

Extended abstract for QTML 2026 submission: Optimal randomized measurements for a family of non-linear quantum properties

Zhenyu Du, Yifan Tang, Andreas Elben, Ingo Roth, Jens Eisert, and Zhenhuan Liu

Note: the technical version is accepted by [PRX Quantum](#).

MOTIVATION

Quantum learning is pivotal for both verifying and extracting information from quantum systems, addressing the growing demands of quantum technologies while at the same time enabling transformative applications [1–4]. To date, by far the majority of quantum learning theory has focused on the estimation of linear properties of quantum states. However, non-linear properties, like the state purity $\text{Tr}(\rho^2)$ and the non-linear expectation value $\text{Tr}(O\rho^2)$, play vital roles in quantum simulation for virtual cooling [5, 6], quantum error mitigation [7–9], and instances of quantum algorithms [10, 11]. Specifically, estimating $\text{Tr}(O\rho^2)/\text{Tr}(\rho^2)$ yields estimates of a quantum system at a lower temperature than the physically prepared thermal state, thereby suppressing potential incoherent noise. Further applications include inferring entropic quantities and the quantum Fisher information of an unknown quantum state [12, 13] and detecting quantum phases of matter in mixed states [14–16].

Yet, the intrinsic linearity of quantum mechanics renders the estimation of non-linear properties considerably more challenging than that of a linear expectation value $\text{Tr}(O\rho)$ of an observable O . For linear estimation, directly measuring single state copies in the observable’s eigenbasis has optimal sample complexity in the Hilbert space dimension d . While quantum memory enables entangled measurements across multiple state copies, such resources only offer exponential advantage in more complex tasks [10, 17–19]. In contrast, when estimating a non-linear property like $\text{Tr}(O\rho^2)$, directly applying observable-driven techniques from linear estimation unavoidably requires coherently-controlled quantum memory [20–27] and renders implementations on quantum devices challenging [24–26].

Existing protocols using only single-copy quantum operations instead resort to general informationally complete measurements, independent of the observable [28, 29] and post-process tensor products of so-called *classical shadows* of the state [30]. On the one hand, these CS-based protocols require $\mathcal{O}(d)$ state copies to accurately estimate $\text{Tr}(P\rho^2)$ for a Pauli operator P with a high probability. However, current lower bound of $\Omega(\sqrt{d})$ suggests that they are indeed sub-optimal [10]. On the other hand, the use of *randomized measurement* (RM) [2, 17, 18, 31–35] yields a sample complexity of $\mathcal{O}(\sqrt{d})$ for the special case of measuring state purity $\text{Tr}(\rho^2)$, which matches the lower bound and is thus optimal. But the case to estimate $\text{Tr}(O\rho^2)$ for a general observable O using only single state copies while maintaining an optimal sample complexity remains an open question:

How to optimize the sample complexity of estimating $\text{Tr}(O\rho^2)$ for a general observable O with single-copy operations of ρ only?

Another crucial quantity we care much about while designing practical quantum learning protocols is the number of experimental settings. Since in most quantum computing platforms, the time overhead of switching between experimental settings is typically orders of magnitude larger than the duration of a single measurement shot [36–39], so it is more favorable to fix a setting and perform many repetitions before changing it. In terms of RM protocols, we want to optimize the number of random unitaries drawn from an ensemble, or equivalently, the measurement bases. We are thus interested in:

How to optimize the number of random unitaries required for estimating $\text{Tr}(O\rho^2)$ for a general observable O with single-copy operations of ρ only?

MAIN RESULTS

In this work, we (partially) answer both questions by proposing protocols to measure $\text{Tr}(O\rho^2)$ for an arbitrary O with sample complexity $\mathcal{O}(\sqrt{d})$ and only $\mathcal{O}(1)$ measurement bases. In the case of O being Pauli operators, local observables, and stabilizer fidelities, we prove that essentially $\Omega(\sqrt{d})$ state copies are necessary for any single-copy RM protocol, ensuring that our protocol achieves the optimal sample complexity. Remarkably, it has a square-root improvement in sample complexity and exponentially reduces the number of measurement settings compared to the prevailing protocols based on classical shadows [30] while estimating Pauli observables. Our main findings are summarized as follows.

