

Exponential speedup in measurement property learning with post-measurement states

I. INTRODUCTION

Every quantum information processing task can essentially be decomposed into three stages: State initialization, quantum evolution, and measurement. Learning the properties of these stages underlies a wide range of tasks in quantum information processing, and hence substantial effort is dedicated to this task in various settings, let this be in notions of benchmarking [1], certification [2, 3] and others. Owing to the intrinsic constraints of quantum mechanics, such as the interplay of disturbance and information gain, extracting information from quantum systems is subject to fundamental limits [4, 5]. Identifying the precise quantum resources that can reduce these costs is, therefore, of both foundational and practical importance in the quantum technologies. For quantum state and channel learning, extensive progress has been made in this direction, revealing resources that yield polynomial or even exponential query complexity speedups. Representative examples include entangled operations for estimating state purity and Pauli expectation values [6–11], auxiliary qubits and coherent queries for estimating channel unitarity and Pauli coefficients [12–15], and adaptive strategies for quantum tomography [16, 17]. Conjugate states [18], pure dilation states [19], and inverse unitaries [20] are also shown to be crucial resources in a wide range of tasks.

Measurement plays a distinctive role as the final step of any quantum information processing task, serving as the interface between quantum systems and classical data. In practical settings, high-quality measurement is essential for quantum randomness generation [21, 22], quantum error correction [23], and quantum metrology [24]. Despite this central importance, existing studies on measurement learning mainly focus on tomography-based protocol design, commonly referred to as “detector tomography” [25–29], various forms of hypothesis testing [30–33], and metrology [34]. While recent studies have successfully leveraged entangled operations to achieve polynomial speedups in detector tomography [35, 36], the specific quantum resources required to unlock *exponential*

speedups in measurement learning remain largely unexplored.

In this work, we identify a measurement property, sharpness, whose estimation query complexity exhibits an exponential separation depending on access to the post-measurement quantum state. Interestingly, this advantage cannot be replicated by conventional resources that are powerful for state and channel learning, such as entangled operations, auxiliary qubits, or adaptive strategies. Specifically, we prove that, with merely having access to measurement outcomes, at least $\Omega(\sqrt{d})$ queries, where d denotes the system dimension, are necessary to distinguish a genuine projective measurement in a random basis from a classical random number generator. This hardness result holds for arbitrary quantum protocols and can be viewed as a quantum generalization of the birthday paradox. In contrast, when the post-measurement quantum states are also accessible, the same task can be solved with constant query complexity, independent of the system size, establishing a strict separation between the two settings. The protocol simply performs two identical successive measurements on the maximally mixed state, without entanglement, auxiliary systems, or adaptivity. Taken together, our results identify a measurement learning task in which conventional resources for state and channel learning are ineffective, while post-measurement states constitute the decisive resource enabling an exponential reduction in query complexity.

II. MEASUREMENT LEARNING

In practice, quantum measurements can be broadly classified into two types: *destructive measurements*, which output only classical measurement outcomes, and *non-destructive measurements* or quantum instruments [37], which additionally provide access to the post-measurement quantum state. A quantum measurement can be described with a set of measurement or Kraus operators $\{K_i\}_i$ satisfying $\sum_i K_i^\dagger K_i = \mathbb{I}$. When performing the measurement on a quantum state ρ , the probability for outputting the result i is $p_i = \text{Tr}(\rho K_i^\dagger K_i)$ and the post-measurement state is

$$\rho_i = \frac{K_i \rho K_i^\dagger}{\text{Tr}(K_i \rho K_i^\dagger)}. \quad (1)$$

A *positive operator-valued measure* (POVM) is a set of positive semi-definite operators $\{M_i\}_i$ satisfying $\sum_i M_i = \mathbb{I}$. The probability of getting the result i is then $\text{Tr}(\rho M_i)$, without specifying the post-measurement state. Given a set of measurement operators $\{K_i\}_i$, the corresponding POVM is $\{M_i = K_i^\dagger K_i\}_i$. Given a set of POVM operators, there is no unique set of measurement operators that corresponds to it.

