

Robust Extraction of Tomographic Information via Randomized Benchmarking

Shelby Kimmel*

*Center for Theoretical Physics, Massachusetts Institute of Technology,
Cambridge, Massachusetts 02139, USA and Raytheon BBN Technologies,
Quantum Information Processing Group, Cambridge, Massachusetts 02138, USA*

Marcus P. da Silva,[†] Colm A. Ryan, Blake R. Johnson, and Thomas Ohki
*Raytheon BBN Technologies, Quantum Information Processing Group, Cambridge,
Massachusetts 02138, USA*

(Received 21 June 2013; published 25 March 2014)

We describe how randomized benchmarking can be used to reconstruct the unital part of any trace-preserving quantum map, which in turn is sufficient for the full characterization of any unitary evolution or, more generally, any unital trace-preserving evolution. This approach inherits randomized benchmarking's robustness to preparation, measurement, and gate imperfections, thereby avoiding systematic errors caused by these imperfections. We also extend these techniques to efficiently estimate the average fidelity of a quantum map to unitary maps outside of the Clifford group. The unitaries we consider correspond to large circuits commonly used as building blocks to achieve scalable, universal, and fault-tolerant quantum computation. Hence, we can efficiently verify all such subcomponents of a circuit-based universal quantum computer. In addition, we rigorously bound the time and sampling complexities of randomized benchmarking procedures, proving that the required nonlinear estimation problem can be solved efficiently.

DOI: 10.1103/PhysRevX.4.011050

Subject Areas: Quantum Physics, Quantum Information

I. INTRODUCTION

While quantum process tomography [1] is a conceptually simple approach to the characterization of quantum operations on states, its implementation suffers from a number of fundamental drawbacks. These obstacles range from its exponential scaling with the size of the system to its dependence on precise knowledge of state preparation and measurement. Precise knowledge about state preparation requires precise knowledge about operations and measurements, leading to a difficult nonlinear estimation problem [2–5]. Lack of precise knowledge about state preparation and measurement can also lead to significant systematic errors in the reconstructed operations [6]. Recently, randomized benchmarking (RB) protocols have been shown to lead to estimates of the average fidelity to Clifford group operations in a manner that is robust against imprecise knowledge about state preparation and measurement, and therefore largely free of some of the systematic errors that can affect standard tomographic reconstructions [7–12].

We describe a procedure that provides an almost complete description of any quantum map in a way that is robust against many errors that plague standard tomographic procedures. Specifically, we can estimate the unital part [13,14] of any trace-preserving map, which includes all parameters necessary to describe deterministic as well as random unitary evolution. Furthermore, we show that a related protocol can be used to efficiently estimate the average fidelity to unitary operations outside the Clifford group, again in a way that is accurate even in the presence of state preparation, measurement, and unitary control errors.

Both procedures use RB protocols as a tool, combined with several new results: We show that Clifford group maps span the unital subspace of quantum maps and that important unitaries outside the Clifford group can be expressed as linear combinations of a few Clifford group maps. These insights, combined with new error strategies and analysis, allow us to robustly characterize maps that were previously inaccessible.

Our error analysis rigorously proves that randomized benchmarking decays can be fit efficiently. We also prove new results on the average fidelity of composed maps, which is important for RB, but is also of significance to any procedure where direct access to a quantum map is limited.

This paper is organized as follows. In Sec. II, we give background on general properties of quantum operations. In Sec. III, we sketch the RB protocol and describe the information that can be extracted from such experiments. In Sec. IV, we describe how the information from RB

*Corresponding author.
skimmel@mit.edu

[†]Corresponding author.
msilva@bbn.com

experiments can be used to tomographically reconstruct the unital part of any experimental map even in the presence of imperfect randomizing operations. In Sec. V, we show that it is possible to efficiently bound the fidelity of any experimental map to a class of unitaries capable of universal quantum computation. Finally, in Sec. VI, we analyze error propagation in these protocols. This section includes new bounds on the effect of imperfect randomizing operations and rigorous bounds on the number of samples needed to achieve some desired error and confidence.

II. COMPLETELY POSITIVE TRACE-PRESERVING MAPS: NOTATION AND PROPERTIES

Throughout this paper, we will restrict the discussion to Hermiticity-preserving linear operations on quantum states—more specifically, linear operations on multiqubit states such that the Hilbert space dimension will always be $d = 2^n$ for n qubits. The physical operations within this class that are commonly considered are completely positive (CP) trace-preserving (TP) operations [15–17]. We refer to these operations on quantum systems as maps and will denote them by the calligraphic fonts \mathcal{A} , \mathcal{B} , etc. The composition of two maps will be denoted $\mathcal{A} \circ \mathcal{B}$, meaning \mathcal{B} acts on a state first and then \mathcal{A} acts on it. Even when discussing unitary evolution, we will refer to the corresponding maps. The notable exceptions are the identity unitary $\hat{\mathbb{I}}$ and the unitaries in the multiqubit Pauli group \mathbf{P} , which will be denoted \hat{P}_i —although the corresponding maps \mathcal{I} and \mathcal{P}_i will also be used in some contexts. We will use the standard convention where $\hat{P}_0 = \hat{\mathbb{I}}$. We use \mathcal{T} to mean the map corresponding to the unitary $e^{-i\hat{\mathcal{Z}}}$.

A map \mathcal{E} is TP iff $\text{tr}\hat{\rho} = \text{tr}\mathcal{E}(\hat{\rho})$ for all $\hat{\rho}$, which in turn leads to the requirement that $\mathcal{E}^\dagger(\hat{\mathbb{I}}) = \hat{\mathbb{I}}$, where \mathcal{E}^\dagger is the Heisenberg picture representation of \mathcal{E} . Any linear map \mathcal{E} can be written as

$$\mathcal{E}(\hat{\rho}) = \sum_{i,j=0}^{d^2-1} \chi_{ij}^{\mathcal{E}} \hat{P}_i \hat{\rho} \hat{P}_j, \quad (2.1)$$

which is known as the χ matrix representation of \mathcal{E} . The map \mathcal{E} is CP iff $\chi^{\mathcal{E}}$ is positive semidefinite, and the TP condition $\mathcal{E}^\dagger(\hat{\mathbb{I}}) = \hat{\mathbb{I}}$ translates to $\sum_{ij} \chi_{ij}^{\mathcal{E}} \hat{P}_j \hat{P}_i = \hat{\mathbb{I}}$, which implies $\text{tr}\chi^{\mathcal{E}} = 1$ [1]. A map \mathcal{E} is unital if $\mathcal{E}(\hat{\mathbb{I}}) = \hat{\mathbb{I}}$.

It is often necessary to compute the representation of the composition of two maps. While such a calculation can be cumbersome in the χ representation, Liouville representations are more convenient for describing the action of composed maps on quantum states [18]. In the Liouville representation, an operator $\hat{\rho}$ is represented by a column vector $|\hat{\rho}\rangle\rangle$, and maps are represented by matrices acting on these vectors, such that the composition of maps corresponds to matrix multiplication. The most convenient choice of basis for these vectors and matrices depends on the application, but for our purposes, we will use the basis

of Pauli operators and will call this the Pauli-Liouville representation (which appears to have no standard name in the literature, despite being widely used [19–24]). For a map \mathcal{E} , the Pauli-Liouville representation is given by

$$\mathcal{E}^{(\text{PL})} = \sum_{i,j=0}^{d^2-1} \frac{\text{tr}[\mathcal{E}(\hat{P}_i)\hat{P}_j]}{d} |i\rangle\langle j|, \quad (2.2)$$

where \hat{P}_i and \hat{P}_j are n -qubit Pauli operators. Hermiticity preservation implies that all matrix elements of $\mathcal{E}^{(\text{PL})}$ are real. The k th entry in the vector $|\hat{\rho}\rangle\rangle$ representing a density matrix $\hat{\rho}$ corresponds to $\text{tr}\hat{\rho}\hat{P}_k$. This ensures that the Pauli-Liouville representation of any CPTP map can be written as [19,20]

$$\mathcal{E}^{(\text{PL})} = \begin{pmatrix} 1 & \vec{0}^T \\ \vec{\tau}_e & \mathbf{E} \end{pmatrix}, \quad (2.3)$$

where $\vec{\tau}_e$ is a $d^2 - 1$ -dimensional column vector, $\vec{0}$ is the corresponding zero vector, and \mathbf{E} is a $(d^2 - 1) \times (d^2 - 1)$ matrix.

We will quantify how distinct a map \mathcal{E} is from a particular unitary map \mathcal{U} by the average fidelity $\bar{F}(\mathcal{E}, \mathcal{U})$, which can be written as

$$\bar{F}(\mathcal{E}, \mathcal{U}) = \int d\mu(\psi) \langle \psi | (\mathcal{U}^\dagger \circ \mathcal{E}(|\psi\rangle\langle\psi|)) | \psi \rangle, \quad (2.4)$$

with integration taken over the unitarily invariant Fubini-Study measure [14]. This definition also implies $\bar{F}(\mathcal{E}, \mathcal{U}) = \bar{F}(\mathcal{E} \circ \mathcal{U}^\dagger, \mathcal{I}) = \bar{F}(\mathcal{U}^\dagger \circ \mathcal{E}, \mathcal{I})$. The average fidelity is closely related to the trace overlap between $\mathcal{E}^{(\text{PL})}$ and $\mathcal{U}^{(\text{PL})}$, as well as to $\chi_{00}^{\mathcal{E} \circ \mathcal{U}^\dagger}$, by the formulas [25,26]

$$\bar{F}(\mathcal{E}, \mathcal{U}) = \frac{\text{tr}\mathcal{U}^\dagger \mathcal{E} + d}{d(d+1)}, \quad (2.5)$$

$$= \frac{\chi_{00}^{\mathcal{U}^\dagger \circ \mathcal{E}} d + 1}{d+1}. \quad (2.6)$$

For simplicity and clarity, here and throughout the paper, we omit the superscripts from the Pauli-Liouville representation of superoperators whenever they occur within trace expressions, as these expressions already include superscripts indicating Hermitian conjugates.

III. RANDOMIZED BENCHMARKING OF CLIFFORD GROUP MAPS

RB [7–12] consists of a family of protocols to robustly estimate the average fidelity $\bar{F}(\mathcal{E}, \mathcal{U})$ between an experimental quantum map \mathcal{E} and an ideal unitary map \mathcal{U} . In this context, robustness refers to the ability to estimate $\bar{F}(\mathcal{E}, \mathcal{U})$ in a manner that is insensitive to imprecise or even biased knowledge about state preparation, measurement, and controlled unitary evolution. Such imperfections can lead to systematic errors, e.g., in fidelity estimates based on standard tomographic reconstruction protocols [5].

We now describe a framework that can be used to understand existing RB protocols but which allows us to highlight how our protocol differs from previous procedures. RB protocols consist of k repeated applications of \mathcal{E} , each time preceded by independently chosen randomizing unitary maps \mathcal{D}_i , where $1 \leq i \leq k$, and, after the last application of \mathcal{E} , followed by a recovery map \mathcal{D}_{k+1} . The randomizing unitaries are chosen such that if (i) the sequence is applied to a fixed initial state $|\psi\rangle$, (ii) \mathcal{E} is identical to a certain unitary map \mathcal{U} , and (iii) the randomizing maps \mathcal{D}_i are perfect, then the final state would be identical to the initial state. If the first k randomizing operations are chosen from the Haar measure over unitary maps [7,14] or from a set with the same first- and second-order moments as the Haar measure [27], the fidelity between the initial and final states can be shown to decay exponentially with k at a rate that depends only on $\bar{F}(\mathcal{E}, \mathcal{U})$ [7,9,10]. The RB literature typically assumes either (1) $\mathcal{U} = \mathcal{I}$ and \mathcal{E} represents the errors from the randomizing operations, or (2) \mathcal{U} is some other unitary map, and \mathcal{E} is its potentially faulty implementation. However, we emphasize that our description is more general, and as we will demonstrate later, it allows us to reconstruct a major portion of *arbitrary* \mathcal{E} , not just implementations of the randomizing operations.

