



Implementation of a general single-qubit positive operator-valued measure on a circuit-based quantum computer

Yordan S. Yordanov  and Crispin H. W. Barnes 

Cavendish Laboratory, Department of Physics, University of Cambridge, Cambridge CB3 0HE, United Kingdom



(Received 30 July 2019; published 13 December 2019)

We derive a deterministic protocol to implement a general single-qubit positive operator-valued measure (POVM) on near-term circuit-based quantum computers. The protocol has a modular structure such that an n -element POVM is implemented as a sequence of $(n - 1)$ circuit modules. Each module performs a two-element POVM. Two variations of the protocol are suggested—one optimal in terms of number of ancilla qubits, the other optimal in terms of number of qubit gate operations and quantum circuit depth. We use the protocol to implement two- and three-element POVMs on two publicly available quantum computing devices. The results we obtain suggest that implementing nontrivial POVMs could be within the reach of the current noisy quantum computing devices.

DOI: [10.1103/PhysRevA.100.062317](https://doi.org/10.1103/PhysRevA.100.062317)

I. INTRODUCTION

In quantum mechanics positive operator-valued measures (POVMs) describe the most general form of quantum measurement. They are able to distinguish probabilistically between nonorthogonal quantum states [1] and can therefore be used to perform optimal state discrimination [2,3] and efficient quantum tomography [4,5]. In quantum communication and cryptography [6] they are used to enable secure device-independent communication [7] or, on the contrary, compromise quantum key distribution protocols by minimizing the damage done by an eavesdropper to a quantum channel [8,9].

POVMs can be implemented experimentally in both bosonic [10–13] and fermionic quantum systems [14]. However, typically, the hardware for these implementations needs to be specifically tailored to the measurement. To realize an arbitrary POVM as part of a quantum communication scheme or on a quantum computer, where the hardware design allows only orthogonal projective measurements in the qubit basis, it is necessary to simulate the action of the POVM using quantum-gate operations. For example, in Ref. [15] a quantum Fourier transform is used to implement a restricted class of projective POVMs. In Refs. [16,17] a probabilistic method based on classical randomness and postselection is proposed to implement projective POVMs. A deterministic method to perform a general POVM can be implemented using Neumark's dilation theorem [18,19], which states that a POVM of n elements can be performed as a projective measurement in an n -dimensional space. In Ref. [20] it is shown that this method can be realized in a duality quantum computer.

In this work we construct a protocol for a general single-qubit POVM on a circuit-based quantum computer using Neumark's theorem. The protocol has a modular structure such that a quantum circuit for an n -element POVM is constructed as a sequence of $(n - 1)$ two-element POVM circuit modules in a similar manner to Ref. [10]. This structure allows for

a straightforward construction of quantum circuits using an optimal number of ancilla qubits and quantum gates. The complexity of the protocol, in terms of number of quantum gates, is $O(n^2)$ using $\lceil \log_2 n \rceil$ ancilla qubits and can be reduced to $O(n \log n)$ at a cost of $(\lceil \log_2 n \rceil - 1)$ additional ancilla qubits. The corresponding circuit depths are $O(n^2)$ and $O(n)$, respectively. We use the protocol to implement two- and three-element POVMs on two public quantum computing devices: IBMQX2 and Aspen4. We measure the output fidelities and compare the performances of the two devices.

In Sec. II we present our protocol. We describe explicitly how to construct a quantum-gate circuit for a two-element POVM and demonstrate how it can be extended to an n -element POVM. In Sec. III we present the results from the POVM implementations on the two quantum devices. We present our concluding remarks in Sec. IV.

II. POVM PROTOCOL

A. Preliminaries

An n -element POVM is defined as a set of n positive operators $\{\hat{E}_i\}$ that satisfy the completeness relation $\sum_{i=1}^n \hat{E}_i = \hat{I}$, where $\hat{E}_i = \hat{M}_i^\dagger \hat{M}_i$ and the $\{\hat{M}_i\}$ are measurement operators. Performing a POVM on a system in initial state $|\psi_0\rangle$ results in wave-function reduction to one of n possible measurement outcomes $|\psi_0\rangle \rightarrow |\psi_i\rangle = \frac{\hat{M}_i|\psi_0\rangle}{\sqrt{\langle\psi_0|\hat{M}_i^\dagger\hat{M}_i|\psi_0\rangle}}$, with probability

$p_i = \langle\psi_0|\hat{M}_i^\dagger\hat{M}_i|\psi_0\rangle$. Using Neumark's theorem, an n -element POVM on a target system A can be performed by introducing an ancilla system B, with Hilbert space spanned by n orthonormal basis states $|i^{(B)}\rangle$ that are in one-to-one correspondence with the POVM measurement outcomes. A unitary operation \hat{U}_{AB} is applied to the joint state of the two systems, such that

$$\hat{U}_{AB}|\psi_0^{(A)}\rangle|0^{(B)}\rangle = \sum_{i=1}^n [\hat{M}_i|\psi_0^{(A)}\rangle]|i^{(B)}\rangle. \quad (1)$$

By performing a projective measurement on system B, system A collapses to one of the n states $\hat{M}_i|\psi_0^{(A)}\rangle$ that correspond to the outcomes of the POVM. For more details on POVM implementation refer to [21,22].