For quantum measurements, we say a measurement is “sharp” if it is close to a projective measurement for which repeated measurements will only yield the same result [38, 39].

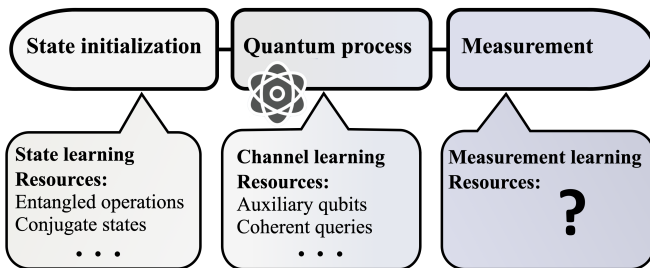


Figure 1. A quantum information processing task consists of state initialization, quantum evolution, and measurement. Although various quantum resources have been identified that yield exponential speedups for state and channel learning, the resource structure of measurement learning remains largely unexplored.

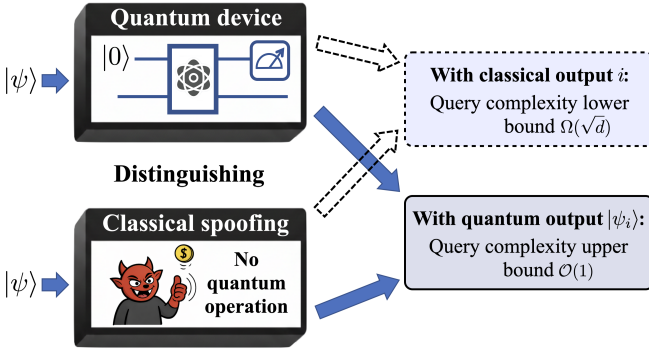


Figure 2. The black box distinguishing task.

This is what von Neumann has been referring to as a measurement of the first kind. Conversely, a measurement is called “fuzzy” when there is more uncertainty in the outcomes of consecutive measurements. Hence, we can define a quantity that faithfully characterizes how close a given POVM is from projective measurement as

$$\mathcal{S}(\{M_i\}_i) := \frac{1}{d} \sum_i \text{Tr}(M_i^2). \quad (2)$$

In the remainder of this work, we will simply refer to this as the *sharpness* of the measurement. It can be easily proved that $\mathcal{S}(\{M_i\}_i)$ reaches its maximum, 1, if and only if the measurement is quantum projective measurements with $M_i M_j = M_i \delta_{i,j}$.

III. EXPONENTIAL LOWER BOUND WITH ONLY CLASSICAL OUTPUTS

To derive the query complexity lower bound for estimating sharpness, we study a black-box distinguishing problem, as shown in Fig. 2. Here, multiple identical and independent copies of an unknown device are given and the tester can choose the input state and do further operations using the output of devices. The device may either faithfully perform a quantum projective measurement in an unknown and randomly chosen basis, or produce outputs sampled from a purely classical probability distribution without executing any quantum operation, precisely put as a promise problem as follows.

Definition 1 (Black-box distinguishing task). *Given query access to a measurement device, the task is to distinguish between the following two scenarios, each occurring with equal prior probability:*

- (i) *The device outputs $i \in \{0, \dots, d-1\}$ uniformly at random and leaves the input state unchanged.*
- (ii) *The device performs a projective measurement with operators $\{\Pi_i = U |i\rangle\langle i| U^\dagger\}_{i=0}^{d-1}$ on the input state, where U is an unknown d -dimensional Haar random unitary, outputs the measurement result i , and collapses the input state to the corresponding post-measurement state.*

Notice that there exists a simple strategy to distinguish between these two kinds of black boxes using the birthday paradox, as shown in Fig. 3(a). In the uniform distribution case (i), when one samples for $\mathcal{O}(\sqrt{d})$ identical and independent times, with a constant probability, one will get a pair of identical outcomes. If we input a fixed pure state, like that defined by a computational basis vector $|0\rangle$, into the black box of case (ii), the output distribution is given by the *Porter–Thomas distribution*. When sampling for $\mathcal{O}(\sqrt{d})$ times, the probability for getting two identical outcomes is almost twice as the probability of case (i), as proven in Appendix ?? and Ref. [40]. Therefore, with sample complexity $\mathcal{O}(\sqrt{d})$, one can successfully distinguish these two different kinds of black boxes with a constant success probability even without any prior knowledge of the random unitary U .

