npj | quantum information

Article

Published in partnership with The University of New South Wales

https://doi.org/10.1038/s41534-025-01135-5

On the query complexity of unitary channel certification

Check for updates

Sangwoo Jeon & Changhun Oh

Certifying the correct functioning of a unitary channel is a critical step toward reliable quantum information processing. In this work, we investigate the query complexity of the unitary channel certification task: testing whether a given d-dimensional unitary channel is identical to or ε-far in diamond distance from a target unitary operation. We show that incoherent algorithms—those without quantum memory—require $\Omega(d/\varepsilon^2)$ queries, matching the known upper bound. In addition, for general quantum algorithms, we prove a lower bound of $\Omega(\sqrt{d}/\varepsilon)$ and present a matching quantum algorithm based on quantum singular value transformation, establishing a tight query complexity of $\Theta(\sqrt{d}/\varepsilon)$. On the other hand, notably, we prove that for almost all unitary channels drawn from a natural average-case ensemble, certification can be accomplished with only $\mathcal{O}(1/\varepsilon^2)$ queries. This demonstrates an exponential query complexity gap between worst- and average-case scenarios in certification, implying that certification is significantly easier for most unitary channels encountered in practice. Together, our results offer both theoretical insights and practical tools for verifying quantum processes.

Reliable quantum information processing critically depends on our ability to verify that quantum processes behave as intended[1]. While quantum process tomography can accomplish this task for small-sized quantum devices, as quantum devices scale up in size and complexity for more sophisticated quantum information processing, this verification step becomes increasingly challenging[2,3]. Therefore, it is becoming essential to find an efficient way to certify a quantum process and ultimately to develop an optimal and practical scheme.

Quantum process certification-the task of verifying that a quantum process operates correctly—is therefore a central challenge in current quantum information processing. From an information-theoretic perspective, extensive research has investigated resources necessary for reliable certification[2–6]. Meanwhile, from a practical engineering perspective, protocols such as quantum process tomography[7–11] and randomized benchmarking[12–15] have been developed and implemented. More recently, quantum channel learning techniques have emerged as a promising approach, as they estimate key error observables without fully reconstructing the entire process, which can significantly reduce the required resources[16–23].

In many practical applications, a desired quantum process to implement is often described by a unitary channel, which plays the role of quantum gates in quantum computing and the perfect transmission of quantum information in quantum communication, because a unitary channel represents a quantum process under ideal and closed-system conditions. Therefore, among the certification tasks, *unitary channel certification*-the problem of certifying a unitary channel—is particularly important and practically relevant. In addition, recent technological advances in quantum coherence have brought laboratory environments closer to ideal closed-system conditions, further underscoring the practical relevance of unitary channel certification[24,25]. However, somewhat surprisingly, unitary channel certification remains largely unexplored. Previous studies on quantum process certification have typically considered noisy environments and have shown that certifying completely positive and trace-preserving (CPTP) channels requires exponentially many channel queries[2,3].

In this work, we investigate the unitary channel certification problem and characterize its query complexity. We first show that incoherent algorithms-those without quantum memory-require exponentially many queries for certification. We then show that coherent algorithms-general quantum algorithms with quantum memory-can achieve a quadratic speedup over incoherent algorithms through our query-optimal algorithm based on quantum singular value transformation (QSVT), although coherent algorithms still require exponentially many queries. On the other hand, we show that this exponential hardness arises only in worst-case scenarios and can be significantly reduced for average-case unitary channels. In particular, we show that there exists a simple algorithm that certifies almost all unitary channels drawn from a natural average-case ensemble using only a constant number of queries. These results demonstrate an exponential gap between worst- and average-case query complexities,

Department of Physics, Korea Advanced Institute of Science and Technology, Daejeon, South Korea.
e-mail: sangw077@gmail.com; changhun0218@gmail.com

suggesting that certification is substantially easier in practice than in the worst-case scenario.

We organize our work as follows. In section “Problem setup”, we provide a detailed definition of the problem setup for unitary channel certification, along with essential definitions. In section “Background and contributions”, we address relevant prior works and highlight our contribution. In section “Worst-case query complexity”, we establish the tight query complexity for unitary channel certification, showing that unitary channel certification requires exponentially many queries. Conversely, in section “Average-case query complexity”, we show that for almost all unitary channels sampled from an average-case ensemble, the query complexity significantly reduces to a constant number. Finally, we summarize our findings and discuss their implications in section “Discussion”.

Problem setup

We define unitary channel certification as the task of testing whether a given unitary channel is either identical to or ε-far from a target unitary channel[2,3,5,6]. We detail the problem setup below. Suppose one has black-box access to a given unitary channel $\mathcal{E}_U(\rho) := U\rho U^\dagger$, where U is a d-dimensional unitary operator acting on an n-qubit system with $d = 2^n$. The given unitary channel $\mathcal{E}_U$ is intended to match a target unitary channel $\mathcal{E}_V$. However, in practice, systematic imperfections such as cross-talk or gate miscalibration may introduce coherent errors, causing $\mathcal{E}_U$ to deviate from $\mathcal{E}_V$. Therefore, certification is required to guarantee that we are implementing a desired unitary circuit, using as few queries to $\mathcal{E}_U$ as possible.

We formally define the certification task as follows: testing whether the channel $\mathcal{E}_U$ is identical to $\mathcal{E}_V$ or ε-far from $\mathcal{E}_V$ using N queries to $\mathcal{E}_U$ with success probability at least 2/3. Here, by applying a unitary transformation of the form $\rho \mapsto V^\dagger \rho V$, we can simplify the task to certifying whether the unitary channel $\mathcal{E}_{UV^\dagger}$ is identical to the identity channel $\mathcal{E}_I$.Thus, without loss of generality, we set the target channel to be the identity channel and redefine the certification task as follows: testing whether the channel $\mathcal{E}_U$ is identical to $\mathcal{E}_I$ or ε-far from $\mathcal{E}_I$ using N queries to $\mathcal{E}_U$ with success probability at least 2/3. Thus, certification can be framed as a hypothesis-testing problem:

$$H_0 : \mathcal{E}_U = \mathcal{E}_I \quad \text{vs.} \quad \mathrm{H}_1 : \mathrm{D}(\mathcal{E}_\mathrm{U}, \mathcal{E}_\mathrm{I}) \geq \varepsilon, \tag{1}$$

with a suitable distance metric $D(\,\cdot\,,\,\cdot\,)$. Here, if $0 < D(\mathcal{E}_U, \mathcal{E}_I) < \varepsilon$, the algorithm is allowed to output either hypothesis. We employ the diamond distance as the distance metric:

$$D(\mathcal{E}_U, \mathcal{E}_V) = \max_\rho \| (\mathcal{E}_U \otimes \mathcal{E}_I)(\rho) - (\mathcal{E}_V \otimes \mathcal{E}_I)(\rho) \|_1, \tag{2}$$

where $\| \cdot \|_1$ denotes the Schatten-1 norm defined by $\| M \|_1 = \mathrm{Tr}(\sqrt{M^\dagger M})$. Note that the diamond distance captures the worst-case trace distance between output states over all possible input states[26].

