Methodology for replacing indirect measurements with direct measurements

Kosuke Mitarai[1,2,*] and Keisuke Fujii[1,3,4,†]

[1]*Graduate School of Engineering Science, Osaka University, 1-3 Machikaneyama, Toyonaka, Osaka 560-8531, Japan*
[2]*QunaSys Inc., High-tech Hongo Building 1F, 5-25-18 Hongo, Bunkyo, Tokyo 113-0033, Japan*
[3]*Graduate School of Science, Kyoto University, Kitashirakawa Oiwake-cho, Sakyo-ku, Kyoto 606-8302, Japan*
[4]*JST, PRESTO, 4-1-8 Honcho, Kawaguchi, Saitama 332-0012, Japan*

In quantum computing, the indirect measurement of unitary operators such as the Hadamard test plays a significant role in many algorithms. However, in certain cases, the indirect measurement can be reduced to the direct measurement, where a quantum state is destructively measured. Here, we investigate under what conditions such a replacement is possible and develop a general methodology for trading an indirect measurement with sequential direct measurements. The results can be applied to construct quantum circuits to evaluate the analytical gradient, metric tensor, Hessian, and even higher order derivatives of a parametrized quantum state. Also, we propose a method to measure the out-of-time-order correlator based on the presented protocol. Our protocols can significantly reduce the depth of a quantum circuit by making the controlled operation unnecessary, and thus are suitable for quantum-classical hybrid algorithms on near-term quantum computers.

I. INTRODUCTION

The output from quantum computation is measured in two ways: indirect and direct measurements of observables. In the former, the measured quantum state is not completely destructed, whereas, in the latter, the state collapses to the basis on which we perform the measurement. The simplest and most important protocol for the indirect method is the Hadamard test (Fig. 1). In the Hadamard test, we add an ancillary qubit and apply a controlled unitary gate, a unitary U to a target quantum state $|\psi\rangle$ conditioned on the ancilla being $|0\rangle$ or $|1\rangle$ to measure the expectation value of U, $\langle\psi|U|\psi\rangle$, as the expectation value of the Pauli Z operator of the ancilla. This measurement allows us to reuse the state $(I \pm U)|\psi\rangle/\sqrt{2}$ after the measurement, which is the property exploited in algorithms like iterative phase estimation [1,2].

Such indirect approaches can achieve a precision of ϵ in $O(1/\epsilon)$ time. However, the implementation of the controlled-U gate can be a hard task especially for so-called noisy intermediate scale quantum (NISQ) [3] devices. In fact, direct measurements can be satisfiable when only the expectation value of an observable is required. A famous example is the estimation of the energy expectation values in the variational quantum eigensolver (VQE) [4], which is one of the most promising applications of NISQ devices. The time required

to achieve a precision of ϵ is $O(1/\epsilon^2)$ in this approach, which is much longer than that of the indirect approach [5,6].

Another example, which replaces the indirect approach with the direct one, is the destructive swap test [7]. The destructive swap test is a direct version of the swap test [8] which measures the overlap $|\langle\psi|\varphi\rangle|^2$ between two quantum states $|\psi\rangle$ and $|\varphi\rangle$. Initially proposed in [7], this method has been rediscovered by the machine learning approach [9], and it is now utilized in the application of NISQ devices [10–12]. Reference [13] has proposed to use the destructive swap test to measure $|\langle\psi|U|\psi\rangle|^2$ for an arbitrary U by substituting $|\varphi\rangle$ with $U|\psi\rangle$, and the protocol was extended to measure the quantity $|\langle\psi|P|\varphi\rangle|^2$, where P is a qubit-permutation operator, which can be employed to estimate nonlinear functionals of a quantum state ρ such as $\text{Tr}(\rho^n)$ [14], with a low-depth circuit.

Furthermore, methods for gradient estimation employed in variational quantum algorithms (VQAs) also illustrate the correspondence between those two approaches for certain cases. VQAs, such as the VQE, employ a parametrized quantum circuit $U(\boldsymbol{\theta})$ and classical optimizer, which minimizes a cost function $\mathcal{L}(\boldsymbol{\theta})$ by iteratively tuning the circuit parameter $\boldsymbol{\theta}$. The cost is usually computed from the expectation values of observables, therefore their gradient can be a key ingredient for the optimization. We can estimate the gradient in two ways. Indirect and direct schemes have been proposed in Ref. [15] and Refs. [16,17], respectively. The indirect method uses two different quantum circuits to estimate one element of the gradient.

These examples motivate us to further develop the methodology for replacing the indirect measurement with the direct measurement. In this work, we describe the general protocol for such replacements. The protocols for the Hadamard test involving a single controlled gate are given in Results 1 and 2. Result 1 is a generalization of the method used in the VQE, and Result 2 is a generalization of the destructive swap test

*u801032f@ecs.osaka-u.ac.jp
†fujii.keisuke.2s@kyoto-u.ac.jp
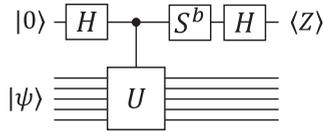
FIG. 1. Simplest Hadamard test. In the figure, $b \in \{0, 1\}$ and U, H, S are an arbitrary quantum gate, the Hadamard gate, and $e^{-i\pi Z/4}$, respectively. When $b = 0$, $\langle Z \rangle = \text{Re} \langle \psi_{\text{in}} | U | \psi_{\text{in}} \rangle$ and when $b = 1$, $\langle Z \rangle = \text{Im} \langle \psi_{\text{in}} | U | \psi_{\text{in}} \rangle$.