In a realistic setting, one cannot assume that the initial state is pure and exactly known, that one knows what observable is measured exactly, or that the randomizing operations are applied noiselessly. However, these assumptions are not necessary for the RB protocol to work: the initial state can be any mixed state $\hat{\rho}_0 \neq \frac{1}{d}\hat{\mathbb{I}}$, the measured observable \hat{M} can be any observable where $\text{tr}\hat{\rho}_0\hat{M} \neq \frac{1}{d}\text{tr}\hat{M}$, and the rate of decay p of the measured expectation value is still related to $\bar{F}(\mathcal{E}, \mathcal{U})$ in the same way. The randomizing operations need not be noiseless either [9,10], as long as the imperfect randomizing operations correspond to $\mathcal{N} \circ \mathcal{D}_i$, with \mathcal{N} representing some arbitrary CPTP error map (some of these restrictions may be relaxed, leading to more complex decays [9,10], and although our protocols generalize straightforwardly to such scenarios, we do not discuss them here for the sake of brevity). Under these more realistic assumptions, $F_k(\mathcal{E}, \mathcal{U})$, the average of $\langle \hat{M} \rangle$ over the choice of randomizing operations, for sequences of length k , is given by

$$F_k(\mathcal{E}, \mathcal{U}) = A_0 p^k + B_0, \quad (3.1)$$

where A_0 and B_0 are constants that contain partial information about the preparation and measurement (including imperfections), and

$$p = \frac{d\bar{F}(\mathcal{E} \circ \mathcal{N}, \mathcal{U}) - 1}{d - 1}, \quad (3.2)$$

$$= \frac{\text{tr}\mathcal{U}^\dagger \mathcal{E} \mathcal{N} - 1}{d^2 - 1}. \quad (3.3)$$

By estimating $F_k(\mathcal{E}, \mathcal{U})$ for different values of k , it is possible to isolate p (which contains the desired information about \mathcal{E}) from A_0 and B_0 (which contain the undesired information about preparation and measurement), creating a protocol that is largely free of systematic errors caused by imprecise knowledge of state preparation and measurement [28].

Case (1) discussed above is the original scenario considered in the RB literature [7–10], where $\mathcal{U} = \mathcal{I}$ and $\mathcal{E} = \mathcal{I}$, so the observed decay leads to a direct estimate of $\bar{F}(\mathcal{N}, \mathcal{I})$, i.e., how well the randomization operations are implemented. Case (2) discussed above is the extension of RB to the extraction of information about $\bar{F}(\mathcal{E}, \mathcal{U})$, where \mathcal{E} is one of the randomizing operations in the experiment and \mathcal{U} is its unitary idealization. This is a recent development sometimes referred to as interleaved RB [11,12], but we do not make such a distinction in this paper. The previously known result in this case is that $\bar{F}(\mathcal{E}, \mathcal{U})$ can be bounded by experimentally estimating $\bar{F}(\mathcal{E} \circ \mathcal{N}, \mathcal{U})$ and $\bar{F}(\mathcal{N}, \mathcal{I})$, and in Sec. VI A, we provide more general bounds (with fewer assumptions) for the same purpose.

While the RB protocol is valid for any choice of randomizing operations discussed above, we emphasize that, in order to ensure that the protocols remain scalable in the number of qubits, \mathcal{U} and \mathcal{D}_i are restricted to be unitary maps in the Clifford group, since this allows for scalable design of the randomizing sequences via the Gottesman-Knill theorem [29]. Moreover, although previous works have applied the RB protocols only to \mathcal{E} very close to Clifford group maps, we emphasize that no restriction beyond \mathcal{E} being CPTP needs to be imposed. The restricted applications of the RB protocols in previous work were partially due to the fact that the bounds used to isolate $\bar{F}(\mathcal{E}, \mathcal{U})$ are only useful when \mathcal{E} is close to a Clifford group map. Since we are interested in extracting information about arbitrary \mathcal{E} , here we consider tomographic reconstruction techniques that *do not* rely on these bounds. We also design efficient techniques for average-fidelity estimates that rely on new and improved general bounds on $\bar{F}(\mathcal{E}, \mathcal{U})$.

In summary, RB allows for efficient estimation of $\bar{F}(\mathcal{E} \circ \mathcal{N}, \mathcal{U})$ and efficient bounding of $\bar{F}(\mathcal{E}, \mathcal{U})$ for \mathcal{U} in the Clifford group. These estimates can be obtained without relying on perfect information about preparation and measurement errors, thereby avoiding some of the systematic errors that may be present in standard tomographic protocols because of these imperfections.

A. RB sequence design

A compact way to describe how RB sequences are constructed refers back to the idea of twirling [27,30–33]. Although this is not how this construction is typically

described, we find it to be convenient and include it for completeness.

If \mathcal{E} is an arbitrary quantum map, and \mathbf{S} is a set of maps $\{\mathcal{C}_0, \dots\}$, the average map

$$\mathbb{E}_i[\mathcal{C}_i^\dagger \circ \mathcal{U}^\dagger \circ \mathcal{E} \circ \mathcal{C}_i] = \frac{1}{|\mathbf{S}|} \sum_{\mathcal{C}_i \in \mathbf{S}} \mathcal{C}_i^\dagger \circ \mathcal{U}^\dagger \circ \mathcal{E} \circ \mathcal{C}_i \quad (3.4)$$

is called the twirl of $\mathcal{U}^\dagger \circ \mathcal{E}$ over \mathbf{S} , where \mathbb{E}_i denotes the expectation value over uniformly random choices for $\mathcal{C}_i \in \mathbf{S}$. If \mathbf{S} is the Clifford group or any other unitary 2-design [27], then

$$\mathbb{E}_i[\mathcal{C}_i^\dagger \circ \mathcal{U}^\dagger \circ \mathcal{E} \circ \mathcal{C}_i(\hat{\rho})] = p\hat{\rho} + \frac{(1-p)}{d} \hat{\mathbb{I}}, \quad (3.5)$$

where $p = \frac{\text{tr} \mathcal{U}^\dagger \mathcal{E} - 1}{d^2 - 1} = \frac{d\bar{F}(\mathcal{E}, \mathcal{U}) - 1}{d-1}$ as before.

A length k RB sequence consists of applying the twirled channel repeatedly to the same state k times, i.e.,

$$\begin{aligned} \mathbb{E}_{\vec{i}}[\mathcal{C}_{i_k}^\dagger \circ \mathcal{U}^\dagger \circ \mathcal{E} \circ \mathcal{C}_{i_k} \circ \dots \circ \mathcal{C}_{i_1}^\dagger \circ \mathcal{U}^\dagger \circ \mathcal{E} \circ \mathcal{C}_{i_1}(\hat{\rho})], \\ = \mathbb{E}_{\vec{i}}[\mathcal{D}_{i_{k+1}} \circ \mathcal{E} \circ \mathcal{D}_{i_k} \circ \mathcal{E} \circ \mathcal{D}_{i_{k-1}} \circ \dots \circ \mathcal{D}_{i_2} \circ \mathcal{E} \circ \mathcal{D}_{i_1}(\hat{\rho})], \\ = p^k \hat{\rho} + \frac{(1-p^k)}{d} \hat{\mathbb{I}}, \end{aligned} \quad (3.6)$$

where

$$\mathcal{D}_{i_\ell} = \begin{cases} \mathcal{C}_{i_1} & \ell = 1 \\ \mathcal{C}_{i_\ell} \circ \mathcal{C}_{i_{\ell-1}}^\dagger \circ \mathcal{U}^\dagger & 1 < \ell \leq k \\ \mathcal{C}_{i_k}^\dagger \circ \mathcal{U}^\dagger & \ell = k+1, \end{cases} \quad (3.7)$$

and $\mathbb{E}_{\vec{i}}$ denotes the expectation value over uniformly random choices for $\mathcal{C}_{i_\ell} \in \mathbf{S}$ for all ℓ .

The RB protocol to estimate $\bar{F}(\mathcal{E}, \mathcal{U})$ then consists of (i) choosing a sequence of \mathcal{C}_{i_ℓ} for $1 < \ell \leq k$, (ii) applying the alternating sequence of \mathcal{D}_{i_ℓ} and \mathcal{E} , as prescribed in (3.6), to a fixed initial state, (iii) measuring the resulting state, and (iv) averaging over random choices for \mathcal{C}_{i_ℓ} to obtain F_k . The F_k can be fit against (3.1), yielding an estimate for p , even in the presence of imperfections. As we prove in Sec. VI, this estimate can be obtained efficiently in the number of qubits, desired accuracy, and confidence. Note that neither \mathcal{E} nor \mathcal{U} needs to be an element of the Clifford group. However, we will generally consider the case where \mathcal{E} is *not* a Clifford group map, while \mathcal{U} *will* be chosen to be a Clifford group map. Choosing \mathcal{U} to be a Clifford group element makes the design of the experiments for n qubits efficient [10,29], while leaving \mathcal{E} unconstrained affords us greater flexibility and has no impact on the design of the experiment.

IV. TOMOGRAPHIC RECONSTRUCTION FROM RB

As discussed above, RB can efficiently provide bounds on the fidelities of an arbitrary CPTP map \mathcal{E} with any element of the Clifford group—in a manner that is robust against preparation and measurement errors, as well as imperfections in the twirling operations. Here, we demonstrate that the collection of such fidelities of a fixed \mathcal{E} to a set of linearly independent Clifford group maps can be used to reconstruct a large portion of \mathcal{E} . The advantage of this approach is that the robustness properties of the estimates obtained via RB carry over to this tomographic reconstruction.

Using the Liouville representation of quantum maps, it is clear that an estimate of the average fidelity $\bar{F}(\mathcal{E}, \mathcal{U})$ leads to an estimate of $\text{tr} \mathcal{U}^\dagger \mathcal{E}$, and thus, all information that can be extracted from these fidelities for a fixed \mathcal{E} is contained in the projection of \mathcal{E} onto the linear span of unitary maps. It is unnecessary to consider the span of arbitrary unitary maps, as the following result demonstrates (see Appendix A for the proof).

Lemma IV.1.—The linear span of unitary maps coincides with the linear span of Clifford group unitary maps. Moreover, the projection of a TP map to this linear span is a unital map.

Given a set of linearly independent vectors that span a subspace, and the inner product of an unknown vector with all elements of that set, it is a simple linear algebraic exercise to determine the projection of the unknown vector onto the subspace. Similarly, measuring the average fidelity of some TP map \mathcal{E} to a Clifford group map \mathcal{C}_i is equivalent to measuring such an inner product—the matrix inner product $\text{tr}(\mathcal{E} \mathcal{C}_i^\dagger)$. Since Clifford maps span the unital subspace of quantum CPTP maps, measuring the inner product of \mathcal{E} with a set of maximal linearly independent elements of the Clifford group is sufficient to reconstruct the projection of \mathcal{E} onto the unital subspace. We call this projection the unital part of \mathcal{E} and denote it by \mathcal{E}' .

Since the unitality condition constrains only how the map acts on the identity component of a state, \mathcal{E}' can be obtained by changing how \mathcal{E} acts on that component. Defining \mathcal{Q} to be the projector into the identity component of any operator and \mathcal{Q}^\perp to be the projection into the orthogonal complement (i.e., $\mathcal{Q} + \mathcal{Q}^\perp = \mathcal{I}$), one finds that

$$\mathcal{E} = \mathcal{E} \circ (\mathcal{Q}^\perp + \mathcal{Q}) = \mathcal{E} \circ \mathcal{Q}^\perp + \mathcal{E} \circ \mathcal{Q}, \quad (4.1)$$

$$\mathcal{E}' = \mathcal{E} \circ \mathcal{Q}^\perp + \mathcal{Q}, \quad (4.2)$$

which indicates that \mathcal{E} and \mathcal{E}' map traceless operators in the same way. The maps \mathcal{E} and \mathcal{E}' have Pauli-Liouville representations

$$\mathcal{E}^{(\text{PL})} = \begin{pmatrix} 1 & \vec{0}^T \\ \vec{\tau}_e & \mathbf{E} \end{pmatrix}, \quad \mathcal{E}'^{(\text{PL})} = \begin{pmatrix} 1 & \vec{0}^T \\ \vec{0} & \mathbf{E} \end{pmatrix}, \quad (4.3)$$

so we refer to $\vec{\tau}_e$ as the nonunital part of \mathcal{E} . It is then clear that \mathcal{E}' is described by $(d^2 - 1)^2$ real parameters if \mathcal{E} is TP, while \mathcal{E} itself is described by $(d^2 - 1)d^2$ real parameters. The unital part of \mathcal{E} contains the vast majority of the parameters needed to describe \mathcal{E} —in fact, over 93% of the parameters for two qubits and over 99% of the parameters for four qubits.