B. Protocol outline

Based on the method described above, we implement a n -element POVM on a target system consisting of a single qubit, using an ancilla system of $\lceil \log_2 n \rceil$ qubits. To implement \hat{U}_{AB} , we divide it into a sequence of $(n-1)$ quantum-gate circuits, which we call modules. Each of these modules, except the first, performs a two-element POVM on one of the outcomes of the preceding module and entangles the additionally produced outcome to a new state of the ancilla system.

C. Two-element POVM module

To construct a quantum circuit performing a two-element POVM, we need a single ancilla qubit. We assume the target qubit starts in an arbitrary state $|\psi_0\rangle = a|0\rangle + b|1\rangle$. Then the initial state of the system, target plus ancilla, is $|\Psi_0\rangle = |\psi_0\rangle|0\rangle$. To perform a two-element POVM we want to transform the system to a state

$$|\Psi_f\rangle = (\hat{M}_1|\psi_0\rangle)|o_1\rangle + (\hat{M}_2|\psi_0\rangle)|o_2\rangle, \quad (2)$$

where \hat{M}_1 and \hat{M}_2 are the two measurement operators and $|o_1\rangle$ and $|o_2\rangle$ are two orthogonal states of the ancilla. First a unitary gate \hat{U} (not to be confused with U_{AB}) is performed on the initial state of the target qubit:

$$|\Psi_0\rangle \rightarrow (\hat{U}|\psi_0\rangle)|0\rangle = (a'|0\rangle + b'|1\rangle)|0\rangle. \quad (3)$$

Then, two controlled y rotations are performed, acting on the ancilla qubit and controlled by the target qubit. The rotations are given by angles θ_1 and θ_2 , and controlled by the target qubit in states $|0\rangle$ or $|1\rangle$, respectively:

$$\begin{aligned} |\Psi\rangle \rightarrow & a'|0\rangle(\cos\theta_1|0\rangle + \sin\theta_1|1\rangle) \\ & + b'|1\rangle(\cos\theta_2|0\rangle + \sin\theta_2|1\rangle). \end{aligned} \quad (4)$$

Rearranging terms, the above state can be written as

$$|\Psi\rangle = (\hat{D}_1\hat{U}|\psi_0\rangle)|0\rangle + (\hat{D}_2\hat{U}|\psi_0\rangle)|1\rangle, \quad (5)$$

where $\hat{D}_1 = \cos\theta_1|0\rangle\langle 0| + \cos\theta_2|1\rangle\langle 1|$ and $\hat{D}_2 = \sin\theta_1|0\rangle\langle 0| + \sin\theta_2|1\rangle\langle 1|$. This result corresponds to performing a two-element POVM specified by arbitrary operators \hat{E}_1 and \hat{E}_2 . However, to fully specify the measurement operators \hat{M}_1 and \hat{M}_2 , we need to perform unitary operations \hat{V}_1 and \hat{V}_2 on the terms in the target qubit state, corresponding to the two outcomes of the POVM. This can be done by two single-qubit unitary gates acting on the target qubit, and controlled by the ancilla states corresponding to the two POVM outcomes, $|0\rangle$ and $|1\rangle$, respectively. This results in a final state

$$|\Psi\rangle \rightarrow |\Psi_f\rangle = (\hat{V}_1\hat{D}_1\hat{U}|\psi_0\rangle)|0\rangle + (\hat{V}_2\hat{D}_2\hat{U}|\psi_0\rangle)|1\rangle, \quad (6)$$

with $\hat{V}_1\hat{D}_1\hat{U} = \hat{M}_1$ and $\hat{V}_2\hat{D}_2\hat{U} = \hat{M}_2$. Since \hat{U} , \hat{V}_1 , and \hat{V}_2 are unitaries, and $\hat{D}_1\hat{D}_1^\dagger + \hat{D}_2\hat{D}_2^\dagger = I$, it is straightforward to check that \hat{M}_1 and \hat{M}_2 satisfy the completeness relation. Furthermore, the expressions for the two measurement operators are in most general form, since they correspond to

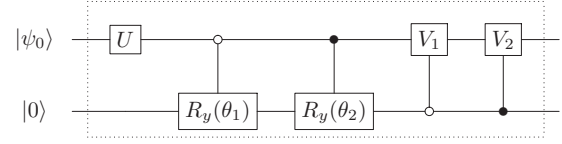


FIG. 1. A quantum circuit for a general single-qubit two-element POVM. The top qubit acts as the target and the bottom as the ancilla. The output state of the circuit is given by Eq. (6). $\hat{R}_y(\theta)$ denotes a controlled single-qubit y rotation by angle θ . \hat{U} , \hat{V}_1 , and \hat{V}_2 denote general single-qubit unitary operations. \hat{V}_1 and \hat{V}_2 are controlled operations, and each of them can be implemented as a combination of controlled z and y rotations. The circuit contains up to 12 CNOTs and 14 single-qubit rotations.

singular value decompositions. Therefore Eq. (6) corresponds to the outcomes of a general two-element POVM. Figure 1 illustrates the complete circuit for the two-element POVM module.

