. Classical Proofs and Subset Verification". In: *43rd International Symposium on Mathematical Foundations of Computer Science (MFCS 2018)*. Vol. 117. Leibniz International Proceedings in Informatics (LIPIcs). 2018, 22:1–22:23. DOI: 10.4230/LIPIcs.MFCS.2018.22. arXiv: 1510.06750. URL: https://arxiv.org/abs/1510.06750 (page 2).

[Fla+26] Steven T. Flammia, Dmitrii Khitrin, Muzhou Ma, Jamie Sikora, Yu Tong, and Alice Zheng. *Autonomous Hamiltonian Certification and Changepoint Detection*. 2026. arXiv: 2603.26655 [quant-ph] (pages 18, 23).

[Fox+26] Ben Foxman, Alex Lombardi, Fermi Ma, Barak Nehoran, and John Wright. *Quantum Lazy Sampling and Path Recording for Any Group*. 2026. arXiv: 2606.30281 [quant-ph]. URL: https://arxiv.org/abs/2606.30281 (pages 2, 6, 7).

[Gao+26] Minbo Gao, Zhengfeng Ji, Qisheng Wang, Wenjun Yu, and Qi Zhao. "Quantum Hamiltonian Certification". In: *Proceedings of the 2026 Annual ACM-SIAM Symposium on Discrete Algorithms (SODA)*. Society for Industrial and Applied Mathematics, Jan. 2026, pp. 1424–1467. DOI: 10.1137/1.9781611978971.53 (pages 2, 3).

[GLZ26] Francisco Escudero Gutiérrez, Junseo Lee, and Sebastian Zur. *Hamiltonian locality testing and certification do not achieve the Heisenberg limit*. 2026. arXiv: 2610.03205 [quant-ph]. URL: https://arxiv.org/abs/2610.03205 (pages 10, 25).

[Goo25] Google Quantum AI and Collaborators. "Observation of constructive interference at the edge of quantum ergodicity". In: *Nature* 646 (2025), pp. 825–830. DOI: 10.1038/s41586-025-09526-6 (page 1).

[GSLW19] András Gilyén, Yuan Su, Guang Hao Low, and Nathan Wiebe. "Quantum Singular Value Transformation and beyond: Exponential Improvements for Quantum Matrix Arithmetics". In: *Proceedings of the 51st Annual ACM SIGACT Symposium on Theory of Computing*. STOC '19. ACM, June 2019, pp. 193–204. DOI: 10.1145/3313276.3316366 (pages 1, 21, 22).

[HKOT23] Jeongwan Haah, Robin Kothari, Ryan O'Donnell, and Ewin Tang. "Query-Optimal Estimation of Unitary Channels in Diamond Distance". In: *2023 IEEE 64th Annual Symposium on Foundations of Computer Science (FOCS)*. IEEE, Nov. 2023, pp. 363–390. DOI: 10.1109/focs57990.2023.00028 (page 3).

[Høy00] Peter Høyer. "Arbitrary Phases in Quantum Amplitude Amplification". In: *Physical Review A* 62.5 (Oct. 2000), p. 052304. DOI: 10.1103/PhysRevA.62.052304. (Visited on 08/30/2026) (page 5).

[HR14] Aram W. Harrow and David J. Rosenbaum. "Uselessness for an Oracle Model with Internal Randomness". In: *Quantum Information and Computation* 14.7&8 (May 2014), pp. 608–624. DOI: 10.26421/QIC14.7-8-5. (Visited on 08/30/2026) (page 10).

[HTFS23] Hsin-Yuan Huang, Yu Tong, Di Fang, and Yuan Su. "Learning Many-Body Hamiltonians with Heisenberg-Limited Scaling". In: *Physical Review Letters* 130.20 (May 2023). DOI: 10.1103/physrevlett.130.200403 (pages 2, 3).

[Hu+25] Hong-Ye Hu, Muzhou Ma, Weiyuan Gong, Qi Ye, Yu Tong, Steven T. Flammia, and Susanne F. Yelin. "Ansatz-Free Hamiltonian Learning with Heisenberg-Limited Scaling". In: *PRX Quantum* 6.4 (Oct. 2025). DOI: 10.1103/j7b8-pb77. URL: http://dx.doi.org/10.1103/j7b8-pb77 (page 2).

[Hua+22] Hsin-Yuan Huang, Michael Broughton, Jordan Cotler, Sitan Chen, Jerry Li, Masoud Mohseni, Hartmut Neven, Ryan Babbush, Richard Kueng, John Preskill, and Jarrod R. McClean. "Quantum advantage in learning from experiments". In: *Science* 376.6598 (2022), pp. 1182–1186. DOI: 10.1126/science.abn7293. eprint: https://www.science.org/doi/pdf/10.1126/science.abn7293. URL: https://www.science.org/doi/abs/10.1126/science.abn7293 (page 1).

[Hug+22] William J. Huggins, Kianna Wan, Jarrod McClean, Thomas E. O'Brien, Nathan Wiebe, and Ryan Babbush. "Nearly Optimal Quantum Algorithm for Estimating Multiple Expectation Values". In: *Physical Review Letters* 129 (2022), p. 240501. DOI: 10.1103/PhysRevLett.129.240501. arXiv: 2111.09283 [quant-ph] (page 1).

[JZ25] Stacey Jeffery and Sebastian Zur. *The Compressed Oracle Is a Worthy (Multiplicative) Adversary*. Sept. 2025. DOI: 10.48550/arXiv.2509.07876. arXiv: 2509.07876 [quant-ph]. (Visited on 09/30/2026) (page 6).

[Kit95] A. Yu. Kitaev. *Quantum Measurements and the Abelian Stabilizer Problem*. 1995. arXiv: quant-ph/9511026 (page 21).