As discussed, one limitation of RB is that in a realistic setting, it can only provide bounds for $\bar{F}(\mathcal{E}, \mathcal{C}_i)$ (and therefore $\text{tr}\mathcal{E}\mathcal{C}_i^\dagger$) because of the imperfections in the randomizing operations. Clearly, these bounds can only lead to a description of parameter-space regions compatible with \mathcal{E}' as opposed to any point estimator, even in the absence of statistical fluctuations. Our approach to reconstruct \mathcal{E}' is to avoid these bounds altogether and instead use the following result, which we prove in Appendix B.

Lemma IV.2.—If $(\mathcal{E} \circ \mathcal{N})'$ is the unital part of $\mathcal{E} \circ \mathcal{N}$ and \mathcal{N}' is the unital part of \mathcal{N} , and all these operations are trace preserving, then $\mathcal{E}' = (\mathcal{E} \circ \mathcal{N})' \circ (\mathcal{N}')^{-1}$ whenever $(\mathcal{N}')^{-1}$ exists.

This allows us to reconstruct \mathcal{E}' from the reconstructions of $(\mathcal{E} \circ \mathcal{N})'$ and \mathcal{N}' . As both $(\mathcal{E} \circ \mathcal{N})'$ and \mathcal{N}' are related directly to decay rates, we can create a point estimate of \mathcal{E}' , without recourse to the bounds needed in standard RB to characterize \mathcal{E} .

It should be noted that the only cases where $(\mathcal{N}')^{-1}$ does not exist are when \mathcal{N} completely dephases some set of observables (i.e., maps them to something proportional to the identity). However, the experimental setting where tomographic reconstructions are interesting is precisely in the regime where \mathcal{N} is far from depolarizing any observable, so $(\mathcal{N}')^{-1}$ is typically well defined [34]. The penalty, of course, is that the application of $(\mathcal{N}')^{-1}$ leads to greater statistical uncertainty in the estimate of \mathcal{E}' thanks to the uncertainties in the reconstructions of \mathcal{N}' and $(\mathcal{E} \circ \mathcal{N})'$ as well as uncertainty propagation due to multiplication by $(\mathcal{N}')^{-1}$. However, larger experimental ensembles can be used to compensate for this, as is discussed in the section that follows.

Moreover, writing the imperfect randomizing operations as $\mathcal{N} \circ \mathcal{C}_i$ instead of $\mathcal{C}_i \circ \mathcal{N}^*$ for some different map \mathcal{N}^* is merely a convention, and Lemma IV.2 can be trivially adjusted to such a different convention. In the physical regimes where RB estimates are expected to be valid, the choice of conventions is largely immaterial (see Appendix E for more details).

This result shows that the average fidelities with a spanning set of Clifford group unitary maps can lead not only to a point estimator of the unital part of any TP map but also to a point estimator of the average fidelity of \mathcal{E} to any unitary map—i.e., information from multiple RB experiments can eliminate the need for the loose bounds

on the average fidelity considered in Ref. [12]. This comes at the cost of efficiency, as the unital part of a map—like the complete map—contains an exponential number of parameters. However, for a small number of qubits, the overhead of reconstructing the unital part is small, and therefore, it is still advantageous to perform this cancellation to get better estimates of the error.

A. Example: Single-qubit maps

In order to reconstruct the unital part of a single-qubit map, one must first consider a set of linearly independent maps corresponding to unitaries in the Clifford group. As this group contains 24 elements, there are many different choices for a linearly independent set spanning the ten-dimensional unital subspace. One particular choice of unitaries leading to linearly independent maps is

$$\hat{C}_0 = \hat{\mathbb{I}}, \quad \hat{C}_1 = e^{-i\frac{\pi}{2}\hat{X}}, \quad (4.4)$$

$$\hat{C}_2 = e^{-i\frac{\pi}{2}\hat{Y}}, \quad \hat{C}_3 = e^{-i\frac{\pi}{2}\hat{Z}}, \quad (4.5)$$

$$\hat{C}_4 = e^{-i\frac{\pi\hat{X}+\hat{Y}+\hat{Z}}{3}\sqrt{3}}, \quad \hat{C}_5 = e^{-i\frac{2\pi\hat{X}+\hat{Y}+\hat{Z}}{3}\sqrt{3}}, \quad (4.6)$$

$$\hat{C}_6 = e^{-i\frac{\pi\hat{X}-\hat{Y}+\hat{Z}}{3}\sqrt{3}}, \quad \hat{C}_7 = e^{-i\frac{2\pi\hat{X}-\hat{Y}+\hat{Z}}{3}\sqrt{3}}, \quad (4.7)$$

$$\hat{C}_8 = e^{-i\frac{\pi\hat{X}+\hat{Y}-\hat{Z}}{3}\sqrt{3}}, \quad \hat{C}_9 = e^{-i\frac{2\pi\hat{X}+\hat{Y}-\hat{Z}}{3}\sqrt{3}}. \quad (4.8)$$

In a noiseless setting, estimating the average fidelities between these Clifford maps and the map

$$\mathcal{H}^{(\text{PL})} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} \quad (4.9)$$

corresponding to the single-qubit Hadamard gate leads to the decays illustrated in Fig. 1. The corresponding p values are

$$p_0 = p_2 = p_8 = p_9 = -\frac{1}{3}, \quad (4.10)$$

$$p_1 = p_3 = p_4 = p_5 = p_6 = p_7 = \frac{1}{3}. \quad (4.11)$$

Note, in particular, that some p values are negative, which simply indicates an oscillatory exponential-decay behavior. While these decay rates are much larger (i.e., the p values are much smaller) than those typically seen in previous RB protocols, we show in Sec. VI B that it is possible to efficiently estimate any decay rate to fixed accuracy, no matter the size.

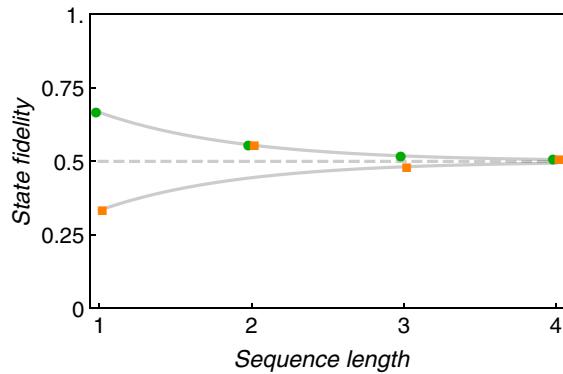


FIG. 1. RB decays used to estimate the fidelity between an ideal Hadamard gate and \hat{C}_0 (green circles, with $p = \frac{1}{3}$) and \hat{C}_1 (orange squares, with $p = -\frac{1}{3}$). The decays corresponding to each of the remaining average fidelities coincide with one of these two representative decays. Note that these decays are much faster than decays previously estimated in RB, as they correspond to the average fidelities between very different maps. The data points are offset along the x axis for clarity.

If one considers a noisy setting, where \mathcal{N} is not the identity, the decay rates are modified by \mathcal{N} , but after reconstructing \mathcal{N}' and $(\mathcal{E} \circ \mathcal{N})'$ separately, one is able to reconstruct \mathcal{E}' . To see that errors in the estimate of \mathcal{N}' will not create unmanageable errors in the estimate of \mathcal{E} , consider how errors in the estimate of \mathcal{N}' affect the estimate of $(\mathcal{N}')^{-1}$. The relative error in the estimate of $(\mathcal{N}')^{-1}$ is given by [35]

$$\frac{\|(\mathcal{N}')^{-1} - (\mathcal{N}' + \mathcal{G}')^{-1}\|}{\|(\mathcal{N}')^{-1}\|} \leq \frac{\kappa(\mathcal{N}')}{1 - \kappa(\mathcal{N}') \frac{\|\mathcal{G}'\|}{\|\mathcal{N}'\|}} \frac{\|\mathcal{G}'\|}{\|\mathcal{N}'\|}, \quad (4.12)$$

as long as

$$\|\mathcal{G}'\| \|\mathcal{N}'^{-1}\| < 1, \quad (4.13)$$

where \mathcal{G}' is the error in the estimate of \mathcal{N}' , and $\kappa(\mathcal{N}')$ is the condition number for the matrix inversion of \mathcal{N}' with respect to the matrix norm $\|\cdot\|$. The condition number of \mathcal{A} is given by $\kappa(\mathcal{A}) = \|\mathcal{A}^{-1}\| \|\mathcal{A}\|$ if \mathcal{A} is nonsingular and ∞ otherwise.

If we choose $\|\cdot\|$ to be the spectral norm, even when \mathcal{N}' is the depolarizing map $\mathcal{D}(\hat{p}) = \delta\hat{p} + (1 - \delta)\frac{\hat{1}}{d}$, the condition number of \mathcal{N}' is given by $\kappa(\mathcal{N}') = \frac{1}{|\delta|}$. Similarly, if \mathcal{N}' is the dephasing map $\mathcal{Z}(\hat{p}) = \frac{1+\gamma}{2}\hat{p} + \frac{1-\gamma}{2}\hat{Z}\hat{p}\hat{Z}$, one finds $\kappa(\mathcal{N}') = \frac{1}{|\gamma|}$. Thus, even for δ and γ polynomially close to 0, a polynomial increase in the number of statistical samples can be used to ensure an estimate of the inverse of \mathcal{N} to any polynomial accuracy with high probability.

B. Beyond unital maps

What does the reconstruction of \mathcal{E}' tell us about the \mathcal{E} ? We prove the following in Appendix C.

Lemma IV.3.—The unital part of a CPTP single-qubit map is always a CPTP map.

This means that the unital part of a single-qubit map imposes no lower bound on the magnitude of the nonunital part of that map—the nonunital part can always be set to 0.

For a single qubit, the unital part does impose stringent conditions on the maximum size of the nonunital part. Up to unitary rotations, any map can be written in the Pauli-Liouville representation as [20]

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ t_1 & \lambda_1 & 0 & 0 \\ t_2 & 0 & \lambda_2 & 0 \\ t_3 & 0 & 0 & \lambda_3 \end{pmatrix}, \quad (4.14)$$

where λ_i and t_i are real-valued parameters. The λ_i , corresponding to the unital part, can be estimated using the techniques already described, but as Lemma IV.3 demonstrates, no useful lower bound on $|t_i|$ can be obtained. However, for the map to be positive, it is necessary that $|t_i| \leq 1 - |\lambda_i|$ [20], which gives upper bounds on the magnitudes of the nonunital parameters.

The fact that, for single-qubit maps, \mathcal{E}' is always CP can be turned around to say that statistically significant non-CP estimates of \mathcal{E}' imply statistically significant non-CP estimates of \mathcal{E} and may be used as witnesses of systematic errors in the experiments [6,36].

Lemma IV.3 fails in the case of multiple qubits, and it is not difficult to construct counterexamples. Numerical experiments indicate that CPTP maps chosen at random by drawing unitary dilations from the Haar distribution lead to non-CP unital parts with probability around 1. This implies that, while it may not be possible to test complete positivity of a general map by testing only its unital part, the reconstruction of the unital part of a multiqubit map yields lower bounds on the magnitudes of the nonunital parameters. Thus, while this result precludes the use of the unital part of a multiqubit map to test for systematic errors in experiments, it does provide more information about the nonunital parameters.