Estimating general observables. Our first result is the sample complexity to measure $\text{Tr}(O\rho^2)$ using a protocol that requires random unitaries sampled from a block-diagonal unitary 4-design. We consider an observable O subject to $\|O\|_\infty \leq 1$ (otherwise, we rescale O according to $O/\|O\|_\infty$). The main observation is that O can be approximately decomposed into the sum of dichotomic observables, with the number of terms logarithmic to the reciprocal of a given precision.

Lemma 1 (Dichotomic decomposition of general observables, Lemma 3 in the manuscript). *For any observable O satisfying $\|O\|_\infty \leq 1$, one can decompose O as*

$$O = \sum_{l=1}^k 2^{-l} O_l + O_\Delta, \quad (1)$$

where $k \in \mathbb{N}^+$, each O_l is a dichotomic observable with eigenvalues ± 1 , and $\|O_\Delta\|_\infty \leq 2^{-k}$.

The following theorem provides upper bounds for sample complexity and the number of measurement bases required of a single-copy RM protocol:

Theorem 1 (Estimating general observables, informal version of Theorem 2 in the manuscript). *Let O be an observable with $\|O\|_\infty \leq 1$ in $\mathcal{L}(\mathbb{C}^d)$, there exists a single-copy RM protocol (e.g., ORM), such that for any input state ρ in a d -dimensional qubit system, it estimates $\text{Tr}(O\rho^2)$ to within additive error ε with probability at least $1 - \delta$, with a sample complexity of*

$$\mathcal{O}\left(\max\left\{\frac{\sqrt{d}}{\varepsilon}, \frac{1}{\varepsilon^2}\right\} \log[\delta^{-1} \log(\varepsilon^{-1})]\right). \quad (2)$$

Specifically, the number of random unitaries required is $N_U = \mathcal{O}\left(\max\left\{1, \frac{1}{d\varepsilon^2}\right\} \log(\varepsilon^{-1})\right)$.

Our protocol shares several benefits with the RM protocol designed for purity estimation [2, 32]: the $\mathcal{O}(\sqrt{d})$ sample complexity and $\mathcal{O}(1)$ measurement bases are the same, which both are shown to be optimal among all single-copy protocols for purity estimation in Ref. [40]. Note that, when the estimation accuracy is not exponentially small, even a single measurement basis is enough to accurately estimate $\text{Tr}(O\rho^2)$. Besides, there is no need to record which unitary is implemented in the quantum data-obtaining process since the post-processing function is irrelevant to this information, and this further reduces potential error in the classical post-processing.

Our observable-driven protocol optimizes its procedure utilizing the preknowledge of the observable O . Thus, while estimating non-linear properties, it shows advantages in sample complexity and the number of measurement bases compared to other prevailing single-copy RM protocols, including the non-linear estimator based on classical shadows [30]. Furthermore, when O is a local (which has a support of $\mathcal{O}(1)$ size) or a Pauli observable, the sample complexity $\mathcal{O}(\sqrt{d})$ achieved by our protocol is provably optimal with the system dimension d [10, 41].

Estimating local observables and Pauli observables using Clifford circuit. Although our proposed ORM protocol applies to a general observable and achieves the optimal sample complexity in many cases, its practical application faces challenges. In the special case of estimating local Pauli observables, the difficulties could be significantly eased by implementing Clifford gates and performing a mid-circuit measurement.