which can be applied to general local unitary gates. Finally, in Result 3, we describe a method to replace the Hadamard test involving multiple controlled gates. It is a generalization of the method to estimate the gradient of observables with direct measurements, that is, we employ multiple quantum circuits to estimate the output of the Hadamard test. The proposed method can significantly reduce the depth of a quantum circuit and the accumulation of noise in the measured quantity. Based on the above results, we propose methods to estimate higher order gradient including the metric tensor $g_{jk} = \frac{\partial \langle \psi(\boldsymbol{\theta}) |}{\partial \theta_j} \frac{\partial | \psi(\boldsymbol{\theta}) \rangle}{\partial \theta_j}$ of the variational quantum state $| \psi(\boldsymbol{\theta}) \rangle$ and the Hessian of an observable. Specifically, the metric tensor is a key quantity in variational quantum simulations [18,19]. Finally, we present a protocol to measure the multipoint correlator, such as the out-of-time-order correlators (OTOCs), which is an important quantity in a quantum many-body system as a possible measure of the quantum chaos [20–23].

II. REPLACEMENT OF CONTROLLED GATES

A. Hadamard test with one controlled gate

Let us first consider the case where the unitary U in Fig. 1 is given by an exponential $U(\boldsymbol{\theta}) = e^{-i\theta G}$ of a Hermitian operator G such that $G^2 = I$. In this case, $\langle Z \rangle$ of the ancilla in the Hadamard test becomes $\langle \psi | U | \psi \rangle = \cos \frac{\theta}{2} - i \sin \frac{\theta}{2} \langle \psi | G | \psi \rangle$. Hence, the measurement of $\langle \psi | G | \psi \rangle$, which is the expectation value of G, is sufficient to replace the Hadamard test. We can evaluate this quantity efficiently if G can be decomposed as $G = \sum_{P \in \mathcal{P}} a_P P$, where $a_P \in \mathbb{R}$ and $\mathcal{P} = \{I, X, Y, Z\}^{\otimes n}$, with a_P being nonzero on the polynomial number of terms with respect to the number of qubits. More generally, if the gate U itself can be decomposed into the sum of the Pauli products consisting of the polynomial number of terms, which naturally includes the previous case, we can measure $\langle U \rangle$ without the Hadamard test. Therefore we have the following.

Result 1. If the gate U can be decomposed into the sum of the Pauli products with the polynomial number of terms with respect to the number of qubits, the output of Fig. 1, $\langle \psi | U | \psi \rangle$, can be estimated by direct measurement by evaluating each Pauli term.

A prototypical example of the above result is the replacement of the phase estimation with direct measurements in the VQE. The tradeoff of the protocol above is the time required to achieve the precision of ϵ. It scales as $O(1/\epsilon^2)$ in the direct approach and $O(1/\epsilon)$ in the indirect approach, i.e., the phase estimation.

Next, we describe another method for the case where the quantum gate U is sufficiently local. It is the generalization

of the destructive swap test [7]. We say U is k-local if U can be decomposed into a tensor product of unitary matrices as $U = \bigotimes_q U_q$ and each U_q acts on at most k-qubit. With this definition, the result can be stated as follows.

Result 2. Let k be an integer such that $k = \text{poly} \log(n)$, where n is the number of qubits. For any k-local quantum gate U, it is possible to estimate $\langle \psi | U | \psi \rangle$ up to the precision ϵ in time $O(k^2 2^k / \epsilon^2)$ without the use of the Hadamard test, with classical preprocessing of time poly $\log(n)$.

This result follows from the following statements. From the definition of the k-local unitary matrix, U can be decomposed into $U = \bigotimes_{q=1}^{Q} U_q$. Let the number of qubits on which U_q acts and eigenvalues of U_q be k_q and $\{\exp(i\phi_{q,m})\}_{m=0}^{2^{k_q}-1}$, respectively, where $\phi_{q,m} \in [0, 2\pi]$. We denote the computational basis of each subsystem by $|m_q\rangle$ using integers $m_q = 0, \ldots, 2^{k_q} - 1$. In this setting, U_q is a $2^{k_q} \times 2^{k_q}$ matrix. With classical computation, we can diagonalize each U_q and obtain a unitary matrix V_q such that $U_q = V_q^\dagger D_q V_q$, where $D_q = \sum_{m=0}^{2^{k_q}-1} e^{i\phi_{q,m}} |m_q\rangle \langle m_q|$, in polynomial time to n by the assumption $k = O(\text{poly} \log(n))$. Then,

$$\langle \psi | U | \psi \rangle = \langle \psi | \left(\bigotimes_{q=1}^{Q} V_q^\dagger \sum_{m_q=0}^{2^{k_q}-1} \exp\left(i\phi_{q,m_q}\right) |m_q\rangle \langle m_q| V_q \right) | \psi \rangle \tag{1}$$

$$= \sum_{m_1=0}^{2^{k_1}-1} \cdots \sum_{m_Q=0}^{2^{k_Q}-1} \left(\prod_{q=1}^{Q} \exp\left(i\phi_{q,m_q}\right) \right)$$

$$\times \left| \left(\bigotimes_{q=1}^{Q} \langle m_q| \right) \left(\bigotimes_{q=1}^{Q} V_q \right) | \psi \rangle \right|^2. \tag{2}$$