V. FIDELITY ESTIMATION BEYOND THE CLIFFORD GROUP

Previous RB results showed how to bound the average fidelity of Clifford operations [10,12]. While the maps in the Clifford group form an integral part of current approaches to scalable fault tolerance in quantum computers, universal quantum computation is only possible if operations outside the Clifford group are also considered. We would like to be able to not only efficiently verify the performance of Clifford gates but also verify the

performance of universal circuits. However, there are strong indications that quantum computers are strictly more powerful than classical computers; for example, if classical computers could efficiently simulate certain classes of nonuniversal quantum circuits, it would imply a collapse of the polynomial hierarchy [37]; thus, it is considered highly unlikely. It is therefore extremely unlikely that classical computers can efficiently predict the behavior of a general poly(n)-depth quantum circuit [38], and without these predictions, it is not possible to check if a quantum computer is behaving as desired. For these fundamental reasons, we do not expect it to be possible to efficiently estimate the average fidelity to a general quantum map.

It is important to note, however, that it is possible to efficiently simulate *some* circuits that contain maps outside the Clifford group. In particular, Aaronson and Gottesman [39] have proven that circuits consisting of Clifford group maps and a logarithmic number of maps outside the Clifford group can be simulated efficiently. Despite efficient simulation being possible, these circuits can be thought of as discrete components that enable universality under composition, and thus the ability to verify their implementation is of great practical importance. We now show how our methods can be extended to allow for efficient estimation of the average fidelity of *any* experiment to such circuits.

A. Average fidelity to \mathcal{T}

The canonical example of a map outside the Clifford group is the operation $\mathcal{T} = e^{-i\frac{\pi}{8}\hat{Z}}$. This gate is commonly used in combination with Clifford group operations to form a gate set that is universal for quantum computation [40]. In this section, we show how to efficiently bound the average fidelity of a map \mathcal{E} to $\mathcal{U} = \mathcal{T}$.

In Sec. IV, we prove that Clifford maps span the space of unital maps. This implies that, in the Pauli-Liouville representation, any unitary map $\mathcal{U}^{(\text{PL})}$ can be written as a linear combination of Clifford maps

$$\mathcal{U}^{(\text{PL})} = \sum_i \beta_i^{\mathcal{U}} \mathcal{C}_i^{(\text{PL})}, \quad (5.1)$$

with $\beta_i \in \mathbb{R}$. By linearity,

$$\text{tr} \mathcal{E} \mathcal{N} \mathcal{U}^\dagger = \sum_i \beta_i^{\mathcal{U}} \text{tr} \mathcal{E} \mathcal{N} (\mathcal{C}_i)^\dagger, \quad (5.2)$$

so

$$\bar{F}(\mathcal{E} \circ \mathcal{N}, \mathcal{U}) = \sum_i \beta_i^{\mathcal{U}} \bar{F}(\mathcal{E} \circ \mathcal{N}, \mathcal{C}_i) + \frac{1}{d+1} \left(1 - \sum_i \beta_i^{\mathcal{U}} \right). \quad (5.3)$$

For an arbitrary unitary \mathcal{U} , the number of nonzero $\beta_i^{\mathcal{U}}$, which we denote by $N_{\mathcal{U}}$, can be as large as $O(d^2)$. However,

$\mathcal{T}^{(\text{PL})}$ can be written as a linear combination of three Clifford maps. The support of $\mathcal{T}^{(\text{PL})}$ is given by the maps corresponding to the Clifford group unitaries, \hat{I} , \hat{Z} , and $e^{-i\frac{\pi}{4}\hat{Z}}$, with the corresponding coefficients $\frac{1}{2}$, $\frac{1-\sqrt{2}}{2}$, and $\frac{1}{\sqrt{2}}$. Thus, to estimate $\bar{F}(\mathcal{E} \circ \mathcal{N}, \mathcal{T})$, one only needs to estimate three average fidelities to Clifford group maps (instead of the ten necessary for reconstruction of the unital part).

Suppose one estimates each fidelity $\bar{F}(\mathcal{E} \circ \mathcal{N}, \mathcal{C}_i)$ for all of the \mathcal{C}_i in the linear combination to within ϵ' with confidence $1 - \delta'$. In Sec. VI B, we show that this requires $O(\frac{N_{\mathcal{U}}}{\epsilon'^4} \log \frac{1}{\delta'})$ samples. From Eq. (5.3), it is clear that one can obtain an estimate \tilde{F} such that

$$\Pr \left(|\tilde{F} - \bar{F}(\mathcal{E} \circ \mathcal{N}, \mathcal{U})| \geq \epsilon' \sum_i |\beta_i^{\mathcal{U}}| \right) \leq N_{\mathcal{U}} \delta'. \quad (5.4)$$

Choosing $\delta' = \delta/N_{\mathcal{U}}$ and $\epsilon' = \epsilon/\sum_i |\beta_i^{\mathcal{U}}|$ gives

$$\Pr(|\tilde{F} - \bar{F}(\mathcal{E} \circ \mathcal{N}, \mathcal{U})| \geq \epsilon) \leq \delta \quad (5.5)$$

and requires $O(N_{\mathcal{U}} (\frac{\sum_i |\beta_i^{\mathcal{U}}|}{\epsilon})^4 \log \frac{N_{\mathcal{U}}}{\delta'})$ samples.

For the particular case of the \mathcal{T} map, one finds $\sum_i |\beta_i^{\mathcal{T}}| = \sqrt{2}$, so an estimate for the average fidelity to \mathcal{T} can be obtained by the following procedure:

- (1) Perform RB with $O(\frac{1}{\epsilon^4} \log \frac{1}{\delta})$ samples for each relevant fidelity $\bar{F}(\mathcal{E} \circ \mathcal{N}, \mathcal{C}_i)$. This requires $O(\frac{1}{\epsilon^4} \log \frac{1}{\delta})$ total samples and results in an estimate \tilde{F} such that

$$P(|\tilde{F} - \bar{F}(\mathcal{E} \circ \mathcal{N}, \mathcal{T})| \geq \epsilon) \leq \delta. \quad (5.6)$$

- (2) Perform RB with $O(\frac{1}{\epsilon^4} \log \frac{1}{\delta})$ samples to obtain an estimate $\tilde{F}_{\mathcal{N}}$ of $\bar{F}(\mathcal{N}, \mathcal{I})$ such that

$$P(|\tilde{F}_{\mathcal{N}} - \bar{F}(\mathcal{N}, \mathcal{I})| \geq \epsilon) \leq \delta. \quad (5.7)$$

- (3) In Sec. VI A, we show how to bound the fidelity of $\bar{F}(\mathcal{E}, \mathcal{U})$, given estimates of $\bar{F}(\mathcal{E} \circ \mathcal{N}, \mathcal{U})$ and $\bar{F}(\mathcal{N}, \mathcal{I})$. Apply the bounds of Sec. VI A for $\bar{F}(\mathcal{E} \circ \mathcal{N}, \mathcal{T}) = \bar{F} \pm \epsilon$, and for $\bar{F}(\mathcal{N}, \mathcal{I}) = \tilde{F}_{\mathcal{N}} \pm \epsilon$, to obtain bounds on $\bar{F}(\mathcal{E}, \mathcal{T})$ that are valid with probability of at least $1 - 2\delta$.

This procedure trivially extends to bounding the fidelity of \mathcal{E} to the case where \mathcal{T} acts on a single qubit and the identity acts on $n - 1$ qubits. The sampling complexity remains the same, but the time complexity changes, as the classical preprocessing time needed to make a single average fidelity estimate scales as $O(n^4)$ [12]. Similar arguments can be used to show that the sampling complexity of determining the average fidelity of \mathcal{E} to any one- or two-qubit unitary acting on n qubits is constant, with the same classical preprocessing time complexity. In the next

section, we will discuss more general operations acting on n qubits.

B. Average fidelity to more general unitaries

It is possible to efficiently bound the average fidelity of a map \mathcal{E} to a unitary \mathcal{U} when \mathcal{U} is a composition of $O(\text{poly}(n))$ Clifford maps and $O(\log(n))$ \mathcal{T} maps on n qubits (i.e., maps that act as \mathcal{T} on one qubit and as the identity on the remaining $n - 1$ qubits). Under these constraints,

- (i) $\mathcal{U}^{(\text{PL})}$ can be efficiently decomposed into a linear combination of $O(\text{poly}(n))$ Clifford maps [i.e., $N_{\mathcal{U}} = O(\text{poly}(n))$];
- (ii) the coefficients $\beta_i^{\mathcal{U}}$ in the linear combination satisfy $\sum_i |\beta_i^{\mathcal{U}}| = O(\text{poly}(n))$.

Following the argument of Sec. V A, the sampling complexity scales like $O(N_{\mathcal{U}}(\sum_i |\beta_i^{\mathcal{U}}|^4) \log \frac{N_{\mathcal{U}}}{\delta})$, so together (i) and (ii) guarantee that the sampling complexity of bounding $F(\mathcal{E}, \mathcal{U})$ is $O(\text{poly}(n))$. Since (i) guarantees that the decomposition is efficient, and the classical preprocessing time needed to make a single sample scales as $O(n^4)$, the time complexity is also $O(\text{poly}(n))$.

We prove (i) by induction on t (the number of \mathcal{T} maps in the circuit) and c (the number of Clifford maps in the circuit). We show that one can decompose $\mathcal{U}^{(\text{PL})}$ into a linear combination of at most 3^t terms, where each Clifford map in the linear combination is written as a composition of at most $t + c$ Clifford maps. The base case is given by the following

- (a) $t = 1, c = 0$: \mathcal{U} is a single \mathcal{T} , and $\mathcal{U}^{(\text{PL})}$ can be written as a linear combination of three Clifford maps.
- (b) $t = 0, c = 1$: \mathcal{U} is a Clifford map, and so $\mathcal{U}^{(\text{PL})}$ can be written as a linear combination of one Clifford map.

For the inductive case, we assume that one has a unitary \mathcal{U} that is a composition of t \mathcal{T} maps and c Clifford maps. By inductive assumption, $\mathcal{U}^{(\text{PL})}$ can be written as

$$\mathcal{U}^{(\text{PL})} = \sum_{i=1}^M \beta_i^{\mathcal{U}} \prod_{j=1}^{N_i} \mathcal{C}_{i,j}^{(\text{PL})}, \quad (5.8)$$

with $M \leq 3^t$ and $N_i \leq t + c$. Now consider composing \mathcal{U} with a Clifford \mathcal{C} . Then

$$\mathcal{C}^{(\text{PL})} \mathcal{U}^{(\text{PL})} = \left(\sum_{i=1}^M \beta_i^{\mathcal{U}} \mathcal{C}^{(\text{PL})} \prod_{j=1}^{N_i} \mathcal{C}_{i,j}^{(\text{PL})} \right), \quad (5.9)$$

and one obtains a linear combination of $\leq 3^t$ terms, each a composition of $c + t + 1$ Clifford maps. Likewise, if \mathcal{U} is composed with \mathcal{T} , then

$$\mathcal{T}^{(\text{PL})} \mathcal{U}^{(\text{PL})} = \sum_{i=1}^M \sum_{k=1}^3 \beta_i^{\mathcal{U}} \beta_k^{\mathcal{T}} \mathcal{C}_k^{(\text{PL})} \prod_{j=1}^{N_i} \mathcal{C}_{i,j}^{(\text{PL})}, \quad (5.10)$$

where the $\mathcal{C}_k^{(\text{T})}$ are the three Clifford maps involved in the linear combination of $\mathcal{T}^{(\text{PL})}$, so one obtains a linear combination of 3^{t+1} elements, each a composition of $t + c + 1$ Clifford maps, as desired.

Therefore, if one has a unitary map \mathcal{U} composed of $O(\text{poly}(n))$ Clifford maps and $O(\log(n))$ \mathcal{T} maps, one can write $\mathcal{U}^{(\text{PL})}$ as a linear combination of $O(\text{poly}(n))$ Clifford maps, where each term in the linear combination is a composition of at most $O(\text{poly}(n))$ Clifford maps. A sequence of $O(\text{poly}(n))$ Clifford maps can be efficiently simplified into a single Clifford map using the Gottesman-Knill theorem [29]. The average fidelity estimate to \mathcal{U} is obtained by estimating the average fidelities to these simplified Clifford maps.