[KL25] John Kallaugher and Daniel Liang. "Hamiltonian Locality Testing via Trotterized Postselection". In: *20th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC 2025)*. Ed. by Bill Fefferman. Vol. 350. Leibniz International Proceedings in Informatics (LIPIcs). Dagstuhl, Germany: Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2025, 10:1–10:20. DOI: 10.4230/LIPIcs.TQC.2025.10 (pages 2–4, 23).

[Kob+24] Bryce Kobrin, Thomas Schuster, Maxwell Block, Weijie Wu, Bradley Mitchell, Emily Davis, and Norman Y. Yao. *A Universal Protocol for Quantum-Enhanced Sensing via Information Scrambling*. 2024. arXiv: 2411.12794 [quant-ph]. URL: https://arxiv.org/abs/2411.12794 (pages 1, 9).

[LC19] Guang Hao Low and Isaac L. Chuang. "Hamiltonian Simulation by Qubitization". In: *Quantum* 3 (July 2019), p. 163. DOI: 10.22331/q-2019-07-12-163 (page 21).

[Li+23] Zeyang Li, Simone Colombo, Chi Shu, Gustavo Velez, Saúl Pilatowsky-Cameo, Roman Schmied, Soonwon Choi, Mikhail Lukin, Edwin Pedrozo-Peñafiel, and Vladan Vuletić. "Improving metrology with quantum scrambling". In: *Science* 380.6652 (2023), pp. 1381–1384. DOI: 10.1126/science.adg9500. arXiv: 2212.13880 [quant-ph] (pages 1, 9).

[LYC16] Guang Hao Low, Theodore J. Yoder, and Isaac L. Chuang. "Methodology of Resonant Equiangular Composite Quantum Gates". In: *Physical Review X* 6.4 (Dec. 2016), p. 041067. DOI: 10.1103/PhysRevX.6.041067. (Visited on 10/01/2026) (page 21).

[LZ19] Qipeng Liu and Mark Zhandry. "On Finding Quantum Multi-Collisions". In: *Advances in Cryptology – EUROCRYPT 2019: 38th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Darmstadt, Germany, May 19–23, 2019, Proceedings, Part III*. Berlin, Heidelberg: Springer-Verlag, 2019, pp. 189–218. DOI: 10.1007/978-3-030-17659-4_7 (page 6).

[MH25] Fermi Ma and Hsin-Yuan Huang. "How to Construct Random Unitaries". In: *Proceedings of the 57th Annual ACM Symposium on Theory of Computing*. Stoc '25. New York, NY, USA: Association for Computing Machinery, 2025, pp. 806–809. DOI: 10.1145/3717823.3718254 (pages 6, 7).

[MRTC21] John M. Martyn, Zane M. Rossi, Andrew K. Tan, and Isaac L. Chuang. "Grand Unification of Quantum Algorithms". In: *PRX Quantum* 2.4 (Dec. 2021), p. 040203. DOI: 10.1103/PRXQuantum.2.040203. (Visited on 10/01/2026) (pages 21, 22).

[ODo21] Ryan O'Donnell. *Analysis of Boolean Functions*. 2021. arXiv: 2105.10386 [cs.DM] (pages 8, 12, 31).

[OKSM24] Tatsuki Odake, Hlér Kristjánsson, Akihito Soeda, and Mio Murao. "Higher-order quantum transformations of Hamiltonian dynamics". In: *Physical Review Research* 6 (2024), p. L012063. DOI: 10.1103/PhysRevResearch.6.L012063. arXiv: 2303.09788 [quant-ph] (page 9).

[OYM25] Tatsuki Odake, Satoshi Yoshida, and Mio Murao. "Analytical Lower Bound on Query Complexity for Transformations of Unknown Unitary Operations". In: *Physical Review Letters* 135 (2025), p. 230603. DOI: 10.1103/drp2-rzzw. arXiv: 2405.07625 [quant-ph]. URL: https://arxiv.org/abs/2405.07625 (page 9).

[Ros23] Ansis Rosmanis. *Quantum Search with Noisy Oracle*. Sept. 2023. DOI: 10.48550/arXiv.2309.14944. arXiv: 2309.14944 [quant-ph]. (Visited on 08/30/2026) (page 10).

[RS08] Oded Regev and Liron Schiff. "Impossibility of a Quantum Speed-Up with a Faulty Oracle". In: *Automata, Languages and Programming*. Ed. by Luca Aceto, Ivan Damgård, Leslie Ann Goldberg, Magnús M. Halldórsson, Anna Ingólfsdóttir, and Igor Walukiewicz. Berlin, Heidelberg: Springer, 2008, pp. 773–781. DOI: 10.1007/978-3-540-70575-8_63 (page 10).

[SBSH16] Brian Swingle, Gregory Bentsen, Monika Schleier-Smith, and Patrick Hayden. "Measuring the scrambling of quantum information". In: *Physical Review A* 94 (2016), p. 040302. DOI: 10.1103/PhysRevA.94.040302. arXiv: 1602.06271 [quant-ph] (page 1).

[SC26] Ruohan Shen and Soonwon Choi. *Oracle Distillation*. 2026. arXiv: 2609.31596 [quant-ph]. URL: https://arxiv.org/abs/2609.31596 (page 10).

[Sha+24] Adam L. Shaw, Zhuo Chen, Joonhee Choi, Daniel K. Mark, Pascal Scholl, Ran Finkelstein, Andreas Elben, Soonwon Choi, and Manuel Endres. "Benchmarking highly entangled states on a 60-atom analogue quantum simulator". In: *Nature* 628.8006 (Mar. 2024), pp. 71–77. DOI: 10.1038/s41586-024-07173-x. URL: http://dx.doi.org/10.1038/s41586-024-07173-x (page 10).

[SHH25] Thomas Schuster, Jonas Haferkamp, and Hsin-Yuan Huang. "Random unitaries in extremely low depth". In: *Science* 389.6755 (2025), eadv8590. DOI: 10.1126/science.adv8590. arXiv: 2407.07754. URL: https://arxiv.org/abs/2407.07754 (page 2).