D. Generalization to n -element POVM

An n -element POVM can be performed sequentially by $(n-1)$ POVM modules that share an ancilla register of $\lceil \log_2 n \rceil$ qubits. The i th module in the sequence will be characterized by rotation angles $\theta_1^{(i)}$ and $\theta_2^{(i)}$, unitary operations $\hat{V}_1^{(i)}$ and $\hat{V}_2^{(i)}$, and two POVM outcomes with corresponding orthogonal ancilla register states $|o_1^{(i)}\rangle$ and $|o_2^{(i)}\rangle$. The first module is additionally characterized by the unitary \hat{U} acting on the target qubit, as shown above. Each of the modules, except the first one, performs a two-element POVM on the second outcome of the preceding module, so that the term in the target qubit state corresponding to this outcome is evolved in a similar way as for the case of the two-element POVM. The output state of the sequence of modules can be written as

$$|\Psi\rangle = \sum_{i=1}^{n-1} (\hat{M}_i|\psi_0\rangle)|o_1^{(i)}\rangle + (\hat{M}_n|\psi_0\rangle)|o_2^{(n-1)}\rangle, \quad (7)$$

with the measurement operators \hat{M}_i given by

$$\hat{M}_i = \begin{cases} \hat{M}_1 = \hat{V}_1^{(1)}\hat{D}_1^{(1)}, & \text{for } i = 1 \\ \hat{V}_1^{(i)}\hat{D}_1^{(i)} \prod_{j=1}^{i-1} (\hat{V}_2^{(j)}\hat{D}_2^{(j)})\hat{U}, & \text{for } 1 < i < n \\ \prod_{j=1}^{n-1} (\hat{V}_2^{(j)}\hat{D}_2^{(j)})\hat{U}, & \text{for } i = n, \end{cases} \quad (8)$$

where $\hat{D}_1^{(i)} = \cos\theta_1^{(i)}|0\rangle\langle 0| + \cos\theta_2^{(i)}|1\rangle\langle 1|$ and $\hat{D}_2^{(i)} = \sin\theta_1^{(i)}|0\rangle\langle 0| + \sin\theta_2^{(i)}|1\rangle\langle 1|$. These measurement operators satisfy the completeness relation and also represent singular value decompositions as in the case of the two-element POVM. Therefore Eq. (7) describes the outcomes of a general single-qubit n -element POVM. Appendix A presents an explicit procedure for the construction of a quantum circuit for the i th module. This procedure can be used iteratively to construct the whole n -element POVM. With a few additional operations the ancilla states $|0_{1/2}^{(j)}\rangle$ can be chosen so that the i th POVM outcome corresponds to the ancilla state with a binary value $(i-1)$. The quantum circuit for a POVM module sequence is illustrated in Fig. 4 in Appendix A.

E. Complexity and circuit depth

In Appendix B we show that the complexity, in terms of number of quantum gates, of the i th POVM module is $O(i)$. Summing over all modules, the complexity for an n -element POVM is $\sum_{i=1}^{n-1} O(i) = O(n^2)$. The depth of the quantum circuit, in terms of CNOTs, scales quadratically with n also. Alternatively, we can use $(\lceil \log_2 n \rceil - 1)$ additional ancilla qubits to reduce the complexity of the i th module to $O(\log i)$. This results in an overall complexity of $O(n \log n)$ for an n -element POVM. In this case the circuit depth for the i th module is constant (at most 18 CNOTs); hence the depth for a n -element POVM becomes linear in n . In the implementation of the two POVM examples in Sec. III, we use the quadratic method, however (which requires fewer ancilla qubits), since for $n = 2$ and $n = 3$, both methods use the same number of quantum gates and have equal maximum circuit depths.

F. Extension to N -qubit POVMs

The modular structure of this protocol can be extended to the case of a POVM on a d -level system by modifying the circuit of the POVM module. In the case of the single-qubit target system, we performed the two rotations θ_1 and θ_2 on the ancilla qubit [Eq. (4)], controlled by the two states of the target qubit. In the case of a d -level target system, we will have to perform d rotations, specified by angles $\{\theta_{i \in [1,d]}\}$ and controlled by the d different states of the target system. The output state of the two-element POVM module is, therefore, given again by Eq. (6), where this time \hat{U} , \hat{V}_1 , and \hat{V}_2 are d -dimensional unitary operations, $\hat{D}_1 = \sum_{i=0}^{d-1} \cos \theta_i |i\rangle\langle i|$ and $\hat{D}_2 = \sum_{i=0}^{d-1} \sin \theta_i |i\rangle\langle i|$. However, implementing any \hat{U} , \hat{V}_1 , and \hat{V}_2 now involve the generic problem of performing a general unitary operation on a multiqubit system. Therefore, the modular structure does simplify but does not fully solve the problem of implementing a general multiqubit POVM.

III. IMPLEMENTATION ON QUANTUM COMPUTING DEVICES

Using our protocol we implement a two- and three-element POVM on two public quantum computing devices: IBM's 5-qubit IBMQX2 [23], and Rigetti's 16-qubit Aspen4 [24]. These devices are capable of performing universal operations [25] on their qubit registers. However, they have high noise levels and imperfect qubit control, and hence are referred to as noisy intermediate-scale quantum (NISQ) devices [26].