To see that (ii) also holds, suppose one calculates a linear combination for $\mathcal{U}^{(\text{PL})}$ based on the above construction. It is possible that different terms in the linear combination result in the same Clifford map, but for simplicity, we treat each term separately so that our estimate of the complexity is an upper bound. Then, if the circuit decomposition of \mathcal{U} contains t \mathcal{T} maps,

$$\sum_i |\beta_i^{\mathcal{U}}| \leq \left(\sum_i |\beta_i^{\mathcal{T}}| \right)^t = \sqrt{2}^t, \quad (5.11)$$

so $\sum_i |\beta_i^{\mathcal{U}}|$ scales, at most, as $O(\text{poly}(n))$ for $t = O(\log n)$.

These results demonstrate that robust estimates of the average fidelities to unitary maps outside the Clifford group can be obtained efficiently, scaling polynomially in the number of qubits.

VI. BOUNDING ERROR IN AVERAGE FIDELITY ESTIMATES

In this section, we bound sources of error that occur in RB procedures. There are two sources of uncertainty we consider. When trying to efficiently estimate the average fidelity \mathcal{E} without inverting \mathcal{N} , as we do in Sec. V, we lack direct access to $\bar{F}(\mathcal{E}, \mathcal{U})$ and instead can only estimate $\bar{F}(\mathcal{E} \circ \mathcal{N}, \mathcal{U})$ and $\bar{F}(\mathcal{N}, \mathcal{I})$. This leads to an error on our estimate of $\bar{F}(\mathcal{E}, \mathcal{U})$. We also consider statistical errors from the sampling of random variables and show that we can efficiently fit RB decays to any constant error. As a consequence, this allows us to efficiently bound the average fidelity to maps outside the Clifford group, as described in Sec. V. We address these two effects separately. These types of uncertainties can be found in many contexts, so we expect the analysis in Secs. VI A and VI B has broader applications.

A. Bounds on average fidelity of composed maps

In this section, we show how to bound $\bar{F}(\mathcal{E}, \mathcal{U})$ when we have estimates of $\bar{F}(\mathcal{E} \circ \mathcal{N}, \mathcal{U})$ and $\bar{F}(\mathcal{N}, \mathcal{I})$.

In Appendix D, we prove

$$\chi_{0,0}^{A \circ B} = \chi_{0,0}^A \chi_{0,0}^B \pm \left(2 \sqrt{(1 - \chi_{0,0}^A) \chi_{0,0}^A (1 - \chi_{0,0}^B) \chi_{0,0}^B} + (1 - \chi_{0,0}^A) (1 - \chi_{0,0}^B) \right). \quad (6.1)$$

Setting $\mathcal{B} = \mathcal{N}$, $\mathcal{A} = \mathcal{U}^\dagger \circ \mathcal{E}$, and using Eq. (2.6) gives bounds on $\bar{F}(\mathcal{E}, \mathcal{U})$ as a function of $\bar{F}(\mathcal{E} \circ \mathcal{N}, \mathcal{U})$ and $\bar{F}(\mathcal{N}, \mathcal{I})$.

This bound is valid for any maps \mathcal{A} and \mathcal{B} . There exist \mathcal{A} and \mathcal{B} that saturate the upper bound, but the lower bound is not tight, for reasons we discuss in Appendix D. Generally, this method gives better bounds when the operation \mathcal{E} is close to \mathcal{U} and when \mathcal{N} is close to \mathcal{I} (i.e., the imperfections in the randomizing operations are small). Because these lower and upper bounds—just like the bounds in Ref. [12]—are not close to each other, except in the regime where \mathcal{E} is close to \mathcal{U} , they are not useful for the type of tomographic reconstruction performed in Sec. IV, where an arbitrary map might be far from a Clifford map or from a map that is composed of Clifford maps and $O(\text{poly}(n))$ \mathcal{T} maps.

Previous work on average-fidelity estimates based on RB have derived the bound [12]

$$\chi_{0,0}^A = \frac{(d^2 - 1) \chi_{0,0}^{A \circ B}}{d^2 \chi_{0,0}^B} \pm E, \quad (6.2)$$

$$E = \left| \chi_{0,0}^B - \frac{(d^2 - 1) \chi_{0,0}^{A \circ B}}{d^2 \chi_{0,0}^B} \right| + \left(\frac{d^2 - 1}{d^2} - \chi_{0,0}^B \right), \quad (6.3)$$

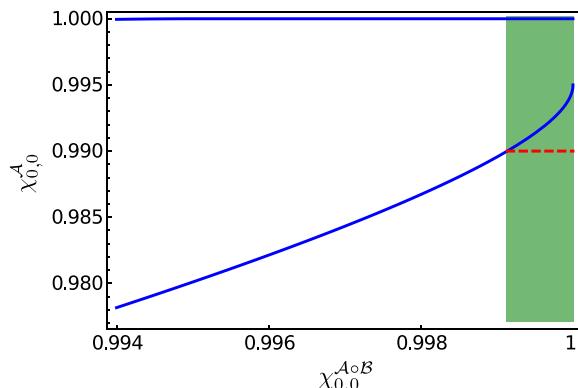


FIG. 2. Bounds on $\chi_{0,0}^A$ versus $\chi_{0,0}^{A \circ B}$, when $\chi_{0,0}^B$ is fixed at 0.995. Our bounds are shown as a solid blue line, while the bounds of Ref. [12] are shown as a red dashed line. The bounds of Ref. [12] are valid in the green shaded region, while our bounds are valid for all values of $\chi_{0,0}^{A \circ B}$.

which is only valid when $\bar{F}(\mathcal{A}, \mathcal{I}) \geq 2\bar{F}(\mathcal{B}, \mathcal{I}) - 1$ or, in the fidelity estimation context, when $\bar{F}(\mathcal{E}, \mathcal{U})$ is close to 1 [41]. There is no way to directly verify from the experimental data that this requirement holds, but in order to compare the bounds in Ref. [12] with the bounds derived here, we use Eq. (6.1) to bound the region of validity of Eq. (6.2). As illustrated in Fig. 2, the bounds derived here are better when $\bar{F}(\mathcal{A} \circ \mathcal{B}, \mathcal{I})$ is close to 1 but are applicable to the entire range of parameters without additional assumptions about the maps involved.

B. Confidence bounds on fidelity estimates

Here, we show how to extract $F(\mathcal{E}, \mathcal{U})$ from the estimated points $F_k(\mathcal{E}, \mathcal{U})$ (the average fidelity of a length- k RB sequence—see Sec. III). We rigorously bound the error and sampling complexity of this nonlinear fit.

One can easily show that, using the Hoeffding bound, an estimate \tilde{F}_k for $F_k(\mathcal{E}, \mathcal{U})$ can be obtained such that [9]

$$\Pr(|\tilde{F}_k - F_k(\mathcal{E}, \mathcal{U})| \geq \epsilon') \leq \delta', \quad (6.4)$$

with a number of samples $O(\frac{1}{\epsilon'^2} \log \frac{1}{\delta'})$, which is independent of the number of qubits in the system. What we show here is that this allows for p [and thus $\bar{F}(\mathcal{E}, \mathcal{U})$] to be estimated with a number of samples that also scales well with some desired accuracy and confidence. In standard RB experiments, p is estimated by numerical fits to the \tilde{F}_k with many different sequence lengths, but the dependence of the error on the number of samples per sequence length is difficult to analyze. Here, we take a different approach that leads to simple bounds on the accuracy and confidence.

Since $F_k(\mathcal{E}, \mathcal{U}) = A_0 p^k + B_0$, it is easy to see that

$$p = \frac{F_2 - F_\infty}{F_1 - F_\infty}, \quad (6.5)$$

and therefore, at least in principle, p can be estimated by using only sequences of length 1 and 2, along with a sequence long enough to ensure $|A_0 p^k| \ll |B_0|$ [42], with the corresponding expectation denoted by F_∞ . Assuming that each \tilde{F}_i is estimated with accuracy ϵ' and confidence $1 - \delta'$, and that 0 is not in the confidence interval for $\tilde{F}_1 - F_\infty$, it follows that the estimate \tilde{p} for $p > 0$ and $A_0 > 0$ satisfies

$$\frac{p - \frac{2\epsilon'}{A_0 p}}{1 + \frac{2\epsilon'}{A_0 p}} \leq \tilde{p} \leq \frac{p + \frac{2\epsilon'}{A_0 p}}{1 - \frac{2\epsilon'}{A_0 p}}, \quad (6.6)$$

with probability of at least $1 - 3\delta'$ (similar expressions hold for the cases of negative p or A_0 , but for simplicity, we focus on the expressions for the positive case). If $|A_0|$ or $|p|$ is small, these bounds diverge, so it is important to test the data to exclude these cases.

Note that A_0 is independent of the sequences being used, so one can choose to estimate A_0 from a sequence with large p . Denoting the F_i estimates for those sequences as \tilde{F}'_i , and assuming that the confidence interval for $\tilde{F}'_2 - \tilde{F}'_\infty$ does not include 0, A_0 is bounded below via

$$A_0 \geq \frac{(\tilde{F}'_1 - \tilde{F}'_\infty - 2\epsilon')^2}{\tilde{F}'_2 - \tilde{F}'_\infty + 2\epsilon'} \equiv a, \quad (6.7)$$

with probability of at least $1 - 3\delta'$. From Eq. (6.4),

$$ap - 2\epsilon' \leq A_0 p - 2\epsilon' \leq \tilde{F}_1 - \tilde{F}_\infty, \quad (6.8)$$

and thus

$$p \leq \frac{\tilde{F}_1 - \tilde{F}_\infty + 2\epsilon'}{a}, \quad (6.9)$$

so if one desires an accuracy ϵ for \tilde{p} , whenever

$$\frac{\tilde{F}_1 - \tilde{F}_\infty + 2\epsilon'}{a} \leq \epsilon, \quad (6.10)$$

one can set $\tilde{p} = 0$, thereby avoiding the divergent confidence intervals while still providing estimates with the desired accuracy.

Similarly, from Eq. (6.4),

$$\tilde{F}_1 - \tilde{F}_\infty \leq A_0 p + 2\epsilon', \quad (6.11)$$

so whenever

$$\frac{\tilde{F}_1 - \tilde{F}_\infty + 2\epsilon'}{a} \geq \epsilon, \quad (6.12)$$

it follows that

$$a\epsilon - 4\epsilon' \leq A_0 p \leq A_0. \quad (6.13)$$

Thus, choosing $\epsilon' = 4\epsilon^2 a$, one can safely Taylor expand Eq. (6.6) to first order in ϵ to obtain

$$p - \epsilon - O(\epsilon^2) \leq \tilde{p} \leq p + \epsilon + O(\epsilon^2), \quad (6.14)$$

with probability of at least $1 - \delta = 1 - 6\delta'$, as desired, using $O(\frac{1}{\epsilon^3} \log \frac{6}{\delta})$ samples.

This immediately gives an estimate \tilde{F} for $\bar{F}(\mathcal{E}, \mathcal{U})$ that can be obtained as

$$\Pr(|\tilde{F}_k - \bar{F}(\mathcal{E}, \mathcal{U})| \geq \epsilon) \leq \delta, \quad (6.15)$$

with $O(\frac{1}{\epsilon^4} \log \frac{1}{\delta})$ samples.

VII. SUMMARY AND OUTLOOK

We have demonstrated that, using information from multiple RB experiments, it is possible to reconstruct the unital part of any completely positive trace-preserving map

in a way that is robust against preparation and measurement errors, thereby avoiding some forms of systematic errors that plague more traditional tomographic reconstruction protocols. The unital part of a map consists of the vast majority of the parameters of that map, including all parameters necessary to describe any deterministic unitary map, as well as any random unitary map, such as dephasing with respect to any eigenbasis.

