In the Shadow of the Hadamard Test: Using the Garbage State for Good and Further Modifications

Paul K. Faehrmann,[1,2] Jens Eisert,[1,3] and Richard Kueng[2]

[1]*Dahlem Center for Complex Quantum Systems, Freie Universität Berlin, 14195 Berlin, Germany*

[2]*Institute for Integrated Circuits and Quantum Computing, Johannes Kepler University Linz, Linz, Austria*

[3]*Helmholtz-Zentrum Berlin für Materialien und Energie, Hahn-Meitner-Platz 1, 14109 Berlin, Germany*

(Received 25 June 2025; accepted 24 September 2025; published 9 October 2025)

The Hadamard test is one of the pillars on which quantum algorithm development rests and, at the same time, is naturally suited for the intermediate regime between the current era of noisy quantum devices and complete fault tolerance. Its applications use measurements of the auxiliary qubit to extract information but disregard the system register completely. Concomitantly, but independently of this development, advances in quantum learning theory have enabled the efficient representation of quantum states via classical shadows. This Letter shows that, strikingly, putting both lines of thought into a new context results in substantial improvements to the Hadamard test on a single auxiliary readout qubit, by suitably exploiting classical shadows on the remaining n-qubit work register. We argue that this combination inherits the best of both worlds and discuss statistical phase estimation as a vignette application. At the same time, the framework is more general and applicable to a wide range of other algorithms. There, we can use the Hadamard test to estimate energies on the auxiliary qubit, while classical shadows on the system register provide access to additional features such as (i) the fidelity of the initial state with certain pure quantum states, (ii) the initial state's energy, and (iii) how pure and how close the initial state is to an eigenstate of the Hamiltonian. Finally, we also discuss how anticontrolled unitaries can further augment this framework and explain how this Letter settles the exploitation of the Hadamard test for intermediate applications.

DOI: 10.1103/cqjw-kl8s

After the recent demonstration of the first logical quantum computations [1–5], we are on the verge of leaving the era of noisy, intermediate-scale quantum devices [6] and entering the era of early fault tolerance or *intermediate scale-quantum devices* [7] and the *megaquop machine* [8], a quantum device that can perform of the order of a million of quantum operations. With only a few error-corrected qubits but intermediate-sized quantum devices available, a natural next step is to combine noisy and error-corrected registers to implement more and more intricate quantum algorithms [9]. Thus, the question arises as to which quantum algorithms best suit these architectures and how to bridge the gap between noisy devices and a fully fault-tolerant quantum computer.

Arguably, the Hadamard test and variations thereof—being among the core primitives of modern quantum algorithm design [10,11]—are ideal candidates because they use a single auxiliary qubit that gets entangled with all other qubits: But then, only this qubit is measured in the end. Its ability to be used as a key subroutine in algorithms that classically combine measurements to reconstruct expectation values of linear combinations of unitaries has sparked the development of several quantum algorithms aimed at resource-efficient energy estimation [12–19], sampling from matrix functions such as for solving linear systems [20], quantum dynamics [21], Gibbs state preparation or properties thereof [20,22–24], estimating dynamical correlations via Green's functions [20,25], linear response of quantum systems [26], computing the density of states [27], entanglement spectroscopy and the estimation of α-Renyi entropies [28,29], estimating matrix elements of certain unitary irreducible representations of groups [30], and approximating the Jones polynomial [31,32], as well as giving rise to the *one clean qubit model of quantum computation* [33].

Furthermore, allowing for additional auxiliary qubits and circuit depth, the Hadamard test can be extended to make use of the existing resources both in the intermediate fault-tolerant regime [34] or in the far-term application of the original quantum phase estimation algorithm [35] or even simplified using phase retrieval techniques to avoid the controlled unitary [36]. These algorithms mostly use adaptations of the Hadamard test by measuring the auxiliary qubit to estimate expectation values of the form $\mathrm{tr}(e^{iHt_i}\rho)$ for some Hamiltonian H and state ρ with different evolution times t_i to

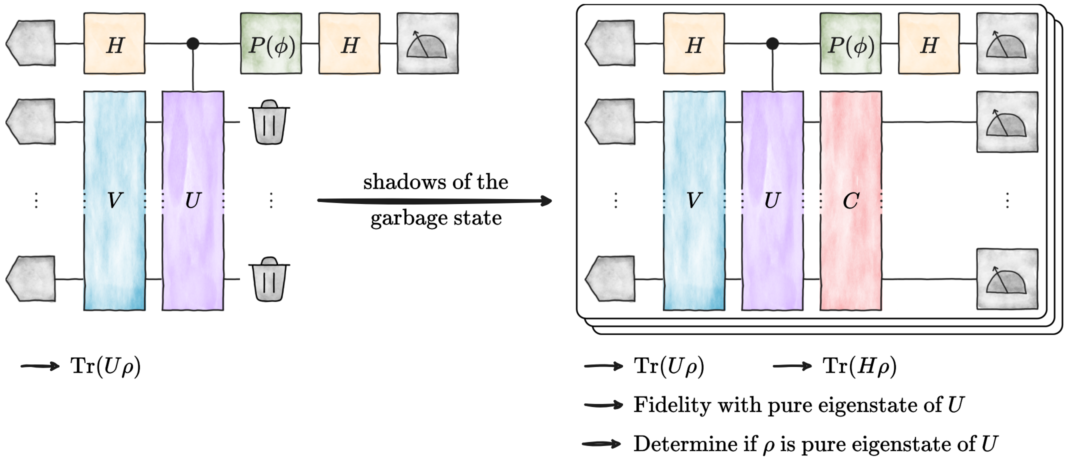

FIG. 1. Cartoon illustration of the proposed adaptation of the Hadamard test: Left: the standard Hadamard test circuit allows for the estimation of $\mathrm{Re}[\mathrm{tr}(U\rho)]$ or $\mathrm{Im}[\mathrm{tr}(U\rho)]$ when using $\phi = 0$ and $\phi = \pi/2$, respectively. Here, V labels the state preparation unitary, but the state can also be mixed. Right: instead of disregarding the system register, we can perform local or global shadow estimation of the postmeasurement state by applying random local or global Clifford gates (C) and, thereby, extract so-far-unused information.

construct Fourier approximations $F(H, t)$ of desired spectral functions in classical postprocessing. However, only information from the auxiliary qubit is extracted for this trace estimation, since the garbled postmeasurement state of the system register is of no apparent use. Notable exceptions are applications using system register measurements for error mitigation within verified phase estimation [37,38] and the combination of the generalized swap test with shadows on the copies of the input state [39].