A. Two-element POVM

First we consider an example of a two-element POVM that exhibits an output state with clear symmetry in terms of its outcomes. We choose two equal measurement operators, defined by $\theta_1 = \theta_2 = \frac{\pi}{4}$, $\hat{V}_1 = \hat{V}_2 = \hat{I}$, $\hat{U}_1 = \frac{1}{2} \begin{pmatrix} 1 & 0 \\ 0 & \sqrt{3} \end{pmatrix}$, and an initial target qubit state $|\psi_0\rangle = |0\rangle$. Note that the resulting measurement operators $\hat{M}_1 = \hat{M}_2 = \frac{1}{2} \begin{pmatrix} 1 & 0 \\ 0 & \sqrt{3} \end{pmatrix}$ are not projective. From Eq. (6) the expected output state is

$$|\Psi\rangle = \frac{(|0\rangle + \sqrt{3}|1\rangle)|0\rangle + (|0\rangle + \sqrt{3}|1\rangle)|1\rangle}{2\sqrt{2}}. \quad (9)$$

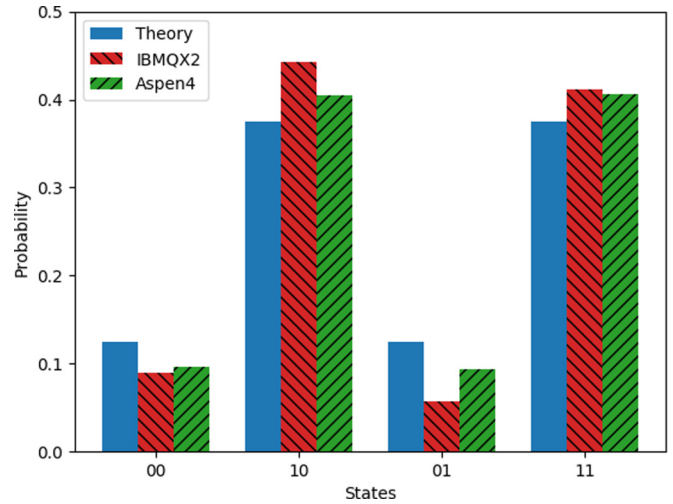


FIG. 2. Measurement probabilities for a two-element POVM, described by $\hat{M}_1 = \hat{M}_2 = \frac{1}{2} \begin{pmatrix} 1 & 0 \\ 0 & \sqrt{3} \end{pmatrix}$, on a qubit in an initial state $|0\rangle$. The IBMQX2 probabilities are obtained from 8192 runs of the circuit, and the Aspen4 probabilities from 10^4 runs. The expected probability values from Eq. (9) are included for reference.

Figure 2 presents the results for the two-element POVM from the two quantum devices. The Aspen4 output has a fidelity of 99.5%.¹ Although the outcome state of the target qubit is not obtained exactly, the expected symmetry between the states corresponding to the two POVM outcomes is obtained. The output from the IBMQX2 is less accurate with a fidelity of 98.0%, exhibiting asymmetry in the measurement probabilities for the values of the ancilla qubit corresponding to the two POVM outcomes. A possible reason for this asymmetry is the fact that IBMQX2 have different CNOT gate error rates depending on which qubit is the control or the target (see [23] for device characterization).

B. Three-element POVM

The second example we implement is a three-element POVM defined by measurement operators that project on three states separated by $\frac{2\pi}{3}$ rad in the x - z plane of the Bloch sphere:

$$\hat{M}_1 = \sqrt{\frac{2}{3}} |0\rangle\langle 0|, \quad (10)$$

$$\hat{M}_2 = \frac{1}{\sqrt{6}} \frac{|0\rangle + \sqrt{3}|1\rangle}{2} \frac{\langle 0| + \sqrt{3}\langle 1|}{2}, \quad (11)$$

$$\hat{M}_3 = \frac{1}{\sqrt{6}} \frac{|0\rangle - \sqrt{3}|1\rangle}{2} \frac{\langle 0| - \sqrt{3}\langle 1|}{2}. \quad (12)$$

This POVM is a classic example, often considered in literature, which can be used to distinguish between two nonorthogonal states (for example, between $|1\rangle$ and $\frac{\sqrt{3}|0\rangle + |1\rangle}{2}$). It is implemented using two POVM modules defined

¹The fidelity values are calculated as the overlap, $F = |\langle \psi | \phi \rangle|^2$, of two pure states instead of as $F = \langle \phi | \sigma_\psi | \phi \rangle$, where σ_ψ is the generally mixed state produced by a real device.

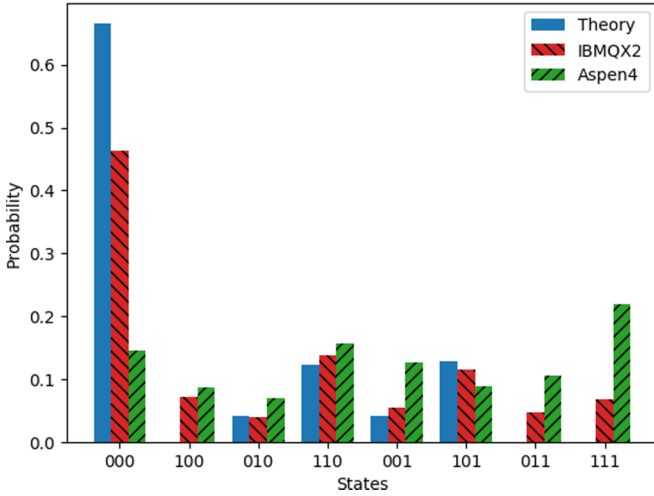


FIG. 3. Measurement probabilities for a three-element POVM, described by measurement operators given by Eqs. (10), (11), and (12), on a qubit in initial state $|0\rangle$. The IBMQX2 probabilities are obtained from 8192 runs of the circuit and the Aspen4 probabilities from 10^4 . The expected probability values from Eq. (13) are included for reference.