[SLO26] Myeongjin Shin, Junseo Lee, and Changhun Oh. *Heisenberg-limited Hamiltonian learning without short-time control*. 2026. arXiv: 2604.27838 [quant-ph]. URL: https://arxiv.org/abs/2604.27838 (page 2).

[SMM09] L Sheridan, D Maslov, and M Mosca. "Approximating fractional time quantum evolution". In: *Journal of Physics A: Mathematical and Theoretical* 42.18 (Apr. 2009), p. 185302. DOI: 10.1088/1751-8113/42/18/185302. URL: http://dx.doi.org/10.1088/1751-8113/42/18/185302 (page 21).

[ST25] Savar D. Sinha and Yu Tong. *Improved Hamiltonian Learning and Sparsity Testing through Bell Sampling*. 2025. arXiv: 2509.07937 [quant-ph] (pages 2, 3, 23).

[ST26] Myeongjin Shin and Yu Tong. *Hamiltonian Learning and Certification via Eigenphase Engineering*. 2026. arXiv: 2609.26596 [quant-ph]. URL: https://arxiv.org/abs/2609.26596 (pages 2, 10).

[SY23] Adrian She and Henry Yuen. "Unitary Property Testing Lower Bounds by Polynomials". In: *14th Innovations in Theoretical Computer Science Conference (ITCS 2023)*. Vol. 251. Leibniz International Proceedings in Informatics (LIPIcs). 2023, 96:1–96:17. DOI: 10.4230/LIPIcs.ITCS.2023.96. arXiv: 2210.05885. URL: https://arxiv.org/abs/2210.05885 (page 2).

[Tem14] Kristan Temme. "Runtime of Unstructured Search with a Faulty Hamiltonian Oracle". In: *Physical Review A* 90.2 (Aug. 2014), p. 022310. DOI: 10.1103/PhysRevA.90.022310. (Visited on 08/30/2026) (page 10).

[TLTC23] Andrew K Tan, Yuan Liu, Minh C Tran, and Isaac L Chuang. "Error correction of quantum algorithms: Arbitrarily accurate recovery of noisy quantum signal processing". In: *arXiv preprint arXiv:2301.08542* (2023) (page 10).

[TW26] Ewin Tang and John Wright. *Amplitude Amplification and Estimation Require Inverses*. 2026. arXiv: 2507.23787 [quant-ph] (pages 1, 2, 4, 6, 7).

[WRJB02] Pawel Wocjan, Martin Rötteler, Dominik Janzing, and Thomas Beth. "Simulating Hamiltonians in quantum networks: Efficient schemes and complexity bounds". In: *Physical Review A* 65 (2002), p. 042309. DOI: 10.1103/PhysRevA.65.042309. arXiv: quant-ph/0109088 (page 9).

[YCZ20] Bin Yan, Lukasz Cincio, and Wojciech H. Zurek. "Information Scrambling and Loschmidt Echo". In: *Physical Review Letters* 124.16 (Apr. 2020). DOI: 10.1103/physrevlett.124.160603. URL: http://dx.doi.org/10.1103/PhysRevLett.124.160603 (page 1).

[Zha19] Mark Zhandry. "How to Record Quantum Queries, and Applications to Quantum Indifferentiability". In: *Advances in Cryptology – CRYPTO 2019: 39th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 18–22, 2019, Proceedings, Part II*. Berlin, Heidelberg: Springer-Verlag, 2019, pp. 239–268. DOI: 10.1007/978-3-030-26951-7_9 (pages 2, 6).

A Operational meaning of normalized Frobenius and operator norms

In this section, we briefly review the natural operational interpretations of the normalized Frobenius norm and operator norms for Hamiltonians in the context of learning and testing, see also [BCO26, Appendix A]. Suppose we are given two traceless Hamiltonians $H_0, H_1 \in \mathbb{C}^{d\times d}$, and our goal is to

distinguish them by evolving forwards in time. If we let $\Delta \coloneqq H_0 - H_1$ and $|\psi\rangle \in \mathbb{C}^d$ be some fixed initial state, then one may verify

$$\mathfrak{R} \coloneqq \lim_{t\to 0} \frac{\sqrt{1-F^2}}{|t|} = \sqrt{\mathrm{Var}_{|\psi\rangle}[\Delta]}, \tag{88}$$

where $F = |\langle\psi|e^{iH_0 t}e^{-iH_1 t}|\psi\rangle|$ is the fidelity of the time-evolved states after time t, and $\mathrm{Var}_{|\psi\rangle}[\Delta] \coloneqq \langle\psi|\Delta^2|\psi\rangle - \langle\psi|\Delta|\psi\rangle^2$ is the variance of the operator Δ with respect to the state $|\psi\rangle$. Note that the quantity $\sqrt{1-F^2}$ in the numerator is just the trace distance. So, Eq. (88) says that the standard deviation $(\mathrm{Var}_{|\psi\rangle}[\Delta])^{1/2}$ is precisely the rate of change of the trace distance between the time-evolved states at time $t = 0$.

Normalized Frobenius norm. If we pick $|\boldsymbol{\psi}\rangle$ uniformly at random with respect to the Haar measure, then we can ask for the expectation value of the random variable $\mathfrak{R}$. This is tightly characterized by the normalized Frobenius norm:

$$\frac{1}{\sqrt{2}}\frac{\sqrt{d}\|\Delta\|_2}{d+1} \;\le\; \mathbb{E}_{|\boldsymbol{\psi}\rangle}\mathfrak{R} \;\le\; \frac{\|\Delta\|_2}{\sqrt{d+1}}, \tag{89}$$

where the upper bound follows from Jensen's inequality and $\mathbb{E}_{|\boldsymbol{\psi}\rangle}\mathrm{Var}_{|\boldsymbol{\psi}\rangle}[\Delta] = \|\Delta\|_2^2/(d+1)$, and the lower bound follows from Hölder's inequality to get $\mathbb{E}\boldsymbol{X} \le (\mathbb{E}\sqrt{\boldsymbol{X}})^{2/3}(\mathbb{E}\boldsymbol{X}^2)^{1/3}$, for $\boldsymbol{X} = \mathrm{Var}_{|\boldsymbol{\psi}\rangle}[\Delta]$. Hence, the normalized Frobenius norm of the difference Hamiltonian Δ characterizes the average rate of change of distinguishability.