Lemma 2 (Estimating traceless dichotomic observables with Clifford circuit, Lemma 4 in the manuscript). *Let O be a traceless dichotomic observable, i.e., the dimensions of its two eigenspaces are $d_+, d_- = d/2 = 2^{n-1}$, there exists a single-copy RM protocol using Clifford circuit and mid-circuit measurements, such that for any input n -qubit state ρ with $n \geq 3$, it estimates $\text{Tr}(O\rho^2)$ to additive error ε with probability at least $1 - \delta$, with a sample complexity of*

$$\mathcal{O}\left(\frac{\sqrt{d}}{\varepsilon^2} \log(\delta^{-1})\right). \quad (3)$$

Specifically, the number of repetitions is $T = \mathcal{O}(\log(\delta^{-1}))$, the number of random unitaries per repetition is $N_U = \mathcal{O}\left(\frac{1}{\varepsilon^2}\right)$, and the number of measurements per unitary is $N_M = \mathcal{O}(\sqrt{d})$.

Utilizing the Pauli sampling technique [42, 43], the non-linear expectation values of a wide range of observables can be estimated using efficient circuit implementation schemes while maintaining the $\mathcal{O}(\sqrt{d})$ sample complexity, which is again optimal for the local observables and Pauli observables [10, 41].

Theorem 2 (Estimating observables via Pauli sampling and block-diagonal Clifford gates, Theorem 3 in the manuscript). *Let O be an observable that admits a Pauli decomposition of K terms, there exists a single-copy RM protocol, such that for any input state ρ in a d -dimensional qubit system, it estimates $\text{Tr}(O\rho^2)$ to additive error ε with probability at least $1 - \delta$, with an expected sample complexity of*

$$\mathcal{O}\left(\frac{K\|O\|_2^2}{\sqrt{d}\varepsilon^2}\log(\delta^{-1})\right). \quad (4)$$

Estimating many low-rank observables. For the specific cases of low-rank observables (i.e., $\text{rank}(O) = \mathcal{O}(1)$), the classical shadow protocol has the same sample complexity of $\mathcal{O}(\sqrt{d})$ as ORM. Thanks to the use of the median-of-means estimator in post-processing, the classical shadow protocol has the favorable logarithmic scaling in simultaneously estimating multiple non-linear quantities, while it scales linearly for ORM. Our third result is the BRM protocol, which has the same sample complexity as the classical shadow but exponentially reduces the number of measurement bases while estimating many low-rank observables.

Theorem 3 (Estimating many low-rank observables, informal version of Theorem 4 in the manuscript). *Let $\{O_m\}_{m=1}^M$ be a collection of observables satisfying $\text{Tr}(O_m^2) = \mathcal{O}(1)$ for all i , there exists a single-copy RM protocol (e.g., BRM), such that for an input state ρ in a d -dimension system, it simultaneously estimates all quantities $\text{Tr}(O_m\rho^2)$ to additive error at most $\varepsilon > 0$ with probability at least $1 - \delta$, with a sample complexity of $\mathcal{O}(\sqrt{d}\varepsilon^{-2}\log(\frac{M}{\delta}))$. Specifically, the number of random unitaries required is $N_U = \mathcal{O}(\varepsilon^{-2})$.*

Summary. Our proposed protocols, both ORM and BRM, remarkably reduce the number of required measurement bases to a constant number, compared to the exponentially many with system size in classical shadow. When O is a local or Pauli observable, the sample complexity achieved by ORM using a Clifford circuit is theoretically optimal among all single-copy RM protocols. BRM also shares the favorable scaling in simultaneously estimating multiple observables with classical shadow.

	Sample complexity	Measurement bases	Random unitary	Information of unitary?	Estimating M independent observables
Classical Shadow [30]	$\mathcal{O}(\sqrt{d\text{Tr}(O^2)})$	$\mathcal{O}(\sqrt{d\text{Tr}(O^2)})$	Unitary 3-design	Yes	$\mathcal{O}(\log M)$
ORM (this work)	$\mathcal{O}(\sqrt{d})$	$\mathcal{O}(1)$	Block-diagonal unitary 4-design	No	$\mathcal{O}(M)$
ORM for local O or Pauli O (this work)	$\mathcal{O}(\sqrt{d})$ (optimal)	$\mathcal{O}(1)$	Clifford	No	$\mathcal{O}(M)$
BRM (this work)	$\mathcal{O}(\sqrt{d\text{Tr}(O^2)})$	$\mathcal{O}(1)$	Unitary 6-design	Yes	$\mathcal{O}(\log M)$

TABLE I: The comparison of different protocols in estimating $\text{Tr}(O\rho^2)$ with constant additive error and failure probability.