We consider two types of algorithms for certification: incoherent and coherent. Incoherent algorithms, illustrated in Fig. 1a, perform positive operator-valued measurements (POVMs) after each of the N queries. These algorithms can be adaptive using classical registers to select both input states and POVMs based on previous measurement outcomes. This approach is practically motivated as storing quantum states across multiple queries in quantum memory is technically challenging. In contrast, coherent algorithms, illustrated in Fig. 1b, maintain quantum coherence across queries by storing intermediate quantum states. More specifically, a single input state sequentially passes through N circuit layers, each consisting of the ancilla-coupled unitary channel $\mathcal{E}_U$ and an interleaved CPTP map $\mathcal{C}_k$ for $1 \leq k \leq N$. A final POVM is then performed for certification. In this work, we extend this conventional framework to cover a wider range of quantum algorithms. Specifically, we allow arbitrarily large ancillary systems for both types of algorithms. We also permit the use of the inverse channel $\mathcal{E}_{U^\dagger}$ in place of certain queries to $\mathcal{E}_U$, noting that such access is often feasible in practice when $\mathcal{E}_U$ is given as a quantum circuit, as reversing the gate sequence and inverting each gate suffices to implement $\mathcal{E}_{U^\dagger}$. Under these assumptions, coherent algorithms represent the most general class, encompassing incoherent algorithms as a special case.

Background and contributions

Let us review prior works to highlight the key contributions of our work in comparison. The most relevant prior studies are the ones in refs. 2,3, which address the general channel certification problem: certifying whether a given CPTP channel is either identical to or ε-far from a target unitary channel in the diamond distance. Specifically, ref. 2 establishes a tight query complexity of $\Theta(d/\varepsilon^2)$ for incoherent algorithms, while ref. 3 proves a lower bound of $\Omega(\sqrt{d}/\varepsilon)$ for coherent algorithms but does not provide a matching upper bound. These results indicate that certifying a CPTP channel in a high-dimensional system is inherently a challenging task.

But is this hardness truly relevant in practice? Recent progress on preserving quantum coherence[24,25] and achieving high gate fidelities[27] suggests that nearly noiseless quantum processes may be feasible in the near term. This allows us to anticipate regimes in which incoherent errors, such as decoherence or dephasing, can be reasonably disregarded, thereby restricting the relevant family of CPTP channels for certification[28]. On the other hand, coherent errors, i.e., unitary-type errors, nevertheless remain, leading us to consider certification of unitary channels as the practically relevant setting.

Thus, it is natural and essential to ask whether the hardness of certification persists when the given CPTP channel is restricted to be unitary. Our first contribution is to show that the same lower bounds hold even under this unitary assumption, i.e., incoherent and coherent algorithms require $\Omega(d/\varepsilon^2)$ and $\Omega(\sqrt{d}/\varepsilon)$ queries for unitary channel certification, respectively, thereby strengthening the previous results. This result has two major implications: First, coherent (i.e., unitary) error is a fundamental source of the exponential hardness in quantum process certification. Second, despite the recent advances in reducing incoherent errors, the exponential hardness of certification remains unavoidable.

Nevertheless, finding an optimal quantum algorithm for certification remains an important challenge. Our second contribution is to develop a query-optimal certification algorithm for coherent strategies, achieving the tight complexity of $\Theta(\sqrt{d}/\varepsilon)$ by employing QSVT. This implies that using quantum memory to combine multiple queries coherently can yield a quadratic speedup in certification.

Due to the high complexity of certification under the diamond distance, prior research has attempted to relax the task by considering alternative distance measures. In particular, these works have employed average-case distances to achieve constant query complexity by avoiding the hardness associated with worst-case instances. Reference [4] showed a constant query complexity $\mathcal{O}(1/\varepsilon^2)$ for certification under a fidelity-based distance $D(\mathcal{E}_U, \mathcal{E}_V) = \sqrt{1 - |\mathrm{Tr}(U^\dagger V)|^2/d^2}$, and more recently ref. 3 showed the same query complexity for an average-case imitation diamond distance $D(\mathcal{E}_U, \mathcal{E}_V) = \| (\mathcal{E}_U \otimes \mathcal{E}_I)(\Phi) - (\mathcal{E}_V \otimes \mathcal{E}_I)(\Phi) \|_1$ where Φ is a maximally entangled state over two d-dimensional Hilbert spaces. Although these average-case results significantly ease the query complexity, their relevance to practical certification remains less clear.

As our last contribution, we show a constant query complexity $\mathcal{O}(1/\varepsilon^2)$ for certification with the diamond distance by considering the average-case *channels*. We show that there exists a simple algorithm achieving this complexity for almost all unitary channels sampled from a natural average-case distribution. Here, the fraction of exceptional channels is on the order of $\exp(-\Omega(d))$, which is exponentially small in the system dimension. This suggests that certification is significantly less challenging in practice than previously believed, offering a highly relevant framework for practical certification.

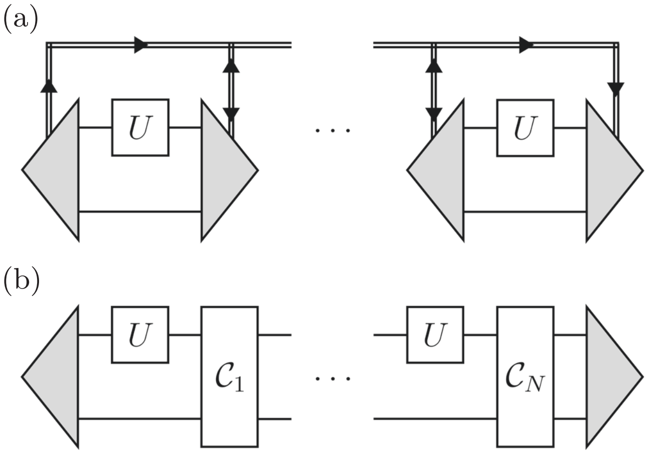

Fig. 1 | Incoherent and coherent algorithms. a Incoherent algorithm. The double line represents the classical registers. **b** Coherent algorithm. $\mathcal{C}_k$ for $1 \le k \le N$ represents a CPTP map that we apply at k-th step as part of the algorithm. We allow arbitrarily large ancillary systems for both algorithms.