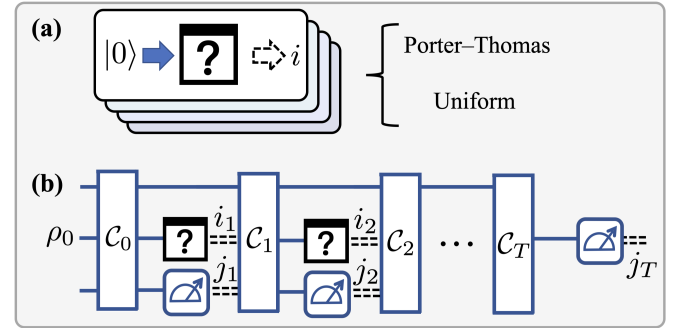


Figure 3. (a) A distinguishing protocol by inputting a fixed state and comparing the output distribution. (b) The most general distinguishing protocol utilizing adaptivity, auxiliary qubits, entangled operation, and controllable measurements. All the measurement outcomes, including the black box measurements and the controllable measurements, represented by blue boxes, will be utilized for the distinguishing task.

As mentioned before, quantum resources can speedup quantum learning tasks, such as entangled operations, coherent queries, and adaptivity. Note that the simple protocol shown in Fig. 3(a) does not utilize any one of these resources. Therefore, it is natural to ask whether one can achieve a better query complexity performance with these resources. We thus consider the most general certification protocol which allows any physical operations, including some controllable measurements in addition to the black box measurements, as shown in Fig. 3(b). Surprisingly, we theoretically prove that, even with the most general physical operations, the query complexity cannot break the lower bound of $\Omega(\sqrt{d})$.

Theorem 1 (Quantum birthday paradox). *For any quantum protocol, the query complexity for solving the task introduced in Definition 1 with only classical outputs with constant success probability is $\Omega(\sqrt{d})$.*

A direct corollary of this theorem is that, with only classical outputs, it is exponentially hard (in terms of query complexity) to align the outcome of random measurements. Specifically, even with arbitrary entangled operations and adaptive strategies or “quantum combs” [41], $\Omega(\sqrt{d})$ query complexity

is needed to see two identical outcomes. We thus regard this theorem as the quantum generalization of birthday paradox.

Note that for case (i), the POVM operators are all $\mathbb{I}/d$ and thus the sharpness is simply given by $1/d$. While for case (ii), the sharpness reaches its maximum value of 1 and the gap between cases (i) and (ii) is a constant. Therefore, if one can accurately estimate the measurement sharpness, one can also solve the distinguishing task. We can thus draw the following conclusion.

Corollary 1 (Query complexity bound). *If there exists a protocol that estimates the sharpness of any measurement to constant additive error with only classical outputs, the protocol must query the measurement at least $\Omega(\sqrt{d})$ times.*

IV. CONSTANT QUERY COMPLEXITY WITH HAVING ACCESS TO POST-MEASUREMENT STATES

If instead of resorting to destructive measurements, we have access to non-destructive measurement apparatus that allow for an access to the post-measurement state, then there exists a simple protocol to estimate the sharpness in our task without any entangled operations and adaptive strategies. The protocol then amounts to simply repeating the following steps:

1. Start by preparing the maximally mixed state $\rho = \mathbb{I}/d$.
2. Measure the state, record the result i and keep the post-measurement state $\rho_i = K_i K_i^\dagger / \text{Tr}(K_i K_i^\dagger)$.
3. Perform the same measurement on the state ρ_i to get the second measurement result j and calculate the probability that $i = j$.