Operator norm. If we pick a state $|\psi\rangle$ that maximizes $\mathfrak{R}$, then we have

$$\frac{\|\Delta\|}{2} \;\le\; \max_{|\psi\rangle}\; \mathfrak{R} \;\le\; \|\Delta\|. \tag{90}$$

The upper bound is straightforward, and the lower bound follows by choosing $|\psi\rangle$ to be an equal superposition of the eigenvectors corresponding to the largest and smallest eigenvalues of Δ. Hence, the operator norm of the difference Hamiltonian Δ characterizes the worst-case rate of change of distinguishability.

B Proof of anchored Efron-Stein inequality

In this section, we prove the anchored Efron-Stein inequality, Lemma 2.5. We begin by recalling the *Efron-Stein decomposition*, a generalization of the Fourier transform to general product domains. While many expositions on the Efron-Stein decomposition exist (see, e.g., [ODo21, Chapter 8]), here we present a self-contained proof of the Efron-Stein decomposition and several of its key properties, which will be used extensively in our proof of the anchored Efron-Stein inequality in Lemma 2.5.

We present the Efron-Stein decomposition for functions $f : \mathbb{R}^n \to \mathbb{C}^m$, though it exists in more general settings. For a probability measure μ on $\mathbb{R}$, we can define a natural inner product on the space of functions from $\mathbb{R}^n$ to $\mathbb{C}^m$ by $\langle f, g\rangle = \mathbb{E}_{\boldsymbol{x}\sim\mu^{\otimes n}}\langle f(\boldsymbol{x}), g(\boldsymbol{x})\rangle$, where $\langle f(\boldsymbol{x}), g(\boldsymbol{x})\rangle$ denotes the Euclidean inner product between $f(\boldsymbol{x})$ and $g(\boldsymbol{x})$. The Efron-Stein decomposition is a particular orthogonal decomposition with respect to this inner product; it has several useful properties, which we present below:

Lemma B.1 (Efron-Stein decomposition)**.** *Let $f : \mathbb{R}^n \to \mathbb{C}^m$ be a function and let μ be a probability measure on $\mathbb{R}$. There exists a decomposition*

$$f = \sum_{S \subseteq [n]} f_S \tag{91}$$

of f into functions $f_S : \mathbb{R}^n \to \mathbb{C}^m$ which satisfies the following properties:

1. *$f_S(x)$ depends only on the coordinates x_i of x such that $i \in S$.*
2. *$f_\varnothing$ is a constant function, equal to $\mathbb{E}_{\boldsymbol{x} \sim \mu^{\otimes n}} f(\boldsymbol{x})$.*
3. *For $S \neq S'$, f_S and $f_{S'}$ are orthogonal.*
4. *For S', S such that $S \not\subseteq S'$, if $g : \mathbb{R}^n \to \mathbb{C}^m$ depends only on the coordinates in S', then g and f_S are orthogonal.*

Proof. We explicitly construct a decomposition satisfying all the desired properties. We begin by defining several operators on the space of functions from $\mathbb{R}^n$ to $\mathbb{C}^m$ which will be used to define this decomposition. For $i \in [n]$, let E_i denote the operator which averages the i-th coordinate of the input over the distribution μ. Let $L_i = I - E_i$, where I denotes the identity operator. Note that all the E_i (and therefore all the L_i) are projectors, because a function no longer depends on the i-th coordinate of the input after averaging once. Further, all the E_i and $L_{i'}$ are mutually commuting, because the order in which x_i and $x_{i'}$ are averaged over does not matter. Therefore, for any $S \subseteq [n]$, we can unambiguously define the projector

$$\Pi_S = \prod_{i \in S} L_i \prod_{i' \notin S} E_{i'}. \tag{92}$$

Note that Π_S and $\Pi_{S'}$ are orthogonal for any $S \neq S'$, since $E_i L_i = 0$ for all $i \in [n]$. We claim that $\sum_{S \subseteq [n]} \Pi_S = I$. To see this, let $1_S \in \{0,1\}^n$ denote the vector with i-th coordinate $1_{S,i} = 1$ if and only if $i \in S$. Then we have

$$\sum_{S \subseteq [n]} \Pi_S = \sum_{1_S \in \{0,1\}^n} \prod_{i=1}^n (1_{S,i} I + (-1)^{1_{S,i}} E_i) \tag{93}$$

$$= \prod_{i=1}^n \sum_{1_{S,i} \in \{0,1\}} (1_{S,i} I + (-1)^{1_{S,i}} E_i) \tag{94}$$

$$= I. \tag{95}$$

Defining $f_S = \Pi_S f$, it follows that $f = \sum_{S \subseteq [n]} f_S$, as desired. Property 1 holds because f_S is averaged over all coordinates $i' \notin S$ of the input. Property 2 holds by construction, since $\Pi_\varnothing$ averages over all coordinates of the input. Property 3 holds because Π_S and $\Pi_{S'}$ are orthogonal projectors for $S \neq S'$. Finally, to prove Property 4, let $i \in S \setminus S'$. Then $g = E_i g$, so $E_i L_i = 0$ implies that g and f_S are orthogonal. □

We now utilize the Efron-Stein decomposition to prove Lemma 2.5.