At the same time, the advent of classical shadows as a tool to efficiently construct approximate classical descriptions of quantum states using very few measurements has impressively showcased the fundamental power of quantum measurements in conjunction with classical postprocessing [40–43], leading to hybrid quantum-classical algorithms enhancing quantum devices with classical shadows [39,44–46]. After the recent breakthrough of Ref. [47] and previous shallow constructions [48], even global classical shadows are provably accessible with extremely low-depth quantum circuits.

Equipped with these tools, it is time to revisit previous quantum algorithms and search for gems in so-far-unmeasured output states by combining insights from quantum algorithms and quantum learning theory. This is especially relevant for intermediate-scale quantum experiments, where we want to get as much information as possible from a limited number of experiments.

We summarize the Hadamard test and its applications before showing that the standard presentation of the Hadamard test can be expanded by including classical shadows of the system register. In classical postprocessing, combining the auxiliary register's measurement results with the system register's shadow measurement allows for estimating additional quantities, inheriting the sample complexity bounds of classical shadows.

To demonstrate the usefulness of this additional information, we sketch three applications: (i) simultaneous estimation of $\mathrm{tr}[F(H, t)\rho]$ for a Fourier approximation $F(H, t)$ of some spectral function and fidelities with known eigenstates (using global shadows), where energy estimation following Refs. [15,16,18] is a specific example, (ii) combining $\mathrm{tr}[F(H, t)\rho]$ with an estimation of $\mathrm{tr}(H\rho)$ (using local shadows), and (iii) additionally estimating a measure of purity and eigenstateness (using local shadows).

Finally, we discuss another modification of the standard Hadamard test used in Refs. [20,21,49] and how applying anticontrolled unitaries can lead to further applications in comparing spectra of unitaries and determining eigenstateness of the input state while providing access to shadows of new types of quantum states.

The Hadamard test and its uses—To perform the standard Hadamard test shown in Fig. 1 (left), we repeat the quantum circuit with $\phi = 0$ [i.e., $P(\phi) = P(0) = \mathbb{I}$] and estimate the outcome probabilities of the measurement of the auxiliary qubit, which are given by

$$p(0) = \frac{1}{2}(\mathrm{tr}(\rho) + \mathrm{Re}[\mathrm{tr}(U\rho)]), \tag{1}$$

$$p(1) = \frac{1}{2}(\mathrm{tr}(\rho) - \mathrm{Re}[\mathrm{tr}(U\rho)]), \tag{2}$$

and then obtain $\mathrm{Re}[\mathrm{tr}(U\rho)] = p(0) - p(1)$ in classical postprocessing by effectively estimating the Pauli-Z expectation value of the auxiliary qubit while tracing over the system register. Repeating the procedure for $\phi = -\pi/2$ allows for the estimation of $\mathrm{Im}[\mathrm{tr}(U\rho)]$.

The linearity in the unitary U is precisely the reason why the Hadamard test has led to so many algorithms aimed at the resource-efficient use of intermediate-scale quantum devices. Given a *linear combination of unitaries* (LCU)

$M_{\mathrm{LCU}} = \sum \alpha_i U_i$, repetitions of the Hadamard test for the individual U_i's allow for an estimation of $\mathrm{tr}(M_{\mathrm{LCU}}\rho)$ in classical postprocessing. This bypasses the block-encoding and amplitude amplification procedures required for a coherent application of M_{LCU}. Furthermore, the linearity also allows for importance sampling procedures not only from M_{LCU}, but also of the U_i's themselves. This can help reduce circuit depths and lead to novel algorithms, as demonstrated in Ref. [16].

Whereas quantum signal processing and qubitization approaches focus on Chebyshev polynomials as a basis to construct linear combinations of unitaries to approximate spectral functions [50–53], the Hadamard test is especially suited to implement Fourier approximations thereof. As such, most proposed applications use $U_i = \mathrm{e}^{\mathrm{i}Ht_i}$ to construct useful Fourier approximations, such as those of step functions or filter functions that allow projections into (potentially low-energy) subspaces or for eigenvalue thresholding [15,16,18]. These applications, thus, combine the Hadamard test with Hamiltonian simulation to access a different basis in which to approximate spectral functions in classical postprocessing.

The construction of further interesting Fourier functions in a highly relevant and ongoing research topic, and any findings in this direction, fit the following discussion of adding system register measurements to the Hadamard test.

The Hadamard test in the light of shadows—While the standard application of the Hadamard test ends with the computation of $\mathrm{tr}(U\rho)$, the adaptations of Refs. [20,21] have shown that appropriate measurements of the system register can lead to the estimation of so-far-unavailable quantities, making better use of the output state of the Hadamard circuit before measurement, given by

$$\begin{aligned}\rho_{\mathrm{out}} = \frac{1}{4}\Big(&|0\rangle\langle 0| \otimes (I + U\mathrm{e}^{\mathrm{i}\phi})\rho(I + U\mathrm{e}^{\mathrm{i}\phi})^\dagger \\ &+ |0\rangle\langle 1| \otimes (I + U\mathrm{e}^{\mathrm{i}\phi})\rho(I - U\mathrm{e}^{\mathrm{i}\phi})^\dagger \\ &+ |1\rangle\langle 0| \otimes (I - U\mathrm{e}^{\mathrm{i}\phi})\rho(I + U\mathrm{e}^{\mathrm{i}\phi})^\dagger \\ &+ |1\rangle\langle 1| \otimes (I - U\mathrm{e}^{\mathrm{i}\phi})\rho(I - U\mathrm{e}^{\mathrm{i}\phi})^\dagger\Big). \end{aligned} \tag{3}$$

Thus, we would like to consider the additional possibilities the Hadamard test circuit offers, including estimating different Pauli expectation values on the auxiliary qubit, tracing out the auxiliary register, and adding observable measurements (that can also result in classical shadows) to the system register.