Therefore, we can estimate $\langle \psi | U | \psi \rangle$ by evaluating the probability of getting the result $\bigotimes_{q=1}^{Q} |m_q\rangle$ from the measurement of $(\bigotimes_{q=1}^{Q} V_q) | \psi \rangle$ in the computational basis. More concretely, let the jth measurement result be $m_q^{(j)}$ and the total number of measurements be N. Then $\langle \psi | U | \psi \rangle$ is estimated by $\langle \psi | U | \psi \rangle \sim \frac{1}{N} \sum_{j=1}^{N} \prod_q \exp(i\phi_{q,m_q^{(j)}})$. The precision of the estimation $\epsilon = |\langle \psi | U | \psi \rangle - \frac{1}{N} \sum_{j=1}^{N} \prod_q \exp(i\phi_{q,m_q^{(j)}})|$ scales to $o(1/\sqrt{N})$ from the Hoeffding's inequality. Since the number of gates to implement V_q is bounded from above by $O(k_q^2 2^{k_q} \text{poly} \log(k_q^2 2^{k_q}))$ [24], the overall time for this protocol is $O(k^2 2^k \text{poly} \log(k^2 2^k)/\epsilon^2)$ with classical preprocessing for the diagonalization of each V_q in time $O(\text{poly} \log(n))$.

Note that in Results 1 and 2, the runtime dependence with respect to ϵ is $1/\epsilon^2$, which is quadratically worse than that of the phase estimation. In the phase estimation, the runtime directly translates to the depth of the quantum circuit, that is, we need a quantum device that can maintain its coherence for $O(1/\epsilon)$ time. Therefore, the phase estimation should be used if the time required to achieve a desired precision is sufficiently shorter than the coherence time. Otherwise, the direct measurement approach is advantageous, which is shown experimentally in Ref. [25].
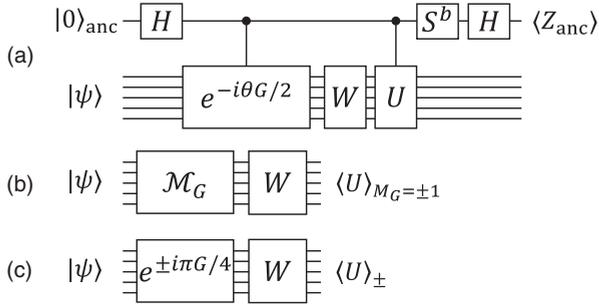
FIG. 2. (a) Hadamard test with two controlled gates. In the figure, W is an arbitrary quantum gate. (b), (c) Quantum circuits to estimate the output of (a) with direct measurement. $\mathcal{M}_G$ is the projective measurement of G.

B. Hadamard test with multiple controlled gates

Now we describe how to reduce a Hadamard test with multiple controlled gates to circuits without an ancilla qubit. The protocol given below is for the Hadamard test with two controlled gates [Fig. 2(a)]. It is straightforward to generalize the method to the case of more than two controlled gates. In the case of Fig. 2(a), the measured quantity is $\langle \psi | W^\dagger U W e^{-i\theta G/2} | \psi \rangle$. If we assume $G^2 = I$,

$$
\langle \psi | W^\dagger U W e^{-i\theta G/2} | \psi \rangle
$$
$$
= \cos\frac{\theta}{2} \langle \psi | W^\dagger U W | \psi \rangle - i \sin\frac{\theta}{2} \langle \psi | W^\dagger U W G | \psi \rangle. \quad (3)
$$

The first term on the right-hand side of the above formula is merely the expectation value of U with respect to the state $W | \psi \rangle$, therefore, if U satisfies one of the conditions mentioned in Results 1 and 2, we can evaluate it efficiently. Even if U does not satisfy either of the conditions, the protocol using the destructive swap test to measure $|\langle \psi | U | \psi \rangle|^2$ [13] can be utilized to estimate it using a quantum computer with $2n$ qubits. For the second term, we present a method involving a projective measurement of G, which we denote by $\mathcal{M}_G$. When G is a Pauli product, i.e., $G \in \{I, X, Y, Z\}^{\otimes n}$, $\mathcal{M}_G$ can be performed by first transferring G to a single qubit Z and then performing a measurement on the qubit nondestructively, for example with the dispersive readout of a superconducting qubit. This protocol for $\mathcal{M}_G$ can, in principle, be generalized to G such that the degeneracy of its eigenvalue ± 1 is equivalent although such a circuit can be exponentially hard to construct. On the other hand, for G which do not satisfy the above conditions, $\mathcal{M}_G$ requires an ancilla qubit due to the impossibility of transferring G to a single qubit Z. To estimate $\langle \psi | W^\dagger U W G | \psi \rangle$, we use the following four quantities for its estimation:

$$
\langle U \rangle_\pm = \langle \psi | e^{\mp i\pi G/4} W^\dagger U W e^{\pm i\pi G/4} | \psi \rangle, \quad (4)
$$

$$
\langle U \rangle_{M_G = \pm 1} = \frac{1}{4p(M_G = \pm 1)} \langle \psi | (I \pm G) W^\dagger U W (I \pm G) | \psi \rangle, \quad (5)
$$

where $p(M_G = \pm 1)$ is the probability of getting the result $M_G = \pm 1$ by performing $\mathcal{M}_G$ on $|\psi\rangle$; $p(M_G = \pm 1) = \| \frac{1}{2}(I \pm G) | \psi \rangle \|^2$. Figures 2(b) and 2(c) show the quantum

circuits to estimate these values. With these, $\langle \psi | W^\dagger U W G | \psi \rangle$ can be estimated by

$$
\langle \psi | W^\dagger U W G | \psi \rangle
$$
$$
= p(M_G = +1) \langle U \rangle_{M_G = +1} - p(M_G = -1) \langle U \rangle_{M_G = -1}
$$
$$
- \frac{i}{2} (\langle U \rangle_+ - \langle U \rangle_-). \quad (6)
$$

Note that when U is Hermitian, the first two terms correspond to the real part, and the rest correspond to the imaginary part of $\langle \psi | W^\dagger U W G | \psi \rangle$. Therefore, we can obtain the following.