Proof of Lemma 2.5. Let $f = \sum_{S \subseteq [n]} f_S$ denote the Efron-Stein decomposition of f. By Property 3, we have

$$\mathop{\mathbb{E}}_{\boldsymbol{x} \sim \mu^{\otimes n}} \left\| f(\boldsymbol{x}) \right\|_2^2 = \sum_{S \subseteq [n]} \mathop{\mathbb{E}}_{\boldsymbol{x} \sim \mu^{\otimes n}} \left\| f_S(\boldsymbol{x}) \right\|_2^2 \tag{96}$$

$$= \mathop{\mathbb{E}}_{\boldsymbol{x}\sim\mu^{\otimes n}} \left\|f_\varnothing(\boldsymbol{x})\right\|_2^2 + \sum_{S\neq\varnothing} \mathop{\mathbb{E}}_{\boldsymbol{x}\sim\mu^{\otimes n}} \left\|f_S(\boldsymbol{x})\right\|_2^2 \tag{97}$$

$$= \left\| \mathop{\mathbb{E}}_{\boldsymbol{x}\sim\mu^{\otimes n}} f(\boldsymbol{x})\right\|_2^2 + \sum_{S\neq\varnothing} \mathop{\mathbb{E}}_{\boldsymbol{x}\sim\mu^{\otimes n}} \left\|f_S(\boldsymbol{x})\right\|_2^2, \tag{98}$$

where in the final line, we have used Property 2. It remains to show that $\sum_{S\neq\varnothing} \mathbb{E}_{\boldsymbol{x}\sim\mu^{\otimes n}} \left\|f_S(\boldsymbol{x})\right\|_2^2$ is at most the right-hand side of Eq. (19). We first have that

$$\sum_{S\neq\varnothing} \mathop{\mathbb{E}}_{\boldsymbol{x}\sim\mu^{\otimes n}} \left\|f_S(\boldsymbol{x})\right\|_2^2 \leq \sum_{S\subseteq[n]} |S| \mathop{\mathbb{E}}_{\boldsymbol{x}\sim\mu^{\otimes n}} \left\|f_S(\boldsymbol{x})\right\|_2^2 \tag{99}$$

$$= \sum_{i=1}^n \sum_{S\ni i} \mathop{\mathbb{E}}_{\boldsymbol{x}\sim\mu^{\otimes n}} \left\|f_S(\boldsymbol{x})\right\|_2^2 \tag{100}$$

$$\leq \sum_{i=1}^n \sum_{S\ni i} \mathop{\mathbb{E}}_{\boldsymbol{x}\sim\mu^{\otimes n}} \left\|f_S(\boldsymbol{x})\right\|_2^2 + \mathop{\mathbb{E}}_{\boldsymbol{x}\sim\mu^{\otimes n}} \left\|f_S(\boldsymbol{x}^{(i\to 0)})\right\|_2^2. \tag{101}$$

For $i \in [n]$, define Z_i as the operator which sets the i-th coordinate of a function's input to zero, so that $Z_i f(x) = f(x^{(i\to 0)})$. Then the right-hand side of Eq. (19) is $\sum_{i=1}^n \mathbb{E}_{\boldsymbol{x}\sim\mu^{\otimes n}} \left\|f(\boldsymbol{x}) - Z_i f(\boldsymbol{x})\right\|_2^2$. Using the Efron-Stein decomposition of f, we have

$$f - Z_i f = \sum_{S\subseteq[n]} f_S - Z_i f_S = \sum_{S\ni i} f_S - Z_i f_S, \tag{102}$$

where we have used Property 1, which implies that $Z_i f_S = f_S$ for $i \notin S$. We claim that all other terms in this decomposition are orthogonal. First, for $S \neq S'$, f_S and $f_{S'}$ are orthogonal by Property 3. Second, for any S, S' which both contain i, f_S and $Z_i f_{S'}$ are orthogonal by Property 4, since $S \not\subseteq S' \setminus \{i\}$. Finally, for any $S \neq S'$ which both contain i, $Z_i f_S$ and $Z_i f_{S'}$ are again orthogonal by Property 4, since either $S \setminus \{i\} \not\subseteq S' \setminus \{i\}$ or vice versa. Thus,

$$\sum_{i=1}^n \mathop{\mathbb{E}}_{\boldsymbol{x}\sim\mu^{\otimes n}} \left\|f(\boldsymbol{x}) - Z_i f(\boldsymbol{x})\right\|_2^2 = \sum_{i=1}^n \sum_{S\ni i} \mathop{\mathbb{E}}_{\boldsymbol{x}\sim\mu^{\otimes n}} \left\|f_S(\boldsymbol{x})\right\|_2^2 + \mathop{\mathbb{E}}_{\boldsymbol{x}\sim\mu^{\otimes n}} \left\|Z_i f_S(\boldsymbol{x})\right\|_2^2, \tag{103}$$

which equals Eq. (101), completing the proof. □

C Proof of reductions in Lemmas 2.3 and 2.4

In this section, we prove each of the reductions appearing in Lemmas 2.3 and 2.4, in order. Recall the setting in Problem 2.1, where we are given a random Hamiltonian $\boldsymbol{H}$ which is equal to zero (null) given $\boldsymbol{b} = 0$ and equal to $\boldsymbol{H}_1 - \mathrm{tr}(\boldsymbol{H}_1)I/d$ (alternative) if $\boldsymbol{b} = 1$. (See Problem 2.1 for the full details.)

C.1 Hamiltonian certification

Here, we prove the first reduction, Item 1 in Lemma 2.3. The claim is a straightforward consequence of:

Lemma C.1 (Alternative is far from zero). *Let $\varepsilon_0 \in (0, 1/10]$ and consider the setting in Problem 2.1. Choose*[9] *parameters as in Lemma 2.3; namely, $d_{\text{eff}} = \min\{d, \lceil 1/\varepsilon_0^2 \rceil\}$, $\mathsf{p} = 50/d_{\text{eff}}$, $\sigma = \varepsilon_0\sqrt{d_{\text{eff}}}/4$, and $\theta_0 = 0$. Conditioned on $\boldsymbol{b} = 1$ we have $\frac{1}{\sqrt{d}}\|\boldsymbol{H}\|_2 \geq \varepsilon_0/16$ with probability at least $4/5$.*

[9] One may verify that this is a valid choice of parameters in Problem 2.1 for every such ε_0 and $d \geq 100$ since $100 \leq d_{\text{eff}} \leq d$ and $0 \leq \sigma < 1/2$ both hold.