We also presented a robust procedure for bounding the average fidelity to an arbitrary unitary and showed that this protocol is efficient for a large class of unitaries outside of the Clifford group. The overhead of the procedure depends on how the unitary is decomposed as a linear combination of Clifford group unitary maps, and we gave rigorous bounds on the number of samples needed to achieve some desired accuracy and confidence in the fidelity estimate.

The extension of these results to nonqubit systems remains an open problem. In addition, the characterization of the nonunital part of a map in a robust manner seems to present a larger challenge than the characterization of the unital part. New techniques are needed to access this important information.

ACKNOWLEDGMENTS

We thank Easwar Magesan for many illuminating discussions. S. K. was supported by the U.S. Department of Energy under cooperative research agreement Contract No. DE-FG02-05ER41360 and by NSF Grant No. DGE-0801525, *IGERT: Interdisciplinary Quantum Information Science and Engineering*. This research was funded by the Office of the Director of National Intelligence (ODNI), Intelligence Advanced Research Projects Activity (IARPA), through the Army Research Office Grant No. W911NF-10-1-0324. All statements of fact, opinion or conclusions contained herein are those of the authors and should not be construed as representing the official views or policies of IARPA, the ODNI, or the U.S. Government.

Note added in proof.—After the paper was accepted and while we were waiting for the publication proofs to appear, we became aware that a more general form of Lemma IV.1 was previously proven independently by Wim van Dam and Mark Howard in Ref. [43].

APPENDIX A: UNITAL MAPS AND THE LINEAR SPAN OF UNITARY MAPS

The Pauli-Liouville representation is particularly convenient when discussing the Clifford group of n -qubit unitary maps because, in this representation, such maps are monomial matrices [44,45]. In the particular case of qubits, $\mathcal{E}_{ij}^{(\text{PL})} \in \{\pm 1, 0\}$ for a unitary in the Clifford group. Given these facts, we can now straightforwardly prove the result about the linear span of Clifford group maps on n qubits. First, we need to prove a small result about Clifford group unitaries.

Claim A.1.—For any two n -qubit Pauli operators $\hat{P}_{i \neq 0}$ and $\hat{P}_{j \neq 0}$, there exists a Clifford group unitary \hat{C} such that $\hat{C}\hat{P}_i\hat{C}^\dagger = \hat{P}_j$.

Proof.—This claim shows that there are no subsets of nonidentity multiqubit Pauli operators that do not mix under the action of the Clifford group. \hat{P}_i and \hat{P}_j can both be written as tensor products of single-qubit Pauli operators and identity operators $\hat{\mathbb{I}}$, where in the tensor product of each, there is at least one element that is not $\hat{\mathbb{I}}$. Using local Clifford group unitaries, one can take each nonidentity element in each tensor product to the single-qubit Pauli operator \hat{X} . We call these new Pauli operators \hat{P}'_i and \hat{P}'_j . Now the problem is equivalent to finding Clifford group unitaries that take one tensor product of \hat{X} and $\hat{\mathbb{I}}$ to another.

Let $\text{CNOT}_{k,l}$ denote the controlled-NOT unitary with qubit k as a control and qubit l as a target. The CNOT is a well-known unitary in the Clifford group with the property that $\text{CNOT}_{k,l}X^{(k)}\text{CNOT}_{k,l} = \hat{X}^{(k)} \otimes X^{(l)}$, where we use $\hat{X}^{(i)}$ to denote \hat{X} acting on the i th qubit. In this way, one can increase or decrease the number of \hat{X} in the tensor product decomposition of \hat{P}'_i using unitary maps, as long as there is at least one \hat{X} in the tensor product. This means that any tensor product of $\hat{\mathbb{I}}$ and \hat{X} on n qubits can be mapped to any other tensor product of $\hat{\mathbb{I}}$ and \hat{X} on n qubits through the use of CNOT unitaries—in particular, one can map \hat{P}'_i to \hat{P}'_j .

Now we can prove the intended result.

Lemma IV.1.—The linear span of unitary maps coincides with the linear span of Clifford group unitary maps. Moreover, the projection of a TP map to this linear span is a unital map.

Proof.—It suffices to show that any matrix element in the unital part of a map (in the Pauli-Liouville representation) can be written as a linear combination of Clifford group unitary maps.

The Pauli-Liouville representations of unitaries in the n -qubit Clifford group are monomial matrices with nonzero entries equal to ± 1 . For any given such unitary \hat{C} , one can construct 4^n orthogonal unitaries of the form $\hat{P}_i\hat{C}$, with corresponding 4^n mutually orthogonal Pauli-Liouville representation matrices. Pauli operators are diagonal in the Pauli-Liouville representation, so for a fixed \hat{C} , the Pauli-Liouville representations of all $\hat{P}_i\hat{C}$ have support in the same set of 4^n matrix elements as the Pauli-Liouville representation of \hat{C} ; thus, the values of any of these matrix elements for any map \mathcal{E} can be recovered by collecting the Hilbert-Schmidt inner products between $\mathcal{E}^{(\text{PL})}$ and the Pauli-Liouville representation of the map for the $\hat{P}_i\hat{C}$, i.e., $\text{tr}\mathcal{E}(\mathcal{P}_i\mathcal{C})^\dagger$. From Claim A.1, one can choose a Clifford group unitary that has support on any particular matrix element in the unital block; therefore, any unital matrix can be written as a linear combination of Clifford group unitary maps. Since Clifford group maps are unital, this concludes the proof.

APPENDIX B: RECONSTRUCTION OF THE UNITAL PART WITH IMPERFECT OPERATIONS

In the main body of this paper, we describe how RB allows for the reconstruction of the unital parts of $\mathcal{E}\circ\mathcal{N}$ and \mathcal{N} , where \mathcal{E} is some quantum operation one would like to characterize, and \mathcal{N} is the error operation associated with each of the randomizing operations. We now prove the result that allows for the estimation of the unital part of \mathcal{E} alone, given an estimate of the unital part of \mathcal{N} .

Lemma IV.2.—If $(\mathcal{E}\circ\mathcal{N})'$ is the unital part of $\mathcal{E}\circ\mathcal{N}$ and \mathcal{N}' is the unital part of \mathcal{N} , and all these operations are trace preserving, then $\mathcal{E}' = (\mathcal{E}\circ\mathcal{N})'\circ(\mathcal{N}')^{-1}$ whenever $(\mathcal{N}')^{-1}$ exists.

Proof.—Any trace-preserving linear map \mathcal{A} can be written in the Pauli-Liouville representation as

$$\mathcal{A}^{(\text{PL})} = \begin{pmatrix} 1 & \vec{0}^T \\ \vec{t}_\mathcal{A} & \mathbf{T}_\mathcal{A} \end{pmatrix}, \quad (\text{B1})$$

where, as discussed previously, the unital part is

$$\mathcal{A}'^{(\text{PL})} = \begin{pmatrix} 1 & \vec{0}^T \\ \vec{0} & \mathbf{T}_\mathcal{A} \end{pmatrix}. \quad (\text{B2})$$

The Pauli-Liouville representation of the composition of two trace-preserving linear maps \mathcal{A} and \mathcal{B} is given by the multiplication of the Pauli-Liouville representations, resulting in

$$(\mathcal{A}\circ\mathcal{B})^{(\text{PL})} = \begin{pmatrix} 1 & \vec{0}^T \\ \vec{t}_\mathcal{A} + \mathbf{T}_\mathcal{A}\vec{t}_\mathcal{B} & \mathbf{T}_\mathcal{A}\mathbf{T}_\mathcal{B} \end{pmatrix}, \quad (\text{B3})$$

and thus

$$(\mathcal{A}\circ\mathcal{B})'^{(\text{PL})} = \begin{pmatrix} 1 & \vec{0}^T \\ \vec{0} & \mathbf{T}_\mathcal{A}\mathbf{T}_\mathcal{B} \end{pmatrix}, \quad (\text{B4})$$

$$= (\mathcal{A})'^{(\text{PL})}(\mathcal{B})'^{(\text{PL})}. \quad (\text{B5})$$

It follows immediately that

$$(\mathcal{A})'^{(\text{PL})} = (\mathcal{A}\circ\mathcal{B})'^{(\text{PL})}[(\mathcal{B})'^{(\text{PL})}]^{-1}, \quad (\text{B6})$$

if the inverse exists, and

$$\mathcal{A}' = (\mathcal{A}\circ\mathcal{B})'\circ(\mathcal{B}')^{-1}, \quad (\text{B7})$$

by the Pauli-Liouville isomorphism. The lemma follows by setting $\mathcal{A} = \mathcal{E}\circ\mathcal{N}$ and $\mathcal{B} = \mathcal{N}$.

APPENDIX C: COMPLETE-POSITIVITY OF THE PROJECTION OF SINGLE-QUBIT OPERATIONS ONTO THE UNITAL SUBSPACE

In this appendix, we prove that for a CPTP map \mathcal{E} acting on a single qubit, \mathcal{E}' , the unital part of \mathcal{E} [see Eq. (4.3)], is always a CPTP map.

Recall that the Pauli-Liouville representation of a single-qubit map \mathcal{E} may be written as

$$\mathcal{E}^{(\text{PL})} = \begin{pmatrix} 1 & \vec{0} \\ \vec{t}_{\mathcal{E}} & \mathbf{T}_{\mathcal{E}} \end{pmatrix}. \quad (\text{C1})$$

King and Ruskai [20] show that there exist unitary maps \mathcal{U} and \mathcal{V} such that

$$\mathcal{U}\check{\mathcal{E}}\mathcal{V} = \mathcal{E}, \quad (\text{C2})$$

where

$$\check{\mathcal{E}}^{(\text{PL})} = \begin{pmatrix} 1 & \vec{0} \\ \vec{\tau} & \mathbf{D} \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ \tau_1 & \lambda_1 & 0 & 0 \\ \tau_2 & 0 & \lambda_2 & 0 \\ \tau_3 & 0 & 0 & \lambda_3 \end{pmatrix}. \quad (\text{C3})$$

To prove \mathcal{E}' is CPTP, we first show that $\check{\mathcal{E}}'$ (the projection of $\check{\mathcal{E}}$ onto the unital block) is always CPTP, and then we prove that if $\check{\mathcal{E}}'$ is CPTP, \mathcal{E}' is CPTP.

Lemma C.1.—For single-qubit operations, $\check{\mathcal{E}}'$ is always CPTP.

Proof.—Ruskai *et al.* [46] prove that \mathcal{E} is CP if and only if

$$(\lambda_1 + \lambda_2)^2 \leq (1 + \lambda_3)^2 - \tau_3^2 - (\tau_1^2 + \tau_2^2) \left(\frac{1 + \lambda_3 \pm \tau_3}{1 - \lambda_3 \pm \tau_3} \right), \quad (\text{C4})$$

$$(\lambda_1 - \lambda_2)^2 \leq (1 - \lambda_3)^2 - \tau_3^2 - (\tau_1^2 + \tau_2^2) \left(\frac{1 - \lambda_3 \pm \tau_3}{1 + \lambda_3 \pm \tau_3} \right), \quad (\text{C5})$$

$$\begin{aligned} (1 - (\lambda_1^2 + \lambda_2^2 + \lambda_3^2) - (\tau_1^2 + \tau_2^2 + \tau_3^2))^2 \\ \geq 4(\lambda_1^2(\tau_1^2 + \lambda_2^2) + \lambda_2^2(\tau_2^2 + \lambda_3^2) + \lambda_3^2(\tau_3^2 + \lambda_1^2) - 2\lambda_1\lambda_2\lambda_3), \end{aligned} \quad (\text{C6})$$

where in Eqs. (C4) and (C5), if $|\lambda_3| + |\tau_3| = 1$, then τ_1 and τ_2 must be 0 for the map to be CP.

To prove the lemma, we need to show that for any values of $\{\tau_i\}$ and $\{\lambda_i\}$ that satisfy Eqs. (C4–C6), these equations are still satisfied when $\tau_i = 0$ for $i = 1, 2, 3$.