DISCUSSION

Our work proposes several single-copy protocols for the estimation of non-linear properties in the form of $\text{Tr}(O\rho^2)$. We prove the optimality of sample complexity for all Pauli observables, matching the complexity bounds and thus closing a gap in the literature of quantum learning theory. Furthermore, our protocols remarkably reduce the number of measurement bases required to reach the same precision compared to prevailing RM protocols. The protocols are presented in an implementable form and have several potential applications, including quantum error mitigation and quantum virtual cooling. We believe our work will be of interest to both theorists studying quantum learning, simulation, and many-body physics, and experimentalists implementing quantum protocols in near-term quantum platforms. We hope it fits well in the topic of “Theoretical foundations of quantum learning” for QTML 2026.

-
- [1] J. Eisert, D. Hangleiter, N. Walk, I. Roth, D. Markham, R. Parekh, U. Chabaud, and E. Kashefi, Quantum certification and benchmarking, *Nat. Rev. Phys.* **2**, 382 (2020).
 - [2] A. Elben, B. Vermersch, C. F. Roos, and P. Zoller, Statistical correlations between locally randomized measurements: A toolbox for probing entanglement in many-body quantum states, *Phys. Rev. A* **99**, 052323 (2019).
 - [3] M. Kliesch and I. Roth, Theory of quantum system certification, *PRX Quantum* **2**, 010201 (2021).
 - [4] M. Cerezo, G. Verdon, H.-Y. Huang, L. Cincio, and P. J. Coles, Challenges and opportunities in quantum machine learning, *Nat. Comput. Sci.* **2**, 567 (2022).
 - [5] A. M. Kaufman, M. E. Tai, A. Lukin, M. Rispoli, R. Schittko, P. M. Preiss, and M. Greiner, Quantum thermalization through entanglement in an isolated many-body system, *Science* **353**, 794 (2016).
 - [6] J. Cotler, S. Choi, A. Lukin, H. Gharibyan, T. Grover, M. E. Tai, M. Rispoli, R. Schittko, P. M. Preiss, A. M. Kaufman, M. Greiner, H. Pichler, and P. Hayden, Quantum virtual cooling, *Phys. Rev. X* **9**, 031013 (2019).
 - [7] Z. Cai, R. Babbush, S. C. Benjamin, S. Endo, W. J. Huggins, Y. Li, J. R. McClean, and T. E. O'Brien, Quantum error mitigation, *Rev. Mod. Phys.* **95**, 045005 (2023).
 - [8] W. J. Huggins, S. McArdle, T. E. O'Brien, J. Lee, N. C. Rubin, S. Boixo, K. B. Whaley, R. Babbush, and J. R. McClean, Virtual distillation for quantum error mitigation, *Phys. Rev. X* **11**, 041036 (2021).
 - [9] B. Koczor, Exponential error suppression for near-term quantum devices, *Phys. Rev. X* **11**, 031057 (2021).
 - [10] H.-Y. Huang, M. Broughton, J. Cotler, S. Chen, J. Li, M. Mohseni, H. Neven, R. Babbush, R. Kueng, J. Preskill, and J. R. McClean, Quantum advantage in learning from experiments, *Science* **376**, 1182–1186 (2022).
 - [11] S. Lloyd, M. Mohseni, and P. Rebentrost, Quantum principal component analysis, *Nat. Phys.* **10**, 631 (2014).
 - [12] A. Rath, C. Branciard, A. Minguzzi, and B. Vermersch, Quantum fisher information from randomized measurements, *Phys. Rev. Lett.* **127**, 260501 (2021).
 - [13] M. Yu, D. Li, J. Wang, Y. Chu, P. Yang, M. Gong, N. Goldman, and J. Cai, Experimental estimation of the quantum fisher information from randomized measurements, *arXiv:2104.00519* (2021).
 - [14] J. Y. Lee, C.-M. Jian, and C. Xu, Quantum criticality under decoherence or weak measurement, *PRX Quantum* **4**, 030317 (2023).