by $\theta_1^{(1)} = \cos^{-1}(\sqrt{\frac{2}{3}})$, $\theta_2^{(1)} = \frac{\pi}{2}$, $\theta_1^{(2)} = 0$, $\theta_2^{(2)} = \frac{\pi}{2}$, $\hat{U} = \hat{I}$, $\hat{V}_2^{(1)} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}$, $\hat{V}_1^{(1)} = \hat{I}$, $\hat{V}_1^{(2)} = \frac{1}{2}\begin{pmatrix} 1/\sqrt{3} & -\sqrt{3} \\ \sqrt{3} & 1 \end{pmatrix}$, and $\hat{V}_2^{(2)} = -\frac{1}{2}\begin{pmatrix} \sqrt{3} & -1 \\ 1 & \sqrt{3} \end{pmatrix}$. In Appendix C we outline explicitly the steps to construct a quantum circuit for the second POVM module. Substituting Eqs. (10), (11), and (12) in Eq. (7) for an initial target qubit in a state $|\psi_0\rangle = |0\rangle$, the expected output state is

$$\Psi = \sqrt{\frac{3}{2}}|0\rangle|00\rangle + \frac{|0\rangle + \sqrt{3}|1\rangle}{2\sqrt{6}}|10\rangle + \frac{|0\rangle - \sqrt{3}|1\rangle}{2\sqrt{6}}|01\rangle. \quad (13)$$

Figure 3 shows the results for the three-element POVM, obtained from the two quantum devices. In this case it is evident that the results from both devices suffer from significantly higher decoherence than in the case of the two-element POVM. The IBMQX2 performs better this time, obtaining an output state with fidelity 80.2%. It produces close to the expected values for the measurement probabilities of the $|010\rangle$, $|110\rangle$, $|001\rangle$, and $|101\rangle$ states. However, the state $|000\rangle$ seems to have decayed to the states with zero expected probability, $|100\rangle$, $|011\rangle$, and $|111\rangle$. The output from the Aspen4 has a fidelity of 46.6% and demonstrates little correlation with the expected output. The reason for these significantly worse results in the case of the three-element POVM is the depth and complexity of the quantum circuit. For comparison, the two-element POVM circuit has 6 CNOTs, resulting in a depth of 6 also, while the three-element POVM circuit has 30 CNOTs, with a maximum depth of 16 for the target qubit.

IV. CONCLUSION

In this paper we presented a deterministic protocol that enables a general POVM to be performed on a qubit in a circuit-based quantum computer using a conventional set

of single- and two-qubit quantum gates. We show that the same protocol can be modified so that it can be applied to several qubits. We implement the POVM as a projective measurement, using Neumark's theorem, on an ancilla register of qubits. The protocol therefore does not measure the target qubit and hence can be used as a subroutine in a larger protocol.

We use the protocol to implement two- and a three-element POVMs on two quantum computing devices: IBM's IBMQX2 and Rigetti's Aspen4. In the case of the two-element POVM, both devices produce high-fidelity results, with the Aspen4 being more accurate and consistent than the IBMQX2. For the three-element POVM, the results from both devices evidently suffer from strong decoherence. Nevertheless, the results of the IBMQX2 demonstrate good correlation with the expected output and fidelity of $\sim 80\%$. This result suggests that there is reason to be optimistic that given the regular upgrades of these devices, it might soon be possible to perform these measurements with high fidelity. This will open the way to their use in a wide variety of applications including quantum tomography and quantum cryptography.

ACKNOWLEDGMENTS

We acknowledge financial support from an EPSRC DTA award and an iCASE award sponsored by Hitachi Europe Ltd (EPSRC). We are grateful to IBM and Rigetti for the opportunity to use their cloud-based quantum computing services. We also would like to thank A. Andreev, A. Lasek, D. Arvidsson-Shukur, H. Lepage, J. Drori, and N. Devlin for useful discussions.

APPENDIX A: CONSTRUCTING THE i TH MODULE OF AN n -ELEMENT POVM

Here we describe the explicit steps to construct the i th module of an n -element POVM. The key is to entangle the two POVM outcomes of the module with suitable computational states of the ancilla register so that one can perform the same operations as in the case of the two-element POVM on the term in the target qubit state corresponding to the second output of the $(i-1)$ th module. To do this, consider the $(i-1)$ th and the i th modules of a POVM module sequence and the ancilla register states corresponding to their pairs of outcomes, $\{|o_1^{(i-1)}\rangle, |o_2^{(i-1)}\rangle\}$ and $\{|o_1^{(i)}\rangle, |o_2^{(i)}\rangle\}$, respectively. The explicit steps for constructing the i th module are as follows:

(1) Entangle the first POVM outcome of the i th module with the ancilla register state used for the second outcome of the $(i-1)$ th module, which is “redirected” to the i th module so it can be “reused.” Hence we get $|o_1^{(i)}\rangle = |o_2^{(i-1)}\rangle$.

(2) Entangle the second outcome of the i th module with the free computational ancilla register state with smallest binary value such that it differs by just one qubit (additional one in its binary expression) from $|o_1^{(i)}\rangle$. If there are no free ancilla register states, add another ancilla qubit in initial state $|0\rangle$.