While a thorough, step-by-step discussion of all of these cases is presented in Sec. II in Supplemental Material [54] and a list summarizing all available quantities is shown in Appendix A, we would like to focus on two specific applications using the postmeasurement (potentially non-normalized) states

$$\rho(Z) = \mathrm{tr}_{\mathrm{aux}}(Z_{\mathrm{aux}}\rho_{\mathrm{out}}) = \frac{1}{2}(U\rho\mathrm{e}^{\mathrm{i}\phi} + \rho U^\dagger\mathrm{e}^{-\mathrm{i}\phi}), \tag{4}$$

$$\rho(I) = \mathrm{tr}_{\mathrm{aux}}(\rho_{\mathrm{out}}) = \frac{1}{2}(\rho + U\rho U^\dagger), \tag{5}$$

where ρ_{out} denotes the output state of the Hadamard test before any measurements.

Although we could instead perform several Hadamard tests in parallel and physically linearly combine their postmeasurement states depending on the measurement outcome, classical shadows allow a direct use of these postmeasurement states, one that is available for all of the algorithms mentioned above, at the (negligible) cost of also measuring the system register. Furthermore, the well-established literature on classical shadows provides rigorous error bounds and guarantees that are directly applicable here as well, as summarized in Sec. IV in Supplemental Material [54].

Using system register measurements for fidelity estimation—To showcase the use of obtaining classical shadows of such postmeasurement states, we turn toward a concrete example: combining the estimation of expectation values of linear combinations of unitaries with fidelities with pure eigenstates of H.

We begin by first discussing the setting of using only a single, fixed U within the Hadamard test. Combining the measurement of the auxiliary qubit of the output state ρ_{out} in the Pauli-Z basis [see Eq. (A12)] results in a statistical estimator for

$$\langle Z \otimes I^{\otimes n}\rangle_{\rho_{\mathrm{out}}} = \mathrm{tr}[\rho(Z)] = \mathrm{Re}(\mathrm{tr}(\mathrm{e}^{\mathrm{i}\phi}U\rho)) \tag{6}$$

and, consequently, in a statistical estimator of $\mathrm{Im}\,(\mathrm{tr}(U\rho))$ for $\phi = -\pi/2$ and, thus, an effective Pauli-Y measurement, as before.

However, we can also measure some observable O on the remaining n-qubit system register, resulting in

$$\langle Z \otimes O\rangle_{\rho_{\mathrm{out}}} = \mathrm{tr}[O\rho(Z)] = \mathrm{Re}(\mathrm{tr}(\mathrm{e}^{\mathrm{i}\phi}OU\rho)). \tag{7}$$

Note that a measurement of O still allows for disregarding that measurement information, thus effectively tracing over the system register, and, therefore, does not affect the original goal of estimating $\mathrm{tr}(U\rho)$.

Now, just as we use separate estimations of the real and imaginary part of $\mathrm{tr}(U\rho)$ for its estimation in classical postprocessing, we can combine the system register measurements to obtain $\mathrm{tr}(OU\rho)$ and, consequently, classical shadows of $\mathrm{Re}(U)\rho$, $\mathrm{Im}(U)\rho$, and $U\rho$. Since this quantity is still linear in U, we can again extend these results to linear combinations of different unitaries, thereby obtaining the same for $M_{\mathrm{LCU}} = \sum \alpha_i U_i$. Thus, when randomly choosing which U_i of the linear combination to implement and further randomizing the observable O, we can obtain information about the (non-normalized) state $\tilde{\rho} = M_{\mathrm{LCU}}\rho$.

Let us make this more concrete for $U_i = \mathrm{e}^{\mathrm{i}Ht_i}$ by restricting to rank-one observables $O = |\lambda\rangle\langle\lambda|$ to obtain

$$\begin{aligned}\langle Z \otimes |\lambda\rangle\langle\lambda|\rangle_{\rho_{\mathrm{out}},i} &= \mathrm{tr}[|\lambda\rangle\langle\lambda|\rho_i(Z)] \\ &= \mathrm{Re}\Big(\mathrm{tr}\big(|\lambda\rangle\langle\lambda|\mathrm{e}^{\mathrm{i}(Ht_i+I\phi)}\rho\big)\Big). \end{aligned} \tag{8}$$

Besides restricting to a single $|\lambda\rangle$, which may or may not be preparable with a shallow circuit, we can also use global shadows on the system register, which are now available with shallow circuits thanks to Ref. [47] or Ref. [48] to estimate this quantity for arbitrary product states.

Now, if we assume that $|\lambda\rangle$ is a pure eigenstate of H with known eigenvalue E, we find

$$\begin{aligned}\langle Z \otimes |\lambda\rangle\langle\lambda|\rangle_{\rho_{\mathrm{out}},i} &= \mathrm{Re}\Big(\mathrm{e}^{\mathrm{i}(Et_i+\phi)}\langle\lambda|\rho|\lambda\rangle\Big) \\ &= \cos(Et_i+\phi)F(\rho, |\lambda\rangle\langle\lambda|), \end{aligned} \tag{9}$$

which, since we know the factor $\cos(Et_i+\phi)$, allows us to estimate the fidelity F between the initial state ρ and known, pure eigenstate $|\lambda\rangle$. Consequently, using this extended version of the Hadamard test, we can use the auxiliary qubit to estimate the usual Hadamard test output $\mathrm{tr}(U\rho)$ and use system register measurements to, at the same time, extract additional information such as fidelities $\mathrm{tr}(\rho|\lambda\rangle\langle\lambda|)$ with certain states $|\lambda\rangle$. More generally, when $M_{\mathrm{LCU}} = \sum \alpha_i \mathrm{e}^{\mathrm{i}Ht_i}$, we can obtain $\mathrm{Re}[M_{\mathrm{LCU}}(\lambda)]F(\rho, |\lambda\rangle\langle\lambda|)$, $\mathrm{Im}[M_{\mathrm{LCU}}(\lambda)]F(\rho, |\lambda\rangle\langle\lambda|)$, and linear combinations thereof.

Thus, when M_{LCU} is a Fourier series of a threshold function projecting the initial state ρ into a (potentially low-energy) subspace, fidelities with pure eigenstates of H with known energy within the same subspace can be estimated. However, since the threshold function yields one for all eigenstates within the selected subspace, we do not need to know the energy explicitly but only that it is within the subspace.

The only additional cost of obtaining these additional estimates is the cost of estimating the required observables on the system register, which, due to recent shallow constructions for global shadows, does not constitute a bottleneck in practice.