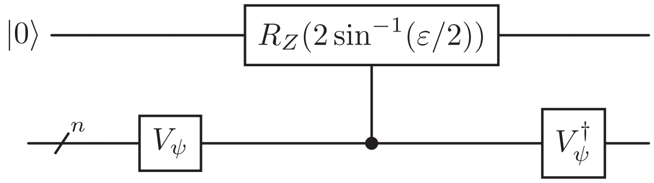

Fig. 2 | Circuit implementation of a single-basis rotation channel $\mathcal{E}_{U_\psi}$. The unitary operator V_ψ maps the basis state $|\psi\rangle$ to the computational basis state $|1\rangle^{\otimes n}$. The controlled-rotation gate applies a phase shift of $2\sin^{-1}(\varepsilon/2)$ to this computational basis component. As a result, the entire circuit behaves as a phase-shifting channel for the $|\psi\rangle$ basis and as an identity channel for all other bases.

Worst-case query complexity

We now present our main result. We begin by establishing the query complexity of unitary channel certification in the standard worst-case scenario, i.e., the number of queries required to certify an arbitrary unitary channel.

Query complexity for incoherent algorithms

We prove that certifying unitary channels requires exponentially many queries for incoherent algorithms even when using arbitrarily large ancillary systems and adaptive strategies. Our result is stated as follows:

Theorem 1. Consider an adaptive, incoherent algorithm with an arbitrarily large ancillary system, which tests whether $D(\mathcal{E}_U, \mathcal{E}_I) \ge \varepsilon$ or $\mathcal{E}_U = \mathcal{E}_I$ with success probability at least 2/3. For $\varepsilon < 1/2$ and $d > 50\varepsilon^2$, the required number of queries to $\mathcal{E}_U$ (or $\mathcal{E}_{U^\dagger}$) is $N = \Omega(d/\varepsilon^2)$.

This result strengthens the established lower bound that incoherent algorithms require $\Omega(d/\varepsilon^2)$ queries to certify general CPTP channels[2]. Specifically, it shows that the same bound applies even when the given CPTP channel is guaranteed to be unitary.

To prove Theorem 1, we consider a related hypothesis-testing task, which serves as a restricted version of the certification task. Let E_ε be an ensemble of ε-perturbed unitary channels $\mathcal{E}_U$, each satisfying $D(\mathcal{E}_U, \mathcal{E}_I) = \varepsilon$. We consider testing whether $\mathcal{E}_U$ is the identity channel or is sampled from the ensemble E_ε:

$$H_0 : \mathcal{E}_U = \mathcal{E}_I \quad \text{vs.} \quad \mathrm{H}_1 : \mathcal{E}_{\mathrm{U}} \sim \mathrm{E}_\varepsilon. \tag{3}$$

Since a channel $\mathcal{E}_U$ sampled from E_ε always satisfies $D(\mathcal{E}_U, \mathcal{E}_I) \ge \varepsilon$ by construction, any algorithm that successfully certifies unitary channels must be able to distinguish these two hypotheses. Thus, the query complexity of this hypothesis test provides a lower bound on the complexity of the original certification task. Therefore, it is sufficient to analyze the query complexity of this problem to derive the lower bound of the unitary channel certification problem.

We now construct an ensemble E_ε to which the corresponding hypothesis testing requires many queries. The ensemble we construct is given as follows:

$$E_\varepsilon = \{\mathcal{E}_{U_\psi}\}_{|\psi\rangle \sim \mathrm{Haar}}, \tag{4}$$

$$U_\psi := I + (e^{2i\sin^{-1}(\varepsilon/2)} - 1)|\psi\rangle\langle\psi|, \tag{5}$$

where $|\psi\rangle$ is a d-dimensional Haar-random state. Here, each unitary channel $\mathcal{E}_{U_\psi}$ in this ensemble induces a phase shift of $2\sin^{-1}(\varepsilon/2)$ only on the basis $|\psi\rangle$ and acts as the identity elsewhere (see Fig. 2). Reflecting this structure, we refer to $\mathcal{E}_{U_\psi}$ as the *single-basis rotation channel* and to the ensemble E_ε as the *single-basis rotation ensemble*. To confirm that E_ε forms an ensemble of ε-perturbed unitary channels from the identity channel, we examine the structure of the diamond distance $D(\mathcal{E}_U, \mathcal{E}_I)$. The following lemma expresses it in terms of the eigenangles $\theta_1, \ldots, \theta_d$, the arguments of the complex eigenvalues $e^{i\theta_1}, \ldots, e^{i\theta_d}$ of the unitary operator U:

Lemma 1. ([6,11]) Let $[\theta_{\min}, \theta_{\max}]$ be the shortest interval including all eigenangles of U. Then for $\varepsilon < 2$, $D(\mathcal{E}_U, \mathcal{E}_I) = \varepsilon$ is equivalent to $\theta_{\max} - \theta_{\min} = 2\sin^{-1}(\varepsilon/2)$.

Applying this lemma to the channel $\mathcal{E}_{U_\psi}$, only one eigenangle corresponding to the $|\psi\rangle$ basis is nonzero (equal to $2\sin^{-1}(\varepsilon/2)$), while the remaining eigenangles are all zero. Thus, we have $\theta_{\min} = 0$ and $\theta_{\max} = 2\sin^{-1}(\varepsilon/2)$, confirming that $\mathcal{E}_{U_\psi}$ is ε-perturbed as $D(\mathcal{E}_{U_\psi}, \mathcal{E}_I) = \varepsilon$; thus, E_ε is an ensemble of ε-perturbed unitary channels from the identity channel.

Now, we conclude that testing the hypothesis-distinguishing an identity channel from a random channel from E_ε-is exponentially hard for an incoherent algorithm, requiring $\Omega(d/\varepsilon^2)$ queries. The rest of the proof is outlined in the following proof sketch:

Proof sketch of Theorem 1. We employ LeCam's two-point method[29] to analyze the hypothesis testing problem defined in Eq. (3). This method relates the testing error probability to the total variation distance (TVD) between the probability distributions of observables under the two hypotheses. More specifically, LeCam's method implies that achieving a small testing error requires a sufficiently large TVD between these distributions. Thus, we show that a query complexity of $\Omega(d/\varepsilon^2)$ is necessary to obtain such a large TVD. This directly implies that the same complexity is required for the certification task.