(3) A $\theta_1^{(i)}$ and $\theta_2^{(i)}$ y rotation [similar to Eq. (4)], are performed on the ancilla qubit, differing between the $|o_1^{(i)}\rangle$ and $|o_2^{(i)}\rangle$ states. These two rotations are controlled by the other

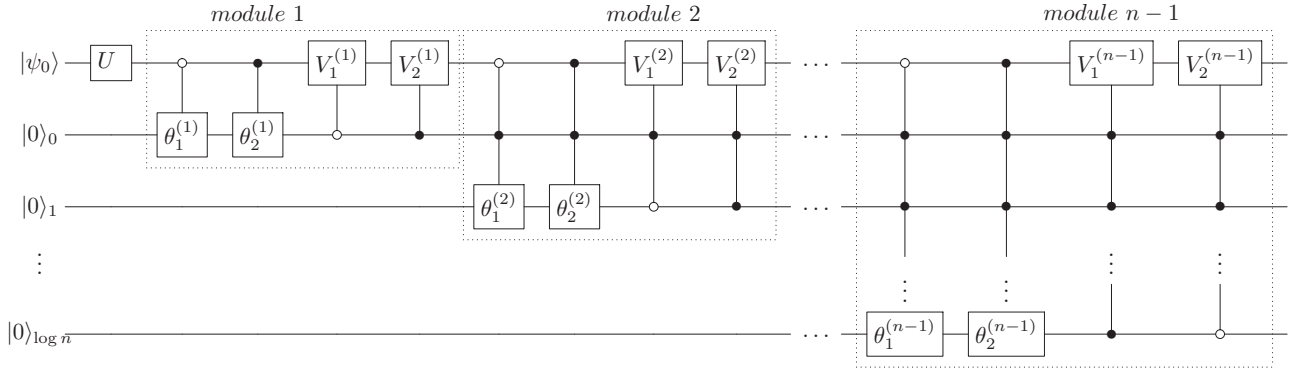


FIG. 4. Representation of a quantum circuit performing an n -element POVM as a sequence of $(n - 1)$ two-element POVM modules. The target qubit is in initial state $|\psi_0\rangle$, and each of the $\lceil \log_2 n \rceil$ ancilla qubits is in initial state $|0\rangle$. Each module consists of two controlled y -rotation gates and two controlled general unitary gates. For the k th module, these operations are controlled by the state of $\lceil \log_2 k \rceil$ qubits. The circuit has a maximum depth of $O(n^2)$ in terms of CNOT gates.

ancilla qubits, having the same values as in $|o_i^{(i)}\rangle$ and the target qubit in states $|0\rangle$ and $|1\rangle$, respectively.

(4) The ancilla state entangled to the second output of the i th module is changed to the unused ancilla register state with smallest binary value. This can be done by applying at most $(\lceil \log_2 i \rceil - 1)$ multiqubit CNOT gates. This is not a necessary step, but it ensures that all POVM outcomes are entangled to ancilla register states in order of increasing binary value.

(5) Finally, $\hat{V}_1^{(i)}$ and $\hat{V}_2^{(i)}$ general unitary operations are performed on the terms of the target qubit state corresponding to the two POVM outcomes of the i th module, entangled to $|o_1^{(i)}\rangle$ and $|o_2^{(i)}\rangle$, respectively. Each of these two unitaries is performed by two $\lceil \log_2 i \rceil$ -qubit-controlled-rotation gates.

Following these steps the i th module transforms the joint state of the target and the ancilla systems after the $(i - 1)$ th module as

$$\begin{aligned}
 |\Psi_{i-1}\rangle &= \sum_{k=0}^{i-2} [\hat{M}_{k+1}|\psi_0\rangle]|k\rangle + \left(\prod_{k=1}^{i-1} \hat{V}_2^{(k)} \hat{D}_2^{(k)} \right) \hat{U} |\psi_0\rangle |i-1\rangle \rightarrow \\
 |\Psi_i\rangle &= \sum_{k=0}^{i-2} [\hat{M}_{k+1}|\psi_0\rangle]|k\rangle + \hat{V}_1^{(i)} \hat{D}_1^{(i)} \left(\prod_{k=1}^{i-1} \hat{V}_2^{(k)} \hat{D}_2^{(k)} \right) \hat{U} |\psi_0\rangle |i-1\rangle + \left(\prod_{k=1}^i \hat{V}_2^{(k)} \hat{D}_2^{(k)} \right) \hat{U} |\psi_0\rangle |i\rangle \\
 &= \sum_{k=0}^{i-1} [\hat{M}_{k+1}|\psi_0\rangle]|k\rangle + \left(\prod_{k=1}^i \hat{V}_2^{(k)} \hat{D}_2^{(k)} \right) \hat{U} |\psi_0\rangle |i\rangle, \tag{A1}
 \end{aligned}$$

where $\hat{D}_1^{(k)} = \cos \theta_1^{(k)} |0\rangle\langle 0| + \cos \theta_2^{(k)} |1\rangle\langle 1|$ and $\hat{D}_2^{(k)} = \sin \theta_1^{(k)} |0\rangle\langle 0| + \sin \theta_2^{(k)} |1\rangle\langle 1|$. In this way we can obtain the output state in Eq. (7) with measurement operators given by Eq. (8). Additionally, the ancilla register state entangled to the k th outcome of the POVM is $|k - 1\rangle$, the state with binary value $(k - 1)$. Constructing an iterative program which performs the same steps for each module is straightforward. The example of constructing a three-element POVM is included in Appendix C.