In general, the same procedure can be used for extended Hadamard test circuits with more than a single auxiliary qubit and a single controlled unitary. However, it is essential to note that the number of measurement outcomes scales exponentially, decreasing the resolution for each postmeasurement shadow. The advantage remains that only a single quantum circuit is required to extract both the original information of these circuits and the information tractable with linear combinations of the postmeasurement shadows.

It is further important to note that stochastic phase estimation achieves Heisenberg limit scaling and, thus, requires only $\mathcal{O}(\epsilon^{-1})$ samples to obtain phase knowledge with an error of at most ϵ [15,18]. In contrast, classical shadows or even simple observable estimation by measurement are sampling procedures, requiring $\mathcal{O}(\epsilon^{-2})$ samples to achieve the same error guarantees. Thus, when focusing on stochastic phase estimation, the additional quantities accessible via system register measurements can only be estimated up to an error of $\mathcal{O}(\sqrt{\epsilon})$.

Using system register measurements for energy estimation—So far, we have used global shadows of the postmeasurement state $\rho(Z)$ to extract information about fidelities. However, as discussed in the Supplemental Material [54] summarized in Appendix A, we can also trace out the auxiliary register to obtain

$$\rho(I) = \mathrm{tr}_{\mathrm{aux}}(\rho_{\mathrm{out}}) = \frac{1}{2}(\rho + U\rho U^{\dagger}). \tag{10}$$

For local Hamiltonians and linear combinations of $U_i = \mathrm{e}^{\mathrm{i}Ht_i}$, local classical shadows, or any other measurement scheme for energy estimation, of the system register can then be used to obtain an additional estimate of the state's energy, since for $O = H$, obtainable in classical postprocessing due to the linearity in O, we have

$$\mathrm{tr}[H\rho_i(I)] = \frac{1}{2}\big(\mathrm{tr}(H\rho) + \mathrm{tr}(H\mathrm{e}^{\mathrm{i}Ht_i}\rho\mathrm{e}^{-\mathrm{i}Ht_i})\big) = \mathrm{tr}(H\rho).$$

Consequently, as a by-product of estimating $\mathrm{tr}(M_{\mathrm{LCU}}\rho)$, we can obtain an energy estimate of ρ, requiring only additional random Pauli measurements of the n-qubit system register. Similarly, the expectation value of other operators commuting with the Hamiltonian can be estimated.

It is important to stress that one of the main early applications of the Hadamard test is stochastic phase estimation [15,18], whose goal is the estimation of a state's eigenenergies and, more importantly, ground state energies. As such, these applications already generate energy information with a Heisenberg scaling of $\mathcal{O}(\epsilon^{-1})$ samples. In contrast, the above use of shadows requires $\mathcal{O}(\epsilon^{-2})$ samples to achieve the same accuracy. However, we envision using statistical phase estimation for ground state energy estimation with simultaneous estimation of the guiding state's energy $\mathrm{tr}(H\rho)$. Therefore, we view this application as an add-on to more intricate phase estimation procedures and an enhancement of Hadamard circuit applications, whose purpose is not foremost in energy estimation.

Using system register measurements for purity and eigenstateness—Less practical but still conceptually interesting, we can further use exponentially many local shadows of $\rho(I)$ to estimate its purity [44], given by

$$\mathrm{tr}(\rho(I)^2) = \frac{1}{2}\big(\mathrm{tr}(\rho^2) + \mathrm{tr}(\rho U\rho U^{\dagger})\big), \tag{11}$$

which is one if and only if ρ is a pure eigenstate of U. Tracing out the auxiliary system, thus, adds these two quantum states, allowing for another quantity to be estimated, albeit not efficiently in this case, since purity estimation is known to require exponentially many copies of the state [55].

Since the system register can be traced over even when measured, we can again combine the estimation of this quantity with the estimation of energy. Furthermore, even though this quantity is no longer linear in U, if $U_i = \mathrm{e}^{\mathrm{i}Ht_i}$, the simulation time does not impact whether ρ is an eigenstate of U_i. Since the introduced phases of $\mathrm{e}^{\pm\mathrm{i}\lambda t_i}$ for an eigenstate $\rho = |\lambda\rangle\langle\lambda|$ with energy λ cancel, we can again use measurement outcomes for different t_i to estimate the same quantity.

Adding anticontrolled unitaries to the Hadamard test—Stepping away from system register measurements, we want to discuss another component of the Hadamard test that has not been explored much: the addition of an anticontrolled unitary W (applied when the auxiliary qubit is zero instead of one), as shown in Fig. 2. Proposed in Ref. [56] to add two unitaries and further discussed in Refs. [20,21,49], this helps to linearize the problem of applying two linear combinations of unitaries in a randomized fashion as required for quantum dynamics or sampling from matrix functions.

This generalization changes the output state of the Hadamard test from Eq. (3) to

$$\begin{aligned}\rho_{\mathrm{out}} = \frac{1}{4}\Big(&|0\rangle\langle 0| \otimes (W + U\mathrm{e}^{\mathrm{i}\phi})\rho(W + U\mathrm{e}^{\mathrm{i}\phi})^\dagger \\ &+ |0\rangle\langle 1| \otimes (W + U\mathrm{e}^{\mathrm{i}\phi})\rho(W - U\mathrm{e}^{\mathrm{i}\phi})^\dagger \\ &+ |1\rangle\langle 0| \otimes (W - U\mathrm{e}^{\mathrm{i}\phi})\rho(W + U\mathrm{e}^{\mathrm{i}\phi})^\dagger \\ &+ |1\rangle\langle 1| \otimes (W - U\mathrm{e}^{\mathrm{i}\phi})\rho(W - U\mathrm{e}^{\mathrm{i}\phi})^\dagger\Big), \end{aligned} \tag{12}$$

effectively replacing the $(I \pm U\mathrm{e}^{\mathrm{i}\phi})$ of the unmodified Hadamard test with $(W \pm U\mathrm{e}^{\mathrm{i}\phi})$, which leads to additional obtainable postmeasurement states and observables,