Result 3. Let W and U be unitary matrices, and G be a Hermitian matrix. Suppose U satisfies one of the conditions specified in Results 1 or 2, and assume $G^2 = I$. It is possible to estimate the output of the circuit in Fig. 2(a), $\langle \psi | W^\dagger U W e^{-i\theta_1 G/2} | \psi \rangle$, by using the four quantum circuits in Figs. 2(b) and 2(c), and by combining their output with Eq. (6). In particular, if the eigenvalues ± 1 of G have equal degeneracy, the protocol works without an ancilla qubit. Even if U does not satisfy either of the conditions specified in Results 1 and 2, the protocol works with the method proposed in Ref. [13] that measures the expectation value of a unitary.

We can easily extend the strategy described in the above to evaluate the output from the Hadamard test in the case where it has more than two controlled gates (see Appendices A and B for details). By the construction of this method, the number of terms that we need to measure grows exponentially with the number of controlled gates. This is a limitation of our protocol. For example, we cannot reduce the depth of the circuit used in the iterative phase estimation, where the Hadamard test plays a crucial role, by our methods. However, this should not be a problem in practical uses of our method on NISQ devices. We aim to apply the proposed technique to algorithms on NISQ devices, such as quantum simulation and VQAs. As described later, this can be applied to measure multipoint correlators such as the OTOC, or to measure derivatives of variational quantum states in VQAs. Since the number of controlled gates to measure the multipoint correlators and the derivatives are proportional to the number of points and the order of differentiation, respectively, a user should not be concerned about the exponential scaling of the technique if he does not wish to measure higher order correlators or derivatives.

III. ADVANTAGE

Here we discuss the possible merits of our protocols. Results 1, 2, and 3 can provide a drastic reduction in the depth of a quantum circuit. The reduction is due to the fact that it is generally a hard task to make a controlled-U gate for a given U. For example, a Toffoli gate, which is a controlled-CNOT gate, requires at least six CNOT gates for its construction [26]. Along with the depth reduction, the removal of the ancilla qubit requirement is a nice advantage for qubit-limited, near-term quantum computers. Result 3 has the same advantages as the above, apart from the noise reduction effect. In the Hadamard tests of the type described in Fig. 2(a), the ancilla qubit has to tolerate a dephasing error during the gate W. In contrast, the ancilla qubit used in the protocol of Result 3

does not have to endure the noise; it is measured projectively at $\mathcal{M}_G$.

IV. APPLICATIONS

A. Derivatives in variational quantum algorithms

For the first application, we describe the direct measurement of derivatives of a parametrized quantum state. In VQAs such as the VQE [4], we employ a parametrized quantum circuit $U(\boldsymbol{\theta})$ and an input state $|\psi_{\text{in}}\rangle$ on an n-qubit quantum computer, and optimize the circuit parameter $\boldsymbol{\theta}$ with respect to an expectation value $\langle A(\boldsymbol{\theta}) \rangle = \langle \psi_{\text{in}} | U^{\dagger}(\boldsymbol{\theta}) A U(\boldsymbol{\theta}) | \psi_{\text{in}} \rangle$ of an observable A. Let us consider the case where the parametrized quantum circuit is constructed as $U(\boldsymbol{\theta}) = U_L(\theta_L) \cdots U_2(\theta_2) U_1(\theta_1)$ and each unitary $U_j(\theta_j)$ is generated by a Pauli product $P_j \in \{I, X, Y, Z\}^{\otimes n}$; $U_j(\theta_j) = \exp(-i\theta_j P_j/2)$. We denote $U_k(\theta_k) \cdots U_j(\theta_1)$ by $U_{k:j}$. In VQAs, we consider A which can be decomposed into a sum of Pauli products, and therefore, without loss of generality, we assume $A \in \{I, X, Y, Z\}^{\otimes n}$.

In Fig. 3(a), we show a quantum circuit to evaluate the analytic gradient of an expectation value of an observable A as presented in Ref. [15]. The circuit of Fig. 3(b) measures an equivalent quantity, and this circuit is equivalent to that in Fig. 2(a) when we replace $e^{-i\theta G/2}$ with P_j, U with A. Since we assumed A is a Pauli product, it satisfies the condition in Result 1. Therefore, Result 3 can be employed to measure the gradient. Note that the gradient of A is

$$\frac{\partial A}{\partial \theta_j} = \text{Im}(\langle \psi_{\text{in}} | U_{j:1}^{\dagger} U_{L:j+1}^{\dagger} A U_{L:j+1} P_j U_{j:1} | \psi_{\text{in}} \rangle), \quad (7)$$

which only involves the last two terms of Eq. (6), and hence we do not need to evaluate the circuit in Fig. 3(b). This gives the equivalent formulation given in Ref. [16]. This method can easily be extended to evaluate the Hessian (Appendix C).