 - [15] J. Y. Lee, Y.-Z. You, and C. Xu, Symmetry protected topological phases under decoherence, *Quantum* **9**, 1607 (2025).
 - [16] Y. Zhang, T. H. Hsieh, Y. B. Kim, and Y. Zou, Probing mixed-state phases on a quantum computer via renyi correlators and variational decoding, *arXiv:2505.02900* (2025).
 - [17] D. Aharonov, J. Cotler, and X.-L. Qi, Quantum algorithmic measurement, *Nat. Commun.* **13**, 887 (2022).
 - [18] S. Chen, J. Cotler, H.-Y. Huang, and J. Li, Exponential separations between learning with and without quantum memory, in *Proc. 62nd Annu. IEEE Symp. Found. Comput. Sci. (FOCS)* (2022) pp. 574–585.
 - [19] W. Gong, J. Haferkamp, Q. Ye, and Z. Zhang, On the sample complexity of purity and inner product estimation, *arXiv:2410.12712* (2024).
 - [20] A. Barenco, A. Berthiaume, D. Deutsch, A. Ekert, R. Jozsa, and C. Macchiavello, Stabilization of quantum computations by symmetrization, *SIAM J. Comput.* **26**, 1541 (1997).
 - [21] H. Buhrman, R. Cleve, J. Watrous, and R. de Wolf, Quantum fingerprinting, *Phys. Rev. Lett.* **87**, 167902 (2001).
 - [22] A. K. Ekert, C. M. Alves, D. K. L. Oi, M. Horodecki, P. Horodecki, and L. C. Kwek, Direct estimations of linear and nonlinear functionals of a quantum state, *Phys. Rev. Lett.* **88**, 217901 (2002).
 - [23] R. Islam, R. Ma, P. M. Preiss, M. Eric Tai, A. Lukin, M. Rispoli, and M. Greiner, Measuring entanglement entropy in a quantum many-body system, *Nature* **528**, 77 (2015).
 - [24] Y. Zhou and Z. Liu, A hybrid framework for estimating nonlinear functions of quantum states, *npj Quantum Inf.* **10**, 62 (2024).
 - [25] Q. Liu, Z. Li, X. Yuan, H. Zhu, and Y. Zhou, Auxiliary-free replica shadow estimation, *arXiv:2407.20865* (2024).
 - [26] D. Miller, K. Levi, L. Postler, A. Steiner, L. Bittel, G. A. L. White, Y. Tang, E. J. Kuehnke, A. A. Mele, S. Khatri, L. Leone, J. Carrasco, C. D. Marciniak, I. Pogorelov, M. Guevara-Bertsch, R. Freund, R. Blatt, P. Schindler, T. Monz, M. Ringbauer, and J. Eisert, Experimental measurement and a physical interpretation of quantum shadow enumerators, *arXiv:2408.16914* (2024).
 - [27] H. Yao, Y. Liu, T. Lin, and X. Wang, Nonlinear functions of quantum states, *arXiv:2412.01696* (2024).
 - [28] A. Elben, R. Kueng, H.-Y. R. Huang, R. van Bijnen, C. Kokail, M. Dalmonte, P. Calabrese, B. Kraus, J. Preskill, P. Zoller, and B. Vermersch, Mixed-state entanglement from local randomized measurements, *Phys. Rev. Lett.* **125**, 200501 (2020).
 - [29] V. Vitale, A. Rath, P. Jurcevic, A. Elben, C. Branciard, and B. Vermersch, Robust estimation of the quantum fisher information on a quantum processor, *PRX Quantum* **5**, 030338 (2024).
 - [30] H.-Y. Huang, R. Kueng, and J. Preskill, Predicting many properties of a quantum system from very few measurements, *Nat. Phys.* **16**, 1050 (2020).
 - [31] S. J. van Enk and C. W. J. Beenakker, Measuring $\text{Tr} \rho^n$ on single copies of ρ using random measurements, *Phys. Rev. Lett.* **108**, 110503 (2012).
 - [32] T. Brydges, A. Elben, P. Jurcevic, B. Vermersch, C. Maier, B. P. Lanyon, P. Zoller, R. Blatt, and C. F. Roos, Probing Rényi entanglement entropy via randomized measurements, *Science* **364**, 260 (2019).
 - [33] A. Elben, S. T. Flammia, H.-Y. Huang, R. Kueng, J. Preskill, B. Vermersch, and P. Zoller, The randomized measurement toolbox, *Nat. Rev. Phys.* **5**, 9 (2023).