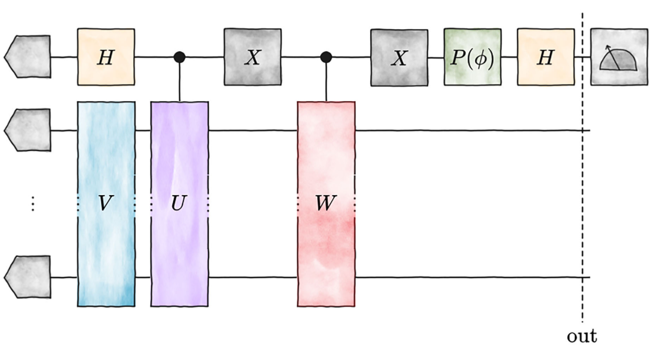

FIG. 2. The Hadamard test with an additional anticontrolled unitary W can help in quantum dynamics and sampling from matrix functions by linearizing the output to allow for randomized approaches [20,21], or to compare spectra of unitaries, determine eigenstateness of a state, and access new types of quantum states, as discussed in the main text.

summarized in Appendix B. Besides the applications of Refs. [20,21,56], we envision another use in obtaining shadows of so-far-inaccessible quantum states, further strengthening the point that small changes to existing algorithms can yield interesting new outcomes.

As an example, consider $U = \mathrm{e}^{\mathrm{i}Ht_1}$ and $W = \mathrm{e}^{\mathrm{i}Ht_2}$ and $\phi = 0$. Then, executing the modified Hadamard test of Fig. 2 yields

$$\rho(Z) = \frac{1}{2}\left(\mathrm{e}^{\mathrm{i}Ht_1}\rho\mathrm{e}^{-\mathrm{i}Ht_2} + \mathrm{e}^{\mathrm{i}Ht_2}\rho\mathrm{e}^{-\mathrm{i}Ht_1}\right).$$

Now, if $\rho = |\psi\rangle\langle\psi|$ with energy $\langle\psi|H|\psi\rangle = E$,

$$\mathrm{tr}[\rho(Z)] = \mathrm{Re}(\mathrm{e}^{\mathrm{i}E(t_1 - t_2)}) = \cos[E(t_1 - t_2)]. \tag{13}$$

However, if ρ is not an eigenstate of H, e.g., when $\rho = |\psi\rangle\langle\psi|$ with

$$|\psi\rangle = \alpha|\mu\rangle + \beta|\nu\rangle \tag{14}$$

for two different eigenstates $|\mu\rangle$ and $|\nu\rangle$ with energies E_1 and $E_2 \neq E_1$, we obtain

$$\begin{aligned}\mathrm{tr}[\rho(Z)] &= \mathrm{Re}\left(\mathrm{tr}\left(\mathrm{e}^{\mathrm{i}Ht_1}\rho\mathrm{e}^{-\mathrm{i}Ht_2}\right)\right) \\ &= \alpha^2\cos[E_1(t_1 - t_2)] + \beta^2\cos[E_2(t_1 - t_2)], \end{aligned} \tag{15}$$

since $\mathrm{tr}(|\mu\rangle\langle\nu|) = \langle\mu|\nu\rangle = 0$. While the above discussion, due to the cyclic property of the trace, also holds for the standard Hadamard test with $U = \mathrm{e}^{\mathrm{i}H(t_2 - t_1)}$, such a construction further provides access to new types of quantum states of the form $\rho = U\rho W^\dagger$ for different unitaries U and W. Although we did not find practical uses for such shadows, we invite further study of the capabilities of this extension of the Hadamard test and a careful examination of using the phase shift $P(\phi)$ to construct new algorithms and discover new applications.

Discussion and outlook—In this Letter, we have improved the Hadamard test by bringing it into contact with advances in quantum learning theory, suitably exploiting recently developed algorithmic subroutines in mind to show that classical shadows of the system register can extract—strikingly so far unused, but highly useful—information: accepting that accessible information has been left ignored so far that can be exploited to improve schemes adds an exciting new twist to the Hadamard test. Furthermore, we have discussed how mild modifications of this well-known circuit can lead to many new applications. Especially for early fault-tolerant quantum devices with only a few error-corrected qubits (and, thus, a limited number of auxiliary qubits) and sampling-based quantum algorithms, this approach enables the extraction of additional information without requiring additional quantum circuits and enhances previous applications using only auxiliary qubit measurements. Additionally, we have revisited the modification of the Hadamard test to incorporate anticontrolled unitaries, demonstrating that this slight adaptation also leads to new capabilities.

We conclude this Letter by making three "meta points" that emphasize the significance of this Letter. First, these results further demonstrate the power of quantum measurement and motivate the continued study of quantum algorithms that disregard qubit registers without measurements. Then, it further shows that relevant progress is often achieved by charting the territory between established fields of research, here quantum algorithm design and learning theory. This mind set opens up novel possibilities, especially with recent breakthroughs that enable both global and local classical shadows with shallow circuits. Third and finally, the gap between the noisy, intermediate-scale quantum and fault-tolerant regime seems painfully large. It is the hope that the tools and ideas presented here will help chart a road map connecting these realms.

Acknowledgments—We thank Stefano Polla for insightful discussions at QCTiP 2025. The Berlin team has been supported by the BMWK (PlanQK), the DFG (CRC 183), the BMBF (QPIC-1, MuniQC-Atoms, HYBRID), the Quantum Flagship (Millenion, Pasquans2), QuantERA (HQCC), and the ERC (DebuQC). R. K. has been supported by the Austrian Science Fund via SFB BeyondC (Grant-DOI: 10.55776/F71), the projects QuantumReady (FFG No. 896217) and High-Performance integrated Quantum Computing (FFG No. 897481) within Quantum Austria (both managed by the FFG), as well as the ERC (q-shadows).

Data availability—To construct our circuit diagrams (all figures), we have used the open source library found at [57], created by Jadwiga Wilkens.

[1] B. W. Reichardt, D. Aasen, R. Chao, A. Chernoguzov, W. van Dam, J. P. Gaebler, D. Gresh, D. Lucchetti, M. Mills, S. A. Moses, B. Neyenhuis, A. Paetznick, A. Paz, P. E. Siegfried, M. P. da Silva, K. M. Svore, Z. Wang, and M. Zanner, Demonstration of quantum computation and error correction with a tesseract code, arXiv:2409.04628.