The metric tensor $g_{jk} = \frac{\partial \langle \psi(\boldsymbol{\theta}) |}{\partial \theta_j} \frac{\partial |\psi(\boldsymbol{\theta}) \rangle}{\partial \theta_j}$ of a variational quantum state $|\psi(\boldsymbol{\theta})\rangle = U(\boldsymbol{\theta}) |\psi_{\text{in}}\rangle$ can be measured in the same manner. This quantity is the key for executing variational quantum simulations. Specifically, the imaginary and the real parts of g_{jk} are employed for the simulation of real [18] and imaginary time [19] evolutions, respectively. A quantum circuit for the measurement of g_{jk} from Refs. [18,19] is shown

FIG. 4. Quantum circuit for the estimation of the real and imaginary parts of the metric tensor g_{jk}. (a) Indirect method from Refs. [18,19]. $b \in \{0, 1\}$. When $b = 0$, $\langle Z_{\text{anc}} \rangle_{jk,0} = 4\text{Re}(g_{jk})$ and when $b = 1$, $\langle Z_{\text{anc}} \rangle_{jk,1} = 4\text{Im}(g_{jk})$. (b) Direct method to estimate the real part of g_{jk} [see Eq. (9)]. (c) Direct method to estimate the imaginary part of g_{jk} [see Eq. (10)].

as Fig. 4(a). The explicit expression for g_{jk}, when $k > j$, can be written as

$$g_{jk} = \frac{1}{4} \langle \psi_{\text{in}} | U_{j:1}^{\dagger} P_j U_{k:j+1}^{\dagger} P_k U_{k:1} | \psi_{\text{in}} \rangle. \quad (8)$$

Figure 4(a) shows the quantum circuit for the indirect measurement of g_{jk}. Again, from Result 3, this circuit can be replaced with the ones in Figs. 4(b) and 4(c). The explicit expression is

$$\text{Re}(g_{jk}) = \frac{1}{4} \big[p(M_{P_j} = +1) \langle P_k \rangle_{M_{P_j} = +1}$$
$$- p(M_{P_j} = -1) \langle P_k \rangle_{M_{P_j} = -1} \big], \quad (9)$$

$$\text{Im}(g_{jk}) = -\frac{\langle P_k \rangle_+ - \langle P_k \rangle_-}{8}. \quad (10)$$

Figure 4(a) differs from Fig. 2(a) with two additional X gates on the ancilla. The consequence of this is a change of sign in the imaginary part [compare Eqs. (10) and (6)].

B. Measurement of out-of-time-ordered correlation

Next, we propose a method to estimate the OTOC on quantum computers. The OTOC $F(t)$ at time t is defined with two noncommuting operators A and B and a system Hamiltonian H as $F(t) = \langle B^{\dagger}(t) A^{\dagger} B(t) A \rangle$, where $B(t) = e^{iHt} B e^{-iHt}$. This is an important quantity in quantum many-body physics which measures how chaotic a given quantum system is [20–23,27]. In Ref. [28] a circuit to evaluate $F(t)$ was proposed, which is shown in Fig. 5. If we assume $A^2 = I$, the circuits in Figs. 2(b) and 2(c) and Eq. (6) with a change of the sign of the imaginary part, which is the consequence of the X gates performed on the ancilla qubit, can be applied. More concretely, to evaluate $F(t)$, we replace W in Eq. (6) with $U^{\dagger}(t) B U(t)$, U and G with

FIG. 3. Quantum circuit for the estimation of $\frac{\partial \langle A(\boldsymbol{\theta}) \rangle}{\partial \theta_j}$. (a) The circuit with an ancillary qubit from [15]. Z_{anc} is the Pauli Z acting only on the ancillary qubit. The output of the circuit, $\langle Z_{\text{anc}} A \rangle_j$, is related to the gradient by $\langle Z_{\text{anc}} A \rangle = -\frac{\partial \langle A(\boldsymbol{\theta}) \rangle}{\partial \theta_j}$. (b) Quantum circuit which has equivalent output as (a); $\langle Z_{\text{anc}} A \rangle_j = \langle Z_{\text{anc}} \rangle_j$.
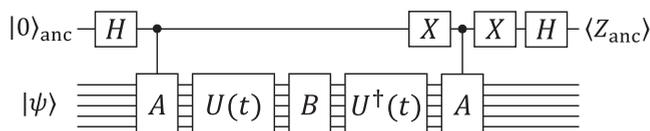
FIG. 5. Indirect approach to measure the OTOC of operators A and B from Ref. [28]. In the figure, $U(t) = e^{-iHt}$.

A. This method can easily be extended to the measurement of higher order correlators.

V. CONCLUSION

We provided general protocols to replace indirect measurements, in particular, the Hadamard test, with the direct measurement. The proposed methods to replace the Hadamard test provide a means to evaluate the analytical gradient, metric tensor, Hessian, and even higher order derivatives with direct measurements for parameter tuning in variational quantum algorithms. They can also be applied for the estimation of OTOCs. The presented protocols can significantly reduce the depth of a quantum circuit, and consequently, are important subroutines for quantum algorithms, especially for those of NISQ devices.

ACKNOWLEDGMENTS
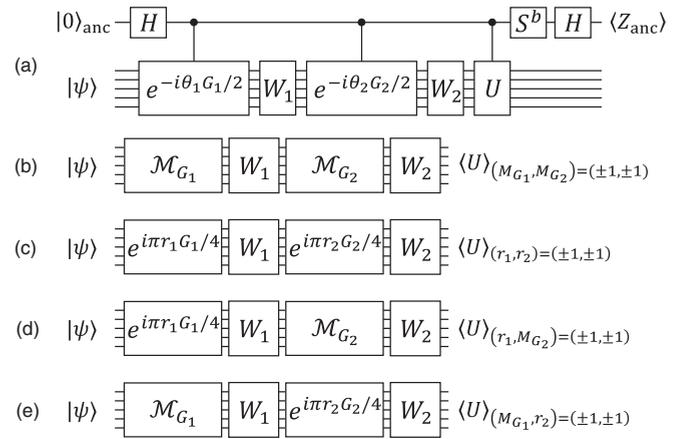
FIG. 6. Hadamard test with three controlled gates (a) and its replacement (b)–(e). In the figure, $b \in \{0, 1\}$ and U, H, S are an arbitrary quantum gate, the Hadamard gate, and $e^{-i\pi Z/4}$, respectively. When $b = 0$, $\langle Z \rangle = \mathrm{Re} \langle \psi_{\mathrm{in}}|U|\psi_{\mathrm{in}} \rangle$ and when $b = 1$, $\langle Z \rangle = \mathrm{Im} \langle \psi_{\mathrm{in}}|U|\psi_{\mathrm{in}} \rangle$.