Notice that in Eqs. (C4–C5) when we set $\tau_i = 0$, we require

$$(\lambda_1 \pm \lambda_2)^2 \leq (1 \pm \lambda_3)^2. \quad (\text{C7})$$

However, it is easy to show [46] that Eqs. (C4–C5) combined with positivity constraints imply

$$(\lambda_1 \pm \lambda_2)^2 \leq (1 \pm \lambda_3)^2, \quad (\text{C8})$$

so we only need to look at Eq. (C6).

Looking at Eq. (C6), we see that we need to show

$$\begin{aligned} (1 - (\lambda_1^2 + \lambda_2^2 + \lambda_3^2))^2 \geq 4((\lambda_1\lambda_2)^2 + (\lambda_2\lambda_3)^2 \\ + (\lambda_3\lambda_1)^2 - 2\lambda_1\lambda_2\lambda_3). \end{aligned} \quad (\text{C9})$$

Because τ 's only increase the value of the right-hand side of Eq. (C6), we have

$$\begin{aligned} (1 - (\lambda_1^2 + \lambda_2^2 + \lambda_3^2) - (\tau_1^2 + \tau_2^2 + \tau_3^2))^2 \\ \geq 4(\lambda_1^2\lambda_2^2 + \lambda_2^2\lambda_3^2 + \lambda_3^2\lambda_1^2 - 2\lambda_1\lambda_2\lambda_3). \end{aligned} \quad (\text{C10})$$

Note that if $(\lambda_1^2 + \lambda_2^2 + \lambda_3^2) + (\tau_1^2 + \tau_2^2 + \tau_3^2) \leq 1$, then we obtain

$$\begin{aligned} (1 - (\lambda_1^2 + \lambda_2^2 + \lambda_3^2))^2 \geq (1 - (\lambda_1^2 + \lambda_2^2 + \lambda_3^2) \\ - (\tau_1^2 + \tau_2^2 + \tau_3^2))^2, \end{aligned} \quad (\text{C11})$$

which, combined with Eq. (C10), gives the desired result.

To show that $(\lambda_1^2 + \lambda_2^2 + \lambda_3^2) + (\tau_1^2 + \tau_2^2 + \tau_3^2) \leq 1$, note that when $\check{\mathcal{E}}$ acts on the completely mixed state, for the outcome to be positive, we require $(\tau_1^2 + \tau_2^2 + \tau_3^2) \leq 1$. Furthermore, when $\check{\mathcal{E}}$ acts on one of the Pauli-Z eigenstates, we obtain $((\lambda_1 \pm \tau_1)^2 + \tau_2^2 + \tau_3^2) \leq 1$, where the \pm depends on which eigenstate is chosen and whether τ_1 and λ_1 have the same sign. This implies that $(\lambda_1^2 + \tau_1^2 + \tau_2^2 + \tau_3^2) \leq 1$, and similarly for λ_2 and λ_3 (with the Pauli-X and -Y eigenstates). Combining these inequalities and the positivity constraint gives

$$\begin{aligned} \lambda_1^2 + \lambda_3^2 + \lambda_3^2 + 3(\tau_1^2 + \tau_2^2 + \tau_3^2) \leq 3, \\ -(\tau_1^2 + \tau_2^2 + \tau_3^2) \geq -1, \\ \rightarrow (\lambda_1^2 + \lambda_2^2 + \lambda_3^2) + (\tau_1^2 + \tau_2^2 + \tau_3^2) \leq 1. \end{aligned} \quad (\text{C12})$$

Lemma IV.3.—The unital part of a CPTP single-qubit map is always a CPTP map.

Proof.—Lemma C.1 shows that the projection of $\check{\mathcal{E}}$ onto its unital part results in a CP map. So, here we show that this implies that the projection of the map \mathcal{E} onto its unital part results in a CP map.

Because \mathcal{U} and \mathcal{V} are unitaries, their Pauli-Liouville representations have the form

$$\mathcal{U}^{(\text{PL})} = \begin{pmatrix} 1 & \vec{0} \\ \vec{0} & \mathbf{U} \end{pmatrix}, \quad \mathcal{V}^{(\text{PL})} = \begin{pmatrix} 1 & \vec{0} \\ \vec{0} & \mathbf{V} \end{pmatrix}. \quad (\text{C13})$$

So,

$$\mathcal{E}^{(\text{PL})} = \mathcal{U}^{(\text{PL})} \check{\mathcal{E}}^{(\text{PL})} \mathcal{V}^{(\text{PL})} = \begin{pmatrix} 1 & \vec{0} \\ \mathbf{U} \vec{t} & \mathbf{UDV} \end{pmatrix}. \quad (\text{C14})$$

Now suppose $\check{\mathcal{E}}'^{(\text{PL})} = \begin{pmatrix} 1 & \vec{0} \\ 0 & \mathbf{D} \end{pmatrix}$ is a valid CP map. Then,

$$\mathcal{W}^{(\text{PL})} = \mathcal{U}^{(\text{PL})} \check{\mathcal{E}}'^{(\text{PL})} \mathcal{V}^{(\text{PL})} = \begin{pmatrix} 1 & \vec{0} \\ 0 & \mathbf{UDV} \end{pmatrix} \quad (\text{C15})$$

is also a valid CPTP map because the composition of valid quantum maps is always a valid quantum map. However, by Eq. (4.3), \mathcal{W} is equal to \mathcal{E}' , so the unital part of a single-qubit map is always CPTP.

APPENDIX D: BOUNDS ON FIDELITY

Recall that for an operation \mathcal{E} , the χ -matrix representation is

$$\mathcal{E}(\hat{\rho}) = \sum_{i,j} \chi_{i,j}^{\mathcal{E}} \hat{P}_i \hat{\rho} \hat{P}_j. \quad (\text{D1})$$

Because of complete positivity constraints, χ matrix elements satisfy

$$\chi_{i,j}^{\mathcal{E}} \leq \sqrt{\chi_{i,i}^{\mathcal{E}} \chi_{j,j}^{\mathcal{E}}}. \quad (\text{D2})$$

Composing two maps, their χ -matrix representations are

$$\mathcal{A} \circ \mathcal{B}(\hat{\rho}) = \sum_{m,n,k,j} \chi_{m,n}^{\mathcal{A}} \chi_{k,j}^{\mathcal{B}} \hat{P}_m \hat{P}_k \hat{\rho} \hat{P}_j \hat{P}_n. \quad (\text{D3})$$

Let $\sigma_i(m)$ be the index such that $\hat{P}_{\sigma_i(m)} \hat{P}_m = \hat{P}_i$. Then, using the fact that the absolute value is greater than the real or imaginary parts of a complex number, we obtain

$$\begin{aligned} \chi_{i,i}^{\mathcal{A} \circ \mathcal{B}} &= \chi_{i,i}^{\mathcal{A}} \chi_{0,0}^{\mathcal{B}} \\ &\pm \left(2 \sum_{m \neq 0} |\chi_{\sigma_i(m),i}^{\mathcal{A}}| |\chi_{m,0}^{\mathcal{B}}| + \sum_{m,n \neq 0} |\chi_{\sigma_i(m),\sigma_i(n)}^{\mathcal{A}}| |\chi_{m,n}^{\mathcal{B}}| \right). \end{aligned} \quad (\text{D4})$$

Looking at the term $\sum_{m \neq 0} |\chi_{\sigma_i(m),i}^{\mathcal{A}}| |\chi_{m,0}^{\mathcal{B}}|$ and using Eq. (D2) and the Cauchy-Schwarz inequality, we have

$$\begin{aligned} \sum_{m \neq 0} |\chi_{\sigma_i(m),i}^{\mathcal{A}}| |\chi_{m,0}^{\mathcal{B}}| &\leq \sqrt{\sum_{m \neq 0} |\chi_{\sigma_i(m),i}^{\mathcal{A}}|^2 \sum_{m \neq 0} |\chi_{m,0}^{\mathcal{B}}|^2} \\ &\leq \sqrt{\sum_{m \neq 0} \chi_{\sigma_i(m),\sigma_i(m)}^{\mathcal{A}} \chi_{i,i}^{\mathcal{A}} \sum_{m \neq 0} \chi_{m,m}^{\mathcal{B}} \chi_{0,0}^{\mathcal{B}}} \\ &= \sqrt{(1 - \chi_{i,i}^{\mathcal{A}}) \chi_{i,i}^{\mathcal{A}} (1 - \chi_{0,0}^{\mathcal{B}}) \chi_{0,0}^{\mathcal{B}}}. \end{aligned} \quad (\text{D5})$$

Similarly, the term $\sum_{m,n \neq 0} |\chi_{\sigma_i(m),\sigma_i(n)}^{\mathcal{A}}| |\chi_{m,n}^{\mathcal{B}}|$ gives

$$\begin{aligned} \sum_{m,n \neq 0} |\chi_{\sigma_i(m),\sigma_i(n)}^{\mathcal{A}}| |\chi_{m,n}^{\mathcal{B}}| &\leq \sqrt{\sum_{m,n \neq 0} |\chi_{\sigma_i(m),\sigma_i(n)}^{\mathcal{A}}|^2 \sum_{m,n \neq 0} |\chi_{m,n}^{\mathcal{B}}|^2} \\ &\leq \sqrt{\sum_{m,n \neq 0} \chi_{\sigma_i(m),\sigma_i(m)}^{\mathcal{A}} \chi_{\sigma_i(n),\sigma_i(n)}^{\mathcal{A}} \sum_{m,n \neq 0} \chi_{m,m}^{\mathcal{B}} \chi_{n,n}^{\mathcal{B}}} \\ &= (1 - \chi_{i,i}^{\mathcal{A}}) (1 - \chi_{0,0}^{\mathcal{B}}). \end{aligned} \quad (\text{D6})$$

So, we have

$$\begin{aligned} \chi_{i,i}^{\mathcal{A} \circ \mathcal{B}} &= \chi_{i,i}^{\mathcal{A}} \chi_{0,0}^{\mathcal{B}} \pm 2 \sqrt{(1 - \chi_{i,i}^{\mathcal{A}}) \chi_{i,i}^{\mathcal{A}} (1 - \chi_{0,0}^{\mathcal{B}}) \chi_{0,0}^{\mathcal{B}}} \\ &\pm (1 - \chi_{i,i}^{\mathcal{A}}) (1 - \chi_{0,0}^{\mathcal{B}}). \end{aligned} \quad (\text{D7})$$

Setting $i = 0$ gives the desired result.

To see why the lower bound is, in general, not tight, consider Eq. (D4). For the lower bound on $\chi_{i,i}^{\mathcal{A} \circ \mathcal{B}}$, we take all of the terms of the form $\chi_{\sigma_i(m),\sigma_i(n)}^{\mathcal{A}} \chi_{m,n}^{\mathcal{B}}$ and replace them with $-\chi_{\sigma_i(m),\sigma_i(n)}^{\mathcal{A}} |\chi_{m,n}^{\mathcal{B}}|$ because many of these terms have unknown phases, which in the worst case, can have a value -1 . However, when $m = n$, because χ is positive semi-definite, we get terms of the form $\chi_{\sigma_i(m),\sigma_i(m)}^{\mathcal{A}} \chi_{m,m}^{\mathcal{B}} = |\chi_{\sigma_i(m),\sigma_i(m)}^{\mathcal{A}}| |\chi_{m,m}^{\mathcal{B}}|$; thus, we are subtracting terms that should actually be added. However, there is no way to address this issue without obtaining more information about the χ matrix.

APPENDIX E: ORDERING OF ERROR MAPS

Throughout this paper, we chose to describe the noisy maps as the composition of the ideal map and some error map (applied in that order). In other words, the noisy implementation of the map \mathcal{C}_i is expressed as

$$\mathcal{N}_i \circ \mathcal{C}_i, \quad (\text{E1})$$

where \mathcal{N}_i is the error map and \mathcal{C}_i is the ideal Clifford map. This choice can be made without loss of generality, and it has no effect on experimental observations. In other words, we could instead express the implementation of the Clifford \mathcal{C}_i as

$$\mathcal{C}_i \circ \mathcal{N}_i^*, \quad (\text{E2})$$

where \mathcal{N}_i^* is, in general, a different error map. The average fidelity of these noisy maps to \mathcal{C}_i is the same, or, equivalently, \mathcal{N}_i and \mathcal{N}_i^* have the same average fidelity to the identity. However, in general, $\mathcal{N}_i \neq \mathcal{N}_i^*$. Other process metrics are immune to this problem because they

take the error to be additive rather than multiplicative, and so there is no ordering choice to be made or imposed.