Proof. Condition on $\boldsymbol{b} = 1$. We will prove that, with probability at least $4/5$, the Hamiltonian $\boldsymbol{H}$ has some pair of eigenvalues separated by at least σ. Suppose this is true; then $\boldsymbol{H}$ has at least one eigenvalue with absolute value at least $\sigma/2$. Since the eigenvalues of $\boldsymbol{H}$ come in blocks of rank $\lfloor d/d_{\text{eff}} \rfloor$, $\boldsymbol{H}$ in fact must have at least $\lfloor d/d_{\text{eff}} \rfloor \geq d/(2d_{\text{eff}})$ eigenvalues of this magnitude. The normalized Frobenius norm of $\boldsymbol{H}$ is therefore

$$\frac{1}{\sqrt{d}}\|\boldsymbol{H}\|_2 \geq \frac{1}{\sqrt{d}}\left(\left(\frac{\sigma}{2}\right)^2 \frac{d}{2d_{\text{eff}}}\right)^{1/2} = \frac{\sigma}{\sqrt{8d_{\text{eff}}}} \geq \frac{\varepsilon_0}{16}, \tag{104}$$

as desired.

We now prove that $\boldsymbol{H}$ has at least one pair of eigenvalues separated by at least σ with probability at least $4/5$. It suffices to prove the claim for $\boldsymbol{H}_1$, since the eigenvalue gaps of $\boldsymbol{H}$ and $\boldsymbol{H}_1$ are the same. For every $j \in [d_{\text{eff}}]$, we have that $\Pr[\boldsymbol{h}_j \geq \sigma/2] = \Pr[\boldsymbol{h}_j \leq -\sigma/2] = \mathsf{p}/4$. By union bound, the probability that either $\boldsymbol{h}_j \geq -\sigma/2$ for every $j \in [d_{\text{eff}}]$ or $\boldsymbol{h}_j \leq \sigma/2$ for every $j \in [d_{\text{eff}}]$ is at most $2(1-\mathsf{p}/4)^{d_{\text{eff}}} \leq 2e^{-25/2} < 1/5$. □

C.2 Hamiltonian locality testing

The proof of Item 2 in Lemma 2.3 is a straightforward consequence of the following lemma.

Lemma C.2 (Alternative is far from k-local)**.** *Let $k \geq 0$ be a fixed integer, let $r_0(k) \coloneqq 4k + 16$, let $\varepsilon_0 \in (0, 2^{-r_0(k)/2}]$, and consider the setting in Problem 2.1. Suppose the system comprises n qubits for some integer $n \geq r_0(k)$, so that $d = 2^n$. Let $r = \min\{n, \lceil \log_2(1/\varepsilon_0^2) \rceil\}$, and note that $r \geq r_0(k)$ by the assumptions on n and ε_0. Choose parameters as in Lemma 2.3; namely, $d_{\text{eff}} = 2^r$, $\mathsf{p} = 50/2^r$, $\sigma = \varepsilon_0 2^{r/2-2}$, and $\theta_0 = 0$. Conditioned on $\boldsymbol{b} = 1$, we have $\boldsymbol{H}$ is $\varepsilon_0/10$-far in normalized Frobenius norm from every k-local Hamiltonian with probability at least $4/5$.*

Proof. To verify the claim about the distance from the set of k-local Hamiltonians, first note that[10]

$$\boldsymbol{H}_1 = \sum_{x \in \{0,1\}^n} \boldsymbol{h}_{j(x)} |x\rangle\langle x| \tag{105}$$

$$= \sum_{x \in \{0,1\}^n} \boldsymbol{h}_{j(x)} \left(\frac{1}{2^n} \sum_{y \in \{0,1\}^n} (-1)^{y \cdot x} \sigma_Z(y) \right) \tag{106}$$

$$= \sum_{y \in \{0,1\}^n} \hat{\boldsymbol{h}}_y \sigma_Z(y) \tag{107}$$

where $j(x) \in [d_{\text{eff}}]$ is the integer representation of the first r bits of x for each $x \in \{0,1\}^n$, $\sigma_Z(y) \coloneqq \prod_{j \in [n]} Z_j^{y_j}$ for Z_j the Pauli-Z operator on the jth qubit, and

$$\hat{\boldsymbol{h}}_y \coloneqq \frac{1}{2^n} \sum_{x \in \{0,1\}^n} (-1)^{x \cdot y} \boldsymbol{h}_{j(x)} \quad \text{for every } y \in \{0,1\}^n. \tag{108}$$

Hence, conditioned on $\boldsymbol{b} = 1$ we have $\boldsymbol{H} = \sum_{y \in \{0,1\}^n \setminus \{0^n\}} \hat{\boldsymbol{h}}_y \sigma_Z(y)$ and therefore the square of the distance to the closest k-local Hamiltonian in normalized Frobenius norm is equal to

$$\Delta^2 \coloneqq \frac{1}{d} \left\| \sum_{y \in \{0,1\}^n \,:\, |y| \geq k+1} \hat{\boldsymbol{h}}_y \sigma_Z(y) \right\|_2^2 = \sum_{y \in \{0,1\}^n \,:\, |y| \geq k+1} \hat{\boldsymbol{h}}_y^2. \tag{109}$$

[10] Here, we pick diagonal projectors in a suitable manner based on the ordering of the computational basis states on n qubits.