Our proof proceeds in two main steps. First, we define a suitable *good set* of the measurement outcomes and show that for arbitrary measurements, most outcomes lie within this set, except possibly for a small fraction. Next, we show that within this good set, the likelihood ratio between the distributions corresponding to the two hypotheses is concentrated around 1, i.e., the two hypotheses are informationally hard to distinguish. To quantify this concentration rigorously, we employ a martingale-based concentration inequality from ref. 19. This step yields an explicit upper bound on the achievable TVD as a function of the number of queries N. Together, these results establish the claimed complexity lower bound. The detailed proof is provided in Supplementary Material (SM) Sec. S1 (Supplemental material). □

Note that this lower bound is tight as there exists a matching upper bound established by ref. 2. Specifically, the following algorithm based on random state preparation and measurement achieves the matching upper bound of $\mathcal{O}(d/\varepsilon^2)$:

Algorithm 1. **Query-optimal incoherent algorithm for unitary channel certification**[2]

```
Input: $N$ copies of an $d$-dimensional unitary channel $\mathcal{E}_U$.
Output: Decide whether $H_0 : \mathcal{E}_U = \mathcal{E}_I$ or $H_1 : D(\mathcal{E}_U, \mathcal{E}_I) \geq \varepsilon$.
for $i = 1$ to $N$ do
    Input Haar-random $|\psi\rangle$ to $\mathcal{E}_U$.
    Measure output with POVM $\{|\psi\rangle\langle\psi|, I - |\psi\rangle\langle\psi|\}$.
    Obtain outcome $X_i = 0$ or $X_i = 1$, respectively.
    if $X_i = 1$ then
        return Decide $H_1$.
return Decide $H_0$.
```

Query complexity for coherent algorithms

In various quantum hypothesis-testing scenarios, jointly measuring multiple queries simultaneously-known as joint measurement-often yields substantial advantages compared to measuring each query individually[30–32]. Thus, it is valuable to extend our analysis beyond incoherent algorithms and consider general coherent algorithms.

We prove that unitary channel certification requires exponentially many queries, even for coherent algorithms with arbitrarily large ancillary systems. This result highlights the fundamental hardness of certification. Our result is stated as follows:

Theorem 2. Consider a coherent algorithm with an arbitrarily large ancillary system, which tests whether $D(\mathcal{E}_U, \mathcal{E}_I) \geq \varepsilon$ or $\mathcal{E}_U = \mathcal{E}_I$ with success probability at least 2/3. For $\varepsilon < 1/2$, the required number of queries to $\mathcal{E}_U$ (or $\mathcal{E}_{U^\dagger}$) is $N = \Omega(\sqrt{d}/\varepsilon)$.

This strengthens the established lower bound that coherent algorithms require $\Omega(\sqrt{d}/\varepsilon)$ queries to certify general CPTP channels[3]. Specifically, it shows that the same lower bound applies even when the channel is guaranteed to be unitary. This also generalizes the lower bound for Boolean function certification, which requires $\Omega(\sqrt{d})$ queries[4].

Proof sketch of Theorem 2. Consider the output states ρ_0 and ρ_1 corresponding to hypotheses H_0 and H_1 in Eq. (3), respectively. The hypothesis-testing error probability is bounded by the trace distance between these two states[33]. In coherent algorithms, each pair of an ancilla-coupled channel $\mathcal{E}_U$ and the CPTP map $\mathcal{C}_k$ can increase this trace distance by at most $\mathcal{O}(\varepsilon/\sqrt{d})$, due to the contractivity of trace distance under CPTP maps[34]. Therefore, achieving an error probability of at least 2/3 requires query complexity $\Omega(\sqrt{d}/\varepsilon)$. The detailed proof is provided in SM Sec. S2 A (Supplemental material). We note that the proof is similar to the one given by ref. 3. □

Theorem 2 highlights the exponential hardness of certification. Meanwhile, we observe that if information about the basis state $|\psi\rangle$ associated with each single-basis rotation channel $\mathcal{E}_{U_\psi} \sim E_\varepsilon$ is given, one can certify $\mathcal{E}_{U_\psi}$ using only constant queries of $\mathcal{O}(1/\varepsilon^2)$ via the Hadamard test on the channel $\mathcal{E}_{U_\psi}$ and the state $|\psi\rangle$. This indicates that the hardness given in Theorem 2 arises from the unknown information on the phase-rotating basis state $|\psi\rangle$ of $\mathcal{E}_{U_\psi}$.

This type of issue is frequently referred to as *finding a needle in a haystack*, as one has to find a single basis state in a large-dimensional Hilbert space. A well-known solution to this is Grover's algorithm, which achieves a quadratic speedup over the brute-force approach in a basis-search problem[35,36]. Motivated by this, we present a novel Grover-like algorithm achieving the optimal query complexity of $\mathcal{O}(\sqrt{d}/\varepsilon)$, thereby exhibiting a *quadratic speedup* compared to incoherent algorithms. Our result is stated as follows:

Theorem 3. There exists a coherent algorithm that tests whether $\mathcal{E}_U = \mathcal{E}_I$ or $D(\mathcal{E}_U, \mathcal{E}_I) \geq \varepsilon$ with success probability at least 2/3 using $N = \mathcal{O}(\sqrt{d}/\varepsilon)$ queries to $\mathcal{E}_U$ and $\mathcal{E}_{U^\dagger}$.

Together with Theorem 2, this establishes a tight query complexity of $\Theta(\sqrt{d}/\varepsilon)$ for unitary channel certification with coherent algorithms. This also implies that allowing quantum memory between queries leads to a quadratic speedup-by a factor of $\Theta(\sqrt{d}/\varepsilon)$-over incoherent algorithms. We note that access to the inverse channel $\mathcal{E}_{U^\dagger}$ is not a stringent assumption as U is often implemented as a quantum circuit composed of a known sequence of standard gates, in which case $\mathcal{E}_{U^\dagger}$ can be realized by simply reversing the gate sequence and replacing each gate with its inverse. In addition, the same assumption is also used in Theorems 1 and 2 for a fair comparison.

We provide an intuitive description of our algorithm by comparing it with Grover's algorithm, leaving the full version to the end of the section. The goal of Grover's algorithm is to search for the bit-flipping basis $|m\rangle$ with an oracle $I - 2|m\rangle\langle m|$. To achieve this, Grover's algorithm amplifies the overlap between an initial superposition state $|s\rangle = (|1\rangle + \cdots + |d\rangle)/\sqrt{d}$ and the target state $|m\rangle$, using alternating rotations around $|s\rangle$ and $|m\rangle$. By precisely tuning the number of rotations, one can drive the input state towards the target state $|m\rangle$, thus achieving the searching task. In contrast, our algorithm performs a process of *amplitude deamplification*, reducing the initially large overlap between two states-a Haar-random state $|\psi\rangle$ and a slightly-rotated $U|\psi\rangle$-to near zero. More specifically, the algorithm takes a Haar-random input state $|\psi\rangle$ and applies alternating rotations around $|\psi\rangle$ and $U|\psi\rangle$. Under H_1, this drives the state toward a state orthogonal to $|\psi\rangle$, while under H_0, the rotations preserve the initial $|\psi\rangle$. A POVM $\{|\psi\rangle\langle\psi|, I - |\psi\rangle\langle\psi|\}$ then distinguishes between H_0 and H_1, certifying the unitary channel.