APPENDIX B: MULTIQUBIT CONTROLLED OPERATIONS AND ANALYSIS OF THE COMPLEXITY

Multiqubit controlled operations are used extensively in our POVM protocol. To carry out a rotation around a single axis of the Bloch sphere of a qubit q_0 controlled by qubits $q_1 \dots q_m$, the rotation is decomposed to two rotations with

$m - 1$ control qubits as

$$\begin{aligned}
 CR_i(\theta, q_1 \dots q_m, q_0) &= \text{CNOT}(q_1, q_0) CR_i\left(-\frac{\theta}{2}, q_2 \dots q_m, q_0\right) \\
 &\quad \times \text{CNOT}(q_1, q_0) CR_i\left(\frac{\theta}{2}, q_2 \dots q_m, q_0\right), \tag{B1}
 \end{aligned}$$

where $i \in \{x, y, z\}$, and CR stands for controlled rotation. By decomposing each controlled rotation further, the overall operation can be brought down to $(2^m - 2)$ CNOTs and $2m$ 1-qubit rotations. Therefore the complexity of this method is exponential with m —the number of control qubits. An alternative method, suggested in [27,28], has linear complexity in terms of m ; however, it needs $m - 1$ additional ancilla qubits. For the examples of the two- and three-element POVMs considered in this paper, the exponential method is preferred, which, for the case of two-qubit controlled gates, has the same complexity and circuit depth as the linear method (both

require six CNOTs and two single-qubit rotations) but does not need an additional ancilla qubit. Nevertheless when implementing many-element POVMs, use of the linear method should be considered.

To find the overall complexity of the protocol for an n -element POVM in terms of number of quantum gates, consider first the complexity of a single module. The i th module requires up to $6 \lceil \log_2 i \rceil$ -qubit controlled operations. Therefore its complexity is either $O(i)$ or $O(\log i)$, respectively, depending on whether the exponential or the linear method for a multiqubit controlled operations is used. The depth of the circuit for the i th module in these two cases is linear with i , $0(i)$, or constant, $O(1)$, respectively.

APPENDIX C: CONSTRUCTING A CIRCUIT FOR THE SECOND POVM MODULE

This section illustrates the procedure for constructing the i th POVM module with the explicit example of the second module of a three-element POVM. The three POVM outcomes require a three-dimensional ancilla space; therefore we need a 2-qubit ancilla register. Starting with the output state of the first POVM module, the system state can be written as

$$\begin{aligned} |\Psi\rangle &= (\hat{V}_1^{(1)} \hat{D}_1^{(1)} \hat{U} |\psi_0\rangle) |00\rangle + (\hat{V}_2^{(1)} \hat{D}_2^{(1)} \hat{U} |\Psi_0\rangle) |10\rangle \\ &= \hat{M}_1 |\psi_0\rangle |00\rangle + (c|0\rangle + d|1\rangle) |10\rangle, \end{aligned} \quad (C1)$$

where an additional ancilla qubit in state $|0\rangle$ is added, and c and d are coefficients such that $(c|0\rangle + d|1\rangle) = \hat{V}_2^{(1)} \hat{D}_2^{(1)} \hat{U} |\psi_0\rangle$. Now we carry out the steps outlined in Appendix A:

(1) Associate the two outcomes of the second module with ancilla register states $|o_1^{(2)}\rangle = |10\rangle$ and $|o_2^{(2)}\rangle = |11\rangle$ (at the end we will change $|o_2^{(2)}\rangle$ to $|01\rangle$).

(2) Perform $\theta_1^{(2)}$ and $\theta_2^{(2)}$ rotations over the second ancilla qubit controlled by the first ancilla qubit in state $|1\rangle$ and the target qubit in states $|0\rangle$ and $|1\rangle$, respectively:

$$\begin{aligned} |\Psi\rangle &\rightarrow |\psi_1\rangle |00\rangle + (c \cos \theta_1^{(2)} |0\rangle + d \cos \theta_2^{(2)} |1\rangle) |10\rangle \\ &\quad + (c \sin \theta_1^{(2)} |0\rangle + d \sin \theta_2^{(2)} |1\rangle) |11\rangle. \end{aligned} \quad (C2)$$

(3) Using a doubly controlled X gate (equivalent to Toffoli gate) change $|o_2^{(2)}\rangle \rightarrow |01\rangle$ so that the POVM outcomes are entangled to states ordered in increasing binary value (taking the leftmost qubit as the least significant bit). Hence,

$$\begin{aligned} |\Psi\rangle &\rightarrow |\psi_1\rangle |00\rangle + (\hat{D}_1^{(2)} \hat{V}_2^{(1)} \hat{D}_2^{(1)} \hat{U} |\Psi_0\rangle) |10\rangle \\ &\quad + (\hat{D}_2^{(2)} \hat{V}_2^{(1)} \hat{D}_2^{(1)} \hat{U} |\Psi_0\rangle) |01\rangle \end{aligned} \quad (C3)$$

(4) Unitary operations $\hat{V}_1^{(2)}$ and $\hat{V}_2^{(2)}$ are performed on the target qubit, controlled by the ancilla register states $|o_1^{(2)}\rangle$ and $|o_2^{(2)}\rangle$, respectively. The system state at this point can be expressed as

$$|\Psi\rangle = (\hat{M}_1 |\psi_0\rangle) |00\rangle + (\hat{M}_2 |\psi_0\rangle) |10\rangle + (\hat{M}_3 |\psi_0\rangle) |01\rangle, \quad (C4)$$

where

$$\hat{M}_1 = \hat{V}_1^{(1)} \hat{D}_1^{(1)} \hat{U}, \quad (C5)$$

$$\hat{M}_2 = \hat{V}_1^{(2)} \hat{D}_1^{(2)} \hat{V}_2^{(1)} \hat{D}_2^{(1)} \hat{U}, \quad (C6)$$

$$\hat{M}_3 = \hat{V}_2^{(2)} \hat{D}_2^{(2)} \hat{V}_2^{(1)} \hat{D}_2^{(1)} \hat{U}. \quad (C7)$$