If all error maps are identical for either of the conventional choices ($\mathcal{N}_i = \mathcal{N}$ or $\mathcal{N}_i^* = \mathcal{N}^*$), then Eq. (3.1) holds, and small deviations from these cases lead to perturbative corrections that generalize the results in Refs. [9,10]. If the error maps are close to the identity, both perturbative models are likely to be valid, so $\mathcal{N} \approx \mathcal{N}^*$ —the question of which convention is used becomes immaterial. However, if either \mathcal{N} or \mathcal{N}^* is far from the identity, low-order perturbative expansions may not be valid for one of the conventions. Fits to individual RB decays cannot differentiate between these two cases, and the bounds used to isolate the error in \mathcal{E} from \mathcal{N} or \mathcal{N}^* do not depend on this conventional choice, thus, as long as Eq. (3.1) holds for *some* separation of the error and ideal channel.

A problem arises when one attempts to use Lemma IV.2, as, unless $\mathcal{N} \approx \mathcal{N}^*$, the choice of conventions becomes important. The physical regime where, e.g., $\mathcal{N}_i \approx \mathcal{N}$ is precisely the regime where $\mathcal{N}_i \approx \mathcal{N}_i^* \approx \mathcal{I}$, and so this is not likely to be a problem in practice; within the accuracy of the perturbative expansions to Eq. (3.1), the inversion in Lemma IV.2 will be valid, as would a similar inversion taking the error map to occur before the ideal map.

In the more general formal cases where, e.g., $\mathcal{N}_i \approx \mathcal{N}$ but the \mathcal{N}_i^* are very different from each other, there appears to be no way to choose the appropriate convention from individual observations. It may simply be the case that the \mathcal{E}' reconstruction via Lemma IV.2 using one convention is highly unphysical, while the other is physical, indicating which convention should be used. In the absence of this indication of systematic errors, however, one should report both reconstructions or simply choose the worst of the two.

-
- [1] I. L. Chuang and M. A. Nielsen, *Prescription for Experimental Determination of the Dynamics of a Quantum Black Box*, *J. Mod. Opt.* **44**, 2455 (1997).
- [2] C. Stark, *Self-Consistent Tomography of the State-Measurement Gram Matrix*, [arXiv:1209.5737](https://arxiv.org/abs/1209.5737).
- [3] C. Stark, *Global Completeness with Applications to Self-Consistent Quantum Tomography*, [arXiv:1209.6499](https://arxiv.org/abs/1209.6499).
- [4] C. Stark, *Simultaneous Estimation of Dimension, States and Measurements: Computation of Representative Density Matrices and POVMs*, [arXiv:1210.1105](https://arxiv.org/abs/1210.1105).
- [5] S. T. Merkel, J. M. Gambetta, J. A. Smolin, S. Poletto, A. D. Córcoles, B. R. Johnson, C. A. Ryan, and M. Steffen, *Self-Consistent Quantum Process Tomography*, *Phys. Rev. A* **87**, 062119 (2013).
- [6] Y. S. Weinstein, T. F. Havel, J. Emerson, N. Boulant, M. Saraceno, S. Lloyd, and D. G. Cory, *Quantum Process Tomography of the Quantum Fourier Transform*, *J. Chem. Phys.* **121**, 6117 (2004).
- [7] J. Emerson, R. Alicki, and K. Zyczkowski, *Scalable Noise Estimation with Random Unitary Operators*, *J. Opt. B: Quantum Semiclassical Opt.* **7**, S347 (2005).
- [8] E. Knill, D. Leibfried, R. Reichle, J. Britton, R. B. Blakestad, J. D. Jost, C. Langer, R. Ozeri, S. Seidelin, and D. J. Wineland, *Randomized Benchmarking of Quantum Gates*, *Phys. Rev. A* **77**, 012307 (2008).
- [9] E. Magesan, J. M. Gambetta, and J. Emerson, *Scalable and Robust Randomized Benchmarking of Quantum Processes*, *Phys. Rev. Lett.* **106**, 180504 (2011).
- [10] E. Magesan, J. M. Gambetta, and J. Emerson, *Characterizing Quantum Gates via Randomized Benchmarking*, *Phys. Rev. A* **85**, 042311 (2012).
- [11] J. P. Gaebler, A. M. Meier, T. R. Tan, R. Bowler, Y. Lin, D. Hanneke, J. D. Jost, J. P. Home, E. Knill, D. Leibfried, and D. J. Wineland, *Randomized Benchmarking of Multiqubit Gates*, *Phys. Rev. Lett.* **108**, 260503 (2012).
- [12] E. Magesan, J. M. Gambetta, B. R. Johnson, C. A. Ryan, J. M. Chow, S. T. Merkel, M. P. da Silva, G. A. Keefe, M. B. Rothwell, T. A. Ohki, M. B. Ketchen, and M. Steffen, *Efficient Measurement of Quantum Gate Error by Interleaved Randomized Benchmarking*, *Phys. Rev. Lett.* **109**, 080505 (2012).
- [13] J. A. Holbrook, D. W. Kribs, and R. Laflamme, *Noiseless Subsystems and the Structure of the Commutant in Quantum Error Correction*, *Quantum Inf. Process.* **2**, 381 (2003).
- [14] I. Bengtsson and K. Zyczkowski, *Geometry of Quantum States: An Introduction to Quantum Entanglement* (Cambridge University Press, Cambridge, England, 2008).
- [15] A. Jamiołkowski, *Rep. Math. Phys.* **3**, 275 (1972).
- [16] M.-D. Choi, *Linear Algebra Appl.* **10**, 285 (1975).
- [17] K. Kraus, *States, Effects and Operations, Fundamental Notions of Quantum Theory* (Springer, New York, 1983).
- [18] K. Blum, *Density Matrix Theory and Applications* (Plenum Press, New York, 1981).
- [19] D. W. Leung, Ph.D. thesis, Stanford University (2000).
- [20] C. King and M. B. Ruskai, *Minimal Entropy of States Emerging from Noisy Quantum Channels*, *IEEE Trans. Inf. Theory* **47**, 192 (2001).
- [21] T. F. Havel, *The Real Density Matrix*, *Quantum Inf. Process.* **1**, 511 (2002).
- [22] B. Rahn, A. C. Doherty, and H. Mabuchi, *Exact Performance of Concatenated Quantum Codes*, *Phys. Rev. A* **66**, 032304 (2002).
- [23] M. Silva, E. Magesan, D. W. Kribs, and J. Emerson, *Scalable Protocol for Identification of Correctable Codes*, *Phys. Rev. A* **78**, 012347 (2008).
- [24] J. M. Chow, J. M. Gambetta, A. D. Córcoles, S. T. Merkel, J. A. Smolin, C. Rigetti, S. Poletto, G. A. Keefe, M. B. Rothwell, J. R. Rozen, M. B. Ketchen, and M. Steffen, *Universal Quantum Gate Set Approaching Fault-Tolerant Thresholds with Superconducting Qubits*, *Phys. Rev. Lett.* **109**, 060501 (2012).
- [25] M. Horodecki, P. Horodecki, and R. Horodecki, *General Teleportation Channel, Singlet Fraction, and Quasidistribution*, *Phys. Rev. A* **60**, 1888 (1999).
- [26] M. A. Nielsen, *A Simple Formula for the Average Gate Fidelity of a Quantum Dynamical Operation*, *Phys. Lett. A* **303**, 249 (2002).
- [27] C. Dankert, R. Cleve, J. Emerson, and E. Livine, *Exact and Approximate Unitary 2-designs and Their Application to Fidelity Estimation*, *Phys. Rev. A* **80**, 012304 (2009).

- [28] In full generality, p corresponds to an eigenvalue of the map resulting from randomizing \mathcal{E} by conjugation with elements of either the full unitary group or the Clifford group [20,22,23,31]. The eigenvalue interpretation can be used to more clearly see how independence of the estimate from the initial and final states comes about, and it can also be more naturally generalized to cases where the randomizing operations are elements of the Pauli group [23]. Randomization over more general operations can also be considered [32].
- [29] D. Gottesman, The Heisenberg Representation of Quantum Computers, in Group22: *Proceedings of the XXII International Colloquium on Group Theoretical Methods in Physics*, edited by S. P. Corney, R. Delbourgo, and P. D. Jarvis (International Press, Cambridge, MA, 1999), pp. 32–43.
- [30] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, *Mixed-State Entanglement and Quantum Error Correction*, *Phys. Rev. A* **54**, 3824 (1996).
- [31] J. Emerson, M. Silva, O. Moussa, C. Ryan, M. Laforest, J. Baugh, D. G. Cory, and R. Laflamme, *Symmetrized Characterization of Noisy Quantum Processes*, *Science* **317**, 1893 (2007).
- [32] S. D. Bartlett, T. Rudolph, and R. W. Spekkens, *Reference Frames, Superselection Rules, and Quantum Information*, *Rev. Mod. Phys.* **79**, 555 (2007).
- [33] O. Moussa, M. P. da Silva, C. A. Ryan, and R. Laflamme, *Practical Experimental Certification of Computational Quantum Gates Using a Twirling Procedure*, *Phys. Rev. Lett.* **109**, 070504 (2012).
- [34] For \mathcal{N} chosen at random to have unitary dilations that are Haar distributed, $(\mathcal{N}')^{-1}$ appears to exist with probability of 1, so it appears that the requirement that \mathcal{N} be close to \mathcal{I} can be significantly weakened.
- [35] R. A. Horn and C. R. Johnson, *Matrix Analysis* (Cambridge University Press, Cambridge, England, 1985).
- [36] T. Moroder, M. Kleinmann, P. Schindler, T. Monz, O. Gühne, and R. Blatt, *Certifying Systematic Errors in Quantum Experiments*, *Phys. Rev. Lett.* **110**, 180401 (2013).
- [37] M. J. Bremner, R. Jozsa, and D. J. Shepherd, *Classical Simulation of Commuting Quantum Computations Implies Collapse of the Polynomial Hierarchy*, *Proc. R. Soc. A* **467**, 459 (2010).
- [38] Here, we take a circuit to mean a composition of quantum maps on n qubits, and the depth to correspond to the number of maps composed.
- [39] S. Aaronson and D. Gottesman, *Improved Simulation of Stabilizer Circuits*, *Phys. Rev. A* **70**, 052328 (2004).
- [40] P. O. Boykin, T. Mor, M. Pulver, V. Roychowdhury, and F. Vatan, *Proceedings of the 40th Annual Symposium on Foundations of Computer Science* (Society Press, Washington, DC, 1999), pp. 486–494.
- [41] In Ref. [12], E is given as the minimum of two functions. However, in almost all realistic cases, this second function never minimizes. In fact, our bounds are always better than the second function, so we have left it out.
- [42] In practice, this sequence length can be estimated roughly from the rough rate of decay in experiments without an accurate estimate for any of the model parameters.
- [43] W. van Dam and M. Howard, *Bipartite Entangled Stabilizer Mutually Unbiased Bases as Maximum Cliques of Cayley Graphs*, *Phys. Rev. A* **84**, 012117 (2011).
- [44] M. Van den Nest, *Simulating Quantum Computers with Probabilistic Methods*, *Quantum Inf. Comput.* **11**, 784 (2011).
- [45] M. Van den Nest, *A Monomial Matrix Formalism to Describe Quantum Many-Body States*, *New J. Phys.* **13**, 123004 (2011).
- [46] M. B. Ruskai, S. Szarek, and E. Werner, *An Analysis of Completely-Positive Trace-Preserving Maps on M_2* , *Linear Algebra Appl.* **347**, 159 (2002).