[2] D. Bluvstein, S. J. Evered, A. A. Geim, S. H. Li, H. Zhou, T. Manovitz, S. Ebadi, M. Cain, M. Kalinowski, D. Hangleiter, J. P. Bonilla Ataides, N. Maskara, I. Cong, X. Gao, P. Sales Rodriguez, T. Karolyshyn, G. Semeghini, M. J. Gullans, M. Greiner, V. Vuletić, and M. D. Lukin, Logical quantum processor based on reconfigurable atom arrays, Nature (London) **626**, 58 (2024).

[3] Google Quantum AI and Collaborators, Quantum error correction below the surface code threshold, Nature (London) **638**, 920 (2025).

[4] B. W. Reichardt *et al.*, Logical computation demonstrated with a neutral atom quantum processor, arXiv:2411.11822.

[5] H. Putterman, K. Noh, C. T. Hann *et al.*, Hardware-efficient quantum error correction via concatenated bosonic qubits, Nature (London) **638**, 927 (2025).

[6] J. Preskill, Quantum computing in the NISQ era and beyond, Quantum **2**, 79 (2018).

[7] J. M. Arrazola, From NISQ to ISQ, (2023), https://pennylane.ai/blog/2023/06/from-nisq-to-isq/ (accessed Jan 13, 2025).

[8] J. Preskill, Beyond NISQ: The megaquop machine, ACM Trans. Quantum Comput. **6**, 1 (2025).

[9] N. Koukoulekidis, S. Wang, T. O'Leary, D. Bultrini, L. Cincio, and P. Czarnik, A framework of partial error correction for intermediate-scale quantum computers, Report No. LA-UR-23-26230, 2023, arXiv:2306.15531.

[10] A. Montanaro, Quantum algorithms: An overview, npj Quantum Inf. **2**, 15023 (2016).

[11] A. M. Dalzell, S. McArdle, M. Berta, P. Bienias, C.-F. Chen, A. Gilyén, C. T. Hann, M. J. Kastoryano, E. T. Khabiboulline, A. Kubica, G. Salton, S. Wang, and F. G. S. L. Brandão, *Quantum Algorithms: A Survey of Applications and End-to-End Complexities* (Cambridge University Press, Cambridge, England, 2025), 10.1017/9781009639651.

[12] A. Y. Kitaev, Quantum measurements and the Abelian stabilizer problem, arXiv:quant-ph/9511026.

[13] K. M. Svore, M. B. Hastings, and M. Freedman, Faster phase estimation, Quantum Inf. Comput. **14**, 306 (2014).

[14] N. Wiebe and C. Granade, Efficient Bayesian phase estimation, Phys. Rev. Lett. **117**, 010503 (2016).

[15] L. Lin and Y. Tong, Heisenberg-limited ground-state energy estimation for early fault-tolerant quantum computers, PRX Quantum **3**, 010318 (2022).

[16] K. Wan, M. Berta, and E. T. Campbell, Randomized quantum algorithm for statistical phase estimation, Phys. Rev. Lett. **129**, 030503 (2022).

[17] L. Clinton, J. Bausch, J. Klassen, and T. Cubitt, Phase estimation of local Hamiltonians on NISQ hardware, New J. Phys. **25**, 033027 (2023).

[18] G. Wang, D. S. França, R. Zhang, S. Zhu, and P. D. Johnson, Quantum algorithm for ground state energy estimation using circuit depth with exponentially improved dependence on precision, Quantum **7**, 1167 (2023).

[19] J. Günther, F. Witteveen, A. Schmidhuber, M. Miller, M. Christandl, and A. Harrow, Phase estimation with partially randomized time evolution, arXiv:2503.05647.

[20] S. Wang, S. McArdle, and M. Berta, Qubit-efficient randomized quantum algorithms for linear algebra, PRX Quantum **5**, 020324 (2024).

[21] P. K. Faehrmann, M. Steudtner, R. Kueng, M. Kieferova, and J. Eisert, Randomizing multi-product formulas for Hamiltonian simulation, Quantum **6**, 806 (2022).

[22] A. N. Chowdhury, G. H. Low, and N. Wiebe, A variational quantum algorithm for preparing quantum Gibbs states, arXiv:2002.00055.

[23] Y. Wang, G. Li, and X. Wang, Variational quantum Gibbs state preparation with a truncated Taylor series, Phys. Rev. Appl. **16**, 054035 (2021).

[24] M. Consiglio, Variational quantum algorithms for Gibbs state preparation, in *Numerical Computations: Theory and Algorithms*, edited by Y. D. Sergeyev, D. E. Kvasov,

and A. Astorino (Springer Nature Switzerland, Cham, 2025), pp. 56–70.

[25] B. Bauer, D. Wecker, A. J. Millis, M. B. Hastings, and M. Troyer, Hybrid quantum-classical approach to correlated materials, Phys. Rev. X **6**, 031045 (2016).

[26] A. Baroni, J. Carlson, R. Gupta, A. C. Y. Li, G. N. Perdue, and A. Roggero, Nuclear two point correlation functions on a quantum computer, Phys. Rev. D **105**, 074503 (2022).

[27] M. L. Goh and B. Koczor, Direct estimation of the density of states for fermionic systems, arXiv:2407.03414.

[28] Y. Subaşı, L. Cincio, and P. J. Coles, Entanglement spectroscopy with a depth-two quantum circuit, J. Phys. A **52**, 044001 (2019).

[29] S. Subramanian and M.-H. Hsieh, Quantum algorithm for estimating α-Renyi entropies of quantum states, Phys. Rev. A **104**, 022428 (2021).

[30] S. P. Jordan, Fast quantum algorithms for approximating some irreducible representations of groups, arXiv:0811.0562.

[31] D. Aharonov, V. Jones, and Z. Landau, A polynomial quantum algorithm for approximating the Jones polynomial, in *Proceedings of the Thirty-Eighth Annual ACM Symposium on Theory of Computing*, STOC '06 (Association for Computing Machinery, New York, 2006), pp. 427–436.

[32] P. W. Shor and S. P. Jordan, Estimating Jones polynomials is a complete problem for one clean qubit, Quantum Inf. Comput. **8**, 681 (2008).

[33] E. Knill and R. Laflamme, Power of one bit of quantum information, Phys. Rev. Lett. **81**, 5672 (1998).

[34] D. Wang, O. Higgott, and S. Brierley, Accelerated variational quantum eigensolver, Phys. Rev. Lett. **122**, 140504 (2019).