-
- [1] A. Peres and D. R. Terno, Optimal distinction between non-orthogonal quantum states, *J. Phys. A: Math. Gen.* **31**, 7105 (1998).
- [2] G. A. Steudle, S. Knauer, U. Herzog, E. Stock, V. A. Haisler, D. Bimberg, and O. Benson, Experimental optimal maximum-confidence discrimination and optimal unambiguous discrimination of two mixed single-photon states, *Phys. Rev. A* **83**, 050304(R) (2011).
- [3] M. Dusek and V. Buzek, Quantum-controlled measurement device for quantum-state discrimination, *Phys. Rev. A* **66**, 022112 (2002).
- [4] A. Bisio, G. Chiribella, G. M. D'Ariano, S. Facchini, and P. Perinotti, Optimal Quantum Tomography of States, Measurements, and Transformations, *Phys. Rev. Lett.* **102**, 010404 (2009).
- [5] D. Petz and L. Ruppert, Optimal quantum-state tomography with known parameters, *J. Phys. A: Math. Theor.* **45**, 085306 (2012).
- [6] S. D. Bartlett, T. Rudolph, and R. W. Spekkens, Classical and Quantum Communication without a Shared Reference Frame, *Phys. Rev. Lett.* **91**, 027901 (2003).
- [7] C. C. W. Lim, C. Portmann, M. Tomamichel, and N. Gisin, Device-Independent Quantum Key Distribution with Local Bell Test, *Phys. Rev. X* **3**, 031006 (2013).
- [8] A. K. Ekert, B. Huttner, G. M. Palma, and A. Peres, Eavesdropping on quantum-cryptographical systems, *Phys. Rev. A* **50**, 1047 (1994).
- [9] H. E. Brandt, J. M. Myers, and S. J. Lomonaco, Aspects of entangled translucent eavesdropping in quantum cryptography, *Phys. Rev. A* **56**, 4456 (1997).
- [10] S. E. Ahnert and M. C. Payne, General implementation of all possible positive-operator-value measurements of single-photon polarization states, *Phys. Rev. A* **71**, 012330 (2005).
- [11] S. E. Ahnert and M. C. Payne, All possible bipartite positive-operator-value measurements of two-photon polarization states, *Phys. Rev. A* **73**, 022333 (2006).
- [12] Z. Bian, J. Li, H. Qin, X. Zhan, R. Zhang, B. C. Sanders, and P. Xue, Realization of Single-Qubit Positive-Operator-Valued Measurement via a One-Dimensional Photonic Quantum Walk, *Phys. Rev. Lett.* **114**, 203602 (2015).
- [13] P. Kurzyński, Y.-y. Zhao, N.-k. Yu, and G.-C. Guo, Experimental realization of generalized qubit measurements based on quantum walks, *Phys. Rev. A* **91**, 042101 (2015).
- [14] D. R. M. Arvidsson-Shukur, H. V. Lepage, E. T. Owen, T. Ferrus, and C. H. W. Barnes, Protocol for fermionic positive-operator-valued measures, *Phys. Rev. A* **96**, 052305 (2017).

- [15] T. Decker, D. Janzing, and T. Beth, Quantum circuits for single-qubit measurements corresponding to platonic solids, *Int. J. Quantum Inf.* **2**, 353 (2004).
- [16] M. Oszmaniec, F. B. Maciejewski, and Z. Puchała, Simulating all quantum measurements using only projective measurements and postselection, *Phys. Rev. A* **100**, 012351 (2019).
- [17] P. Wittek, M. Oszmaniec, L. Guerini, and A. Acn, Simulating Positive-Operator-Valued Measures with Projective Measurements, *Phys. Rev. Lett.* **119**, 190501 (2017).
- [18] M. A. Naimark, A. I. Loginov, and V. S. Shul'man, Non-self-adjoint operator algebras in Hilbert space, *J. Sov. Math.* **5**, 250 (1976).
- [19] A. Peres, Neumark's theorem and quantum inseparability, *Found. Phys.* **20**, 1441 (1990).
- [20] Y. Liu and J.-X. Cui, Realization of Kraus operators and POVM measurements using a duality quantum computer, *Chin. Sci. Bull.* **59**, 2298 (2014).
- [21] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*, 2nd ed. (Cambridge University Press, Cambridge, 2010), pp. 90–93.
- [22] J. Preskill, *Lecture Notes for Ph219/CS219: Quantum Information. Foundations II: Measurement and Evolution* (California Institute of Technology, California, 2018), Chap. 3, pp. 5–19.
- [23] IBM Q, <https://quantum-computing.ibm.com>.
- [24] Rigetti, www.rigetti.com.
- [25] D. P. DiVincenzo, Two-bit gates are universal for quantum computation, *Phys. Rev. A* **51**, 1015 (1995).
- [26] J. Preskill, Quantum computing in the NISQ era and beyond, *Quantum* **2**, 79 (2018).
- [27] A. Barenco, C. H. Bennett, R. Cleve, D. P. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J. Smolin, and H. Weinfurter, Elementary gates for quantum computation, *Phys. Rev. A* **52**, 3457 (1995).
- [28] R. Jozsa, *Quantum Computation Lecture Notes, Exercise Sheet 2* (University of Cambridge, Cambridge, 2019), p. 3.