- [34] P. Cieřliński, S. Imai, J. Dziewior, O. Gühne, L. Knips, W. Laskowski, J. Meinecke, T. Paterek, and T. Vértesi, Analysing quantum systems with randomised measurements, *Phys. Rep.* **1095**, 1 (2024), analysing quantum systems with randomised measurements.
- [35] M. Ohliger, V. Nesme, and J. Eisert, Efficient and feasible state tomography of quantum many-body systems, *New J. Phys.* **15**, 015024 (2013).
- [36] A. H. Myerson, D. J. Szwer, S. C. Webster, D. T. C. Allcock, M. J. Curtis, G. Imreh, J. A. Sherman, D. N. Stacey, A. M. Steane, and D. M. Lucas, High-fidelity readout of trapped-ion qubits, *Phys. Rev. Lett.* **100**, 200502 (2008).
- [37] F. Lenzini, J. Janousek, O. Thearle, M. Villa, B. Haylock, S. Kasture, L. Cui, H.-P. Phan, D. V. Dao, H. Yonezawa, P. K. Lam, E. H. Huntington, and M. Lobino, Integrated photonic platform for quantum information with continuous variables, *Science Advances* **4**, eaat9331 (2018), <https://www.science.org/doi/pdf/10.1126/sciadv.aat9331>.
- [38] R. Dassonneville, T. Ramos, V. Milchakov, L. Planat, E. Dumur, F. Foroughi, J. Puertas, S. Leger, K. Bharadwaj, J. Delaforce, C. Naud, W. Hasch-Guichard, J. J. García-Ripoll, N. Roch, and O. Buisson, Fast high-fidelity quantum nondemolition qubit readout via a nonperturbative cross-kerr coupling, *Phys. Rev. X* **10**, 011045 (2020).
- [39] A. Opremcak, C. H. Liu, C. Wilen, K. Okubo, B. G. Christensen, D. Sank, T. C. White, A. Vainsencher, M. Giustina, A. Megrant, B. Burkett, B. L. T. Plourde, and R. McDermott, High-fidelity measurement of a superconducting qubit using an on-chip microwave photon counter, *Phys. Rev. X* **11**, 011027 (2021).
- [40] A. Anshu, Z. Landau, and Y. Liu, Distributed quantum inner product estimation, in *Proc. 54th Annu. ACM Symp. Theory Comput.*, STOC 2022 (Association for Computing Machinery, New York, NY, USA, 2022) p. 44–51.
- [41] Q. Ye, Z. Liu, and D.-L. Deng, Exponential advantage from one more replica in estimating nonlinear properties of quantum states, *arXiv:2509.24000* (2025).
- [42] S. T. Flammia and Y.-K. Liu, Direct fidelity estimation from few pauli measurements, *Phys. Rev. Lett.* **106**, 230501 (2011).
- [43] H.-Y. Huang, R. Kueng, and J. Preskill, Efficient estimation of pauli observables by derandomization, *Phys. Rev. Lett.* **127**, 030503 (2021).