[35] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information: 10th Anniversary Edition* (Cambridge University Press, Cambridge, England, 2010).

[36] L. Clinton, T. S. Cubitt, R. Garcia-Patron, A. Montanaro, S. Stanisic, and M. Stroeks, Quantum phase estimation without controlled unitaries, arXiv:2410.21517.

[37] S. Polla, G.-L. R. Anselmetti, and T. E. O'Brien, Optimizing the information extracted by a single qubit measurement, Phys. Rev. A **108**, 012403 (2023).

[38] T. E. O'Brien, S. Polla, N. C. Rubin, W. J. Huggins, S. McArdle, S. Boixo, J. R. McClean, and R. Babbush, Error mitigation via verified phase estimation, PRX Quantum **2**, 020317 (2021).

[39] Y. Zhou and Z. Liu, A hybrid framework for estimating nonlinear functions of quantum states, npj Quantum Inf. **10**, 1 (2024).

[40] H.-Y. Huang, R. Kueng, and J. Preskill, Predicting many properties of a quantum system from very few measurements, Nat. Phys. **16**, 1050 (2020).

[41] 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).

[42] J. Morris and B. Dakić, Selective quantum state tomography, arXiv:1909.05880.

[43] M. Paini, A. Kalev, D. Padilha, and B. Ruck, Estimating expectation values using approximate quantum states, Quantum **5**, 413 (2021).

[44] S. H. Sack, R. A. Medina, A. A. Michailidis, R. Kueng, and M. Serbyn, Avoiding barren plateaus using classical shadows, PRX Quantum **3**, 020365 (2022).

[45] H. H. S. Chan, R. Meister, M. L. Goh, and B. Koczor, Algorithmic shadow spectroscopy, PRX Quantum **6**, 010352 (2025).

[46] P. K. Faehrmann, Short-time simulation of quantum dynamics by Pauli measurements, Phys. Rev. A **112**, 012602 (2025).

[47] T. Schuster, J. Haferkamp, and H.-Y. Huang, Random unitaries in extremely low depth, Science **389**, 92 (2025).

[48] C. Bertoni, J. Haferkamp, M. Hinsche, M. Ioannou, J. Eisert, and H. Pashayan, Shallow shadows: Expectation estimation using low-depth random Clifford circuits, Phys. Rev. Lett. **133**, 020602 (2024).

[49] S. Chakraborty, Implementing any linear combination of unitaries on intermediate-term quantum computers, Quantum **8**, 1496 (2024).

[50] G. H. Low and I. L. Chuang, Hamiltonian simulation by qubitization, Quantum **3**, 163 (2019).

[51] G. H. Low and I. L. Chuang, Optimal Hamiltonian simulation by quantum signal processing, Phys. Rev. Lett. **118**, 010501 (2017).

[52] J. M. Martyn, Z. M. Rossi, A. K. Tan, and I. L. Chuang, Grand unification of quantum algorithms, PRX Quantum **2**, 040203 (2021).

[53] A. Gilyén, Y. Su, G. H. Low, and N. Wiebe, Quantum singular value transformation and beyond: Exponential improvements for quantum matrix arithmetics, in *Proceedings of the 51st Annual ACM SIGACT Symposium on Theory of Computing*, STOC 2019 (Association for Computing Machinery, New York, 2019), pp. 193–204.

[54] See Supplemental Material at http://link.aps.org/supplemental/10.1103/cqjw-kl8s for additional information.

[55] S. Chen, J. Cotler, H.-Y. Huang, and J. Li, Exponential separations between learning with and without quantum memory, in *Proceedings of the 2021 IEEE 62nd Annual Symposium on Foundations of Computer Science (FOCS)* (IEEE, New York, 2022), pp. 574–585.

[56] A. M. Childs and N. Wiebe, Hamiltonian simulation using linear combinations of unitary operations, Quantum Inf. Comput. **12**, 901 (2012).

[57] https://github.com/wilkensJ/quantum-circuit-drawio-library.

End Matter

In the following, we summarize the quantities available with the Hadamard test and its extension. Derivations thereof and a more thorough discussion can be found in Secs. I–III in Supplemental Material [54].

Appendix A: Summary of quantities accessible with the Hadamard test—To summarize, with the Hadamard test applied to an initial state ρ, we can obtain the postmeasurement (observable) states and observables

$$\rho(I) = \mathrm{tr}_{\mathrm{aux}}(I\rho_{\mathrm{out}}) = \frac{1}{2}(\rho + U\rho U^\dagger), \tag{A1}$$

$$\langle I \otimes O\rangle_{\rho_{\mathrm{out}}} = \mathrm{tr}(O\rho(I)) = \frac{1}{2}\mathrm{tr}\big(O(\rho + U\rho U^\dagger)\big), \tag{A2}$$

$$\langle I \otimes I^{\otimes n}\rangle_{\rho_{\mathrm{out}}} = \mathrm{tr}(\rho(I)) = \mathrm{tr}(\rho), \tag{A3}$$

$$\rho(X) = \mathrm{tr}_{\mathrm{aux}}(X_{\mathrm{aux}}\rho_{\mathrm{out}}) = \frac{1}{2}(\rho - U\rho U^\dagger), \tag{A4}$$

$$\langle X \otimes O\rangle_{\rho_{\mathrm{out}}} = \mathrm{tr}(O\rho(X)) = \frac{1}{2}\mathrm{tr}\big(O(\rho - U\rho U^\dagger)\big), \tag{A5}$$

$$\langle X \otimes I^{\otimes n}\rangle_{\rho_{\mathrm{out}}} = \mathrm{tr}(\rho(X)) = 0, \tag{A6}$$

$$\begin{aligned}\rho(Y) &= \mathrm{tr}_{\mathrm{aux}}(Y_{\mathrm{aux}}\rho_{\mathrm{out}})\\ &= -\frac{\mathrm{i}}{2}(U\rho \mathrm{e}^{\mathrm{i}\phi} - \rho U^\dagger \mathrm{e}^{-\mathrm{i}\phi}),\end{aligned} \tag{A7}$$

$$\langle Y \otimes O\rangle_{\rho_{\mathrm{out}}} = \mathrm{tr}(O\rho(Y)) = \mathrm{Im}\,\big(\mathrm{tr}(O\mathrm{e}^{\mathrm{i}\phi}U\rho)\big), \tag{A8}$$