A central challenge in adapting Grover's approach lies in the uncertainty of the appropriate number of rotations. Grover's algorithm requires a precise number of rotations, which is a fixed value depending on the initial overlap $\langle s|m\rangle = 1/\sqrt{d}$. In our case, the number of rotations depends on the overlap $\langle\psi|U^\dagger|\psi\rangle$ between $|\psi\rangle$ and $U|\psi\rangle$, which is unknown and varies with both U and the randomly chosen $|\psi\rangle$. Thus, we cannot directly adopt Grover's iterative structure.

Therefore, we leverage QSVT, a powerful framework for designing quantum algorithms based on polynomial transformations of operators[37,38]. We briefly introduce the key concept of QSVT to fully construct our algorithm. Suppose one has black-box access to a unitary operator V and its inverse $V^\dagger$. Let Π and $\tilde{\Pi}$ be orthogonal projections, and consider the sub-block $S = \Pi V \tilde{\Pi}$ of V, which can be expressed in block-encoding form as:

$$V = \begin{array}{cc} & \Pi \\ \tilde{\Pi} & \begin{bmatrix} S & \cdot \\ \cdot & \cdot \end{bmatrix} \end{array}. \tag{6}$$

QSVT enables a polynomial transformation of the singular values of S using V, $V^\dagger$, and phase rotations controlled by the projectors Π and $\tilde{\Pi}$. To illustrate, let $S = W\Sigma\tilde{W}^\dagger$ be the singular value decomposition of the sub-block S. Then, QSVT yields a new operator $P^{(SV)}(S) = WP(\Sigma)\tilde{W}^\dagger$ for a real polynomial P satisfying certain conditions. This leads to the following transformed block encoding:

$$V_\Phi = \begin{array}{cc} & \Pi \\ \tilde{\Pi} \text{ or } \Pi & \begin{bmatrix} P^{(SV)}(S) & \cdot \\ \cdot & \cdot \end{bmatrix} \end{array}, \tag{7}$$

where V_Φ is the result of a QSVT circuit. The procedure for constructing the QSVT circuit is formally stated in the following lemma:

Lemma 2. ([37]) Let Π and $\tilde{\Pi}$ be orthogonal projections and define Π_ϕ: $=e^{i\phi(2\Pi-I)}$ as a projector-controlled phase-rotation gate with angle ϕ. Suppose P is a real polynomial satisfying:

(1) $\deg(P) = n$
(2) P shares the same parity as n.
(3) $|P(x)| \leq 1$ for $x \in [-1, 1]$.

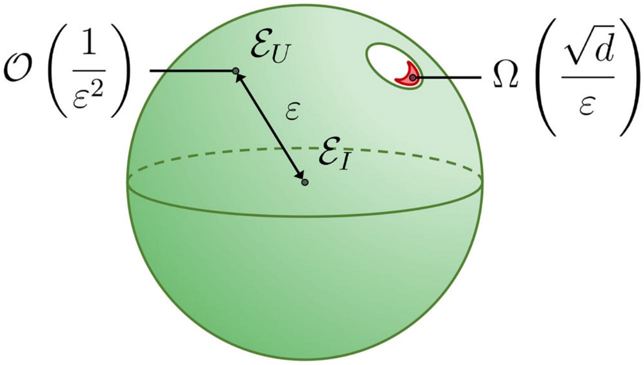
$\mathcal{O}\left(\frac{1}{\varepsilon^2}\right)$
$\mathcal{E}_U$
ε
$\mathcal{E}_I$
$\Omega\left(\frac{\sqrt{d}}{\varepsilon}\right)$

Fig. 3 | Visualization of query complexities for ε-perturbed unitary channels. The spherical shell represents the set of ε-perturbed unitary channels sampled from $\varepsilon-$CUE. The green region represents average-case channels, which can be certified using $\mathcal{O}(1/\varepsilon^2)$ queries. The red region represents the single-basis rotation ensemble E_ε, which requires $\Omega(\sqrt{d}/\varepsilon)$ queries for certification. The white region represents a small exceptional subset of measure $\exp(-\Omega(d))$ with unknown complexity. Note that the colored regions do not correspond to genuine geometric relations in the space of $\varepsilon-$CUE.

Then, for a given unitary operator V, there exist angles $\Phi = (\phi_1, \ldots, \phi_n)$ such that the unitary operator

$$V_\Phi = \begin{cases} \tilde{\Pi}_{\phi_1} V \prod_{k=1}^{(n-1)/2} \Pi_{\phi_{2k}} V^\dagger \tilde{\Pi}_{\phi_{2k+1}} V & n \text{ is odd} \\ \prod_{k=1}^{n/2} \Pi_{\phi_{2k-1}} V^\dagger \tilde{\Pi}_{\phi_{2k}} V & n \text{ is even} \end{cases} \tag{8}$$

satisfies

$$P^{(\mathrm{SV})}(\Pi V \tilde{\Pi}) = \begin{cases} \Pi V_\Phi \tilde{\Pi} & n \text{ is odd} \\ \Pi V_\Phi \Pi & n \text{ is even} \end{cases}. \tag{9}$$

Details on determining the rotation angles Φ from the polynomial P can be found in ref. 37.

Collecting the results, we now present the full description of our algorithm. Our algorithm proceeds in three steps: prepare a Haar-random state $|\psi\rangle$, apply a QSVT operator V_Φ, and perform a POVM $\{|\psi\rangle\langle\psi|, I - |\psi\rangle\langle\psi|\}$. Following the notation in Lemma 2, we construct the operator V_Φ using projections $\Pi = |\psi\rangle\langle\psi|$ and $\tilde{\Pi} = U|\psi\rangle\langle\psi|U^\dagger$, along with a real polynomial P chosen as a rescaled Chebyshev polynomial. Under this construction, V_Φ corresponds to a sequence of alternating rotations around $|\psi\rangle$ and $U|\psi\rangle$ with rotation angles determined by the polynomial P. We show that for almost every Haar-random $|\psi\rangle$, this transformation maps the initial singular value $|\langle\psi|U^\dagger|\psi\rangle|$ to a transformed singular value $|\langle\psi|V_\Phi|\psi\rangle|$ that is close to one under H_0 and close to zero under H_1, without requiring knowledge of the exact overlap between $|\psi\rangle$ and $U|\psi\rangle$. This ensures that the measurement outcome reliably distinguishes between the two hypotheses, therefore enabling certification of the given channel. Furthermore, we show that the QSVT circuit V_Φ can be implemented using $\mathcal{O}(\sqrt{d}/\varepsilon)$ queries to $\mathcal{E}_U$ and $\mathcal{E}_{U^\dagger}$, thereby proving Theorem 3. The complete proof is provided in SM Sec. S2 B (Supplemental material), and we summarize the algorithm below:

Algorithm 2. **Query-optimal coherent algorithm for unitary channel certification**

```
Input: Unitary channel $\mathcal{E}_{V_\Phi}$ from QSVT, using $N$ copies of $\mathcal{E}_U$ and $\mathcal{E}_{U^\dagger}$.
Output: Decide whether $H_0 : \mathcal{E}_U = \mathcal{E}_I$ or $H_1 : D(\mathcal{E}_U, \mathcal{E}_I) \geq \varepsilon$.
Input Haar-random $|\psi\rangle$ to $\mathcal{E}_{V_\Phi}$.
Measure output with POVM $\{|\psi\rangle\langle\psi|, I - |\psi\rangle\langle\psi|\}$.
Obtain outcome $M = 0$ or $M = 1$, respectively.
if $M = 0$ then
    return Decide $H_0$.
else
    return Decide $H_1$.
```

Average-case query complexity

So far, we have established the exponential hardness of unitary channel certification by showing that the identity channel is hard to distinguish from a randomly sampled single-phase rotation channel $\mathcal{E}_{U_\psi}$, where $|\psi\rangle$ is sampled from the Haar measure. Here, the channel $\mathcal{E}_{U_\psi}$ can be viewed as a multiqubit-controlled phase rotating operation (see Fig. 2), which is highly nonlocal and unlikely to arise under standard local noise models. This naturally raises the question of whether the exponential hardness we established is overly pessimistic or rarely encountered in practical situations. Indeed, efficient algorithms for average-case scenarios commonly exist across various quantum testing frameworks, such as quantum channel learning[39] and quantum state certification[40]. Motivated by these observations, we examine the following question: Can the hardness of certification be relaxed if we consider average-case unitary channels?

To address this question, we first need to clearly define what constitutes the *average case* for random unitary channels. A conventional and natural choice of a random unitary ensemble is the circular unitary ensemble (CUE), which corresponds to the Haar measure over the unitary group[41,42]. However, in our setting, the CUE itself is not an appropriate notion of average-case unitary channels because the CUE does not adequately represent ε-perturbed unitary channels, and thus fails to offer a fair comparison with the single-basis rotation ensemble E_ε. For a fair comparison, we must instead consider an ensemble consisting exclusively of ε-perturbed unitary channels. Thus, we introduce the ensemble ε-CUE, defined as the marginal distribution of the CUE conditioned on the channel being ε-perturbed. Precisely, its corresponding measure $\mu_{\varepsilon-\mathrm{CUE}}$ is given as:

$$\mu_{\varepsilon-\mathrm{CUE}}(A) := \Pr_{U\sim\mathrm{CUE}}(U \in A | D(\mathcal{E}_U, \mathcal{E}_I) = \varepsilon) \tag{10}$$

for a set A.

We show that for almost every randomly chosen unitary $U \sim \varepsilon-$CUE, except for an exponentially small fraction, there exists a simple, non-adaptive, and ancilla-free algorithm capable of certifying the channel $\mathcal{E}_U$ using only a *constant number of queries*. Our result is stated as follows:

Theorem 4. Suppose a random unitary channel $\mathcal{E}_U$ is given with $U \sim \varepsilon-$CUE under $\varepsilon < 1/2$ and dimension $d \geq 4$. There exists an algorithm that tests whether $D(\mathcal{E}_U, \mathcal{E}_I) \geq \varepsilon$ or $\mathcal{E}_U = \mathcal{E}_I$ with success probability at least 2/3 using $N = \mathcal{O}(1/\varepsilon^2)$ queries, except for $\exp(-\Omega(d))$ fraction of U.

In other words, this implies the existence of an efficient algorithm that can test the following hypotheses with high probability:

$$H_0 : \mathcal{E}_U = \mathcal{E}_I \quad \text{vs.} \quad H_1 : U \sim \varepsilon - \mathrm{CUE}. \tag{11}$$

Theorem 4 establishes an exponentially large gap between the query complexity of worst-case and average-case scenarios, as illustrated in Fig. 3. This emphasizes the importance and practical relevance of considering the average-case scenario in quantum process certification.

Algorithm 1 introduced in section "Query complexity for incoherent algorithms" achieves the query complexity stated in Theorem 4. We point out that the algorithm employs simple methods involving random state preparation and measurement, without requiring ancillas or adaptive operations. In addition, it can be efficiently simulated using a unitary 2-design, which can be implemented with shallow quantum circuits of depth $\mathcal{O}(\log\log\log d)$ composed of random Clifford gates[43]. These observations show that the optimal query complexity can be achieved by an algorithm with a simple structure.

The constant query complexity of Algorithm 1 in the average-case scenario stems from a structural property of Haar-random unitaries. The eigenvalues of the CUE can be modeled as interacting Brownian particles on a

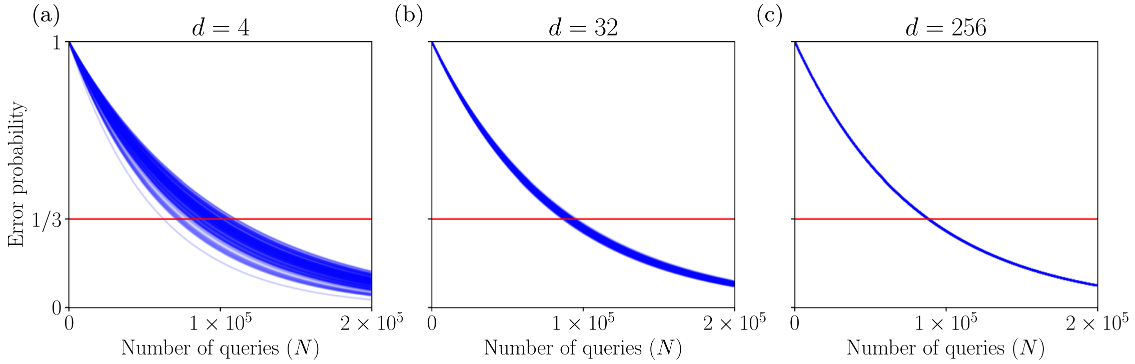

Fig. 4 | Simulated error probabilities from numerical experiments of Algorithm 1. We plot error probabilities for 200 randomly sampled unitary channels drawn from ε—CUE, with the error threshold $\varepsilon = 0.01$ and dimensions **a** $d = 4$, **b** $d = 32$, and **c** $d = 256$. Each blue curve represents the error probability of a single channel as a function of the number of queries N. The red horizontal line indicates the targeted error threshold of 1/3.