APPENDIX A: THREE CONTROLLED GATES

In the main text, we have shown how to replace the Hadamard test with two controlled gates to the sequence of direct measurements. Here, as a simple extension, we show such a replacement for the one with three controlled gates in Fig. 6. The circuit in Fig. 6(a) can estimate the following quantity:

$$
\langle \psi | W_1^\dagger W_2^\dagger U W_2 e^{-i\theta_2 G_2/2} W_1 e^{-i\theta_1 G_1/2} |\psi \rangle
$$

$$
= \cos \frac{\theta_1}{2} \cos \frac{\theta_2}{2} \langle \psi | W_1^\dagger W_2^\dagger U W_2 W_1 |\psi \rangle - i \cos \frac{\theta_1}{2} \sin \frac{\theta_2}{2} \langle \psi | W_1^\dagger W_2^\dagger U W_2 G_2 W_1 |\psi \rangle
$$

$$
- i \sin \frac{\theta_1}{2} \cos \frac{\theta_2}{2} \langle \psi | W_1^\dagger W_2^\dagger U W_2 W_1 G_1 |\psi \rangle - \sin \frac{\theta_1}{2} \sin \frac{\theta_2}{2} \langle \psi | W_1^\dagger W_2^\dagger U W_2 G_2 W_1 G_1 |\psi \rangle . \tag{A1}
$$

If $b = 0$ the real part of the above can be obtained as $\langle Z_{\mathrm{anc}} \rangle$, and if $b = 1$ we get the imaginary part. In the above four terms, the first term, $\langle \psi | W_1^\dagger W_2^\dagger U W_2 W_1 |\psi \rangle$, can be estimated by measuring the expectation value of U with respect to $W_2 W_1 |\psi \rangle$. The second and third terms, $\langle \psi | W_1^\dagger W_2^\dagger U W_2 G_2 W_1 |\psi \rangle$ and $\langle \psi | W_1^\dagger W_2^\dagger U W_2 W_1 G_2 |\psi \rangle$, have the same structure as in the case of two controlled gates, which is described in the main text, and thus can be measured using the same strategy, that is, we can use Eq. (3) of the main text for the evaluation of these two terms. For the fourth term, we must use the circuits in Figs. 6(b)–6(e). Namely, we measure the following 16 quantities.

$$
\langle U \rangle_{(r_1, r_2)=(a_1, a_2)} = \langle \psi | e^{-a_1 i\pi G_1/4} W_1^\dagger e^{-a_2 i\pi G_2/4} W_2^\dagger U W_2 e^{a_2 i\pi G_1/4} W_1 e^{a_1 i\pi G_1/4} |\psi \rangle , \tag{A2}
$$

$$
\langle U \rangle_{(M_{G_1}, M_{G_2})=(a_1, a_2)} = \frac{\langle \psi | (I + a_1 G_1) W_1^\dagger (I + a_2 G_2) W_2^\dagger U W_2 (I + a_2 G_2) W_1 (I + a_1 G_1) |\psi \rangle}{16 p[(M_{G_1}, M_{G_2}) = (a_1, a_2)]} , \tag{A3}
$$

$$
\langle U \rangle_{(r_1, M_{G_2})=(a_1, a_2)} = \frac{\langle \psi | e^{-a_1 i\pi G_1/4} W_1^\dagger (I + a_2 G_2) W_2^\dagger U W_2 (I + a_2 G_2) W_1 e^{a_1 i\pi G_1/4} |\psi \rangle}{4 p(M_{G_2} = a_2 | r_1 = a_1)} , \tag{A4}
$$

$$
\langle U \rangle_{(M_{G_1}, r_2)=(a_1, a_2)} = \frac{\langle \psi | (I + a_1 G_1) W_1^\dagger e^{-a_2 i\pi G_2/4} W_2^\dagger U e^{-a_2 i\pi G_2/4} W_1 (I + a_1 G_1) |\psi \rangle}{4 p(M_{G_1} = a_1)} , \tag{A5}
$$

where the subscript r_i and M_{G_i} indicate which of a rotation generated by G_i or the projective measurement of G_i is inserted, $a_i \in \{-1, 1\}$ denotes directions of rotations and results of measurement, and

$$
p[(M_{G_1}, M_{G_2}) = (a_1, a_2)] = \left| \langle \psi | \frac{I + a_1 G_1}{2} W_1^\dagger \frac{I + a_2 G_2}{2} W_1 \frac{I + a_1 G_1}{2} |\psi \rangle \right|^2 , \tag{A6}
$$

$$p\big[(M_{G_1}, r_2) = (a_1, a_2)\big] = \left|\langle\psi|\frac{I + a_1 G_1}{2}|\psi\rangle\right|^2, \tag{A7}$$