Next, using the fact that $j(x)$ depends only on the first r bits, one may verify that $\hat{\boldsymbol{h}}_y = 0$ unless the final $n-r$ bits of y are equal to zero, in which case we have $y = (y', 0^{n-r})$ for some $y' \in \{0,1\}^r$ and

$$\hat{\boldsymbol{h}}_{(y',0^{n-r})} = \frac{1}{2^r} \sum_{x' \in \{0,1\}^r} (-1)^{x' \cdot y'} \boldsymbol{h}_{j(x',0^{n-r})}. \tag{110}$$

We thus abuse notation slightly and write $\hat{\boldsymbol{h}}_{y'} \coloneqq \hat{\boldsymbol{h}}_{(y',0^{n-r})}$ and $\boldsymbol{h}_{x'} \coloneqq \boldsymbol{h}_{j(x',0^{n-r})}$ for any $x', y' \in \{0,1\}^r$, and we may view $\boldsymbol{h}, \hat{\boldsymbol{h}} \in \mathbb{R}^{\{0,1\}^r}$ as random vectors in 2^r dimensions, in the obvious way. With this notation,

$$\Delta^2 = \|\hat{\boldsymbol{h}}\|_2^2 - \|\hat{\boldsymbol{h}}_{\le k}\|_2^2 \tag{111}$$

where $\hat{\boldsymbol{h}}_{\le k} \coloneqq \sum_{y \in \{0,1\}^r \colon |y| \le k} \hat{\boldsymbol{h}}_y |y\rangle$. We will show the first term on the right-hand side is sufficiently large and the second term being subtracted is sufficiently small, with high probability. We begin with the second term, whose expectation is

$$\begin{aligned}
\mathbb{E}\, \|\hat{\boldsymbol{h}}_{\le k}\|_2^2 &= \sum_{\substack{y \in \{0,1\}^r \\ |y| \le k}} \mathbb{E}\, |\hat{\boldsymbol{h}}_y|^2 && (112)\\
&= \frac{1}{2^{2r}} \sum_{\substack{y \in \{0,1\}^r \\ |y| \le k}} \sum_{x,x' \in \{0,1\}^r} (-1)^{y \cdot (x+x')}\, \mathbb{E}\, \boldsymbol{h}_x \boldsymbol{h}_{x'} && (113)\\
&= \frac{N_k(r)}{2^r}\, \mathbb{E}\, \boldsymbol{h}_{0^n}^2 && (114)\\
&= \frac{N_k(r)}{2^r} \cdot \frac{\mathsf{p}\sigma^2}{3}, && (115)
\end{aligned}$$

where $N_k(r) \coloneqq \sum_{j=0}^k \binom{r}{j}$ is the number of $y \in \{0,1\}^r$ with $|y| \le k$. Here, the third line follows from the fact that $\boldsymbol{h}_x$ and $\boldsymbol{h}_{x'}$ are centered and independent for $x \neq x'$. By Markov's inequality, for any $a_0 > 0$ we have

$$\Pr[\|\hat{\boldsymbol{h}}_{\le k}\|_2^2 \ge a_0] \le \frac{N_k(r)}{2^r} \cdot \frac{\mathsf{p}\sigma^2}{3a_0}. \tag{116}$$

Next, consider the first term in Eq. (111),

$$\|\hat{\boldsymbol{h}}\|_2^2 = \frac{1}{2^r} \|\boldsymbol{h}\|_2^2 = \frac{1}{2^r} \sum_{x \in \{0,1\}^r} \boldsymbol{h}_x^2. \tag{117}$$

Set $\boldsymbol{X}_x \coloneqq \boldsymbol{h}_x^2 - \frac{\mathsf{p}\sigma^2}{3}$ for every $x \in \{0,1\}^r$. Then the $\boldsymbol{X}_x$ are iid and centered, with

$$\mathbb{E}\, \boldsymbol{X}_{0^r}^2 = \mathbb{E}\, \boldsymbol{h}_{0^r}^4 - \left(\frac{\mathsf{p}\sigma^2}{3}\right)^2 \le \frac{\mathsf{p}\sigma^4}{5}. \tag{118}$$

Since $\|\hat{\boldsymbol{h}}\|_2^2 - \frac{\mathsf{p}\sigma^2}{3} = \frac{1}{2^r} \sum_x \boldsymbol{X}_x$, Chebyshev's inequality gives, for any $a_1 > 0$,

$$\Pr\left[\|\hat{\boldsymbol{h}}\|_2^2 \le \frac{\mathsf{p}\sigma^2}{3} - a_1\right] \le \frac{1}{2^{2r} a_1^2} \sum_{x \in \{0,1\}^r} \mathbb{E}\, \boldsymbol{X}_x^2 \le \frac{\mathsf{p}\sigma^4}{5 \cdot 2^r a_1^2}. \tag{119}$$

Putting $a_1 = \mathsf{p}\sigma^2/4$, the right-hand side of Eq. (119) is equal to $\frac{16}{5\cdot 2^r \mathsf{p}} = \frac{16}{250} \le \frac{1}{10}$, and putting $a_0 = \mathsf{p}\sigma^2/24$ the right-hand side of Eq. (116) is equal to $8N_k(r)/2^r$. To bound this, let $\boldsymbol{S} \sim \mathrm{Bin}(r, 1/2)$, so that $N_k(r)/2^r = \Pr[\boldsymbol{S} \le k]$. Since $r \ge r_0(k) = 4k + 16$, we have $k \le (r-16)/4$, and hence $r/2 - k \ge r/4 + 4 > 0$. Hoeffding's inequality then gives

$$\frac{N_k(r)}{2^r} = \Pr\left[\boldsymbol{S} \le \frac{r}{2} - \left(\frac{r}{2} - k\right)\right] \tag{120}$$

$$\le \exp\left(-\frac{2(r/2-k)^2}{r}\right) \tag{121}$$

$$\le \exp\left(-\frac{2(r/4+4)^2}{r}\right) \tag{122}$$

$$= \exp\left(-\frac{r}{8} - 4 - \frac{32}{r}\right) \tag{123}$$

$$\le e^{-8}, \tag{124}$$

where the last step uses $\frac{r}{8} + \frac{32}{r} \ge 4$ (AM–GM). Therefore

$$\frac{8N_k(r)}{2^r} \le 8e^{-8} \le \frac{1}{16}. \tag{125}$$

Thus, except with probability at most $\frac{1}{10} + \frac{1}{16} \le \frac{1}{5}$ we have

$$\Delta^2 \ge \frac{\mathsf{p}\sigma^2}{3} - \frac{\mathsf{p}\sigma^2}{4} - \frac{\mathsf{p}\sigma^2}{24} = \frac{\mathsf{p}\sigma^2}{24} = \frac{25\varepsilon_0^2}{192} \ge \frac{\varepsilon_0^2}{100}. \tag{126}$$