unit circle with inter-particle repulsion[44]. Thus, for ε—CUE, these eigenvalues behave as repulsive particles confined within an arc of length $2\sin^{-1}(\varepsilon/2)$. Consequently, the eigenangles from ε—CUE are well-distributed within this region with high probability, leading to an eigenangle variance of order ε^2. In contrast, worst-case channels from E_ε channels have highly concentrated eigenangles; Only one eigenangle differs significantly, resulting in an exponentially smaller eigenangle variance of order ε^2/d. Our proof of Theorem 4 leverages this observation, showing that Algorithm 1 can certify channels having *well-distributed eigenangles* with $\mathcal{O}(1/\varepsilon^2)$ queries. A detailed proof is given in SM Sec. S3 (Supplemental material).

We numerically simulate Algorithm 1 on unitary channels sampled from ε—CUE and verify our theoretical results. To sample unitary channels from ε—CUE, we apply the rejection sampling method using the eigenvalue distribution of the 2-Jacobi ensemble[45]. Then, for each sampled channel, we simulate the corresponding error probability, as shown in Fig. 4. The average behavior of the error probability curves is independent of the dimension d, even for a low dimension such as $d = 4$. Additionally, the variance in error probability greatly decreases as the dimension d increases. This aligns with our theoretical prediction that the proportion of exceptional edge cases decays exponentially as $\exp(-\Omega(d))$. The figure also indicates that the required query complexity lies within realistic experimental ranges. Algorithm 1 requires ~10^5 queries to certify unitary channels up to precision $\varepsilon = 0.01$, corresponding to a deviation of roughly 1% in the worst-case basis. This query count is comparable to the number of circuit executions reported in recent large-scale experiments, such as Google's Willow processor, which performed up to 10^6 surface-code cycles with a 1.1 μs repetition time[46].

We distinguish our result from those in refs. 3,4, which show that certification under *average-case distance* requires a constant query complexity of $\mathcal{O}(1/\varepsilon^2)$. In our case, we show that the same query complexity suffices for certifying *average-case channels* under the more stringent diamond distance. Our approach is operationally meaningful, as certification under the diamond distance provides uniform performance guarantees across all input states, whereas certification under average-case distance ensures correctness only on a specific input state[26]. Accordingly, our result indicates that fully reliable certification is available for almost every unitary channel, offering a stronger and more practical contribution to reliable quantum information processing.

Discussion

In this work, we have investigated the query complexity for unitary channel certification. We proved that an exponential number of queries is required to certify all unitary channels, while coherent algorithms can achieve a quadratic speedup over incoherent algorithms. We then proved that exponential hardness can be significantly relaxed for average-case unitary channels, which can be certified with a constant number of queries.

We highlight a notable technical contribution from our proof of Theorem 1. In many quantum hypothesis testing problems, proofs establishing query lower bounds for incoherent algorithms use a common technique: reducing the problem to distinguishing between a target object and an ensemble of slightly perturbed target objects[2,3,16–19,22,23,47]. Due to technical challenges, previous works relied on ensembles containing mixedness, such as an ensemble of mixed states or noisy channels. Our proof overcomes this limitation by extending the technique to an ensemble consisting solely of unitary channels (see SM Sec. S1 for details (Supplemental material)). Thus, we anticipate further applications of our approach in future work, including potential extensions of this lower bound to continuous variable systems, where analogous certification challenges remain largely unexplored.

We suggest some intriguing directions for future research. Extending our average-case result to general CPTP channel would be a critical step for efficient certification in practice. In this case, defining an appropriate measure of average-case CPTP channel would be essential. One could also investigate the query-optimal coherent certification algorithm that does not rely on the inverse channel $\mathcal{E}_{U^\dagger}$.

Data availability

No datasets were generated or analyzed during the current study.

Code availability

Code used to generate data in this study are available from the corresponding author upon reasonable request.

Received: 18 August 2025; Accepted: 22 October 2025;
Published online: 29 December 2025

References

1. Preskill, J. Reliable quantum computers. *Proc. R. Soc. Lond. Ser. A Math., Phys. Eng. Sci.* **454**, 385–410 (1998).
2. Fawzi, O., Flammarion, N., Garivier, A. & Oufkir, A. Quantum channel certification with incoherent strategies. In *COLT 23-36th Annual Conference on Learning Theory* 1–58 (2023).
3. Rosenthal, G., Aaronson, H., Subramanian, S., Datta, A. & Gur, T. Quantum channel testing in average-case distance. https://doi.org/10.48550/arXiv.2409.12566 (2024).
4. Montanaro, A. & de Wolf, R. A survey of quantum property testing. *Theory Comput.* 1–81 (2016).
5. Eisert, J. et al. Quantum certification and benchmarking. *Nat. Rev. Phys.* **2**, 382–390 (2020).
6. Kliesch, M. & Roth, I. Theory of quantum system certification. *PRX quantum* **2**, 010201 (2021).
7. Chuang, I. L. & Nielsen, M. A. Prescription for experimental determination of the dynamics of a quantum black box. *J. Mod. Opt.* **44**, 2455–2467 (1997).
8. Acín, A., Jané, E. & Vidal, G. Optimal estimation of quantum dynamics. *Phys. Rev. A* **64**, 050302 (2001).