According to the definition of quantum measurement, the probability we calculate is actually the unbiased estimator of the sharpness

$$p(i = j) = \sum_i p(i)p(j = i|i) = \mathcal{S}(\{M_i\}_i) \quad (3)$$

whenever we have $[K_i, K_i^\dagger] = 0$, which holds for the task defined in Definition 1. As the value of $p(i = j)$ is contained in the interval $[0, 1]$, the variance for single-shot estimation is upper bounded by some constant. Therefore, a constant repeating times is enough to estimate the sharpness with constant additive error. We thus arrive at the following conclusion.

Theorem 2 (Estimating sharpness). *There exists a protocol that estimates the sharpness with constant additive error and thus solves the task in Definition 1 with constant success probability using $\mathcal{O}(1)$ queries, provided that the black box outputs both classical outcomes and post-measurement quantum states defined in Eq. (1), and the measurement operators are normal operators.*

V. QUANTUMNESS CERTIFICATION

While before we have been concerned with the abstract question of deriving query complexity bounds, we now turn to the question of how this can be used in quantumness certification, and how the results may offer useful insights for the design of certifiable quantum devices. For certain classical computational problems, certification can rely on intrinsic mathematical structure. For instance, in Shor's algorithm for integer factorization [42], the output can be efficiently verified classically, the problem at hand being contained in NP. However, this paradigm does not extend to intrinsically quantum tasks such as quantum many-body simulation, where reliable certification would in general require trusted quantum operations of comparable complexity. Moreover, for non-computational tasks such as quantum random number generation [43], purely classical devices may mimic quantum output statistics, rendering certification based solely on classical outcomes fundamentally difficult [44, 45].

In digital quantum computing platforms, measurements are typically implemented as a unitary evolution U followed by a computational basis measurement. If measurements are restricted to a fixed and known basis, such as the computational basis, then even with access to post-measurement states, the distinguishing task remains exponentially hard by virtue of Theorem 1: Obviously, having access to the post-measurement state does not provide any additional information. However, if the device provider additionally supplies the inverse unitary $U^\dagger$ applied to the post-measurement state before releasing it, the client can implement the simple "measuring twice" protocol using only a maximally mixed state and a single bit of quantum randomness. In this way, quantumness can be certified with constant query complexity and minimal quantum capability on the verifier's side. This demonstrates how the resource identified in this work can be operationally leveraged in practical certification settings.

VI. DISCUSSION

At this point, we discuss the broader implications of our technical results. As stressed before, state preparation and measurement constitute the first and final stages of any quantum information processing task and exhibit a natural duality: For this reason, detector and state tomography can be seen as being dual to each other [16, 28, 35, 36]. Only on rare occasions, one can acquire knowledge about both at the same time [46]. It is, therefore, tempting to expect that similar quantum resources would be useful for both state learning and measurement learning, for instance, entangled operations for purity estimation. However, our results reveal a striking contrast and asymmetry in those tasks: There exist measurement learning tasks for which entangled operations provide no advantage when only classical measurement outcomes are available. In contrast, access to post-measurement quantum states enables an exponential query complexity speedup of order $\sqrt{d}$ through repeated measurements, paralleling the role of entangled operations in state purity estimation [7].