$$p\big[(r_1, M_{G_2}) = (a_1, a_2)\big] = \left|\langle\psi|e^{a_1 i\pi G_1/4}W_1^\dagger\frac{I + a_2 G_2}{2}W_1 e^{a_1 i\pi G_1/4}|\psi\rangle\right|^2 \tag{A8}$$

is the probability of getting specific results at the measurements. The above system of equations, Eqs. (A2)–(A5) can be solved to obtain the desired quantities. The explicit expression of $\langle\psi|W_1^\dagger W_2^\dagger U W_2 G_2 W_1 G_1|\psi\rangle$ is

$$\langle\psi|W_1^\dagger W_2^\dagger U W_2 G_2 W_1 G_1|\psi\rangle = \sum_{a_1,a_2\in\{-1,1\}} a_1 a_2\Bigg(p\big[(M_{G_1}, M_{G_2}) = (a_1, a_2)\big]\langle U\rangle_{(M_{G_1}, M_{G_2})=(a_1, a_2)} - \frac{1}{4}\langle U\rangle_{(r_1, r_2)=(a_1, a_2)}$$
$$- \frac{i}{2}\big\{p\big[(M_{G_1}, r_2) = (a_1, a_2)\big]\langle U\rangle_{(M_{G_1}, r_2)=(a_1, a_2)} + p\big[(r_1, M_{G_2}) = (a_1, a_2)\big]\langle U\rangle_{(r_1, M_{G_2})=(a_1, a_2)}\big\}\Bigg). \tag{A9}$$

In a case where one of $e^{-i\theta_1 G_1/2}$, $e^{-i\theta_2 G_2/2}$ is controlled on the ancilla state being $|0\rangle$, we would want to measure $\langle\psi|W_1^\dagger G_2 W_2^\dagger U W_2 W_1 G_1|\psi\rangle$. It can also be obtained by solving Eqs. (A2)–(A5), that is,

$$\langle\psi|W_1^\dagger W_2^\dagger U W_2 G_2 W_1 G_1|\psi\rangle = \sum_{a_1,a_2\in\{-1,1\}} a_1 a_2\Bigg(p\big[(M_{G_1}, M_{G_2}) = (a_1, a_2)\big]\langle U\rangle_{(M_{G_1}, M_{G_2})=(a_1, a_2)} + \frac{1}{4}\langle U\rangle_{(r_1, r_2)=(a_1, a_2)}$$
$$+ \frac{i}{2}\big\{p\big[(M_{G_1}, r_2) = (a_1, a_2)\big]\langle U\rangle_{(M_{G_1}, r_2)=(a_1, a_2)} - p\big[(r_1, M_{G_2}) = (a_1, a_2)\big]\langle U\rangle_{(r_1, M_{G_2})=(a_1, a_2)}\big\}\Bigg). \tag{A10}$$

APPENDIX B: GENERAL CASE

We can extend the strategy to more general cases. An output from the Hadamard test with n controlled gates can be obtained from the following system of equations.

$$\langle U\rangle_{c_1, c_2, \ldots, c_n} = \langle\phi_{c_1,\ldots,c_n}|U|\phi_{c_1,\ldots,c_n}\rangle, \tag{B1}$$

where

$$|\phi_{c_1,\ldots,c_n}\rangle = C_{c_1,\ldots,c_n}W_n(1 + c_n G_n)\cdots W_2(1 + c_2 G_2)W_1(1 + c_1 G_1)|\psi\rangle, \tag{B2}$$

$c_j \in \{1, -1, i, -i\}$, and $C_{c_1,\ldots,c_n}$ is a normalization factor that guarantees $\langle\phi_{c_1,\ldots,c_n}|\phi_{c_1,\ldots,c_n}\rangle = 1$. Note that $c_j = \pm 1$ and $c_j = \pm i$ correspond to the projective measurement and the rotation, respectively. Since each c_j takes four possible values and we need to measure all combinations, the process takes $O(4^n)$ measurements.

APPENDIX C: GRADIENT AND HESSIAN EVALUATION

The gradient of an expectation value of A, $\langle A(\boldsymbol{\theta})\rangle = \langle\psi_{\text{in}}|U^\dagger(\boldsymbol{\theta})A U(\boldsymbol{\theta})|\psi_{\text{in}}\rangle$, where each U is a product of unitary matrices generated by a Pauli product P_j as $U_j(\theta_j) = \exp(-i\theta_j P_j/2)$, can be measured by using the following equation.

$$\frac{\partial\langle A(\boldsymbol{\theta})\rangle}{\partial\theta_j} = \frac{1}{2}\bigg[\Big\langle A\Big(\boldsymbol{\theta} + \frac{\pi}{2}\boldsymbol{e}_j\Big)\Big\rangle - \Big\langle A\Big(\boldsymbol{\theta} - \frac{\pi}{2}\boldsymbol{e}_j\Big)\Big\rangle\bigg], \tag{C1}$$

where $\boldsymbol{e}_j$ is a vector which has 0 as its elements except for 1 at the jth. As for the Hessian of $\langle A(\boldsymbol{\theta})\rangle$, one direct way to apply our result is (1) write down the explicit expression of the Hessian, (2) construct a circuit based on the Hadamard test with three controlled gates following the construction of the circuit in Fig. 3 in the main text, and (3) replace the circuit using our strategy. However, for the Hessian, we do not need to do those steps. Observe that, since we have the expression for the gradient as the above, we get

$$\frac{\partial}{\partial\theta_j}\frac{\partial\langle A(\boldsymbol{\theta})\rangle}{\partial\theta_j} = \frac{1}{2}\bigg[\frac{\partial}{\partial\theta_j}\Big\langle A\Big(\boldsymbol{\theta} + \frac{\pi}{2}\boldsymbol{e}_k\Big)\Big\rangle - \frac{\partial}{\partial\theta_j}\Big\langle A\Big(\boldsymbol{\theta} - \frac{\pi}{2}\boldsymbol{e}_k\Big)\Big\rangle\bigg]. \tag{C2}$$