9. Altepeter, J. B. et al. Ancilla-assisted quantum process tomography. *Phys. Rev. Lett.* **90**, 193601 (2003).
10. Yang, Y., Renner, R. & Chiribella, G. Optimal universal programming of unitary gates. *Phys. Rev. Lett.* **125**, 210501 (2020).
11. Haah, J., Kothari, R., O'Donnell, R. & Tang, E. Query-optimal estimation of unitary channels in diamond distance. In *2023 IEEE 64th Annual Symposium on Foundations of Computer Science (FOCS)* 363–390 (IEEE, 2023).
12. Emerson, J., Alicki, R. & Życzkowski, K. Scalable noise estimation with random unitary operators. *J. Opt. B Quantum Semiclassical Opt.* **7**, S347 (2005).
13. Knill, E. et al. Randomized benchmarking of quantum gates. *Phys. Rev. A* **77**, 012307 (2008).
14. Dankert, C., Cleve, R., Emerson, J. & Livine, E. Exact and approximate unitary 2-designs and their application to fidelity estimation. *Phys. Rev. A Mol. Opt. Phys.* **80**, 012304 (2009).
15. Magesan, E., Gambetta, J. M. & Emerson, J. Scalable and robust randomized benchmarking of quantum processes. *Phys. Rev. Lett.* **106**, 180504 (2011).
16. Chen, S., Zhou, S., Seif, A. & Jiang, L. Quantum advantages for Pauli channel estimation. *Phys. Rev. A* **105**, 032435 (2022).
17. Chen, S., Cotler, J., Huang, H.-Y. & Li, J. Exponential separations between learning with and without quantum memory. In *2021 IEEE 62nd Annual Symposium on Foundations of Computer Science (FOCS)* 574–585 (IEEE, 2022).
18. Chen, S., Li, J., Huang, B. & Liu, A. Tight bounds for quantum state certification with incoherent measurements. In *Proc. IEEE 63rd Annual Symposium on Foundations of Computer Science (FOCS)* 1205–1213 (IEEE, 2022).
19. Chen, S. & Gong, W. Efficient pauli channel estimation with logarithmic quantum memory. *PRX Quantum* **6**, 020323 (2025).
20. Huang, H.-Y., Chen, S. & Preskill, J. Learning to predict arbitrary quantum processes. *PRX Quantum* **4**, 040337 (2023).
21. Chen, K., Wang, Q., Long, P. & Ying, M. Unitarity estimation for quantum channels. *IEEE Trans. Inf. Theory* **69**, 5116–5134 (2023).
22. Chen, S., Oh, C., Zhou, S., Huang, H.-Y. & Jiang, L. Tight bounds on pauli channel learning without entanglement. *Phys. Rev. Lett.* **132**, 180805 (2024).
23. Oh, C. et al. Entanglement-enabled advantage for learning a bosonic random displacement channel. *Phys. Rev. Lett.* **133**, 230604 (2024).
24. Park, J. et al. Passive and active suppression of transduced noise in silicon spin qubits. *Nat. Commun.* **16**, 78 (2025).
25. Salhov, A. et al. Protecting quantum information via destructive interference of correlated noise. *Phys. Rev. Lett.* **132**, 223601 (2024).
26. Wilde, M. M. *Quantum Information Theory* (Cambridge University Press, 2013).
27. Hughes, A. et al. Trapped-ion two-qubit gates with >99.99% fidelity without ground-state cooling. *arXiv preprint* https://doi.org/10.48550/arXiv.2510.17286 (2025).
28. Kueng, R., Long, D. M., Doherty, A. C. & Flammia, S. T. Comparing experiments to the fault-tolerance threshold. *Phys. Rev. Lett.* **117**, 170502 (2016).
29. LeCam, L. Convergence of estimates under dimensionality restrictions. *Ann. Stat.* **1**, 38–53 (1973).
30. Shapiro, J. H. The quantum illumination story. *IEEE Aerosp. Electron. Syst. Mag.* **35**, 8–20 (2020).
31. Zhuang, Q. Quantum ranging with Gaussian entanglement. *Phys. Rev. Lett.* **126**, 240501 (2021).
32. Coroi, E. & Oh, C. Exponential advantage in continuous-variable quantum state learning. *arXiv preprint* https://doi.org/10.48550/arXiv.2501.17633 (2025).
33. Helstrom, C. W. Quantum detection and estimation theory. *J. Stat. Phys.* **1**, 231–252 (1969).
34. Nielsen, M. A. & Chuang, I. L. *Quantum Computation and Quantum Information* (Cambridge University Press, 2010).
35. Grover, L. K. A fast quantum mechanical algorithm for database search. In *Proc. Twenty-Eighth Annual ACM Symposium on Theory of Computing* 212–219 (ACM, 1996).
36. Bennett, C. H., Bernstein, E., Brassard, G. & Vazirani, U. Strengths and weaknesses of quantum computing. *SIAM J. Comput.* **26**, 1510–1523 (1997).
37. Gilyén, A., Su, Y., Low, G. H. & Wiebe, N. Quantum singular value transformation and beyond: exponential improvements for quantum matrix arithmetics. In *Proc. 51st Annual ACM SIGACT Symposium on Theory of Computing* 193–204 (ACM, 2019).
38. Martyn, J. M., Rossi, Z. M., Tan, A. K. & Chuang, I. L. Grand unification of quantum algorithms. *PRX quantum* **2**, 040203 (2021).
39. Huang, H.-Y., Kueng, R. & Preskill, J. Information-theoretic bounds on quantum advantage in machine learning. *Phys. Rev. Lett.* **126**, 190505 (2021).
40. Huang, H.-Y., Preskill, J. & Soleimanifar, M. Certifying almost all quantum states with few single-qubit measurements. In *Proc. IEEE 65th Annual Symposium on Foundations of Computer Science (FOCS)* 1202–1206 (IEEE, 2024).
41. Dyson, F. J. The threefold way. algebraic structure of symmetry groups and ensembles in quantum mechanics. *J. Math. Phys.* **3**, 1199–1215 (1962).
42. Brandao, F. G., Harrow, A. W. & Horodecki, M. Local random quantum circuits are approximate polynomial-designs. *Commun. Math. Phys.* **346**, 397–434 (2016).
43. Schuster, T., Haferkamp, J. & Huang, H.-Y. Random unitaries in extremely low depth. *Science* **389**, 92–96 (2025).
44. Dyson, F. J. A Brownian-motion model for the eigenvalues of a random matrix. *J. Math. Phys.* **3**, 1191–1198 (1962).
45. Dumitriua, I. & Edelmanb, A. Matrix models for beta ensembles. *J. Math. Phys.* **43**, 11 (2002).
46. Acharya, R. et al. Quantum error correction below the surface code threshold. *Nature* **638**, 920–926 (2024).
47. Liu, Z.-H. et al. Quantum learning advantage on a scalable photonic platform. *Science* **389**, 1332–1335 (2025).

Acknowledgements

S.J. and C.O. were supported by the National Research Foundation of Korea Grants (No. RS-2024-00431768 and No. RS-2025-00515456) funded by the Korean government (Ministry of Science and ICT (MSIT)) and the Institute of Information & Communications Technology Planning & Evaluation (IITP) Grants funded by the Korea government (MSIT) (No. IITP-2025-RS-2025-02283189 and IITP-2025-RS-2025-02263264).

Author contributions

S.J. and C.O. led and analyzed the main results. S.J. wrote the manuscript, and C.O. revised it.

Competing interests

The authors declare no competing interests.

Additional information

Supplementary information The online version contains supplementary material available at https://doi.org/10.1038/s41534-025-01135-5.

Correspondence and requests for materials should be addressed to Sangwoo Jeon or Changhun Oh.

Reprints and permissions information is available at http://www.nature.com/reprints

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.