This completes the proof. □

C.3 Amplitude estimation

In this section, we prove the reduction to amplitude estimation, which is Item 3 of Lemma 2.3. We first observe a lower bound on the transition probability after time-evolving some fixed initial state. Here, we let $\mathrm{Var}_{|\psi\rangle}[H] \coloneqq \langle\psi|H^2|\psi\rangle - \langle\psi|H|\psi\rangle^2$ be the variance of an observable H with respect to the state $|\psi\rangle$.

Lemma C.3. *Let $H \in \mathbb{C}^{d\times d}$ be a traceless Hamiltonian such that $\|H\| \le 1$. It holds that*

$$|\langle\psi|e^{-i\pi H/2}|\psi\rangle|^2 \le 1 - \mathrm{Var}_{|\psi\rangle}[H] \tag{127}$$

for any state $|\psi\rangle \in \mathbb{C}^d$.

Proof. Let $\{|j\rangle\}_{j=1}^d$ be an orthonormal eigenbasis of H such that $H = \sum_{j=1}^d E_j\,|j\rangle\langle j|$ for some real $-1 \le E_j \le 1$. We have

$$|\langle\psi|e^{-i\pi H/2}|\psi\rangle|^2 = \sum_{j,k=1}^d p_j p_k e^{-i\pi(E_j-E_k)/2} = \sum_{j,k=1}^d p_j p_k \cos(\pi(E_j-E_k)/2)\,, \tag{128}$$

where $p_j \coloneqq |\langle j|\psi\rangle|^2$ for each $j \in [d]$. The right-hand side of the above is at most

$$\sum_{j,k=1}^d p_j p_k \cos(\pi(E_j-E_k)/2) \le \sum_{j,k=1}^d p_j p_k (1 - (E_j-E_k)^2/2) \tag{129}$$

$$= 1 - \sum_j p_j E_j^2 + \Big(\sum_j p_j E_j\Big)^2 \tag{130}$$

$$= 1 - \langle\psi|H^2|\psi\rangle + \langle\psi|H|\psi\rangle^2 \tag{131}$$

$$= 1 - \mathrm{Var}_\psi[H]\,, \tag{132}$$

where we made use of the inequality $\cos(\pi x/2) \le 1 - x^2/2$ for all $x \in [-2, 2]$, and the second line follows from $\sum_j p_j = 1$. □

This proves the reduction, since taking $|\psi\rangle = |s\rangle \coloneqq \frac{1}{\sqrt{d}} \sum_{j=1}^d |j\rangle$ in the above we have

$$\mathrm{Var}_{|s\rangle}[\boldsymbol{H}] = \langle s|\boldsymbol{H}^2|s\rangle = \frac{\|\boldsymbol{H}\|_2^2}{d} \tag{133}$$

where in the first equality we used the fact that $\boldsymbol{H}$ is traceless. And we have already shown in Lemma C.1 that $\|\boldsymbol{H}\|_2^2/d \ge (\varepsilon_0/16)^2$ with constant probability of success, conditioned on $\boldsymbol{b} = 1$.

The reduction from amplitude amplification proceeds similarly, with one small difference. If $H = 0$, then since the state $e^{-iHt}|s\rangle$ has no support in the image of $I - |s\rangle\langle s|$, the marked amplitude $a = 0$, and *any* state is a valid solution to amplitude amplification. This pathological case can be repaired by giving the null instance a small nonzero good component, after which the logic of the reduction is unchanged.

C.4 Search with coherent errors

The final reduction is to unstructured search with coherent errors, as described in Problem 1.7

Proof of Lemma 2.4. Consider the setting in Problem 2.1 with $d_{\mathrm{eff}} = d$, $\mathsf{p} = 50/d_{\mathrm{eff}}$, $\theta_0 = \pi$, and any fixed $\sigma \in [0, 1/2)$. We will show there exists an algorithm which solves this problem using one call to a successful algorithm for unstructured search with coherent errors, Problem 1.7. First, note that in the alternative event $\boldsymbol{b} = 1$ we have $\boldsymbol{H} = \boldsymbol{H}_1 - \mathrm{tr}(\boldsymbol{H}_1)I/d$ where $\boldsymbol{H}_1$ is a diagonal Hamiltonian. Let $\boldsymbol{S} \subseteq [d]$ denote the subset of random indices corresponding to the nonzero entries of $\boldsymbol{H}_1$, and note that, by a Chernoff bound, $\boldsymbol{S}$ satisfies $20 \le |\boldsymbol{S}| \le 80$ with probability at least 0.99. Moreover, each of the nonzero diagonal entries is in the interval $[\pi - \sigma, \pi + \sigma]$. We can therefore implement a valid oracle for Problem 1.7 (up to an irrelevant global phase) by evolving forwards in time under $\boldsymbol{H}$ to obtain $e^{-i\boldsymbol{H}}$, and each call to this oracle adds one to the total evolution time. Solving Problem 1.7 in this case outputs an element in $\boldsymbol{S}$ with probability at least 0.99. By contrast, if $\boldsymbol{b} = 0$, then time evolution under $\boldsymbol{H}$ is identity with certainty, and solving Problem 1.7 with the oracle outputs NONE with probability at least 0.99. By union bound, the failure probability for solving the block distinguishing task from Lemma 2.4 in this manner is at most 0.02. □