-
- [1] A. Hashim, L. B. Nguyen, N. Goss, B. Marinelli, R. K. Naik, T. Chistolini, J. Hines, J. Marceaux, Y. Kim, P. Gokhale, T. Tomesh, S. Chen, L. Jiang, S. Ferracin, K. Rudinger, T. Proctor, K. C. Young, I. Siddiqi, and R. Blume-Kohout, Practical introduction to benchmarking and characterization of quantum computers, *PRX Quantum* **6**, 030202 (2025).
 - [2] J. Eisert, D. Hangleiter, N. Walk, I. Roth, D. Markham, R. Parekh, U. Chabaud, and E. Kashefi, Quantum certification and benchmarking, *Nature Rev. Phys.* **2**, 382 (2020).
 - [3] M. Kliesch and I. Roth, Theory of quantum system certification, *PRX Quantum* **2**, 010201 (2021).
 - [4] C. W. Helstrom, *Quantum detection and estimation theory*, Mathematics in Science and Engineering, Vol. 123 (Academic Press, New York, 1976).
 - [5] A. Anshu and S. Arunachalam, A survey on the complexity of learning quantum states, *Nature Rev. Phys.* **6**, 59 (2024).
 - [6] D. Aharonov, J. Cotler, and X.-L. Qi, Quantum algorithmic measurement, *Nature Comm.* **13**, 887 (2022).
 - [7] S. Chen, J. Cotler, H.-Y. Huang, and J. Li, Exponential separations between learning with and without quantum memory, in *2021 IEEE 62nd Annual Symposium on Foundations of Computer Science (FOCS)* (2022) pp. 574–585.
 - [8] H.-Y. Huang, M. Broughton, J. Cotler, S. Chen, J. Li, M. Mohseni, H. Neven, R. Babbush, R. Kueng, J. Preskill, *et al.*, Quantum advantage in learning from experiments, *Science* **376**, 1182 (2022).
 - [9] S. Chen, W. Gong, and Q. Ye, Optimal tradeoffs for estimating Pauli observables, in *2024 IEEE 65th Annual Symposium on Foundations of Computer Science (FOCS)* (2024) pp. 1086–1105.
 - [10] W. Gong, J. Haferkamp, Q. Ye, and Z. Zhang, On the sample complexity of purity and inner product estimation, *arXiv preprint arXiv:2410.12712* (2024).
 - [11] R. King, D. Gosset, R. Kothari, and R. Babbush, Triply efficient shadow tomography, *PRX Quantum* **6**, 010336.
 - [12] K. Chen, Q. Wang, P. Long, and M. Ying, Unitarity estimation for quantum channels, *IEEE Trans. Inf. Th.* **69**, 5116 (2023).
 - [13] S. Chen, S. Zhou, A. Seif, and L. Jiang, Quantum advantages for Pauli channel estimation, *Phys. Rev. A* **105**, 032435 (2022).
 - [14] S. Chen, C. Oh, S. Zhou, H.-Y. Huang, and L. Jiang, Tight bounds on Pauli channel learning without entanglement, *Phys. Rev. Lett.* **132**, 180805 (2024).
 - [15] S. Chen and W. Gong, Efficient Pauli channel estimation with logarithmic quantum memory, *PRX Quantum* **6**, 020323 (2025).
 - [16] S. Chen, B. Huang, J. Li, A. Liu, and M. Sellke, When does adaptivity help for quantum state learning?, in *2023 IEEE 64th Annual Symposium on Foundations of Computer Science (FOCS)* (2023) pp. 391–404.
 - [17] S. Chen, W. Gong, and Z. Zhang, Adaptivity can help exponentially for shadow tomography, *arXiv preprint arXiv:2412.19022* (2024).
 - [18] R. King, K. Wan, and J. R. McClean, Exponential learning advantages with conjugate states and minimal quantum memory, *PRX Quantum* **5**, 040301 (2024).
 - [19] Z. Liu, W. Gong, Z. Du, and Cai, Exponential separations between quantum learning with and without purification, *arXiv preprint arXiv:2410.17718* (2024).
 - [20] E. Tang and J. Wright, Amplitude amplification and estimation require inverses, *arXiv preprint arXiv:2507.23787* (2025).
 - [21] G. Senno, T. Strohm, and A. Acín, Quantifying the intrinsic randomness of quantum measurements, *Phys. Rev. Lett.* **131**, 130202 (2023).
 - [22] H. Dai, B. Chen, X. Zhang, and X. Ma, Intrinsic randomness under general quantum measurements, *Phys. Rev. Res.* **5**, 033081 (2023).