Substituting each term by Eq. (C1), we obtain

$$\frac{\partial}{\partial\theta_j}\frac{\partial\langle A(\boldsymbol{\theta})\rangle}{\partial\theta_j} = \frac{1}{4}\bigg[\Big\langle A\Big(\boldsymbol{\theta} + \frac{\pi}{2}(\boldsymbol{e}_k + \boldsymbol{e}_j)\Big)\Big\rangle - \Big\langle A\Big(\boldsymbol{\theta} + \frac{\pi}{2}(\boldsymbol{e}_k - \boldsymbol{e}_j)\Big)\Big\rangle - \Big\langle A\Big(\boldsymbol{\theta} - \frac{\pi}{2}(\boldsymbol{e}_k + \boldsymbol{e}_j)\Big)\Big\rangle + \Big\langle A\Big(\boldsymbol{\theta} - \frac{\pi}{2}(\boldsymbol{e}_k - \boldsymbol{e}_j)\Big)\Big\rangle\bigg]. \tag{C3}$$

[1] E. Knill, G. Ortiz, and R. D. Somma, Phys. Rev. A **75**, 012328 (2007).

[2] M. Dobšíček, G. Johansson, V. Shumeiko, and G. Wendin, Phys. Rev. A **76**, 030306(R) (2007).

[3] J. Preskill, Quantum **2**, 79 (2018).

[4] A. Peruzzo, J. McClean, P. Shadbolt, M.-H. Yung, X.-Q. Zhou, P. J. Love, A. Aspuru-Guzik, and J. L. O'Brien, Nat. Commun. **5**, 4213 (2014).

[5] D. Wecker, M. B. Hastings, and M. Troyer, Phys. Rev. A **92**, 042303 (2015).

[6] D. Wang, O. Higgott, and S. Brierley, Phys. Rev. Lett. **122**, 140504 (2019).

[7] J. C. Garcia-Escartin and P. Chamorro-Posada, Phys. Rev. A **87**, 052330 (2013).

[8] H. Buhrman, R. Cleve, J. Watrous, and R. de Wolf, Phys. Rev. Lett. **87**, 167902 (2001).

[9] L. Cincio, Y. Subasi, A. T. Sornborger, and P. J. Coles, New J. Phys. **20**, 113022 (2018).

[10] O. Higgott, D. Wang, and S. Brierley, Quantum **3**, 156 (2019).

[11] T. Jones, S. Endo, S. McArdle, X. Yuan, and S. C. Benjamin, Phys. Rev. A **99**, 062304 (2019).

[12] R. LaRose, A. Tikku, É. O'Neel-Judy, L. Cincio, and P. J. Coles, npj Quantum Inf. **5**, 8 (2019).

[13] Y. Subaşı, L. Cincio, and P. J. Coles, J. Phys. A: Math. Theor. **52**, 044001 (2019).

[14] A. K. Ekert, C. M. Alves, D. K. L. Oi, M. Horodecki, P. Horodecki, and L. C. Kwek, Phys. Rev. Lett. **88**, 217901 (2002).

[15] G. G. Guerreschi and M. Smelyanskiy, arXiv:1701.01450.

[16] K. Mitarai, M. Negoro, M. Kitagawa, and K. Fujii, Phys. Rev. A **98**, 032309 (2018).

[17] J. Li, X. Yang, X. Peng, and C.-P. Sun, Phys. Rev. Lett. **118**, 150503 (2017).

[18] Y. Li and S. C. Benjamin, Phys. Rev. X **7**, 021050 (2017).

[19] S. McArdle, S. Endo, T. Jones, Y. Li, S. Benjamin, and X. Yuan, arXiv:1804.03023.

[20] E. B. Rozenbaum, S. Ganeshan, and V. Galitski, Phys. Rev. Lett. **118**, 086801 (2017).

[21] B. Swingle and D. Chowdhury, Phys. Rev. B **95**, 060201(R) (2017).

[22] Y. Huang, Y.-L. Zhang, and X. Chen, Ann. Phys. (NY) **529**, 1600318 (2017).

[23] D. A. Roberts and B. Yoshida, J. High Energy Phys. 04 (2017) 121.

[24] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, 2010).

[25] P. J. J. O'Malley, R. Babbush, I. D. Kivlichan, J. Romero, J. R. McClean, R. Barends, J. Kelly, P. Roushan, A. Tranter, N. Ding, B. Campbell, Y. Chen, Z. Chen, B. Chiaro, A. Dunsworth, A. G. Fowler, E. Jeffrey, E. Lucero, A. Megrant, J. Y. Mutus, M. Neeley, C. Neill, C. Quintana, D. Sank, A. Vainsencher, J. Wenner, T. C. White, P. V. Coveney, P. J. Love, H. Neven, A. Aspuru-Guzik, and J. M. Martinis, Phys. Rev. X **6**, 031007 (2016).

[26] V. V. Shende and I. L. Markov, Quant. Inf. Comp. **9**, 461 (2009).

[27] J. Dressel, J. R. González Alonso, M. Waegell, and N. Yunger Halpern, Phys. Rev. A **98**, 012132 (2018).

[28] B. Swingle, G. Bentsen, M. Schleier-Smith, and P. Hayden, Phys. Rev. A **94**, 040302(R) (2016).