$$\langle Y \otimes I^{\otimes n}\rangle_{\rho_{\mathrm{out}}} = \mathrm{tr}(\rho(Y)) = \mathrm{Im}\,\big(\mathrm{tr}(\mathrm{e}^{\mathrm{i}\phi}U\rho)\big), \tag{A9}$$

$$\begin{aligned}\rho(Z) &= \mathrm{tr}_{\mathrm{aux}}(Z_{\mathrm{aux}}\rho_{\mathrm{out}})\\ &= \frac{1}{2}\big((U\rho \mathrm{e}^{\mathrm{i}\phi} + \rho U^\dagger \mathrm{e}^{-\mathrm{i}\phi})\big),\end{aligned} \tag{A10}$$

$$\langle Z \otimes O\rangle_{\rho_{\mathrm{out}}} = \mathrm{tr}(O\rho(Z)) = \mathrm{Re}\big(\mathrm{tr}(O\mathrm{e}^{\mathrm{i}\phi}U\rho)\big), \tag{A11}$$

$$\langle Z \otimes I^{\otimes n}\rangle_{\rho_{\mathrm{out}}} = \mathrm{tr}(\rho(Z)) = \mathrm{Re}\big(\mathrm{tr}(\mathrm{e}^{\mathrm{i}\phi}U\rho)\big). \tag{A12}$$

Appendix B: Summary of quantities accessible with the extended Hadamard test—Similarly, for the extended Hadamard test, including the anticontrolled application of the unitary W, where the output state is given by

$$\begin{aligned}\rho_{\mathrm{out}} = \frac{1}{4}\Big(&|0\rangle\langle 0| \otimes (W + U\mathrm{e}^{\mathrm{i}\phi})\rho(W + U\mathrm{e}^{\mathrm{i}\phi})^\dagger\\ &+ |0\rangle\langle 1| \otimes (W + U\mathrm{e}^{\mathrm{i}\phi})\rho(W - U\mathrm{e}^{\mathrm{i}\phi})^\dagger\\ &+ |1\rangle\langle 0| \otimes (W - U\mathrm{e}^{\mathrm{i}\phi})\rho(W + U\mathrm{e}^{\mathrm{i}\phi})^\dagger\\ &+ |1\rangle\langle 1| \otimes (W - U\mathrm{e}^{\mathrm{i}\phi})\rho(W - U\mathrm{e}^{\mathrm{i}\phi})^\dagger\Big),\end{aligned} \tag{B1}$$

we obtain the postmeasurement (observable) states and observables

$$\rho(I) = \mathrm{tr}_{\mathrm{aux}}(I\rho_{\mathrm{out}}) = \frac{1}{2}(W\rho W^\dagger + U\rho U^\dagger), \tag{B2}$$

$$\langle I \otimes O\rangle_{\rho_{\mathrm{out}}} = \mathrm{tr}(O\rho(I)) = \frac{1}{2}\mathrm{tr}\big(O(W\rho W^\dagger + U\rho U^\dagger)\big), \tag{B3}$$

$$\langle I \otimes I^{\otimes n}\rangle_{\rho_{\mathrm{out}}} = \mathrm{tr}(\rho(I)) = \mathrm{tr}(\rho), \tag{B4}$$

$$\rho(X) = \mathrm{tr}_{\mathrm{aux}}(X_{\mathrm{aux}}\rho_{\mathrm{out}}) = \frac{1}{2}(W\rho W^\dagger - U\rho U^\dagger), \tag{B5}$$

$$\langle X \otimes O\rangle_{\rho_{\mathrm{out}}} = \mathrm{tr}(O\rho(X)) = \frac{1}{2}\mathrm{tr}\big(O(W\rho W^\dagger - U\rho U^\dagger)\big), \tag{B6}$$

$$\langle X \otimes I^{\otimes n}\rangle_{\rho_{\mathrm{out}}} = \mathrm{tr}(\rho(X)) = 0, \tag{B7}$$

$$\begin{aligned}\rho(Y) &= \mathrm{tr}_{\mathrm{aux}}(Y_{\mathrm{aux}}\rho_{\mathrm{out}})\\ &= -\frac{\mathrm{i}}{2}(U\rho W^\dagger \mathrm{e}^{\mathrm{i}\phi} - W\rho U^\dagger \mathrm{e}^{-\mathrm{i}\phi}),\end{aligned} \tag{B8}$$

$$\langle Y \otimes O\rangle_{\rho_{\mathrm{out}}} = \mathrm{tr}(O\rho(Y)) = \mathrm{Im}\,\big(\mathrm{tr}(W^\dagger O\mathrm{e}^{\mathrm{i}\phi}U\rho)\big), \tag{B9}$$

$$\langle Y \otimes I^{\otimes n}\rangle_{\rho_{\mathrm{out}}} = \mathrm{tr}(\rho(Y)) = \mathrm{Im}\,\big(\mathrm{tr}(\mathrm{e}^{\mathrm{i}\phi}W^\dagger U\rho)\big), \tag{B10}$$

$$\begin{aligned}\rho(Z) &= \mathrm{tr}_{\mathrm{aux}}(Z_{\mathrm{aux}}\rho_{\mathrm{out}})\\ &= \frac{1}{2}\big((U\rho W^\dagger \mathrm{e}^{\mathrm{i}\phi} + W\rho U^\dagger \mathrm{e}^{-\mathrm{i}\phi})\big),\end{aligned} \tag{B11}$$

$$\langle Z \otimes O\rangle_{\rho_{\mathrm{out}}} = \mathrm{tr}(O\rho(Z)) = \mathrm{Re}\big(\mathrm{tr}(W^\dagger O\mathrm{e}^{\mathrm{i}\phi}U\rho)\big), \tag{B12}$$

$$\langle Z \otimes I^{\otimes n}\rangle_{\rho_{\mathrm{out}}} = \mathrm{tr}(\rho(Z)) = \mathrm{Re}\big(\mathrm{tr}(\mathrm{e}^{\mathrm{i}\phi}W^\dagger U\rho)\big). \tag{B13}$$

For these modifications, it can also be beneficial to consider randomized approaches where U and W are both drawn from the same ensemble $\{p_i, U_i\}$, which produces some interesting linear combination $\sum p_i U_i$ in expectation, such as approximations of the time evolution operator [21].