 - [23] A. deMarti iOlius, P. Fuentes, R. Orús, P. M. Crespo, and J. Etchezarreta Martinez, Decoding algorithms for surface codes, *Quantum* **8**, 1498 (2024).
 - [24] V. Giovannetti, S. Lloyd, and L. Maccone, Quantum-enhanced measurements: Beating the standard quantum limit, *Science* **306**, 1330 (2004).
 - [25] A. Luis and L. L. Sánchez-Soto, Complete characterization of arbitrary quantum measurement processes, *Phys. Rev. Lett.* **83**, 3573 (1999).
 - [26] J. Fiurášek, Maximum-likelihood estimation of quantum measurement, *Phys. Rev. A* **64**, 024102 (2001).
 - [27] G. M. D’Ariano, L. Maccone, and P. L. Presti, Quantum calibration of measurement instrumentation, *Phys. Rev. Lett.* **93**, 250407 (2004).
 - [28] J. S. Lundeen, A. Feito, H. Coldenstrodt-Ronge, K. L. Pregnell, C. Silberhorn, T. C. Ralph, J. Eisert, M. B. Plenio, and I. A. Walmsley, Tomography of quantum detectors, *Nature Phys.* **5**, 27 (2009).
 - [29] A. Feito, J. S. Lundeen, H. Coldenstrodt-Ronge, J. Eisert, M. B. Plenio, and I. A. Walmsley, Measuring measurement: Theory and practice, *New J. Phys.* **11**, 093038 (2009).
 - [30] A. Bisio, G. M. D’Ariano, P. Perinotti, and M. Sedlák, Quantum learning algorithms for quantum measurements, *Phys. Lett. A* **375**, 3425 (2011).
 - [31] M. Sedlák and M. Ziman, Optimal single-shot strategies for discrimination of quantum measurements, *Phys. Rev. A* **90**, 052312 (2014).
 - [32] H.-C. Cheng, M.-H. Hsieh, and P.-C. Yeh, The learnability of unknown quantum measurements, *arXiv preprint arXiv:1501.00559* (2015).
 - [33] Z. Puchała, L. Pawela, A. Krawiec, and R. Kukulski, Strategies for optimal single-shot discrimination of quantum measurements, *Phys. Rev. A* **98**, 042103 (2018).
 - [34] A. Das, S. K. Yung, L. O. Conlon, Ö. Erkiş, A. Walsh, Y.-S. Kim, P. K. Lam, S. M. Assad, and J. Zhao, Precision bounds for characterising quantum measurements, *Nature Communications* **17**, 1821 (2026).
 - [35] L. Zambrano, S. Ramos-Calderer, and R. Kueng, Fast quantum measurement tomography with dimension-optimal error bounds, *arXiv preprint arXiv:2507.04500* (2025).
 - [36] A. A. Mele and L. Bittel, Optimal learning of quantum channels in diamond distance, *arXiv preprint arXiv:2512.10214* (2025).
 - [37] E. B. Davies and J. T. Lewis, An operational approach to quantum probability, *Comm. Math. Phys.* **17**, 239 (1970).
 - [38] F. Buscemi, K. Kobayashi, and S. Minagawa, A complete and operational resource theory of measurement sharpness, *Quantum* **8**, 1235 (2024).
 - [39] N. Saberian, S. J. Akhtarshenas, and F. Shahbeigi, Measurement sharpness and disturbance tradeoff, *Phys. Rev. A* **109**, 012201 (2024).
 - [40] A. Mari, Counting collisions in random circuit sampling for benchmarking quantum computers, *APL Quantum* **1** (2024).
 - [41] G. A. L. White, P. Jurcevic, C. D. Hill, and K. Modi, Unifying non-Markovian characterization with an efficient and self-consistent framework, *Phys. Rev. X* **15**, 021047 (2025).

- [42] P. W. Shor, Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer, *SIAM Rev.* **41**, 303 (1999).
- [43] M. Herrero-Collantes and J. C. Garcia-Escartin, Quantum random number generators, *Rev. Mod. Phys.* **89**, 015004 (2017).
- [44] S. Pironio, A. Acín, S. Massar, A. B. de la Giroday, D. N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. A. Manning, and C. Monroe, Random numbers certified by Bell's theorem, *Nature* **464**, 1021 (2010).
- [45] S. Mal, M. Banik, and S. K. Choudhary, Temporal correlations and device-independent randomness, *Quantum Information Processing* **15**, 2993 (2016).
- [46] I. Roth, J. Wilkens, D. Hangleiter, and J. Eisert, Semi-device-dependent blind quantum tomography, *Quantum* **7**, 1053 (2023).